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

Contents

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.

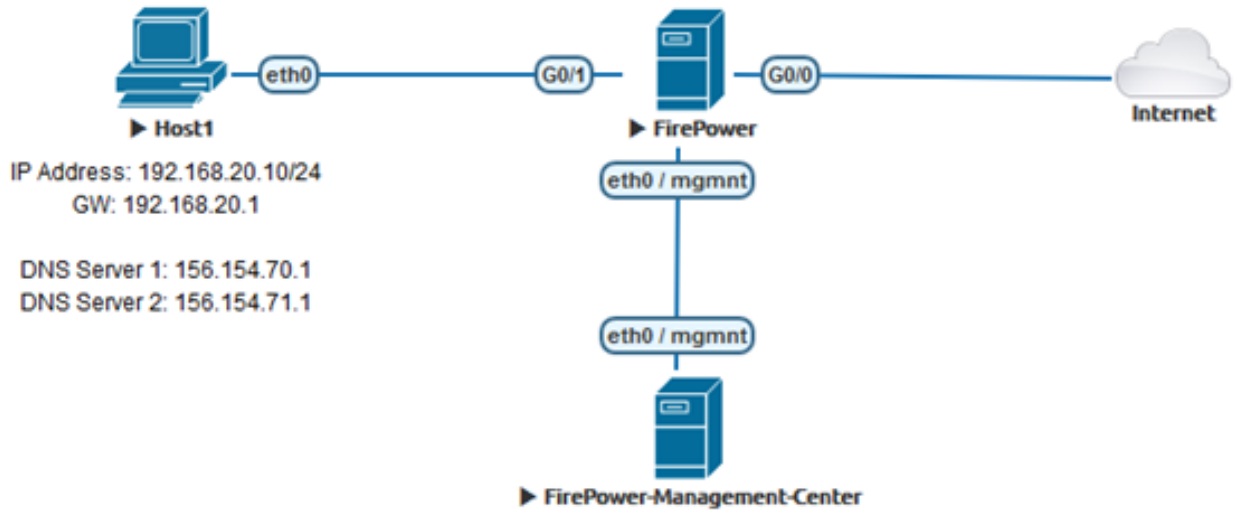
O exemplo usou o domínio dos blocos 1:

- 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.

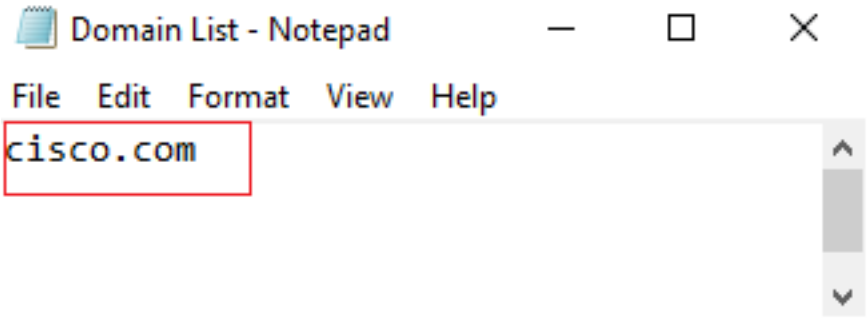
Diagrama de Rede



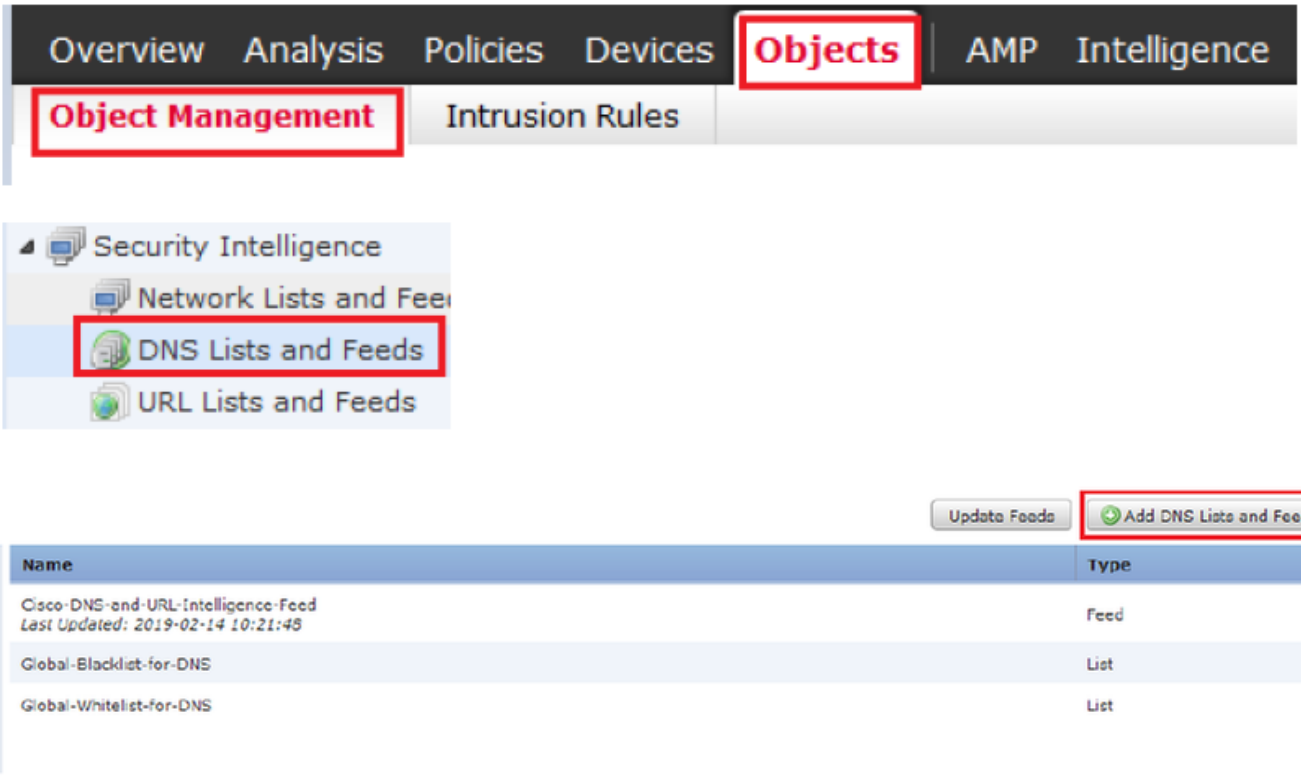
Configurar

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

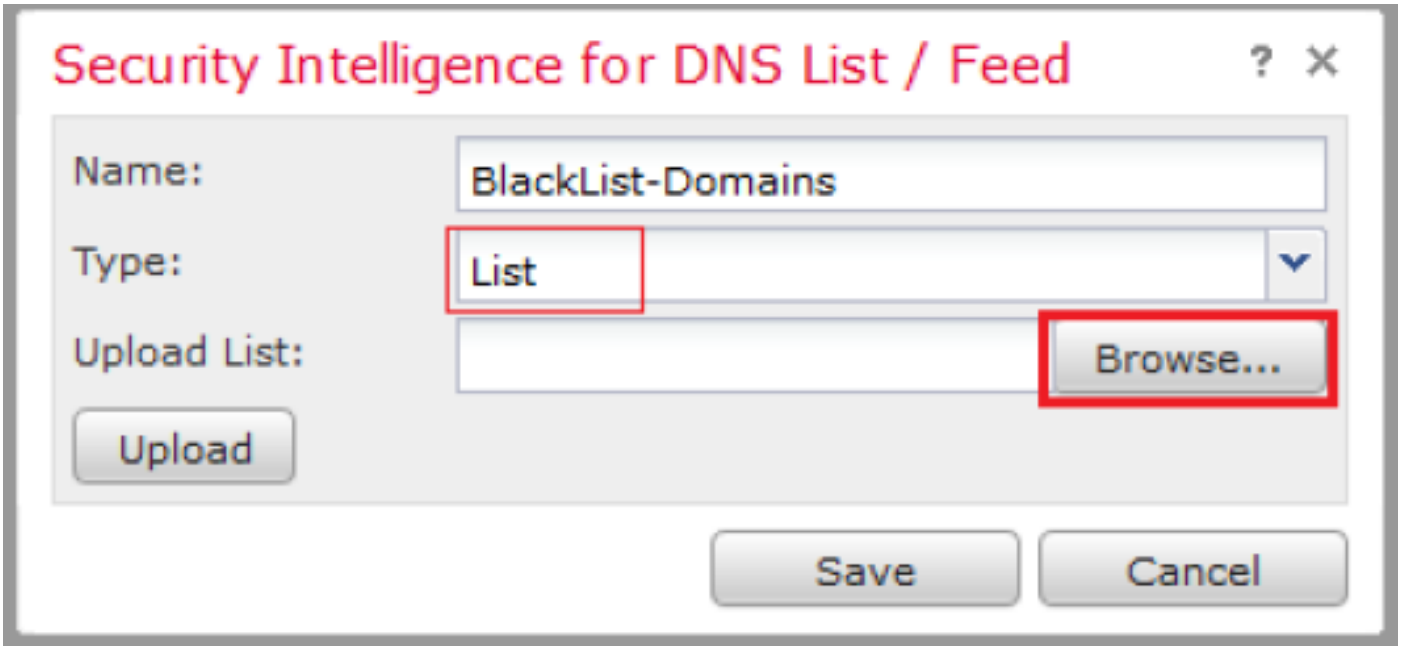
Etapa 1. Crie um arquivo .txt com os domínios que você gostaria de bloquear. Salve o arquivo .txt no computador:

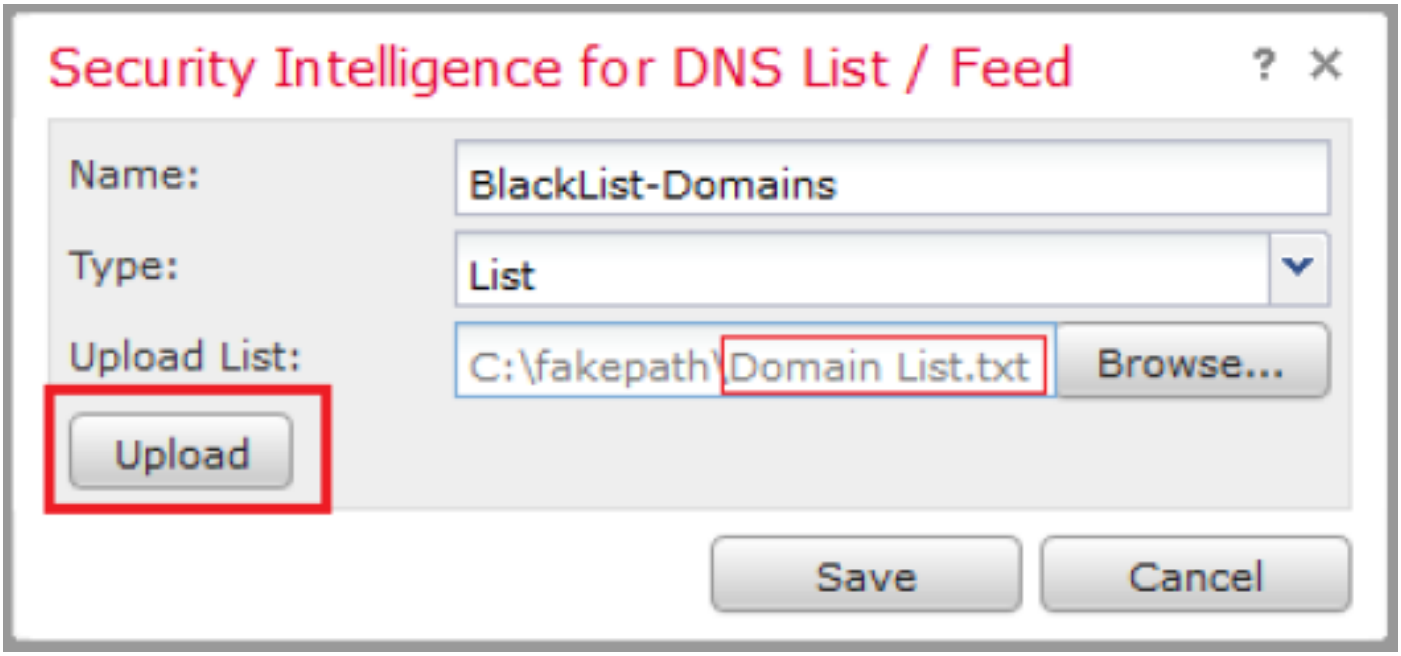


Etapa 2. No FMC, navegue até Object > Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds (Objeto > Gerenciamento de objetos >> Listas e feeds DNS >> Add DNS List and Feeds).

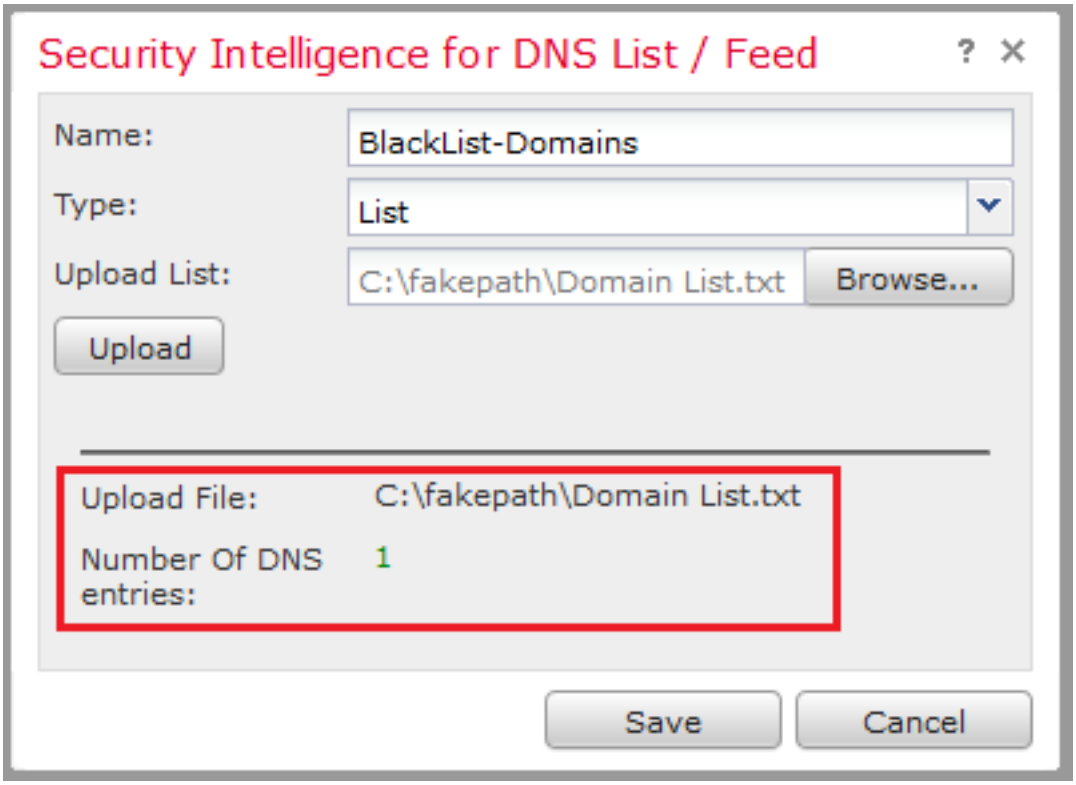


Etapa 3. Crie uma lista chamada "BlackList-Domains", o tipo deve ser uma lista e o arquivo .txt com os domínios em questão deve ser carregado conforme visto nas imagens:





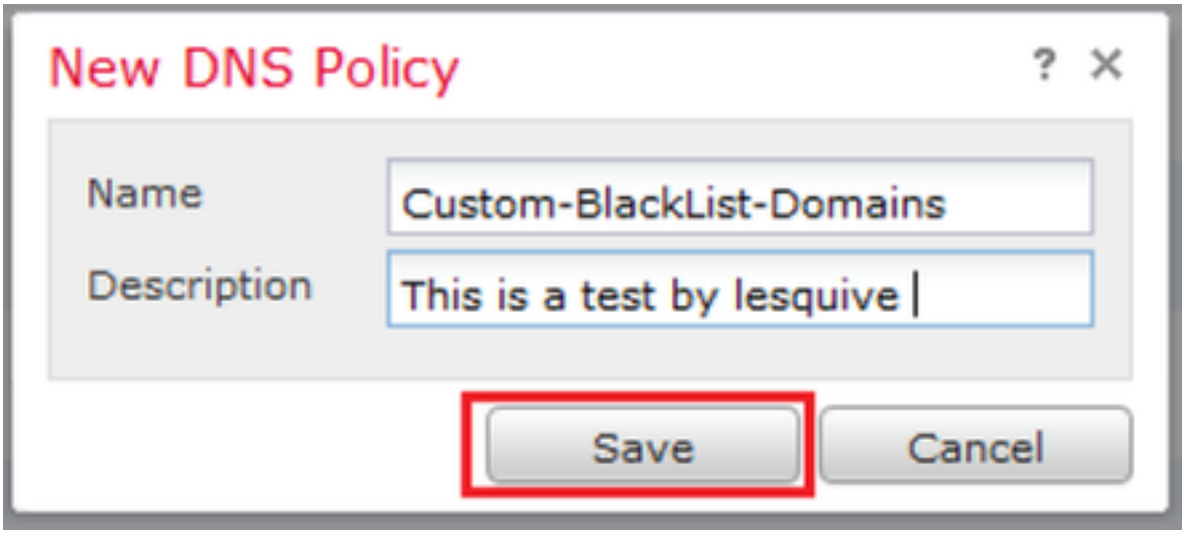
*Observe que quando você carrega o arquivo .txt, o número de entradas DNS deve ler todos os domínios. Neste exemplo, um total de 1:



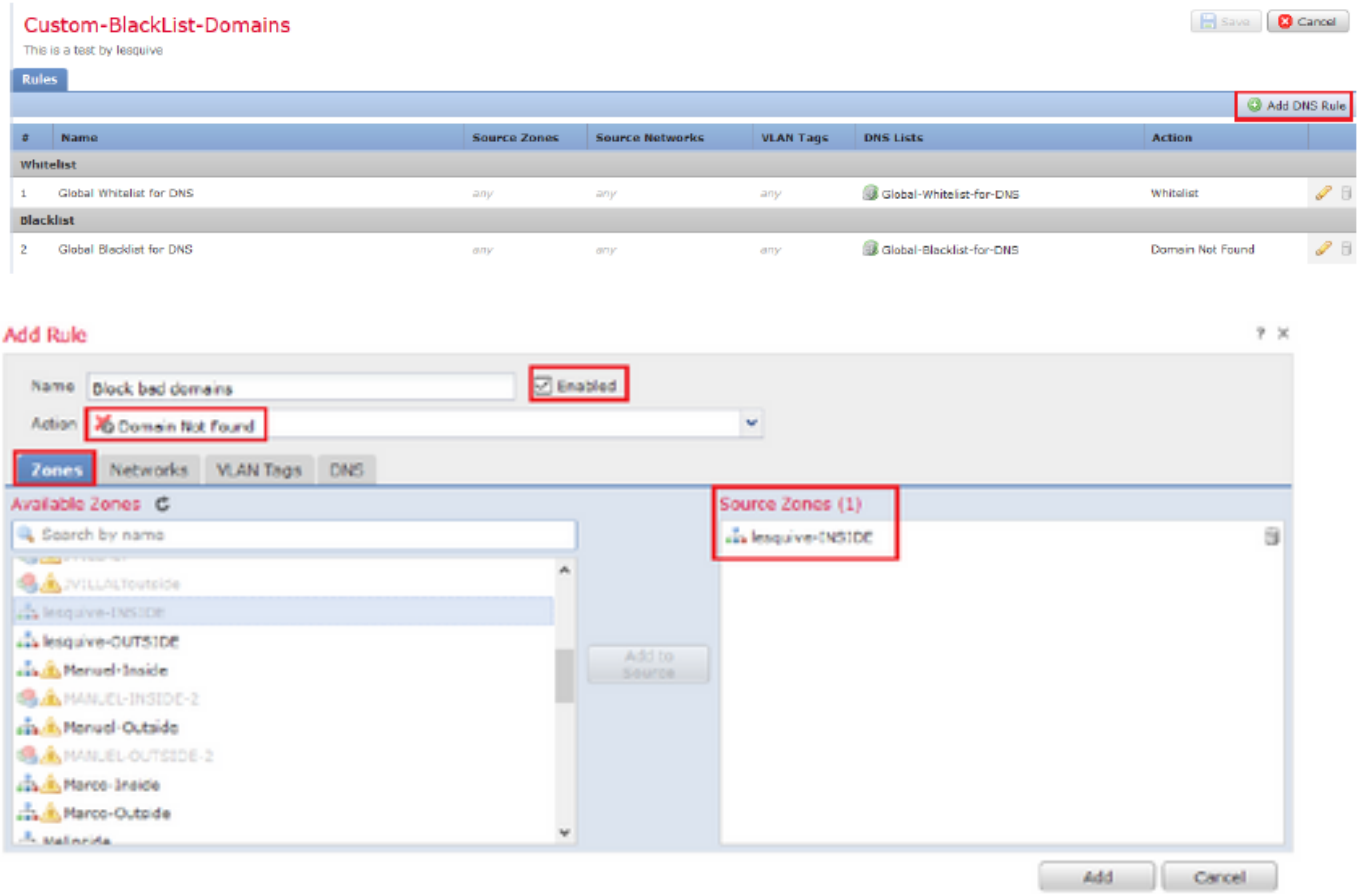
Adicionar uma nova política DNS com a 'ação configurada para 'domínio não encontrado'

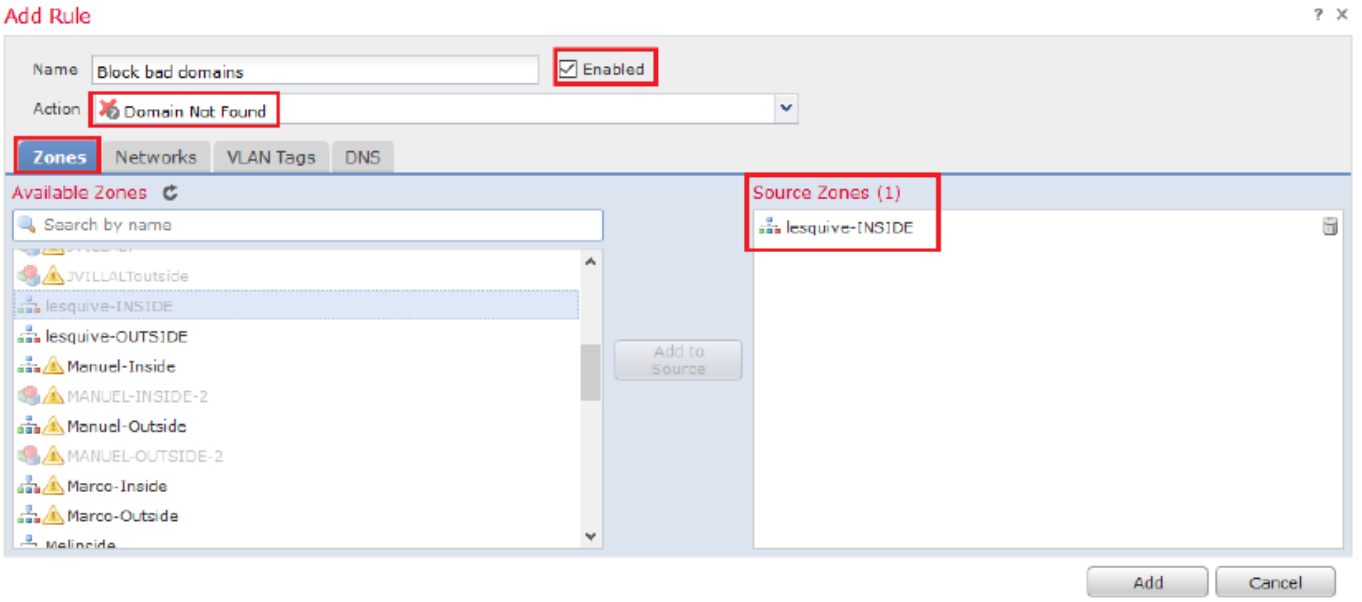
*Certifique-se de adicionar uma zona de origem, uma rede de origem e uma lista DNS.

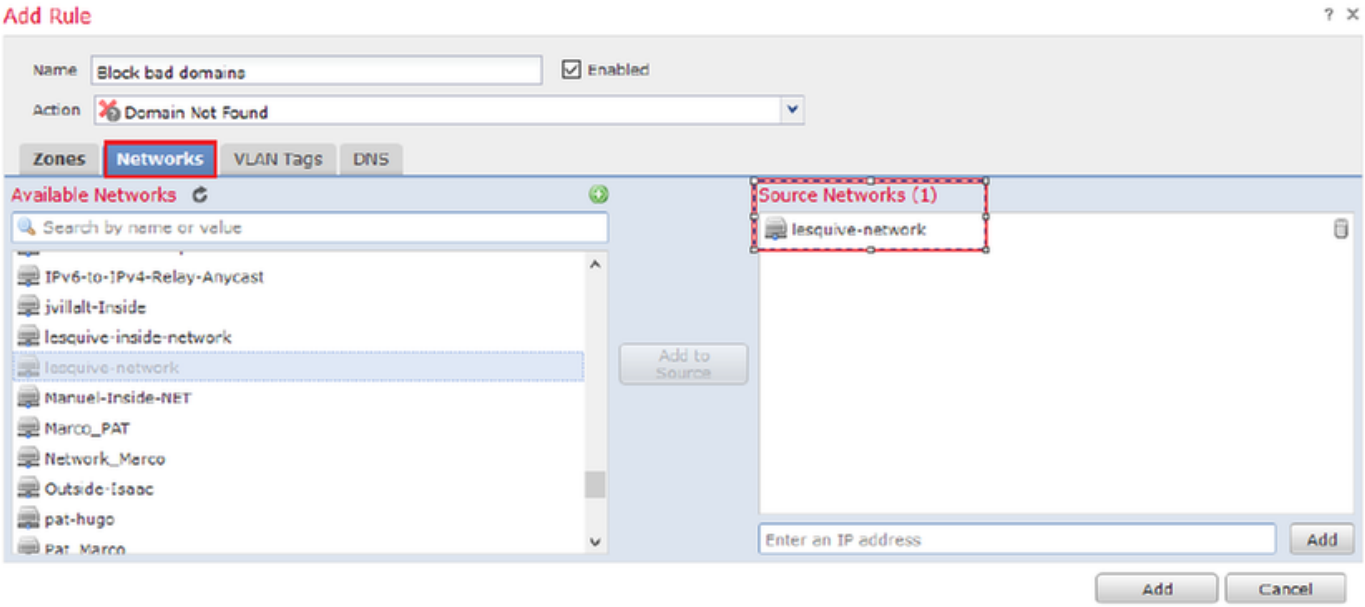
Etapa 1. Navegue até Políticas >> Controle de acesso >> DNS >> Adicionar política DNS:

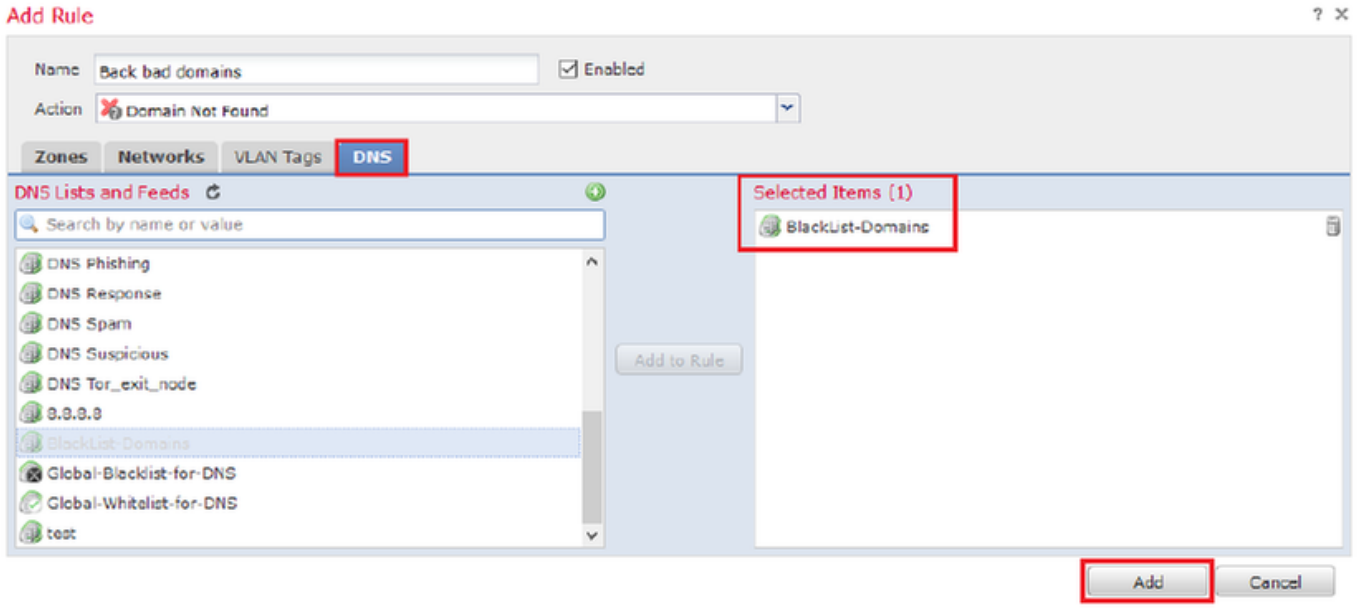


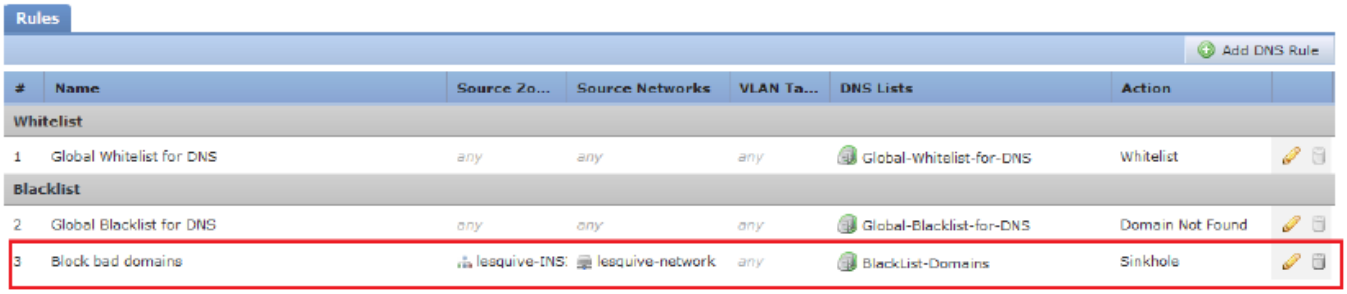
Etapa 2. Adicione uma regra de DNS conforme vista na imagem:




Add Rule
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

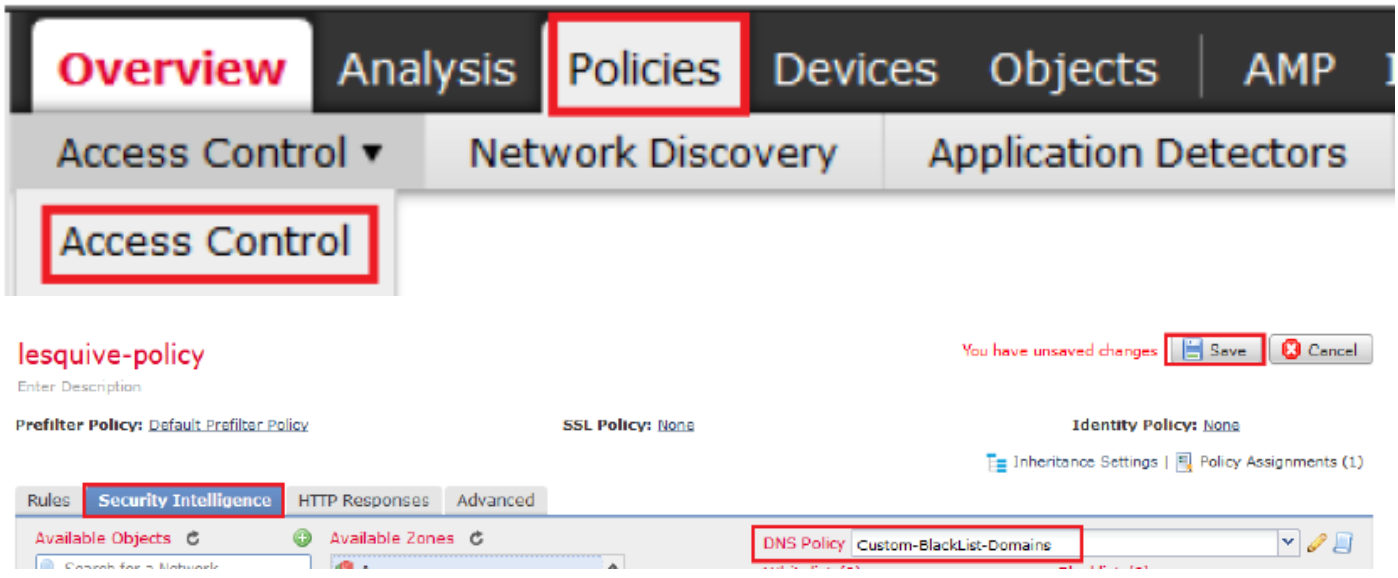


Informações importantes sobre a ordem das regras:

- 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.

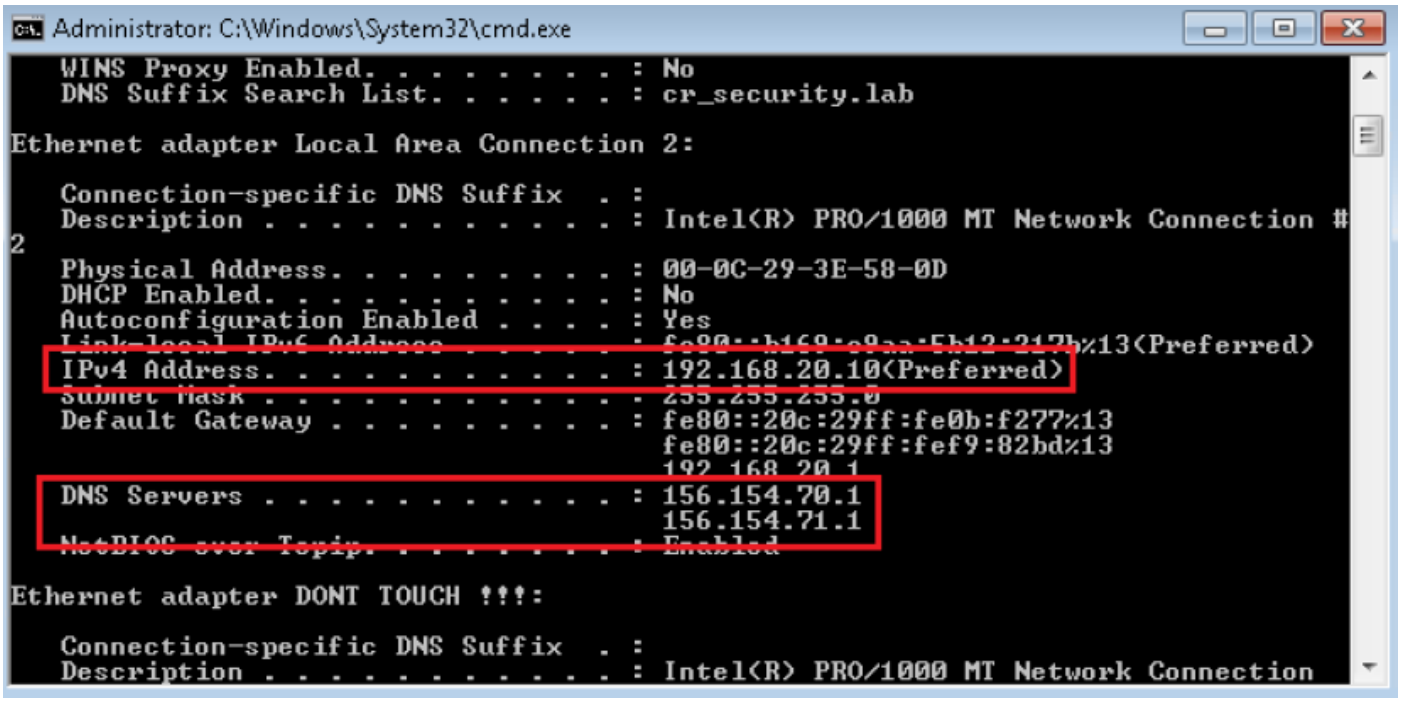


Certifique-se de implantar todas as alterações quando terminar.

