BlokDNS met Security Intelligence met FireSIGHT Management Center

Inhoud

Inleiding

Dit document beschrijft de procedure om een DNS-lijst (Domain Name System) aan een DNS-beleid toe te voegen, zodat u deze met Security Intelligence (SI) kunt toepassen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA 5550X configuratie voor bedreigingsverdediging
- Cisco Firepower Management Center-configuratie

Gebruikte componenten

- Cisco ASA 5506W-X Threat Defense (75) versie 6.2.3.4 (gebouwd 42)
- Cisco FireSIGHT Management Center voor VMWare Softwareversie: 6.2.3.4 (bouw 42)IOS: Cisco FirePOWER Linux OS 6.2.3 (bouw13)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Security Intelligence werkt door verkeer naar of vanuit IP-adressen, URL's of domeinnamen te blokkeren die een bekende slechte reputatie hebben. In dit document ligt de nadruk vooral op zwarte lijsten van domeinnamen.

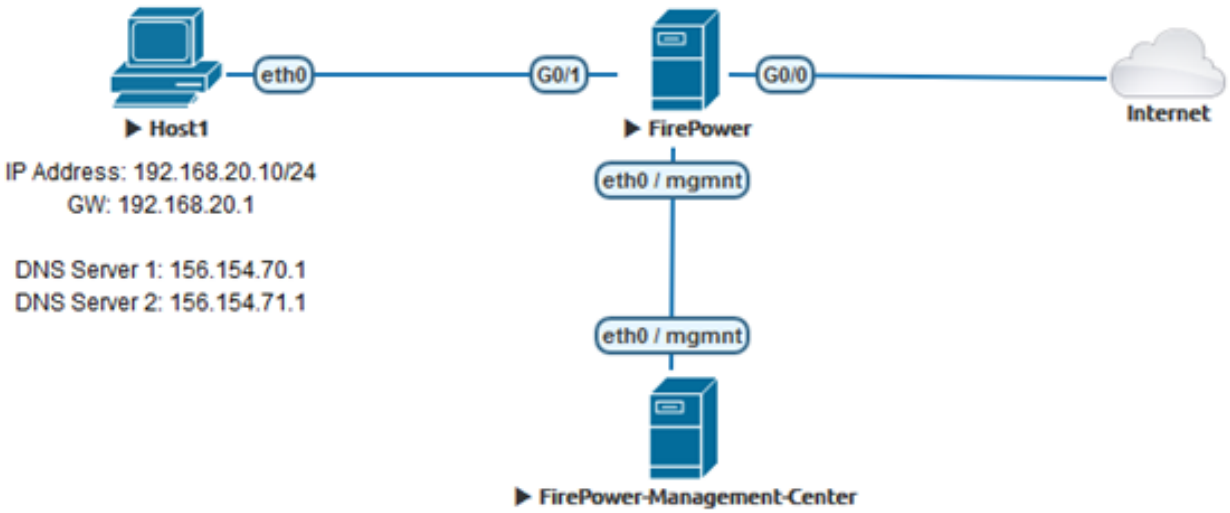
Het voorbeeld gebruikte blokken 1 domein:

- cisco.com

U kunt URL-filtering gebruiken om een aantal van deze sites te blokkeren, maar het probleem is dat de URL een exacte overeenkomst moet zijn. Aan de andere kant kan DNS-blokkering met SI zich op domeinen als "cisco.com" richten zonder zich zorgen te hoeven maken over subdomeinen of veranderingen in URL.

Aan het eind van dit document wordt ook een optionele configuratie van het Sinkgat aangetoond.

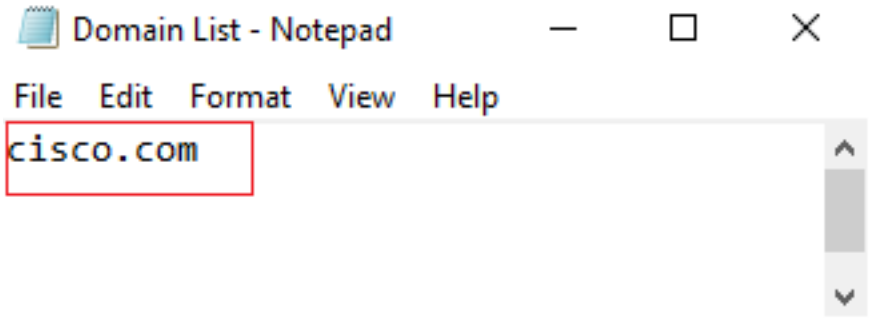
Netwerkdiagram



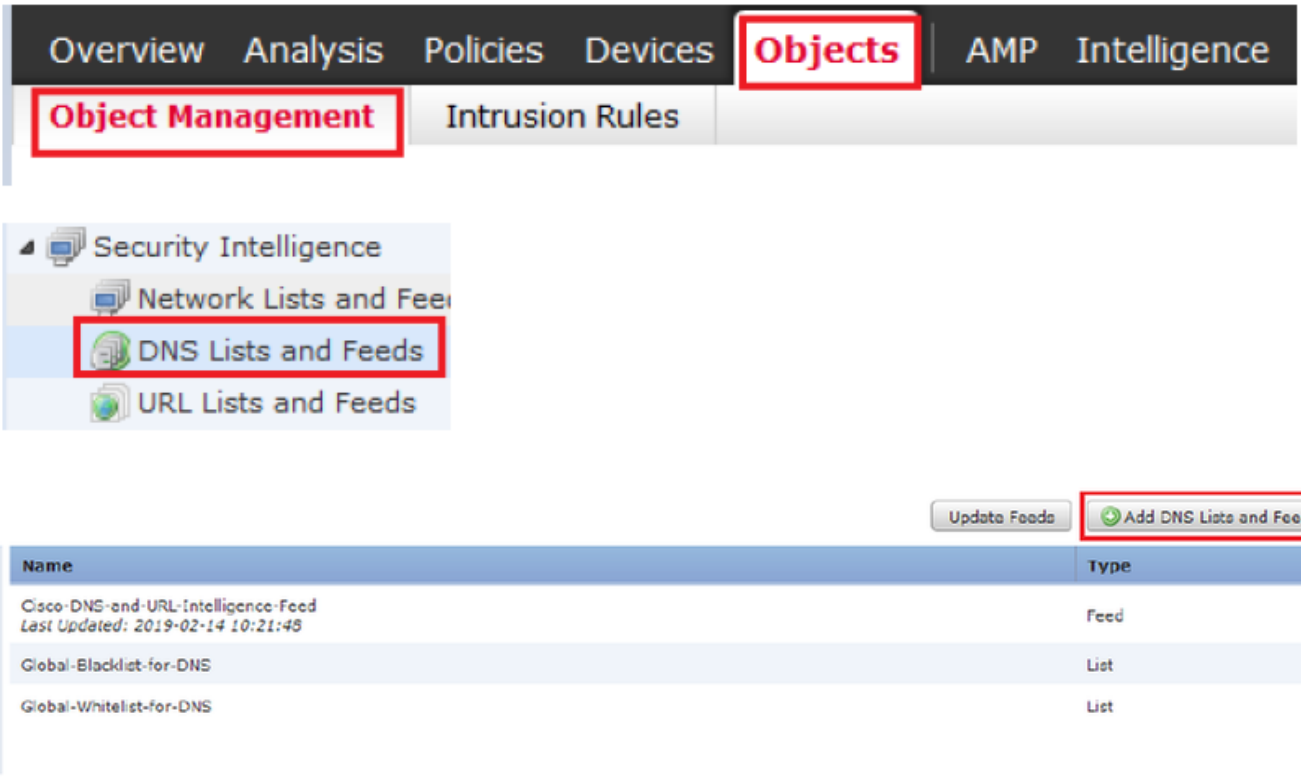
Configureren

Configuratie van een aangepaste DNS-lijst met de domeinen die we willen blokkeren en uploaden de lijst naar FMC

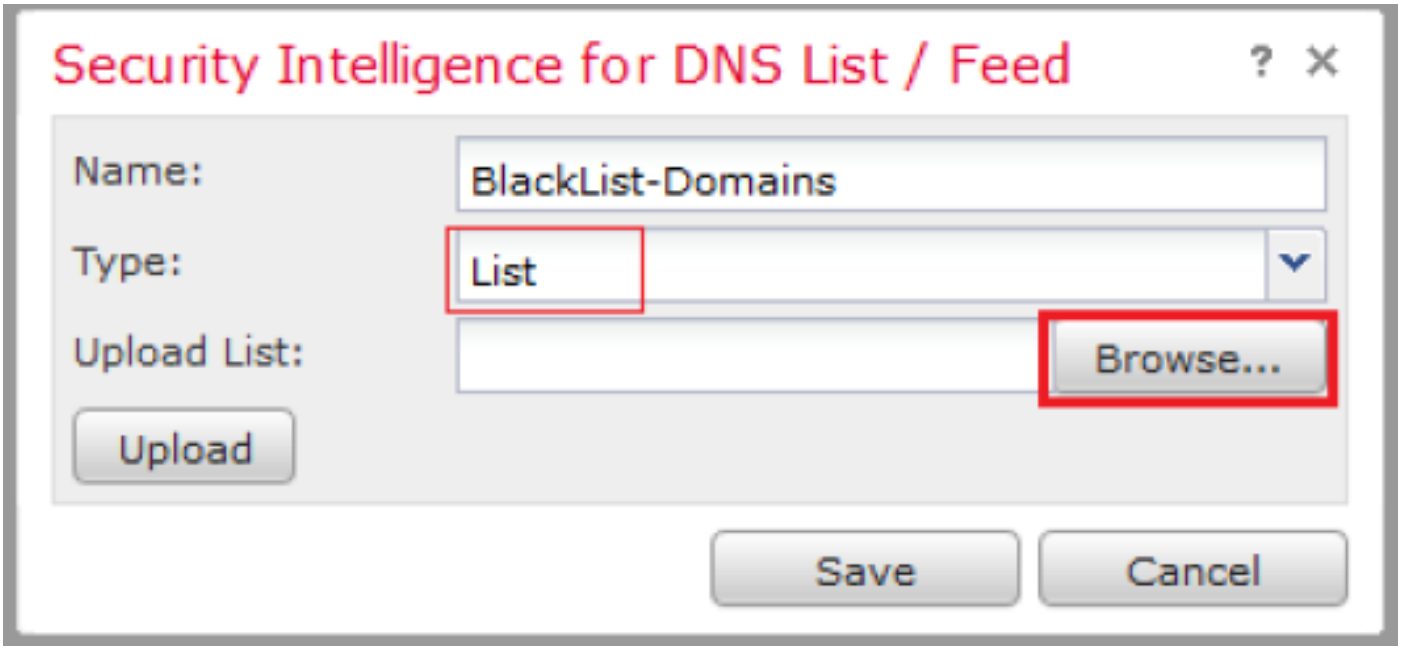
Stap 1. Maak een .txt-bestand met de domeinen die u wilt blokkeren. Sla het .txt-bestand op de computer op:

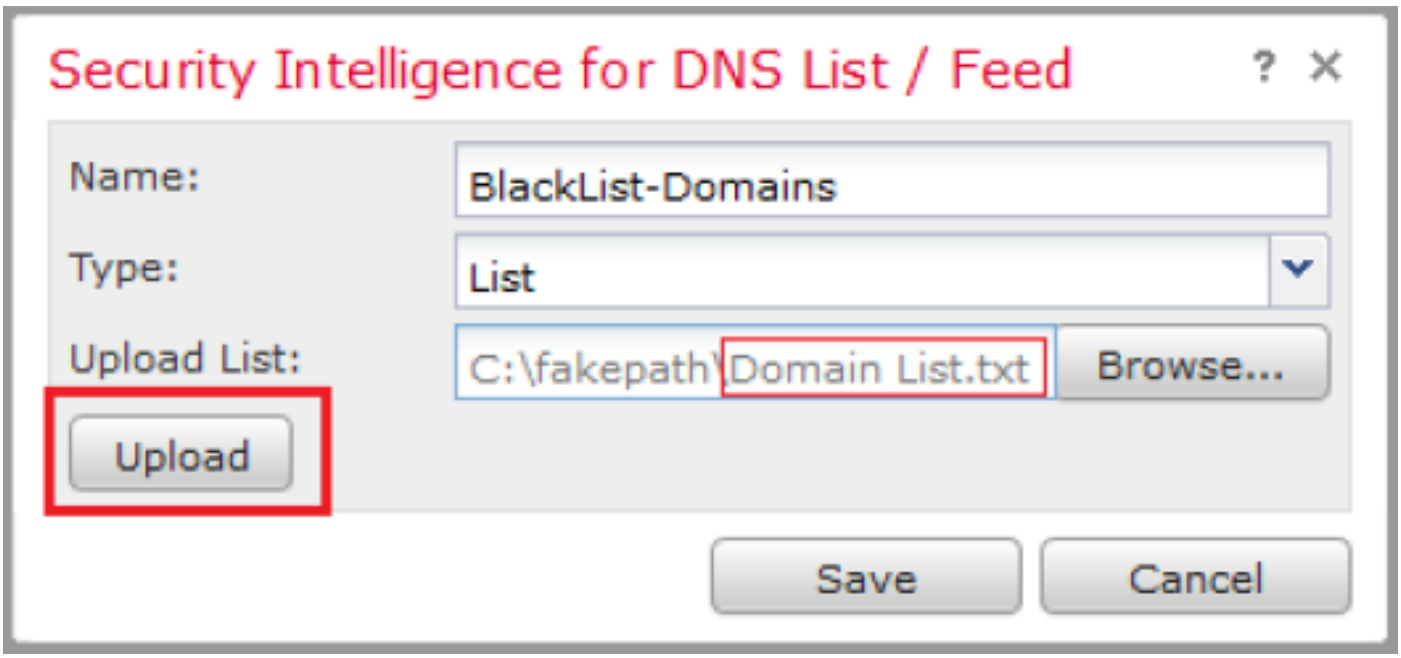


Stap 2. In FMC navigeer u om object > Objectbeheer > DNS-lijsten en velden >> DNS-lijst en velden toevoegen.

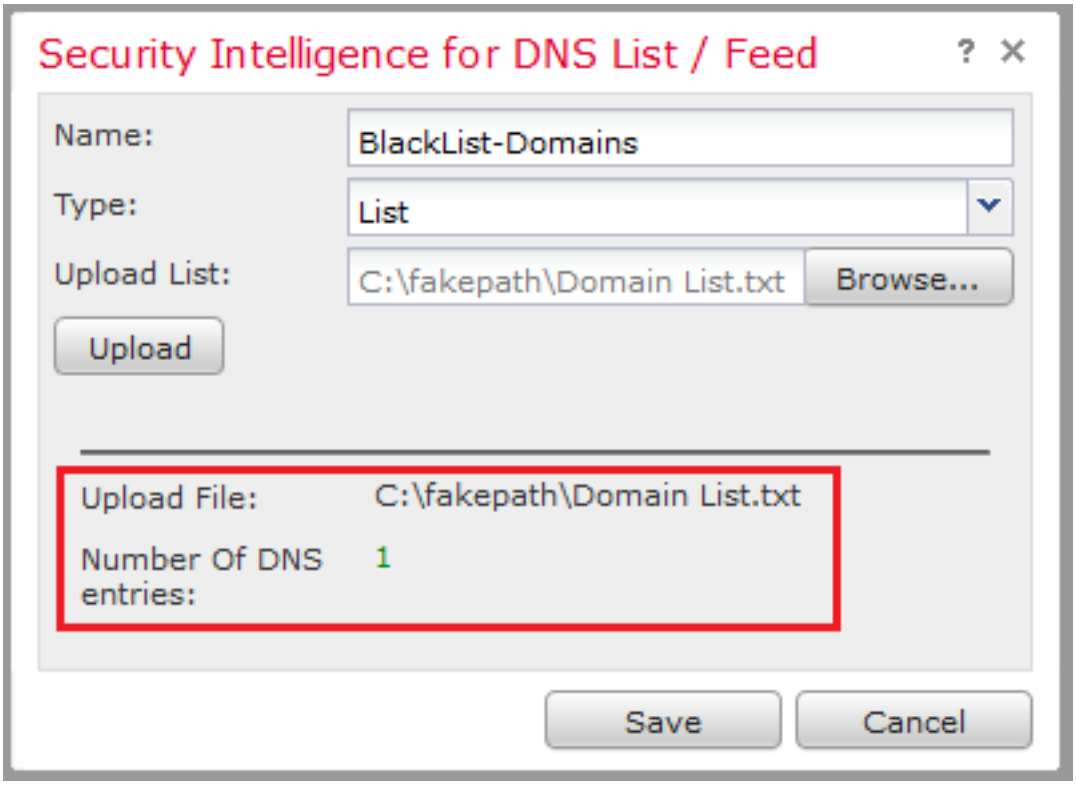


Stap 3. Maak een lijst met de naam "BlackList-Domains", het type is een lijst en het .txt-bestand met de betrokken domeinen moet zoals in de afbeeldingen worden geüpload:





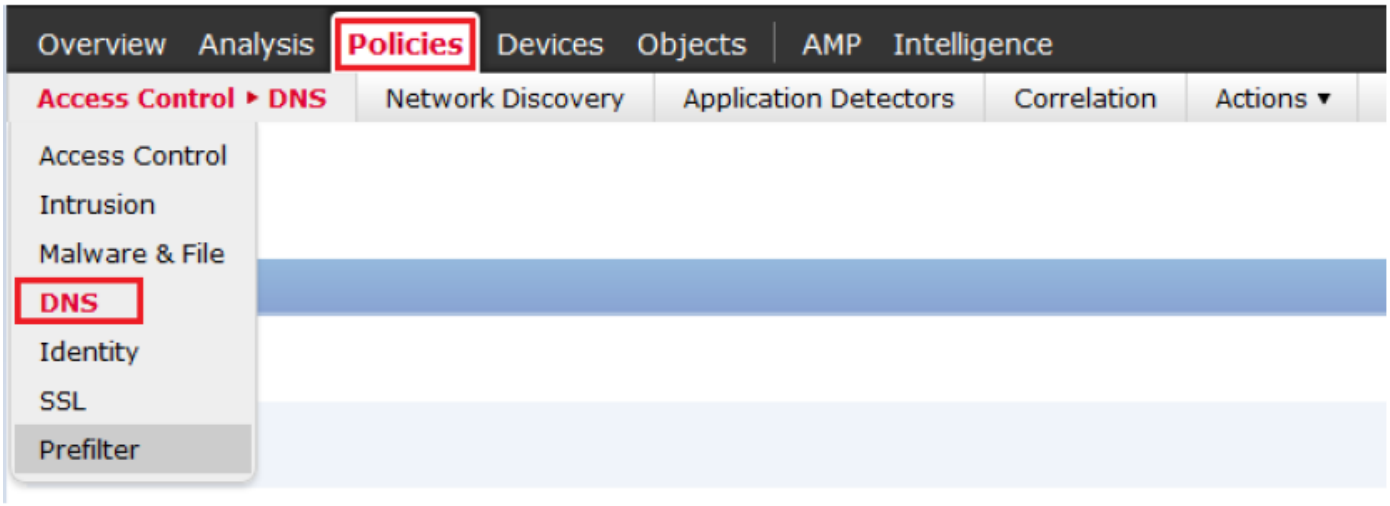
*Merk op dat wanneer u het .txt-bestand uploaden, het aantal DNS-items alle domeinen moet lezen. In dit voorbeeld in totaal 1:

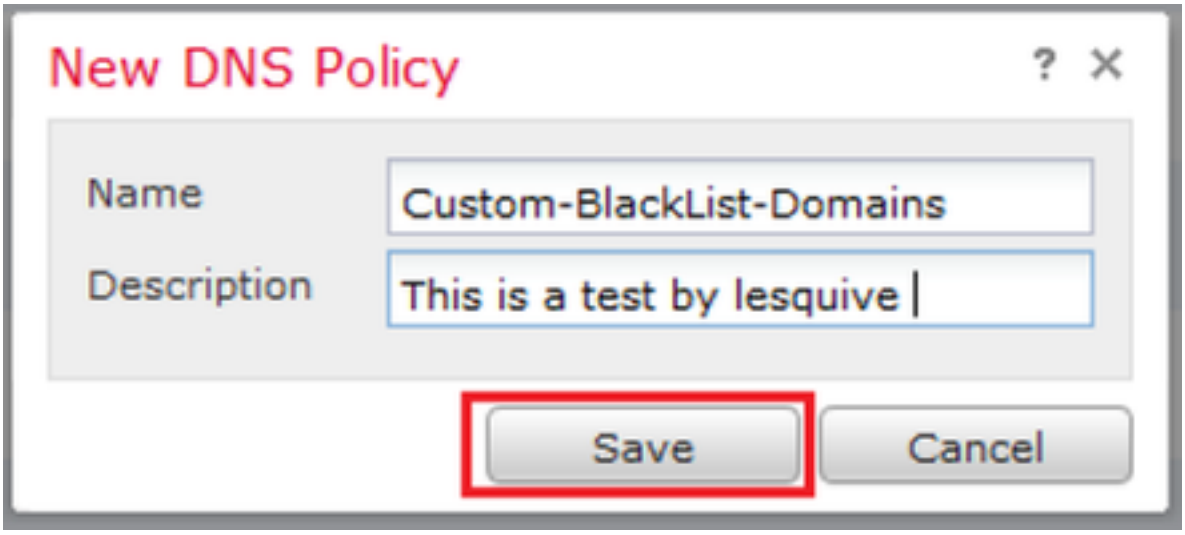


Voeg een nieuw DNS-beleid toe met de 'actie ingesteld op 'domeinniet gevonden'

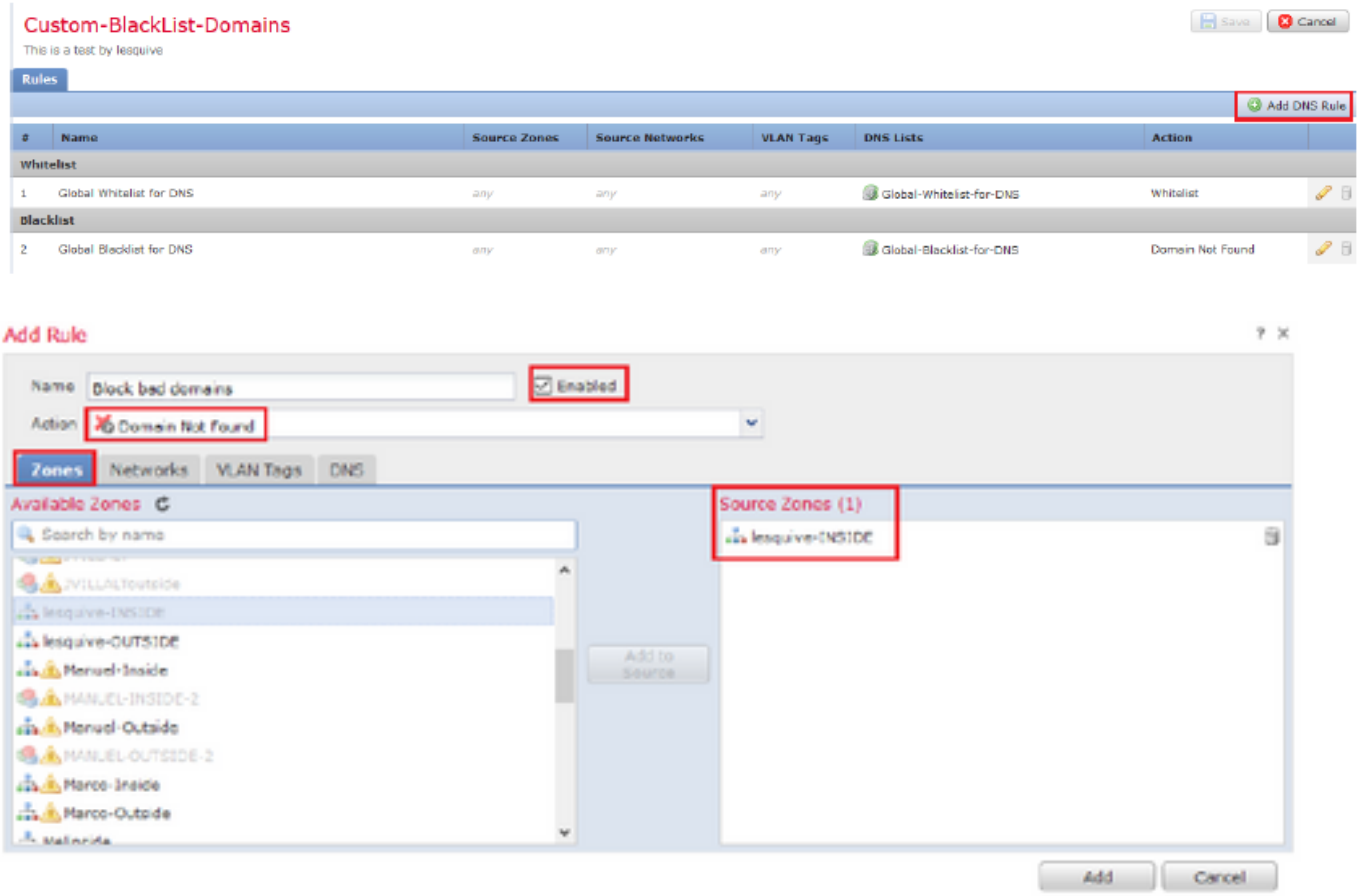
*Zorg ervoor dat u een bronzone, bronnetwerk en DNS-lijst toevoegt.

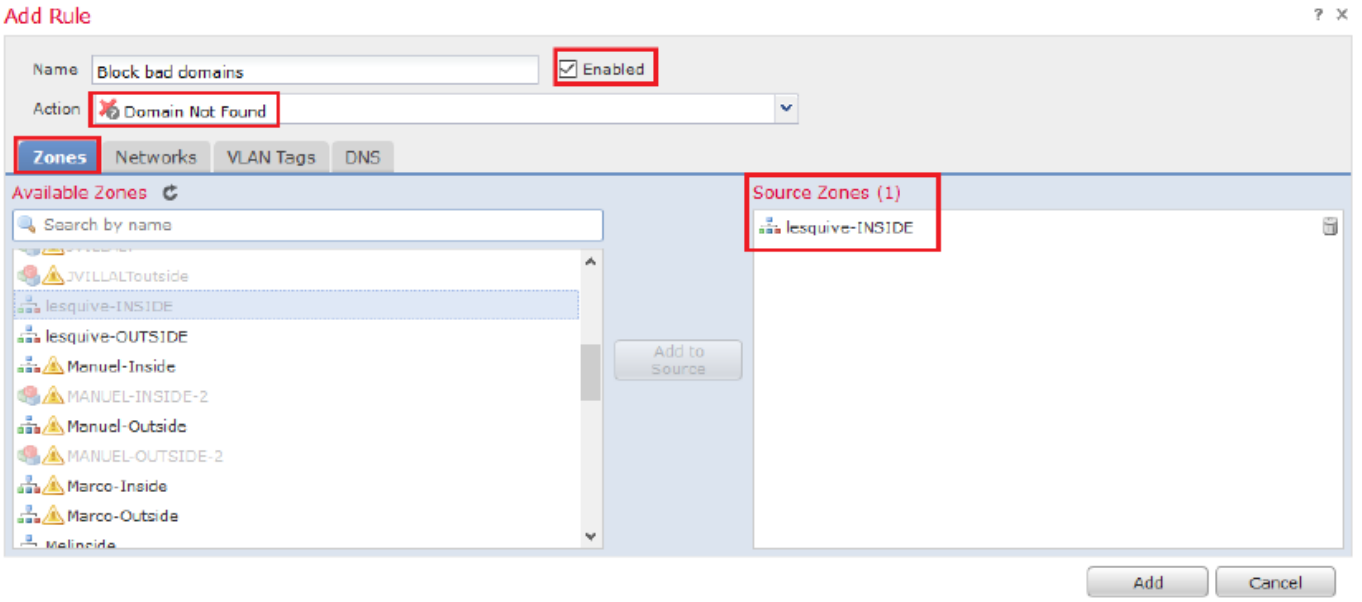
Stap 1. navigeren naar beleid > Toegangsbeheer > DNS > Toevoegen DNS-beleid:

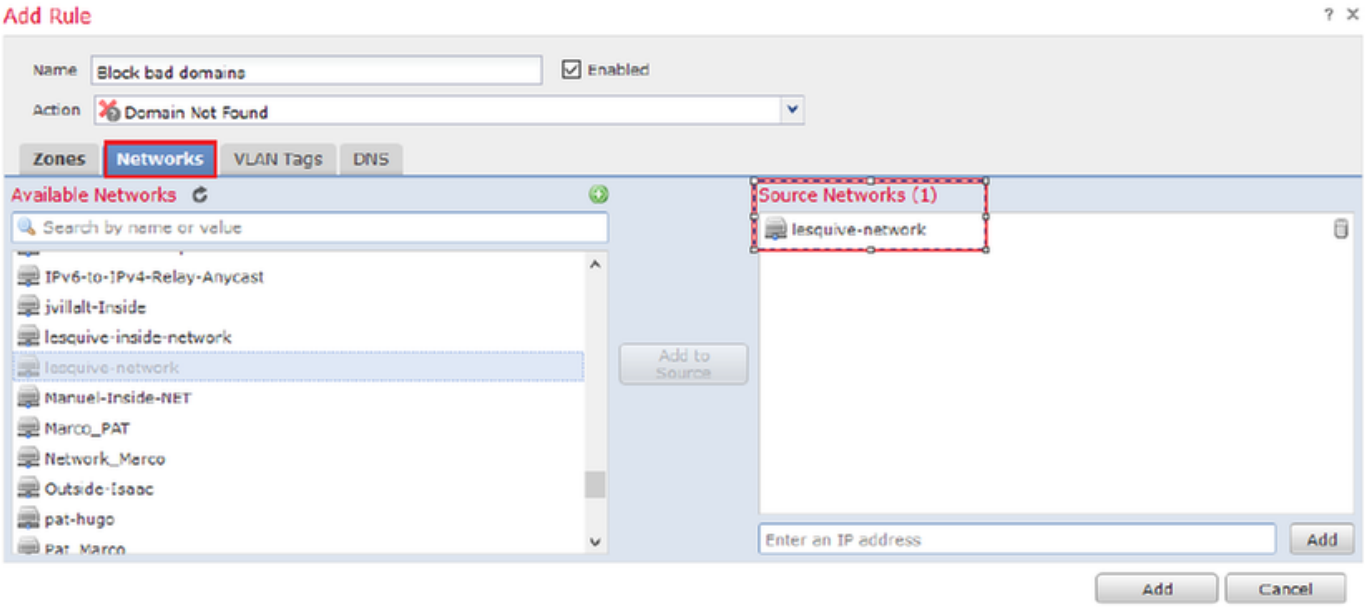


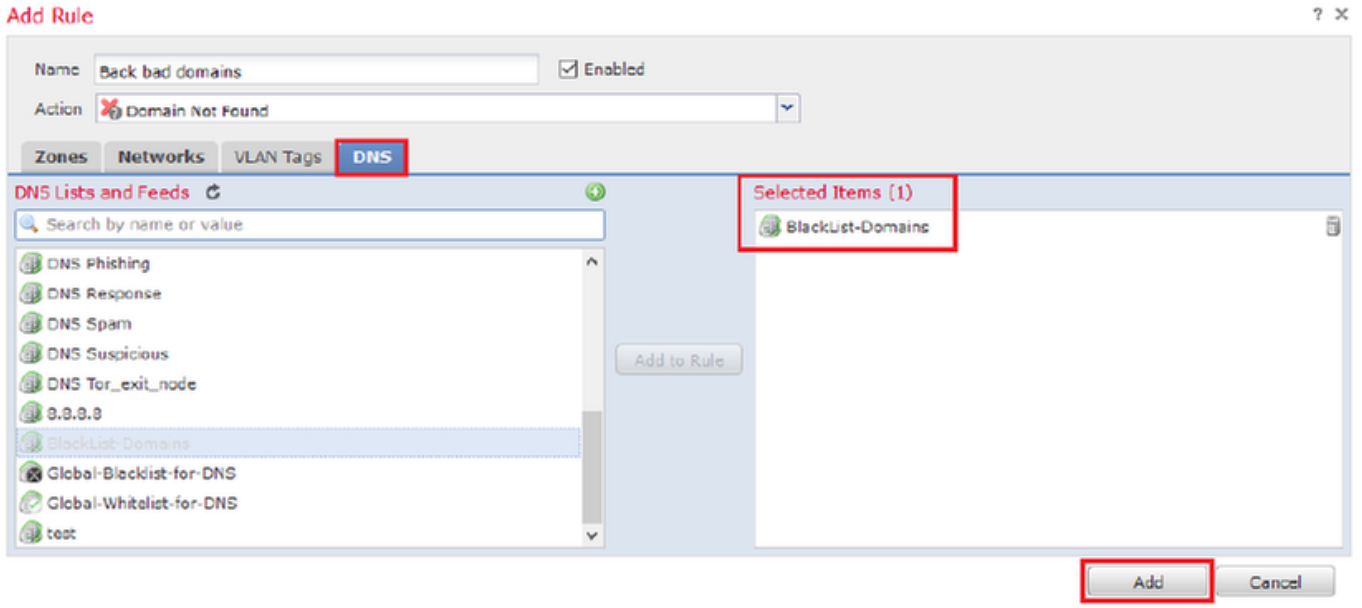


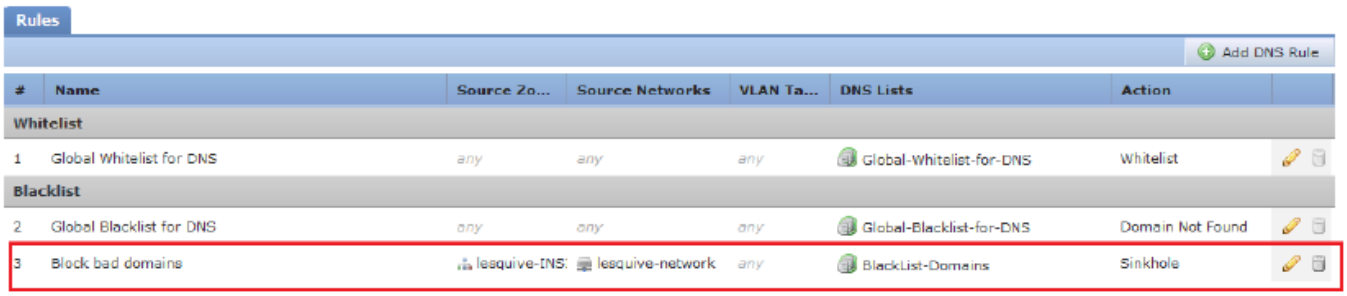
Stap 2. Voeg een DNS-regel toe zoals in de afbeelding:




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

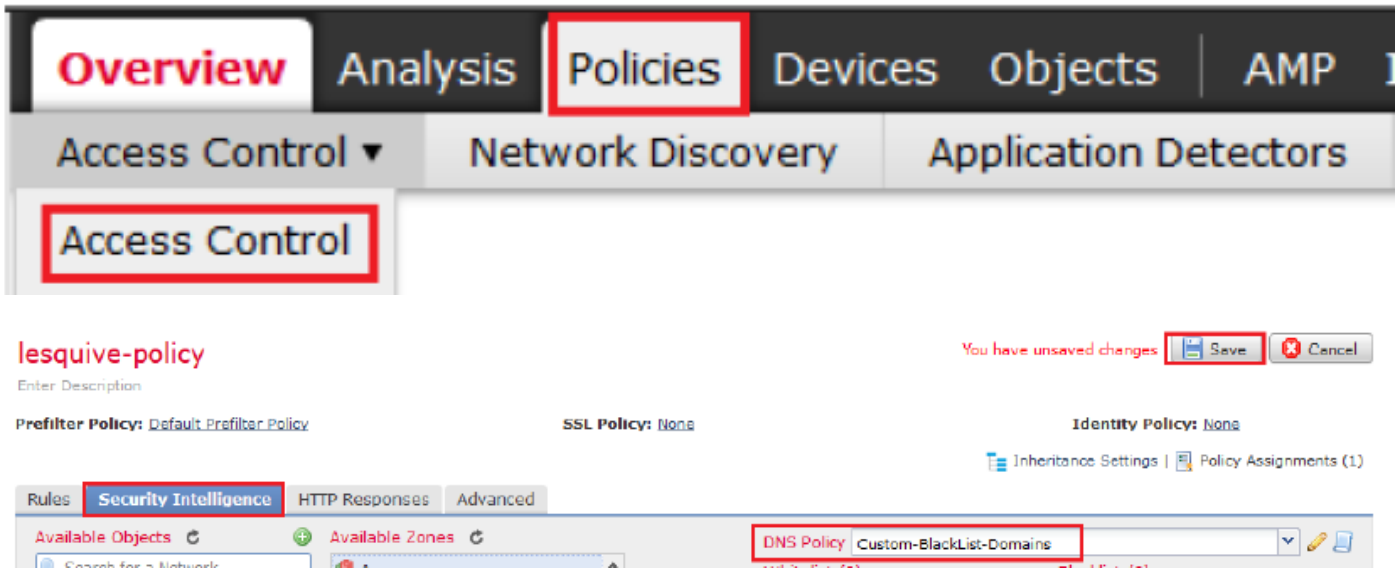


Belangrijke informatie over de volgorde van de regels:

- Het mondiale Whitelist is altijd de eerste en heeft voorrang op alle andere regels.
- De DNS-Whitelists-regel van descendant verschijnt alleen in implementaties met meerdere domeinen, in niet-bladdomeinen. Het is altijd de tweede en krijgt voorrang boven alle andere regels, behalve het Mondiale Whitelist.
- Het Whitelist-gedeelte gaat vooraf aan de Blacklist-sectie. blanke regels hebben altijd voorrang boven andere regels .
- The Global Blacklist is altijd de eerste in de Blacklist sectie en heeft voorrang op alle andere Monitor en zwarte list regels.
- De DNS Blacklists-regel van Descendant verschijnt alleen in implementaties met meerdere domeinen, in niet-bladeservers. Het is altijd de tweede in de Blacklist sectie en krijgt voorrang boven alle andere Monitor en zwarte list regels behalve de Global Blacklist.
- De sectie Blacklist bevat monitorregels en zwarte lijsten.
- Wanneer u voor het eerst een DNS-regel maakt, ligt de systeempositie als laatste in het Whitelist-gedeelte als u een Whitelist-actie toewijst of in het Blacklist-gedeelte als u een andere actie toewijst

Wijs het DNS-beleid aan uw toegangsbeheerbeleid toe

Ga naar beleid > Toegangsbeheer >> Het beleid voor uw FTD > Beveiligingsinformatie > DNS-beleid en voeg het beleid toe dat u hebt gemaakt.

