FQDN-Funktion auf FirePOWER Threat Defense (FMC-verwaltet)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der FQDN-Funktion (ab Version 6.3.0) für das Firepower Management Center (FMC) und die Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Management Center

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Firepower Threat Defense (FTD) Virtual mit Softwareversion 6.3.0
- FirePOWER Management Center Virtual (vFMC) mit Softwareversion 6.3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird die Konfiguration der FQDN-Funktion (Fully Qualified Domain Name) beschrieben, die mit der Softwareversion 6.3.0 für Firepower Management Center (FMC) und Firepower Threat Defense (FTD) eingeführt wurde.

Diese Funktion ist in der Cisco Adaptive Security Appliance (ASA) enthalten, wurde jedoch in den ersten Softwareversionen von FTD nicht verwendet.

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie FQDN-Objekte konfigurieren:

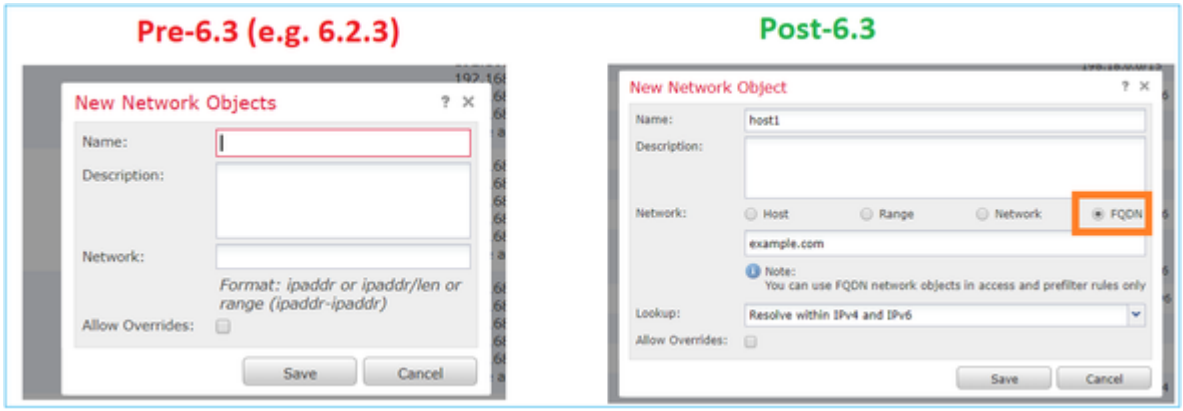
- Das Firepower Management Center muss Version 6.3.0 oder höher ausführen. Sie kann physisch oder virtuell sein.
- Firepower Threat Defense muss Version 6.3.0 oder höher ausführen. Sie kann physisch oder virtuell sein.

Funktionsüberblick

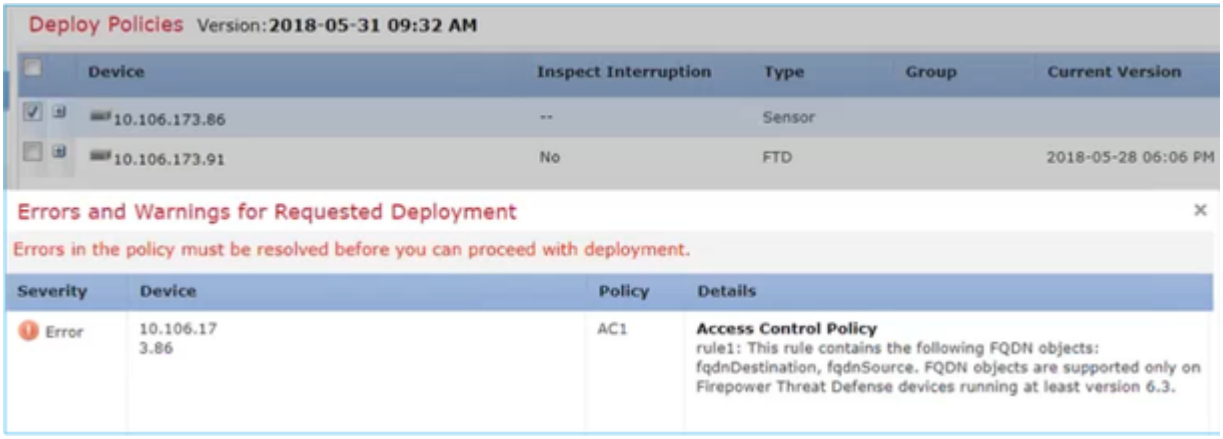
Diese Funktion löst einen FQDN in eine IP-Adresse auf und verwendet diese, um Datenverkehr zu filtern, wenn eine Zugriffskontrollregel oder eine Vorfilterrichtlinie darauf verweist.

Was ist mit älteren Versionen als 6.3?

