了解Firepower威胁防御（FMC管理）上的FQDN功能

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 功能概述
- 6.3之前的版本如何

配置

- 网络图
- 架构 — 重要点
- 配置步骤

验证

故障排除

- 收集FMC故障排除文件
- 常见问题/错误消息
- 部署失败
- 建议的故障排除步骤
- 没有激活的FQDN

问题解答

简介

本文档介绍如何将FQDN功能（从v6.3.0开始）配置到Firepower管理中心(FMC)和Firepower威胁防御(FTD)。

先决条件

要求

思科建议您先了解下列主题的相关知识：

- Firepower 管理中心

使用的组件

本文档中的信息基于以下软件版本：

- 运行软件版本6.3.0的Cisco Firepower威胁防御(FTD)虚拟
- 运行软件版本6.3.0的Firepower管理中心虚拟(vFMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍由软件版本6.3.0引入到Firepower管理中心(FMC)和Firepower威胁防御(FTD)的完全限定域名(FQDN)功能的配置。此功能存在于思科自适应安全设备(ASA)中，但不在FTD的初始软件版本中。

在配置FQDN对象之前，请确保满足以下条件：

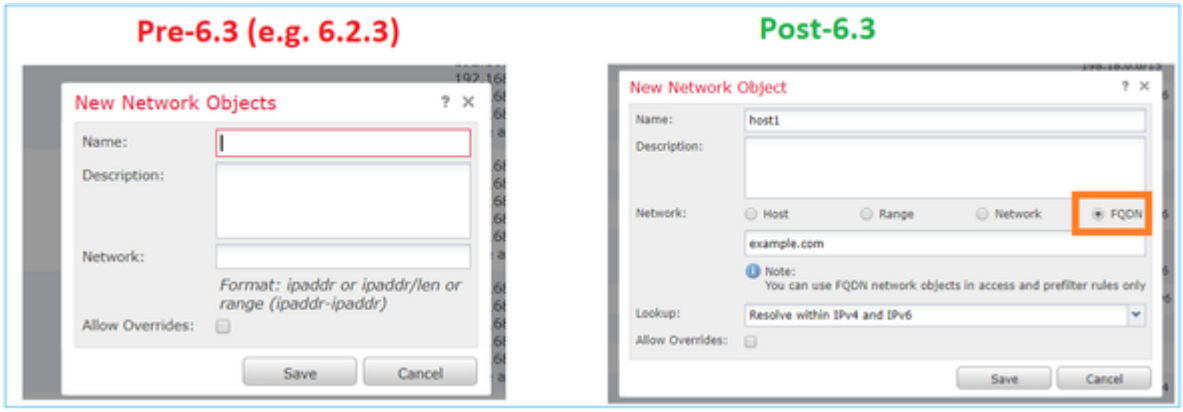
- Firepower管理中心必须运行版本6.3.0或更高版本。它可以是物理或虚拟
- Firepower威胁防御必须运行版本6.3.0或更高版本。它可以是物理或虚拟

功能概述

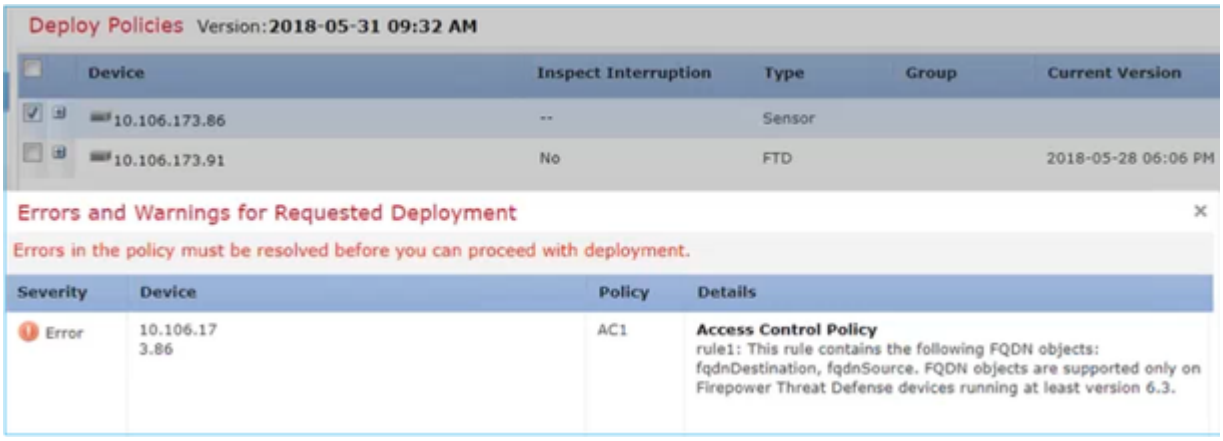
此功能将FQDN解析为IP地址，并在访问控制规则或预过滤器策略引用后使用后者过滤流量。

