

Bloqueie o DNS com inteligência de segurança usando o Firepower Management Center

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configurar uma lista de DNS personalizada com os domínios que queremos bloquear e carregar a lista para a FMC](#)

[Adicionar uma nova política DNS com a 'ação configurada para 'domínio não encontrado'](#)

[Atribua a política DNS à sua política de controle de acesso](#)

[Verificar](#)

[Antes de a política DNS ser aplicada](#)

[Depois que a política de DNS for aplicada](#)

[Configuração opcional do sinkhole](#)

[Verifique se o sinkhole está funcionando](#)

[Troubleshoot](#)

Introduction

Este documento descreve o procedimento para adicionar uma Lista de Sistema de Nome de Domínio (DNS - Domain Name System) a uma Política DNS para que você possa aplicá-la com a Inteligência de Segurança (SI - Security Intelligence).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ASA55XX Threat Defense
- Configuração do Cisco Firepower Management Center

Componentes Utilizados

- Cisco ASA5506W-X Threat Defense (75) versão 6.2.3.4 (Build 42)
- Cisco Firepower Management Center para VMWare Versão de software: 6.2.3.4 (build 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A inteligência de segurança funciona bloqueando o tráfego de ou para endereços IP, URLs ou nomes de domínio que têm uma reputação reconhecidamente incorreta. Neste documento, o foco principal é a lista negra de nomes de domínio.

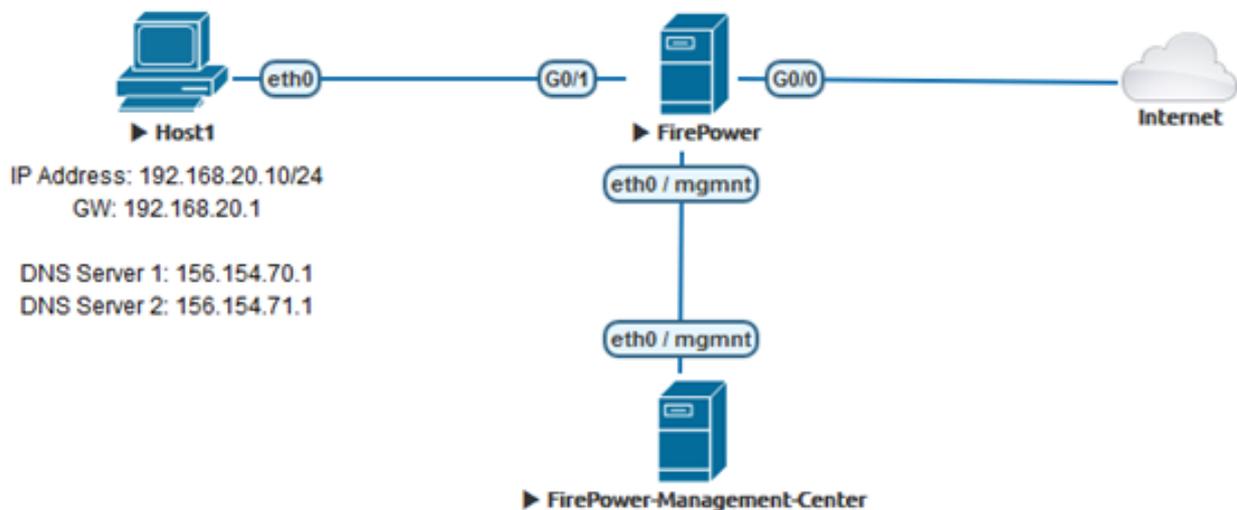
O exemplo usou o domínio dos blocos 1:

- cisco.com

Você pode usar a filtragem de URL para bloquear alguns desses sites, mas o problema é que a URL deve ser uma correspondência exata. Por outro lado, a lista negra de DNS com SI pode focar em domínios como "cisco.com" sem a necessidade de se preocupar com subdomínios ou alterações na URL.

No final deste documento, uma configuração opcional do Sinkhole também é demonstrada.

