Bloqueo de DNS con inteligencia de seguridad mediante Firepower Management Center

Contenido

Introducción

Este documento describe el procedimiento para agregar una lista de sistema de nombres de dominio (DNS) a una política DNS para que pueda aplicarla con Security Intelligence (SI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Cisco ASA55XX Threat Defense
- configuración de Cisco Firepower Management Center

Componentes Utilizados

- Defensa frente a amenazas Cisco ASA5506W-X (75) Versión 6.2.3.4 (Compilación 42)
- Cisco Firepower Management Center para VMWare Versión del software: 6.2.3.4 (compilación 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 tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La inteligencia de seguridad funciona bloqueando el tráfico hacia o desde direcciones IP, URL o nombres de dominio que tienen una mala reputación conocida. En este documento, el enfoque principal es la lista negra de nombres de dominio.

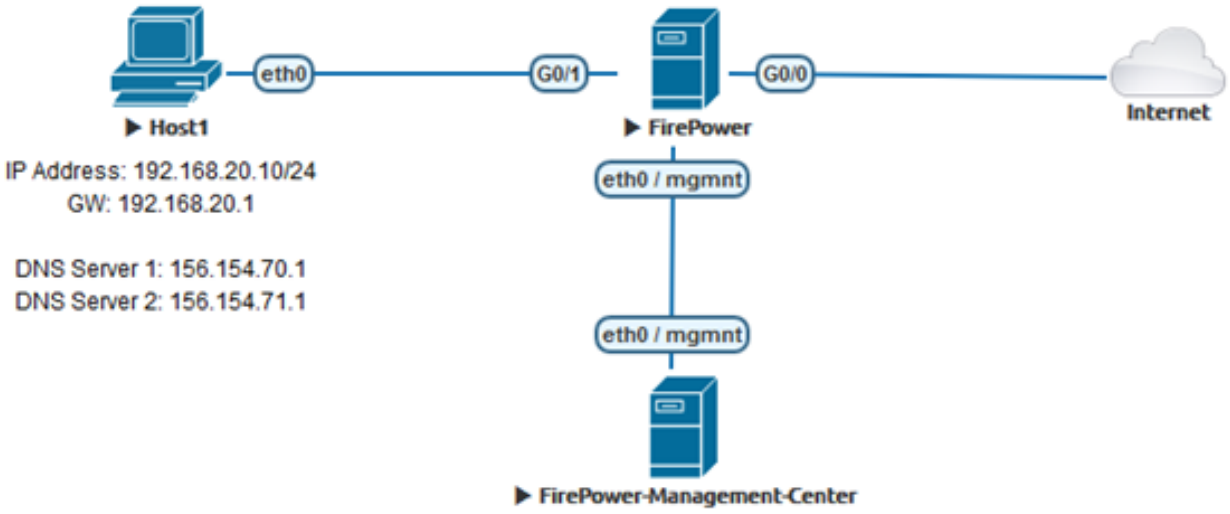
El ejemplo utilizado bloquea el dominio 1:

- cisco.com

Puede utilizar el filtrado de URL para bloquear algunos de estos sitios, pero el problema es que la URL debe ser una coincidencia exacta. Por otra parte, las listas negras de DNS con SI pueden centrarse en dominios como "cisco.com" sin necesidad de preocuparse por subdominios o cambios en las URL.

Al final de este documento, también se muestra una configuración de Sinkhole opcional.

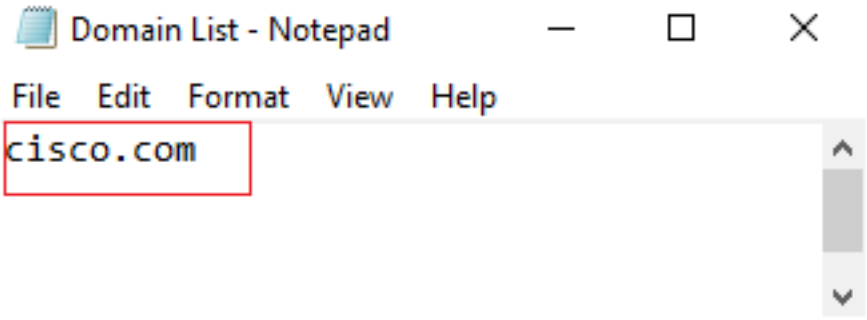
Diagrama de la red



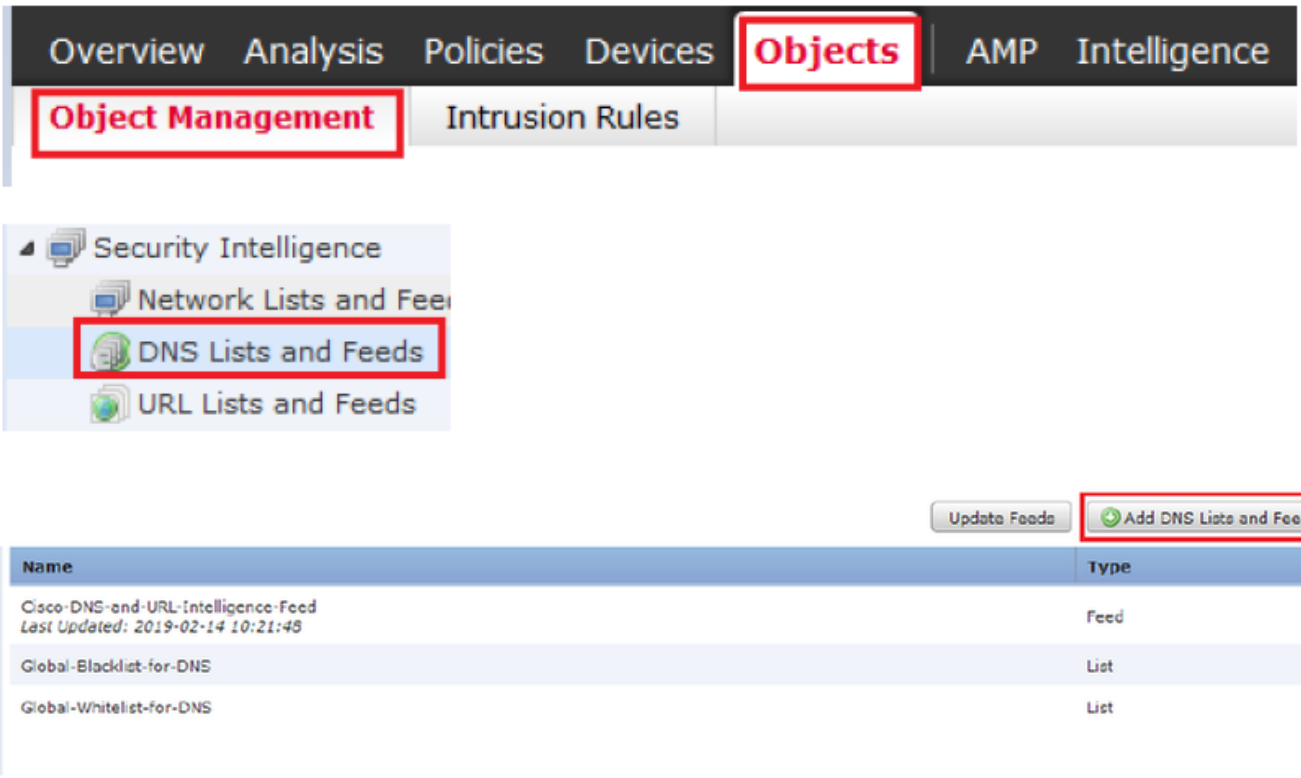
Configurar

Configure una lista DNS personalizada con los dominios que queremos bloquear y cargue la lista en FMC

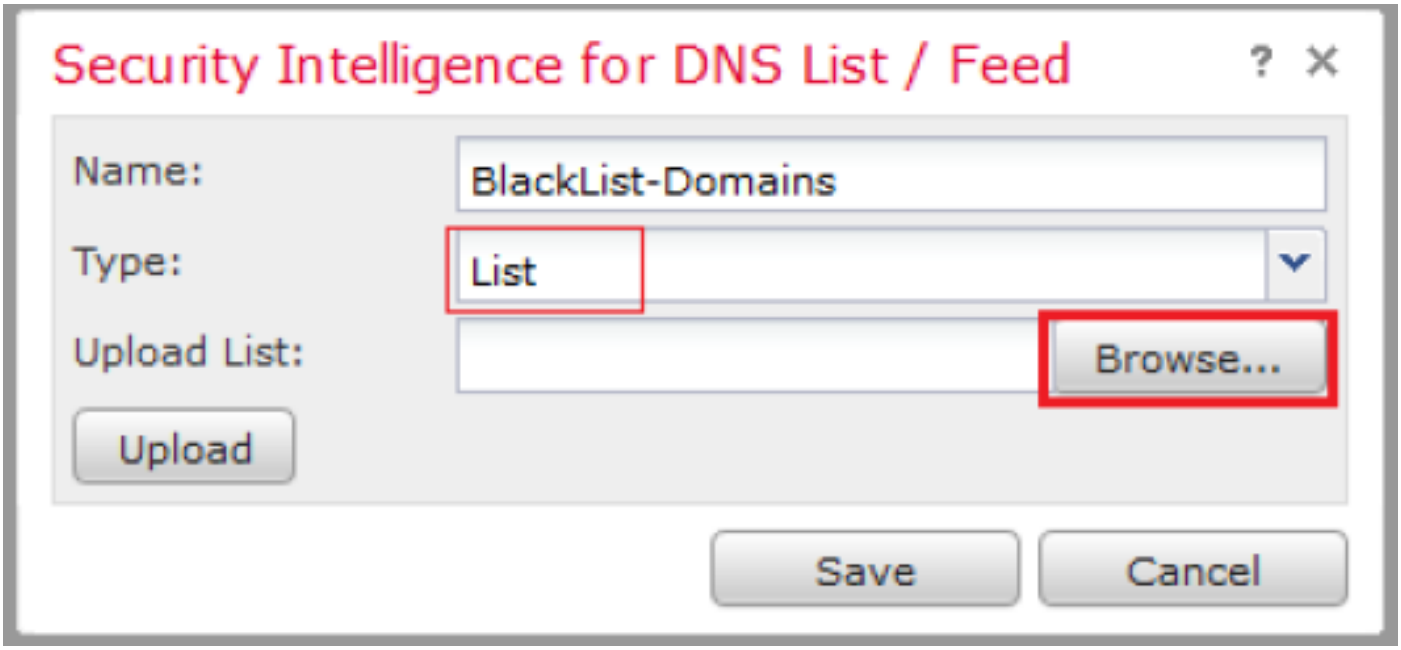
Paso 1. Cree un archivo .txt con los dominios que desea bloquear. Guarde el archivo .txt en el equipo:

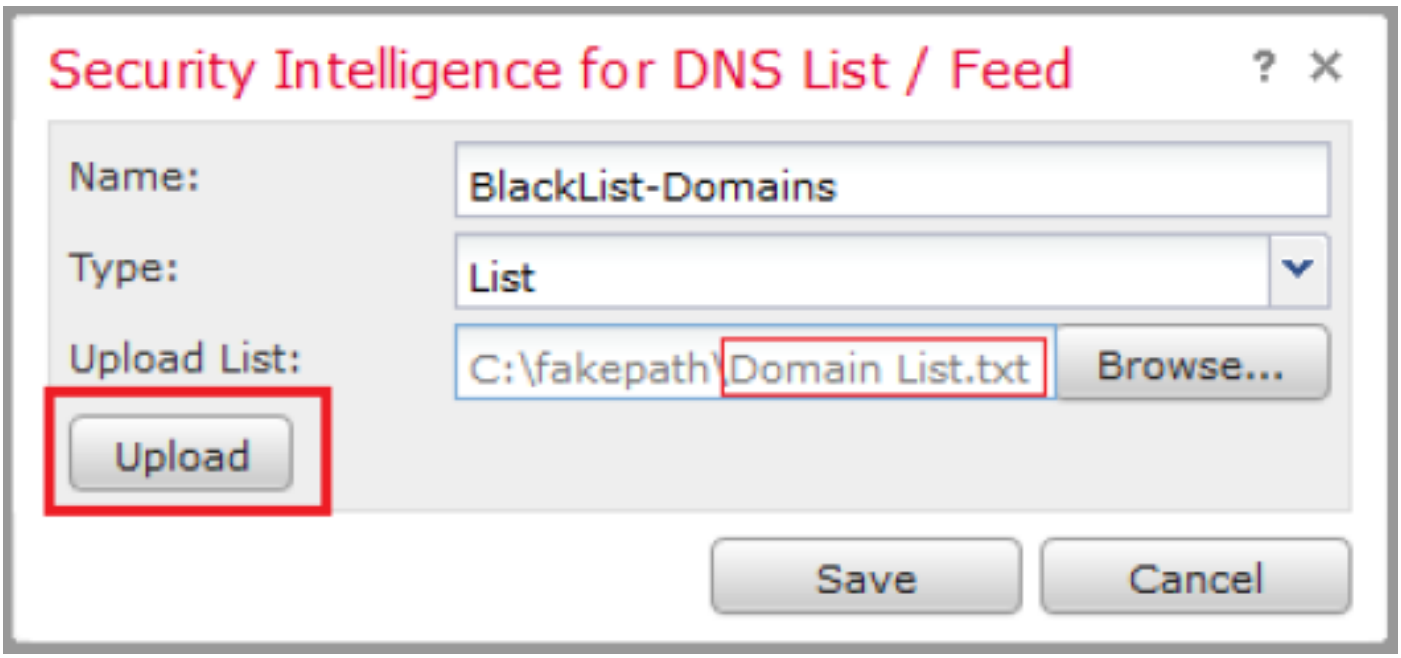


Paso 2. En FMC vaya a Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds .

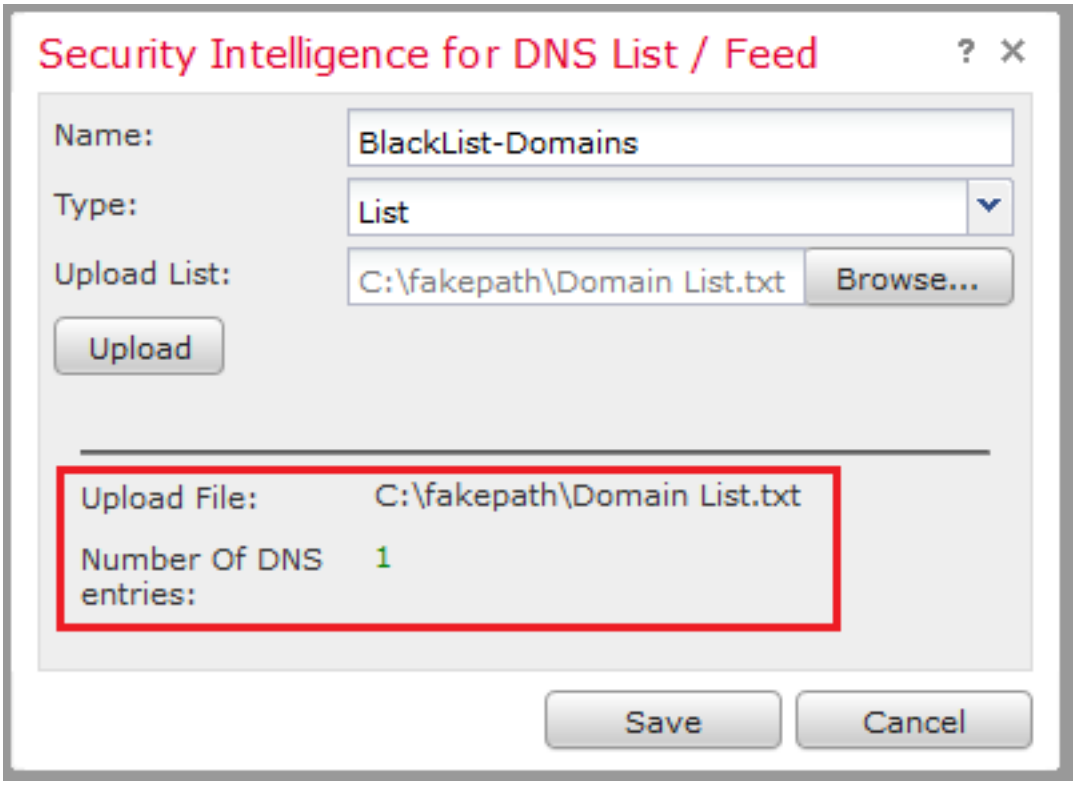


Paso 3. Cree una lista llamada "BlackList-Domains", el tipo debe ser lista y el archivo .txt con los dominios en cuestión debe cargarse como se ve en las imágenes:





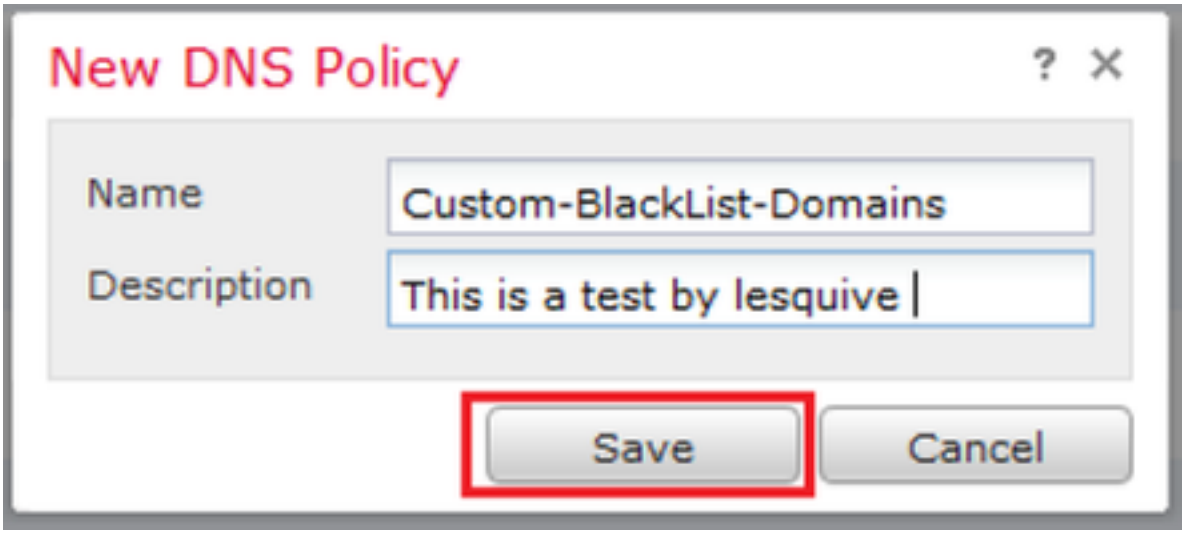
*Observe que cuando carga el archivo .txt, el número de entradas DNS debe leer todos los dominios. En este ejemplo, un total de 1:



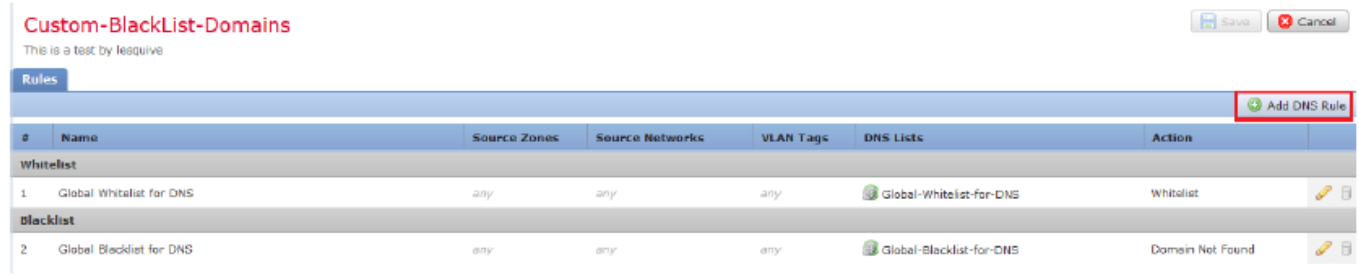
Agregue una nueva política DNS con la acción 'configurada en 'dominio no encontrado'