6.3之前的版本如何

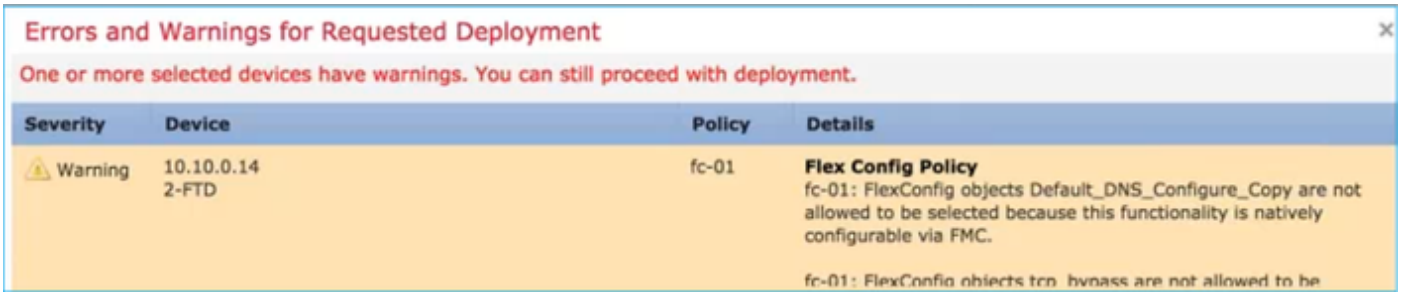
- 运行早于6.3.0版本的FMC和FTD无法配置FQDN对象。



- 如果FMC运行版本6.3或更高版本，但FTD运行早于6.3的版本，则策略的部署将显示以下错误：

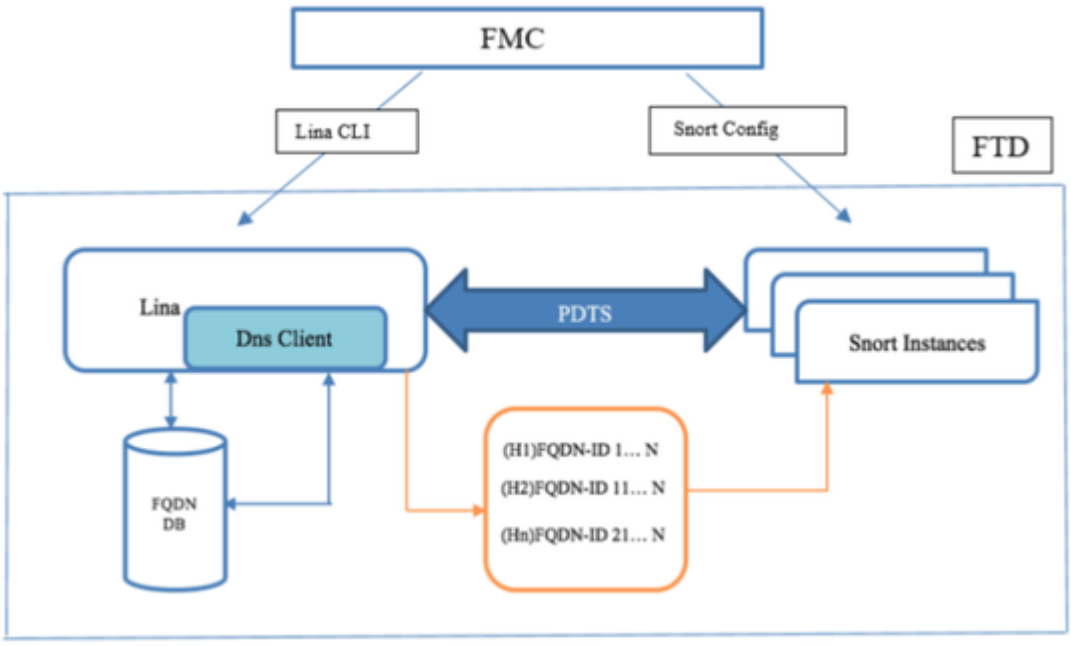


- 此外，如果通过FlexConfig配置DNS对象，则会出现以下警告：



配置

网络图



架构 — 重要点

- DNS解析（DNS到IP）发生在LINA中。
- LINA将映射存储在其数据库中。
- 基于每个连接，此映射从LINA发送到snort。
- FQDN的解析独立于高可用性或集群配置。