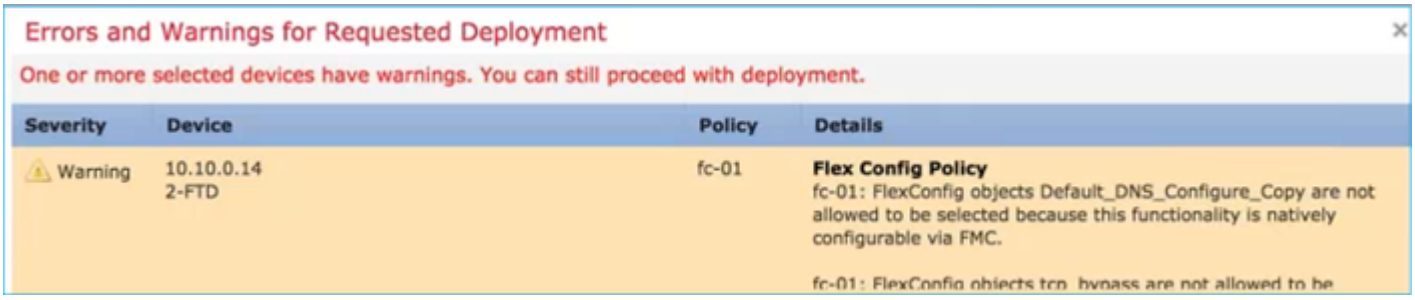
- FMC und FTD, die eine frühere Version als 6.3.0 ausführen, können keine FQDN-Objekte konfigurieren.



- Wenn FMC Version 6.3 oder höher ausführt, FTD jedoch eine frühere Version als 6.3 ausführt, wird bei der Bereitstellung einer Richtlinie folgender Fehler angezeigt:

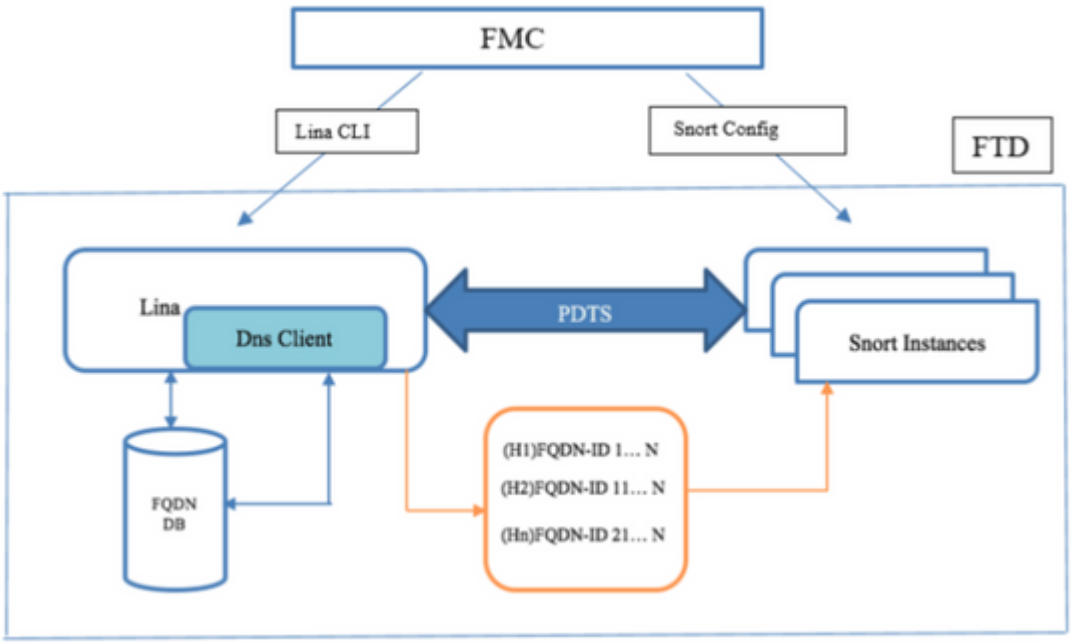


- Wenn Sie ein DNS-Objekt über FlexConfig konfigurieren, wird diese Warnung angezeigt:



Konfigurieren

Netzwerkdiagramm



Architektur - Wichtige Punkte

- DNS-Auflösung (DNS zu IP) erfolgt in LINA
- LINA speichert die Zuordnung in seiner Datenbank
- Diese Zuordnung wird pro Verbindung von LINA an snort gesendet.
- Die Auflösung von FQDN erfolgt unabhängig von Hochverfügbarkeit oder Cluster-Konfiguration