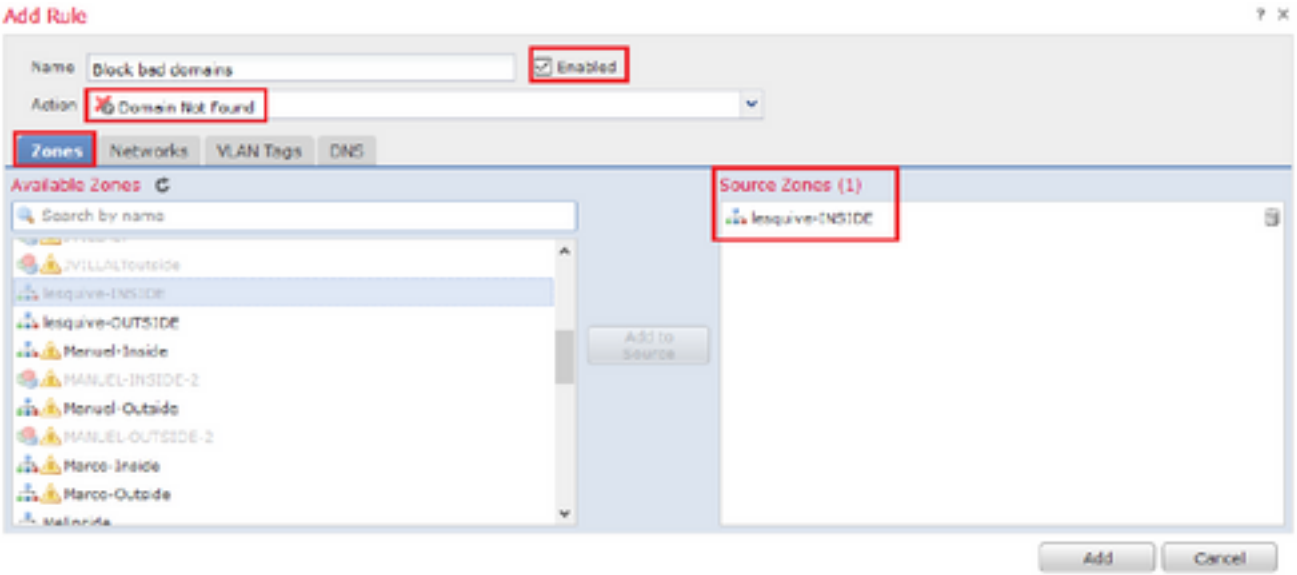
*Asegúrese de agregar una zona de origen, una red de origen y una lista DNS.

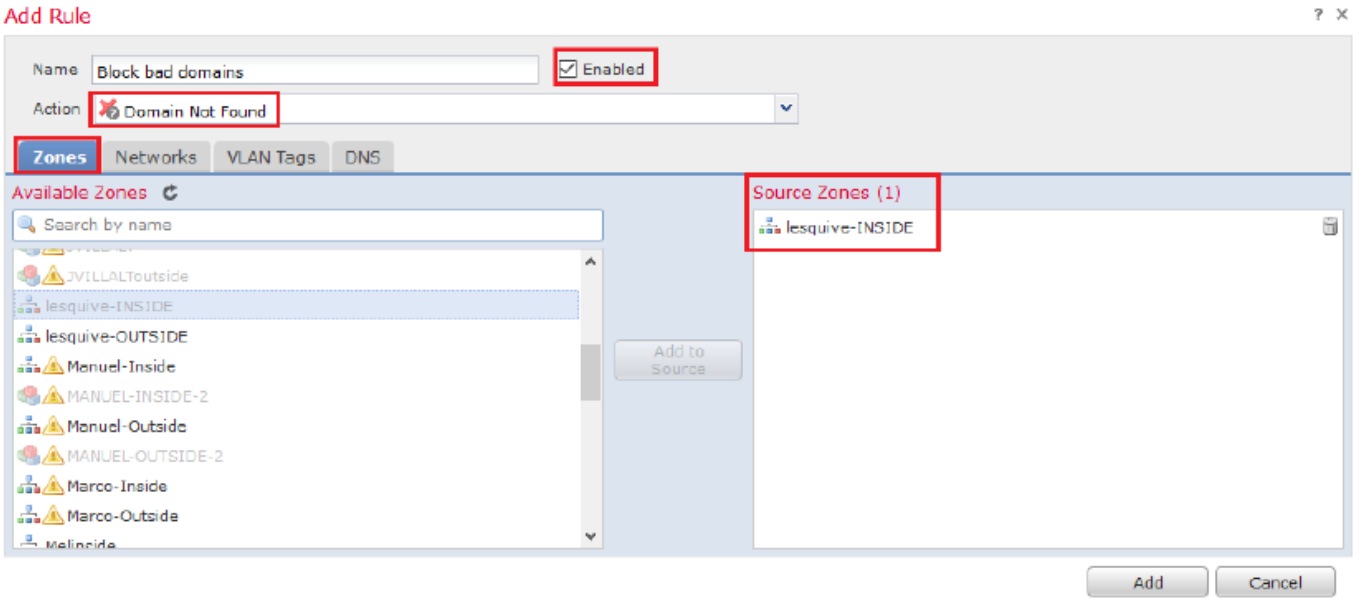
Paso 1. Vaya a Políticas >> Control de acceso >> DNS >> Agregar política DNS:

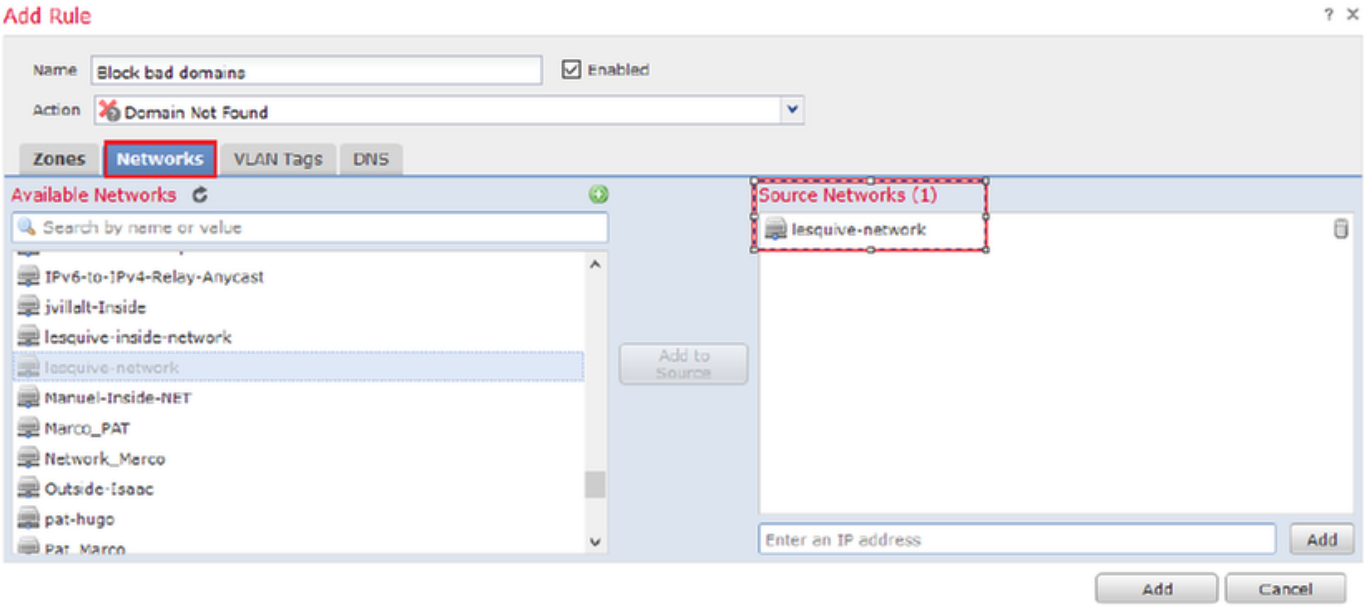


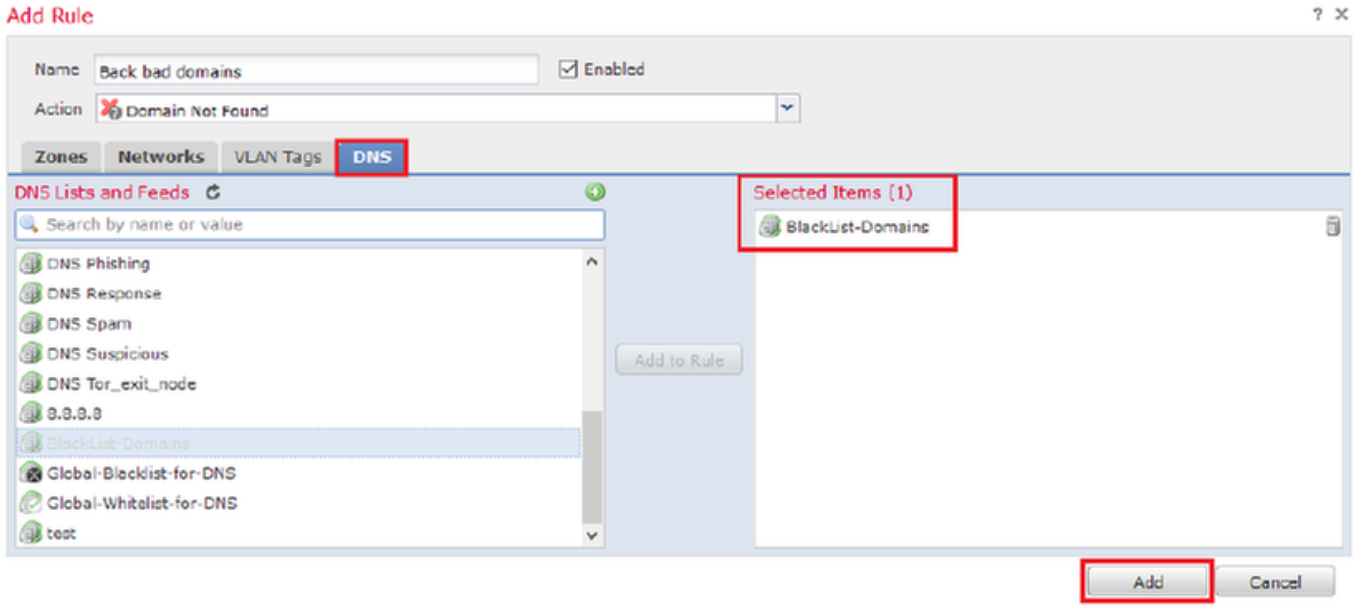
Paso 2. Agregue una regla DNS como se ve en la imagen:

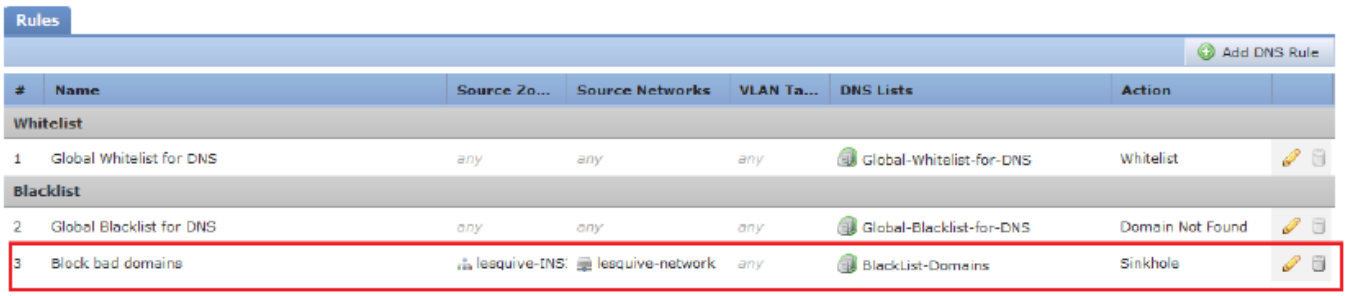





Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-INSIDE
lesquive-OUTSIDE
Manuel-Inside
MANUEL-INSIDE-2
Manuel-Outside
MANUEL-OUTSIDE-2
Marco-Inside
Marco-Outside
Add to Source
Source Zones (1)
lesquive-INSIDE
Add
Cancel


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

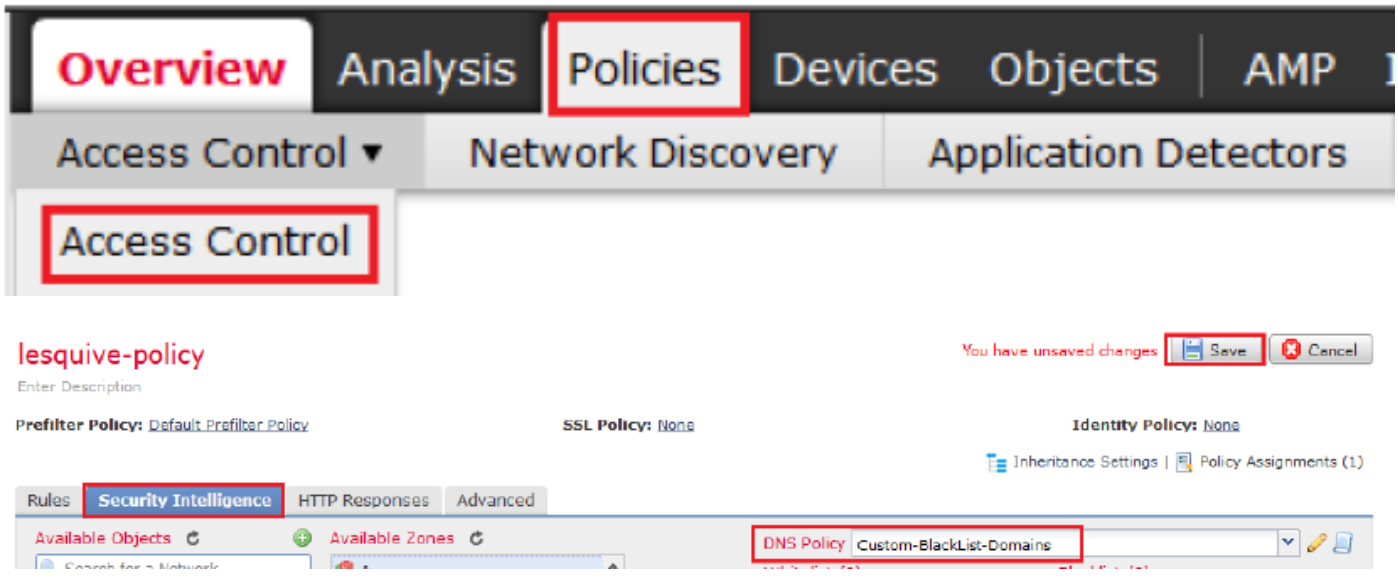


Información importante sobre el orden de reglas:

- La lista blanca global siempre es la primera y tiene prioridad sobre todas las demás reglas.
- La regla Lista blanca de DNS descendente sólo aparece en implementaciones de varios dominios, en dominios no hoja. Siempre está en segundo lugar y tiene prioridad sobre todas las demás reglas excepto la lista blanca global.
- La sección Lista blanca precede a la sección Lista negra; las reglas de la lista blanca siempre tienen prioridad sobre otras reglas.
- La lista negra global siempre aparece en primer lugar en la sección Lista negra y tiene prioridad sobre todas las demás reglas de supervisión y lista negra.
- La regla Descendant DNS Blacklists (Listas negras de DNS Descendente) sólo aparece en implementaciones de varios dominios, en dominios que no son de hoja. Siempre ocupa el segundo lugar en la sección Lista negra y tiene prioridad sobre todas las demás reglas de supervisión y lista negra excepto la lista negra global.
- La sección Lista negra contiene reglas de supervisión y lista negra.
- Cuando se crea por primera vez una regla DNS, la posición del sistema se sitúa por última vez en la sección Lista blanca si se asigna una acción de lista blanca, o por última vez en la sección Lista negra si se asigna otra acción

Asignar la política DNS a la política de control de acceso

Vaya a Policies >> Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy y agregue la política que creó.

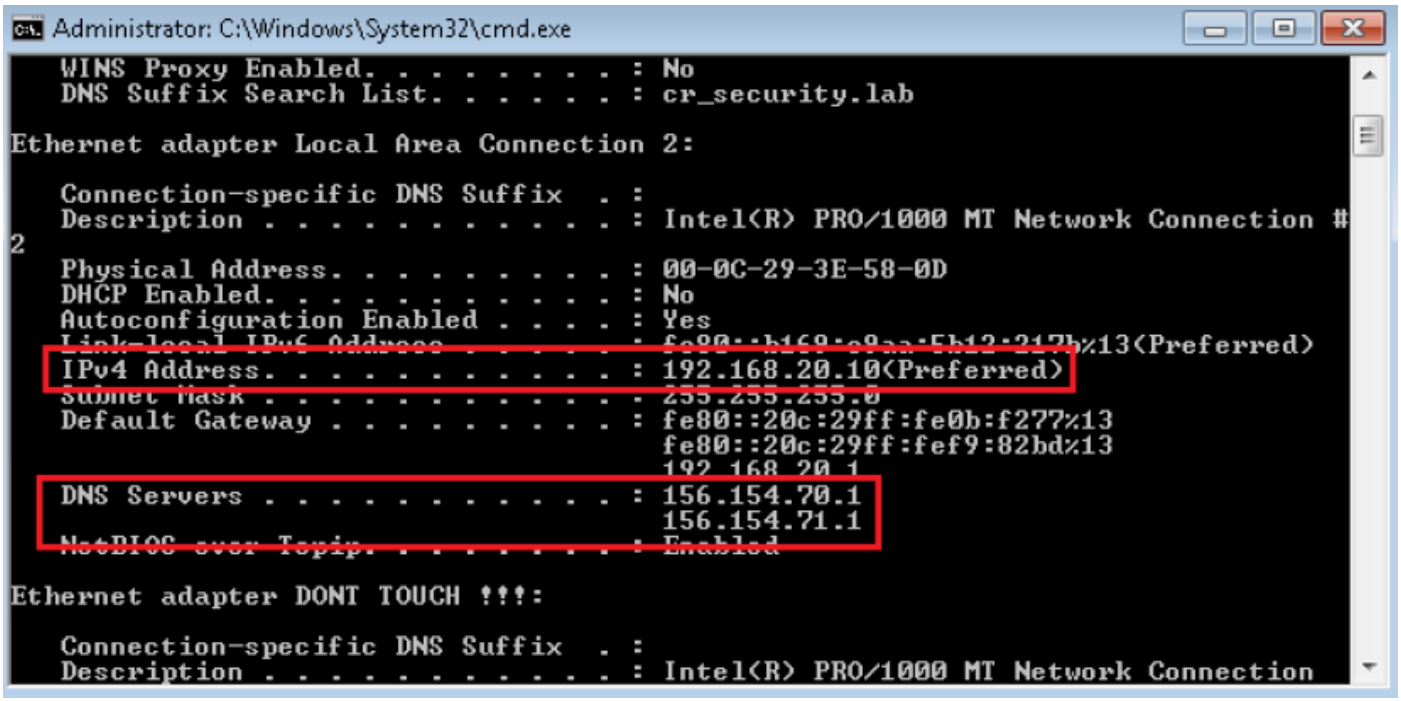


Asegúrese de implementar todos los cambios cuando haya terminado.

