Bloquer DNS avec Security Intelligence à l'aide de Firepower Management Center

Contenu

Introduction

Ce document décrit la procédure à suivre pour ajouter une liste DNS à une stratégie DNS afin que vous puissiez l'appliquer avec Security Intelligence (SI).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco ASA55XX Threat Defense
- Configuration de Cisco Firepower Management Center

Components Used

- Cisco ASA5506W-X Threat Defense (75) Version 6.2.3.4 (build 42)
- Cisco Firepower Management Center pour VMWare Version du logiciel: 6.2.3.4 (construction 42)OS : Cisco Fire Linux OS 6.2.3 (build13)

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

Security Intelligence fonctionne en bloquant le trafic en provenance ou à destination d'adresses IP, d'URL ou de noms de domaine dont la réputation est mauvaise. Dans ce document, l'accent principal est mis sur la liste noire des noms de domaine.

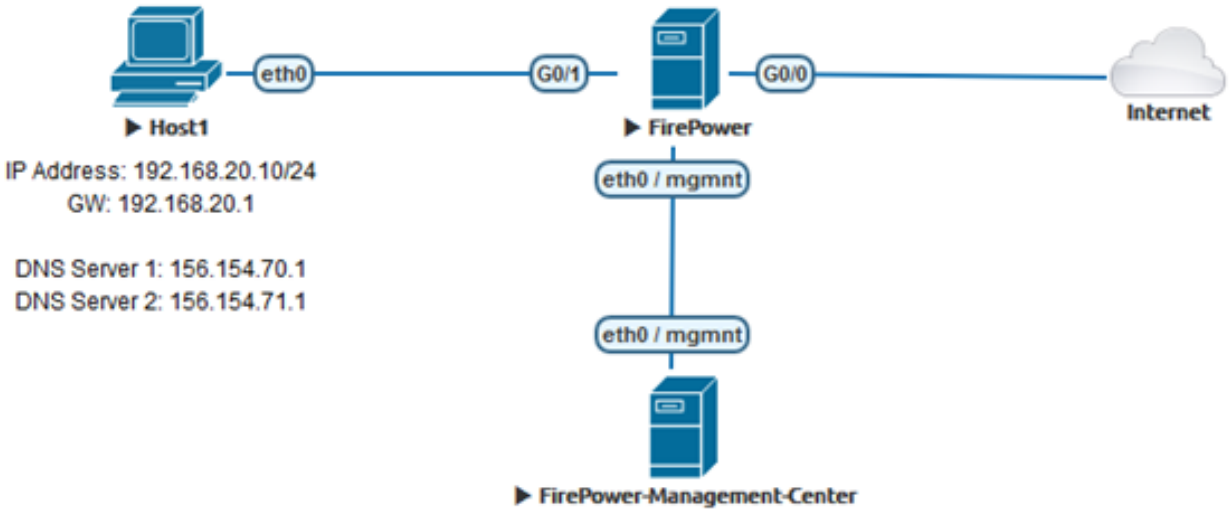
L'exemple a utilisé le domaine des blocs 1 :

- cisco.com

Vous pouvez utiliser le filtrage d'URL pour bloquer certains de ces sites, mais le problème est que l'URL doit correspondre exactement. D'autre part, la liste noire DNS avec SI peut se concentrer sur des domaines tels que “ cisco.com ” sans avoir à se soucier des sous-domaines ou des modifications d'URL.

Àla fin de ce document, une configuration Sinkhole facultative est également présentée.

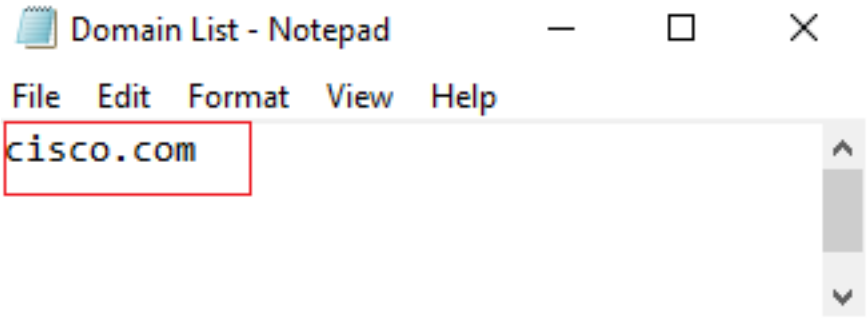
Diagramme du réseau



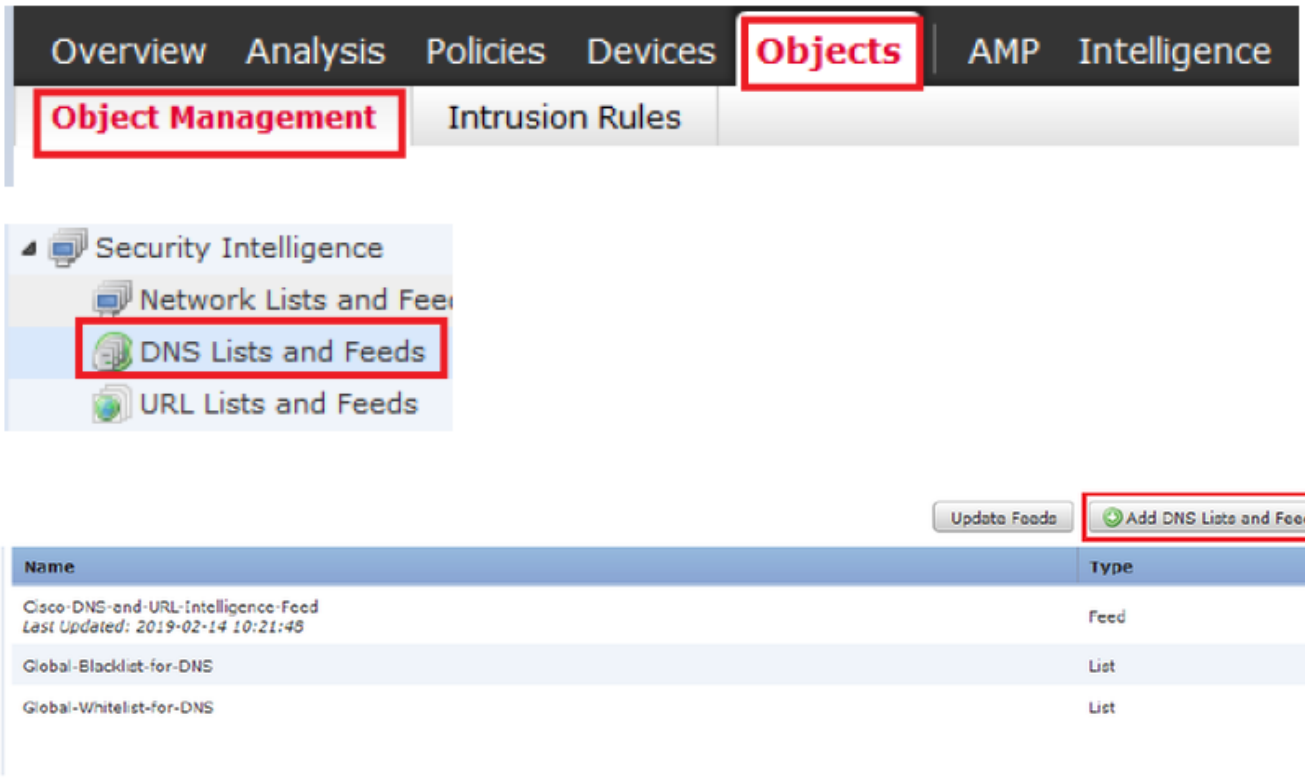
Configuration

Configurer une liste DNS personnalisée avec les domaines que nous voulons bloquer et charger la liste dans FMC

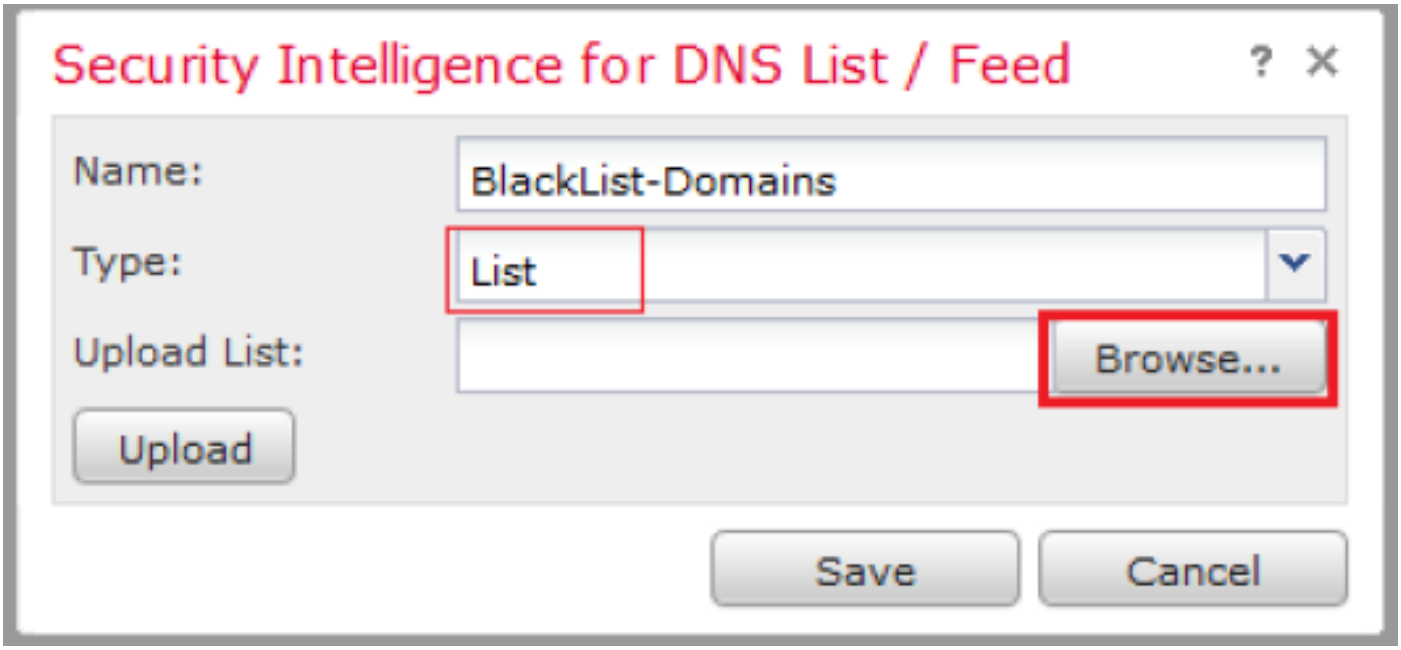
Étape 1. Créez un fichier .txt avec les domaines que vous souhaitez bloquer. Enregistrez le fichier .txt sur votre ordinateur :

