Comprendre la fonctionnalité FQDN de Firepower Threat Defense (gérée par FMC)

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Présentation des fonctionnalités
  - Et les versions antérieures à la version 6.3 ?
- Configurer
  - Diagramme du réseau
  - Architecture - Points saillants
  - Configuration Steps
- Vérifier
- Dépannage
  - Collecte des fichiers de dépannage FMC
  - Problèmes courants/Messages d'erreur
  - Échec du déploiement
  - Étapes de dépannage recommandées
  - Aucun FQDN activé
- Q&R

Introduction

Ce document décrit la configuration de la fonctionnalité FQDN (à partir de la version 6.3.0) vers Firepower Management Center (FMC) et Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Centre de gestion Firepower

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Threat Defense (FTD) Virtual, qui exécute la version logicielle 6.3.0
- Firepower Management Center Virtual (vFMC) qui exécute la version logicielle 6.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit la configuration de la fonctionnalité FQDN (Fully Qualified Domain Name) introduite par la version logicielle 6.3.0 dans Firepower Management Center (FMC) et Firepower Threat Defense (FTD).

Cette fonctionnalité est présente dans l'appareil de sécurité adaptatif Cisco (ASA), mais elle ne figurait pas dans les versions logicielles initiales de FTD.

Assurez-vous que ces conditions sont remplies avant de configurer les objets FQDN :

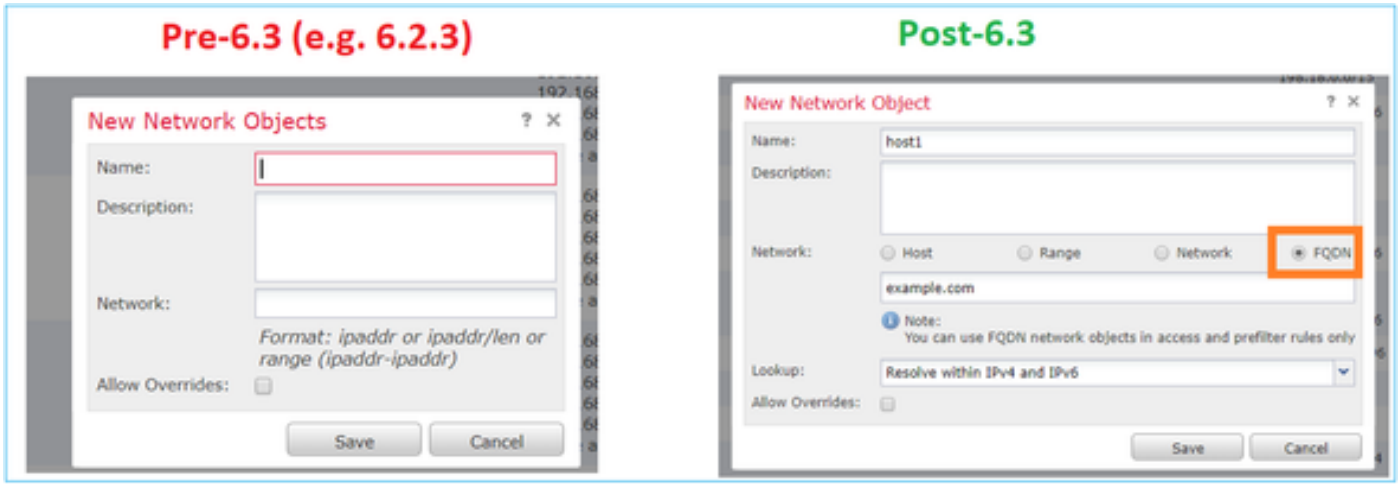
- Firepower Management Center doit exécuter la version 6.3.0 ou ultérieure. Il peut être physique ou virtuel
- Firepower Threat Defense doit exécuter la version 6.3.0 ou ultérieure. Il peut être physique ou virtuel

Présentation des fonctionnalités

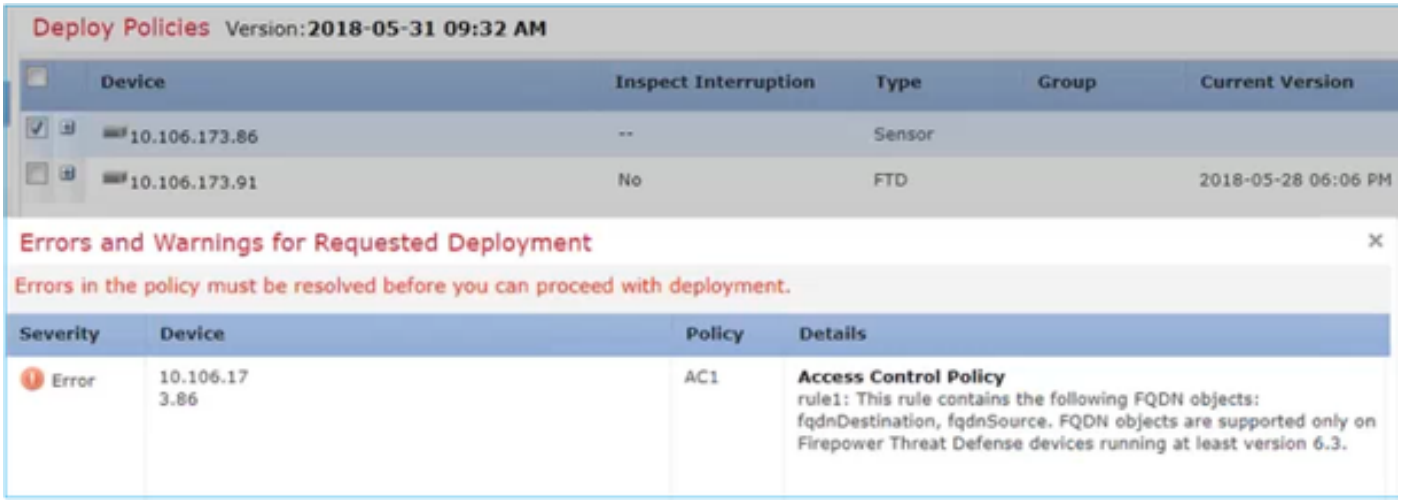
Cette fonctionnalité résout un nom de domaine complet en adresse IP et utilise cette dernière pour filtrer le trafic lorsqu'elle est référencée par une règle de contrôle d'accès ou une stratégie de préfiltrage.