配置步骤

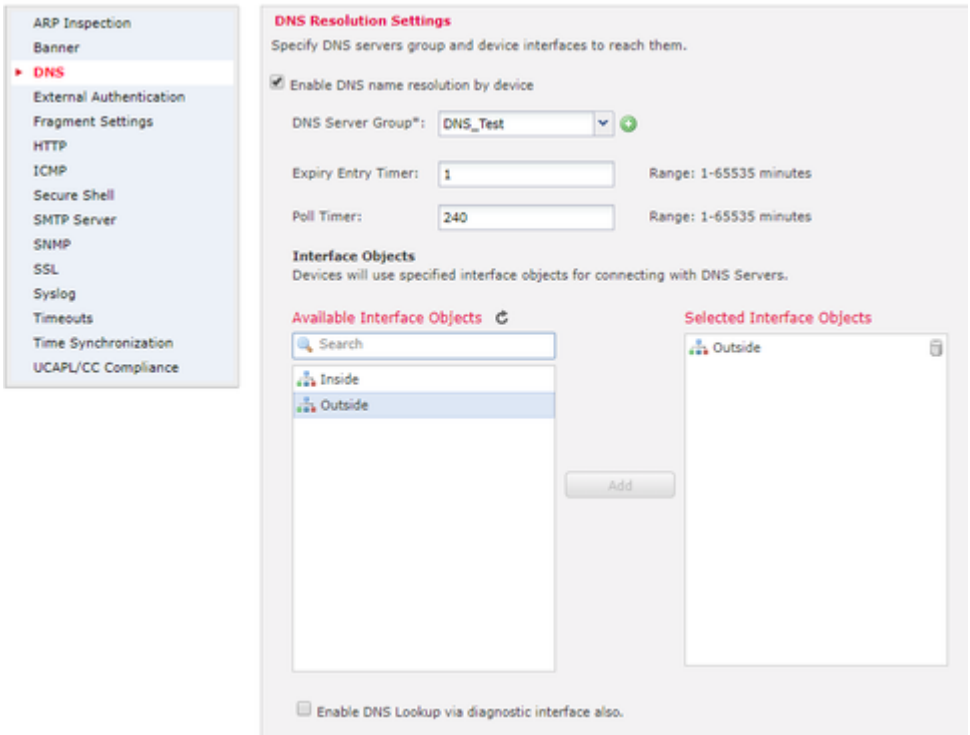
步骤1.配置DNS服务器组对象。



- DNS服务器组名称不能超过63个字符。

- 在多域部署中，对象名称在域层次结构中必须是唯一的。系统可以识别与当前域中无法查看的对象名称的冲突。
- 默认域（可选）用于附加到非完全限定的主机名。
- 默认的Retries和Timeout值已预填充。
    - Retries — 系统未收到响应时重试DNS服务器列表的次数（从0到10）。默认值为 2。
    - Timeout — 另一个尝试连接下一个DNS服务器之前经过的秒数（1到30）。默认时间为 2 秒钟。每次系统重试服务器列表时，此超时值会加倍。
- 输入要加入此组的DNS服务器。这可以是IPv4或IPv6格式，以逗号分隔值。
- DNS服务器组用于解析在Platform Settings中配置的一个或多个接口对象。
- 支持REST API for DNS Server Group object CRUD。

步骤2.配置DNS（平台设置）。