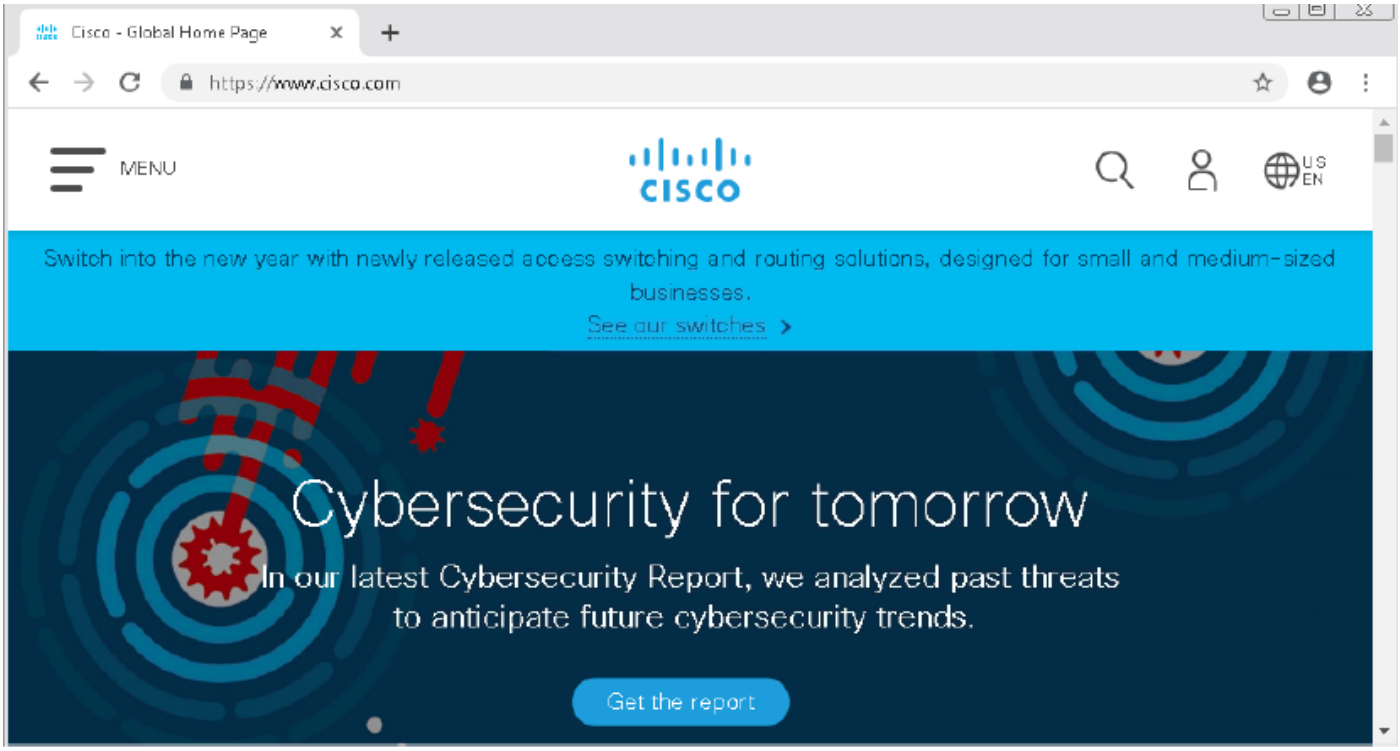
Verificar

Antes de a política DNS ser aplicada

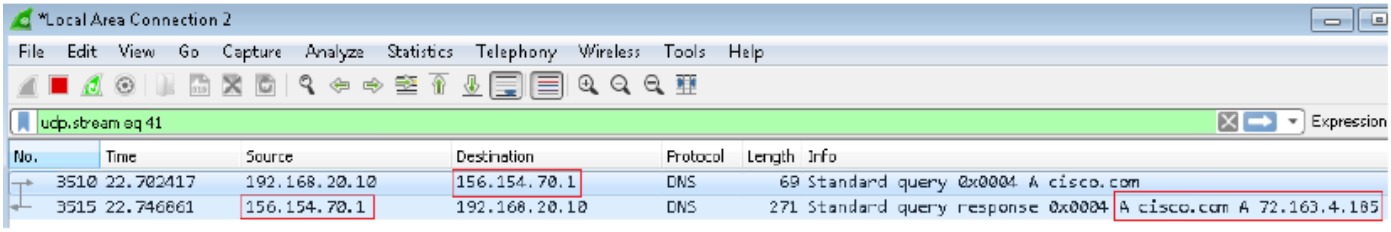
Etapa 1. Verifique as informações do servidor DNS e do endereço IP na máquina host conforme visto na imagem:

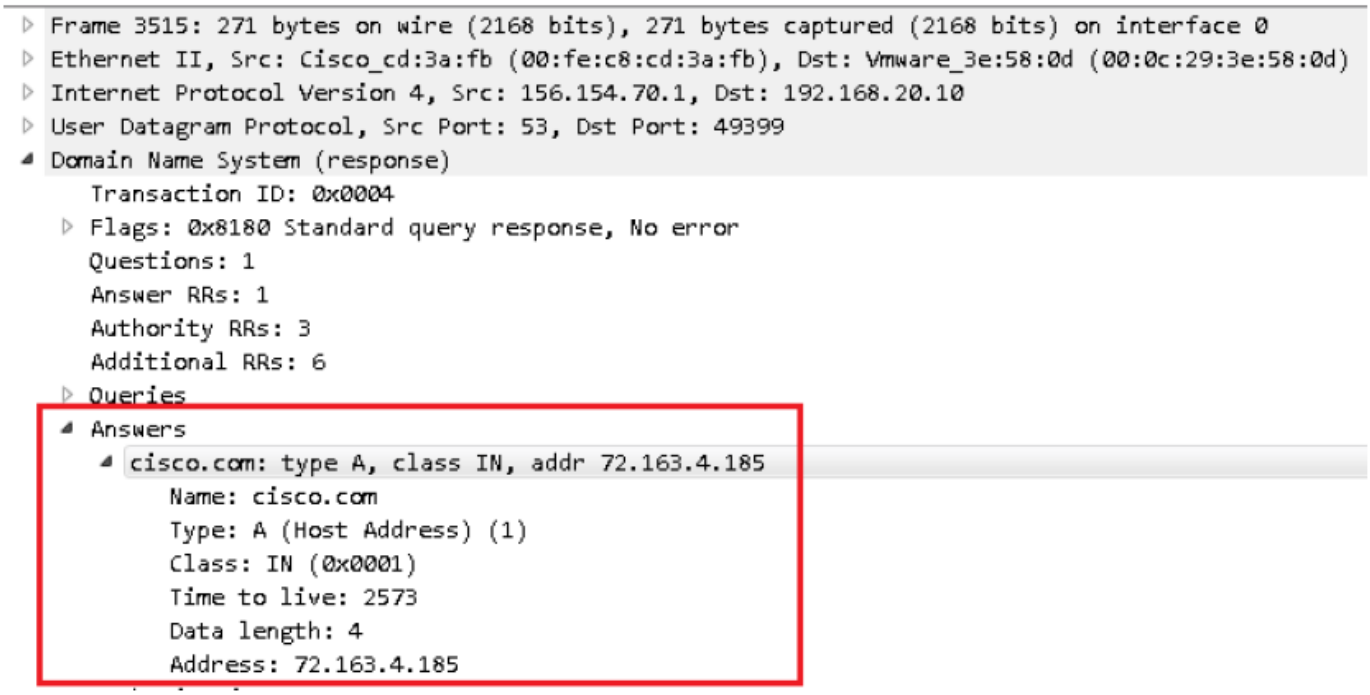


Etapa 2. Confirme se você pode navegar para cisco.com conforme visto na imagem:



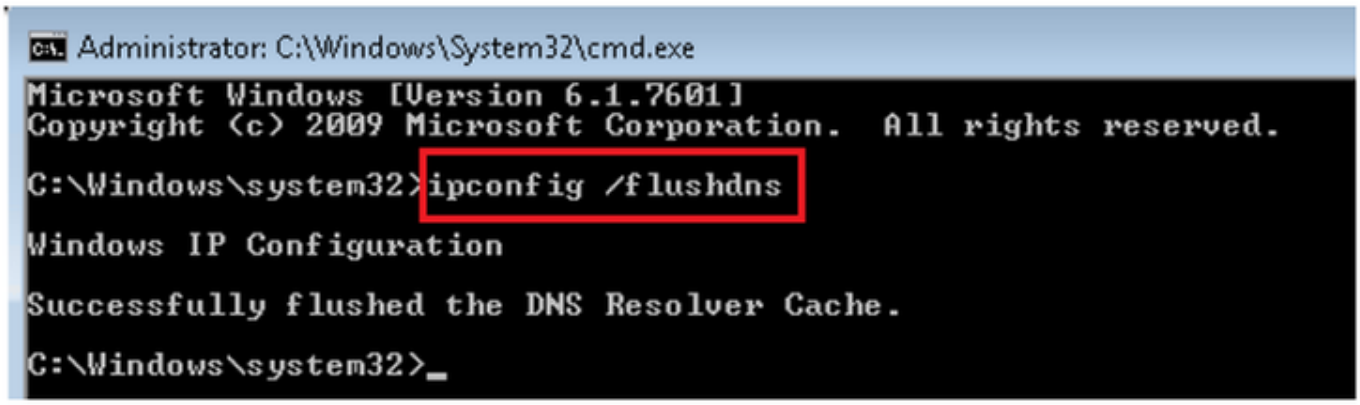
Etapa 3. Confirme com as capturas de pacotes que o DNS foi resolvido corretamente:



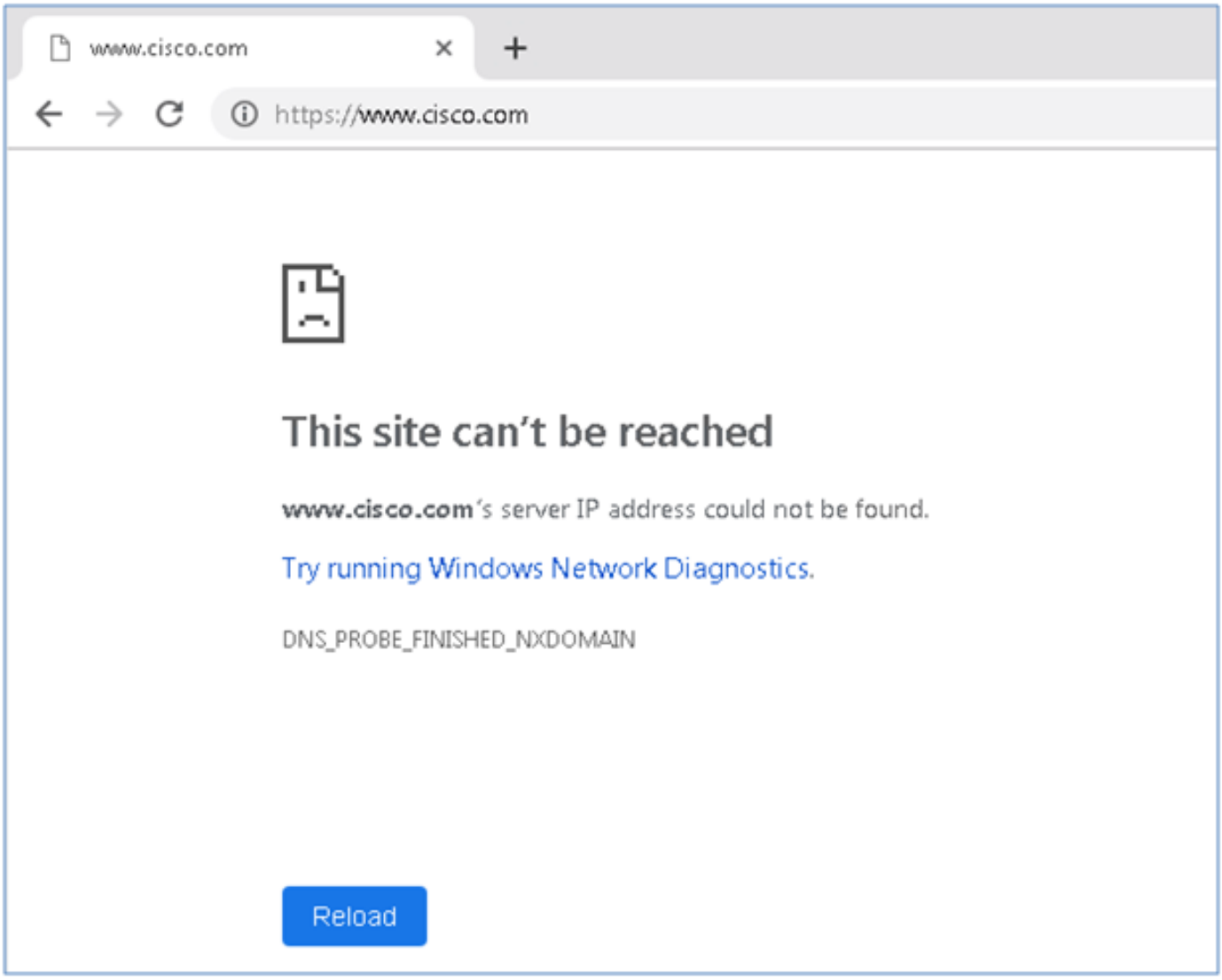


Depois que a política de DNS for aplicada

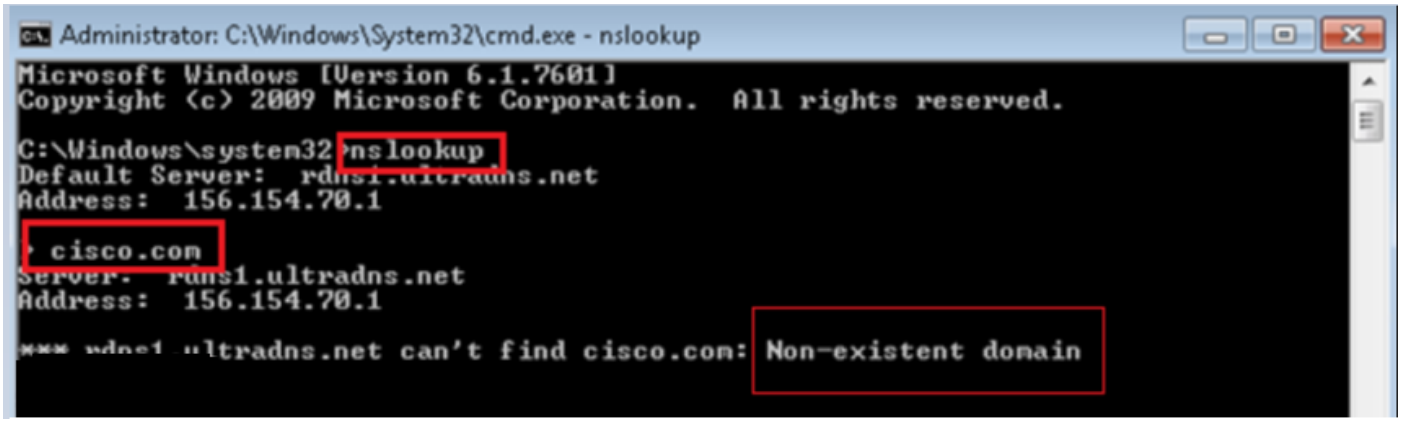
Etapa 1. Limpe o cache DNS no host com o comando **ipconfig /flushdns.**



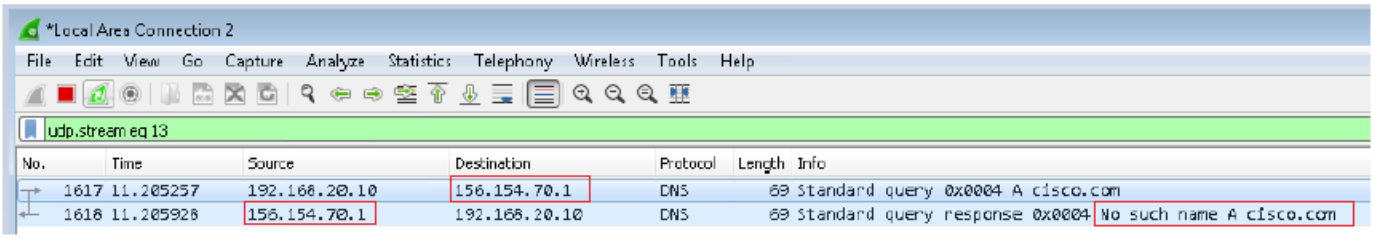
Etapa 2. Navegue até o domínio em questão com um navegador da Web. Deve ser inalcançável:

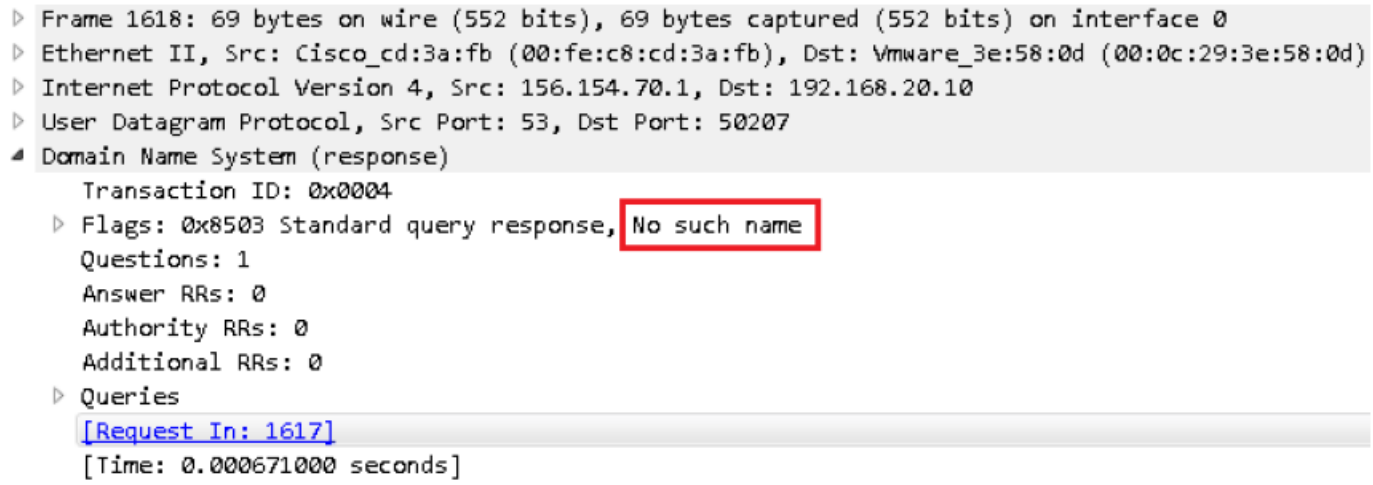


Etapa 3. Tente emitir **nslookup** no domínio cisco.com. A resolução do nome falha.