Et les versions antérieures à la version 6.3 ?

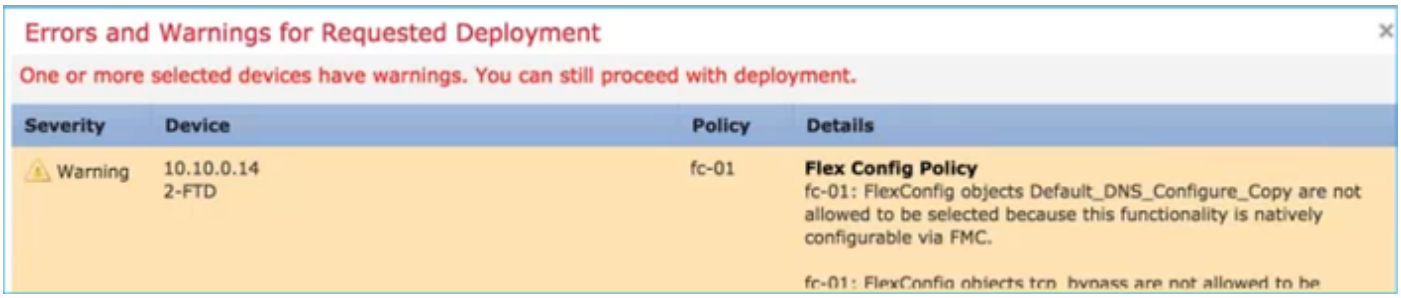
- FMC et FTD qui exécutent une version antérieure à 6.3.0 ne peuvent pas configurer d'objets FQDN.



- Dans le cas où FMC exécute la version 6.3 ou ultérieure, mais que FTD exécute une version antérieure à la version 6.3, le déploiement d'une stratégie affiche cette erreur :

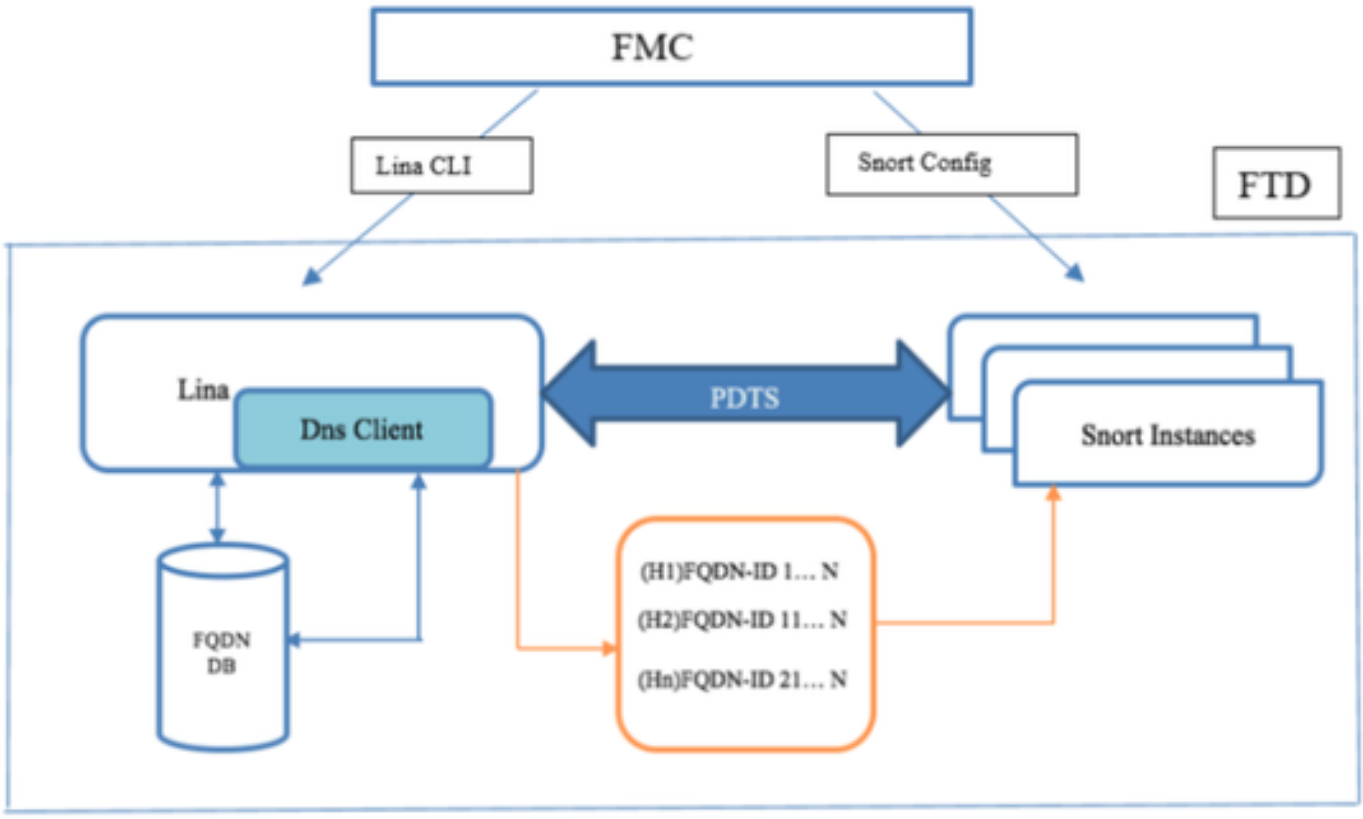


- En outre, si vous configurez un objet DNS via FlexConfig, cet avertissement apparaît :