- （可选）修改到期条目计时器和轮询计时器值（以分钟为单位）：

到期条目计时器选项指定在其生存时间(TTL)到期后从DNS查找表中删除已解析FQDN的IP地址的时间限制。删除条目需要重新编译表，因此频繁删除会增加设备上的进程负载。此设置实际上扩展了TTL。

轮询计时器选项指定时间限制，超过此时间后，设备将查询DNS服务器以解析在网络对象组中定义

的FQDN。FQDN会在轮询计时器过期或解析的IP条目的TTL过期时定期解析，以先发生者为准。

- （可选）从可用列表中选择所需的接口对象，然后将其添加到Selected Interface Objects列表，并确保可以通过所选接口访问DNS服务器：

对于Firepower威胁防御6.3.0设备，如果未选择任何接口，并且禁用诊断接口进行DNS查找，则DNS解析将通过包含诊断接口的任何接口进行（应用dnsdomain-lookup any命令）。

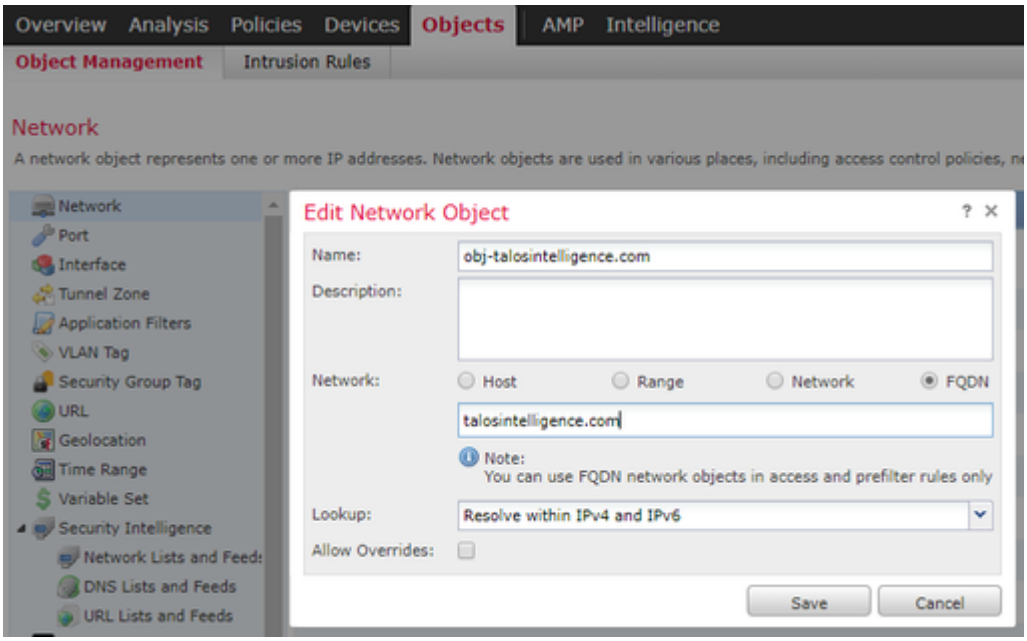
如果未指定任何接口，并且未在诊断接口上启用DNS查找，则FTD将使用数据路由表来确定接口。如果没有匹配项，则使用管理路由表。