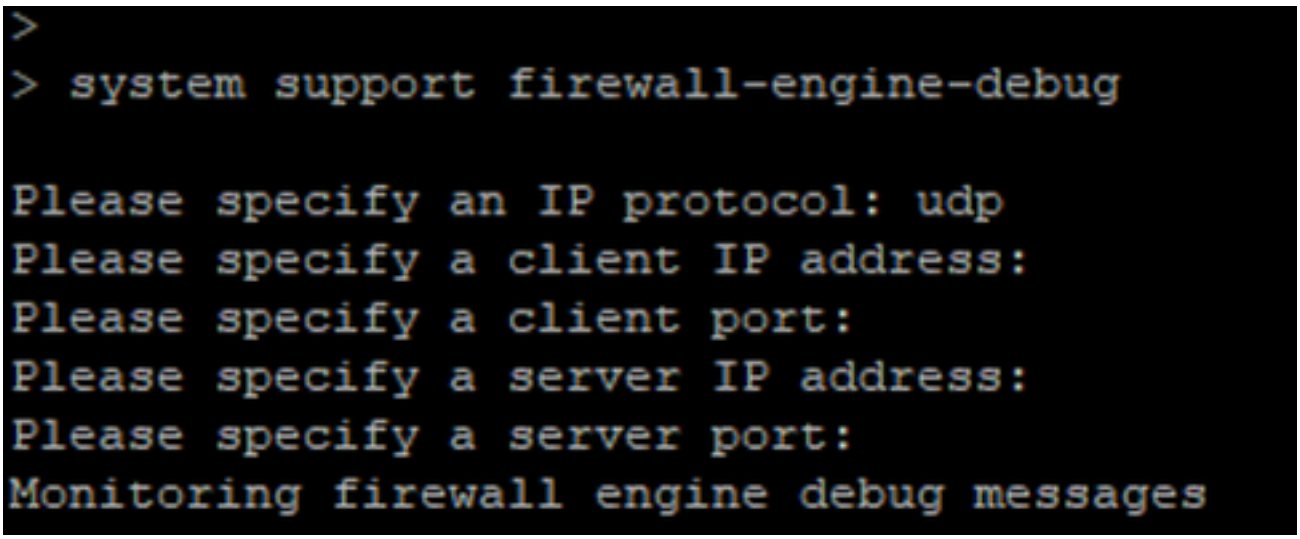


Etapa 4. As capturas de pacotes mostram uma resposta do FTD, em vez do servidor DNS.





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



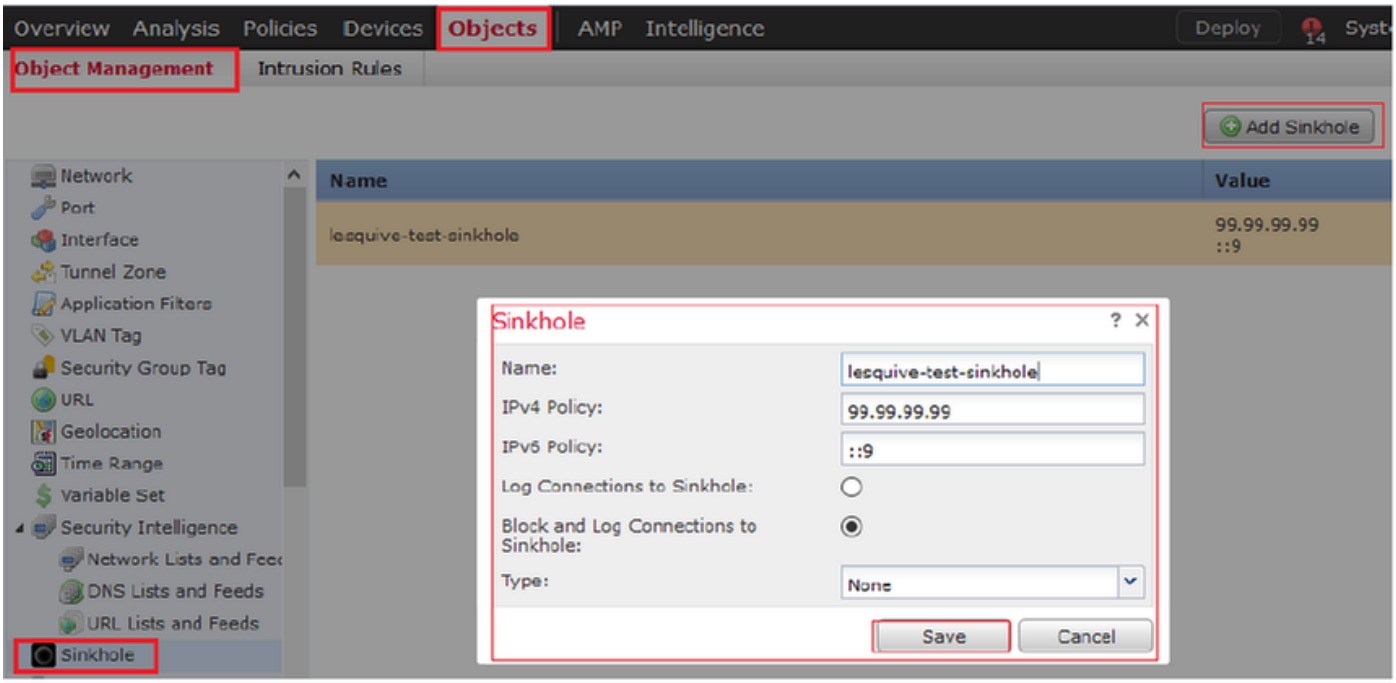
*Depurações quando cisco.com é compatível:

```
> 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 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
```