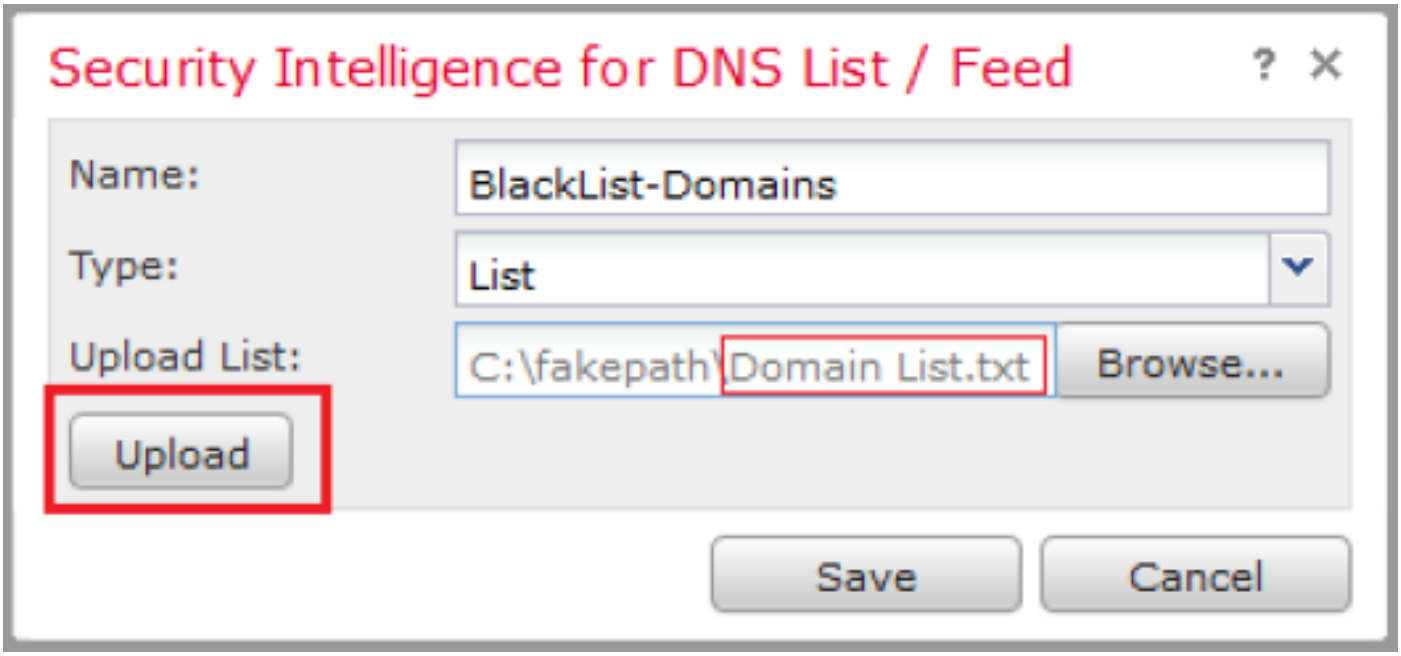


Étape 2. Dans FMC, accédez à Objet » Gestion des objets » Listes et flux DNS » Ajouter une liste et des flux DNS.

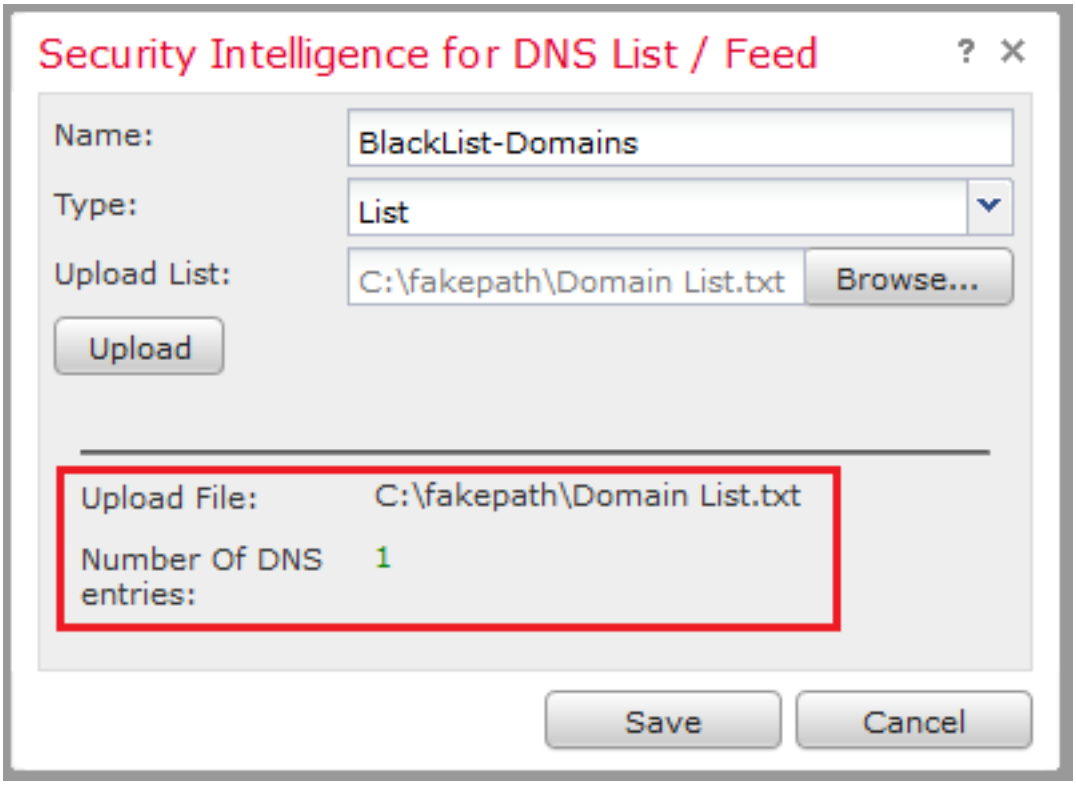


Étape 3. Créez une liste appelée “ BlackList-Domains ”, le type doit être liste et le fichier .txt avec les domaines en question doit être téléchargé comme le montrent les images :





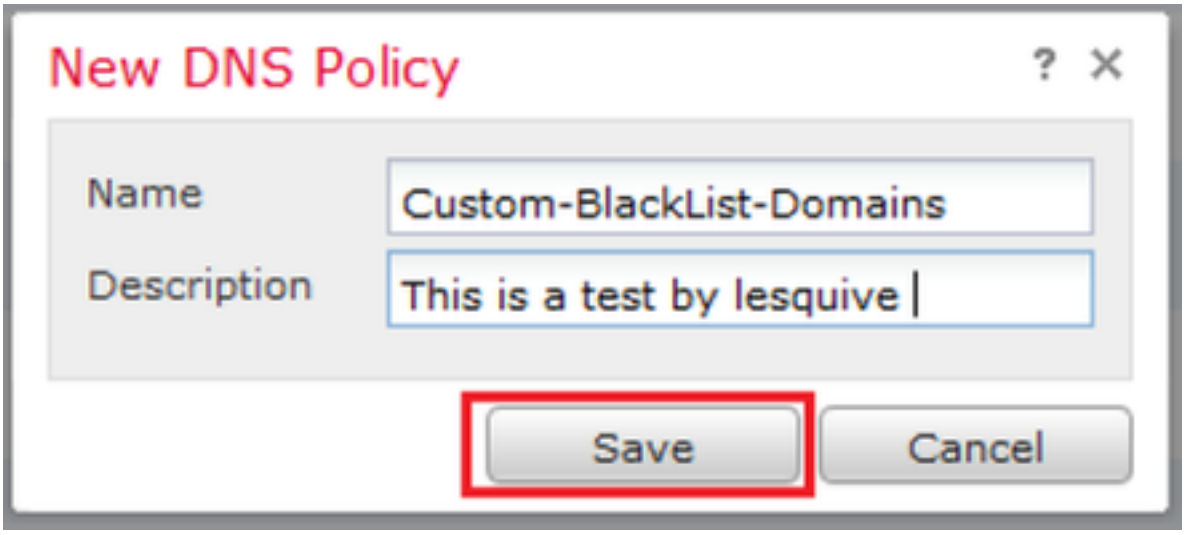
*Notez que lorsque vous téléchargez le fichier .txt, le nombre d'entrées DNS doit lire tous les domaines. Dans cet exemple, un total de 1 :



