

Bloqueo de DNS con inteligencia de seguridad mediante Firepower Management Center

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configurar](#)

[Configure una lista DNS personalizada con los dominios que queremos bloquear y cargue la lista en FMC](#)

[Agregue una nueva política DNS con la acción 'configurada en 'dominio no encontrado'](#)

[Asignar la política DNS a la política de control de acceso](#)

[Verificación](#)

[Antes de que se aplique la política DNS](#)

[Después de aplicar la política DNS](#)

[Configuración de sinkhole opcional](#)

[Verifique que Sinkhole funcione](#)

[Troubleshoot](#)

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.

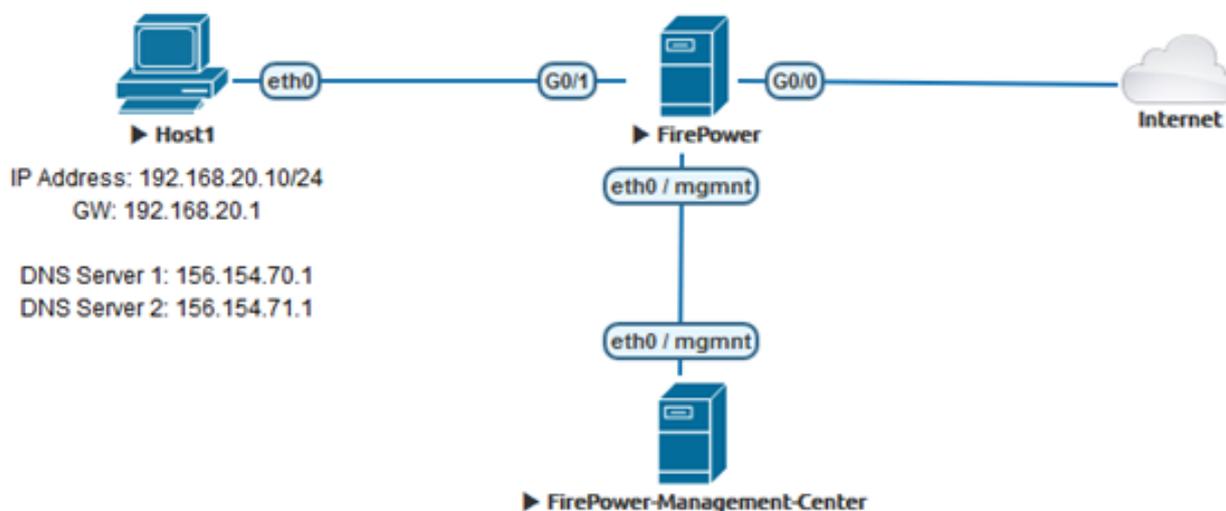
El ejemplo utilizado bloquea el dominio 1:

- 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.

