

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configurer une liste DNS personnalisée avec les domaines que nous voulons bloquer et charger la liste dans FMC](#)

[Ajouter une nouvelle stratégie DNS avec l'action configurée sur 'domaine introuvable'](#)

[Affecter la stratégie DNS à votre stratégie de contrôle d'accès](#)

[Vérification](#)

[Avant l'application de la stratégie DNS](#)

[Une fois la stratégie DNS appliquée](#)

[Configuration Sinkhole optionnelle](#)

[Vérification du fonctionnement de Sinkhole](#)

[Dépannage](#)

## 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.

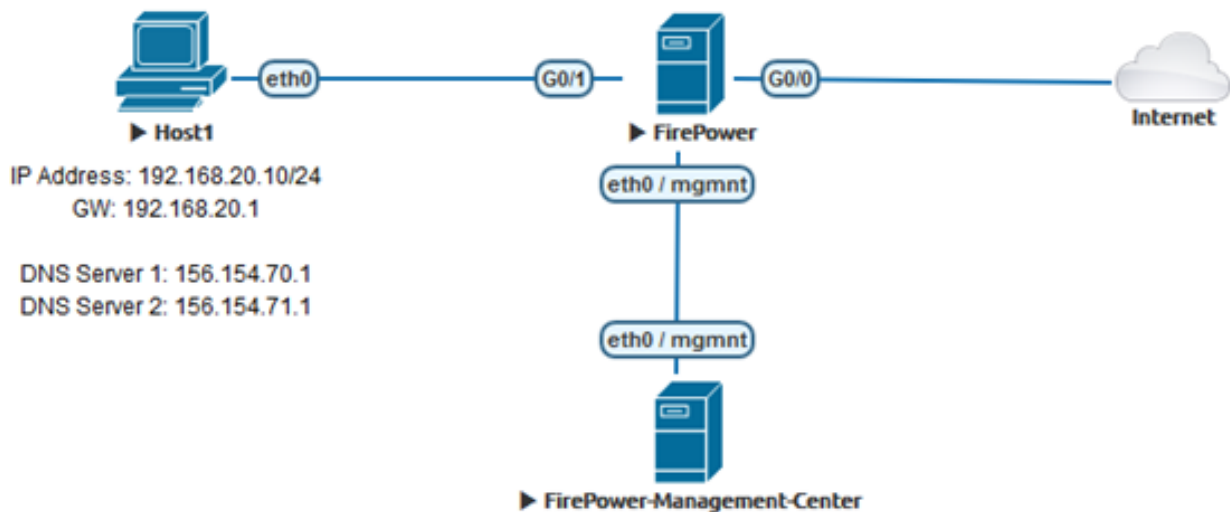
L'exemple a utilisé le domaine des blocs 1 :

- 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.