Configurer

Diagramme du réseau

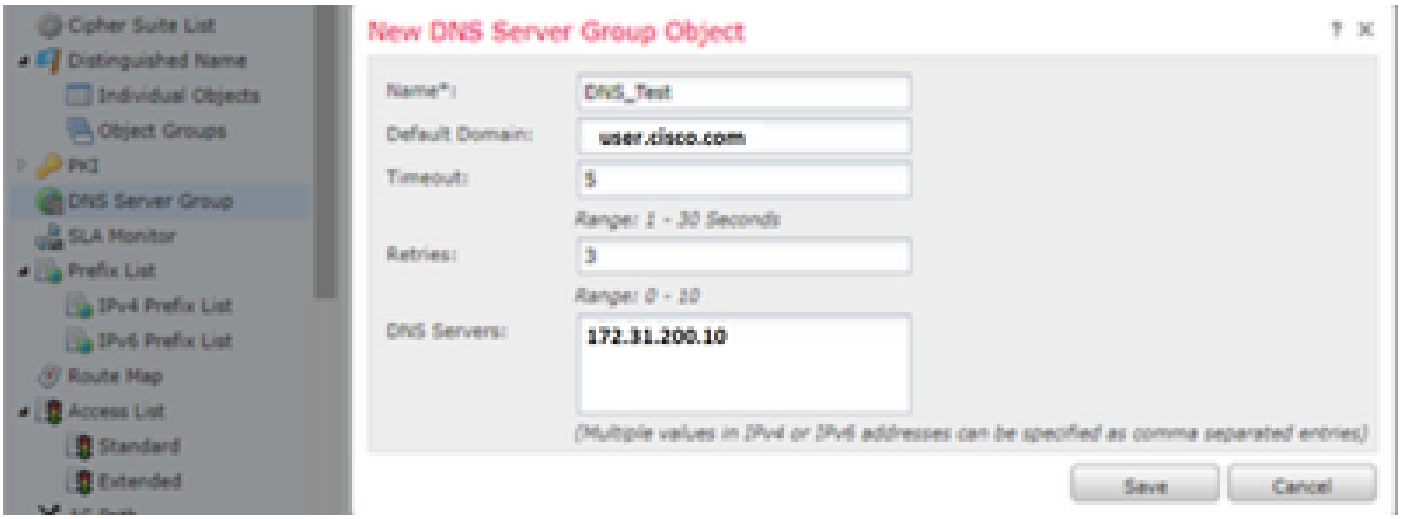


Architecture - Points saillants

- La résolution DNS (DNS vers IP) se produit dans LINA
- LINA stocke le mappage dans sa base de données
- Sur une base par connexion, ce mappage est envoyé de LINA à Snort
- La résolution du nom de domaine complet s'effectue indépendamment de la haute disponibilité ou de la configuration de cluster

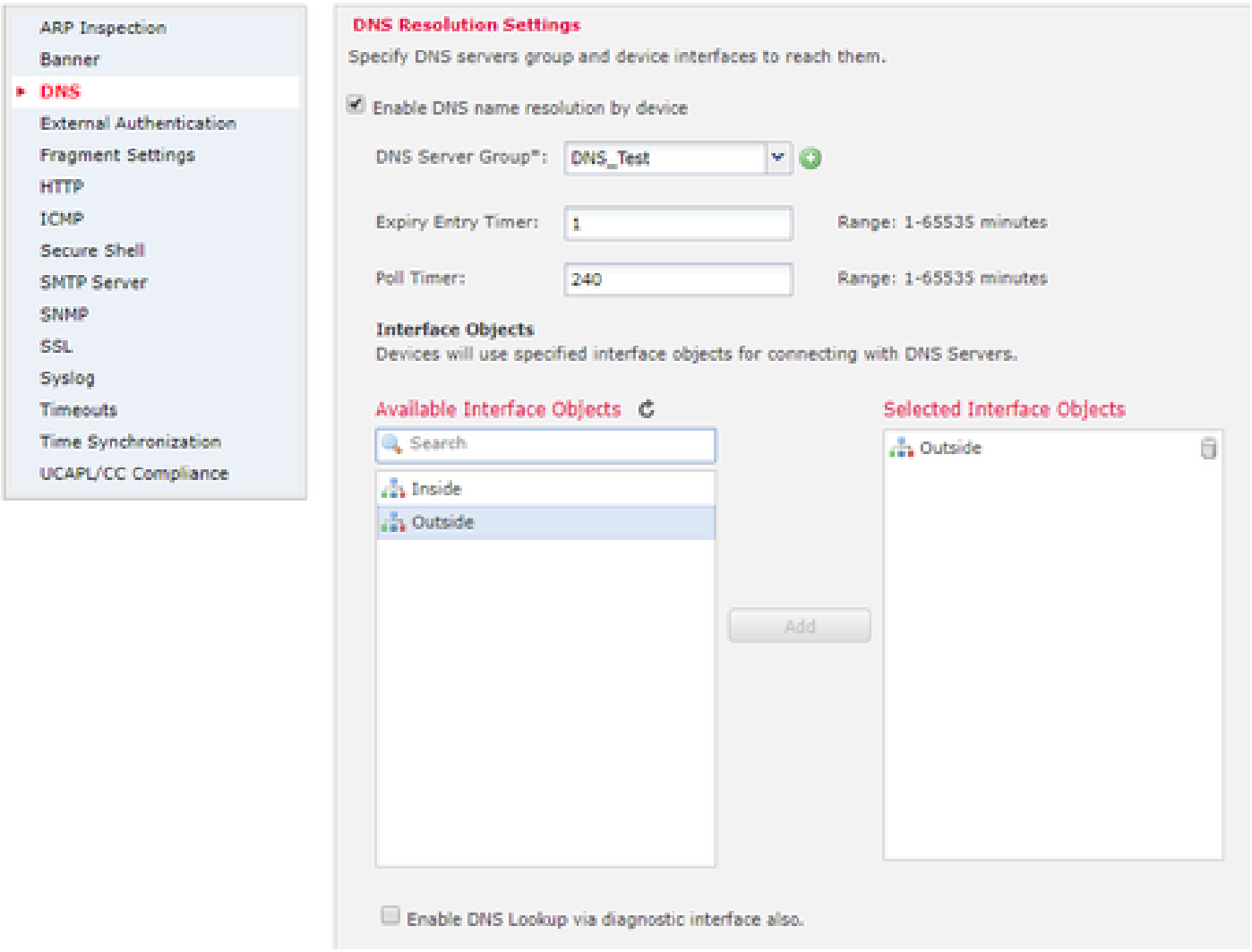
Configuration Steps

Étape 1 : configuration de l’objet « DNS Server Group Object »