- （可选）选中Enable DNS Lookup via the diagnostic interface also复选框。

如果启用，Firepower威胁防御使用所选数据接口和诊断接口进行DNS解析。请务必在Devices > Device Management > edit device > Interfaces页面上为诊断接口配置IP地址。

步骤3.配置对象网络FQDN

导航到对象(Objects)>对象管理(Object Management)，并在网络对象内选择FQDN选项。

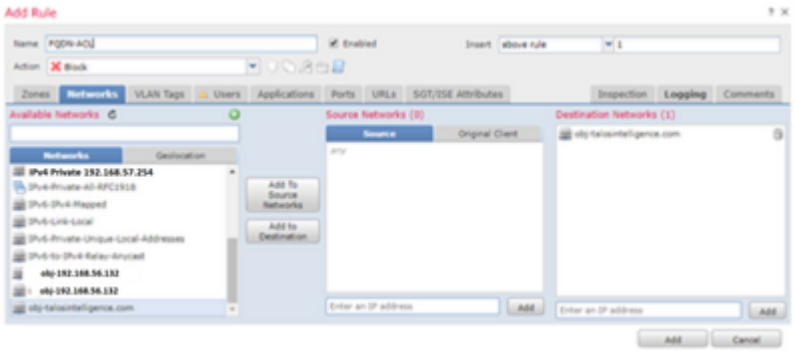


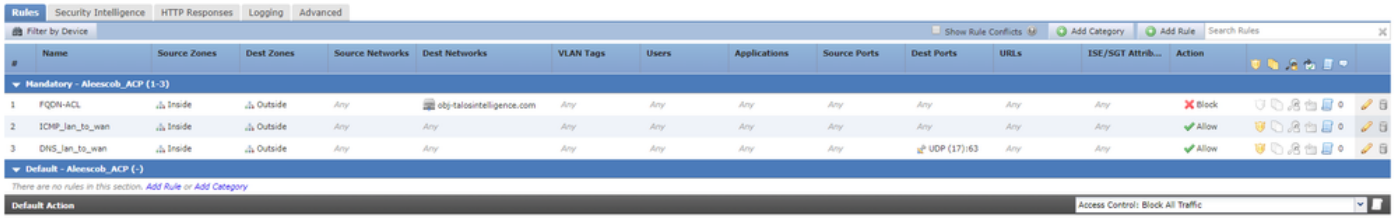
- 用户创建FQDN对象时生成32位唯一ID。
- 此ID从FMC推送到LINA和Snort。
- 在LINA中，此ID与对象关联。

- 在snort中，此ID与包含该对象的访问控制规则相关联。

步骤4.创建访问控制规则

使用之前的FQDN对象创建规则并部署策略：





注意：在访问控制策略中部署FQDN对象时，将发生FQDN解析的第一个实例

验证

使用本部分可确定配置能否正常运行。

- 这是部署FQDN之前的FTD初始配置：

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

- 这是FQDN部署后的配置：

```
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
```

- 以下是FQDN对象在LINA中的显示方式：

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

- 如果已部署FQDN，则这是FQDN访问列表在LINA中的显示方式：

```
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)中的情况如下：

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



注意：在此方案中，由于FQDN对象用于目标，因此将其列为dstfqdn。

- 如果选中show dns和show fqdn命令，您会发现该功能已开始解析tallosintelligence的IP:

```
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

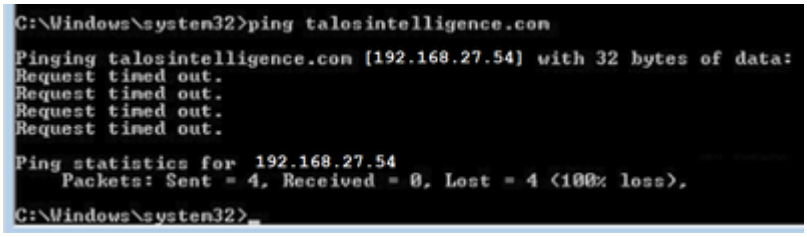
ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