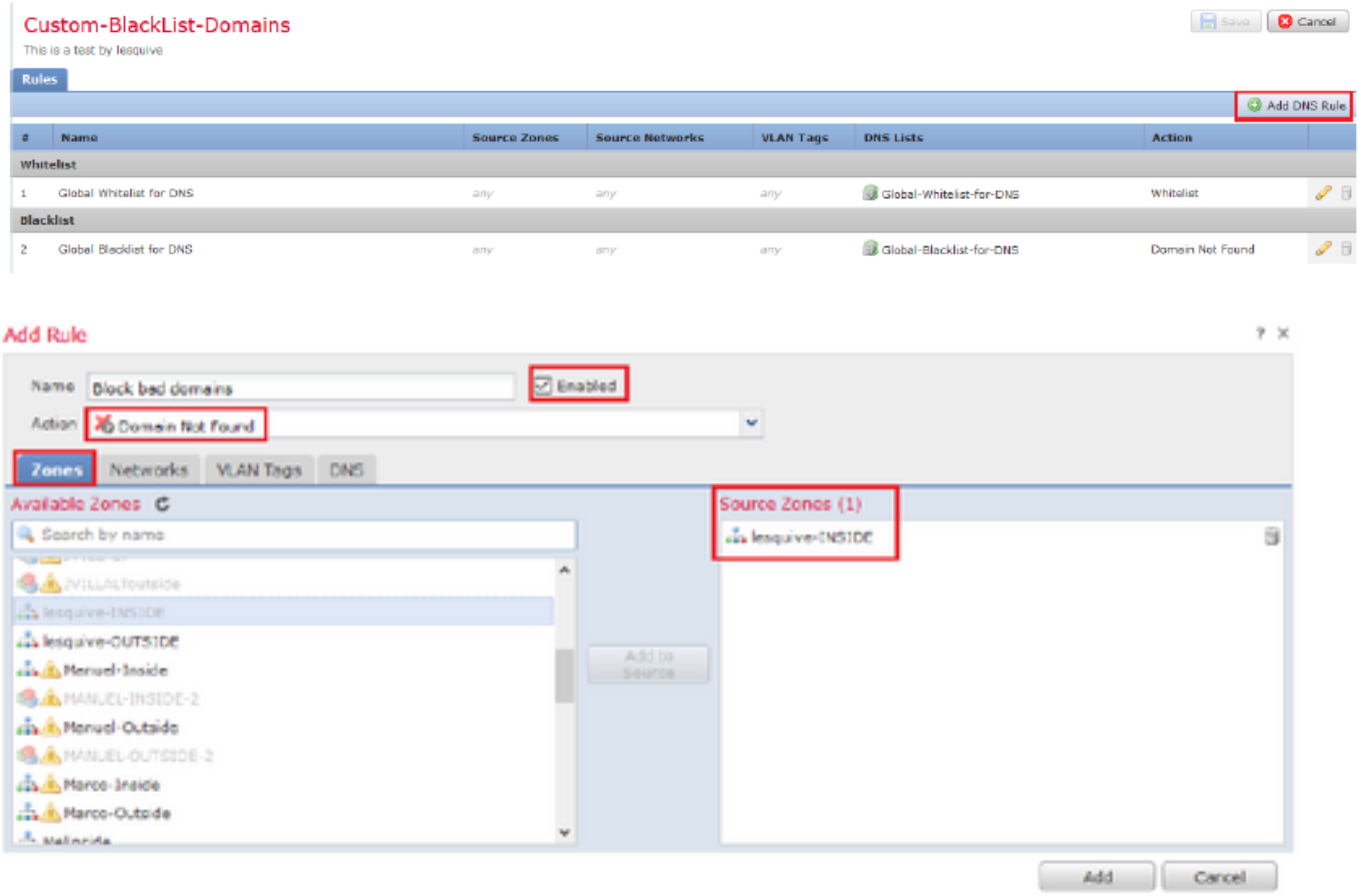
Ajouter une nouvelle stratégie DNS avec l'action configurée sur 'domaine introuvable'

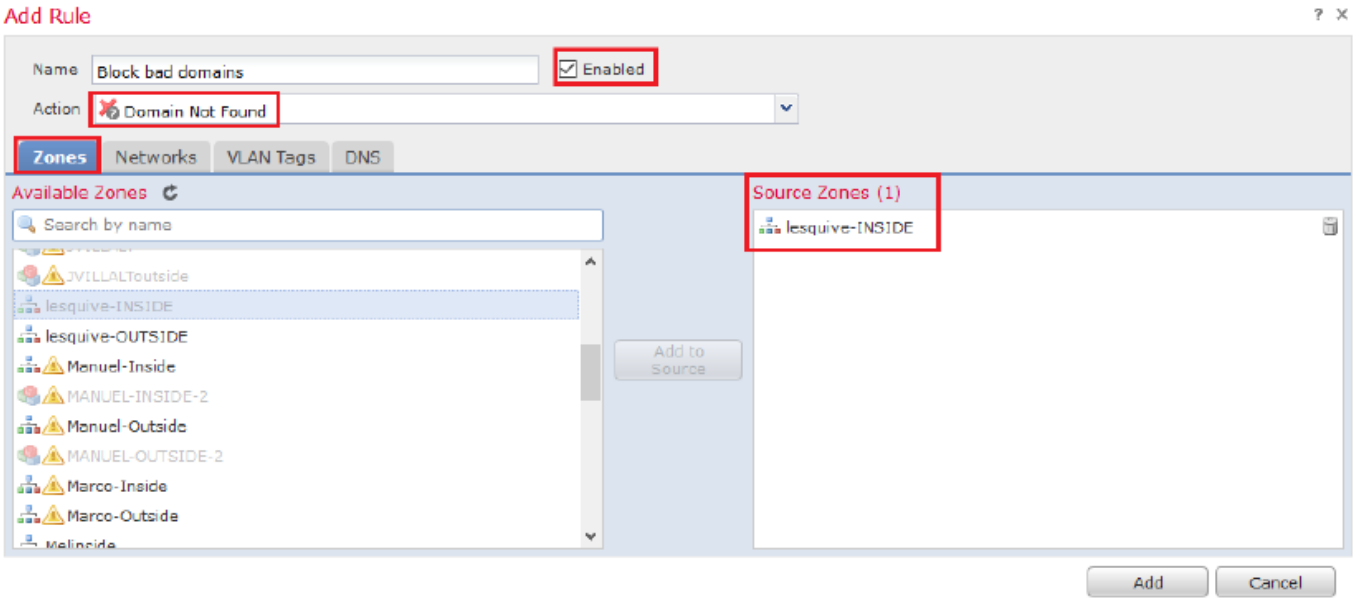
*Assurez-vous d'ajouter une zone source, un réseau source et une liste DNS.

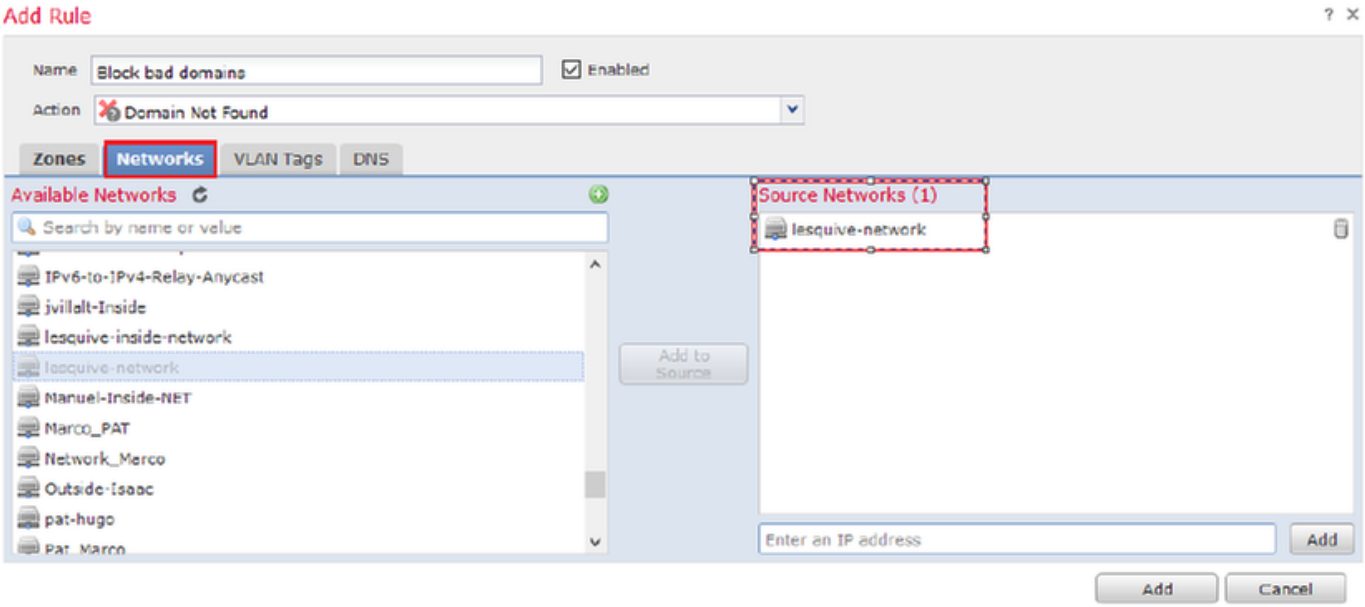
Étape 1. Accédez à Politiques » Contrôle d'accès » DNS » Ajouter une stratégie DNS :