- Le nom du groupe de serveurs DNS ne doit pas dépasser 63 caractères
- Dans un déploiement multidomaine, les noms d'objet doivent être uniques au sein de la hiérarchie des domaines. Le système peut identifier un conflit avec le nom d'un objet que vous ne pouvez pas afficher dans votre domaine actuel
- Le domaine par défaut (facultatif) est utilisé pour ajouter aux noms d'hôte qui ne sont pas entièrement qualifiés
- Les valeurs par défaut Retries et Timeout sont préremplies.
    - Retries : nombre de tentatives, de 0 à 10, de la liste des serveurs DNS lorsque le système ne reçoit pas de réponse. Il est défini par défaut à 2.
    - Timeout : nombre de secondes, de 1 à 30, avant une nouvelle tentative vers le serveur DNS suivant. 2 secondes sont établies par défaut. Chaque fois que le système tente à nouveau la liste des serveurs, ce délai double.
- Entrez les serveurs DNS à inclure dans ce groupe. Il peut s'agir d'un format IPv4 ou IPv6 sous forme de valeurs séparées par des virgules
- Le groupe de serveurs DNS est utilisé pour la résolution avec le ou les objets d'interface configurés dans les paramètres de la plate-forme
- L'API REST pour l'objet Groupe de serveurs DNS CRUD est prise en charge

Étape 2 : configuration de DNS (Platform Settings)



- (Facultatif) Modifiez les valeurs Expiry Entry Timer et Poll Timer en minutes :

L'option du minuteur d'entrée d'expiration spécifie la limite de temps pour supprimer l'adresse IP d'un nom de domaine complet résolu de la table de recherche DNS après l'expiration de sa durée de vie (TTL). La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de processus sur le périphérique. Ce paramètre étend virtuellement la durée de vie.

L'option poll timer spécifie le délai après lequel le périphérique interroge le serveur DNS pour résoudre le nom de domaine complet (FQDN) défini dans un groupe d'objets réseau. Un nom de domaine complet est résolu périodiquement, soit lorsque le minuteur d'interrogation a expiré, soit lorsque la durée de vie de l'entrée IP résolue a expiré, selon ce qui se produit en premier.

- (Facultatif) Sélectionnez les objets d'interface requis dans la liste disponible et ajoutez-les à la liste Objets d'interface sélectionnés et assurez-vous que le serveur DNS est accessible via les interfaces sélectionnées :

Pour les périphériques Firepower Threat Defense 6.3.0, si aucune interface n'est sélectionnée et que l'interface de diagnostic est désactivée pour la recherche DNS, la résolution DNS s'effectue via n'importe quelle interface qui inclut l'interface de diagnostic (la commande dnsdomain-lookup any est appliquée).

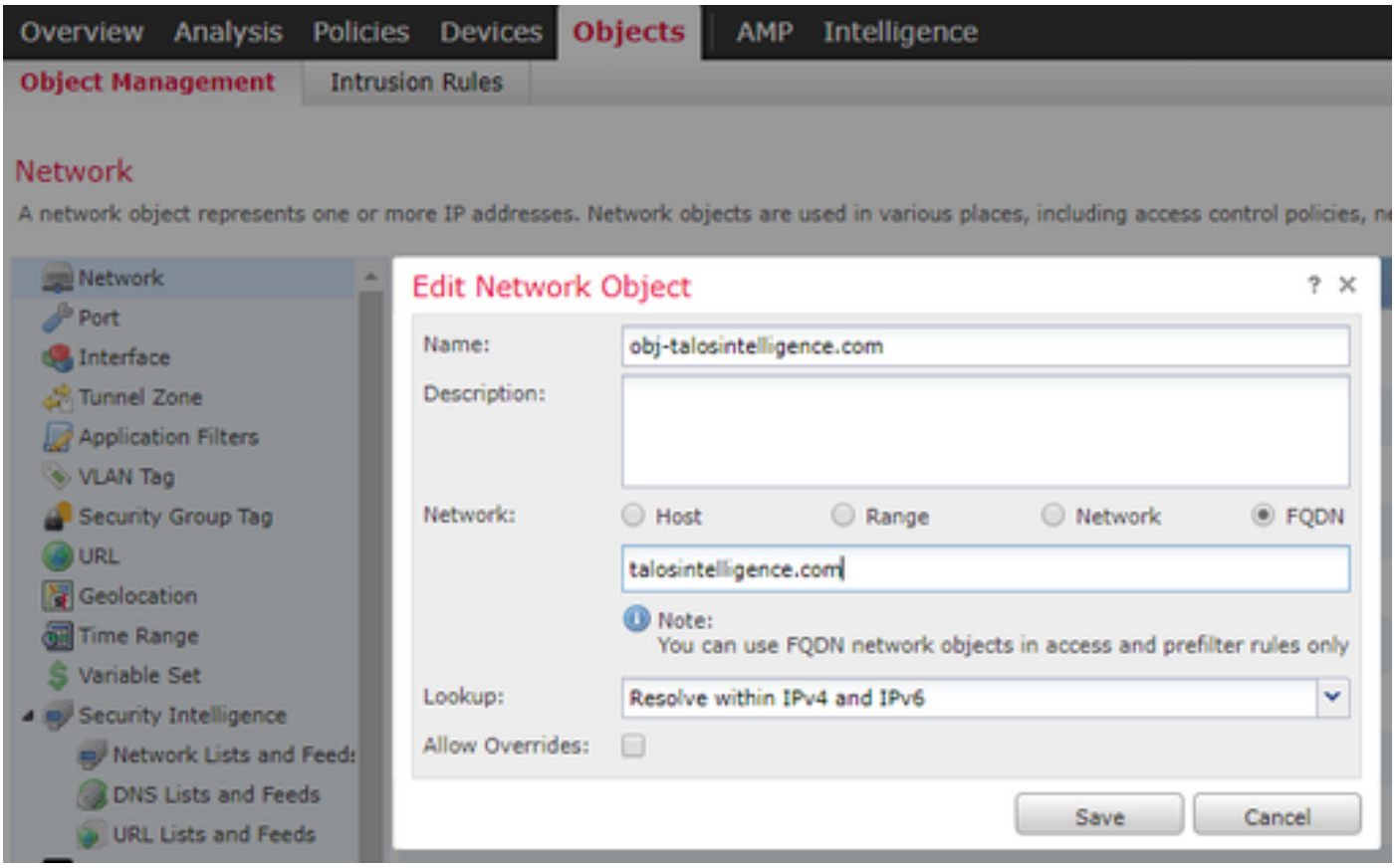
Si vous ne spécifiez aucune interface et n'activez pas la recherche DNS sur l'interface de diagnostic, le FTD utilise la table de routage des données pour déterminer l'interface. En l'absence de correspondance, il utilise la table de routage de gestion.