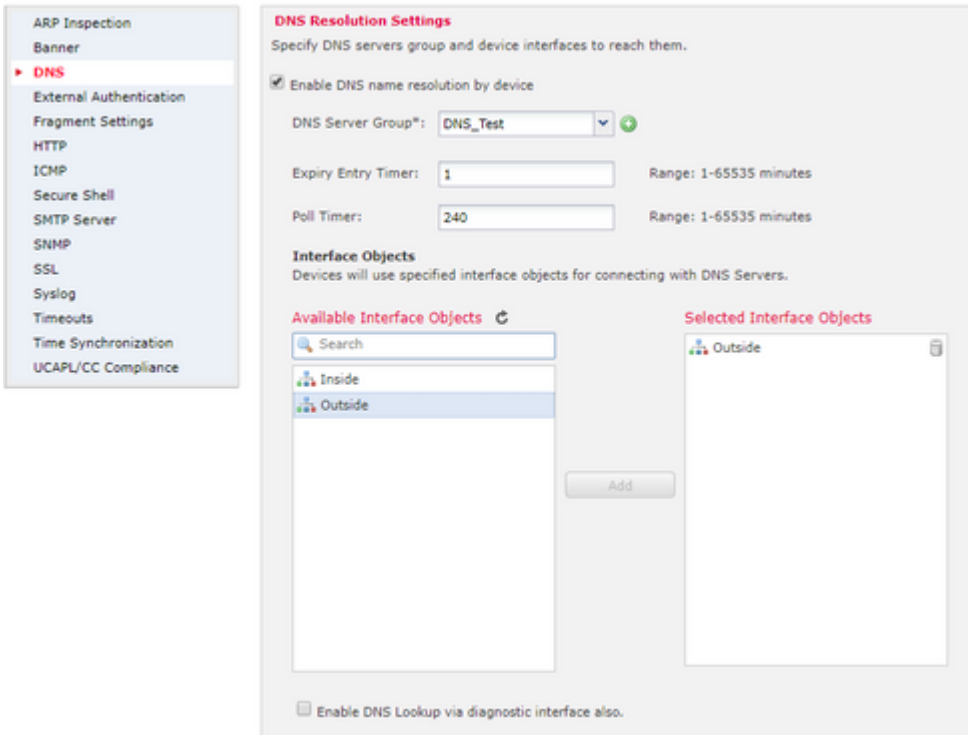
Konfigurationsschritte

Schritt 1: Konfigurieren Sie das DNS-Server-Gruppenobjekt.

â€ƒ

- Der Name der DNS-Servergruppe darf 63 Zeichen nicht überschreiten.
- In einer Bereitstellung mit mehreren Domänen müssen Objektnamen innerhalb der Domänenhierarchie eindeutig sein. Das System kann einen Konflikt mit dem Namen eines Objekts identifizieren, das in der aktuellen Domäne nicht angezeigt werden kann.
- Die Standarddomäne (optional) wird verwendet, um die Hostnamen anzuhängen, die nicht vollständig qualifiziert sind.
- Die Standardwerte für Wiederholungen und Zeitüberschreitung sind vorausgefüllt.
    - Retries (Wiederholungen): Die Anzahl der Wiederholungen der Liste der DNS-Server von 0 bis 10, wenn das System keine Antwort erhält. Der Standardwert ist 2.
    - Timeout - Die Anzahl der Sekunden von 1 bis 30, bevor ein weiterer Versuch zum nächsten DNS-Server unternommen wird. Der Standardwert ist 2 Sekunden. Jedes Mal, wenn das System die Serverliste erneut versucht, verdoppelt sich diese Zeitüberschreitung.
- Geben Sie die DNS-Server ein, die dieser Gruppe angehören sollen. Dabei kann es sich entweder um ein IPv4- oder IPv6-Format als kommagetrennte Werte handeln.
- Die DNS-Servergruppe wird für die Auflösung mit dem Schnittstellenobjekt oder den in den Plattformeinstellungen konfigurierten Objekten verwendet.
- REST-API für DNS-Servergruppenobjekt-CRUD wird unterstützt

Schritt 2: DNS konfigurieren (Plattformeinstellungen)



- (Optional) Ändern Sie die Werte für den Timer für Ablauftermine und den Abfragetimer in Minuten:

Die Timer-Option für den Ablauftermin gibt das Zeitlimit an, nach dem die IP-Adresse eines aufgelösten FQDN aus der DNS-Lookup-Tabelle entfernt wird, nachdem die TTL (Time-to-Live) abgelaufen ist. Um einen Eintrag entfernen zu können, muss die Tabelle neu kompiliert werden, sodass häufige Entfernungen die Prozesslast auf dem Gerät erhöhen können. Durch diese Einstellung wird die TTL praktisch erweitert.

Die Option "Polling Timer" gibt das Zeitlimit an, nach dem das Gerät den DNS-Server abfragt, um den FQDN aufzulösen, der in einer Netzwerkobjektgruppe definiert wurde. Ein FQDN wird regelmäßig aufgelöst, entweder wenn der Abfragezeitgeber abgelaufen ist oder wenn die TTL des aufgelösten IP-Eintrags abgelaufen ist, je nachdem, welches Ereignis zuerst eintritt.

- (Optional) Wählen Sie die erforderlichen Schnittstellenobjekte aus der Liste "Verfügbare Schnittstellen" aus, fügen Sie sie der Liste "Ausgewählte Schnittstellenobjekte" hinzu, und stellen Sie sicher, dass der DNS-Server über die ausgewählten Schnittstellen erreichbar ist:

Wenn für Firepower Threat Defense 6.3.0-Geräte keine Schnittstellen ausgewählt sind und die Diagnoseschnittstelle für die DNS-Suche deaktiviert ist, erfolgt die DNS-Auflösung über jede Schnittstelle, die die Diagnoseschnittstelle enthält (der Befehl dnsdomain-lookup any wird angewendet).