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

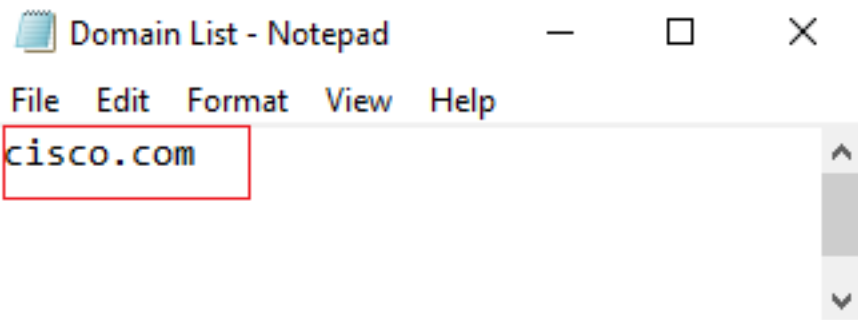
## Diagramme du réseau



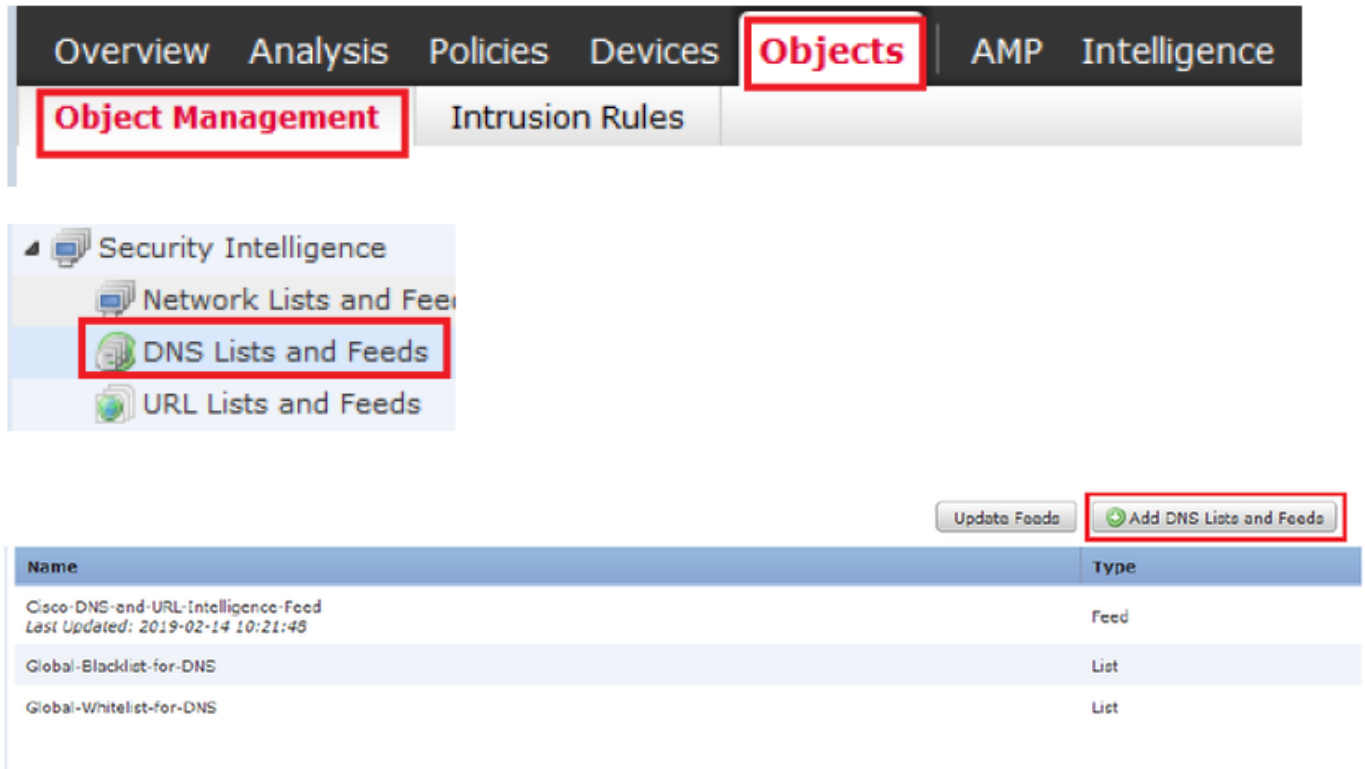
## Configuration

### 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 :

### Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

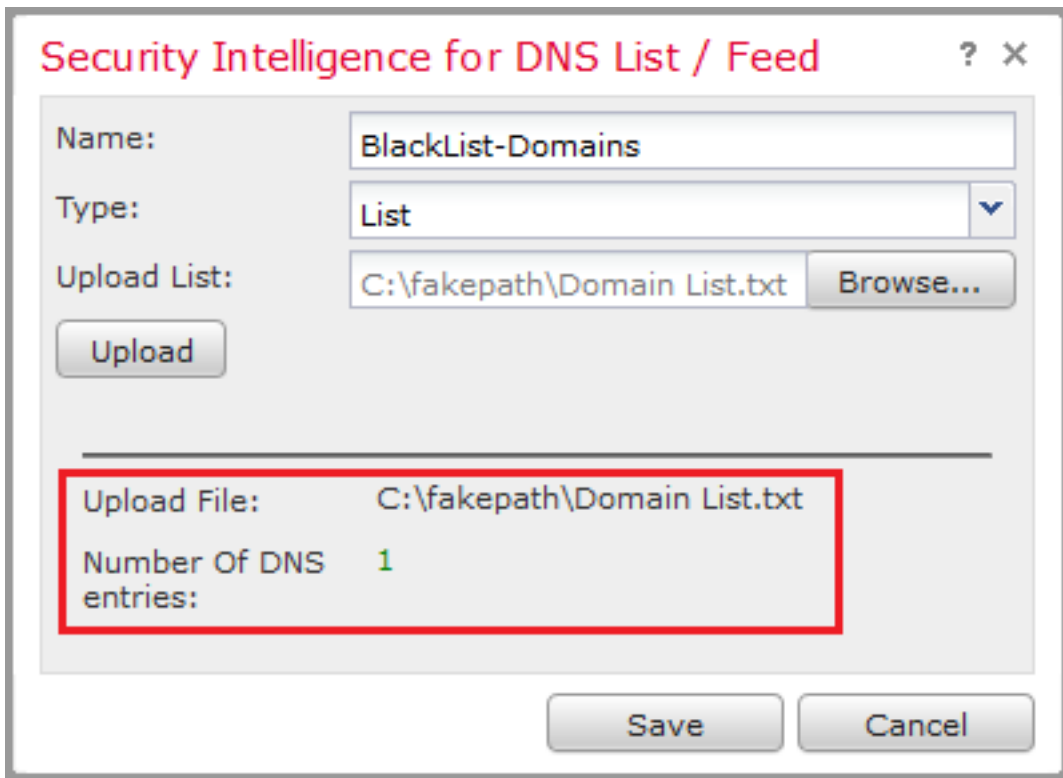
### Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

