

Blockieren von DNS mit Security Intelligence mit FirePOWER Management Center

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Konfigurieren einer benutzerdefinierten DNS-Liste mit den Domänen, die blockiert werden sollen, und Hochladen der Liste auf das FMC](#)

[Fügen Sie eine neue DNS-Richtlinie hinzu, und fügen Sie die Aktion "Action configured to 'domain not found" \(Aktion für "Domäne nicht gefunden" konfiguriert\) hinzu.](#)

[Zuweisen der DNS-Richtlinie zu Ihrer Zugriffskontrollrichtlinie](#)

[Überprüfen](#)

[Bevor die DNS-Richtlinie angewendet wird](#)

[Nachdem die DNS-Richtlinie angewendet wurde](#)

[Optionale Sinkloch-Konfiguration](#)

[Überprüfen Sie, ob das Sinkloch funktioniert.](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird die Vorgehensweise zum Hinzufügen einer DNS-Liste (Domain Name System) zu einer DNS-Richtlinie beschrieben, sodass Sie diese mit Security Intelligence (SI) anwenden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ASA55XX Threat Defense-Konfiguration
- Konfiguration des Cisco FirePOWER Management Center

Verwendete Komponenten

- Cisco ASA5506W-X Threat Defense (75) Version 6.2.3.4 (Build 42)
- Cisco FirePOWER Management Center für VMware Softwareversion: 6.2.3.4 (Build 42) Betriebssystem: Cisco Fire Linux OS 6.2.3 (Build13)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Mithilfe von Sicherheitsinformationen wird Datenverkehr von oder zu IP-Adressen, URLs oder Domännennamen blockiert, die eine bekannte schlechte Reputation aufweisen. In diesem Dokument liegt der Schwerpunkt auf der Blacklisting von Domännennamen.

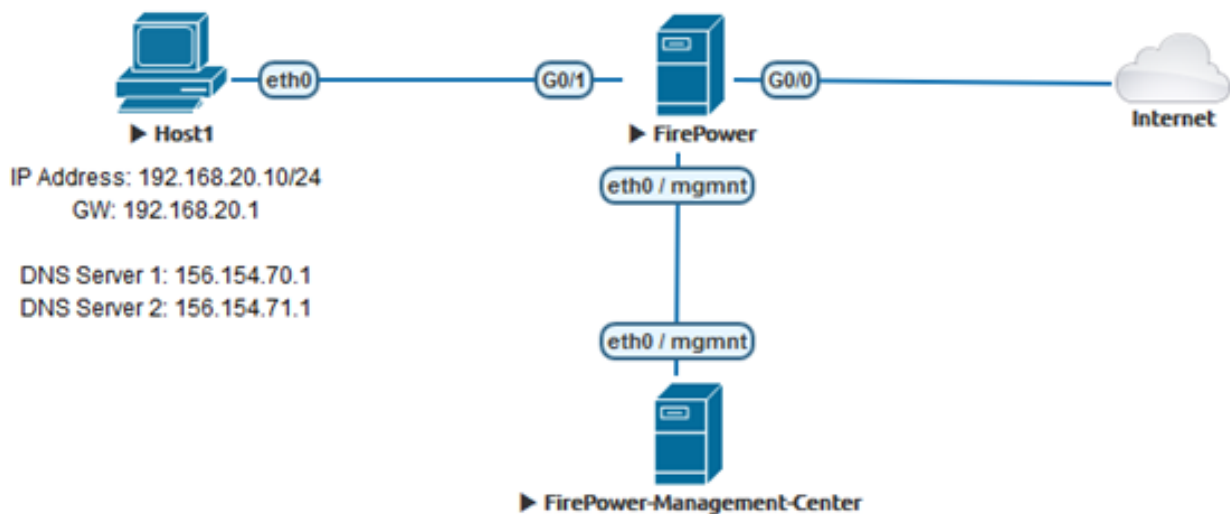
Im Beispiel wird die Domäne 1 blockiert:

- Cisco.com

Sie können die URL-Filterung verwenden, um einige dieser Sites zu blockieren. Das Problem besteht jedoch darin, dass die URL exakt der Übereinstimmung entsprechen muss. Auf der anderen Seite können DNS-Blacklisting mit SI sich auf Domänen wie "cisco.com" konzentrieren, ohne sich um Unterdomänen oder Änderungen der URL kümmern zu müssen.