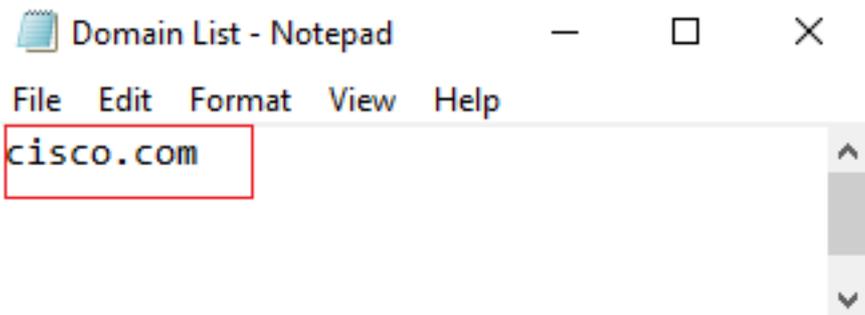
Diagrama de Rede



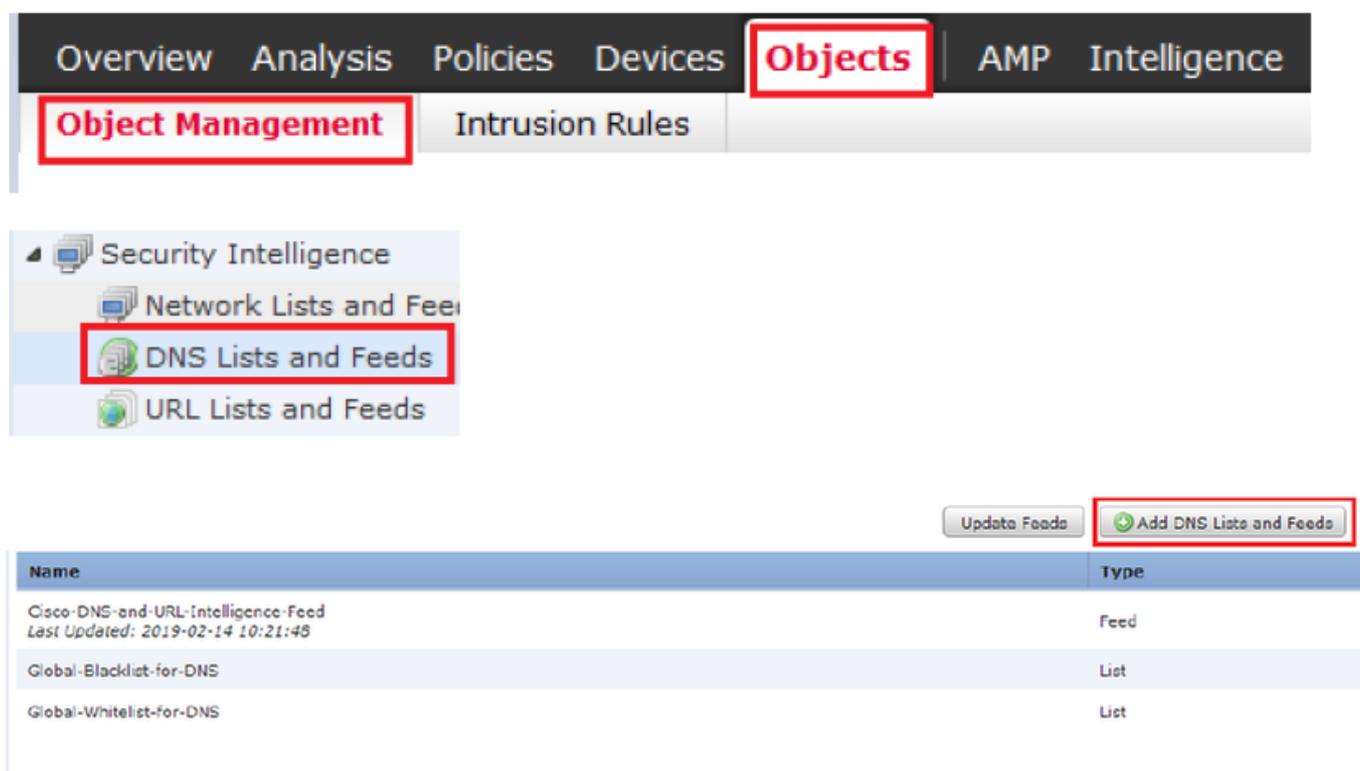
Configurar

Configurar uma lista de DNS personalizada com os domínios que queremos bloquear e carregar a lista para a FMC

Etapa 1. Crie um arquivo .txt com os domínios que você gostaria de bloquear. Salve o arquivo .txt no computador:



Etapa 2. No FMC, navegue até Object > Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds (Objeto > Gerenciamento de objetos >> Listas e feeds DNS >> Add DNS List and Feeds).



Etapa 3. Crie uma lista chamada "BlackList-Domains", o tipo deve ser uma lista e o arquivo .txt com os domínios em questão deve ser carregado conforme visto nas imagens:

Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

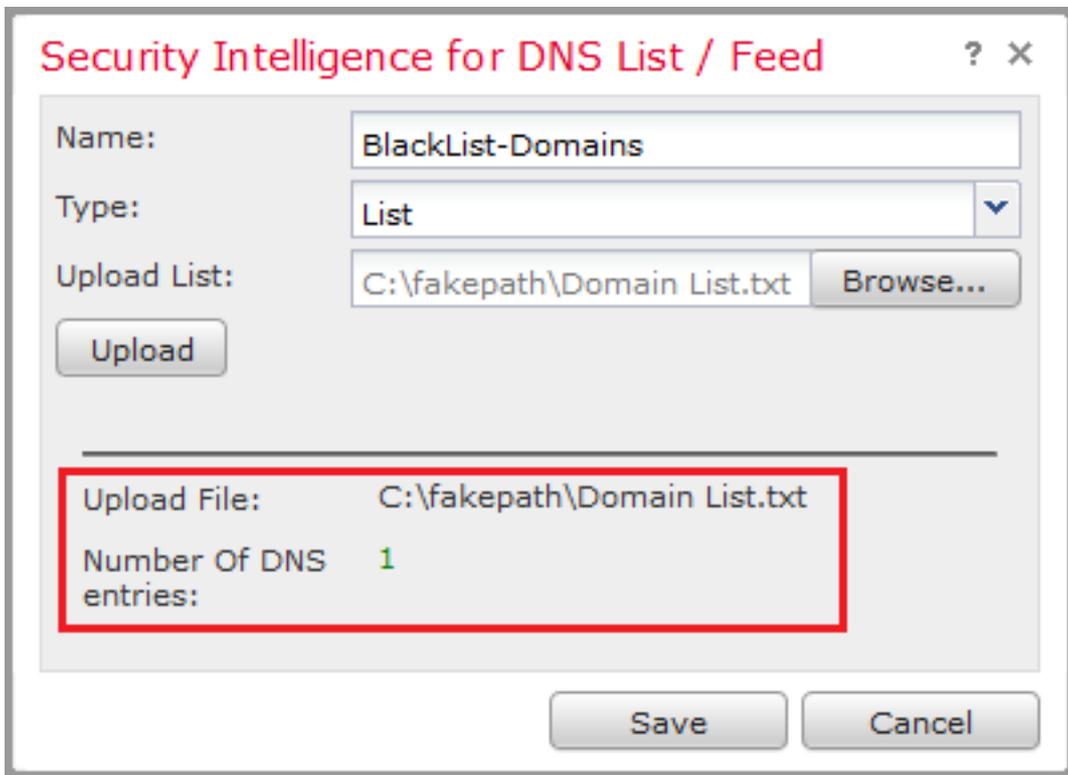
Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

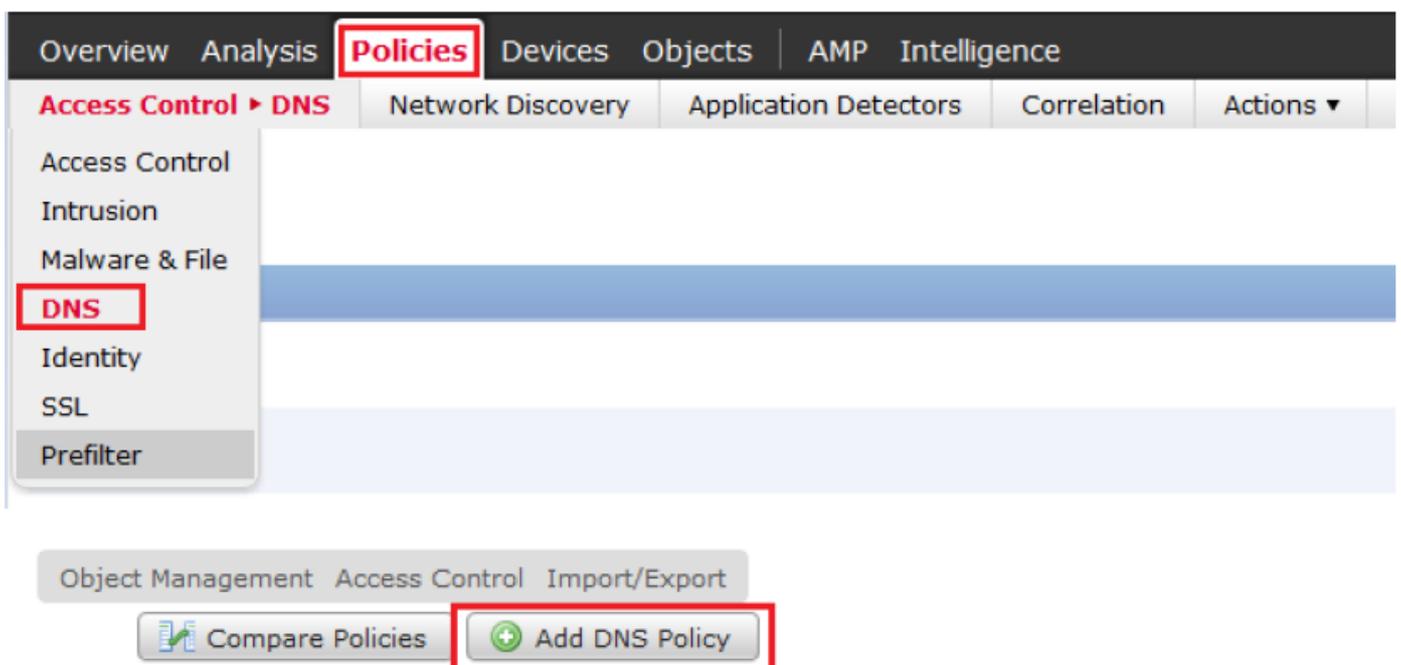
*Observe que quando você carrega o arquivo .txt, o número de entradas DNS deve ler todos os domínios. Neste exemplo, um total de 1:

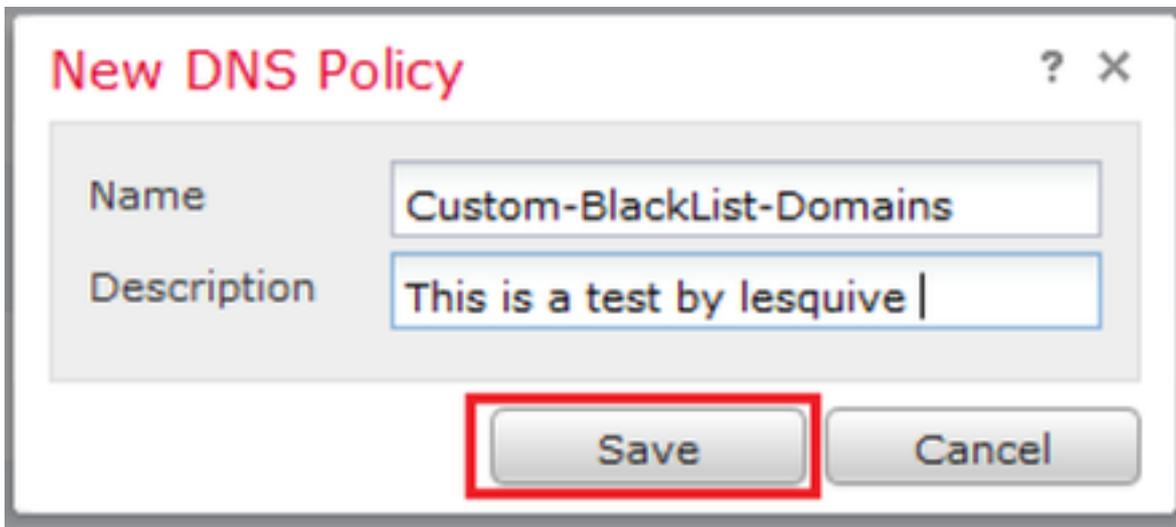


Adicionar uma nova política DNS com a 'ação configurada para 'domínio não encontrado'

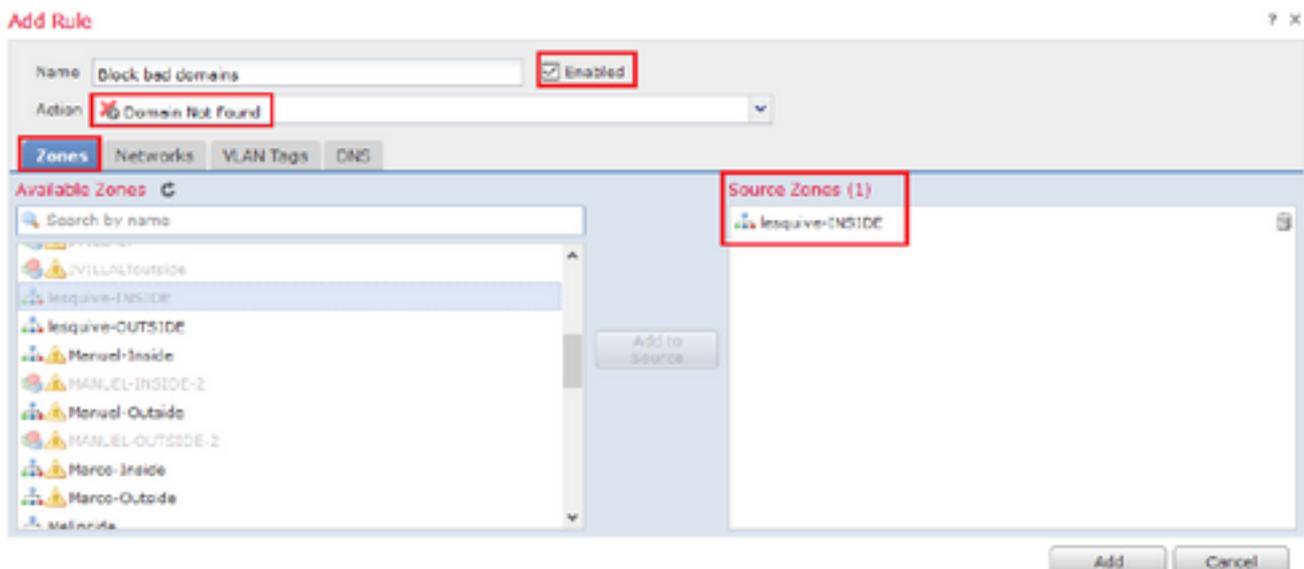
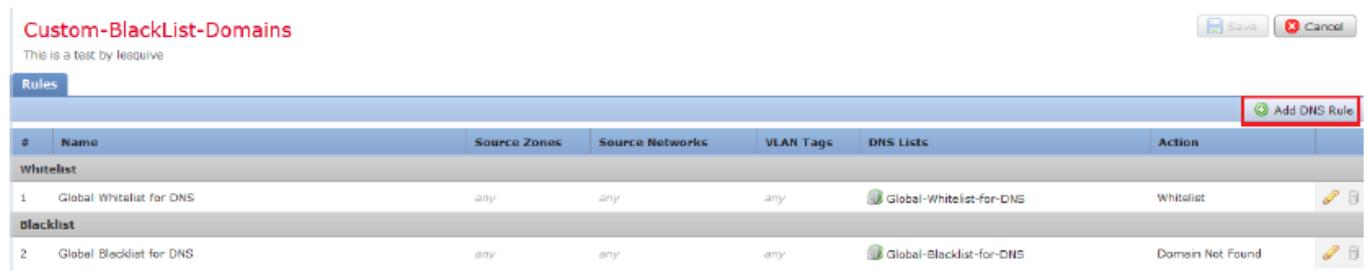
*Certifique-se de adicionar uma zona de origem, uma rede de origem e uma lista DNS.