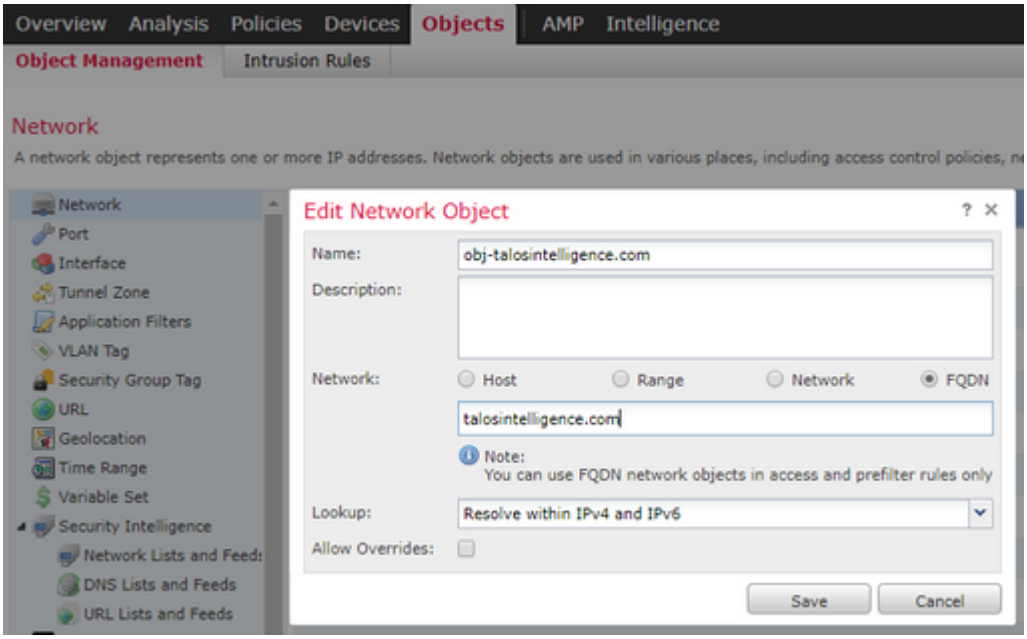
Wenn Sie keine Schnittstellen angeben und die DNS-Suche auf der Diagnoseschnittstelle nicht aktivieren, bestimmt die FTD die Schnittstelle anhand der Data Routing Table. Wird keine Übereinstimmung gefunden, wird die Management-Routing-Tabelle verwendet.

- (Optional) Aktivieren Sie das Kontrollkästchen DNS-Suche auch über die Diagnoseschnittstelle aktivieren.

Wenn diese Option aktiviert ist, verwendet Firepower Threat Defense sowohl die ausgewählten Datenschnittstellen als auch die Diagnoseschnittstelle für DNS-Auflösungen. Stellen Sie sicher, dass Sie auf der Seite Devices (Geräte) > Device Management (Geräteverwaltung) > Edit Device (Gerät) > Interfaces (Schnittstellen) eine IP-Adresse für die Diagnoseschnittstelle konfigurieren.

Schritt 3: Konfigurieren des FQDN des Objektnetzwerks

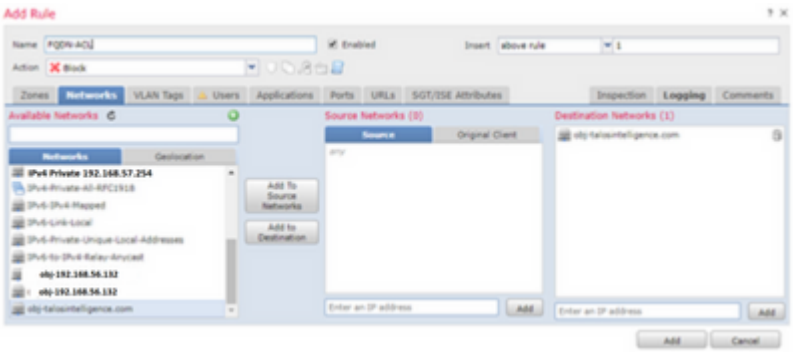
Navigieren Sie zu Objekte > Objektverwaltung. Wählen Sie innerhalb eines Netzwerkobjekts die Option FQDN aus.



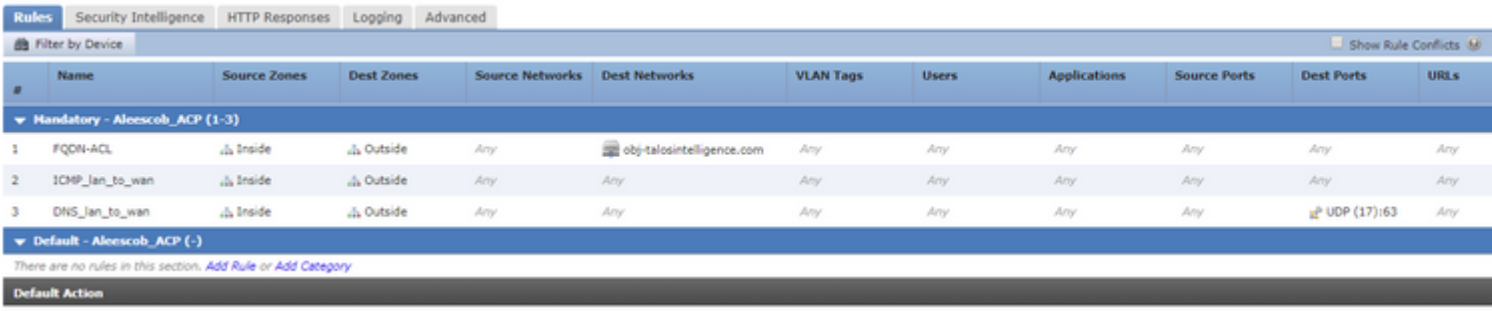
- Eine eindeutige 32-Bit-ID wird generiert, wenn der Benutzer ein FQDN-Objekt erstellt.
- Diese ID wird von FMC an LINA und Snort weitergeleitet.
- In LINA ist diese ID dem Objekt zugeordnet.
- Im Snort ist diese ID der Zugriffskontrollregel zugeordnet, die dieses Objekt enthält.