Am Ende dieses Dokuments wird auch eine optionale Sinkhole-Konfiguration gezeigt.

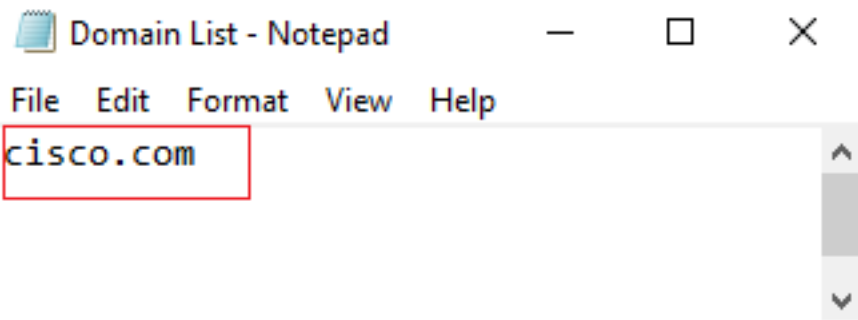
Netzwerkdiagramm



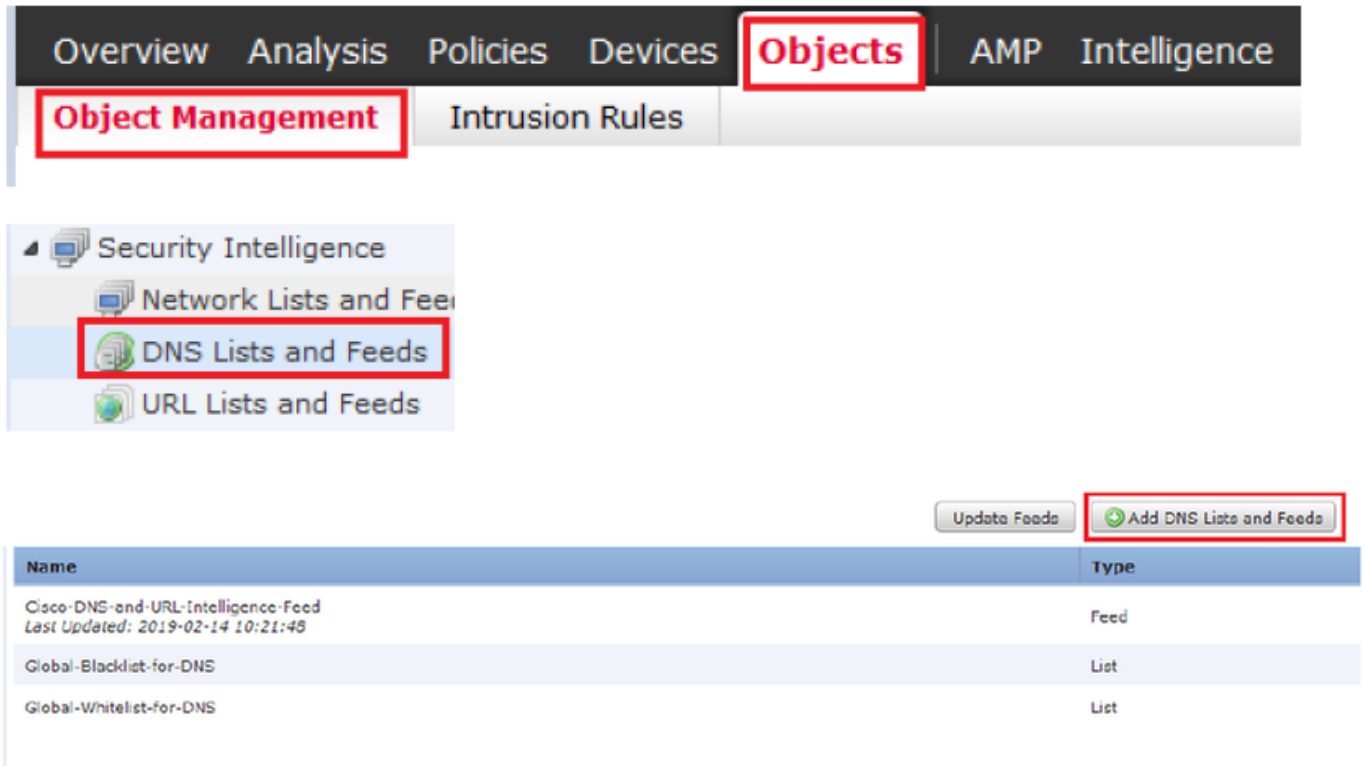
Konfigurieren

Konfigurieren einer benutzerdefinierten DNS-Liste mit den Domänen, die blockiert werden sollen, und Hochladen der Liste auf das FMC

Schritt 1: Erstellen Sie eine TXT-Datei mit den Domänen, die Sie blockieren möchten. Speichern Sie die TXT-Datei auf Ihrem Computer:



Schritt 2: Navigieren Sie in FMC zu Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds.



Schritt 3: Erstellen Sie eine Liste mit dem Namen "BlackList-Domains". Der Typ sollte eine Liste sein, und die TXT-Datei mit den betreffenden Domänen sollte hochgeladen werden, wie in den Bildern gezeigt:

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

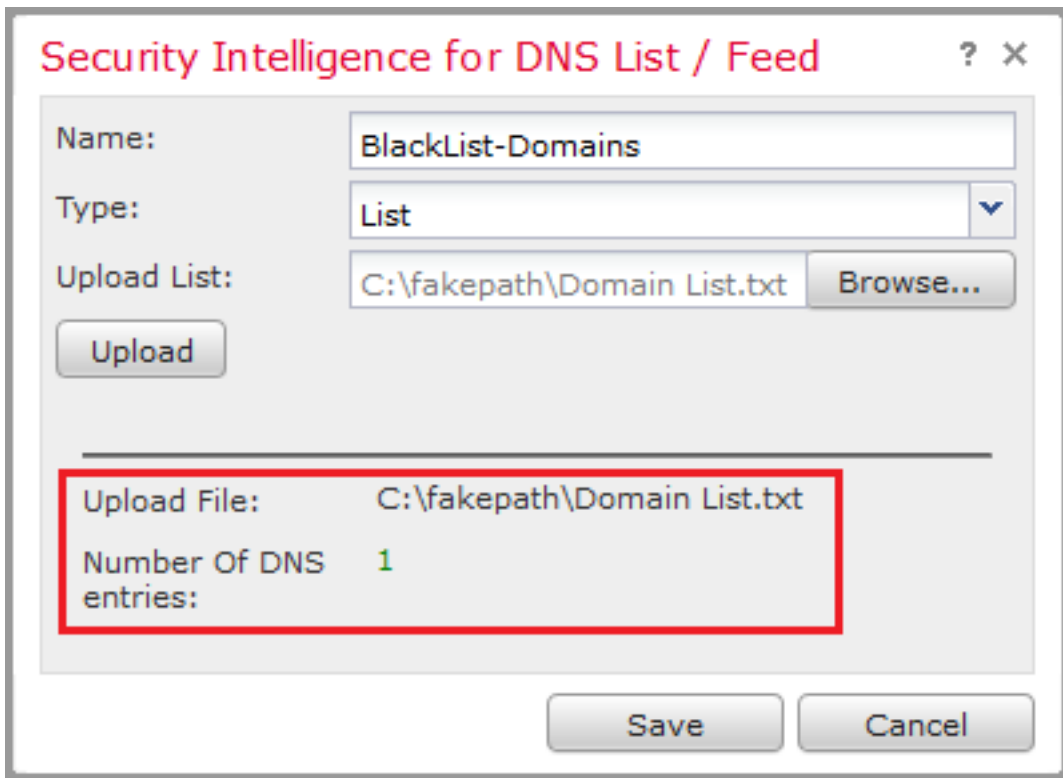
Type: List

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

Upload

Save Cancel