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
```

- 如果您在LINA中选中show access-list，您会注意到每个解析和命中计数所对应的扩展条目：

```
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
```

- 如图所示，对talosintelligence.com执行ping操作失败，因为访问列表中存在FQDN的匹配项。FTD阻止ICMP数据包后，DNS解析就发挥了作用。



- 从LINA对以前发送的ICMP数据包的命中计数：

```
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请求在入口接口被捕获并显示丢弃：

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端口59396 unreachable 2:18:04:12.322126 192.168.56.132 > 172.31.4.161 icmp:回应请求3:18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp:应答 4:18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp:回应请求5:18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp:应答6:18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp:回应请求7:18:04:14.475424 172.31.4.161> 192.168.56.132 icmp:应答8:18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp:回应请求9:18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp:回应应答10:18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp:回应请求 11:18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp:回应请求12:18:04:35.711480 192.168.56.132 > 192.168.27.54 icmp:回应请求13:18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp:echo request aleescob# sho cap asp |在192.168.27.54 162中 ：18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp:回应请求165:18:04:30.704355 192.168.56.132 > 192.168.27.54 icmp:回应请求168:18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp:回应请求176:18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp:回送请求。

- 以下是跟踪查找以下ICMP数据包之一的方式：

```
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
```

- 如果访问控制规则的操作为Allow，则这是system support firewall-engine-debug的输出示例

```
> 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
```

- 当FQDN部署为预过滤器(Fastpath)的一部分时，它是在ngfw中的显示方式。规则：

```
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.
```

- 从LINA的角度和跟踪数据包来看：

```
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:
```

故障排除

1. 从FMC配置

- 验证策略和DNS服务器设置是否配置正确。
- 验证部署是否成功。

2. 在FTD上部署检查

- 运行show dns和show access-list以查看是否已解析FQDN和AC规则是否已展开。
- 运行show run object network，并记下与对象关联的ID（例如，X表示源）。
- 运行show fqdn id X以检查FQDN是否已正确解析为源IP。
- 验证ngfw.rules文件是否具有以FQDN ID X作为源的AC规则。
- 运行system support firewall-engine-debug并检查Snort判定。

收集FMC故障排除文件

所需的所有日志都从FMC故障排除中收集。要从FMC收集所有重要日志，请从FMC GUI运行故障排除。否则，从FMC Linux提示符运行sf_troubleshoot.pl。如果您发现问题，请向思科技术支持中心(TAC)提交FMC故障排除和报告。

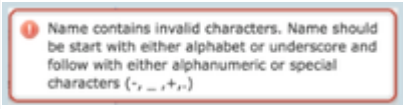
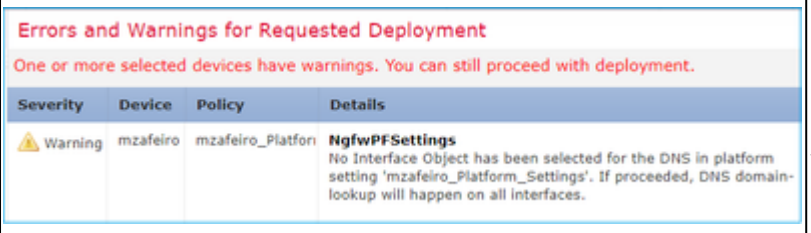
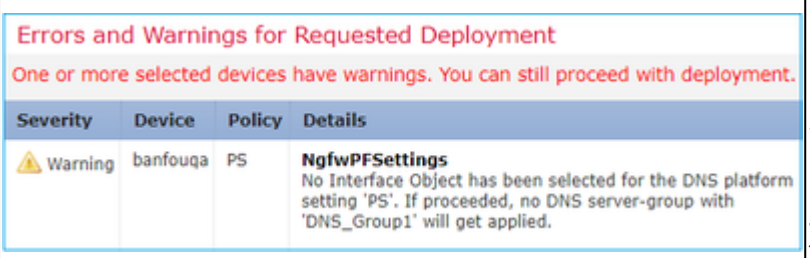
FMC日志