\*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 :

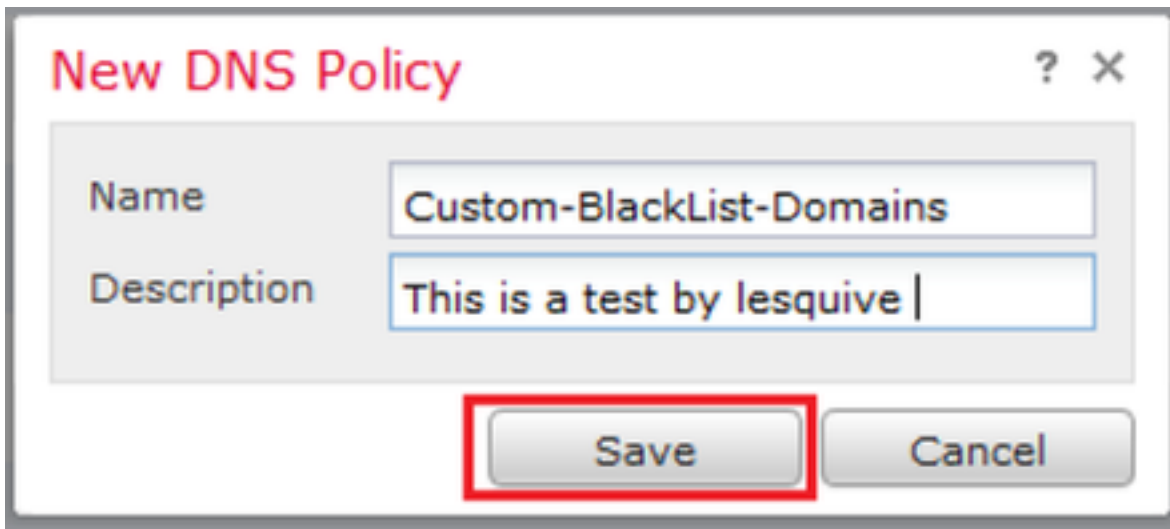


**Ajouter une nouvelle stratégie DNS avec l'action configurée sur 'domaine introuvable'**

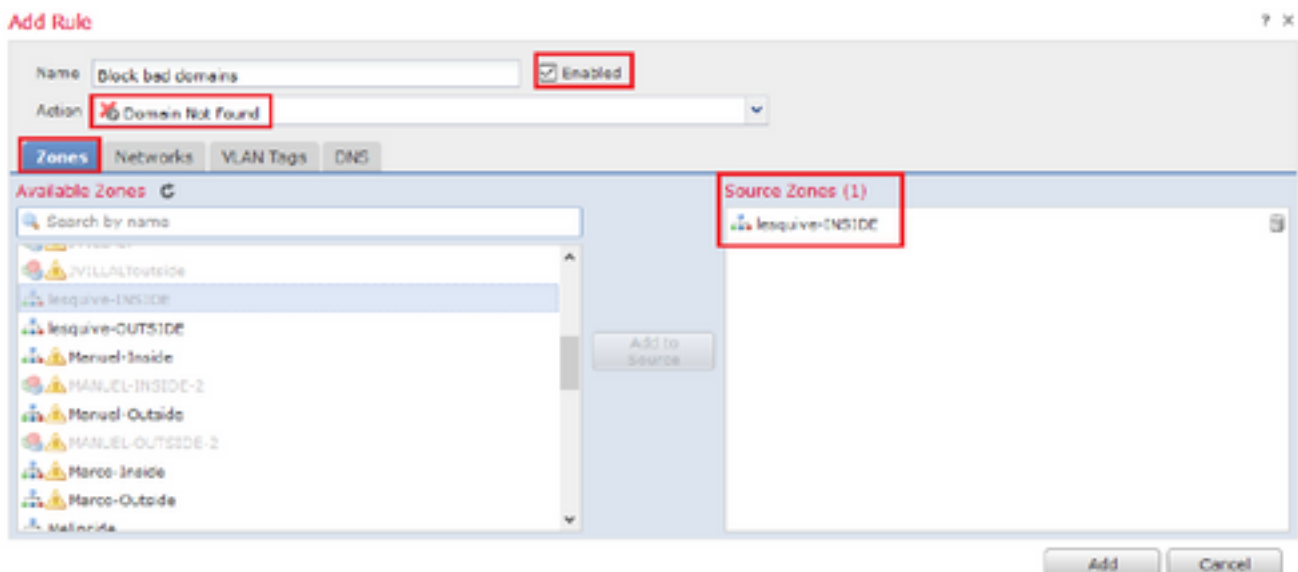
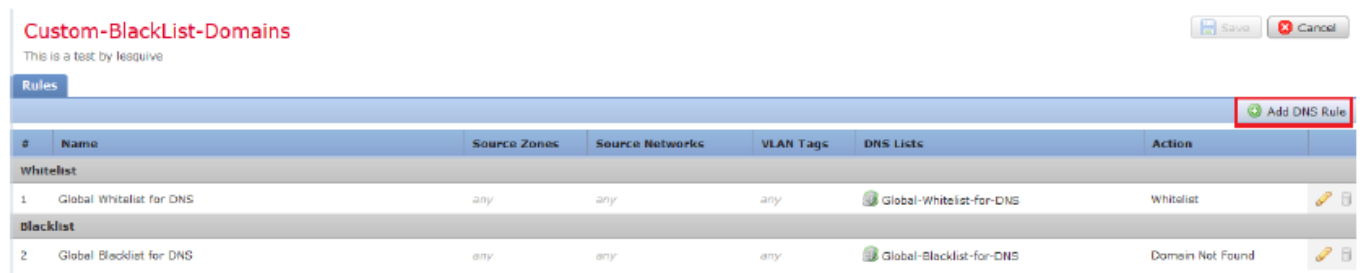
\*Assurez-vous d'ajouter une zone source, un réseau source et une liste DNS.

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

? X

Name:   Enabled

Action:

**Zones** | Networks | VLAN Tags | DNS

Available Zones

- Search by name
- JVILLALToutside
- lesquive-INSIDE
- lesquive-OUTSIDE
- Manuel-Inside
- MANUEL-INSIDE-2
- Manuel-Outside
- MANUEL-OUTSIDE-2
- Marco-Inside
- Marco-Outside
- Melincide

Source Zones (1)

- lesquive-INSIDE

Add to Source

Add Cancel

### Add Rule

? X

Name:   Enabled

Action:

**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\_Merco
- Outside-isaac
- pat-hugo
- Pat\_Marco

Source Networks (1)

- lesquive-network

Add to Source

Enter an IP address  Add

Add Cancel

### Add Rule

? X

Name:   Enabled

Action:

**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
- 0.0.0.0
- BlackList-Domains
- Global-Blocklist-for-DNS
- Global-Whitelist-for-DNS
- test

Selected Items (1)

- BlackList-Domains

Add to Rule

Add Cancel

#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
<b>Whitelist</b>						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
<b>Blacklist</b>						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Block bad domains	lesquive-INS	lesquive-network	any	BlackList-Domains	Sinkhole

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.

The screenshot shows the 'Policies' tab in the management console. Under 'Access Control', the 'lesquive-policy' is selected. The 'Security Intelligence' tab is active, and the 'DNS Policy' dropdown menu is set to 'Custom-BlackList-Domains'. A 'Save' button is visible, indicating unsaved changes.