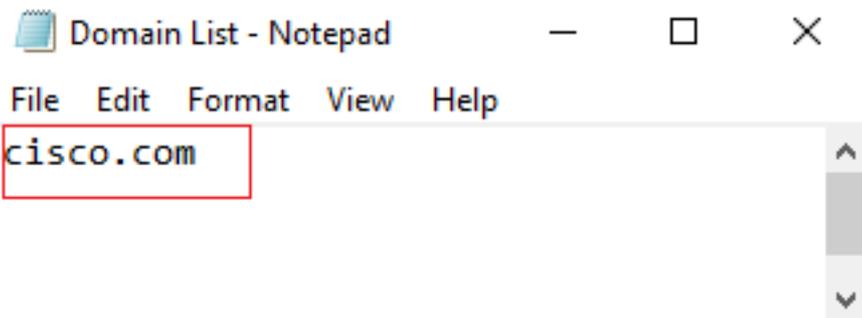
Diagrama de la red



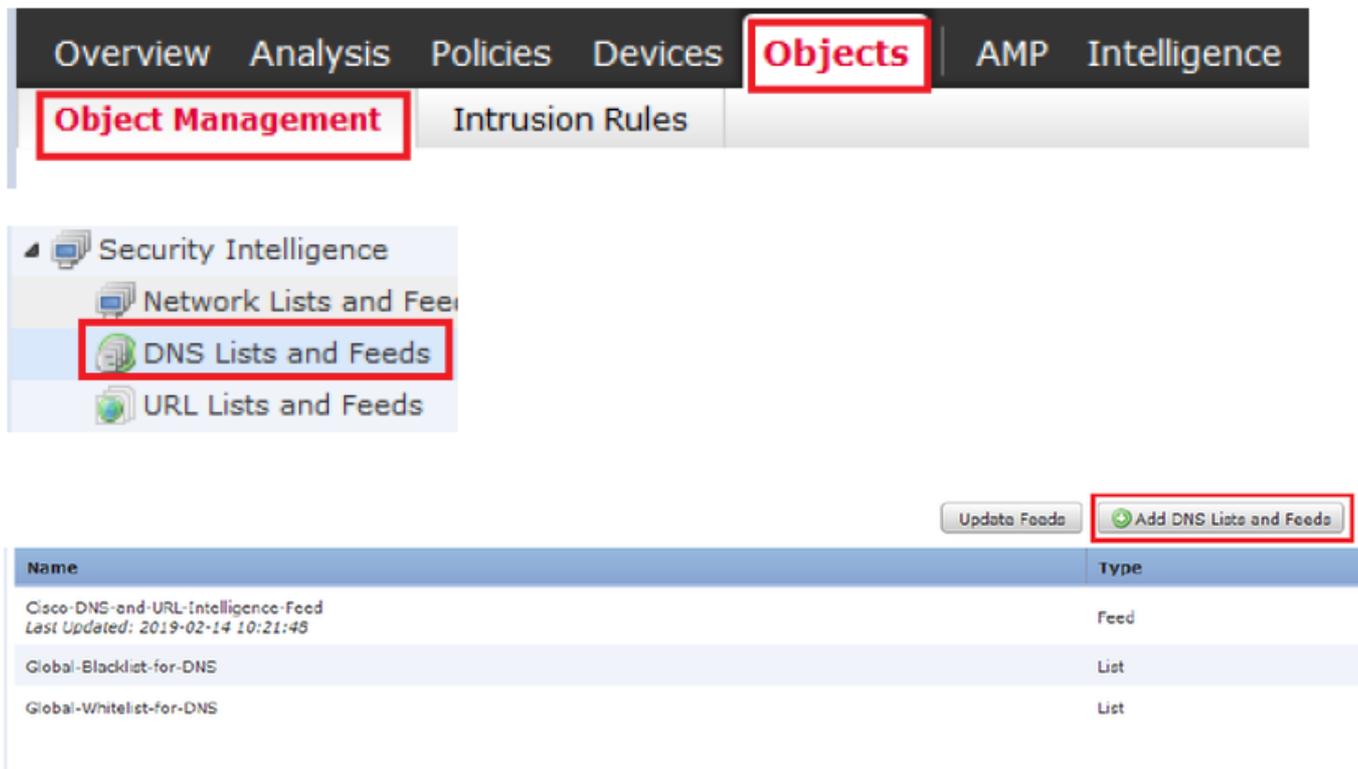
Configurar

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:

Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

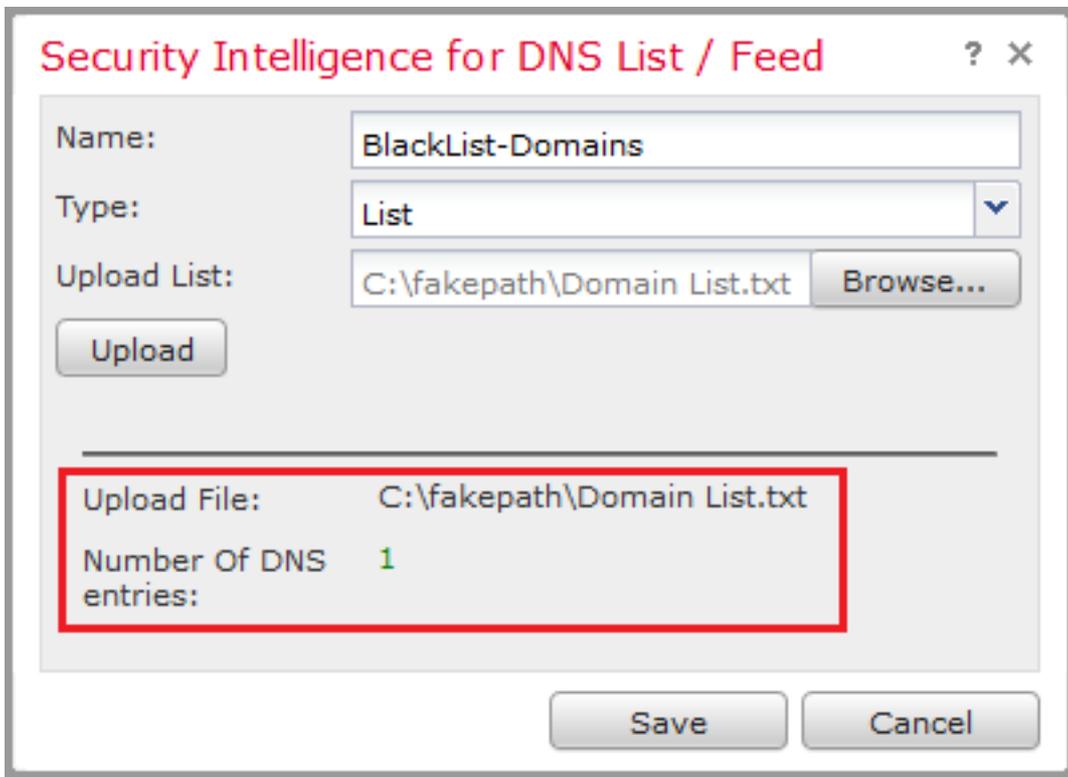
Security Intelligence for DNS List / Feed

