

BlokDNS met Security Intelligence met FireSIGHT Management Center

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Configuratie van een aangepaste DNS-lijst met de domeinen die we willen blokkeren en uploaden de lijst naar FMC](#)

[Voeg een nieuw DNS-beleid toe met de 'actie ingesteld op 'domeinniet gevonden'](#)

[Wijs het DNS-beleid aan uw toegangsbeheerbeleid toe](#)

[Verifiëren](#)

[Voordat het DNS-beleid wordt toegepast](#)

[Nadat het DNS-beleid is toegepast](#)

[Optioneel: configuratie van het Sinusgat](#)

[Controleer of het putje werkt](#)

[Problemen oplossen](#)

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.

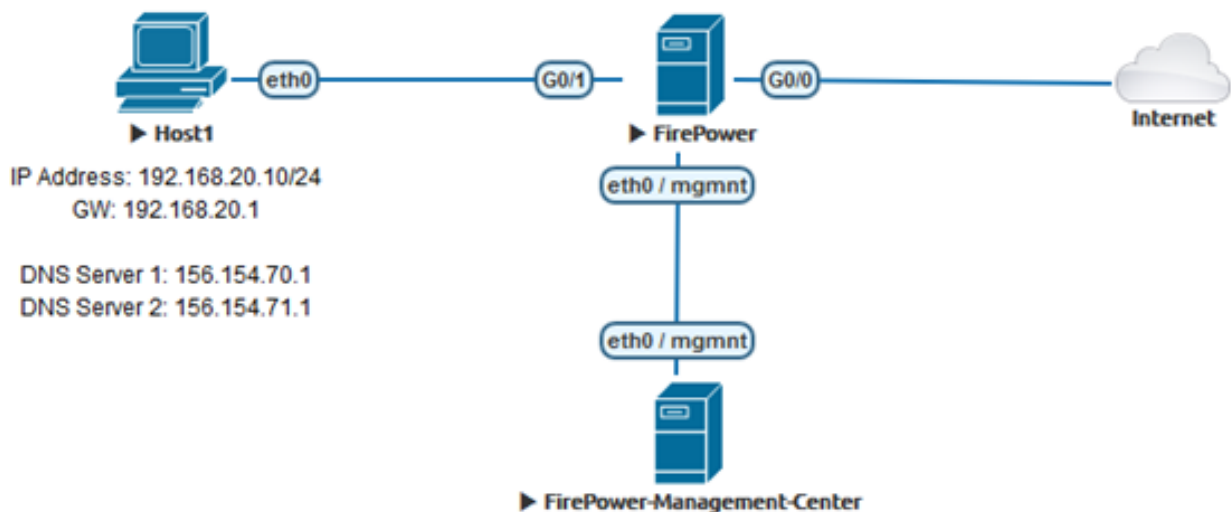
Het voorbeeld gebruikte blokken 1 domein:

- 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.

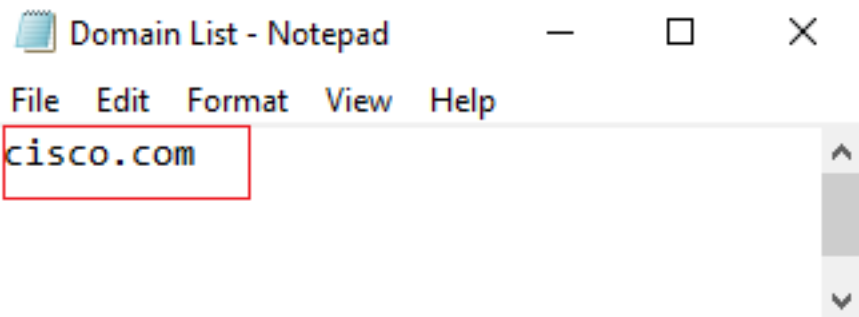
Netwerkdigram



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.

Name	Type
Cisco-DNS-and-URL-Intelligence-Feed <i>Last Updated: 2019-02-14 10:21:48</i>	Feed
Global-Blacklist-for-DNS	List
Global-Whitelist-for-DNS	List

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:

Security Intelligence for DNS List / Feed

Name: BlackList-Domains

Type: List

Upload List: Browse...