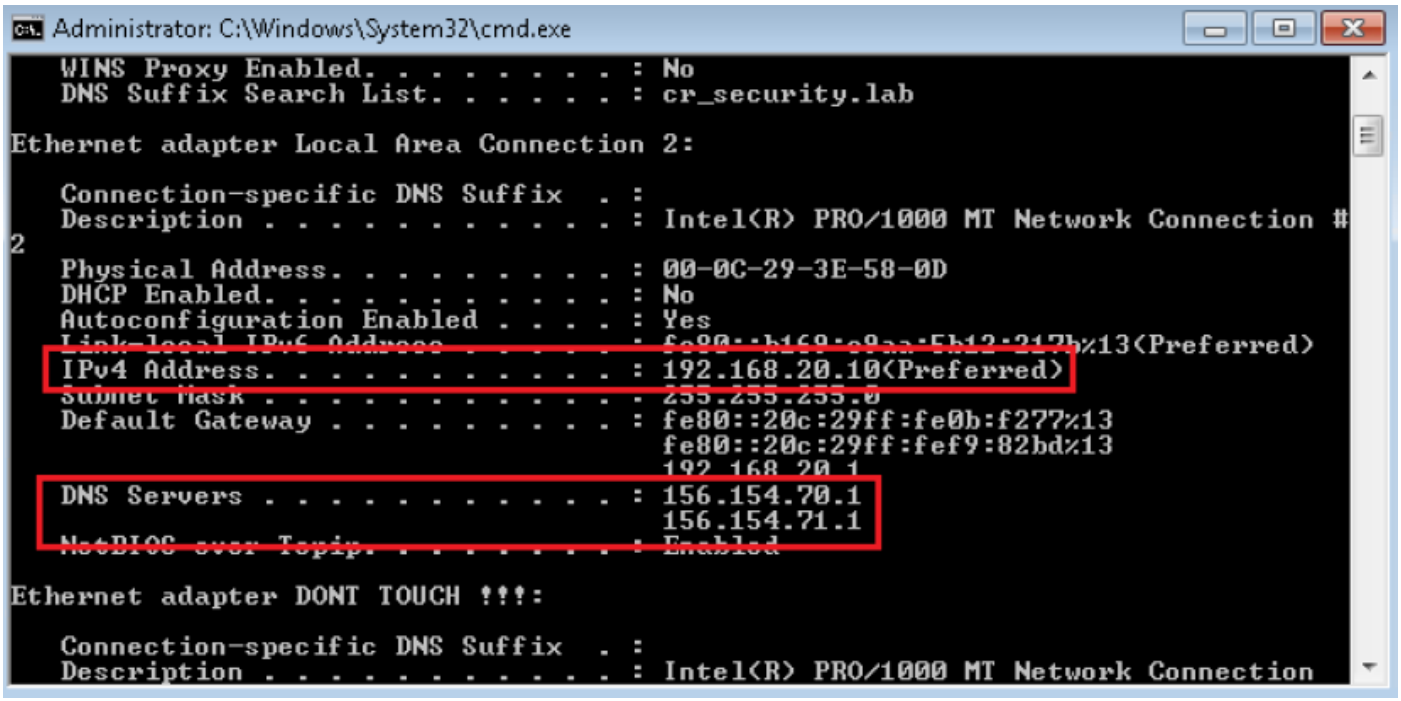


Zorg ervoor dat u alle veranderingen na voltooiing opstelt.

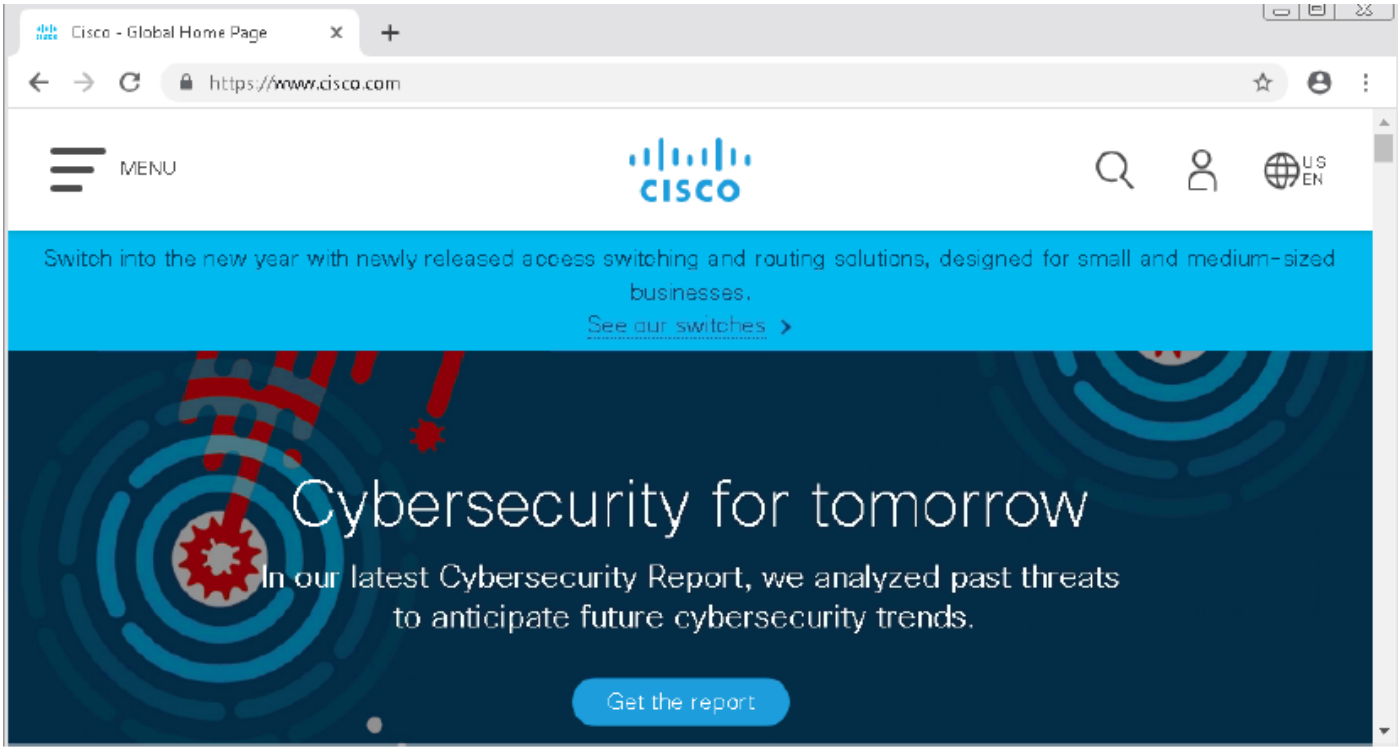
Verifiëren

Voordat het DNS-beleid wordt toegepast

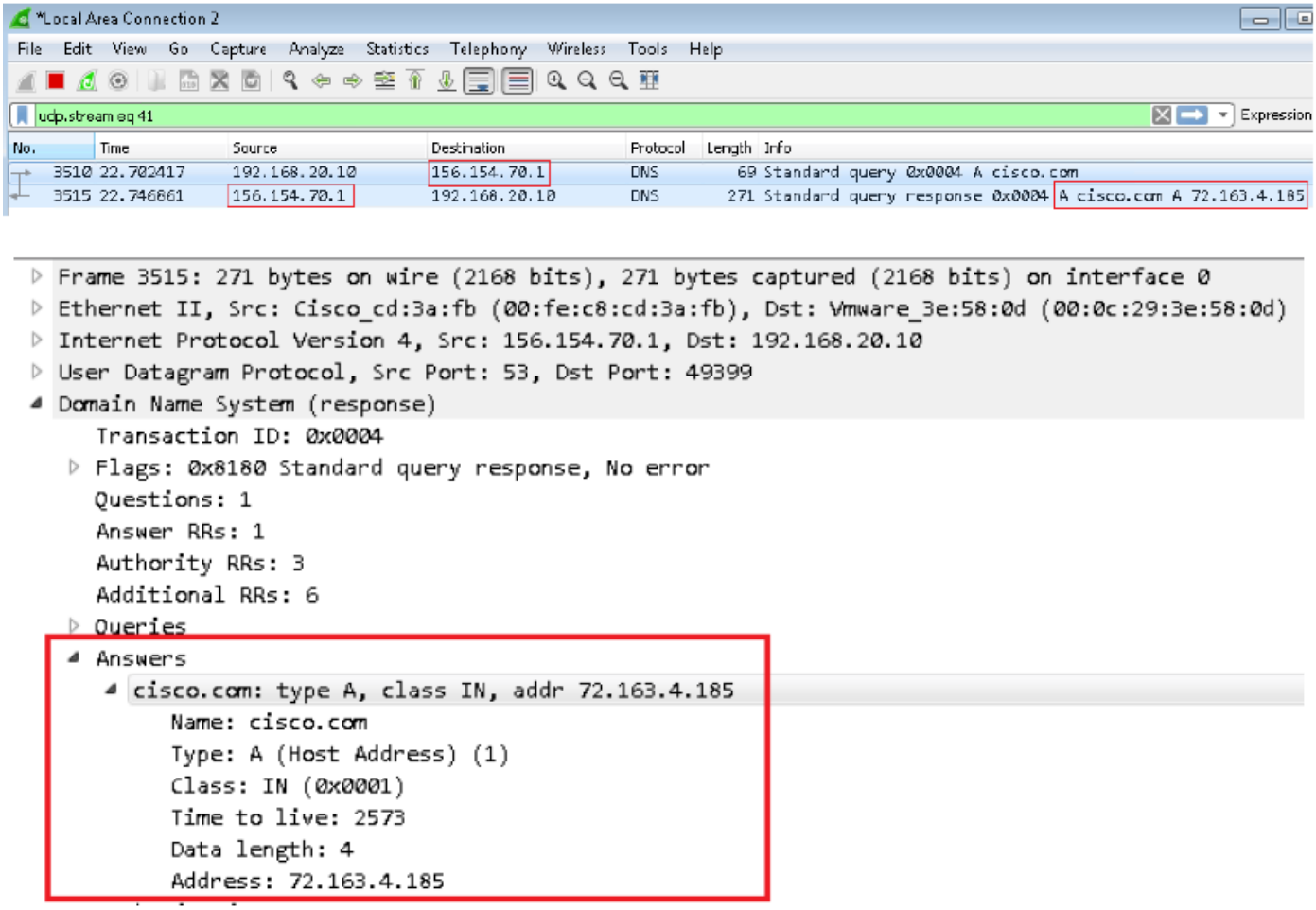
Stap 1. Controleer de DNS-server en IP-adresinformatie op uw host-machine zoals in de afbeelding:



Stap 2. Bevestig dat u naar cisco.com kunt navigeren zoals in de afbeelding:

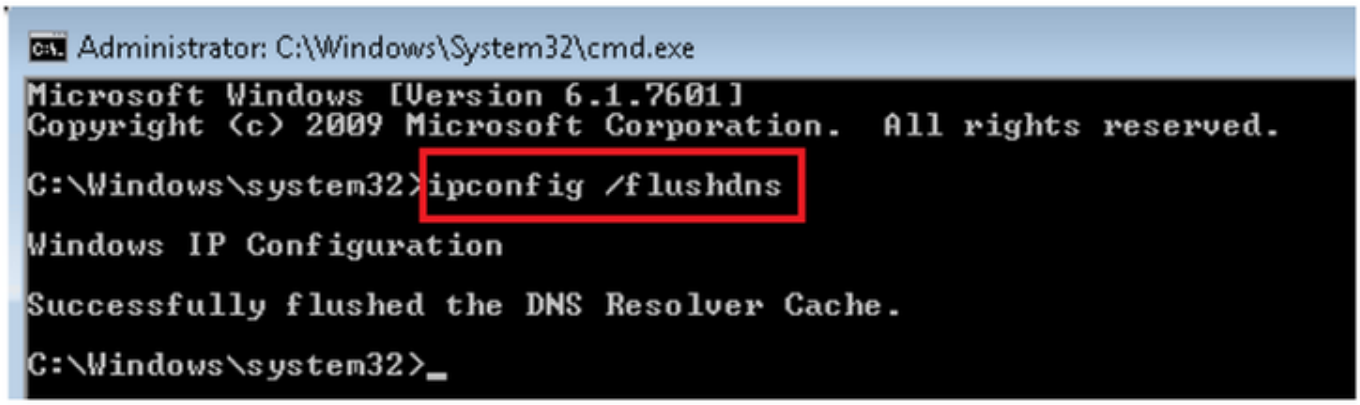


Stap 3. Controleer met pakketvastlegging dat DNS correct is opgelost:

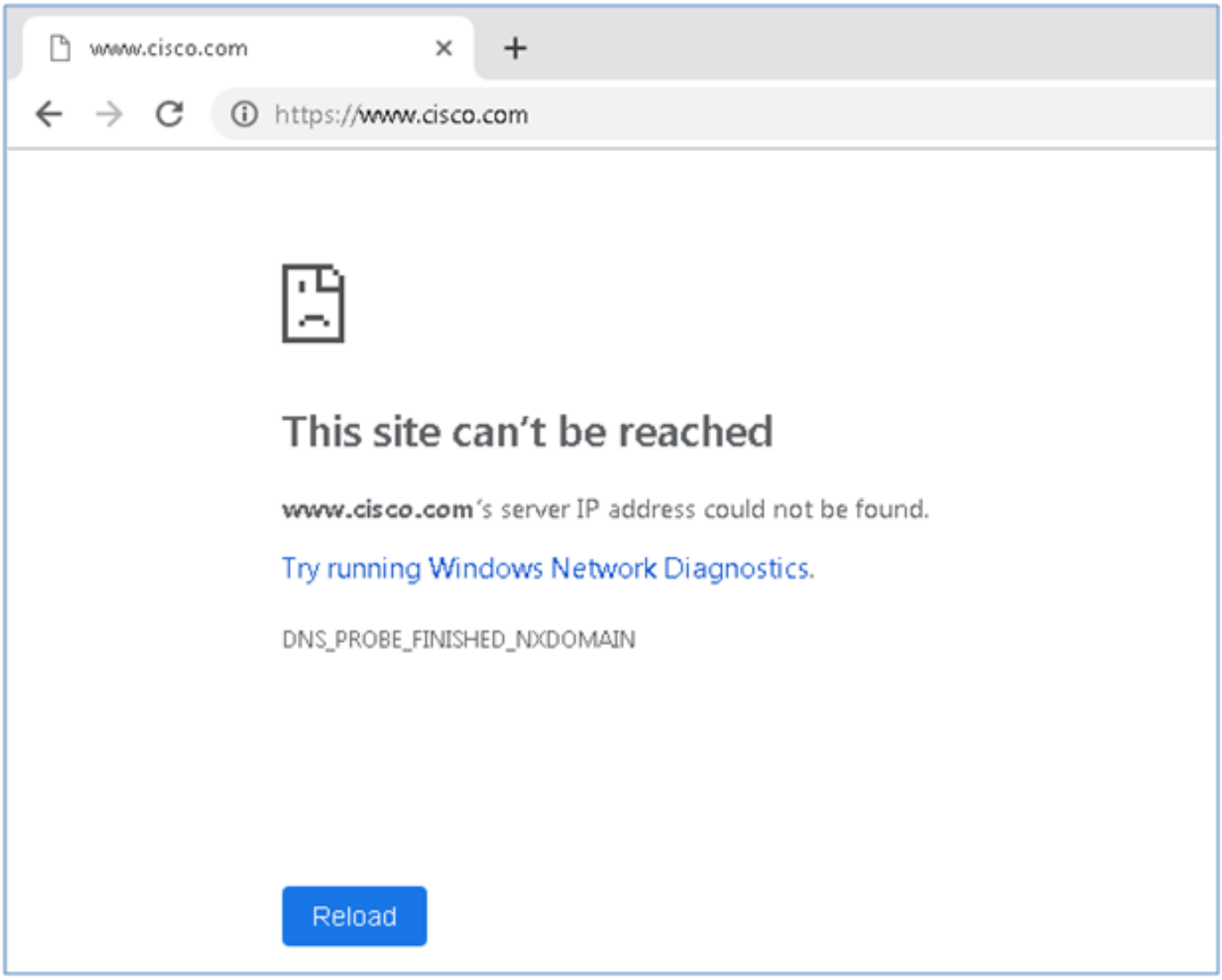


Nadat het DNS-beleid is toegepast

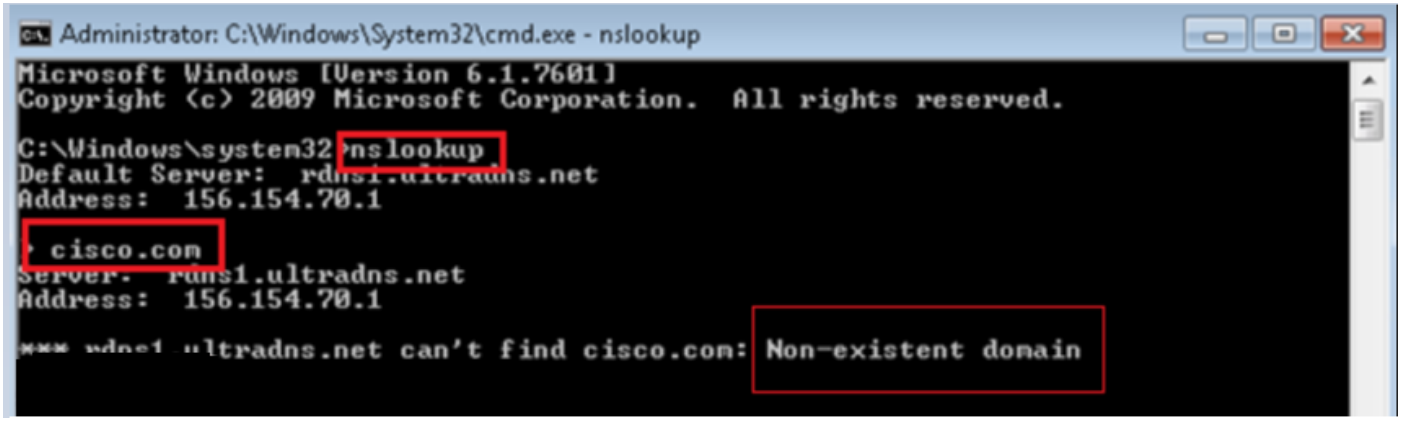
Stap 1. Schakel DNS cache op uw host uit met de opdracht **ipfig /flushdns.**



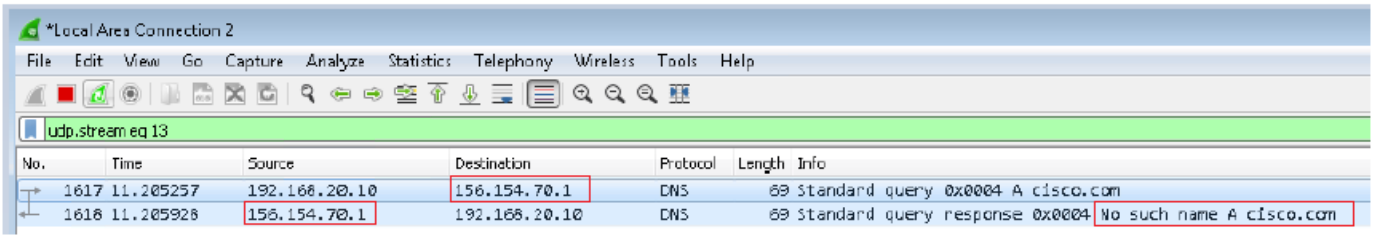
Stap 2. Navigeer naar het betrokken domein met een webbrowser. Het moet onbereikbaar zijn:

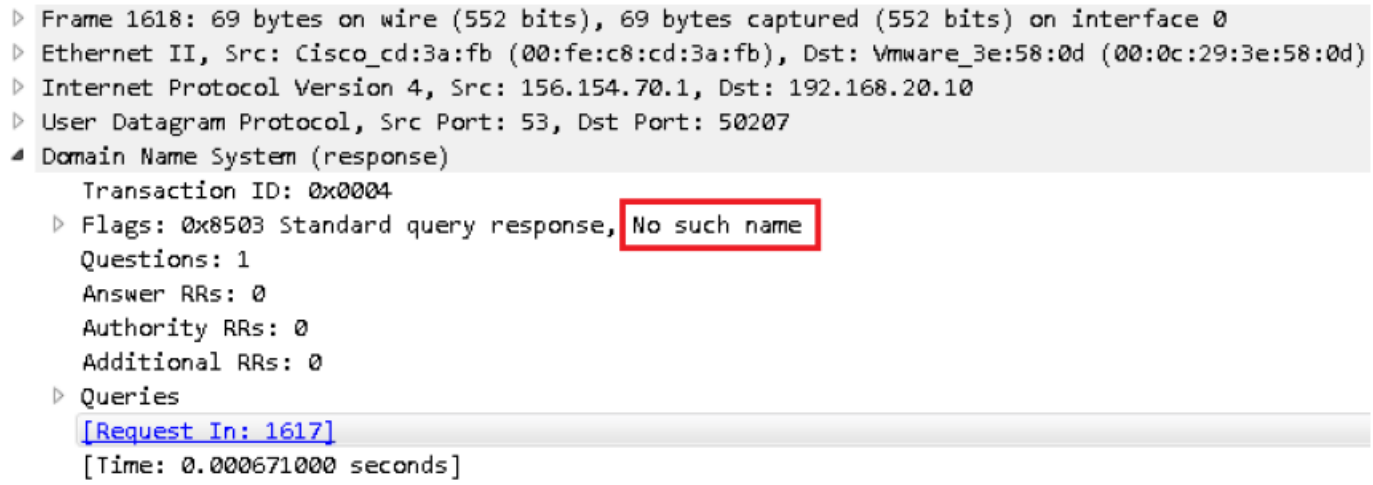


Stap 3. Probeer het volgende overzicht op het domein cisco.com uit te geven. De naamresolutie is mislukt.

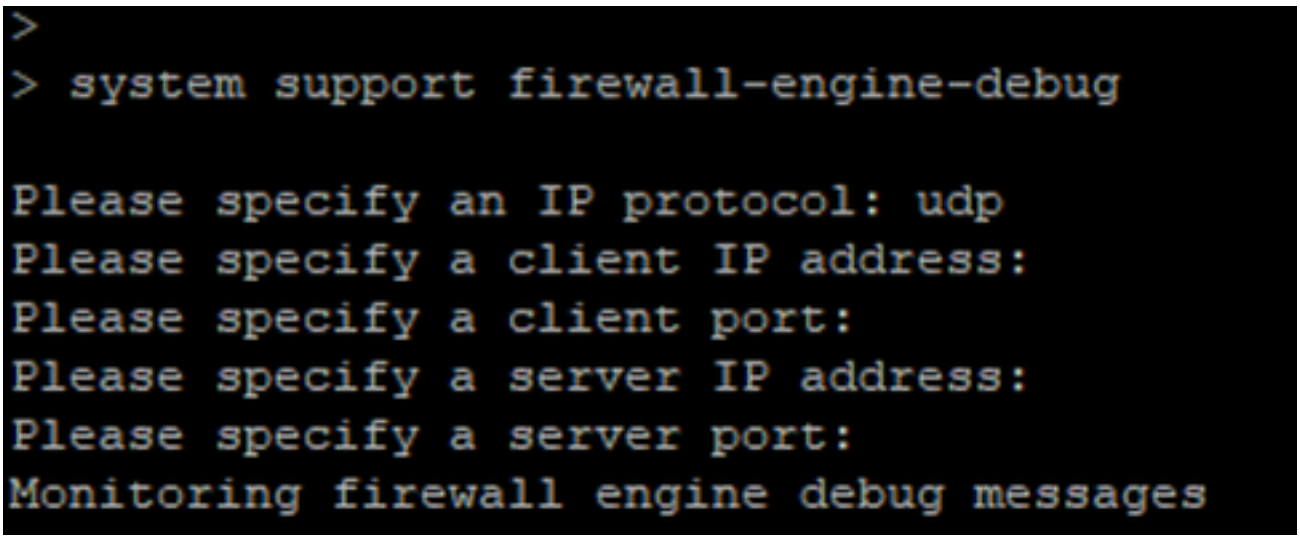


Stap 4. Packet Captures tonen een antwoord van de FTD, in plaats van de DNS server.





Stap 5. Start uiteinden in FTD CLI: systeemondersteuning voor firewall-engine-debug en specificeer UDP-protocol.



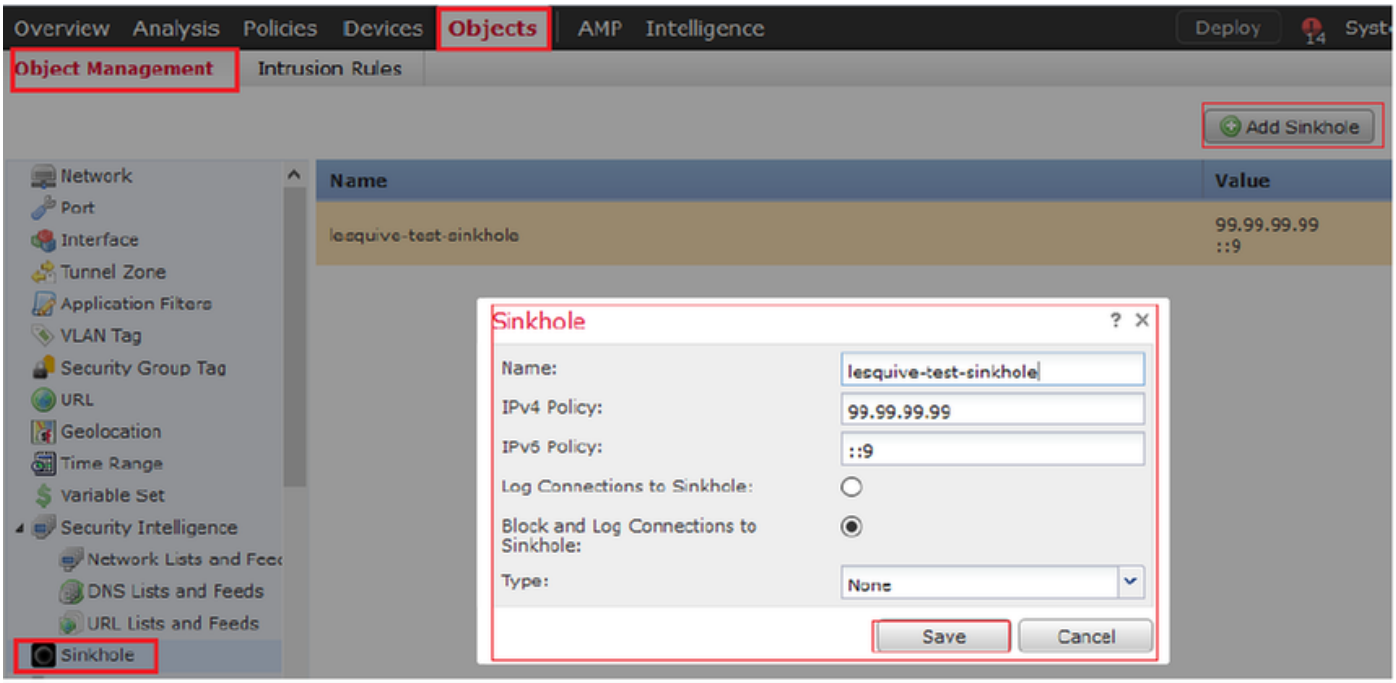
*Debugs wanneer cisco.com is afgesloten:

```
> 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
```

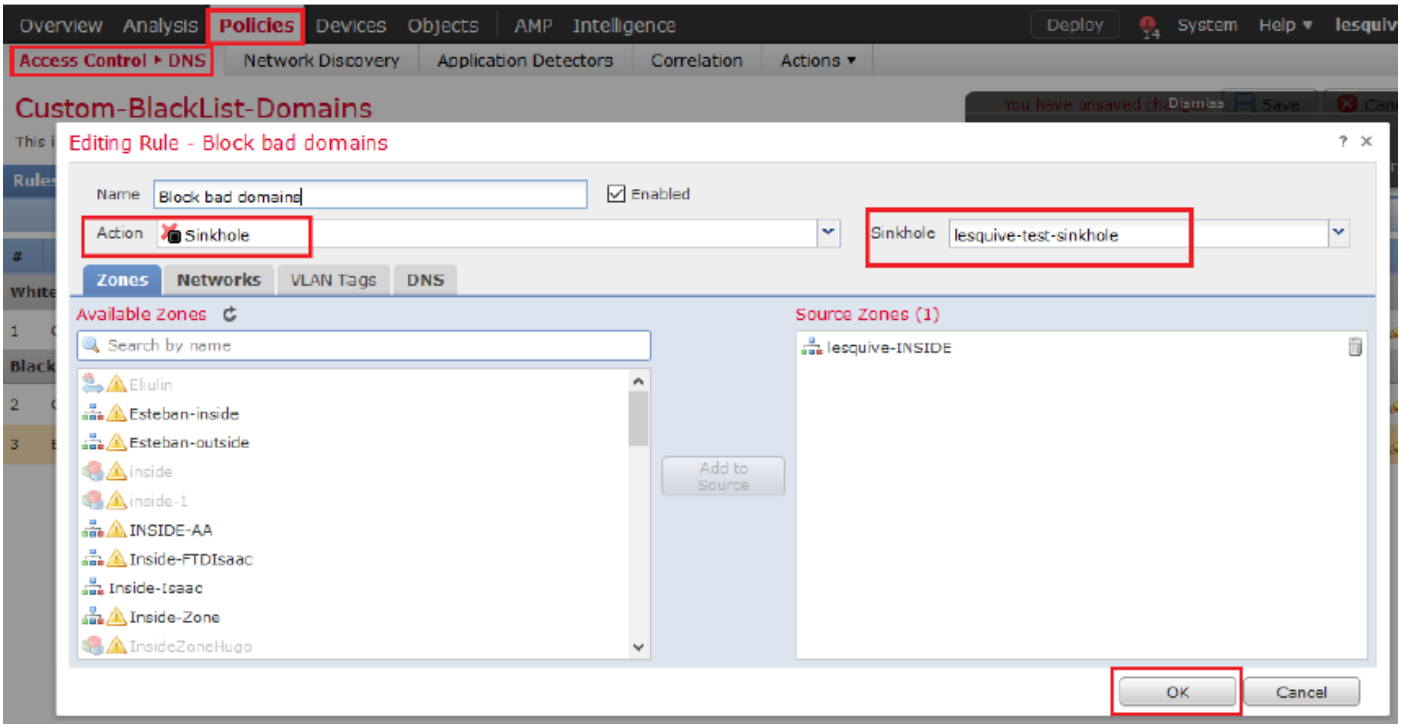
Optioneel: configuratie van het Sinusgat