Name:

Type:

Upload List:

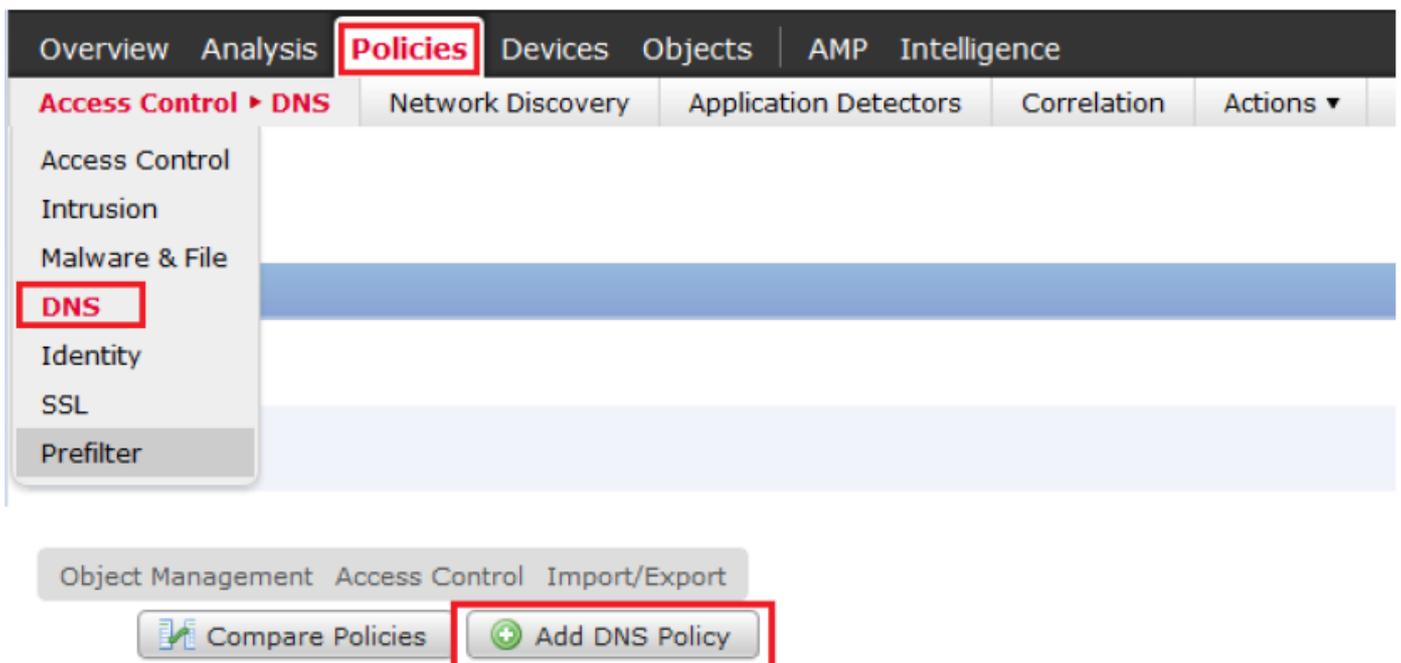
*Observe que cuando carga el archivo .txt, el número de entradas DNS debe leer todos los dominios. En este ejemplo, un total de 1:

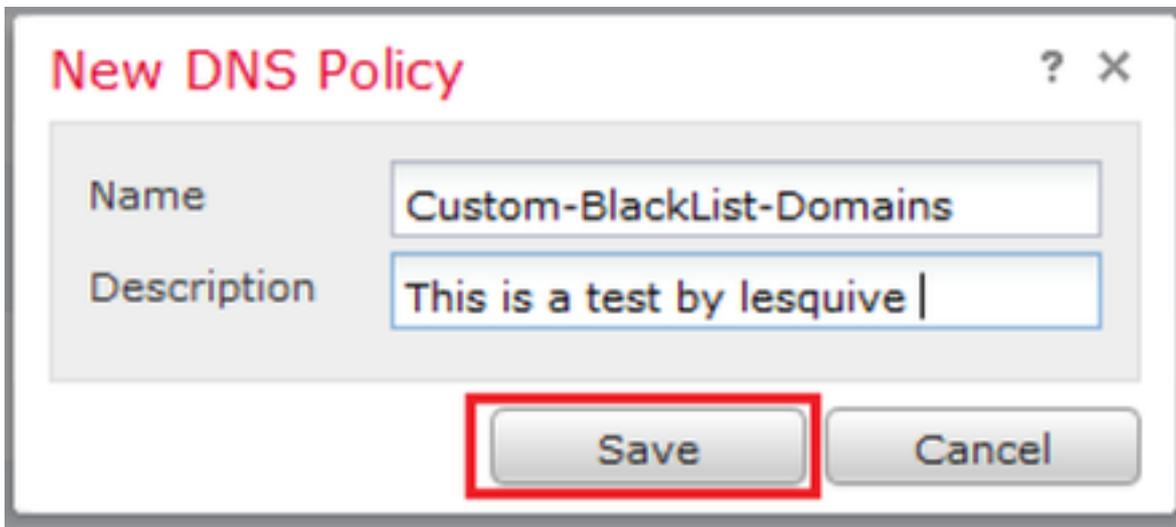


Agregue una nueva política DNS con la acción 'configurada en 'dominio no encontrado'

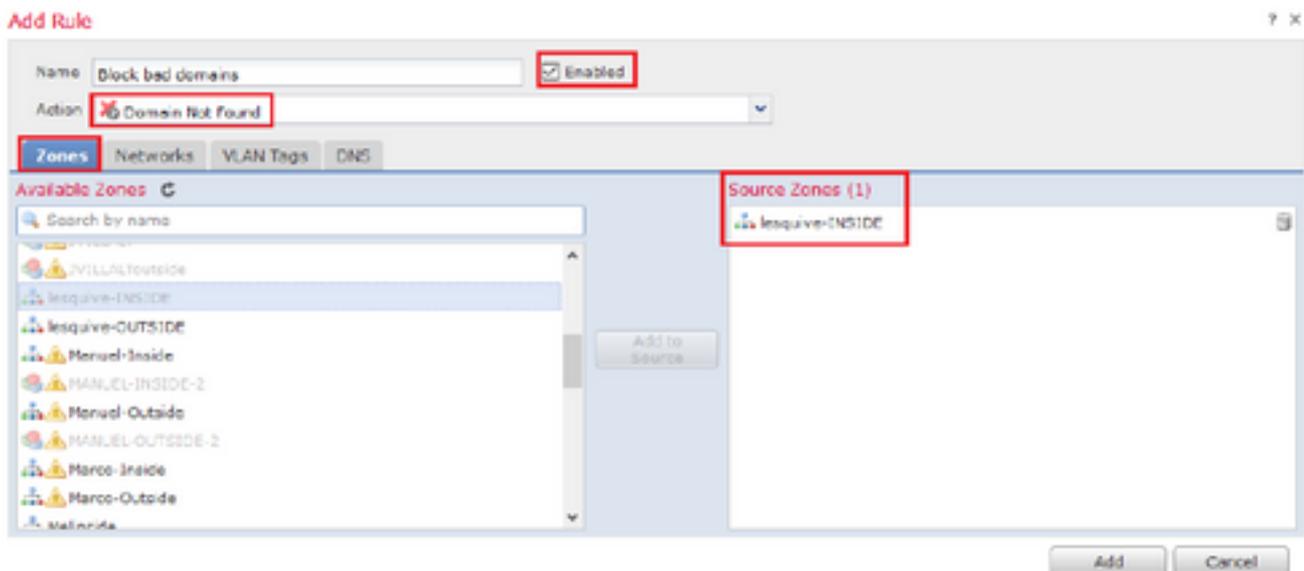
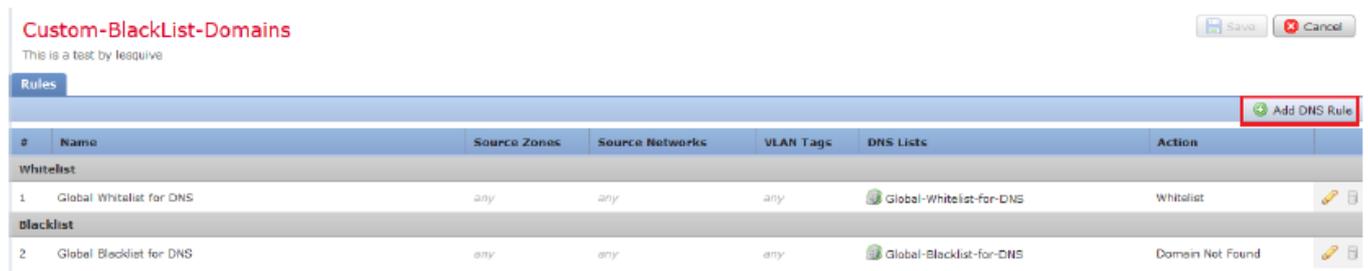
*Asegúrese de agregar una zona de origen, una red de origen y una lista DNS.