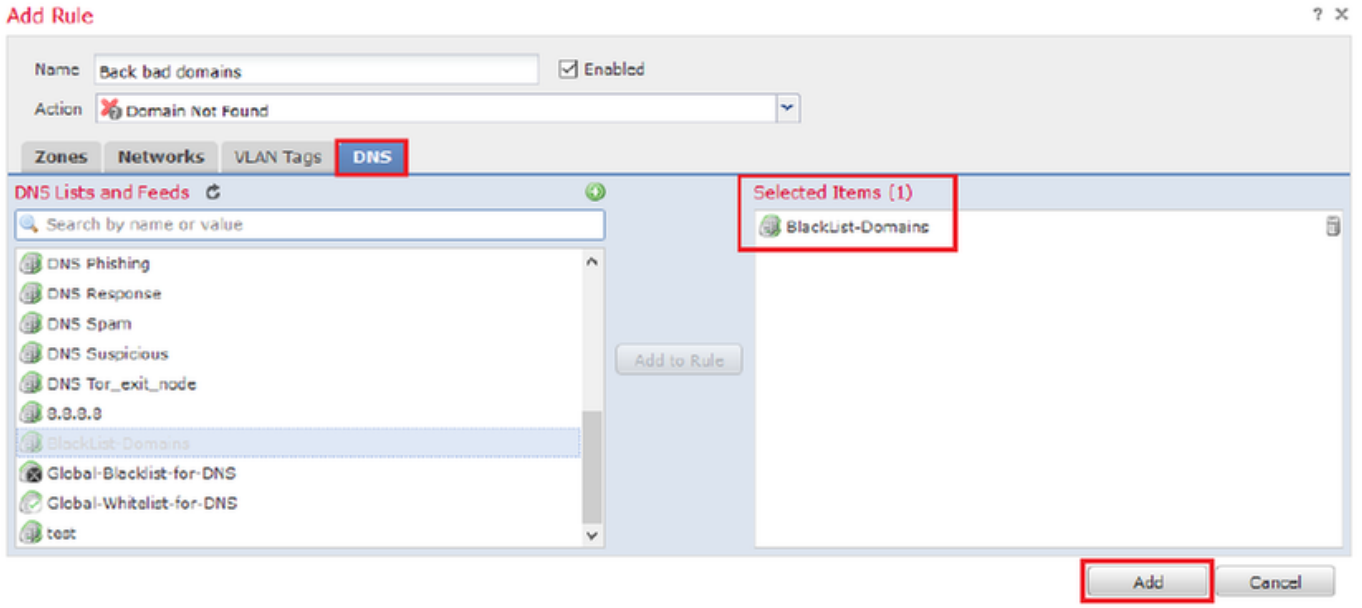


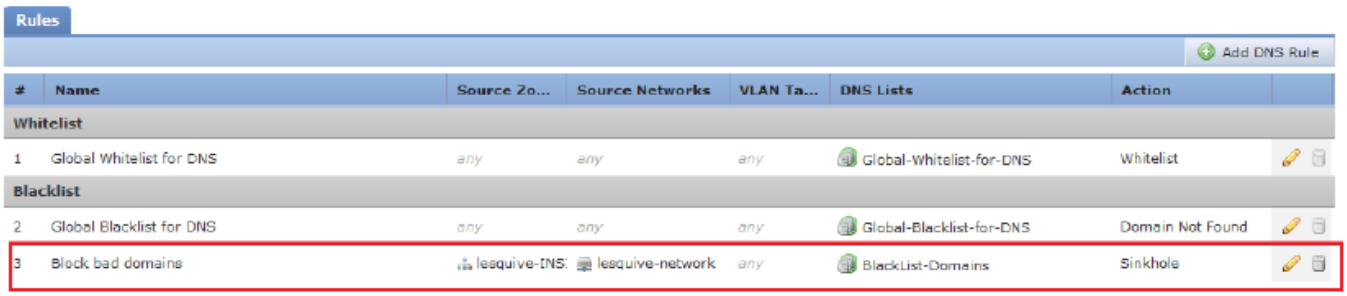
Étape 2. Ajouter une règle DNS telle qu'elle apparaît dans l'image :




Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-INSIDE
lesquive-OUTSIDE
Manuel-Inside
MANUEL-INSIDE-2
Manuel-Outside
MANUEL-OUTSIDE-2
Marco-Inside
Marco-Outside
Add to Source
Source Zones (1)
lesquive-INSIDE
Add
Cancel


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Networks
Search by name or value
IPv6-to-IPv4-Relay-Anycast
jvillalt-Inside
lesquive-inside-network
lesquive-network
Manuel-Inside-NET
Marco_PAT
Network_Marco
Outside-Isaac
pat-hugo
Add to Source
Source Networks (1)
lesquive-network
Enter an IP address
Add
Add
Cancel


Add Rule
Name
Back bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
DNS Lists and Feeds
Search by name or value
DNS Phishing
DNS Response
DNS Spam
DNS Suspicious
DNS Tor_exit_node
8.8.8.8
BlackList-Domains
Global-Blacklist-for-DNS
Global-Whitelist-for-DNS
test
Add to Rule
Selected Items (1)
BlackList-Domains
Add
Cancel

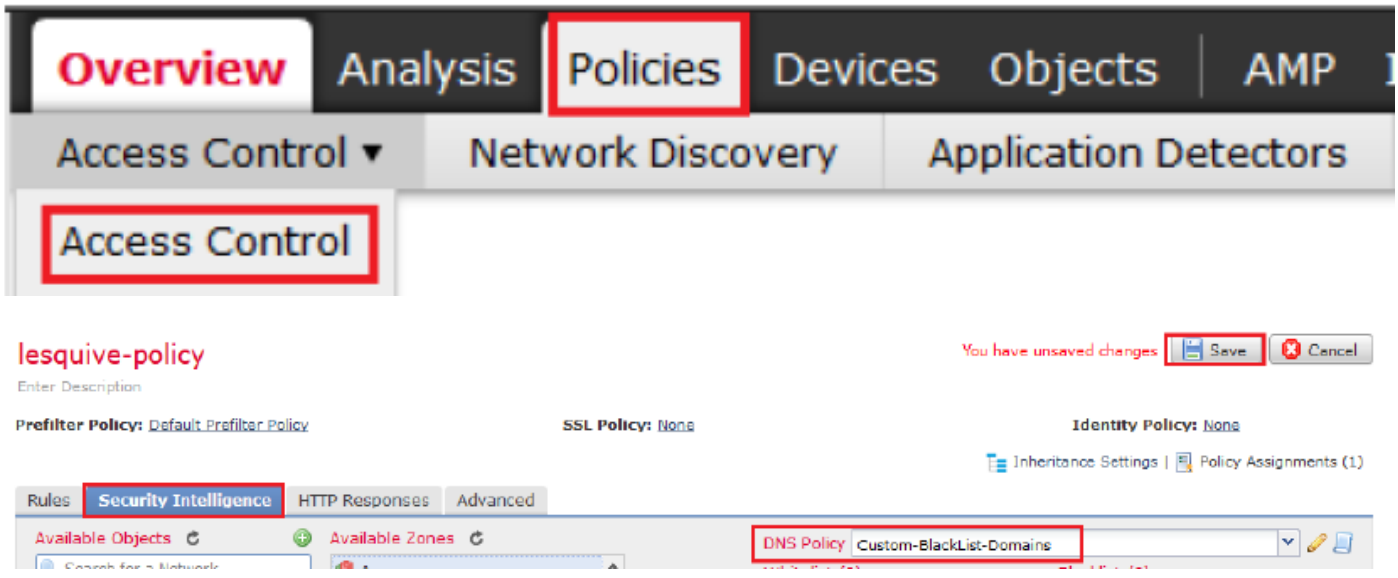


Informations importantes sur l'ordre des règles :

- La liste blanche globale est toujours la première et prime sur toutes les autres règles.
- La règle des listes blanches DNS descendantes apparaît uniquement dans les déploiements multidomaines, dans les domaines non-leaf. Il est toujours en deuxième position et prime sur toutes les autres règles, à l'exception de la liste blanche globale.
- La section Liste blanche précède la section Liste noire ; les règles de liste blanche ont toujours préséance sur les autres règles.
- La liste de blocage globale est toujours la première dans la section Liste de blocage et prime sur toutes les autres règles de surveillance et de liste de blocage.
- La règle des listes noires DNS descendantes apparaît uniquement dans les déploiements multidomaines, dans les domaines non-leaf. Il est toujours en deuxième position dans la section Liste noire et prime sur toutes les autres règles de surveillance et de liste noire, à l'exception de la liste noire globale.
- La section Liste noire contient les règles de surveillance et de liste noire.
- Lorsque vous créez une règle DNS pour la première fois, la position du système s'arrête en dernier dans la section Liste blanche si vous affectez une action Liste blanche ou en dernier dans la section Liste noire si vous affectez une autre action

Affecter la stratégie DNS à votre stratégie de contrôle d'accès

Accédez à Stratégies » Contrôle d'accès » Stratégie de votre FTD » Intelligence de sécurité » Stratégie DNS et ajoutez la stratégie que vous avez créée.