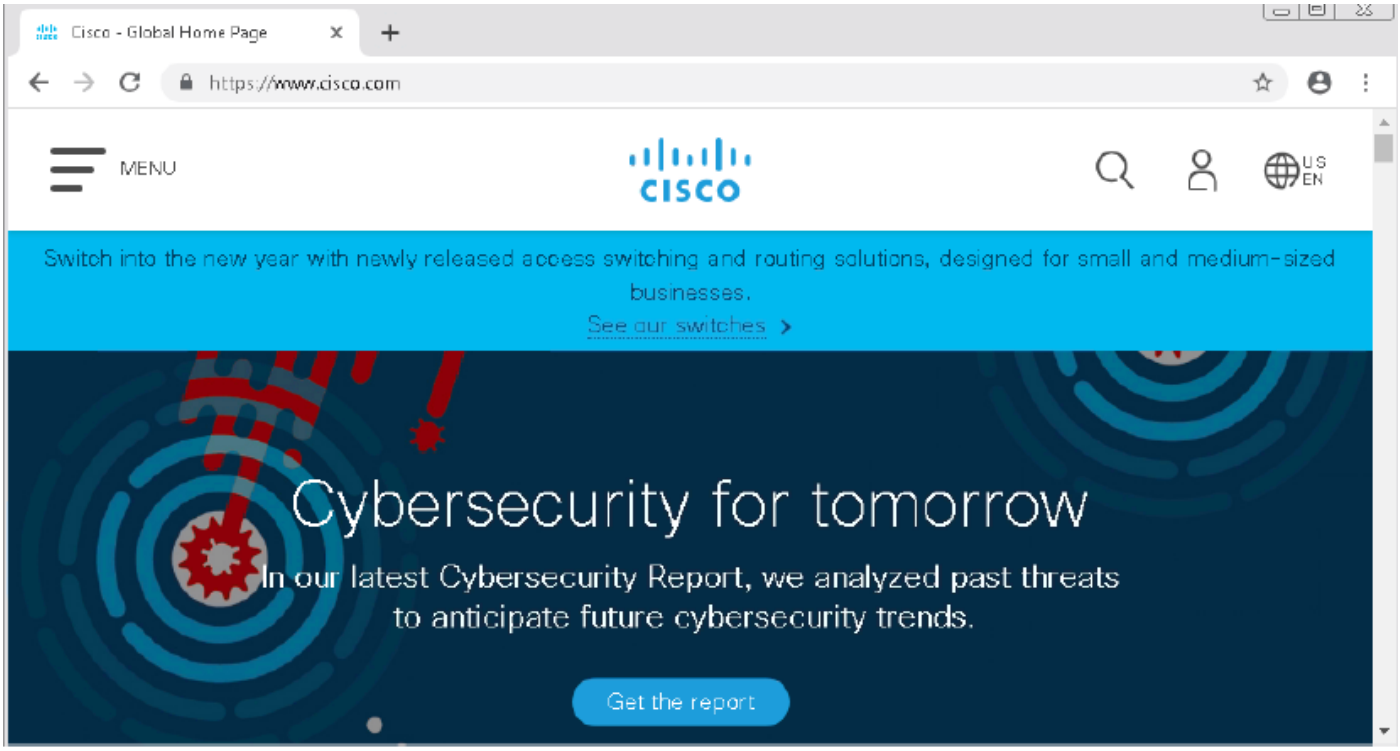
Verificación

Antes de que se aplique la política DNS

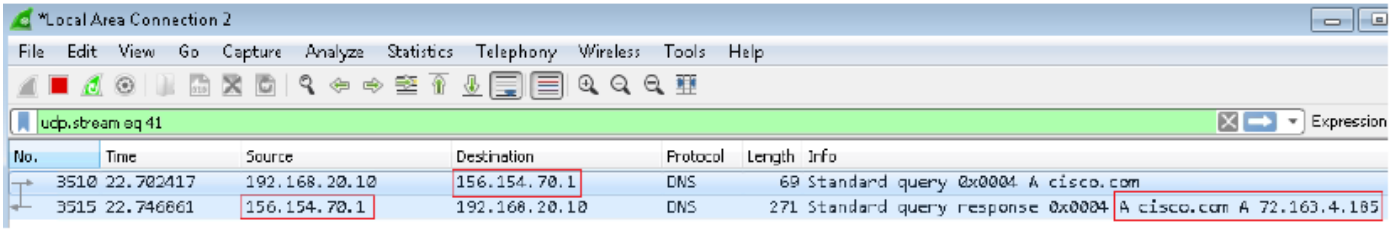
Paso 1. Compruebe la información del servidor DNS y de la dirección IP en el equipo host como se ve en la imagen:

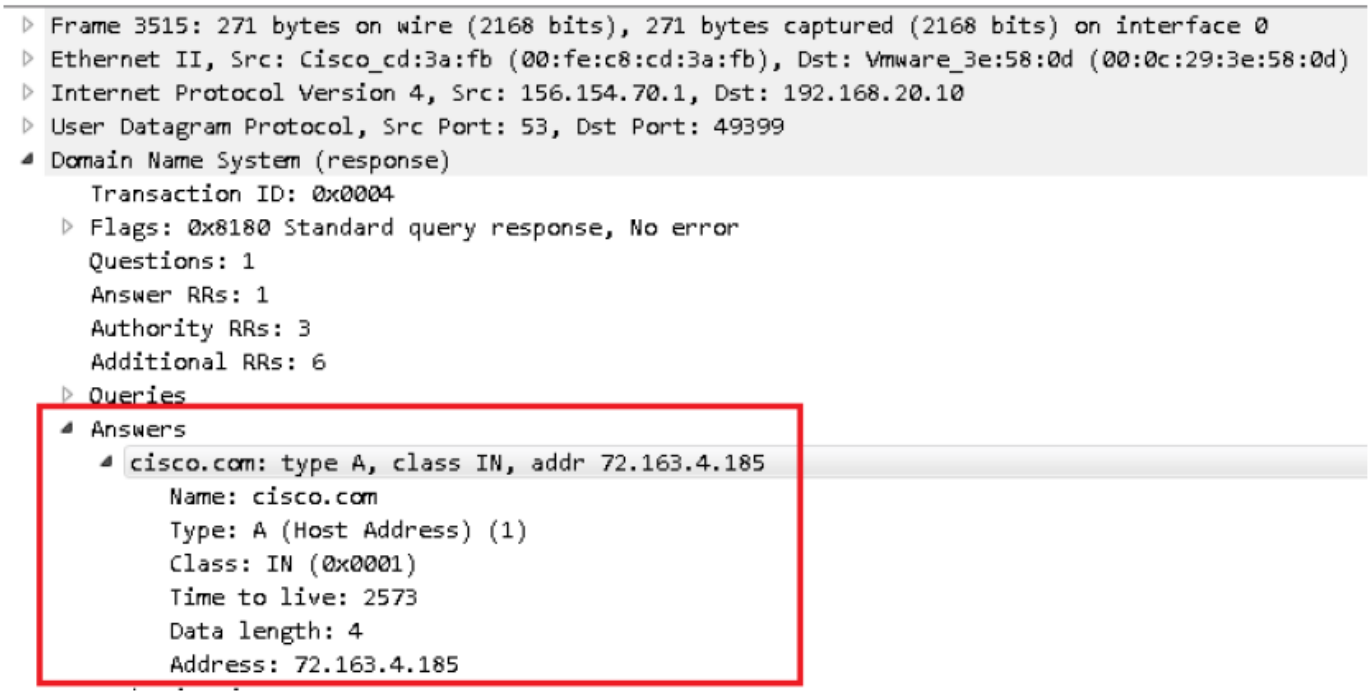


Paso 2. Confirme que puede navegar a cisco.com como se ve en la imagen:



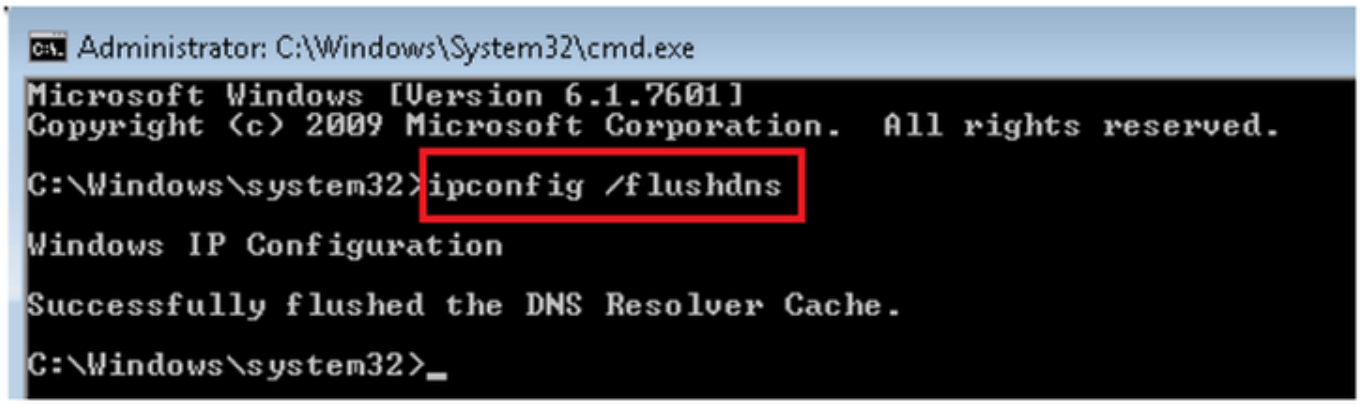
Paso 3. Confirme con capturas de paquetes que el DNS se resuelve correctamente:



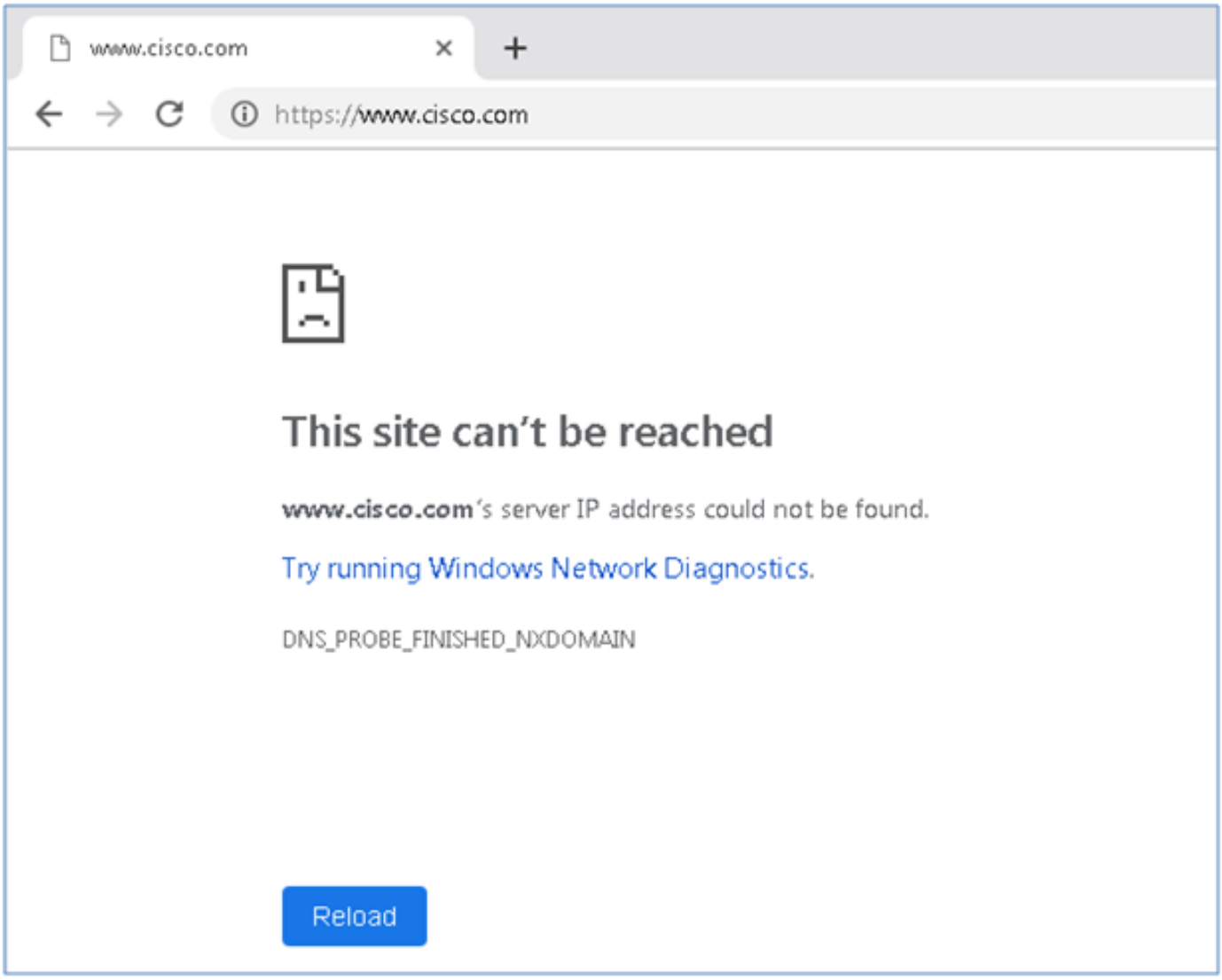


Después de aplicar la política DNS

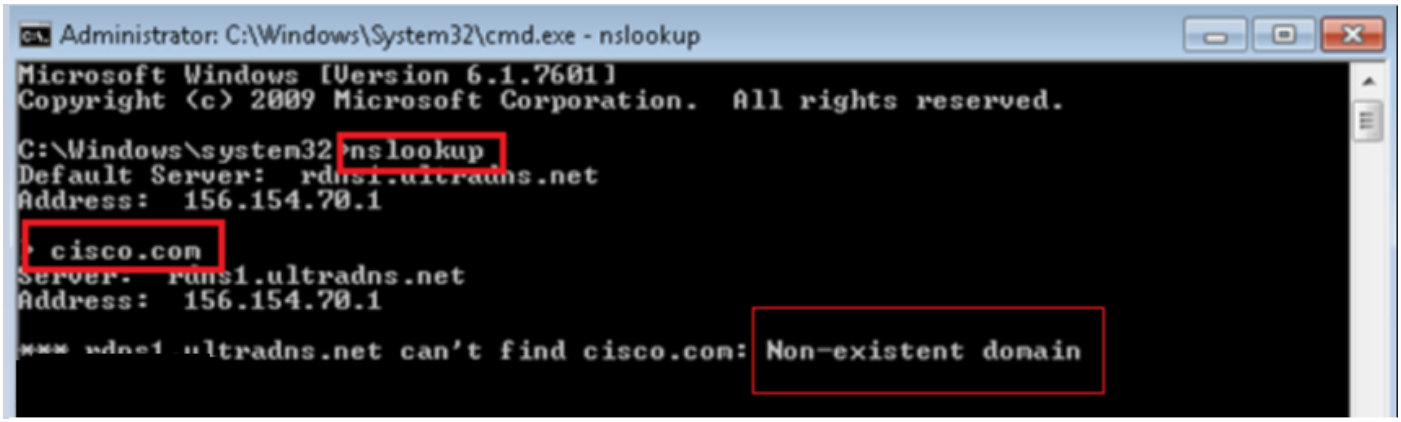
Paso 1. Borre la memoria caché DNS en su host con el comando **ipconfig /flushdns.**



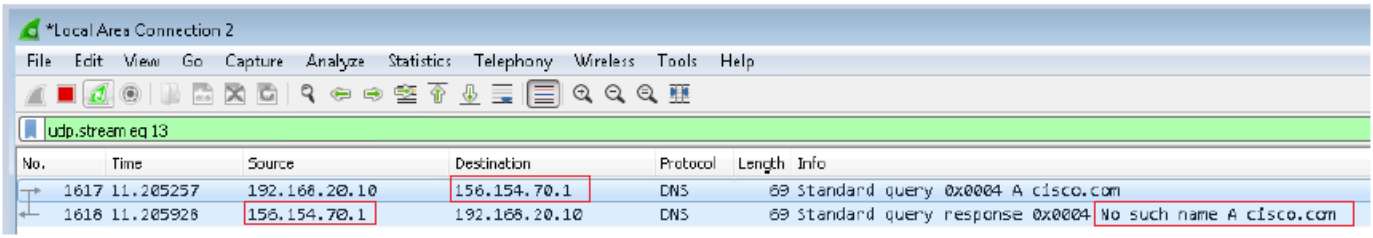
Paso 2. Navegue hasta el dominio en cuestión con un navegador web. Debe ser inalcanzable:

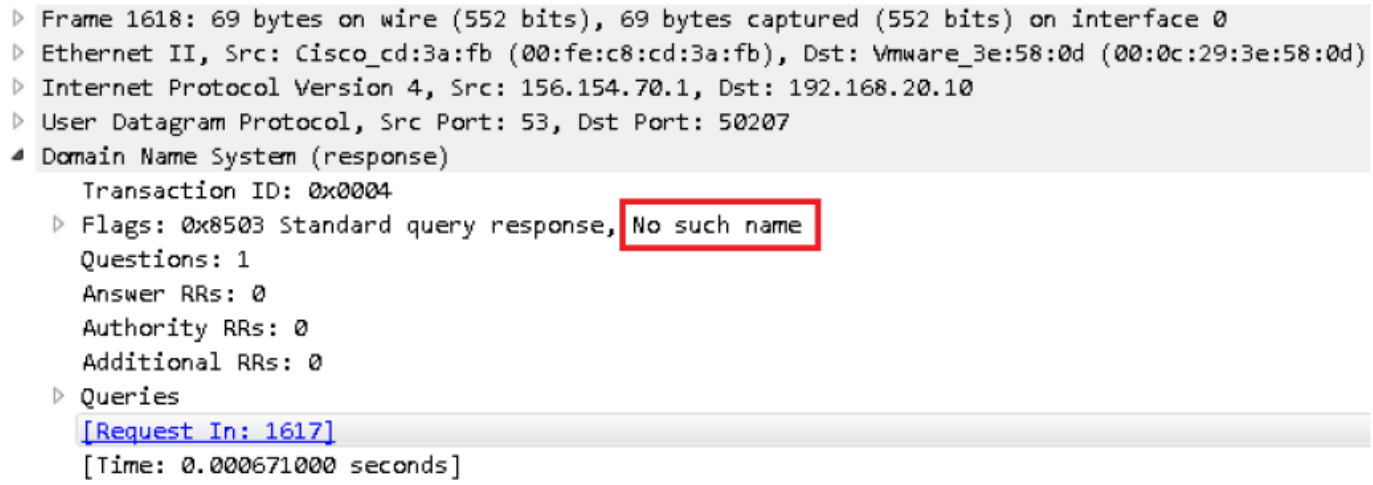


Paso 3. Intente ejecutar **nslookup** en el dominio cisco.com. La resolución del nombre falla.