- (Facultatif) Cochez la case Activer la recherche DNS via l'interface de diagnostic également

Si cette option est activée, Firepower Threat Defense utilise à la fois les interfaces de données sélectionnées et l'interface de diagnostic pour les résolutions DNS. Veillez à configurer une adresse IP pour l'interface de diagnostic sur la page Périphériques > Gestion des périphériques > Modifier le périphérique > Interfaces.

Étape 3 : configuration du nom de domaine complet du réseau objet

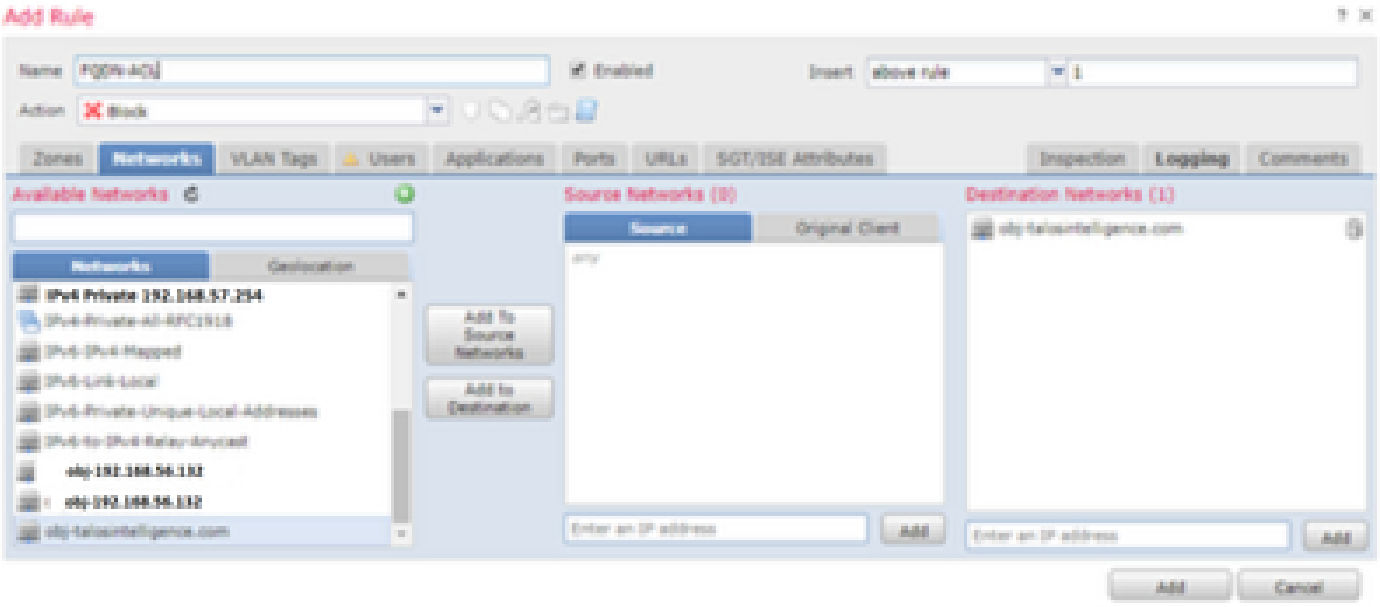
Accédez à Objets > Gestion des objets, dans un objet réseau, spécifiez l'option FQDN.

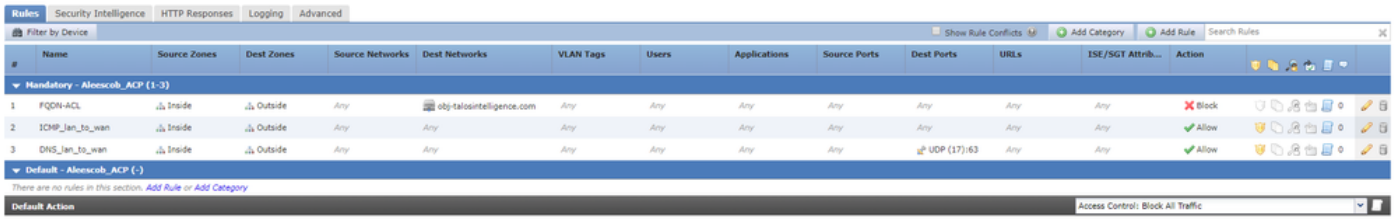


- Un ID unique 32 bits est généré lorsque l'utilisateur crée un objet FQDN
- Cet ID est transmis de FMC à LINA et à Snort
- Dans LINA, cet ID est associé à l'objet
- Dans Snort, cet ID est associé à la règle de contrôle d'accès qui contient cet objet

Étape 4. Création d’une règle de contrôle d’accès

Créez une règle avec l'objet FQDN précédent et déployez la stratégie :





Remarque : La première instance de la résolution du nom de domaine complet se produit lorsque l'objet FQDN est déployé dans une stratégie de contrôle d'accès

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Voici la configuration initiale FTD avant le déploiement du nom de domaine complet :

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

- Voici la configuration après le déploiement du nom de domaine complet :

```
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
```

- Voici à quoi ressemble l'objet FQDN dans LINA :

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

- Lorsqu'elle est déjà déployée, voici à quoi ressemble la liste d'accès FQDN dans LINA :

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

- Voici à quoi il ressemble dans Snort (ngfw.rules) :

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

Remarque : Dans ce scénario, puisque l'objet FQDN a été utilisé pour la destination, il est répertorié en tant que dstfqdn.