Etapa 1. Navegue até Políticas >> Controle de acesso >> DNS >> Adicionar política DNS:





Etapa 2. Adicione uma regra de DNS conforme vista na imagem:



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	

Informações importantes sobre a ordem das regras:

- A lista branca global é sempre a primeira e tem precedência sobre todas as outras regras.
- A regra de Listas brancas de DNS descendente aparece somente em implantações de vários domínios, em domínios não-folha. É sempre a segunda e tem precedência sobre todas as outras regras, exceto a lista branca global.
- A seção Lista branca precede a seção Lista negra; as regras da lista branca sempre têm precedência sobre outras regras.
- A lista negra global é sempre a primeira na seção Lista negra e tem precedência sobre todas as outras regras de monitoramento e lista negra.
- A regra de listas negras de DNS descendente aparece somente em implantações de vários domínios, em domínios não leaf. Ele é sempre o segundo na seção de lista negra e tem precedência sobre todas as outras regras de monitoramento e lista negra, exceto a lista negra global.
- A seção Lista negra contém regras de monitoramento e lista negra.
- Quando você cria uma regra DNS pela primeira vez, a posição do sistema fica em último lugar na seção Lista branca se você atribuir uma ação Lista branca ou em último lugar na seção Lista negra se você atribuir qualquer outra ação

Atribua a política DNS à sua política de controle de acesso

Vá para Políticas >> Controle de acesso >> A política para seu FTD >> Inteligência de segurança >> Política DNS e adicione a política criada.

The screenshot shows the Fortinet web interface for configuring a policy. The 'Policies' tab is selected, and the 'Access Control' sub-tab is active. The policy name is 'lesquive-policy'. The 'DNS Policy' dropdown is set to 'Custom-BlackList-Domains'. The 'Save' button is highlighted.

Certifique-se de implantar todas as alterações quando terminar.

Verificar

Antes de a política DNS ser aplicada

Etapa 1. Verifique as informações do servidor DNS e do endereço IP na máquina host conforme visto na imagem:

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

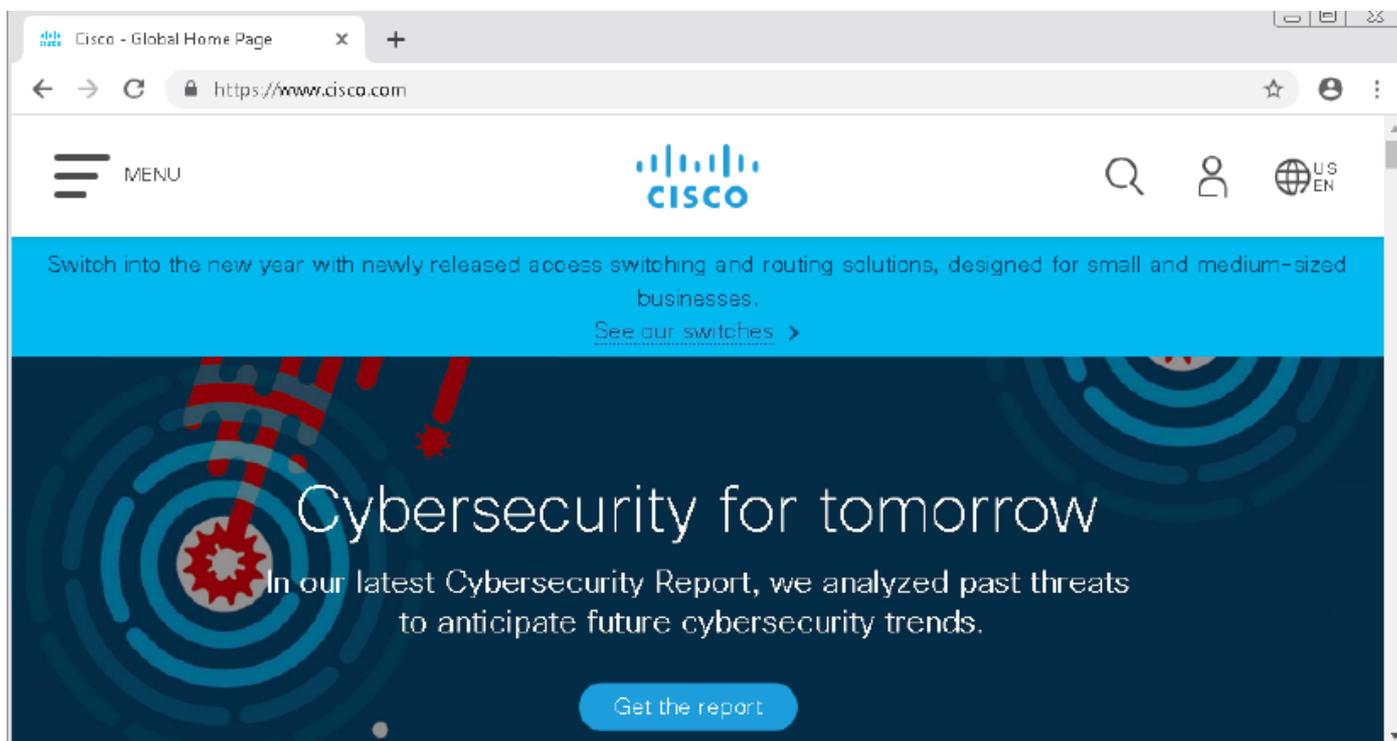
Ethernet adapter Local Area Connection 2:

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
```

Etapa 2. Confirme se você pode navegar para cisco.com conforme visto na imagem:



Etapa 3. Confirme com as capturas de pacotes que o DNS foi resolvido corretamente:

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

Depois que a política de DNS for aplicada

Etapa 1. Limpe o cache DNS no host com o comando `ipconfig /flushdns`.

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

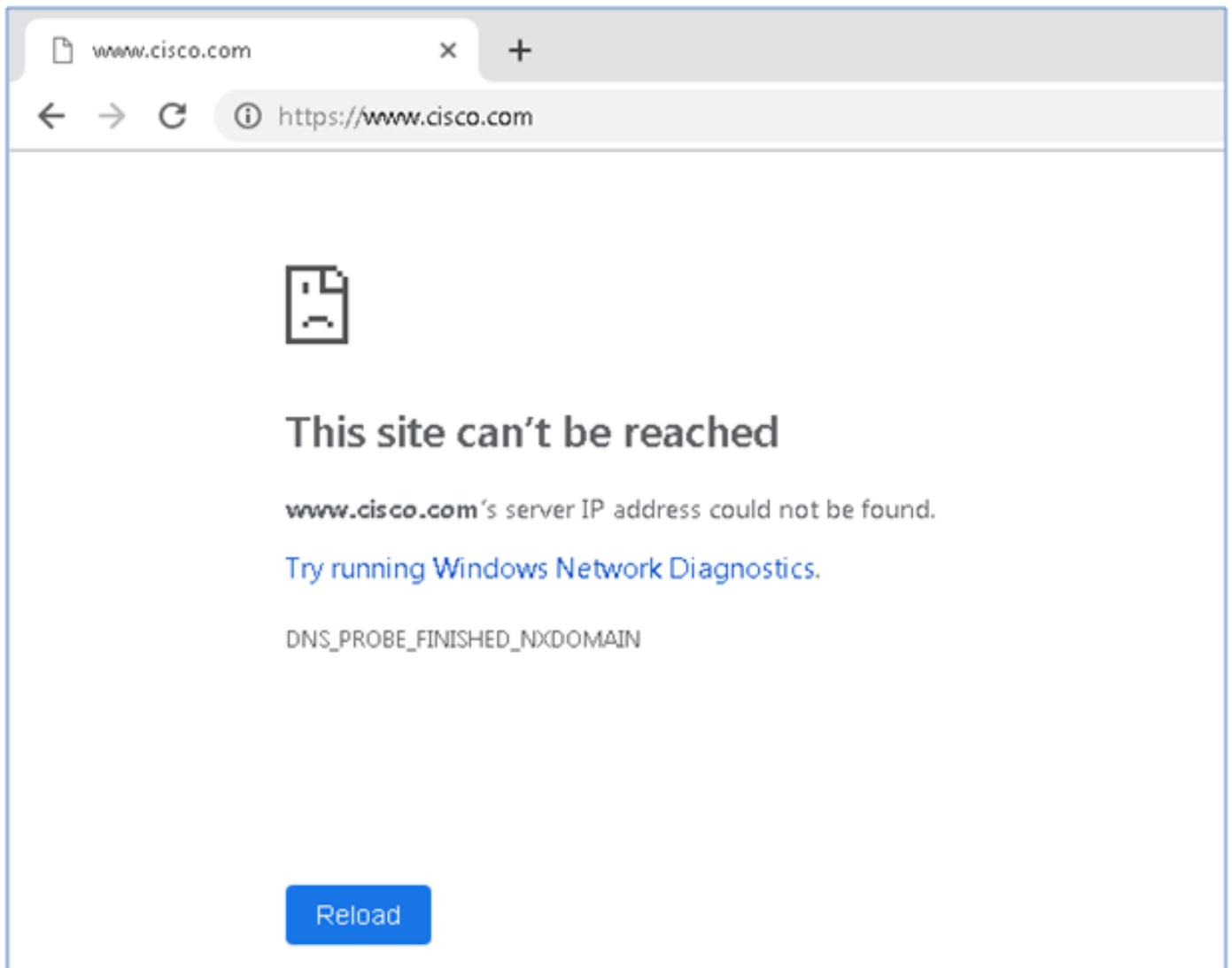
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
```