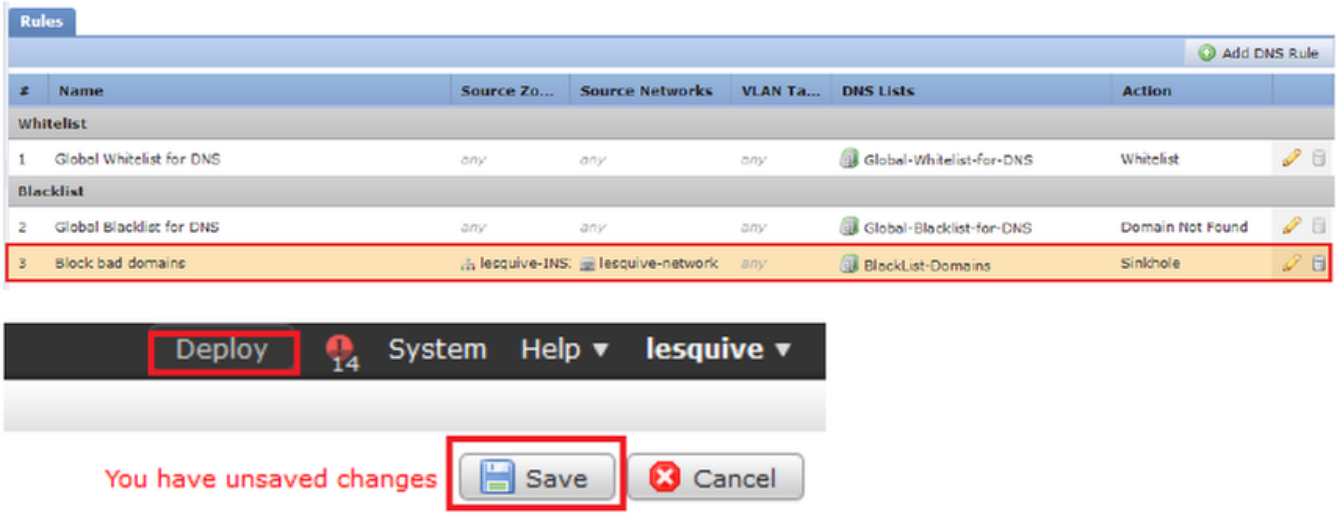
Een DNS-gat is een DNS-server die foutieve informatie biedt. In plaats van een DNS-reactie van "No dergelijke name" op DNS-vragen op domeinen die u blokkeert, geeft het een nep IP-adres terug.

Stap 1. Navigeer naar objecten > Objecten > Objectbeheer > Sinkopening >> Voeg zwart-gat toe en ontwerp de valse IP-adresinformatie.

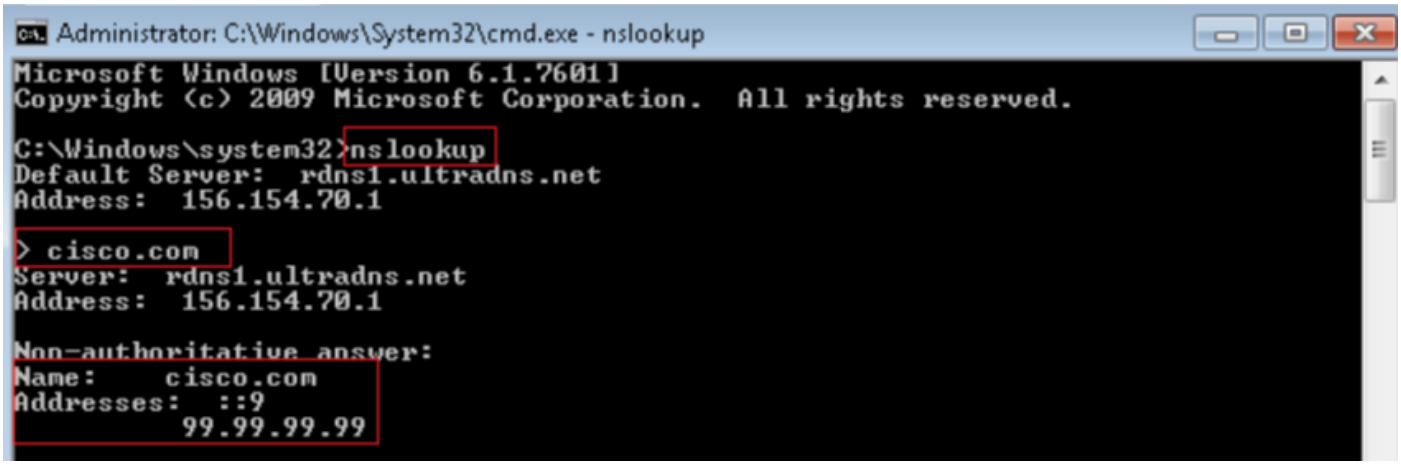


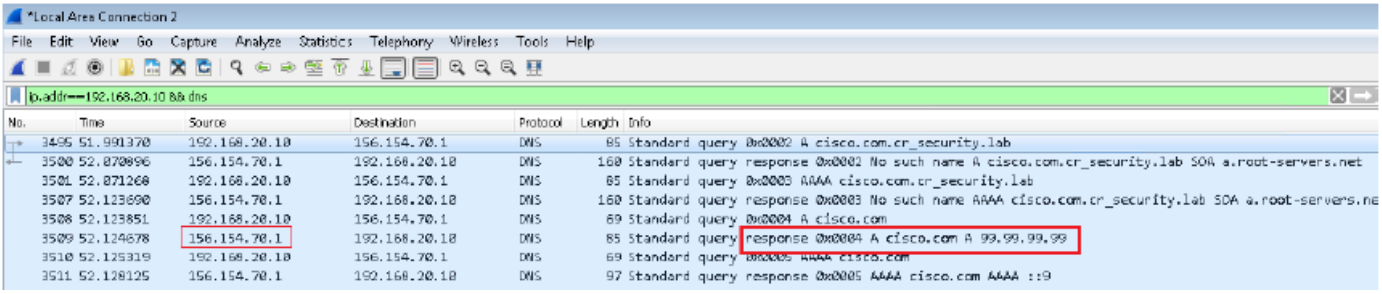
Stap 2. Pas het putje op uw DNS beleid toe en stel veranderingen in FTD in.





Controleer of het putje werkt





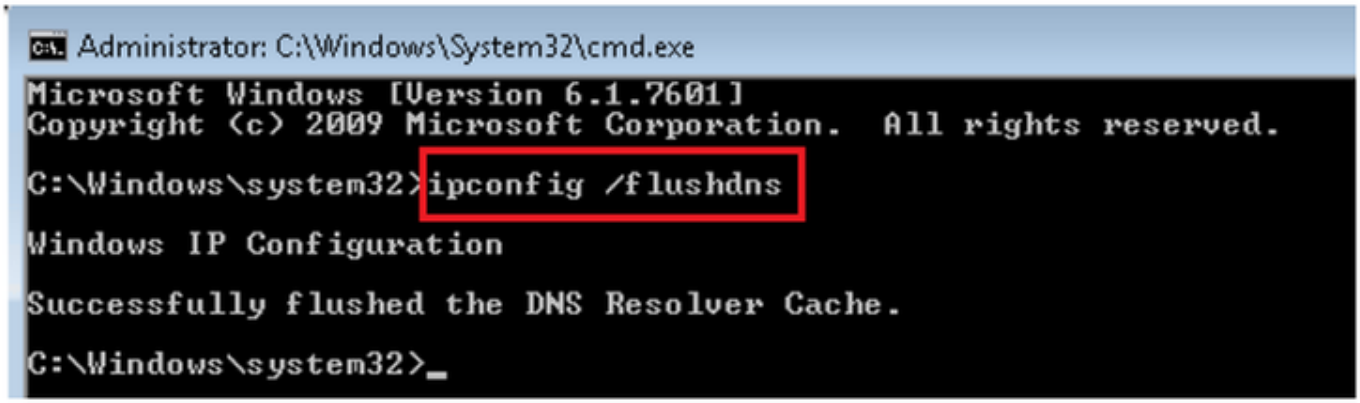
Problemen oplossen

Navigeer aan Analyse >> Connections > Security Intelligence Event om alle gebeurtenissen te volgen die door SI worden geactiveerd zolang u houtkap in het DNS-beleid hebt ingeschakeld:

U kunt ook **systeemondersteuning** gebruiken **voor** bestandsindelingen **voor het** debug **van firewalls** op de FTD die door het FMC worden beheerd.

```
>
> 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
```

Packet Captures kan behulpzaam zijn om te bevestigen dat DNS verzoeken het aan de FTD server maken. Vergeet niet de cache op uw lokale host te wissen bij het testen.


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>