Upload

Save Cancel

Security Intelligence for DNS List / Feed

Name: BlackList-Domains

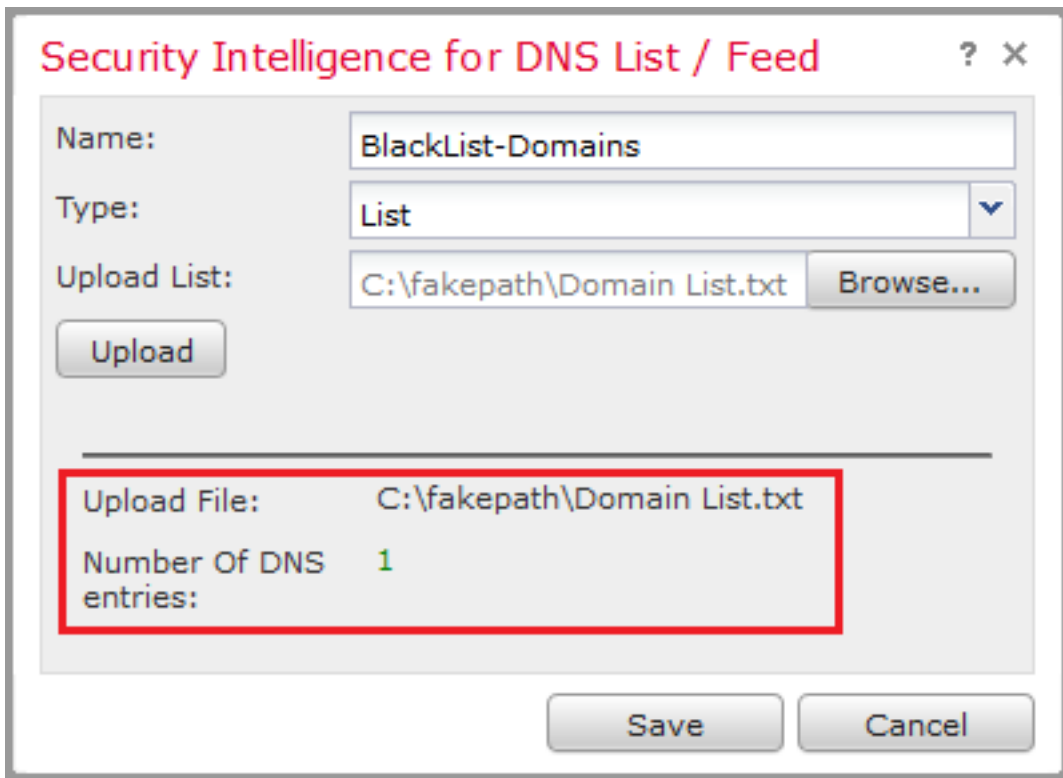
Type: List

Upload List: C:\fakepath\Domain List.txt Browse...