Etapa 2. Navegue até o domínio em questão com um navegador da Web. Deve ser inalcançável:



Etapa 3. Tente emitir `nslookup` no domínio `cisco.com`. A resolução do nome falha.

```
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
```

Etapa 4. As capturas de pacotes mostram uma resposta do FTD, em vez do servidor DNS.

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

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

The bottom pane shows the details of the selected packet (Frame 1618):

- 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]

Etapa 5. Executar depurações na CLI do FTD: o sistema suporta firewall-engine-debug e especifica o protocolo 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
```

*Depurações quando cisco.com é compatível:

```
> system support firewall-engine-debug

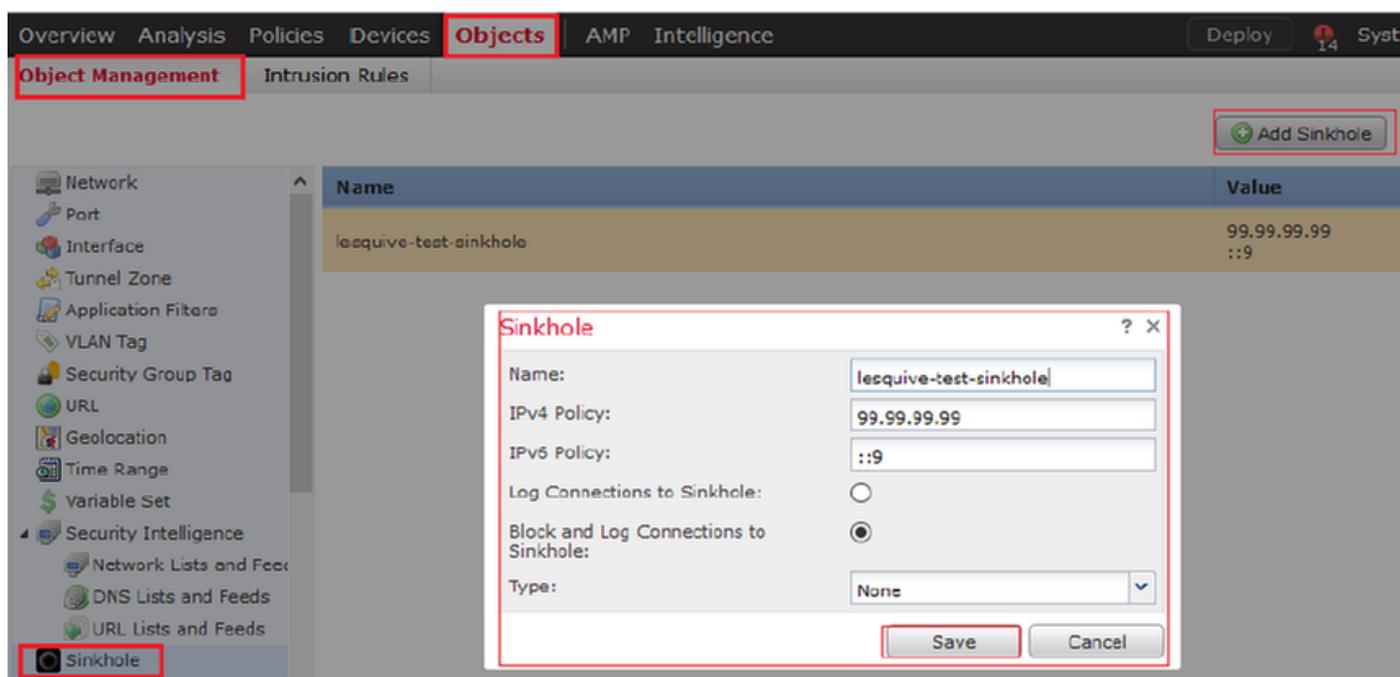
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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
```

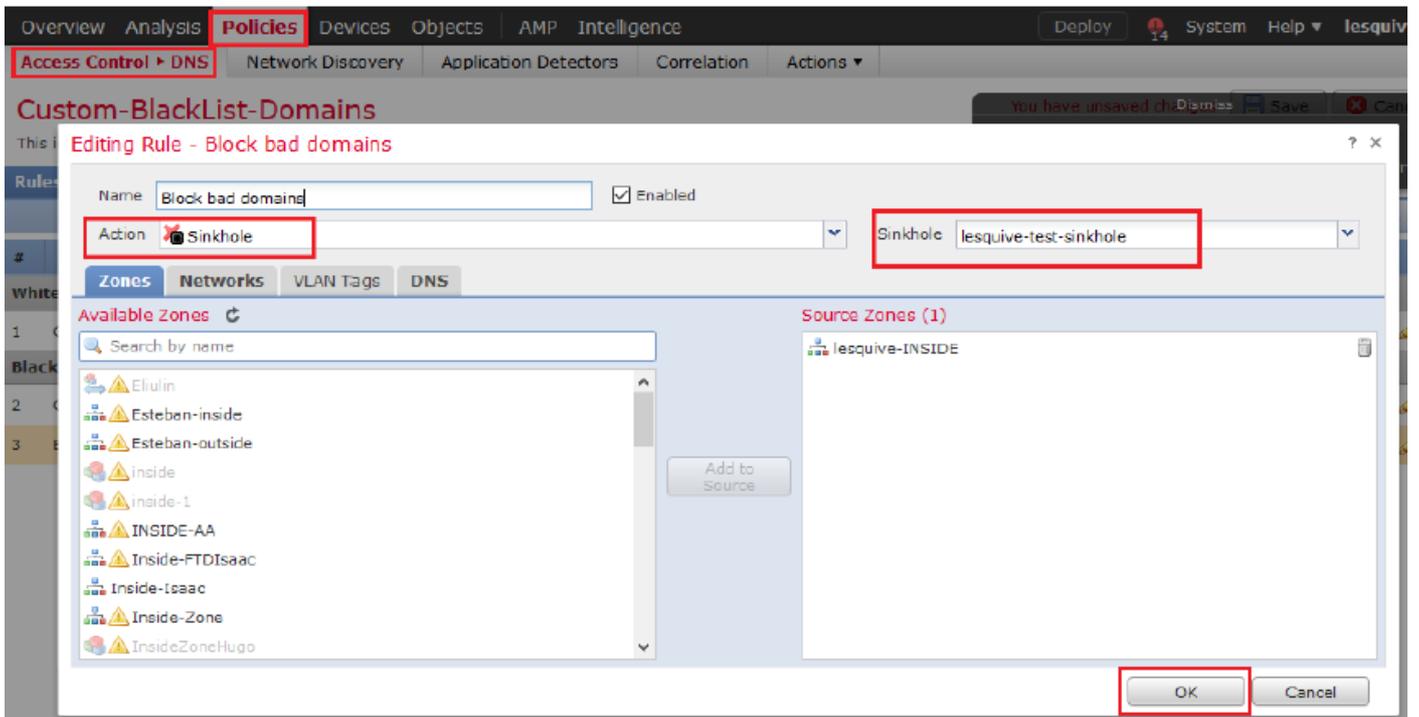
Configuração opcional do sinkhole

Um sinkhole DNS é um servidor DNS que fornece informações falsas. Em vez de retornar uma resposta de DNS "Sem esse nome" para consultas de DNS em domínios que você está bloqueando, ele retorna um endereço IP falso.

Etapa 1. Navegue até Objects > Object Management >> Sinkhole >> Add Sinkhole e crie informações de endereço IP falsas.



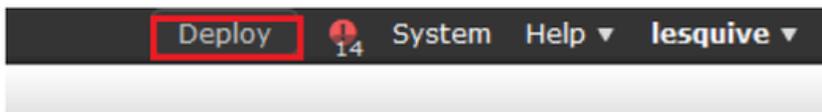
Etapa 2. Aplique o sinkhole à sua política de DNS e implante alterações no FTD.



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



You have unsaved changes



Verifique se o sinkhole está funcionando

```
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

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

Troubleshoot

Navegue para Analysis >> Connections >> Security Intelligence Events para rastrear todos os eventos disparados pelo SI, desde que você tenha ativado o registro na Política 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...	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	

Você também pode usar o comando `system support firewall-engine-debug` no FTD que é gerenciado pelo 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
```

Capturas de pacotes podem ser úteis para confirmar se as solicitações DNS estão sendo feitas no servidor FTD. Não se esqueça de limpar o cache em seu host local ao testar.

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>_