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 :

```
Administrator: C:\Windows\System32\cmd.exe
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cr_security.lab

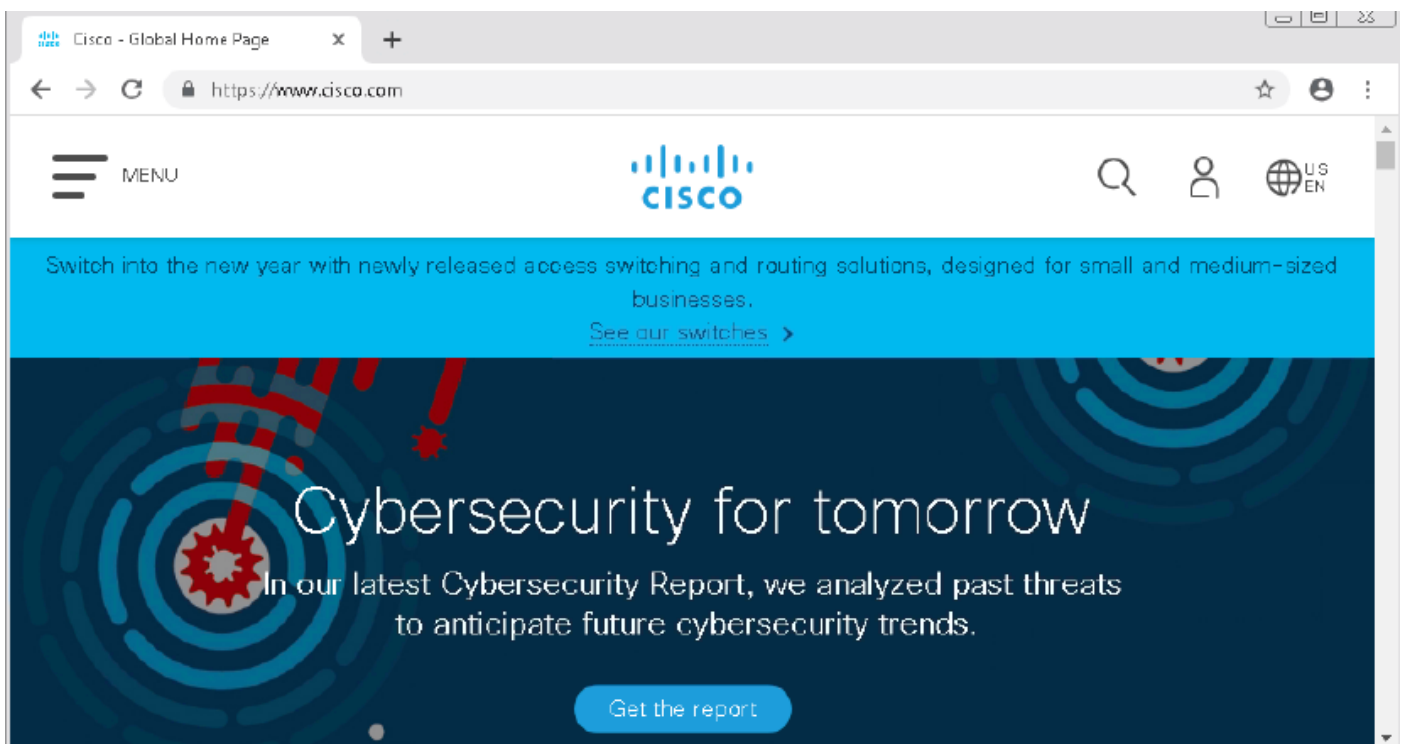
Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #
2
Physical Address. . . . . : 00-0C-29-3E-58-0D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b169:a9aa:5b12:217b%13(Preferred)
IPv4 Address. . . . . : 192.168.20.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fe0b:f277%13
                             fe80::20c:29ff:fef9:82bd%13
                             192.168.20.1
DNS Servers . . . . . : 156.154.70.1
                             156.154.71.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter DONT TOUCH !!!:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
```

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 :

The screenshot shows a network traffic capture in Wireshark. The top pane displays a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
3510	22.702417	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0004 A cisco.com
3515	22.746661	156.154.70.1	192.168.20.10	DNS	271	Standard query response 0x0004 A cisco.com A 72.163.4.185

The bottom pane shows the detailed view of frame 3515, which is a DNS response. The 'Answers' section is highlighted with a red box and contains the following information:

- Answers
  - cisco.com: type A, class IN, addr 72.163.4.185
    - Name: cisco.com
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 2573
    - Data length: 4
    - Address: 72.163.4.185