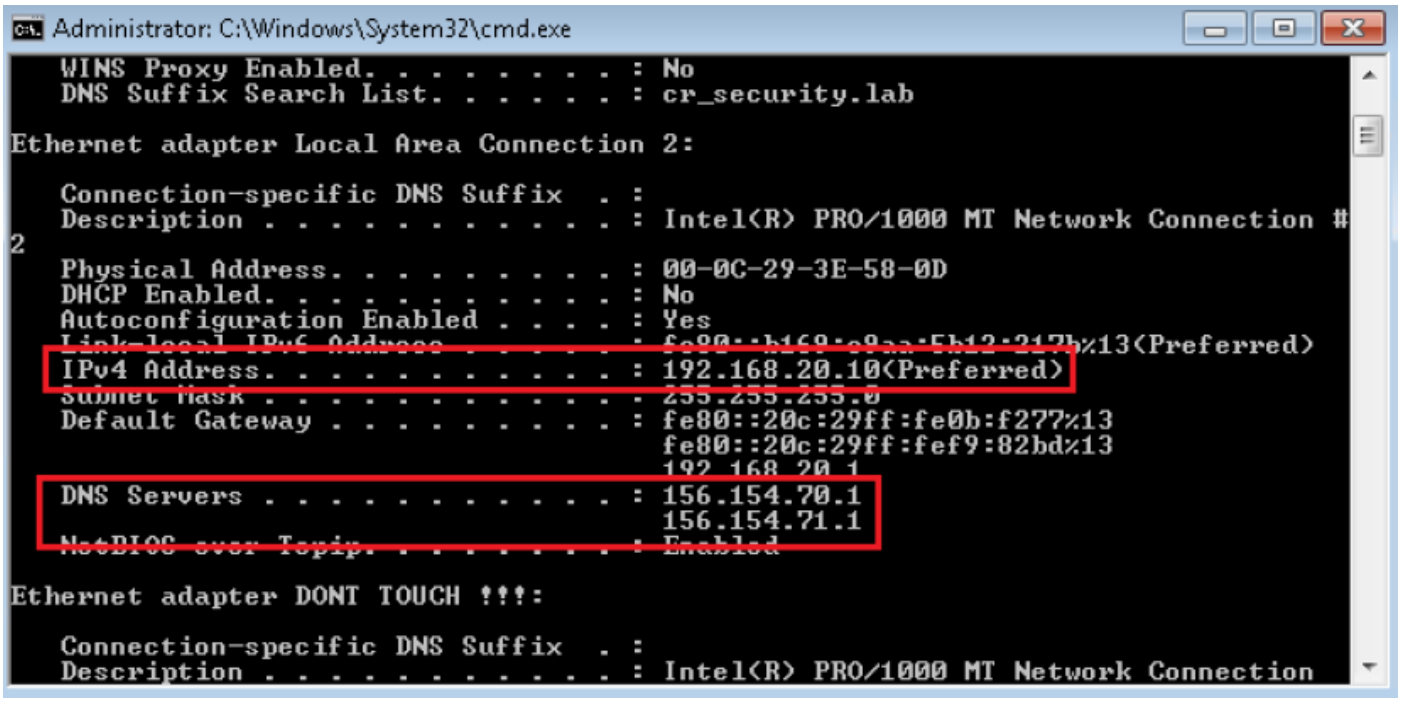


Assurez-vous de déployer toutes les modifications lorsque vous avez terminé.

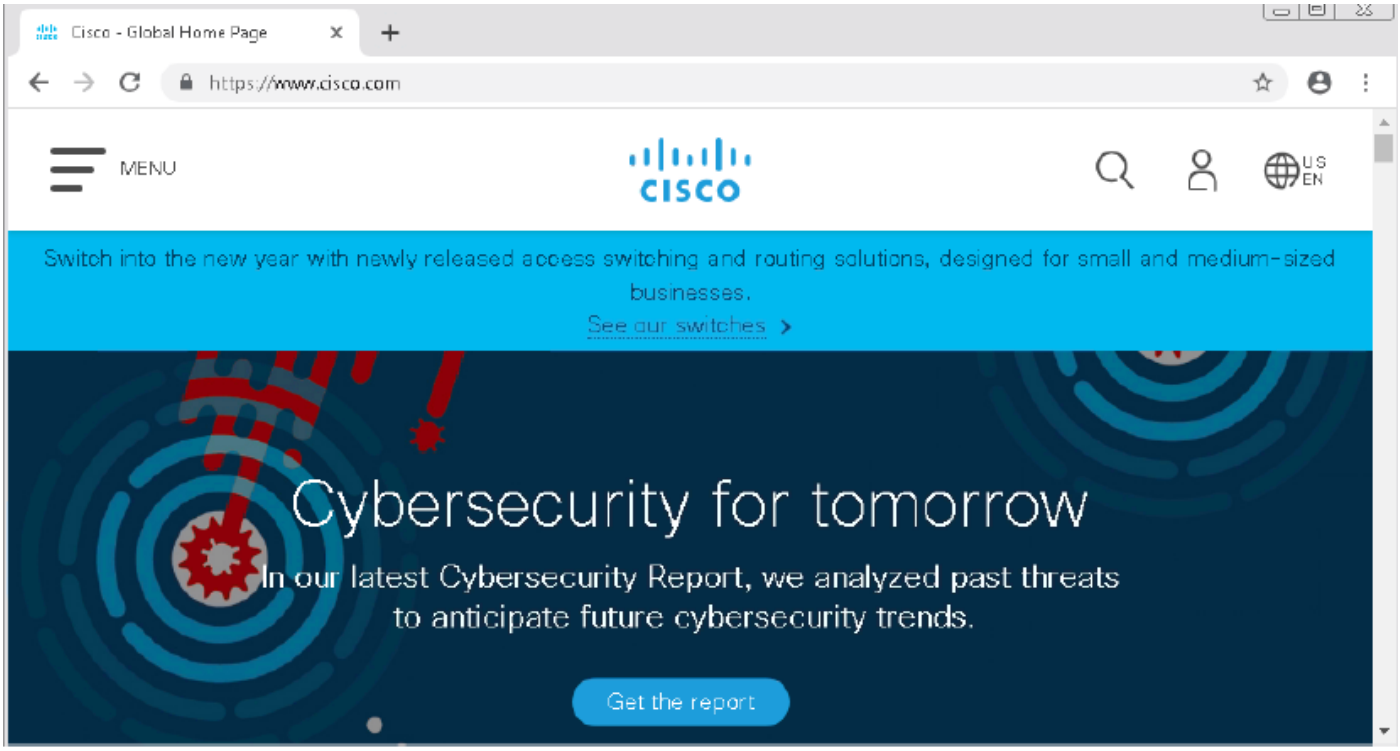
Vérification

Avant l'application de la stratégie DNS

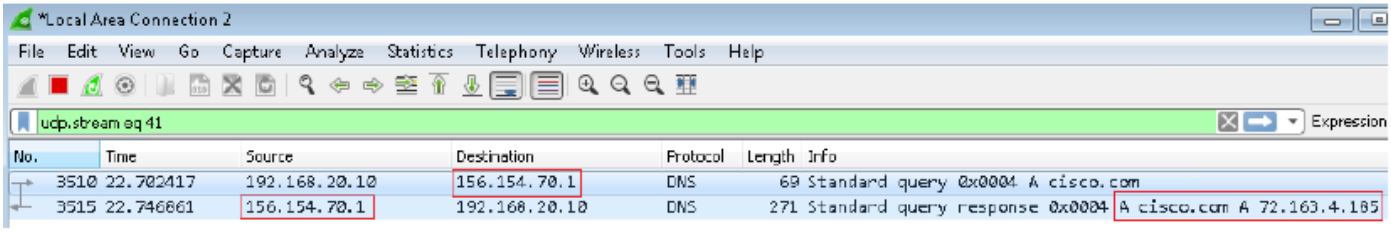
Étape 1. Vérifiez les informations relatives au serveur DNS et à l'adresse IP sur votre machine hôte, comme le montre l'image :

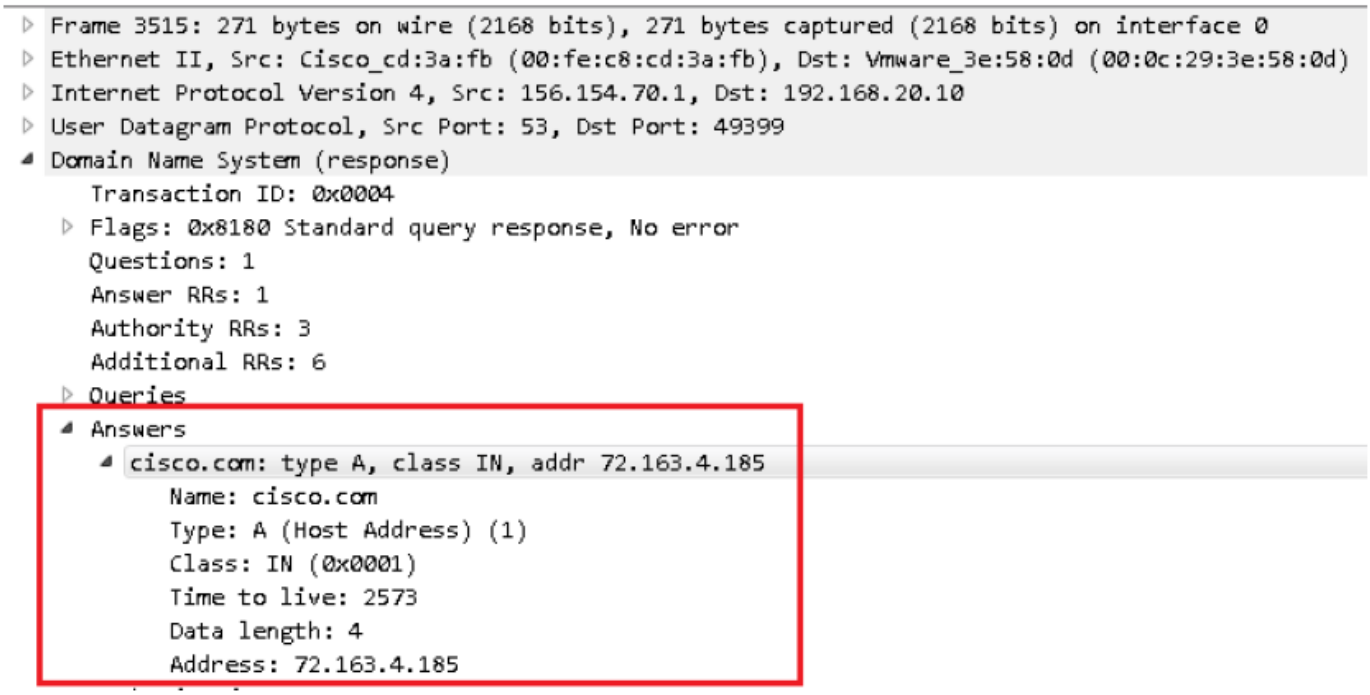


Étape 2. Confirmez que vous pouvez accéder à cisco.com comme le montre l'image :