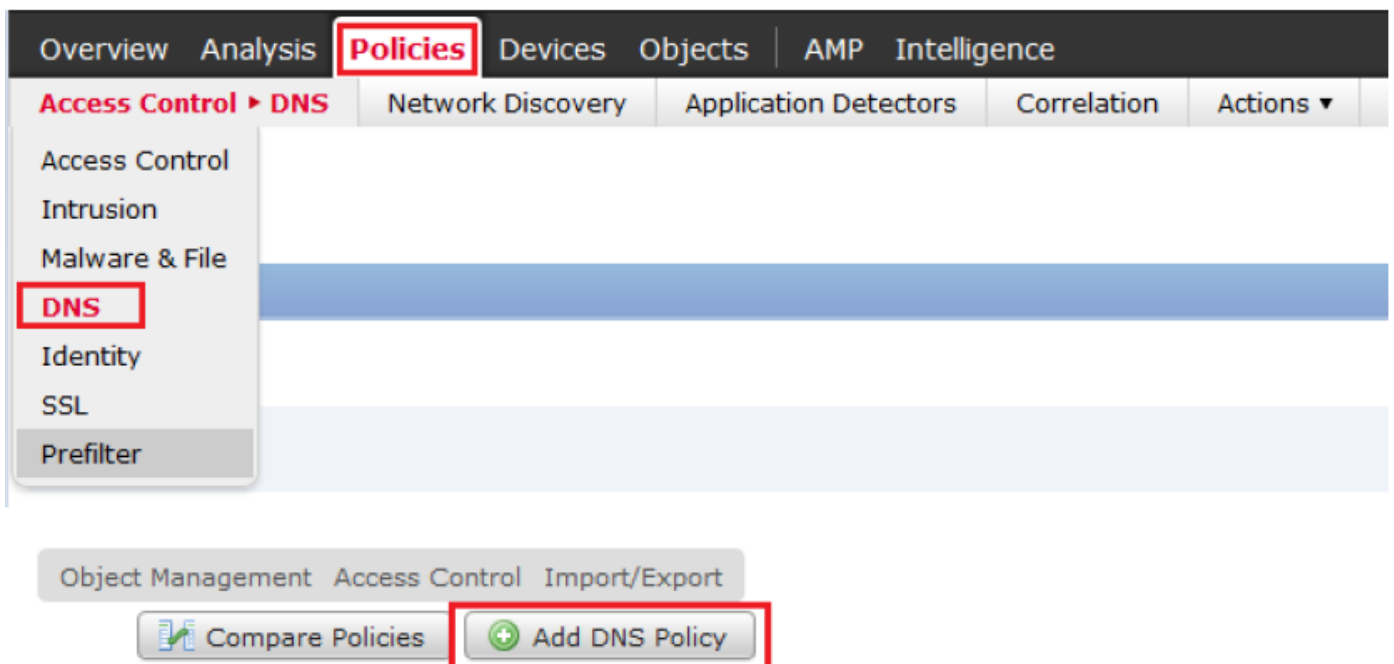
* Beachten Sie, dass beim Hochladen der TXT-Datei die Anzahl der DNS-Einträge alle Domänen lesen soll. In diesem Beispiel ergibt sich insgesamt 1:

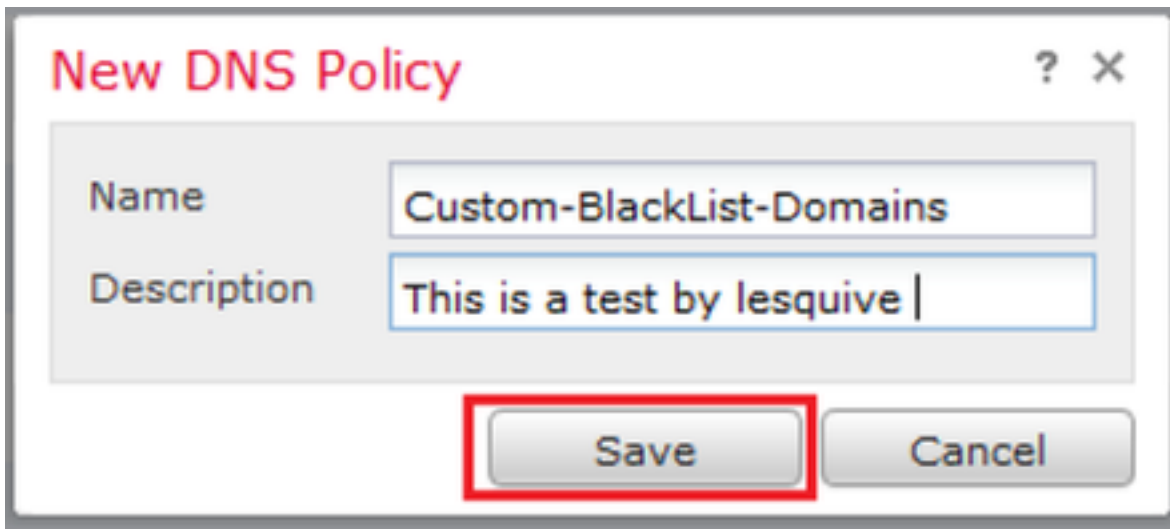


Fügen Sie eine neue DNS-Richtlinie hinzu, und fügen Sie die Aktion "Action configured to 'domain not found'" (Aktion für "Domäne nicht gefunden" konfiguriert) hinzu.