## Une fois la stratégie DNS appliquée

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

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

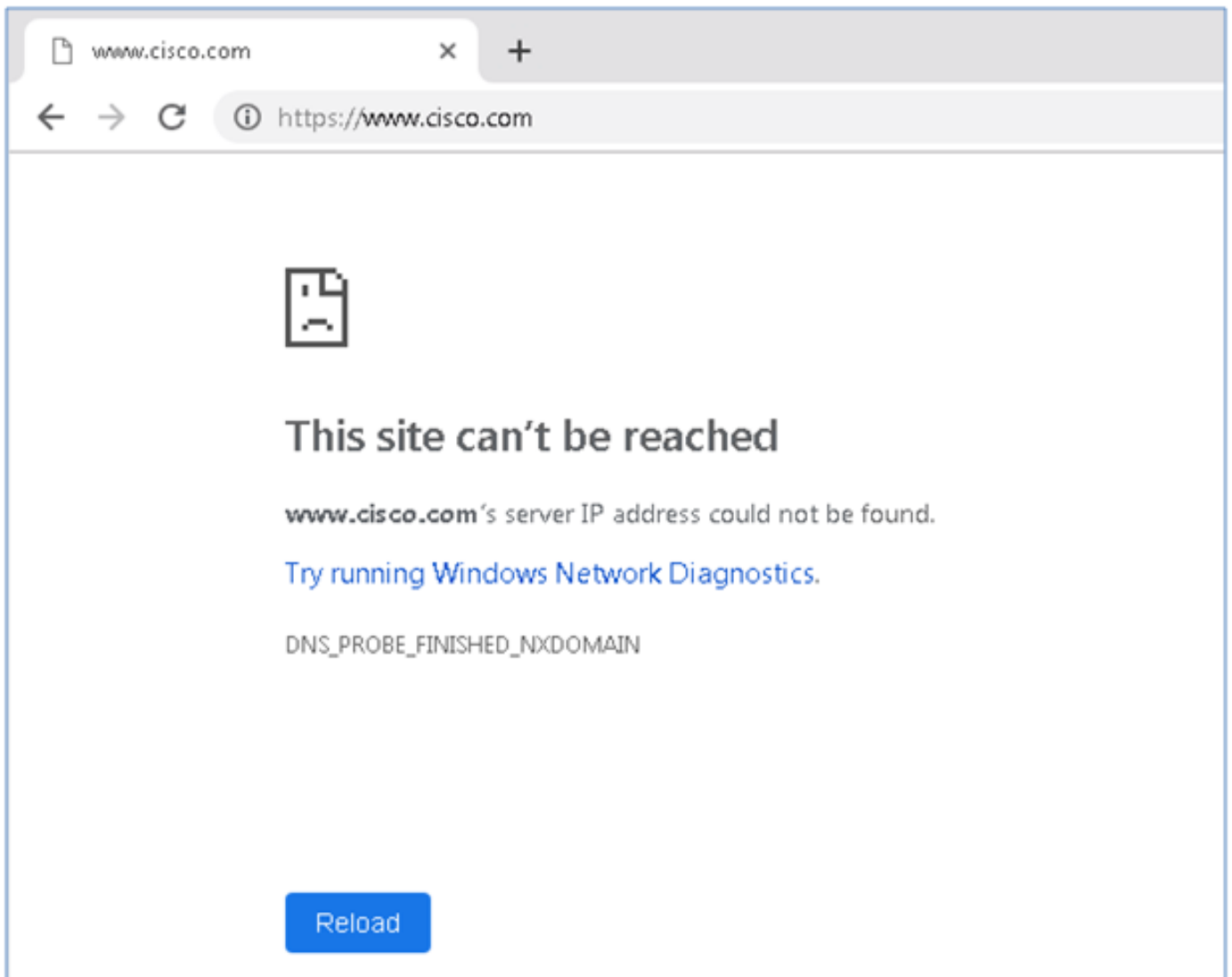
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
  
```

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.

```
Administrator: C:\Windows\System32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> nslookup
Default Server: rdnsl.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdnsl.ultradns.net
Address: 156.154.70.1

*** rdnsl.ultradns.net can't find cisco.com: Non-existent domain
```

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

Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 13

No.	Time	Source	Destination	Protocol	Length	Info
1617	11.205257	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0004 A cisco.com
1618	11.205926	156.154.70.1	192.168.20.10	DNS	69	Standard query response 0x0004 No such name A cisco.com

▶ Frame 1618: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0  
 ▶ Ethernet II, Src: Cisco\_cd:3a:fb (00:fe:c8:cd:3a:fb), Dst: Vmware\_3e:58:0d (00:0c:29:3e:58:0d)  
 ▶ Internet Protocol Version 4, Src: 156.154.70.1, Dst: 192.168.20.10  
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 50207  
 ▶ Domain Name System (response)  
     Transaction ID: 0x0004  
     ▶ Flags: 0x8503 Standard query response, No such name  
     Questions: 1  
     Answer RRs: 0  
     Authority RRs: 0  
     Additional RRs: 0  
     ▶ Queries  
         [Request In: 1617]  
         [Time: 0.000671000 seconds]

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