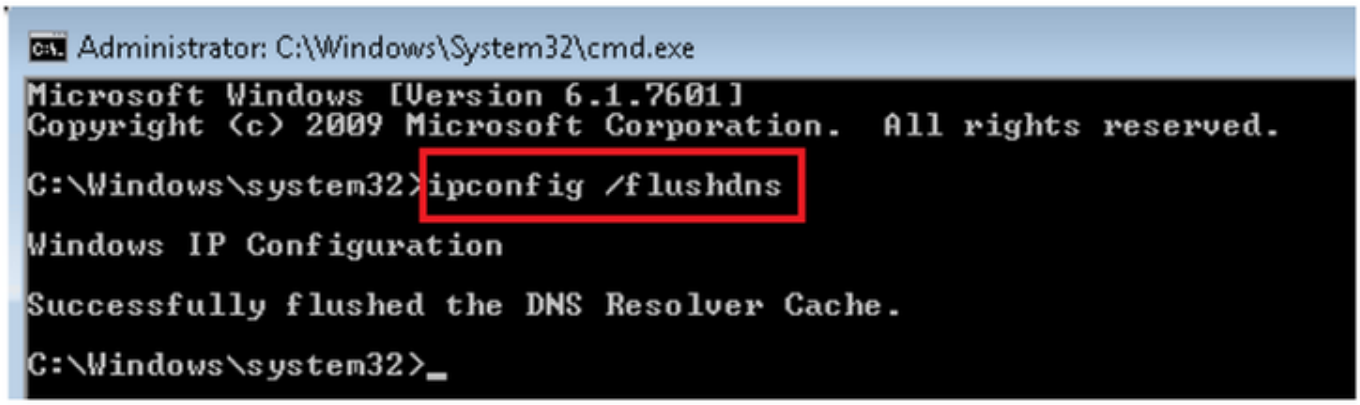
Étape 3. Confirmer avec des captures de paquets que le DNS est résolu correctement :



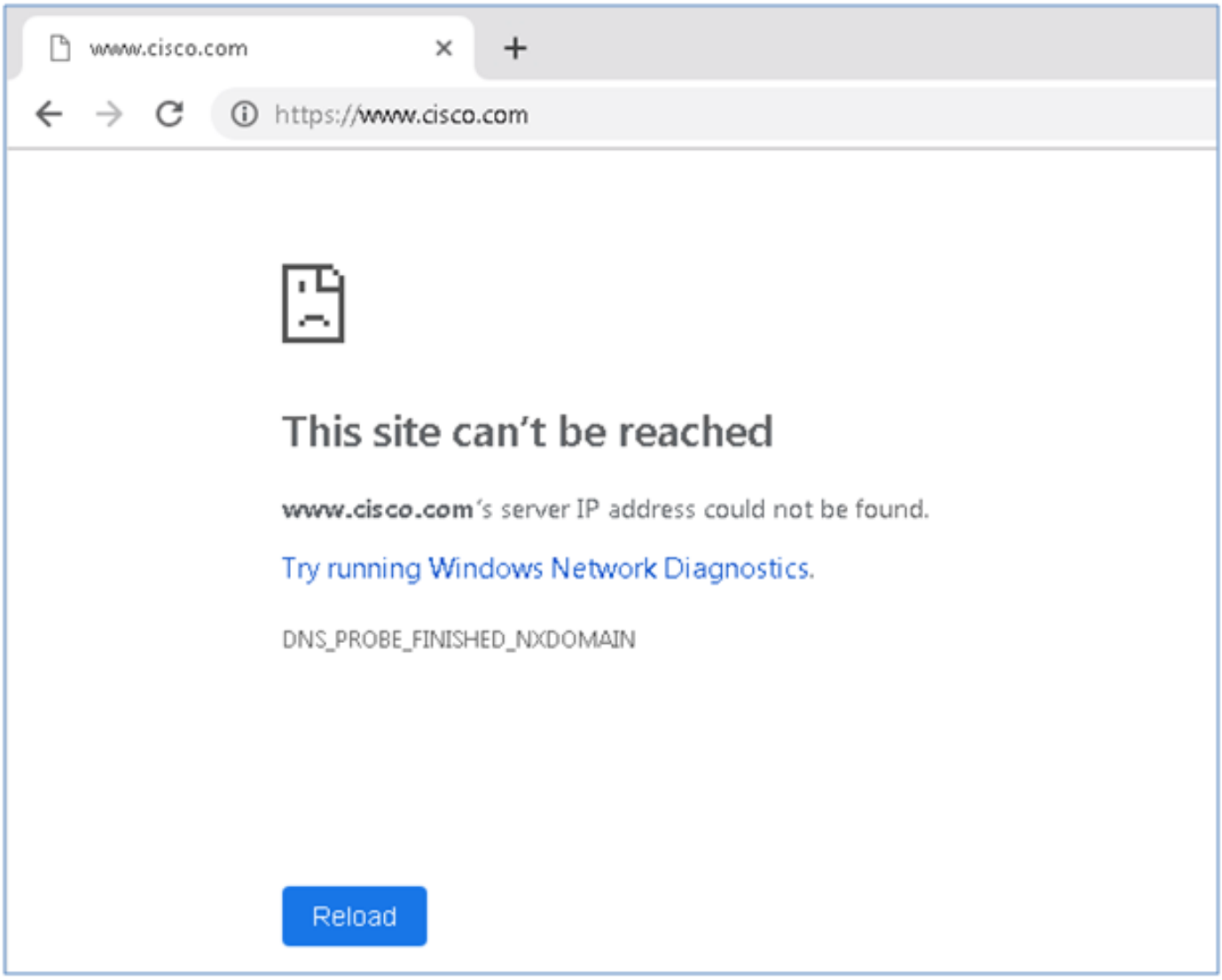


Une fois la stratégie DNS appliquée

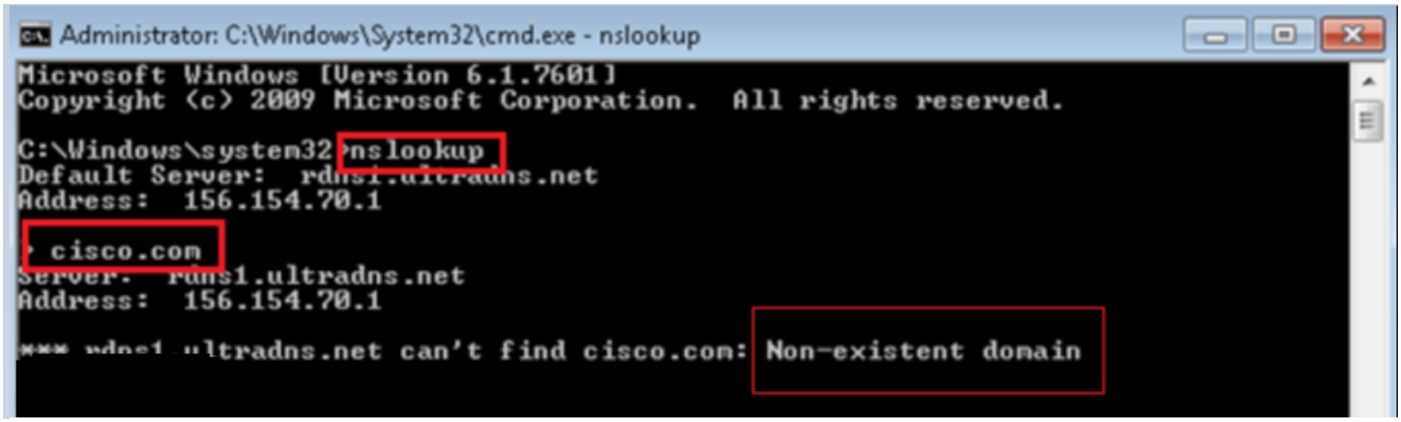
Étape 1. Effacez le cache DNS sur votre hôte à l'aide de la commande **ipconfig /flushdns.**



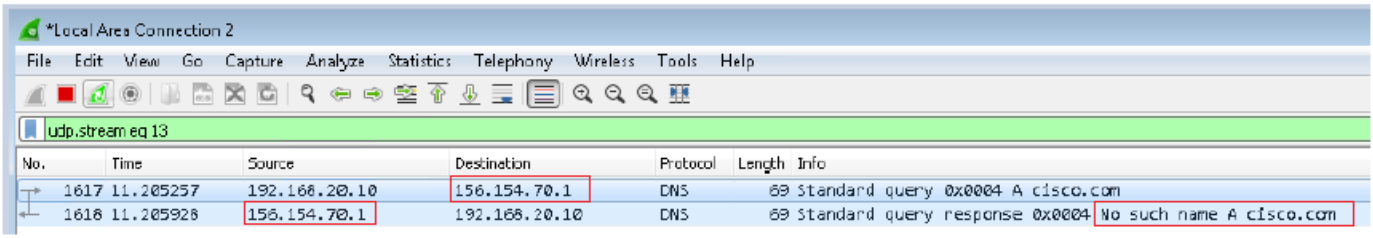
Étape 2. Accédez au domaine en question à l'aide d'un navigateur Web. Elle doit être inaccessible :

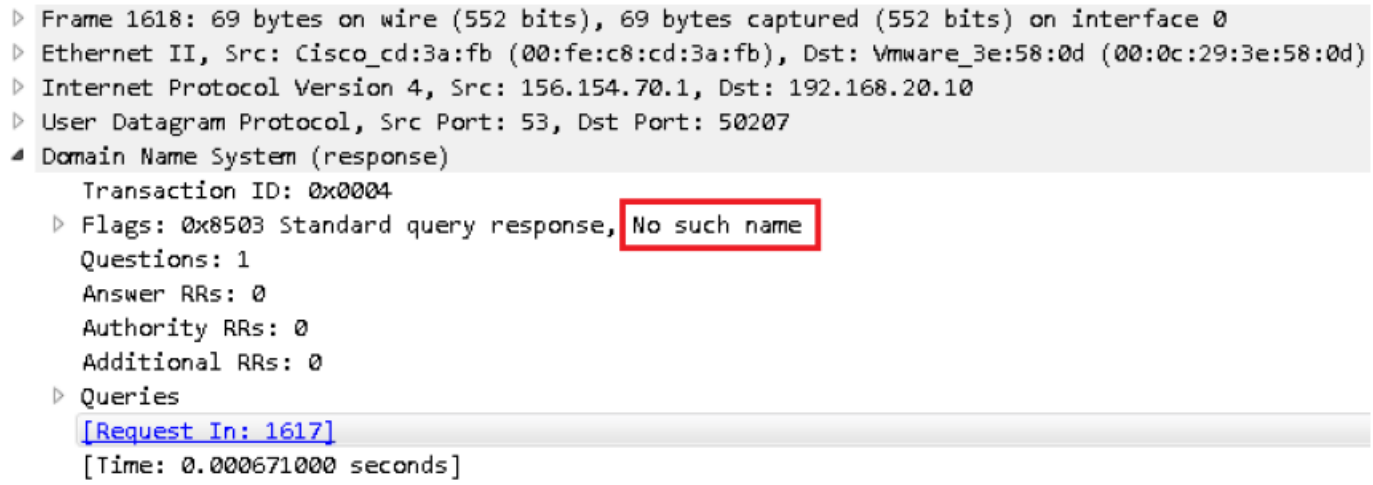


Étape 3. Essayez d'émettre **nslookup** sur le domaine cisco.com. La résolution de noms échoue.