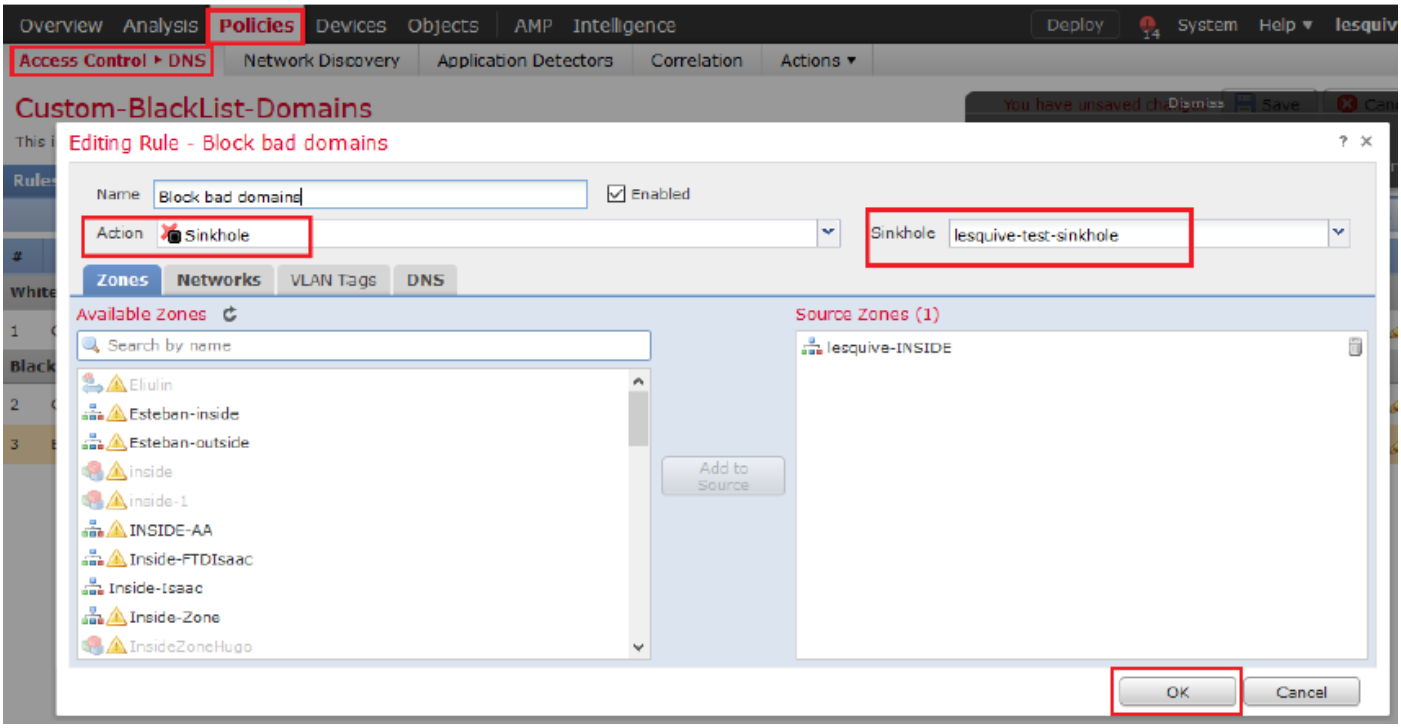
Configuração opcional do sinkhole

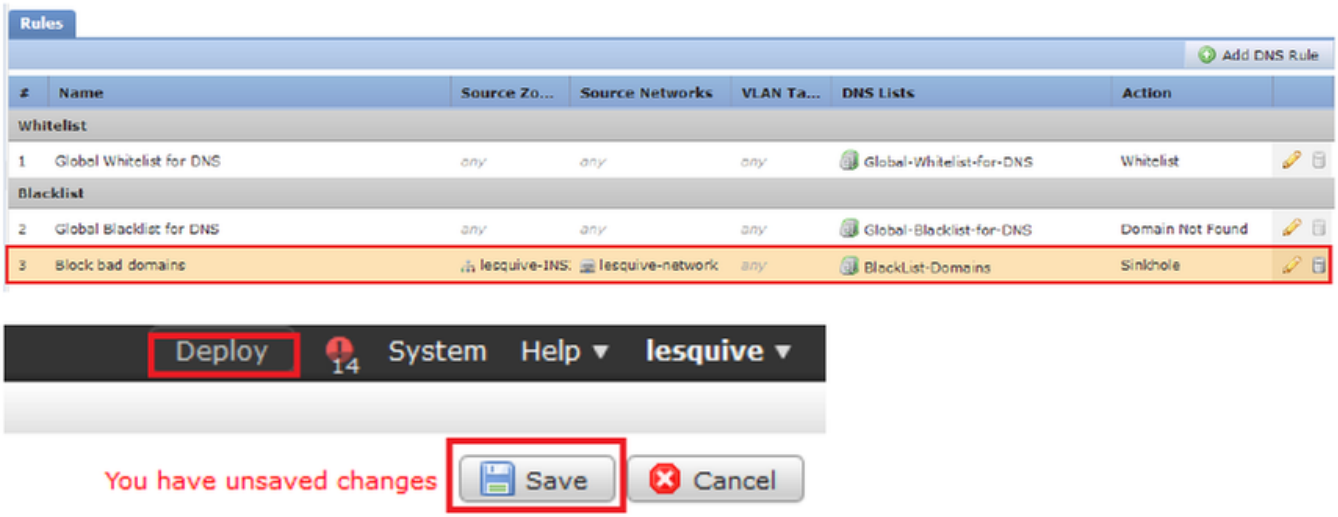
Um sinkhole DNS é um servidor DNS que fornece informações falsas. Em vez de retornar uma resposta de DNS "Sem esse nome" para consultas de DNS em domínios que você está bloqueando, ele retorna um endereço IP falso.

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

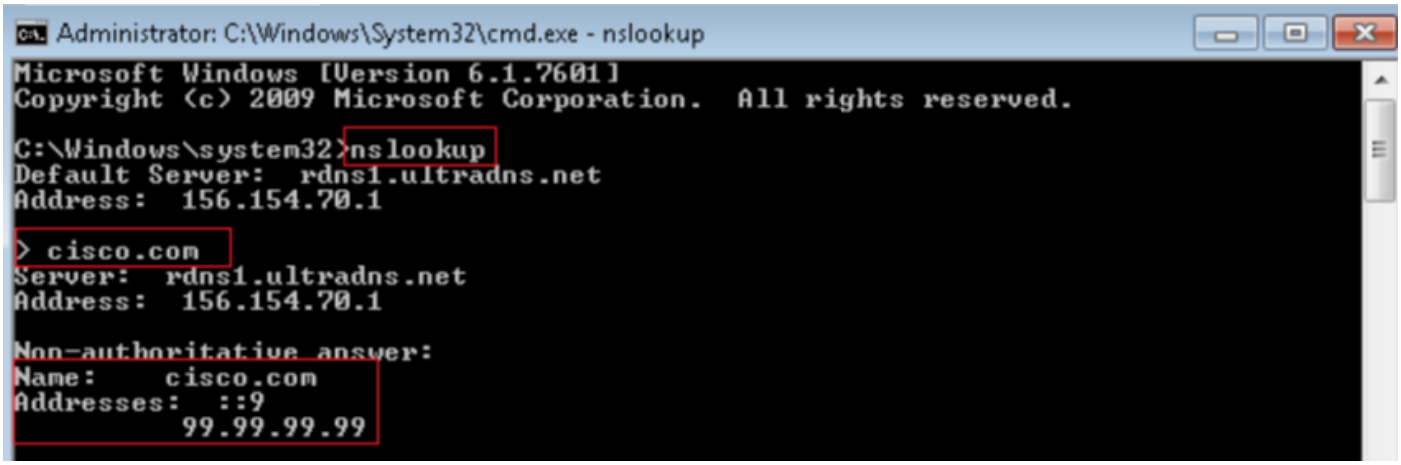


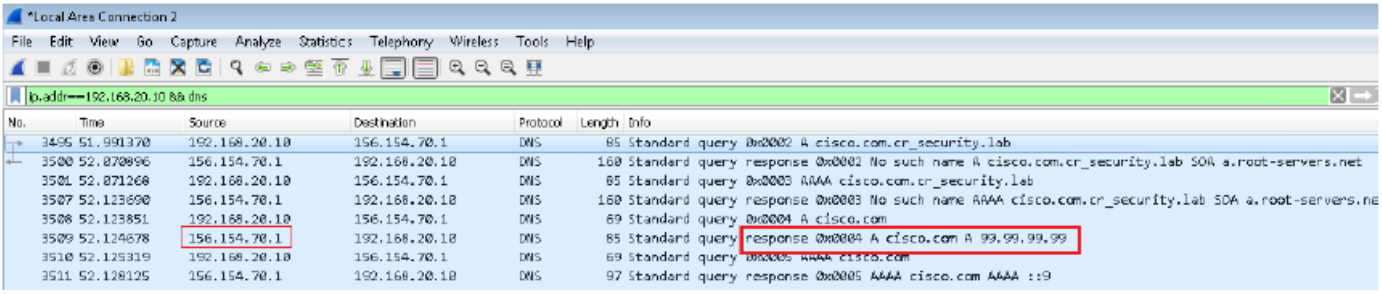
Etapa 2. Aplique o sinkhole à sua política de DNS e implante alterações no FTD.





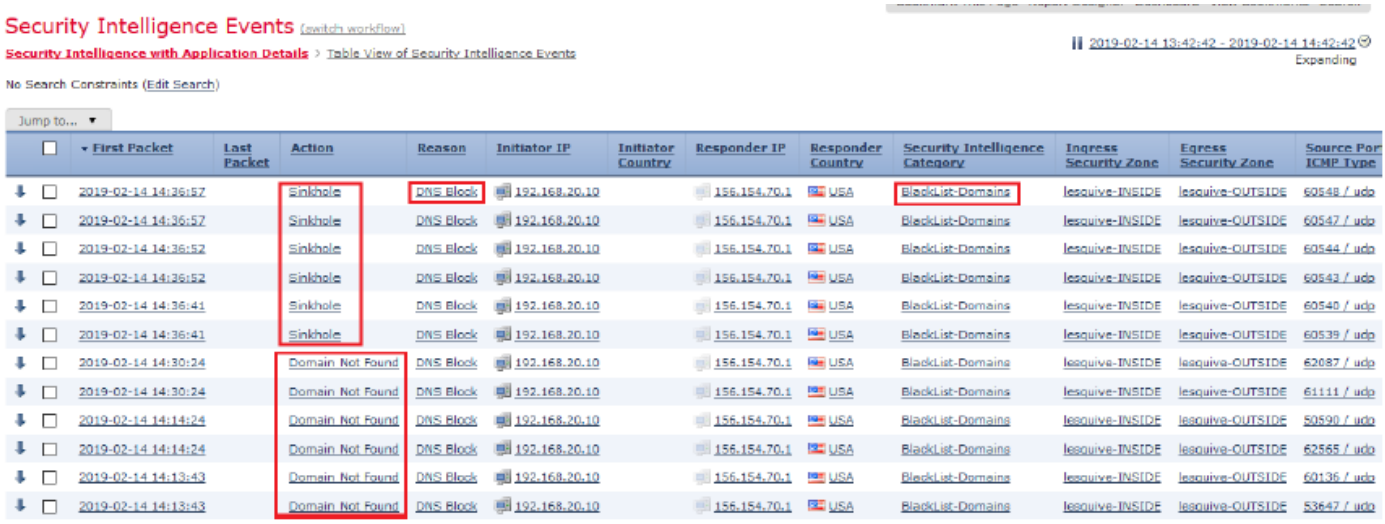
Verifique se o sinkhole está funcionando





Troubleshoot

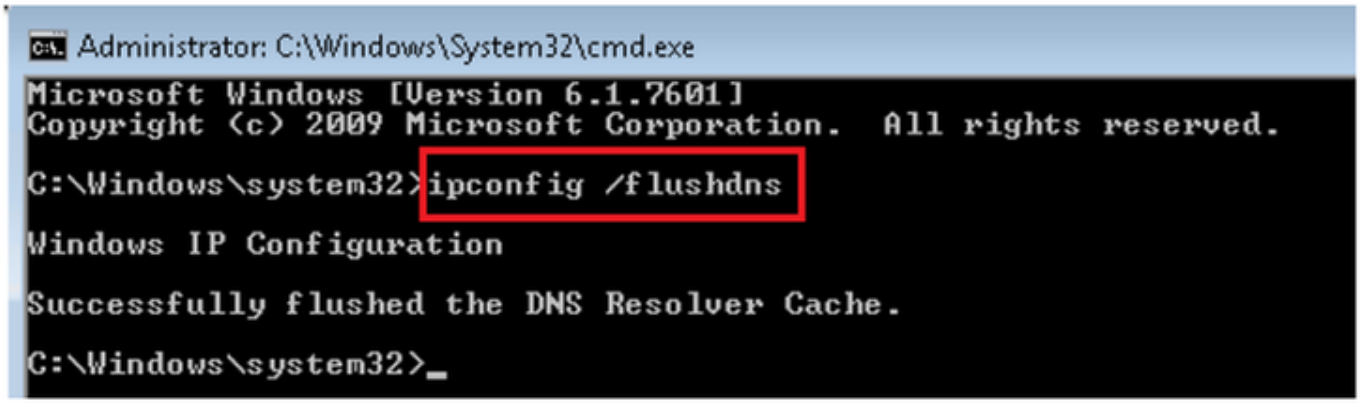
Navegue para Analysis >> Connections >> Security Intelligence Events para rastrear todos os eventos disparados pelo SI, desde que você tenha ativado o registro na Política DNS:



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>