```
>
> 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
```

\*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

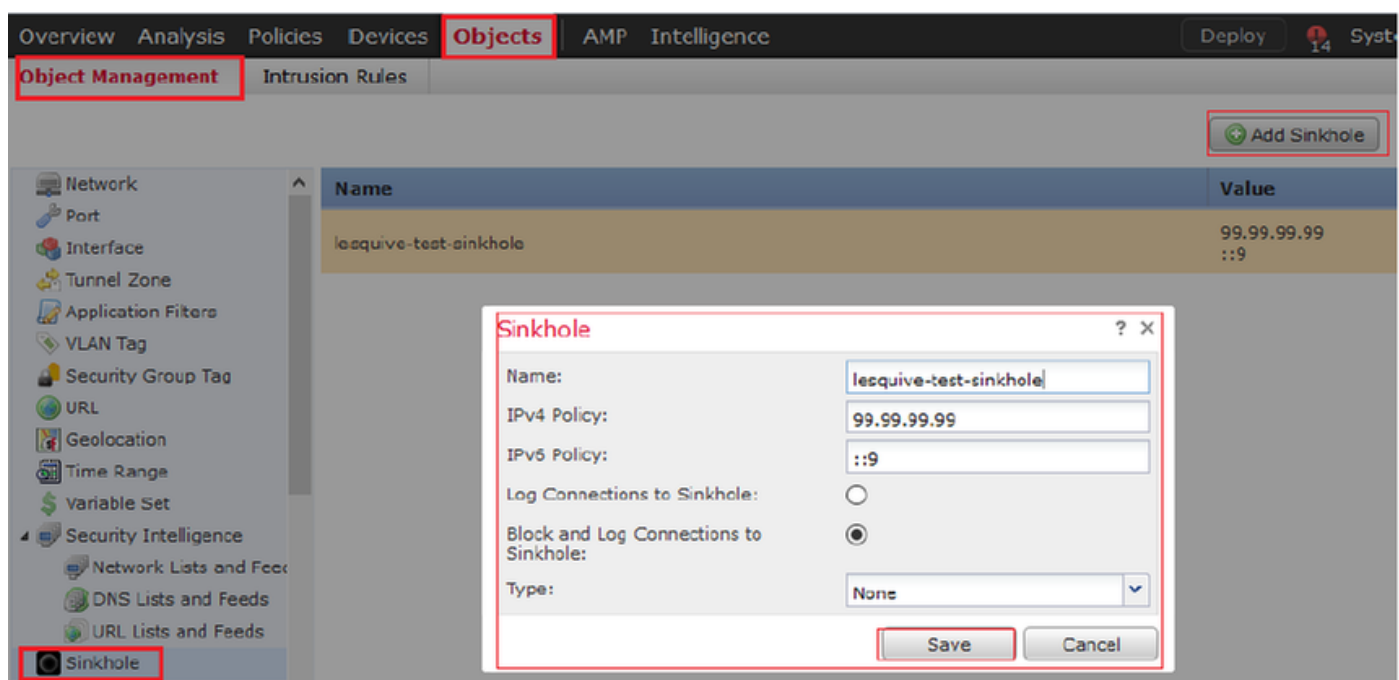
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.cr security.lab
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Skipping DNS rule lookup for cisco.com.cr security.lab since we've already gotten a response
192.168.20.10-61373 > 156.154.70.1-53 17 AS 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 intf's 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 intf's 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