Schritt 4: Erstellen einer Zugriffskontrollregel

Erstellen Sie eine Regel mit dem vorherigen FQDN-Objekt, und stellen Sie die Richtlinie bereit:



â€ƒ



Hinweis: Die erste Instanz der FQDN-Auflösung tritt auf, wenn das FQDN-Objekt in einer Zugriffssteuerungsrichtlinie bereitgestellt wird.

Überprüfung

In diesem Abschnitt können Sie überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Dies ist die FTD-Erstkonfiguration vor der Bereitstellung von FQDN:

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

- Dies ist die Konfiguration nach der FQDN-Bereitstellung:

```
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
```

- So sieht das FQDN-Objekt in LINA aus:

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

- Wenn die FQDN-Zugriffsliste bereits bereitgestellt ist, sieht sie in LINA folgendermaßen aus:

```
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
```

- So sieht es in Snort (ngfw.rules) aus:

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

Hinweis: Da in diesem Szenario das FQDN-Objekt für das Ziel verwendet wurde, wird es als dstfqdn aufgeführt.

- Wenn Sie show dns und show fqdn-Befehle aktivieren, können Sie feststellen, dass die Funktion begonnen hat, die IP-Adresse für tallosintelligence aufzulösen:

```
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
```

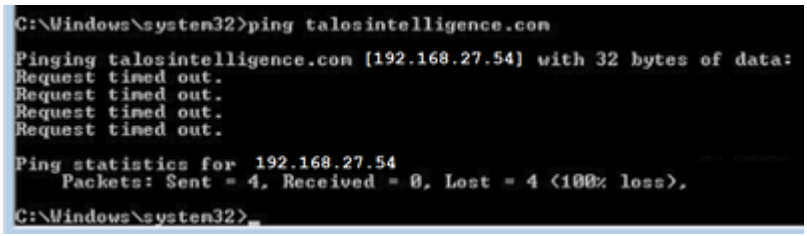
```
ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

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:DB
```

- Wenn Sie das Kontrollkästchen show access-list in LINA aktivieren, werden die erweiterten Einträge für jede Auflösung und Trefferanzahl angezeigt:

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintell
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- Wie im Bild gezeigt, schlägt ein Ping zu talosintelligence.com fehl, da in der Zugriffsliste ein Treffer für den FQDN vorhanden ist. Die DNS-Auflösung hat funktioniert, da das ICMP-Paket vom FTD blockiert wird.



â€ƒ

- Trefferanzahl von LINA für zuvor gesendete ICMP-Pakete:

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintellig
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- ICMP-Anforderungen werden erfasst und in der Eingangsschnittstelle als verworfen angezeigt:

aleescob# show cap in 13 erfasste Pakete 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 > 19 2.168.56.132 icmp: echo reply 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: echo request 5: 18:04:13.462149 17 2.31.4.161 > 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 > 17 2.31.4.161 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: Echoanfrage 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 192.168.56.1 32 > 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: Echoanfrage 168: 18:04:35.711556 192.168.56.132 > 192.1 68.27.54 icmp: echo request 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp: echo request

- So sucht die Ablaufverfolgung nach einem der folgenden ICMP-Pakete:

```
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.com
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
```

- Wenn die Aktion für die Zugriffskontrollregel Allow lautet, ist dies ein Beispiel für die Ausgabe von 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 wit
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:2
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
```

- Wenn der FQDN als Teil eines Vorfilters (Fastpath) bereitgestellt wird, sieht er in "ngfw.rules" folgendermaßen aus:

```
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.
```

- Vom LINA-Standpunkt aus mit einem verfolgten Paket:

```
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-l
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:
```

Fehlerbehebung

1. Konfiguration von FMC

- Überprüfen Sie, ob die Richtlinien und die DNS-Servereinstellungen richtig konfiguriert sind.
- Überprüfen der erfolgreichen Bereitstellung

2. Aktivieren auf FTD

- Führen Sie show dns und show access-list aus, um festzustellen, ob FQDN aufgelöst und AC-Regeln erweitert wurden.
- Führen Sie show run object network aus, und notieren Sie sich die ID des Objekts (z. B. X als Quelle).
- Führen Sie show fqdn id X aus, um zu überprüfen, ob der FQDN in die Quell-IP aufgelöst wurde.
- Überprüfen Sie, ob die Datei "ngfw.rules" eine AC-Regel mit der FQDN-ID X als Quelle enthält.
- Führen Sie den Systemsupport firewall-engine-debug aus und überprüfen Sie das Snort-Verdict.

FMC-Fehlerbehebungsdateien sammeln

Alle erforderlichen Protokolle wurden bei einer FMC-Fehlerbehebung erfasst. Um alle wichtigen Protokolle vom FMC zu erfassen, führen Sie eine Fehlerbehebung über die FMC-GUI aus. Führen Sie andernfalls von einer FMC Linux-Eingabeaufforderung aus sf_troubleshoot.pl aus. Wenn Sie ein Problem finden, senden Sie ein FMC Troubleshoot mit Ihrem Bericht an das Cisco Technical Assistance Center (TAC).

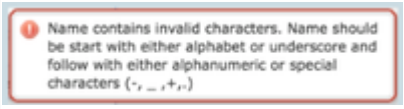
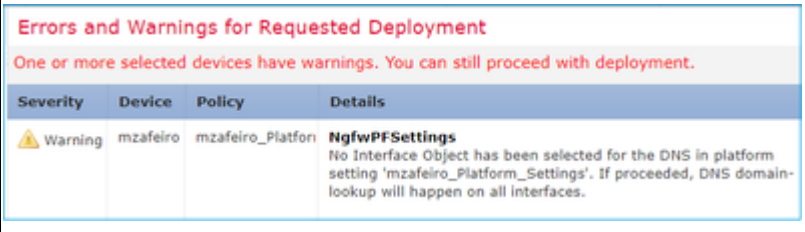
FMC-Protokolle

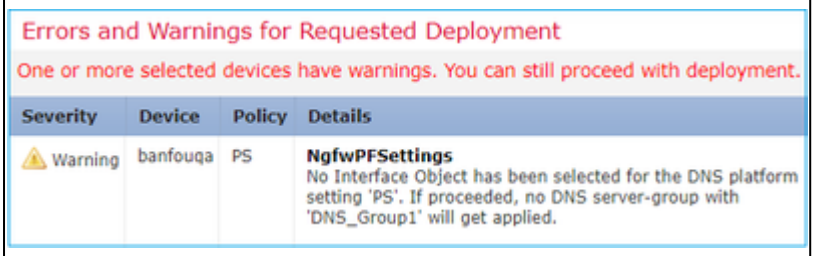
Name/Speicherort der Protokolldatei	Zweck
`/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log`	Alle API-Aufrufe
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	Alle API-Aufrufe
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	CLI-Generierungsprotokolle

`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Tomcat-Protokolle
`/var/log/mojo.log`	Mojo Logs
`/var/log/CSMAgent.log`	REST-Anrufe zwischen CSM und RZ
`/var/log/action_queue.log`	Aktionswarteschlangen-Protokoll des Rechenzentrums

Häufige Probleme/Fehlermeldungen

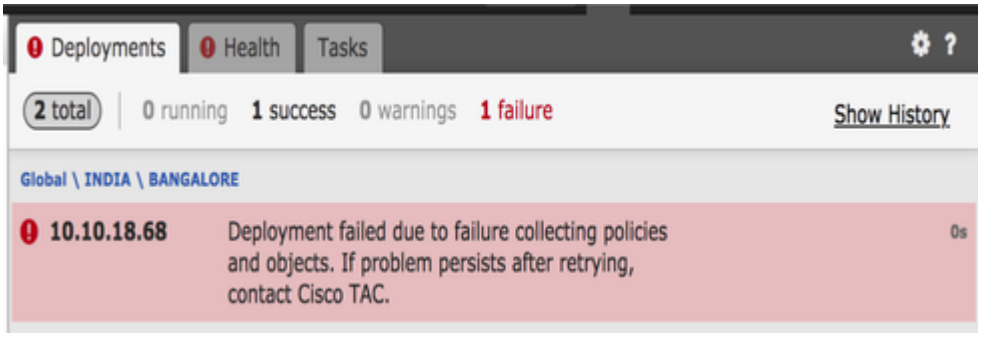
Dies sind die Fehler/Warnungen, die in der Benutzeroberfläche für das FQDN- und DNS-Servergruppenobjekt und die DNS-Einstellungen angezeigt werden:

Fehler/Warnung	Szenario	Beschreibung
 Der Name enthält ungültige Zeichen. Namen müssen entweder mit einem Buchstaben oder einem Unterstrich beginnen und danach entweder mit alphanumerischen Zeichen oder mit Sonderzeichen. (-,_,+,)	Benutzer Konfiguration falscher Namen	Der Benutzer wird über die erlaubten Zeichen und maximaler Bereich.
 Ungültiger Standard-Domänenwert	Benutzer konfiguriert falschen Domänennamen	Der Benutzer wird über die zulässigen Zeichen und den maximalen Bereich informiert.
 In der Plattformeinstellung "mzafeiro_Platform_Settings" wurde kein Schnittstellenobjekt für den DNS ausgewählt.	Benutzer wählt keine Schnittstelle für die Domänensuche aus Für Geräte nach 6.3	Der Benutzer wird darauf hingewiesen, dass der DNS Servergruppen-CLI wird bald angewendet an alle

Wenn der Vorgang fortgesetzt wird, erfolgt die DNS-Domänensuche bald auf allen Schnittstellen.		Schnittstellen.
 In der Plattformeinstellung "mzafeiro_Platform_Settings" wurde kein Schnittstellenobjekt für den DNS ausgewählt. Wird fortgefahren, wird in Kürze keine DNS-Servergruppe mit "DNS" angewendet.	Benutzer wählt keine Schnittstelle für die Domänensuche aus Für ein Gerät der Version 6.2.3	Benutzer wird gewarnt dass der DNS Servergruppen-CLI ist nicht generiert.