- Si vous cochez les commandes show dns et show fqdn, vous pouvez remarquer que la fonctionnalité a commencé à résoudre l'adresse IP pour tallosintelligence :

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

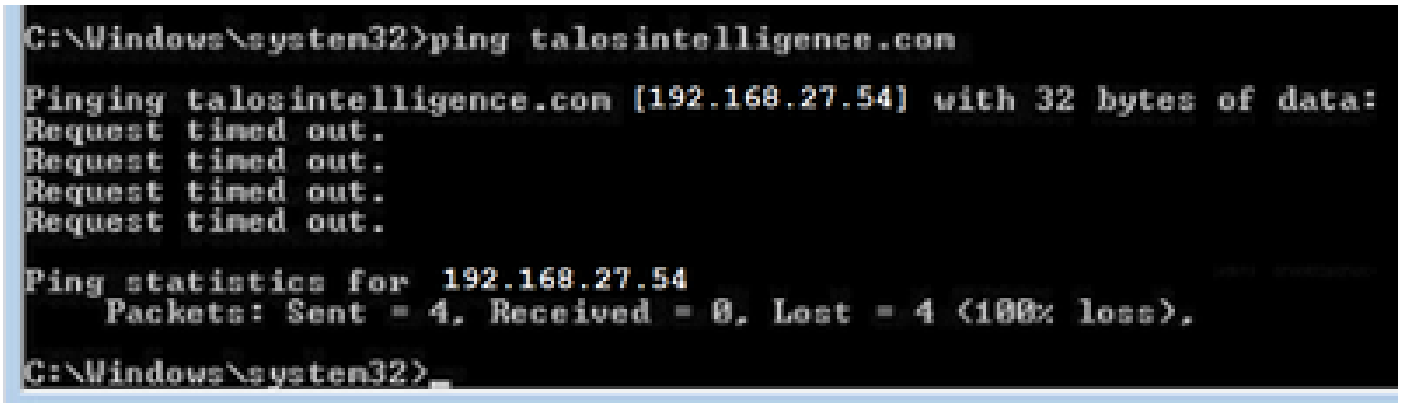
```
aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436
```

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

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

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

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

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

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

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

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

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

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

- Si vous cochez la case show access-list dans LINA, vous pouvez remarquer les entrées développées pour chaque résolution et nombre d'occurrences :

```
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
```

- Comme l'illustre l'image, une requête ping vers talosintelligence.com échoue car il existe une correspondance pour le nom de domaine complet dans la liste de contrôle d'accès. La résolution DNS a fonctionné puisque le paquet ICMP est bloqué par le FTD.



- Nombre d'occurrences à partir de LINA pour les paquets ICMP précédemment envoyés :

```
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
```

- Les requêtes ICMP sont capturées et affichées comme abandonnées dans l'interface d'entrée :

alescob# show cap dans 13 paquets capturés 1 : 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp : 192.168.56.132 port udp 59396 inaccessible 2 : 18:04:12.322126 192.168.56.132 > 172.31.4.161 icmp : echo request 3 : 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp : réponse d'écho 4 : 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp : echo request 5 : 18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp : réponse d'écho 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 : réponse d'écho 8 : 18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp : echo request 9 : 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp : réponse d'écho 10 : 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp : echo request 11 : 18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp : echo request 12 : 18:04:35.711480 192.168.56.132 > 192.168.27.54 icmp : echo request 13 : 18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp : echo request alescob# show cap asp | en 192.168.27.54 162 : 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp : echo request 165 : 18:04:30.704355 192.168.56.132 > 192.168.27.54 icmp : echo request 168 : 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp : echo request 176 : 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp : demande d'écho

- Voici comment la trace recherche l'un des paquets ICMP suivants :

```
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
```

- Si l'action pour la règle de contrôle d'accès est Allow, ceci est un exemple du résultat de 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
```

- Lorsque le nom de domaine complet est déployé dans le cadre d'un préfiltre (FastPath), voici à quoi il ressemble dans ngfw.rules :

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

- Du point de vue LINA avec un paquet suivi :