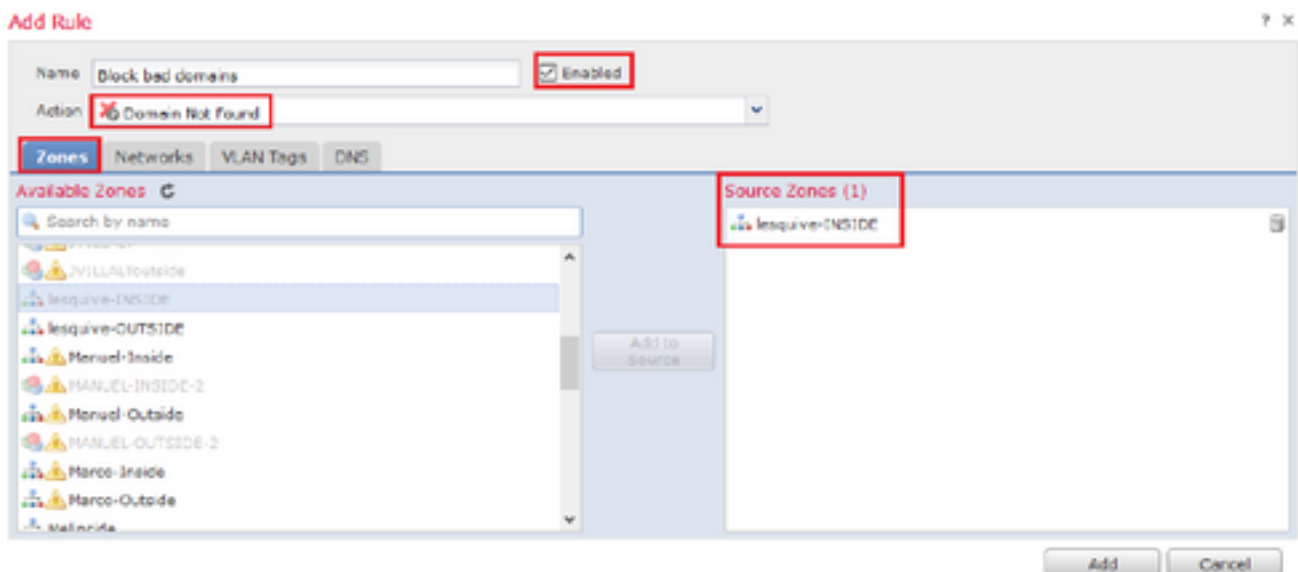
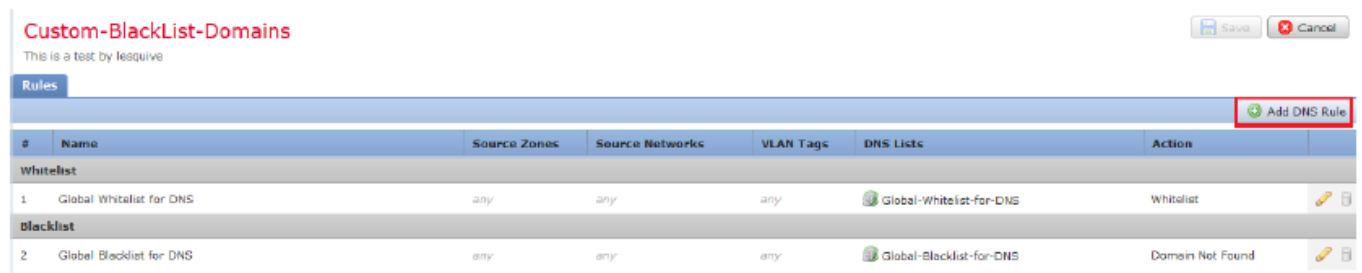
* Stellen Sie sicher, dass Sie eine Quellzone, ein Quellnetzwerk und eine DNS-Liste hinzufügen.

Schritt 1: Navigieren Sie zu Richtlinien >> Zugriffskontrolle >> DNS >> DNS-Richtlinie hinzufügen:





Schritt 2: Fügen Sie eine DNS-Regel hinzu, wie im Bild gezeigt:



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

#	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

Wichtige Informationen zur Regelreihenfolge:

- Die globale Whitelist ist immer der erste und hat Vorrang vor allen anderen Regeln.
- Die Descendant DNS Whitelists-Regel wird nur in Multi-Domain-Bereitstellungen und in Nicht-Leaf-Domänen angezeigt. Er ist immer zweitklassig und hat Vorrang vor allen anderen Regeln außer der globalen Whitelist.
- Der Whitelist-Abschnitt geht dem Blacklist-Abschnitt voraus. Whitelist-Regeln haben immer Vorrang vor anderen Regeln.
- Die globale Blacklist steht immer an erster Stelle im Blacklist-Abschnitt und hat Vorrang vor allen anderen Monitor- und Blacklist-Regeln.
- Die Descendant DNS Blacklists-Regel wird nur in Multi-Domain-Bereitstellungen und in Nicht-Leaf-Domänen angezeigt. Er ist immer auf Platz 2 im Blacklist-Abschnitt und hat Vorrang vor allen anderen Monitor- und Blacklist-Regeln außer der Global Blacklist.
- Der Blacklist-Abschnitt enthält Monitor- und Blacklist-Regeln.
- Wenn Sie zum ersten Mal eine DNS-Regel erstellen, wird die Systemposition zuletzt im Whitelist-Abschnitt angezeigt, wenn Sie eine Whitelist-Aktion zuweisen, oder zuletzt im Blacklist-Abschnitt, wenn Sie eine andere Aktion zuweisen.

Zuweisen der DNS-Richtlinie zu Ihrer Zugriffskontrollrichtlinie

Gehen Sie zu Policies > Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy, und fügen Sie die von Ihnen erstellte Policy hinzu.