Bereitstellungsfehler

Wenn ein FQDN in einer anderen Richtlinie als der Richtlinie für Wechselstromrichtlinien/Vorfilter verwendet wird, kann dieser Fehler auftreten und in der FMC-Benutzeroberfläche angezeigt werden:



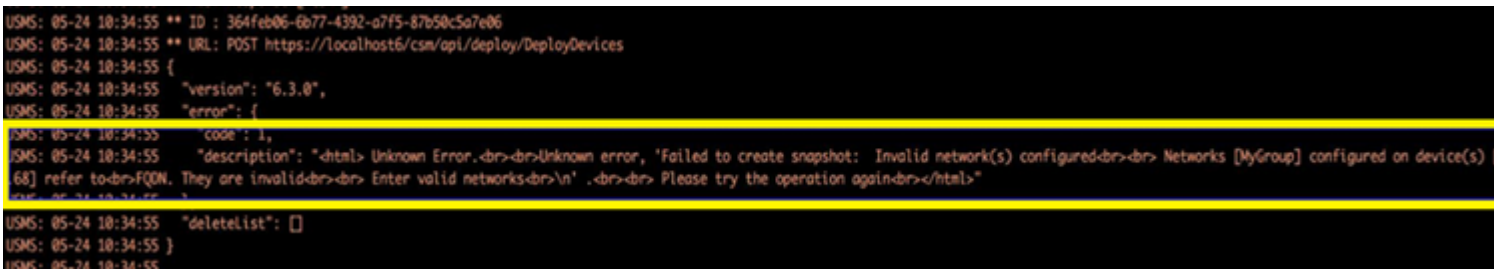
Empfohlene Schritte zur Fehlerbehebung

1) Öffnen Sie die Protokolldatei: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Überprüfen Sie die Validierungsmeldung ähnlich:

"Ungültige(s) konfigurierte(s) Netzwerk(e). Netzwerke [NetworksContainingFQDN], die auf den Geräten konfiguriert sind[DeviceNames], verweisen auf FQDN"

â€ƒ



â€ƒ

3) Vorgeschlagene Maßnahmen:

Überprüfen Sie, ob eine oder mehrere der unten genannten Richtlinien bereits mit einem FQDN oder einer Gruppe konfiguriert sind, die ein oder mehrere FQDN-Objekte enthält, und wiederholen Sie die Bereitstellung derselben, nachdem diese Objekte entfernt wurden.

a) Identitätsrichtlinie

b) Variablensätze, die einen FQDN enthalten, der auf eine AC-Richtlinie angewendet wird

Kein aktivierter FQDN

Das System kann über die FTD-CLI den nächsten Befehl anzeigen:

> show dns INFO: kein aktivierter FQDN

Der DNS wird erst aktiviert, wenn ein Objekt mit einem definierten fqdn angewendet wurde. Nachdem ein Objekt angewendet wurde, wird es aufgelöst.

Fragen und Antworten

F: Ist der Packet-Tracer mit FQDN ein gültiger Test zur Fehlerbehebung?
A: Ja, Sie können die Option fqdn mit Packet-Tracer verwenden.

Frage: Wie oft aktualisiert die FQDN-Regel die IP-Adresse des Servers?
A: Dies hängt vom TTL-Wert der DNS-Antwort ab. Nach Ablauf des TTL-Werts wird der FQDN mit einer neuen DNS-Abfrage wieder aufgelöst.
Dies hängt auch vom Umfrage-Timer-Attribut ab, das in der DNS-Serverkonfiguration definiert ist. Die FQDN-Regel wird regelmäßig aufgelöst, wenn der DNS-Timer für die Abfrage abgelaufen ist oder wenn die TTL des aufgelösten IP-Eintrags abgelaufen ist, je nachdem, welcher Fall zuerst eintritt.

F: Funktioniert dies für Round-Robin-DNS?
A: Round-Robin-DNS funktioniert nahtlos, da diese Funktion auf dem FMC/FTD unter Verwendung eines DNS-Clients funktioniert und die Round-Robin-DNS-Konfiguration auf der Seite des DNS-Servers erfolgt.

Frage: Gibt es eine Beschränkung für DNS-Werte mit niedriger TTL?
A: Wenn eine DNS-Antwort mit 0 TTL geliefert wird, fügt das FTD-Gerät 60 Sekunden hinzu. In diesem Fall beträgt der TTL-Wert mindestens 60 Sekunden.

F: Standardmäßig behält die FTD den Standardwert von 60 Sekunden bei?
A: Der Benutzer kann die TTL mit der Einstellung "Expire Entry Timer" (Timer für abgelaufene Einträge) auf dem DNS-Server immer überschreiben.

F: Wie funktioniert es mit Anycast DNS-Antworten? DNS-Server können beispielsweise unterschiedliche IP-Adressen bereitstellen, je nachdem, wo sich die Anfragen befinden. Ist es möglich, alle IP-Adressen für einen FQDN anzufordern? Gefällt Ihnen der Befehl "dig" unter Unix?
A: Ja, wenn FQDN mehrere IP-Adressen auflösen kann, werden alle an das Gerät gesendet, und die AC-Regel wird entsprechend erweitert.

Frage: Gibt es Pläne für eine Vorschaufunktion, die anzeigt, dass die Befehle vor einer Änderung der Bereitstellung übertragen werden?