```
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:
```

Dépannage

1. Configuration depuis FMC

- Vérifiez que les stratégies et les paramètres du serveur DNS sont correctement configurés
- Vérifier que le déploiement a réussi

2. Déployer la vérification sur FTD

- Exécutez les commandes show dns et show access-list pour voir si le nom de domaine complet est résolu et si les règles AC sont développées
- Exécutez la commande show run object network et notez l'ID associé à l'objet (par exemple, X pour la source)
- Exécutez la commande show fqdn id X pour vérifier que le nom de domaine complet est correctement résolu vers l'adresse IP source
- Vérifiez si le fichier ngfw.rules contient une règle AC avec l'ID FQDN X comme source
- Exécutez la commande system support firewall-engine-debug et vérifiez le verdict Snort

Collecte des fichiers de dépannage FMC

Tous les journaux nécessaires sont collectés à partir d'un dépannage FMC. Pour collecter tous les journaux importants à partir de FMC, exécutez un dépannage à partir de l'interface utilisateur graphique de FMC. Sinon, à partir d'une invite FMC Linux, exécutez sf_troubleshoot.pl. Si vous rencontrez un problème, envoyez un rapport de dépannage FMC avec votre rapport au Centre d'assistance technique Cisco (TAC).

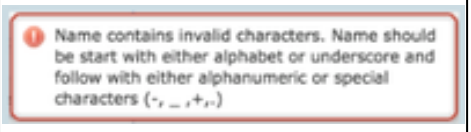
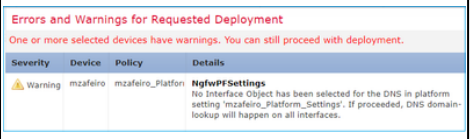
Journaux FMC

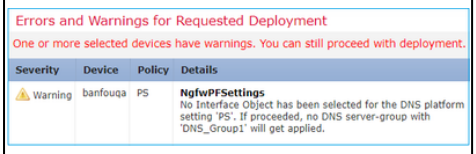
Nom/emplacement du fichier journal	Objectif
`/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log`	Tous les appels API
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	Tous les appels API
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	Journaux de génération CLI
`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Journaux Tomcat
`/var/log/mojo.log`	Journaux Mojo

/var/log/CSMAgent.log	Appels REST entre CSM et DC
/var/log/action_queue.log	Journal de la file d'attente des actions du DC

Problèmes courants/Messages d'erreur

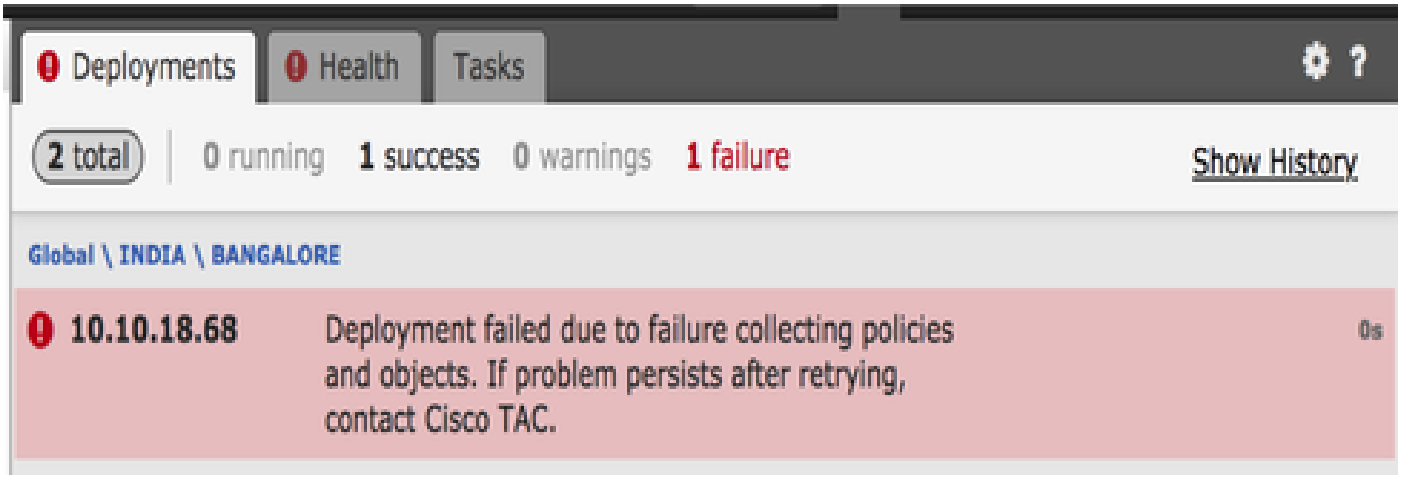
Voici les erreurs/avertissements affichés dans l'interface utilisateur pour l'objet de groupe de serveurs FQDN et DNS et les paramètres DNS :

Erreur/avertissement	Scénario	Description
 Le nom contient des caractères non valides. Les noms doivent commencer par un caractère alphabétique ou un trait de soulignement, suivi de caractères alphanumériques ou de caractères spéciaux. (-,_,+,.)	Utilisateur Configure un nom incorrect	L'utilisateur est informé des autorisations caractères et plage max.
Valeur de domaine par défaut non valide	L'utilisateur configure un nom de domaine incorrect	L'utilisateur est informé des caractères autorisés et de la plage maximale.
 Aucun objet d'interface n'a été sélectionné pour le DNS dans le paramètre de plateforme « mzafeiro_Platform_Settings ». Si vous continuez, la recherche de domaine DNS aura bientôt lieu sur toutes les interfaces	L'utilisateur ne sélectionne aucune interface pour la recherche de domaine Pour un périphérique post-6.3	L'utilisateur est averti que le DNS l'interface CLI du groupe de serveurs sera bientôt appliquée à toutes les interfaces.

 Aucun objet d'interface n'a été sélectionné pour le DNS dans le paramètre de plateforme « mzafeiro_Platform_Settings ». Si vous continuez, aucun groupe de serveurs DNS avec « DNS » ne sera bientôt appliqué	L'utilisateur ne sélectionne aucune interface pour la recherche de domaine Pour un périphérique 6.2.3	L'utilisateur est averti que le DNS CLI du groupe de serveurs non générées.

Échec du déploiement

Lorsqu'un nom de domaine complet est utilisé dans une stratégie autre que la stratégie de stratégie/préfiltre AC, cette erreur peut se produire et s'afficher dans l'interface utilisateur FMC :



Étapes de dépannage recommandées

1) Ouvrez le fichier journal : /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Recherchez un message de validation similaire à :

«Réseau(s) configuré(s) non valide(s). Les réseaux [NetworksContainingFQDN] configurés sur le ou les périphériques[DeviceNames] font référence à « FQDN »

3) Mesure suggérée :

Vérifiez si une ou plusieurs des stratégies mentionnées ci-dessous sont déjà configurées avec un nom de domaine complet (FQDN) ou un groupe qui contient un ou plusieurs objets FQDN, puis réessayez de les déployer une fois ces objets supprimés.

a) Politique d'identité

b) Jeux de variables contenant un nom de domaine complet appliqué à la politique AC

Aucun FQDN activé

Le système peut afficher le suivant via l'interface de ligne de commande FTD :

> show dns INFO : aucun FQDN activé

Le DNS n'est pas activé tant qu'un objet avec un nom de domaine complet défini n'est pas appliqué. Une fois qu'un objet est appliqué, ce problème est résolu.

Q&R

Q : Packet-tracer avec FQDN est-il un test valide pour résoudre les problèmes ?
A : Oui, vous pouvez utiliser l'option fqdn avec packet-tracer.

Q : À quelle fréquence la règle FQDN met-elle à jour l’adresse IP du serveur ?
A : Cela dépend de la valeur TTL de la réponse DNS. Une fois la valeur TTL expirée, le nom de domaine complet est résolu à nouveau avec une nouvelle requête DNS.
Cela dépend également de l'attribut Poll Timer défini dans la configuration du serveur DNS. La règle FQDN est résolue périodiquement lorsque le minuteur DNS d'interrogation a expiré ou lorsque la durée de vie de l'entrée IP résolue a expiré, selon la première éventualité.

Q : Cela fonctionne-t-il pour le DNS round-robin ?