Upload

Save Cancel

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

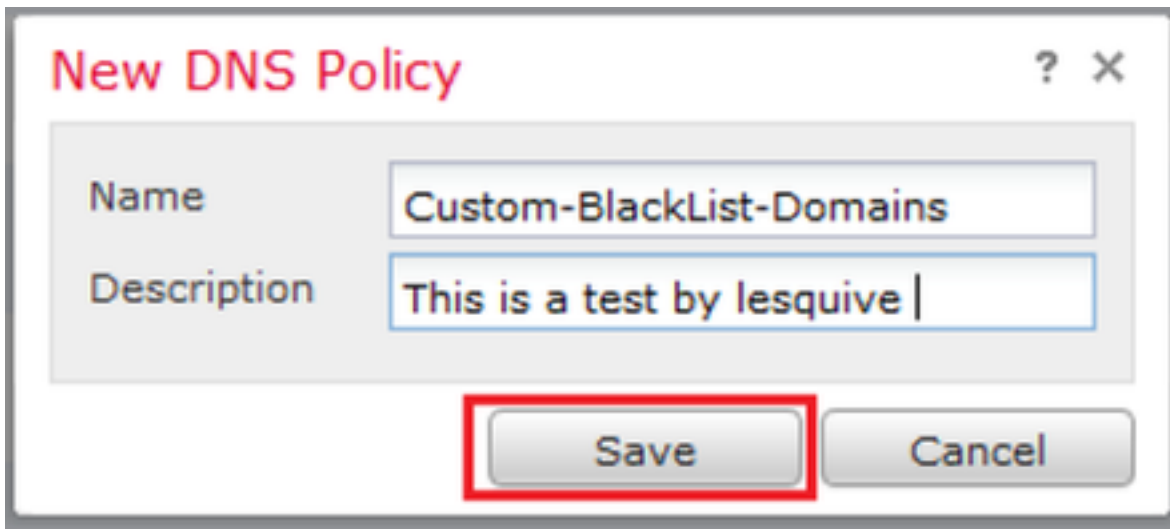


Voeg een nieuw DNS-beleid toe met de 'actie ingesteld op 'domeinniet gevonden'

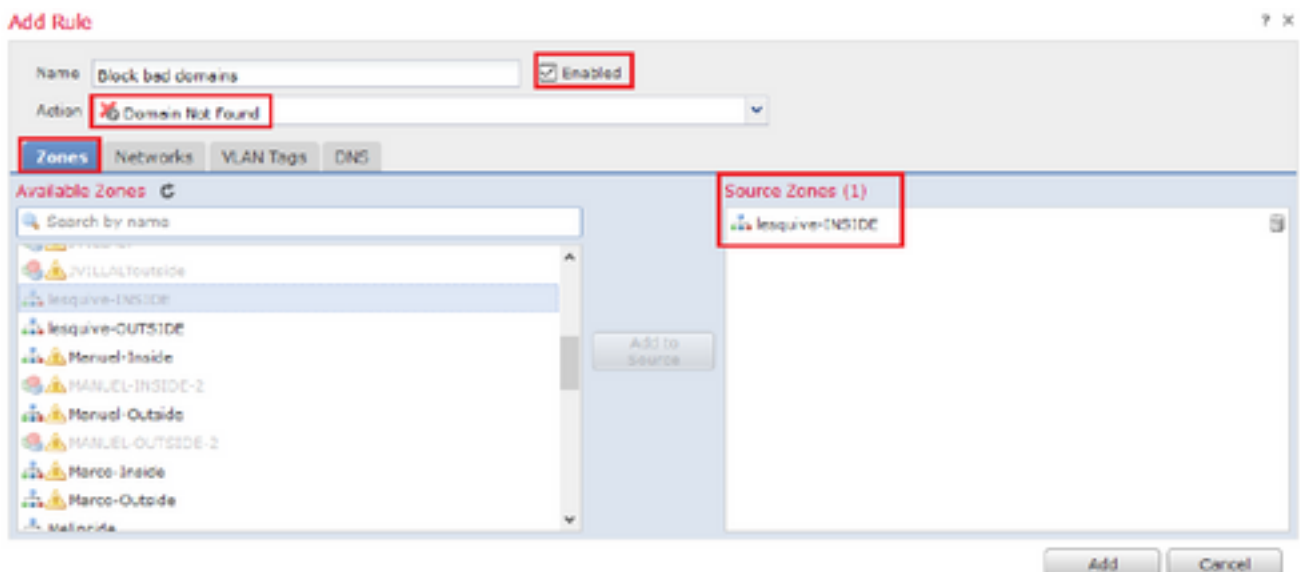
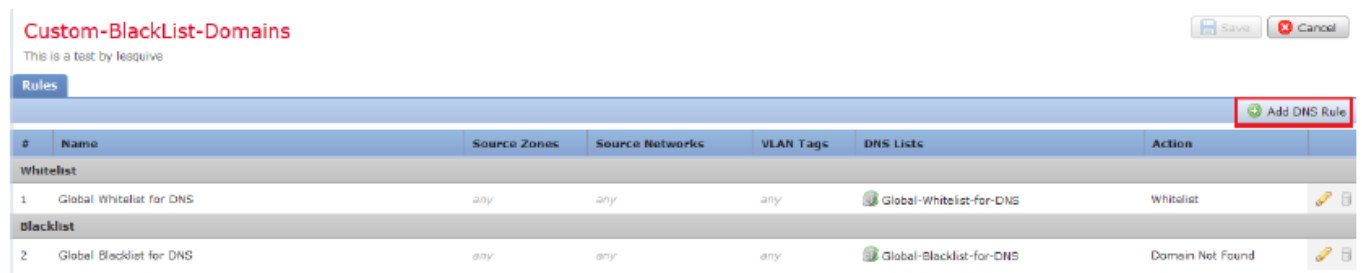
*Zorg ervoor dat u een bronzone, bronnetwerk en DNS-lijst toevoegt.