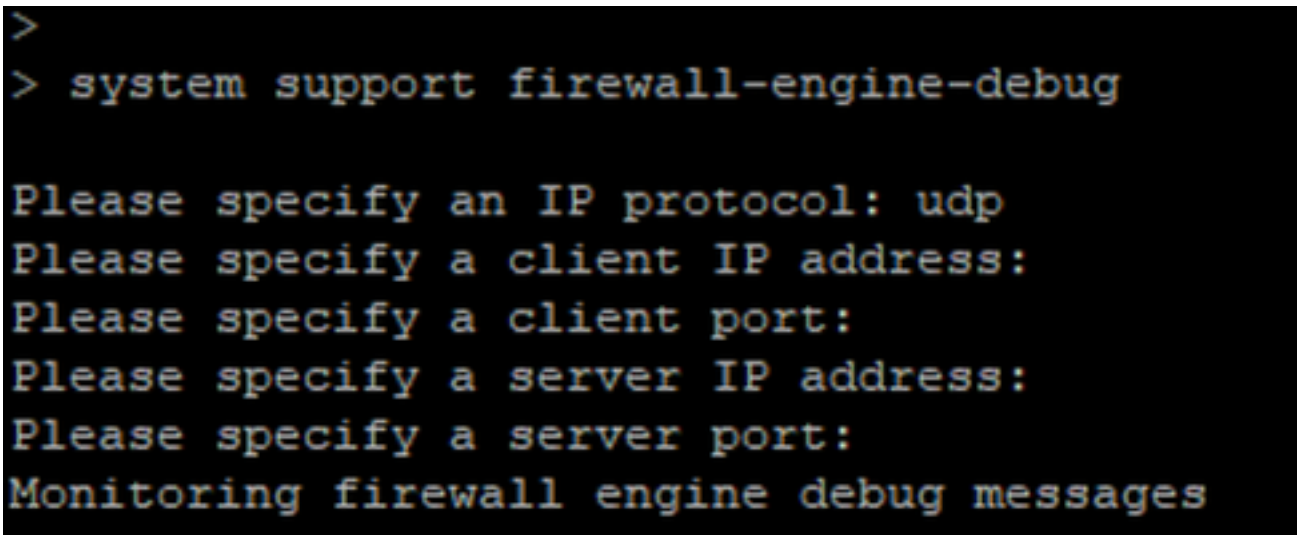


Paso 4. Las capturas de paquetes muestran una respuesta del FTD, en lugar del servidor DNS.





Paso 5. Ejecutar depuraciones en FTD CLI: system support firewall-engine-debug y especifique el protocolo UDP.



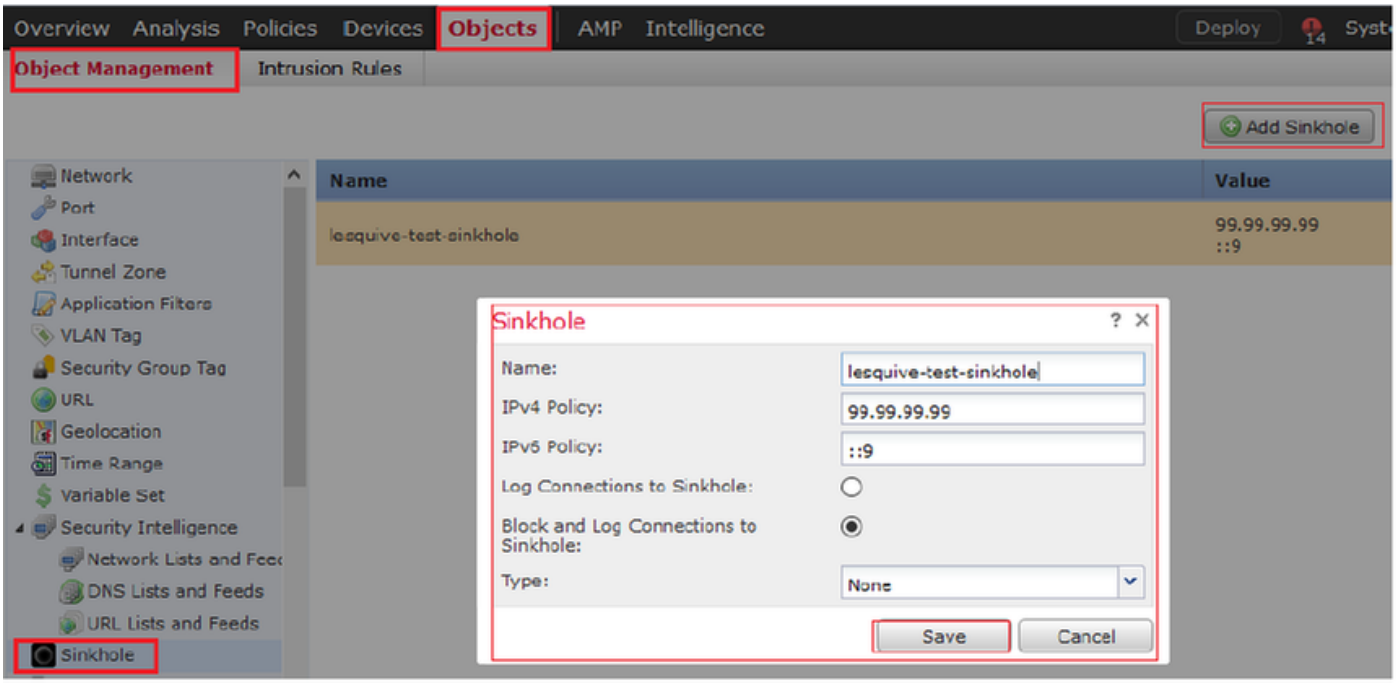
*Depuraciones cuando se compara cisco.com:

```
> 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
```

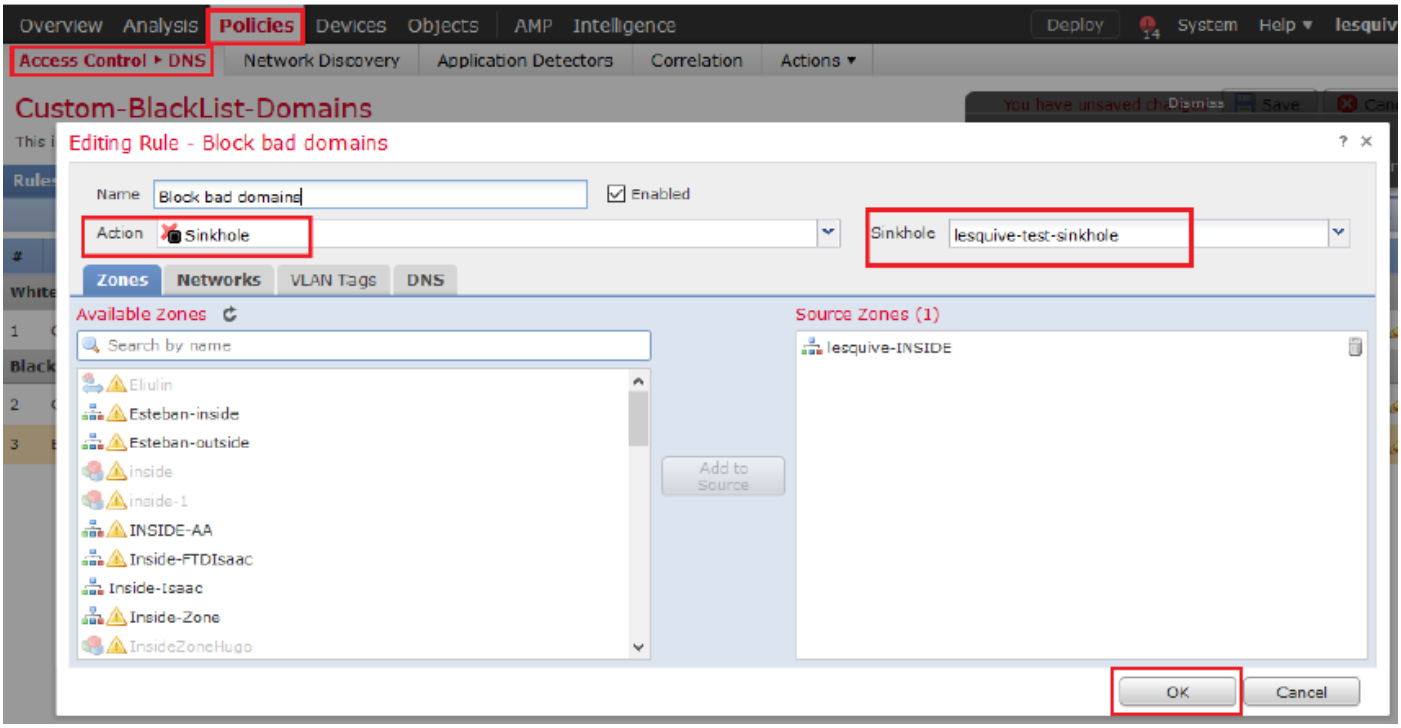
Configuración de sinkhole opcional

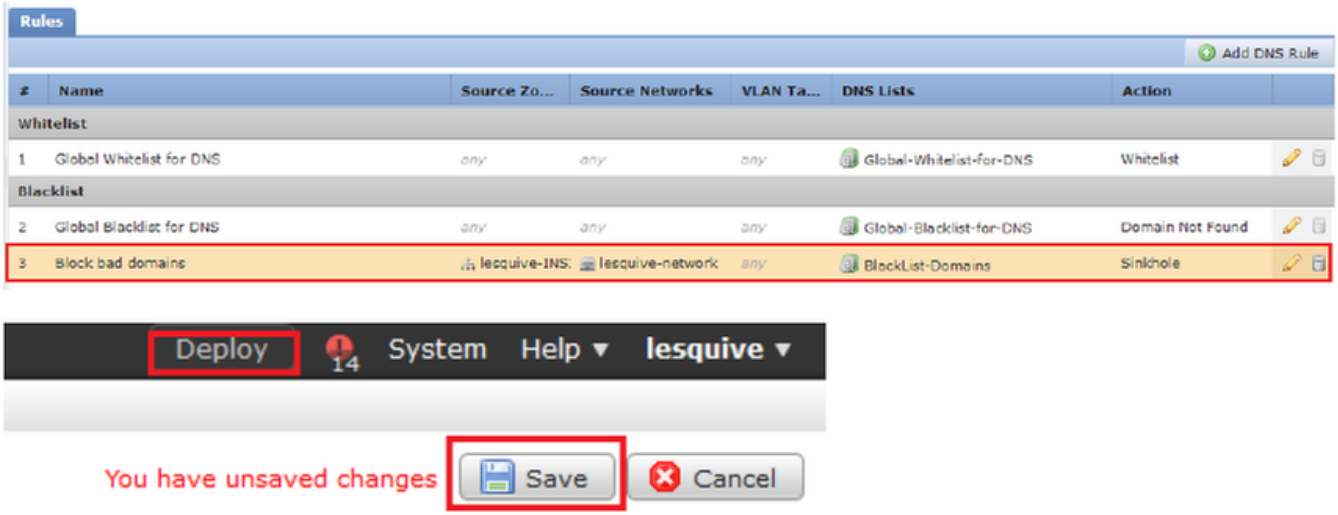
Un sinkhole DNS es un servidor DNS que proporciona información falsa. En lugar de devolver una respuesta DNS de "No existe tal nombre" a las consultas DNS en dominios que está bloqueando, devuelve una dirección IP falsa.