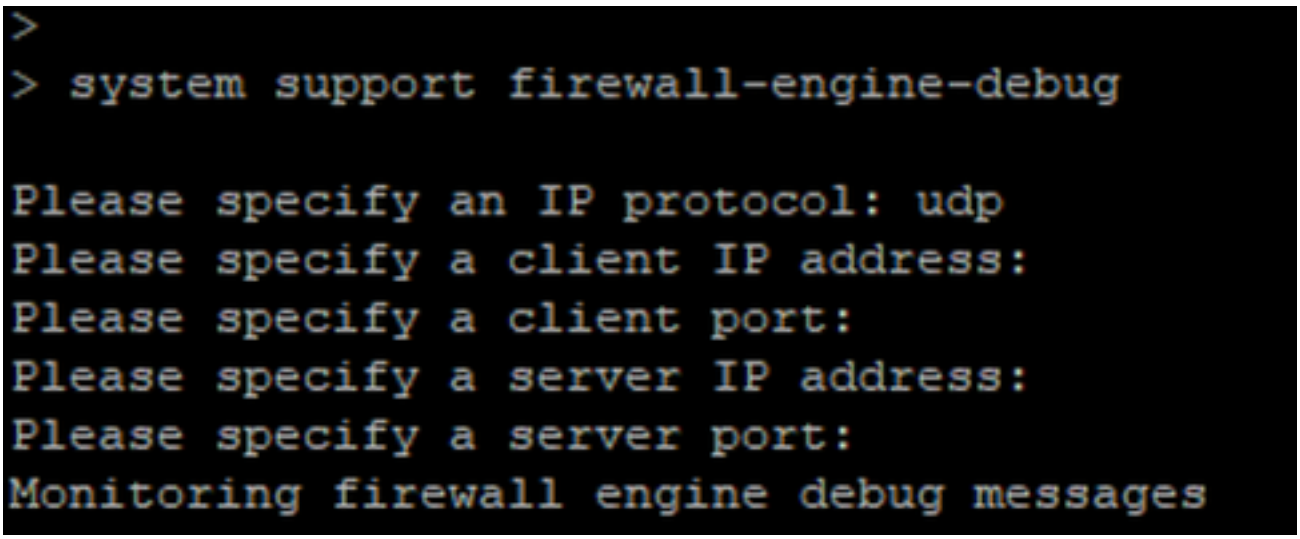


Étape 4. Les captures de paquets montrent une réponse du FTD, au lieu du serveur DNS.





Étape 5. Exécuter des débogages dans l'interface CLI FTD : le système prend en charge firewall-engine-debug et spécifie le protocole UDP.



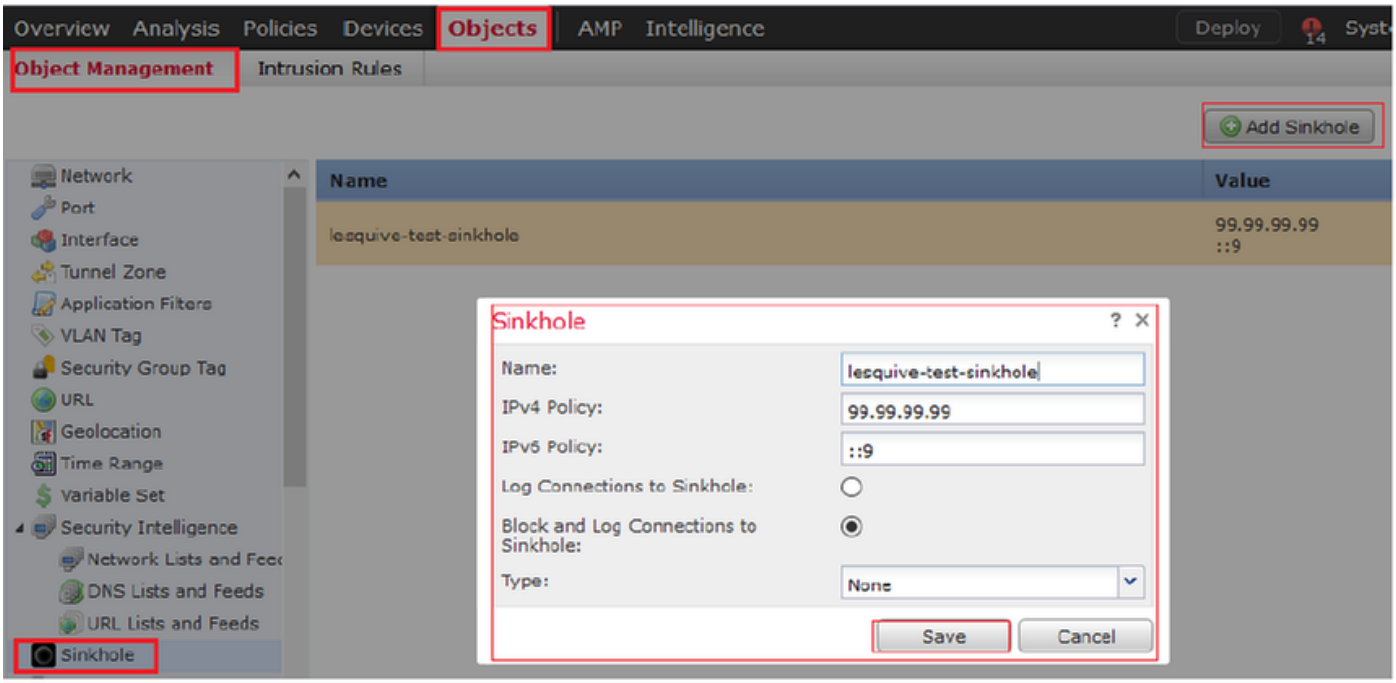
*Débogue lorsque cisco.com correspond :

```
> system support firewall-engine-debug

Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.cr_security.lab
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Got end of flow event from hardware with flags 00000000
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup returned 0 for cisco.com.cr_security.lab
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 00000000
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup returned 1 for cisco.com
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Starting SrcZone first with intfs 1 -> 0, vlan 0
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 1, id 1 action Allow
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 3, id 5 action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got DNS list match. si list 1048620
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Firing DNS action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Injecting NX domain reply.
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 DNS SI: Matched rule order 3, Id 5, si list id 1048620, action 22, reason 2048, SI Categories 1048620,0
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 1 for cisco.com
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Starting SrcZone first with intfs 1 -> 0, vlan 0
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 1, id 1 action Allow
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 2, id 3 action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 3, id 5 action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Got DNS list match. si list 1048620
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Firing DNS action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Injecting NX domain reply.
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 DNS SI: Matched rule order 3, Id 5, si list id 1048620, action 22, reason 2048, SI Categories 1048620,0
```