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





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



Add Rule

? 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

Rules							Add DNS Rule
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action	
Whitelist							
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	
Blacklist							
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	

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.

The screenshot shows the Fortinet web interface for configuring a policy. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Below this, there are sub-tabs for 'Access Control', 'Network Discovery', and 'Application Detectors'. The 'Access Control' sub-tab is selected. The policy configuration page for 'lesquive-policy' is displayed. It shows the 'Rules' section with 'Security Intelligence' selected. The 'DNS Policy' is set to 'Custom-BlackList-Domains'. The 'Save' button is highlighted with a red box. There is also a 'Cancel' button and a message 'You have unsaved changes'.

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:

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

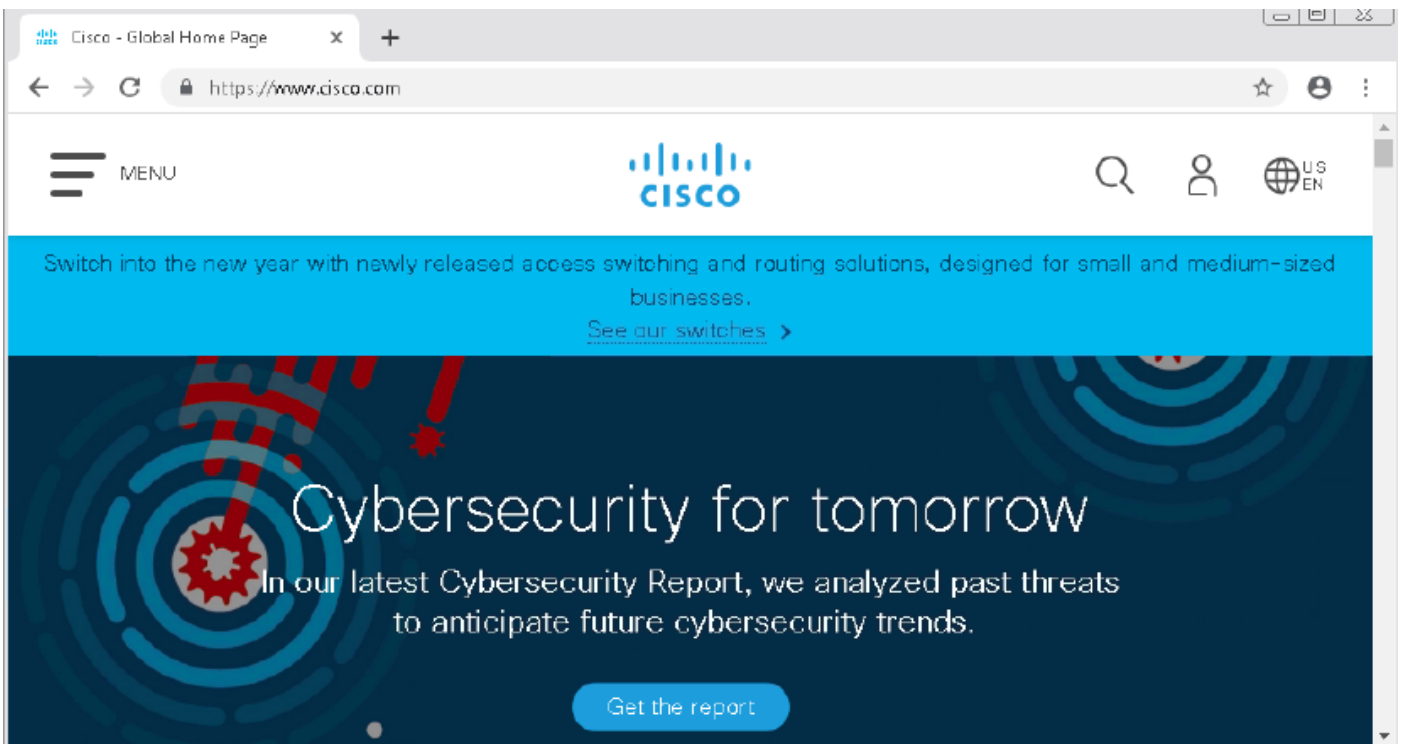
Ethernet adapter Local Area Connection 2:

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::b169:29aa: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
```

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



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

The screenshot shows a Wireshark capture of network traffic on the interface 'Local Area Connection 2'. The packet list pane shows two 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 packet details pane for packet 3515 shows the following structure:

- Frame 3515: 271 bytes on wire (2168 bits), 271 bytes captured (2168 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: 49399
- Domain Name System (response)
 - Transaction ID: 0x0004
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 3
 - Additional RRs: 6
 - Queries
 - 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

Nadat het DNS-beleid is toegepast

Stap 1. Schakel DNS cache op uw host uit met de opdracht `ipconfig /flushdns`.

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

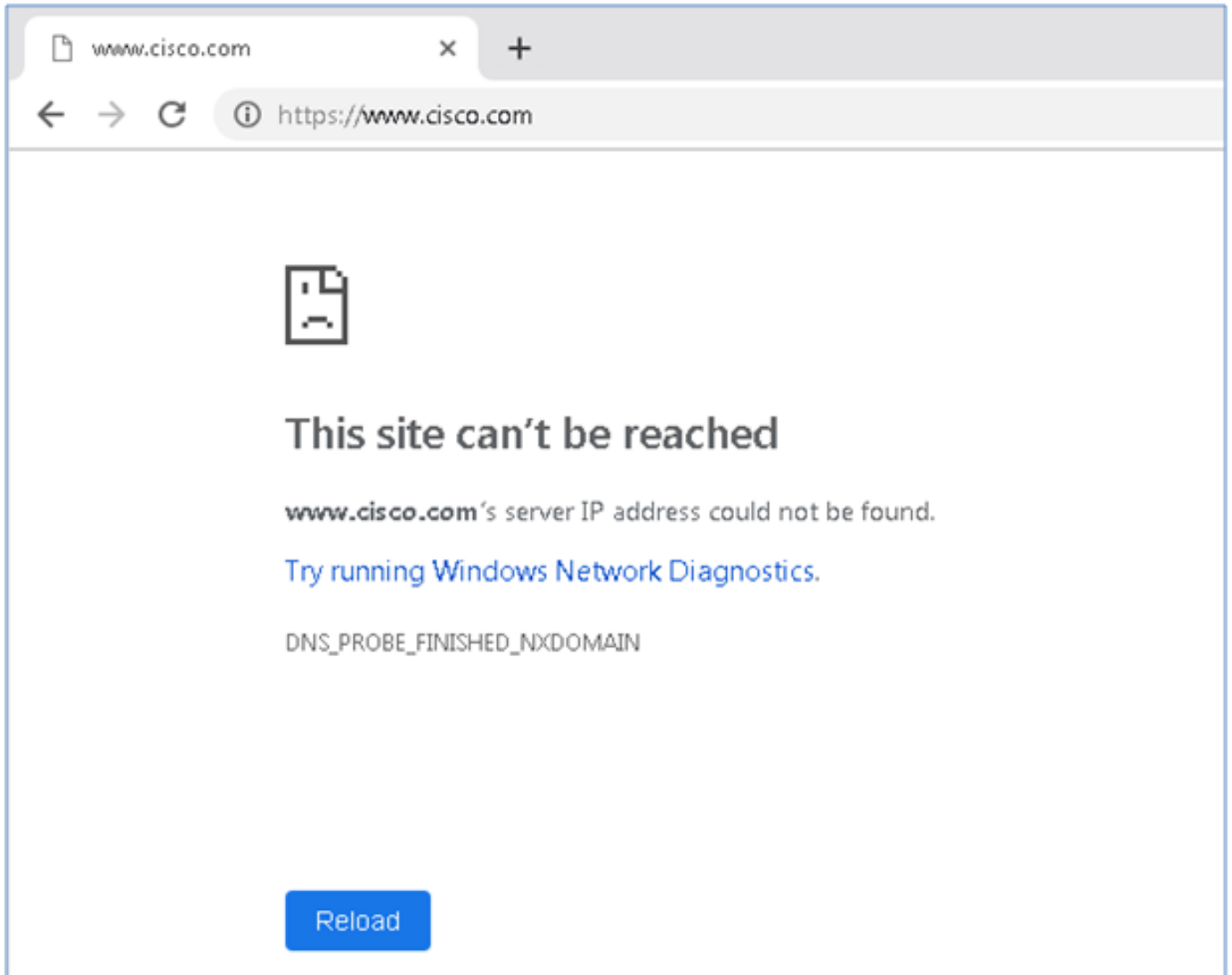
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
```