A: Dies ist Teil der Option "**Preview config"**, die über Flex config zur Verfügung steht. Die Vorschau ist bereits vorhanden, aber in der Flex Config-Richtlinie ausgeblendet. Es gibt einen Plan, es zu verschieben und es generisch zu machen.

F: Welche Schnittstelle der FTD wird für die DNS-Suche verwendet?
A: Es ist konfigurierbar. Wenn keine Schnittstellen konfiguriert sind, werden alle benannten Schnittstellen in FTD für die DNS-Suche aktiviert.

F: Führt jede verwaltete NGFW ihre eigene DNS-Auflösung und FQDN-IP-Umwandlung separat durch, selbst wenn auf alle NGFWs mit demselben FQDN-Objekt die gleiche Zugriffsrichtlinie angewendet wird?
A: Ja.

Frage: Kann der DNS-Cache für FQDN-ACLs gelöscht werden, um eine Fehlerbehebung zu ermöglichen?
A: Ja, Sie können die Befehle **clear dns** und **clear dns-hosts cache** auf dem Gerät ausführen.

F: Wann genau wird die FQDN-Auflösung ausgelöst?
A: Die FQDN-Auflösung erfolgt, wenn das FQDN-Objekt in einer AC-Richtlinie bereitgestellt wird.

F: Ist es möglich, den Cache nur für einen einzigen Standort zu löschen?
A: Ja. Wenn Sie den Domänennamen oder die IP-Adresse kennen, können Sie sie löschen. Es gibt jedoch keinen Befehl, der aus Sicht der Zugriffskontrollliste erforderlich ist. Beispielsweise ist der Befehl **clear dns host agni.tejas.com** vorhanden, um den Cache auf Host-Basis mit dem Schlüsselwort host wie in **dns host agni.tejas.com** zu löschen.

Frage: Ist es möglich, Platzhalter wie *.microsoft.com zu verwenden?
A: Nein. FQDN muss mit einer Ziffer oder einem Buchstaben beginnen und enden. Nur Buchstaben, Ziffern und Bindestriche sind als interne Zeichen zulässig.

F: Wird die Namensauflösung zur Zeit der AC-Kompilierung und nicht zur Zeit der ersten oder nachfolgenden Anfragen durchgeführt? Können einige IP-Adressen verpasst werden, wenn die TTL niedrig ist (weniger als AC-Kompilierungszeit, Fast-Flux oder etwas Anderes)?
A: Die Namensauflösung erfolgt, sobald die AC-Richtlinie bereitgestellt wird. Nach Ablauf der TTL-Zeit erfolgt die Verlängerung.

Frage: Gibt es Pläne für die Verarbeitung der Microsoft Office 365 Cloud-IP-Adressliste (XML)?
A: Dies wird derzeit nicht unterstützt.

Frage: Ist FQDN in der SSL-Richtlinie verfügbar?
A: Derzeit nicht (Softwareversion 6.3.0). FQDN-Objekte werden im Quell- und Zielnetzwerk nur für die AC-Richtlinie unterstützt.

Frage: Gibt es Verlaufsprotokolle, die Informationen zu aufgelösten FQDNs bereitstellen können? Wie zum Beispiel LINA Syslogs.
A: Um den FQDN an einem bestimmten Ziel zu beheben, können Sie den Befehl **system support trace** verwenden. Die Ablaufverfolgungen zeigen die FQDN-ID des Pakets an. Sie können die ID zur Fehlerbehebung vergleichen. Sie können auch die Syslog-Meldungen 746015 und 746016 aktivieren, um die FQDN-DNS-Auflösungsaktivität zu verfolgen.

F: Protokolliert das Gerät FQDN in der Verbindungstabelle mit aufgelöster IP?
A: Um den FQDN an einem bestimmten Ziel zu beheben, können Sie den Befehl **system support trace** verwenden, wobei die Traces die FQDN-ID des Pakets anzeigen. Sie können die ID zur Fehlerbehebung vergleichen. Es ist geplant, künftig FQDN-Protokolle in der Ereignisanzeige auf FMC bereitzustellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.