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

? 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

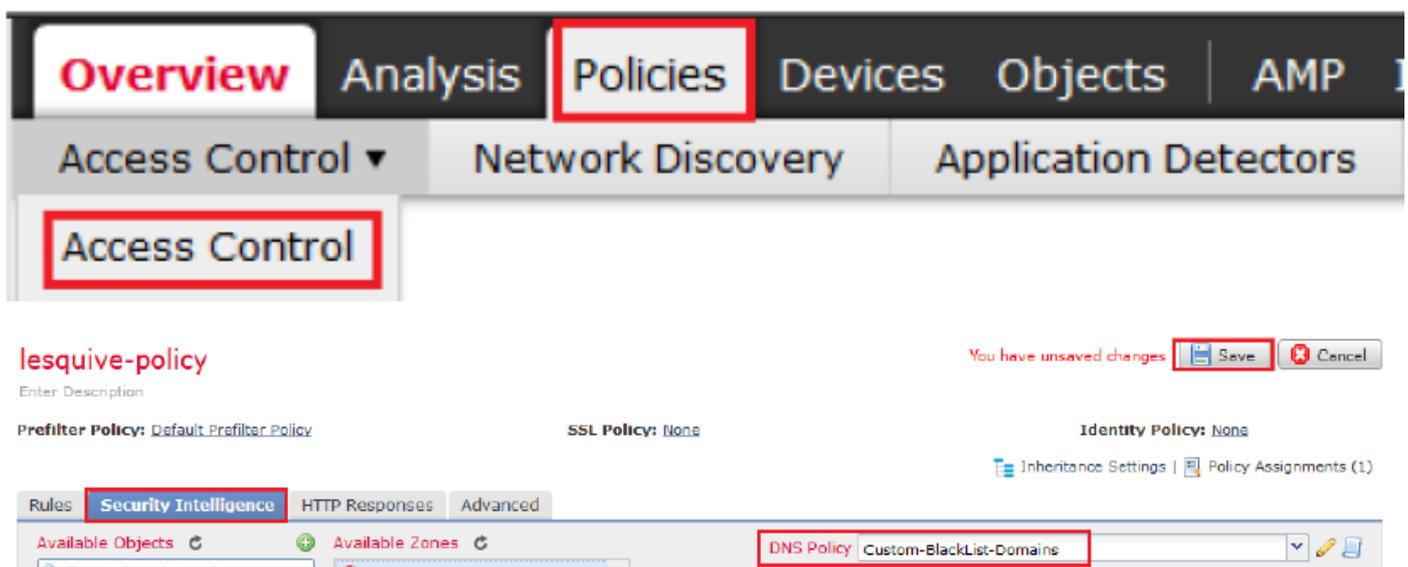
Rules							Add DNS Rule
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action	
Whitelist							
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	 
Blacklist							
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	 
3	Block bad domains	lesquive-INS	lesquive-network	any	BlackList-Domains	Sinkhole	 

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.



The screenshot shows the 'Policies' tab in the management console. Under 'Access Control', the 'lesquive-policy' is selected. The 'Rules' section is set to 'Security Intelligence'. In the 'Available Objects' list, the 'DNS Policy' is selected, and the specific policy 'Custom-BlackList-Domains' is chosen from the dropdown menu. A 'Save' button is visible in the top right corner, indicating unsaved changes.

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:

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

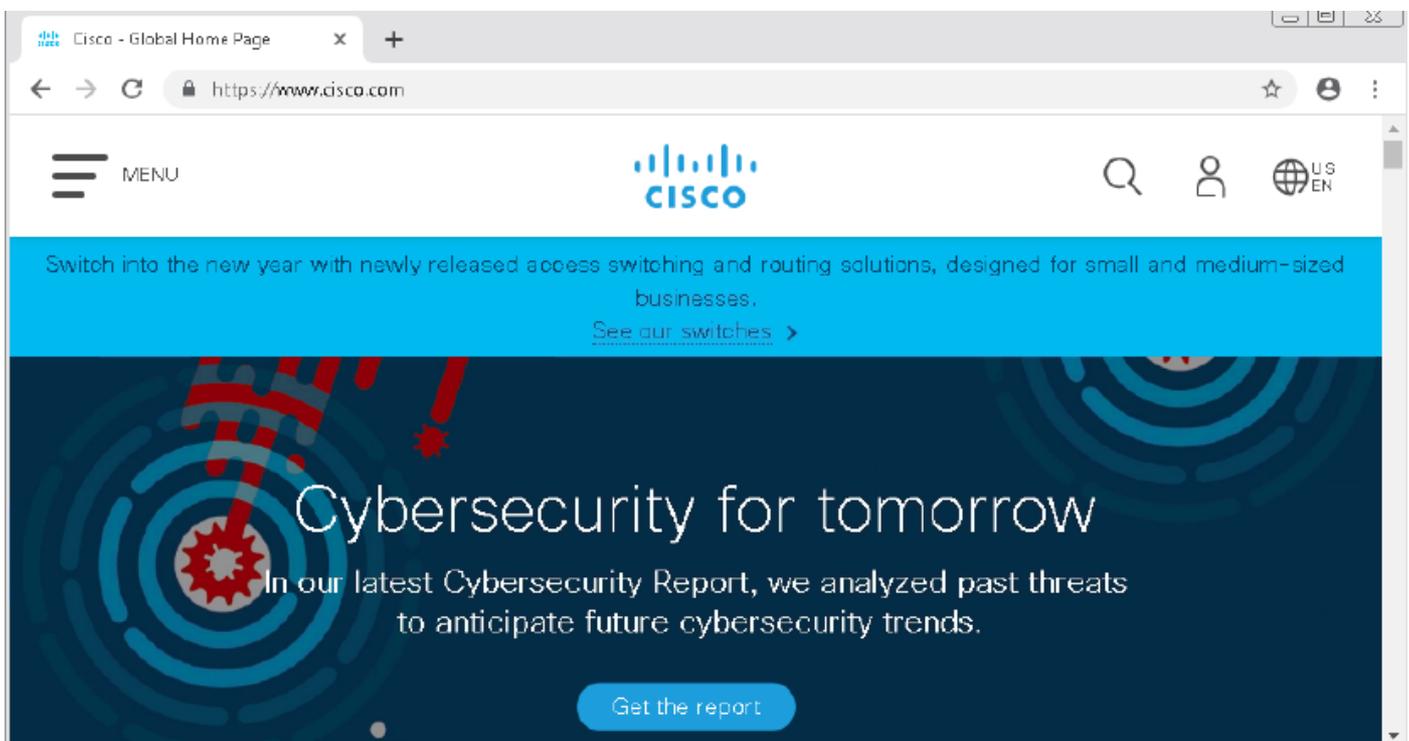
Ethernet adapter Local Area Connection 2:

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
```

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:

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets. Packet 3515 is a DNS standard query response from 156.154.70.1 to 192.168.20.10, containing an answer for cisco.com with IP address 72.163.4.185. The bottom pane shows the detailed view of this packet, highlighting the 