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.

```
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: rdnsl1.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdnsl1.ultradns.net
Address: 156.154.70.1

www.wdnet.ultradns.net can't find cisco.com: Non-existent domain
```

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

*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]

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

```
>
> 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
```

*Debugs wanneer cisco.com is afgesloten:

```
> system support firewall-engine-debug

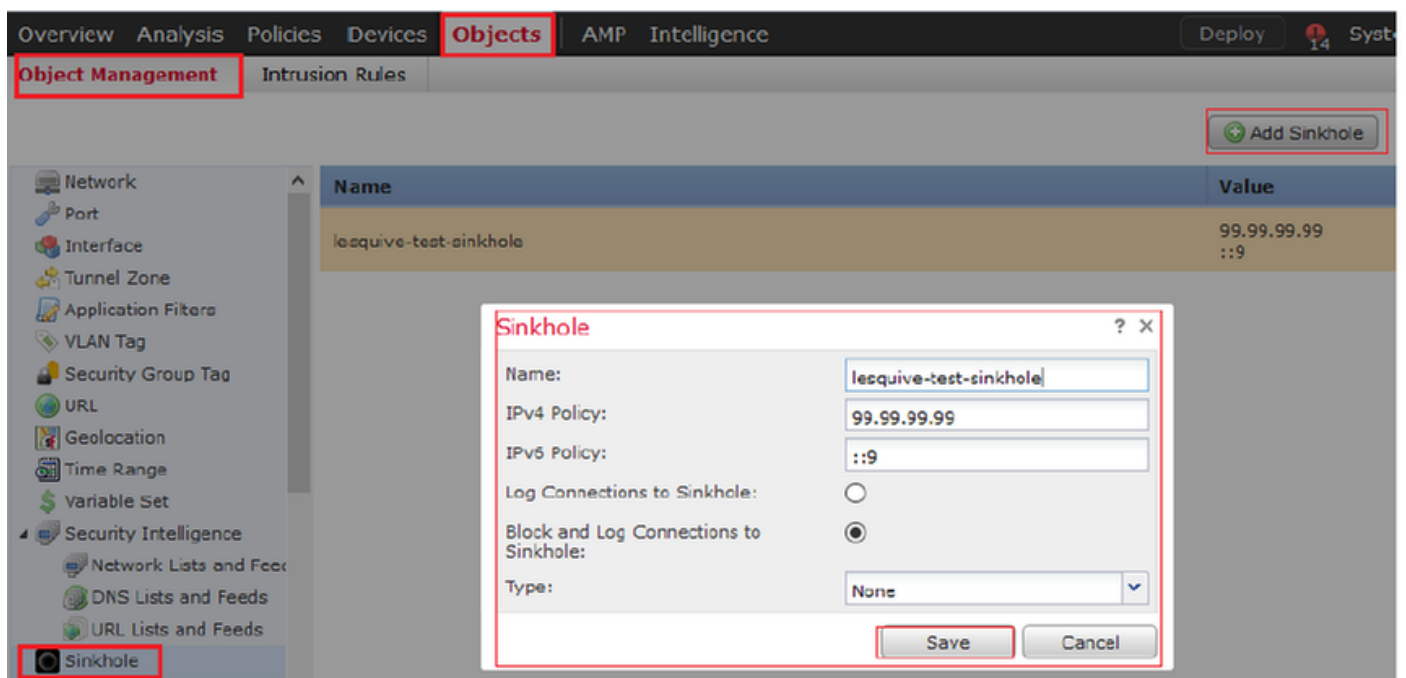
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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 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
```