日志文件名称/位置	目的
/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log	所有API调用
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	所有API调用
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	CLI生成日志
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	Tomcat日志
/var/log/mojo.log	Mojo日志
	CSM和DC之间的REST呼叫

/var/log/CSMAgent.log	
/var/log/action_queue.log	DC的操作队列日志

常见问题/错误消息

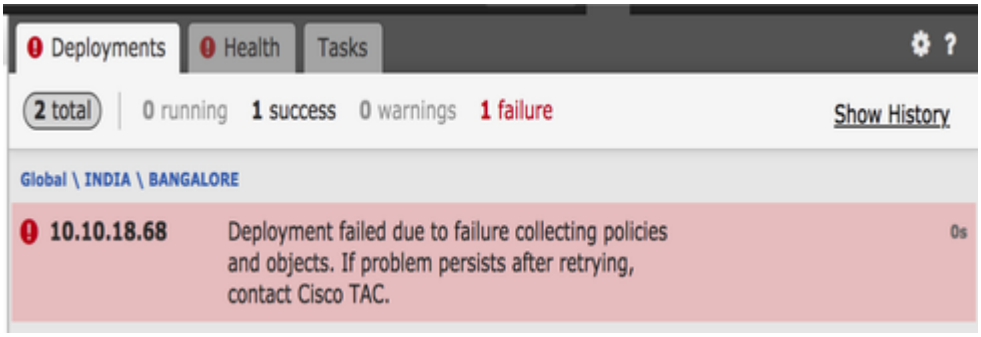
以下是FQDN和DNS服务器组对象和DNS设置的UI中显示的错误/警告：

错误/警告	场景	描述
 名称包含无效字符。名称必须以字母或下划线开头，之后可以是字母数字字符，也可以是特殊字符。(-、_、+、.)	用户配置错误的名称。	用户将获知允许的字符和最大范围。
 默认域值无效	用户配置了错误的域名。	系统将通知用户允许的字符和最大范围。
 在平台设置“mzafeiro_Platform_Settings”中未为DNS选择接口对象。如果继续，DNS域名查找很快就会在所有接口上发生	用户没有选择任何接口进行域查找。 对于6.3之后的设备	系统会警告用户，DNS 服务器组CLI即将应用 到所有接口。
 在平台设置“mzafeiro_Platform_Settings”中未为DNS选择	用户没有选择任何接口进行域查找。 对于6.2.3设备	警告用户 DNS 服务器组CLI不是 已生成。

接口对象。如果继续，则不会很快应用任何具有“DNS”的DNS服务器组		

部署失败

在除AC策略/预过滤器策略之外的策略中使用FQDN时，可能会发生此错误，并且显示在FMC UI中：



建议的故障排除步骤

1)打开日志文件：/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2)检查验证消息，类似于：

“配置的网络无效。在设备[DeviceNames]上配置的网络[NetworksContainingFQDN]引用FQDN"



3)建议的操作：

验证上述一个或多个策略是否已配置有包含FQDN对象的FQDN或组，并在删除这些对象后重新尝试部署。

a)身份策略

b)包含应用于AC策略的FQDN的变量集

没有激活的FQDN

系统可以通过FTD CLI显示下一条：

> show dns INFO:没有激活的FQDN

在应用具有定义fqdn的对象之前，不会激活DNS。应用对象后，将解决此问题。

问题解答

问:使用FQDN的Packet Tracer是排除故障的有效测试吗？
A：是，您可以将fqdn选项与packet-tracer一起使用。

问:FQDN规则多久更新一次服务器的IP地址？
A：取决于DNS响应的TTL值。TTL值到期后，将使用新的DNS查询再次解析FQDN。
这也取决于DNS服务器配置中定义的Poll Timer属性。当轮询DNS计时器过期或解析的IP条目的TTL过期时（以先到者为准），会定期解析FQDN规则。