'Answers' section which lists the record for cisco.com: type A, class IN, address 72.163.4.185.

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

```

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
  
```

Después de aplicar la política DNS

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

```

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

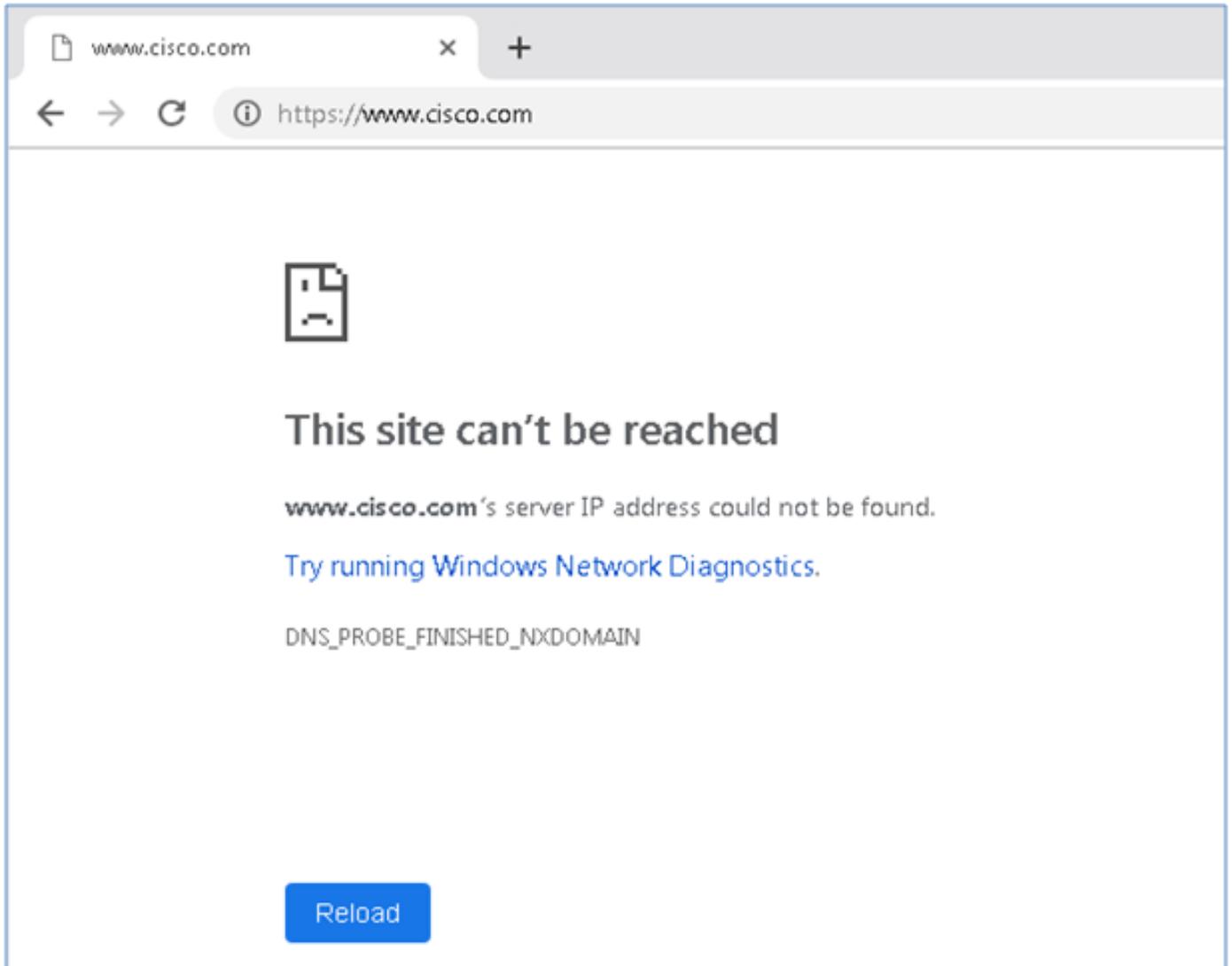
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
  
```

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.