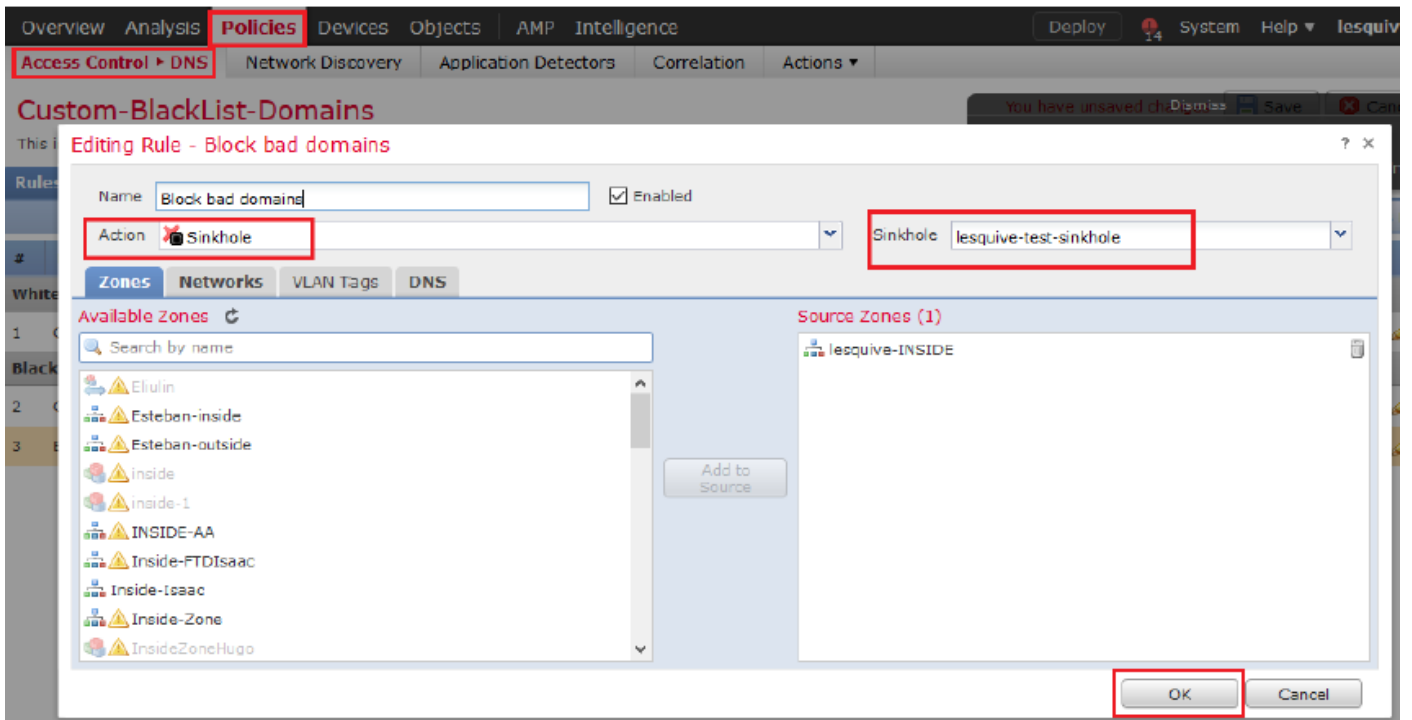
Optioneel: configuratie van het Sinusgat

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.

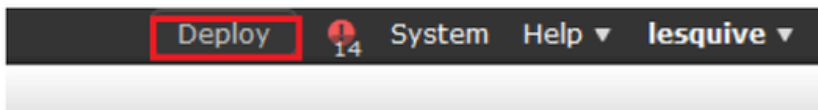


Stap 2. Pas het putje op uw DNS beleid toe en stel veranderingen in FTD in.



Rules

#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
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



You have unsaved changes



Controleer of het putje werkt

```
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

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:

Security Intelligence Events (switch workflow)

Security Intelligence with Application Details > Table View of Security Intelligence Events

No Search Constraints (Edit Search)

2019-02-14 13:42:42 - 2019-02-14 14:42:42 Expanding

	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
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	
↓	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	

U kunt ook **systemondersteuning** 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>_