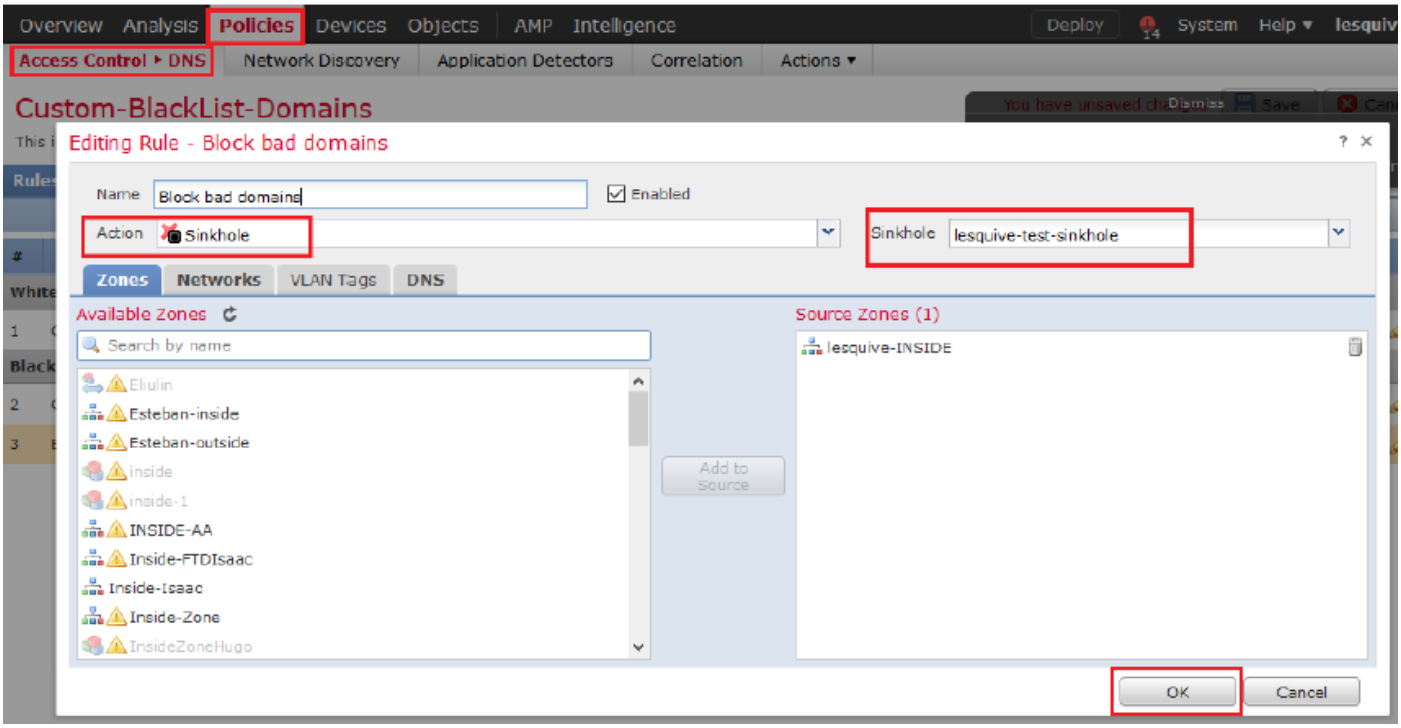
Configuration Sinhole optionnelle

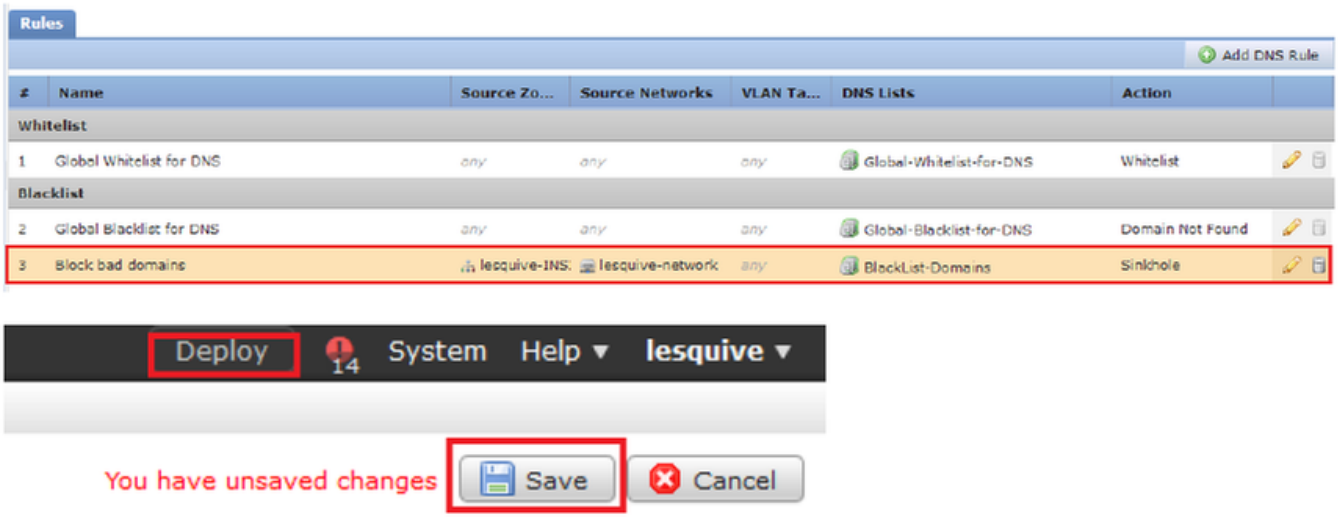
Un trou d'accès DNS est un serveur DNS qui fournit des informations fausses. Au lieu de renvoyer un " Aucun nom " réponse DNS aux requêtes DNS sur les domaines que vous bloquez, il retourne une fausse adresse IP.

Étape 1. Naviguez jusqu'à Objets » Gestion des objets » Sinkhole » Ajouter Sinkhole et créez les fausses informations d'adresse IP.

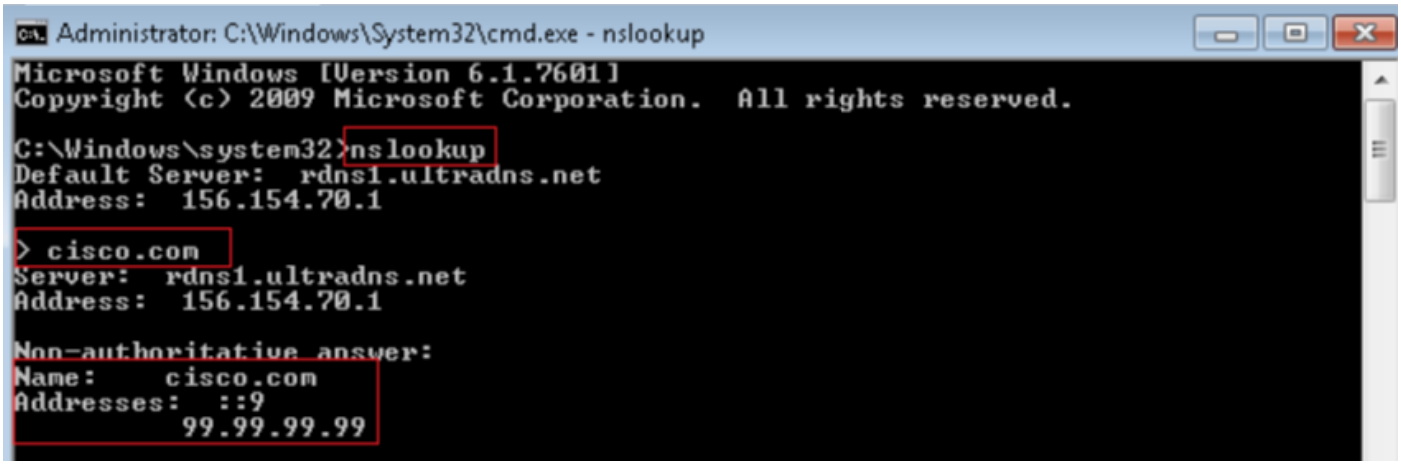


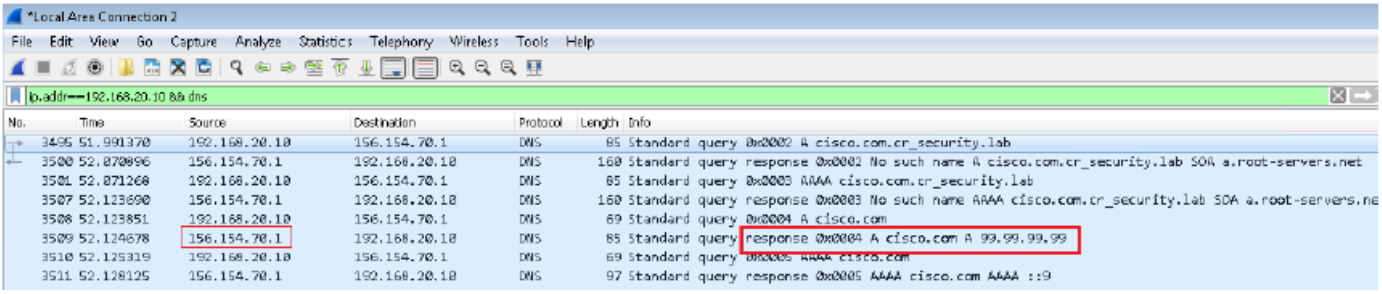
Étape 2. Appliquez le trou d'étranglement à votre stratégie DNS et déployez les modifications sur FTD.





Vérification du fonctionnement de Sinkhole





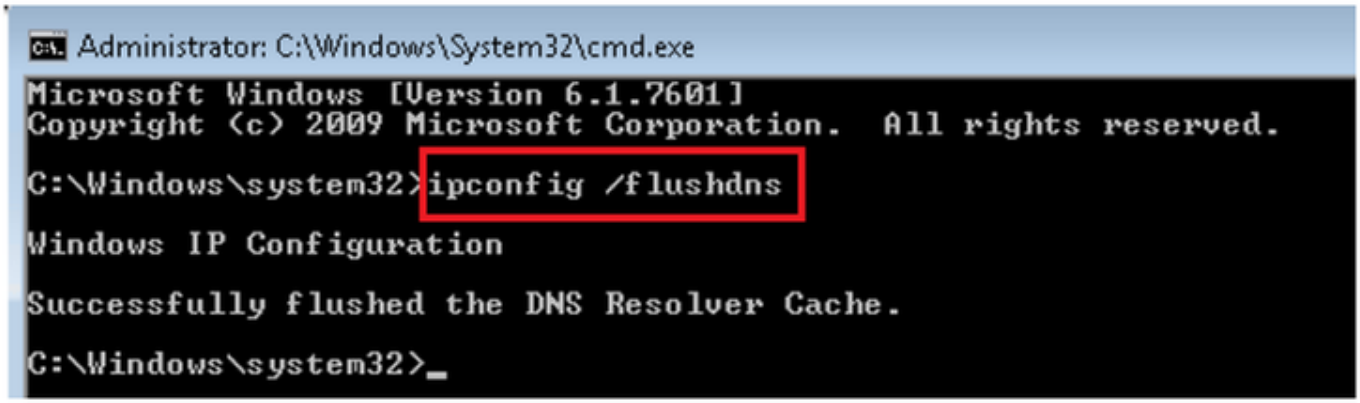
Dépannage

Accédez à Analyse » Connexions » Événements Security Intelligence pour suivre tous les événements déclenchés par SI tant que vous avez activé la connexion dans la stratégie DNS :

Vous pouvez également utiliser la commande **system support firewall-engine-debug** sur le FTD géré par le FMC.

```
>
> system support firewall-engine-debug

Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

Les captures de paquets peuvent être utiles pour confirmer que les requêtes DNS parviennent au serveur FTD. N'oubliez pas d'effacer le cache de votre hôte local lors du test.


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Windows\system32>