```
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: rdnst1.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdnst1.ultradns.net
Address: 156.154.70.1

*** rdnst1.ultradns.net can't find cisco.com: Non-existent domain
```

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

The screenshot shows a network traffic capture in Wireshark. The packet list pane displays two 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 packet details pane for packet 1618 shows the following information:

- 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]

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

*Depuraciones cuando se compara cisco.com:

```
> system support firewall-engine-debug

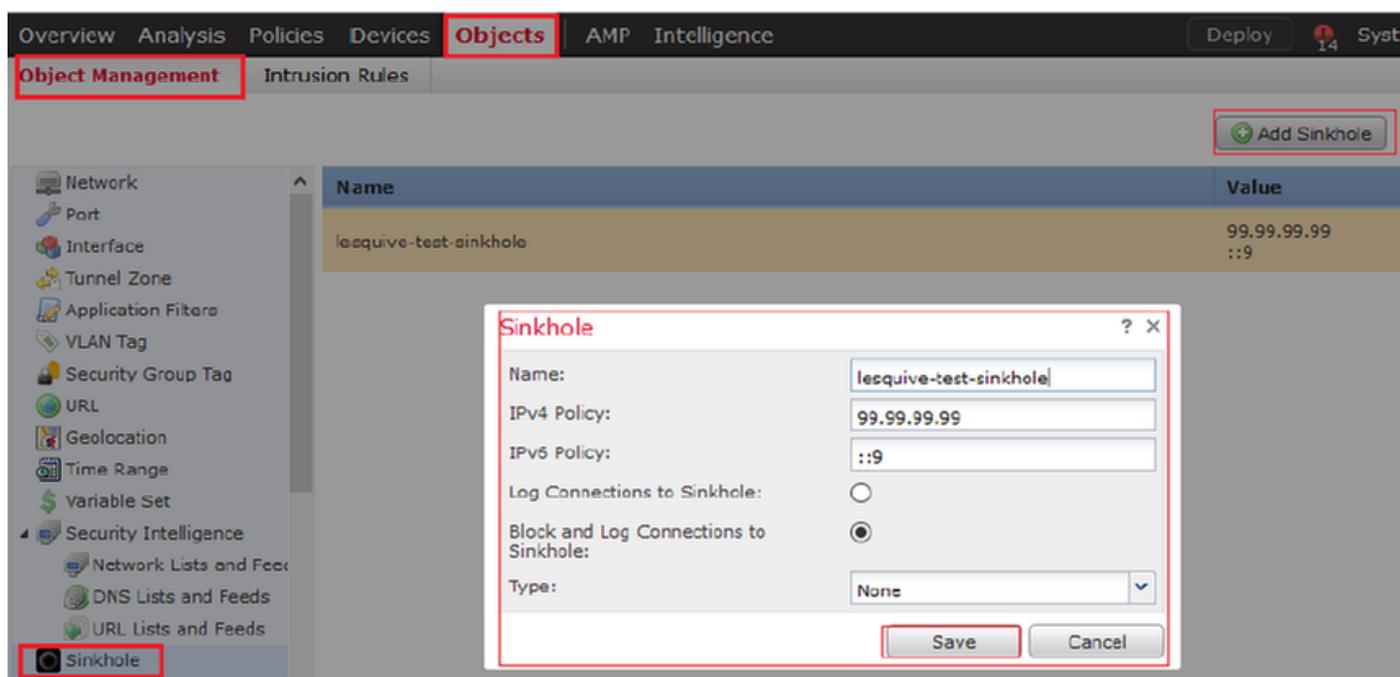
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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 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
```

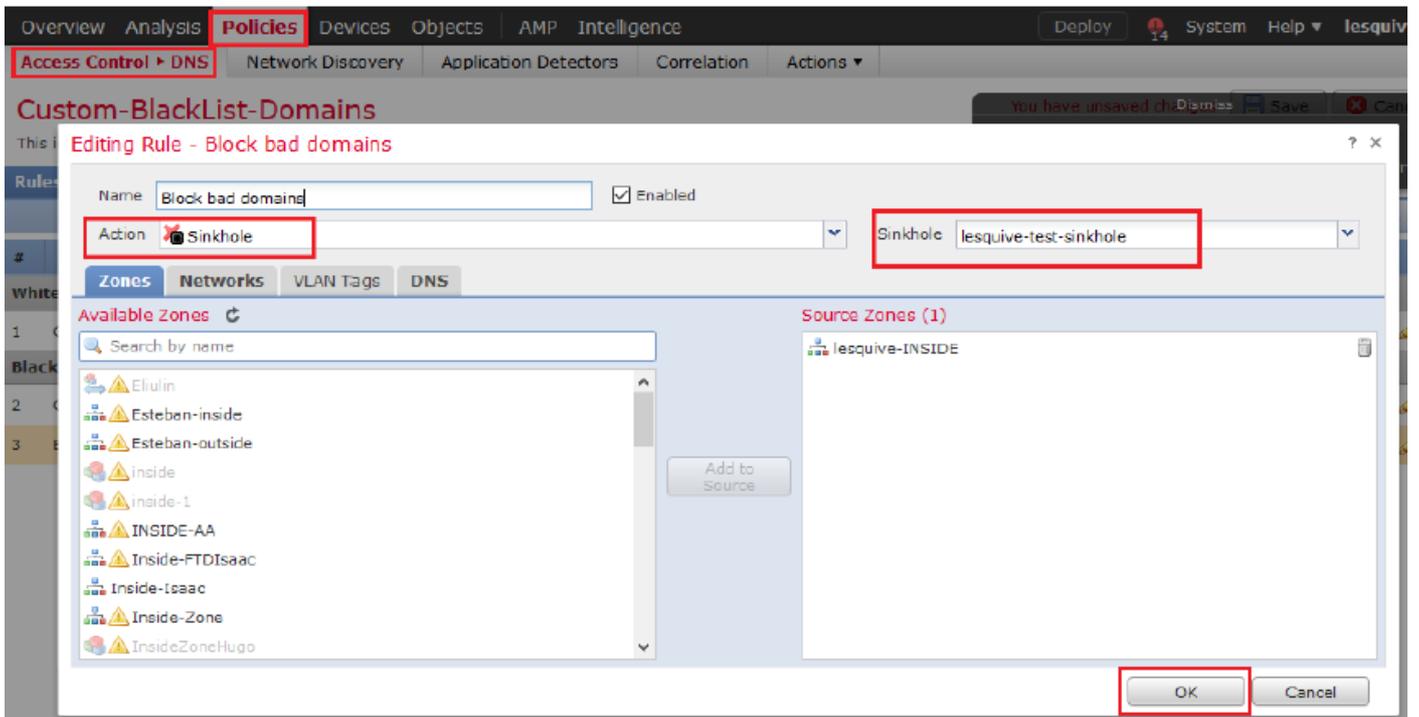
Configuración de sinkhole opcional

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.

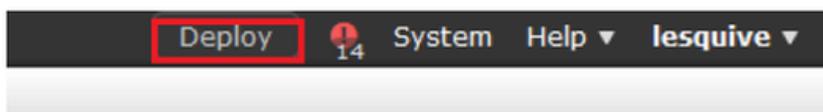
Paso 1. Vaya a Objects >> Object Management >> Sinkhole >> Add Sinkhole y cree la información de dirección IP falsa.



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



#	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 que Sinkhole funcione

```
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

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:

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 14:36:52		Sinkhole	DNS Block	192.168.20.10	USA	156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60548 / udp	
	2019-02-14 14:36:52		Sinkhole	DNS Block	192.168.20.10	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	53647 / udp	

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>_