Paso 1. Vaya a Objects >> Object Management >> Sinkhole >> Add Sinkhole y cree la información de dirección IP falsa.

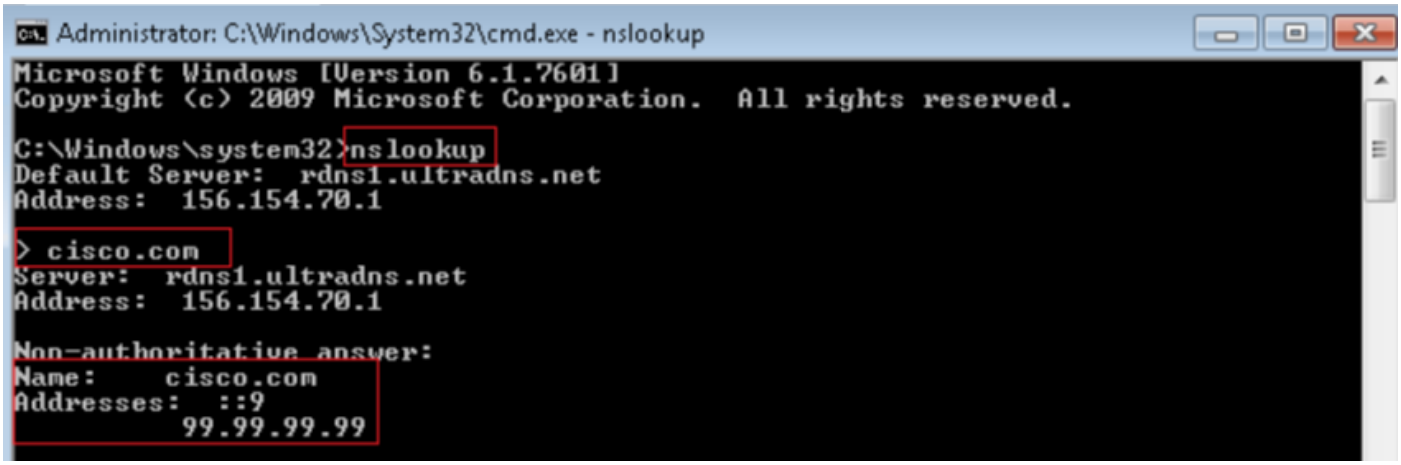


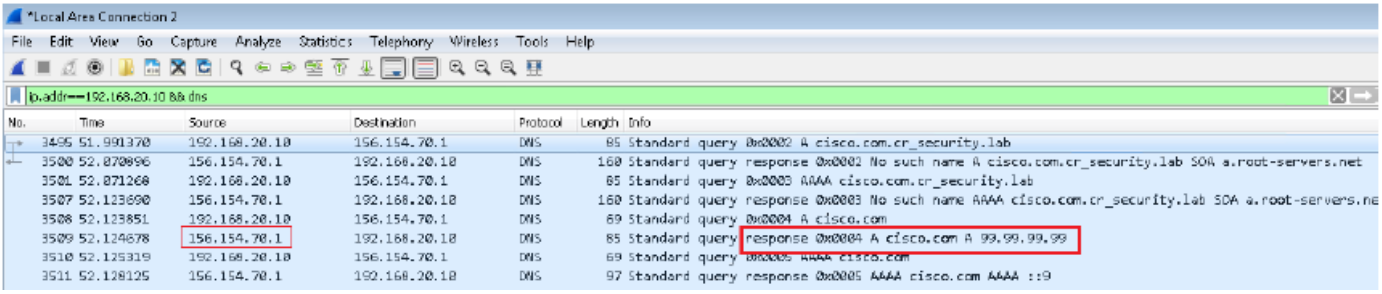
Paso 2. Aplique el sinkhole a su política DNS e implemente cambios en FTD.





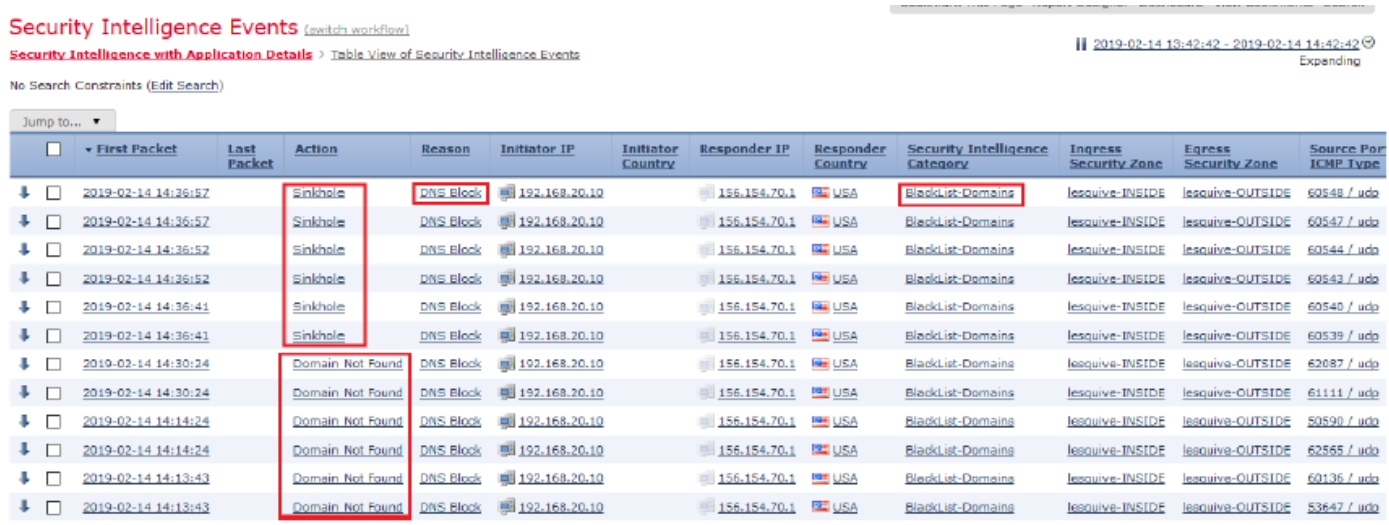
Verifique que Sinkhole funcione





Troubleshoot

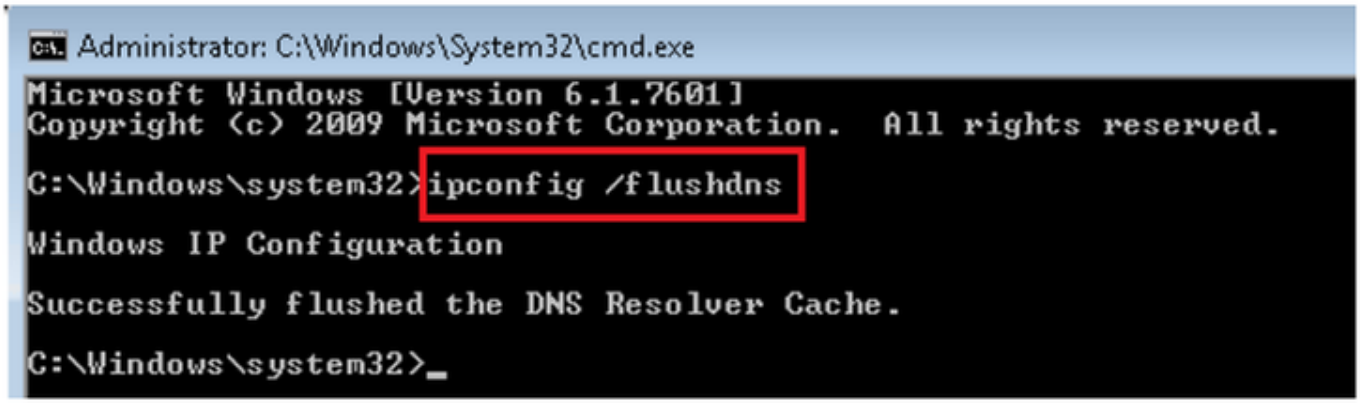
Navegue hasta Análisis >> Conexiones >> Eventos de inteligencia de seguridad para realizar un seguimiento de todos los eventos que se activan por SI siempre que haya habilitado el inicio de sesión en la política DNS:



También puede utilizar el comando **system support firewall-engine-debug** en el FTD administrado por el 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
```

Las capturas de paquetes pueden resultar útiles para confirmar que las solicitudes DNS llegan al servidor FTD. No olvide borrar la memoria caché de su host local cuando realice la prueba.


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>