问:这是否适用于轮询DNS?
A：轮询DNS可以无缝运行，因为此功能在FMC/FTD上使用DNS客户端运行，轮询DNS配置在DNS服务器端。

问:TTL DNS值是否有限制？
A：如果DNS响应包含0 TTL，则FTD设备会添加60秒。在这种情况下，TTL值至少为60秒。

问:因此，默认情况下，FTD将保留默认值60秒？
A：用户始终可以在DNS服务器上使用过期条目计时器设置覆盖TTL。

问:它如何与任播DNS响应交互操作？例如，DNS服务器可以根据地理位置为请求者提供不同的IP地址。是否可以请求FQDN的所有IP地址？像Unix上的dig命令吗？
A：是，如果FQDN能够解析多个IP地址，则所有地址都会推送到设备，AC规则会相应地扩展。

问:是否计划包括预览选项，显示任何部署更改之前已推送的命令？
A：这是通过Flex配置提供的Preview配置选项的一部分。预览已经存在，但是在Flex Config策略中隐藏了预览。我们计划将其移出，使其具有通用性。

问:FTD上的哪个接口用于执行DNS查找？
A：它是可配置的。当未配置任何接口时，FTD上的所有命名接口均启用DNS查找。

问:每个托管NGFW是否单独执行自己的DNS解析和FQDN IP转换，即使对于具有相同FQDN对象的所有托管NGFW都应用相同的访问策略？
A：Yes.

问:是否可以清除DNS缓存，以便对FQDN ACL进行故障排除？
A：可以，您可以在设备上执行clear dns和clear dns-hosts cache命令。

问:何时触发FQDN解析？
A：当FQDN对象部署在AC策略中时，会发生FQDN解析。

问:是否可以仅清除单个站点的缓存？
A：Yes.如果您知道域名或IP地址，则可以清除它，但从ACL的角度来看，没有这样的命令。例如，使用clear dns host agni.tejas.com命令，可以使用关键字host逐个主机清除主机上的缓存，如dns host agni.tejas.com。

问:是否可以使用通配符，如*.microsoft.com?
A：否。FQDN必须以数字或字母开始和结束。内部字符只能是字母、数字和连字符。

问:名称解析是在交流编译时执行，而不是在第一次或后续请求时执行？如果您的TTL较低（小于AC编译时间、快速流量或其他因素），是否会丢失某些IP地址？
A：部署AC策略后立即进行名称解析。根据TTL时间到期，续订会继续进行。

问:是否计划能够处理Microsoft Office 365云IP地址(XML)列表？
A：目前不支持此功能。

问:SSL策略中是否提供FQDN?
A：暂时不会（软件版本6.3.0）。仅AC策略的源网络和目标网络支持FQDN对象。

问:是否有任何历史日志可以提供有关已解析的FQDN的信息？例如LINA系统日志。
A：要排除特定目标的FQDN故障，您可以使用system support trace命令。跟踪显示数据包的FQDN ID。您可以比较该ID进行故障排除。您还可以启用系统日志消息746015,746016以跟踪

FQDN dns解析活动。

问:设备是否使用已解析的IP在连接表中记录FQDN?
A：要排除特定目标的FQDN故障，您可以使用system support trace命令，其中跟踪显示数据包的FQDN ID。您可以比较该ID进行故障排除。计划将来在FMC上的事件查看器中安装FQDN日志。

问:FQDN规则功能有什么缺点？

A：如果在经常更改IP地址的目标上使用FQDN规则(例如：TTL到期时间为零的互联网服务器)，工作站可能最终拥有不再与FTD DNS缓存匹配的新IP地址。因此，它与ACP规则不匹配。默认情况下，FTD在从DNS响应收到的TTL到期时间的基础上增加1分钟，且不能设置为零。在这些情况下，强烈建议使用最适合此使用案例的URL过滤功能。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。