```

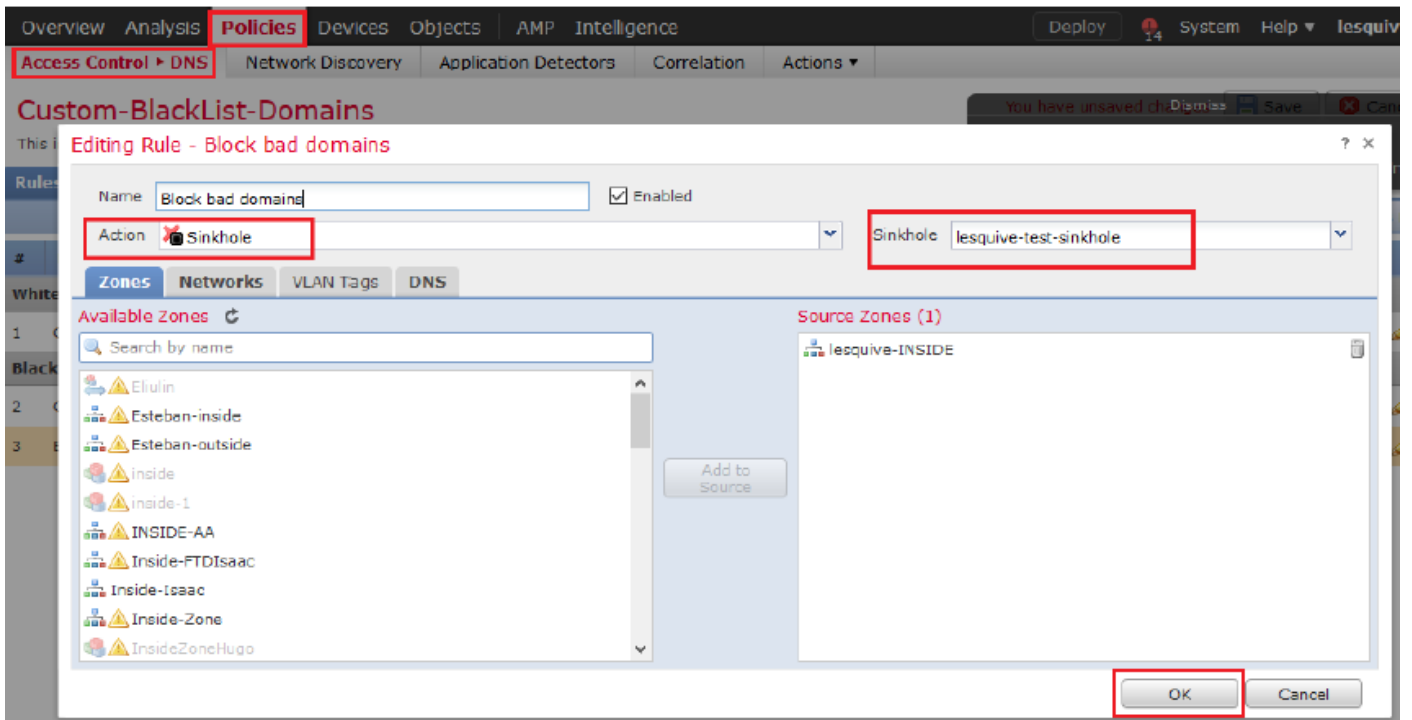
## Configuration Sinhole optionnelle

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.

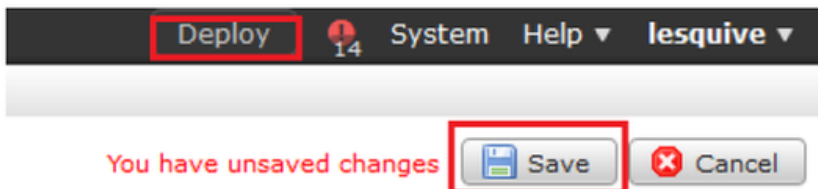
Étape 1. Naviguez jusqu'à Objets » Gestion des objets » Sinkhole » Ajouter Sinkhole et créez les fausses informations d'adresse IP.



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



#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
<b>Whitelist</b>						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
<b>Blacklist</b>						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Block bad domains	lesquive-INS...	lesquive-network	any	BlackList-Domains	Sinkhole



## Vérification du fonctionnement de Sinkhole

```
Administrator: C:\Windows\System32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server: rdns1.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdns1.ultradns.net
Address: 156.154.70.1

Non-authoritative answer:
Name: cisco.com
Addresses: ::9
          99.99.99.99
```

No.	Time	Source	Destination	Protocol	Length	Info
3495	51.991370	192.168.20.10	156.154.70.1	DNS	85	Standard query 0x0002 A cisco.com.cr_security.lab
3500	52.870896	156.154.70.1	192.168.20.10	DNS	160	Standard query response 0x0002 No such name A cisco.com.cr_security.lab SOA a.root-servers.net
3501	52.871268	192.168.20.10	156.154.70.1	DNS	85	Standard query 0x0003 AAAA cisco.com.cr_security.lab
3507	52.123890	156.154.70.1	192.168.20.10	DNS	160	Standard query response 0x0003 No such name AAAA cisco.com.cr_security.lab SOA a.root-servers.net
3508	52.123851	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0004 A cisco.com
3509	52.124678	156.154.70.1	192.168.20.10	DNS	85	Standard query response 0x0004 A cisco.com A 93.99.99.99
3510	52.125319	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0005 AAAA cisco.com
3511	52.128125	156.154.70.1	192.168.20.10	DNS	97	Standard query response 0x0005 AAAA cisco.com AAAA ::9

## 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 :

Security Intelligence Events [\[switch workflow\]](#)  
 Security Intelligence with Application Details > Table View of Security Intelligence Events  
 2019-02-14 13:42:42 - 2019-02-14 14:42:42 Expanding

No Search Constraints (Edit Search)

Jump to...

<input type="checkbox"/>	▼ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port	ICMP Type
↓	<input type="checkbox"/>	2019-02-14 14:36:57	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60548 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:36:57	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60547 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:36:52	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60544 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:36:52	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60543 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:36:41	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60540 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:36:41	Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60539 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:30:24	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	62087 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:30:24	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	61111 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:14:24	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	50590 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:14:24	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	62565 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:13:43	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60136 / udp	
↓	<input type="checkbox"/>	2019-02-14 14:13:43	Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	53647 / udp	

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>\_