A : Le DNS round-robin fonctionne de manière transparente, car cette fonctionnalité fonctionne sur le FMC/FTD avec l’utilisation d’un client DNS et la configuration DNS round-robin est du côté du serveur DNS.

Q : Existe-t-il une limitation pour les valeurs DNS TTL faibles ?
A : Si une réponse DNS est fournie avec une durée de vie de 0, le périphérique FTD ajoute 60 secondes. Dans ce cas, la valeur TTL est d'au moins 60 secondes.

Q : Par défaut, le FTD conserve donc la valeur par défaut de 60 secondes ?
A : L'utilisateur peut toujours remplacer le paramètre TTL avec Expire Entry Timer sur le serveur DNS.

Q : Comment interagit-il avec les réponses DNS anycast ? Par exemple, les serveurs DNS peuvent fournir différentes adresses IP en fonction de la géolocalisation aux demandeurs. Est-il possible de demander toutes les adresses IP pour un nom de domaine complet ? Comme la commande dig sous Unix ?
A : Oui, si le FQDN est capable de résoudre plusieurs adresses IP, toutes les adresses sont envoyées au périphérique et la règle AC se développe en conséquence.

Q : Est-il prévu d'inclure une option d'aperçu qui montre que les commandes sont diffusées avant toute modification du déploiement ?
A : Cela fait partie de l'option Preview config disponible via Flex config. L'aperçu est déjà présent, mais il est masqué dans la stratégie de configuration Flex. Il y a un plan pour le déplacer et le rendre générique.

Q : Quelle interface du FTD est utilisée pour effectuer la recherche DNS ?
A : Il est configurable. Lorsqu'aucune interface n'est configurée, toutes les interfaces nommées sur FTD sont activées pour la recherche DNS.

Q : Chaque pare-feu de nouvelle génération géré effectue-t-il sa propre résolution DNS et sa propre traduction IP FQDN séparément, même si la même stratégie d'accès est appliquée à tous les pare-feu de nouvelle génération avec le même objet FQDN ?
A : Oui.

Q : Le cache DNS peut-il être effacé pour le dépannage des ACL FQDN ?
A : Oui, vous pouvez exécuter les commandes clear dns et clear dns-hosts cache sur le périphérique.

Q : Quand exactement la résolution FQDN est-elle déclenchée ?
A : La résolution du FQDN se produit lorsque l'objet FQDN est déployé dans une stratégie AC.

Q : Est-il possible de purger le cache uniquement pour un seul site ?
A : Oui. Si vous connaissez le nom de domaine ou l'adresse IP, vous pouvez l'effacer, mais il n'y a pas de commande en tant que telle selon la perspective ACL. Par exemple, la commande clear dns host agni.tejas.com est présente pour effacer le cache sur la base hôte par hôte avec le mot clé host comme dans dns host agni.tejas.com.

Q : Est-il possible d'utiliser des caractères génériques, comme *.microsoft.com ?
A : Non. Le nom de domaine complet doit commencer et se terminer par un chiffre ou une lettre. Seuls les lettres, les chiffres et les tirets sont autorisés en tant que caractères internes.

Q : La résolution de noms est-elle effectuée au moment de la compilation AC et non au moment de la première demande ou des demandes suivantes ? Si nous atteignons un TTL faible (inférieur au temps de compilation AC, au flux rapide ou autre), certaines adresses IP peuvent-elles être manquées ?
A : La résolution de nom se produit dès que la stratégie AC est déployée. Conformément à l'expiration du délai de durée de vie, le renouvellement s'ensuit.

Q : Est-il prévu de pouvoir traiter la liste d'adresses IP (XML) du cloud Microsoft Office 365 ?
A : Cette fonctionnalité n'est pas prise en charge actuellement.

Q : Le nom de domaine complet est-il disponible dans la stratégie SSL ?
A : Pas pour l'instant (version 6.3.0). Les objets FQDN sont uniquement pris en charge dans le réseau source et de destination pour la stratégie AC uniquement.

Q : Existe-t-il des journaux historiques qui peuvent fournir des informations sur les FQDN résolus ? Comme les syslogs LINA, par exemple.
A : Pour dépanner le nom de domaine complet vers une destination particulière, vous pouvez utiliser la commande system support trace. Les suivis indiquent l'ID de nom de domaine complet du paquet. Vous pouvez comparer l'ID à dépanner. Vous pouvez également activer les messages Syslog 746015 et 746016 pour suivre l'activité de résolution DNS FQDN.

Q : Le périphérique consigne-t-il le nom de domaine complet dans la table des connexions avec IP résolue ?
A : Pour dépanner le nom de domaine complet vers une destination particulière, vous pouvez utiliser la commande system support trace, où les traces indiquent l'ID de nom de domaine complet du paquet. Vous pouvez comparer l'ID à dépanner. Il est prévu d'avoir des journaux FQDN dans l'observateur d'événements sur FMC à l'avenir.

Q : Quelles sont les lacunes de la fonction de règle FQDN ?

A : La fonctionnalité n'est pas mise à l'échelle si la règle FQDN est utilisée sur une destination qui change fréquemment d'adresse IP (par exemple : des serveurs Internet dont la durée de vie (TTL) expire à zéro), les stations de travail peuvent finir par avoir de nouvelles adresses IP qui ne correspondent plus au cache DNS FTD. Par conséquent, il ne correspond pas à la règle ACP. Par défaut, le FTD ajoute 1 minute en plus de l'expiration de la durée de vie reçue de la réponse DNS et ne peut pas être défini sur zéro. Dans ces conditions, il est vivement recommandé d'utiliser la fonctionnalité de filtrage d'URL la mieux adaptée à ce cas d'utilisation.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.