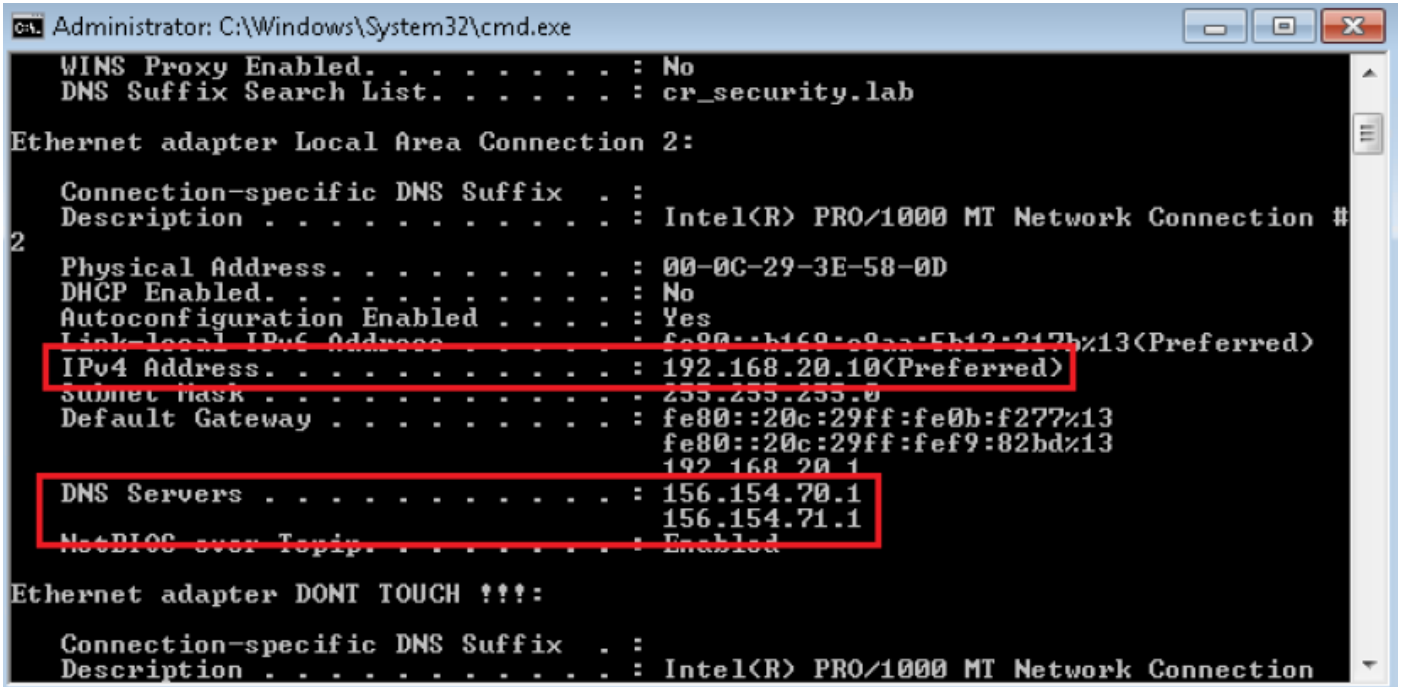
The screenshot shows the 'Policies' tab in the management console. Under 'Access Control', the 'lesquive-policy' is selected. The 'Security Intelligence' rule is active, and the 'DNS Policy' dropdown menu is set to 'Custom-BlackList-Domains'. A 'Save' button is highlighted, indicating that changes have been made.

Stellen Sie sicher, dass Sie alle Änderungen nach Abschluss bereitstellen.

Überprüfen

Bevor die DNS-Richtlinie angewendet wird

Schritt 1: Überprüfen Sie die DNS-Server- und IP-Adressinformationen auf Ihrem Hostcomputer, wie im Abbild dargestellt:



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

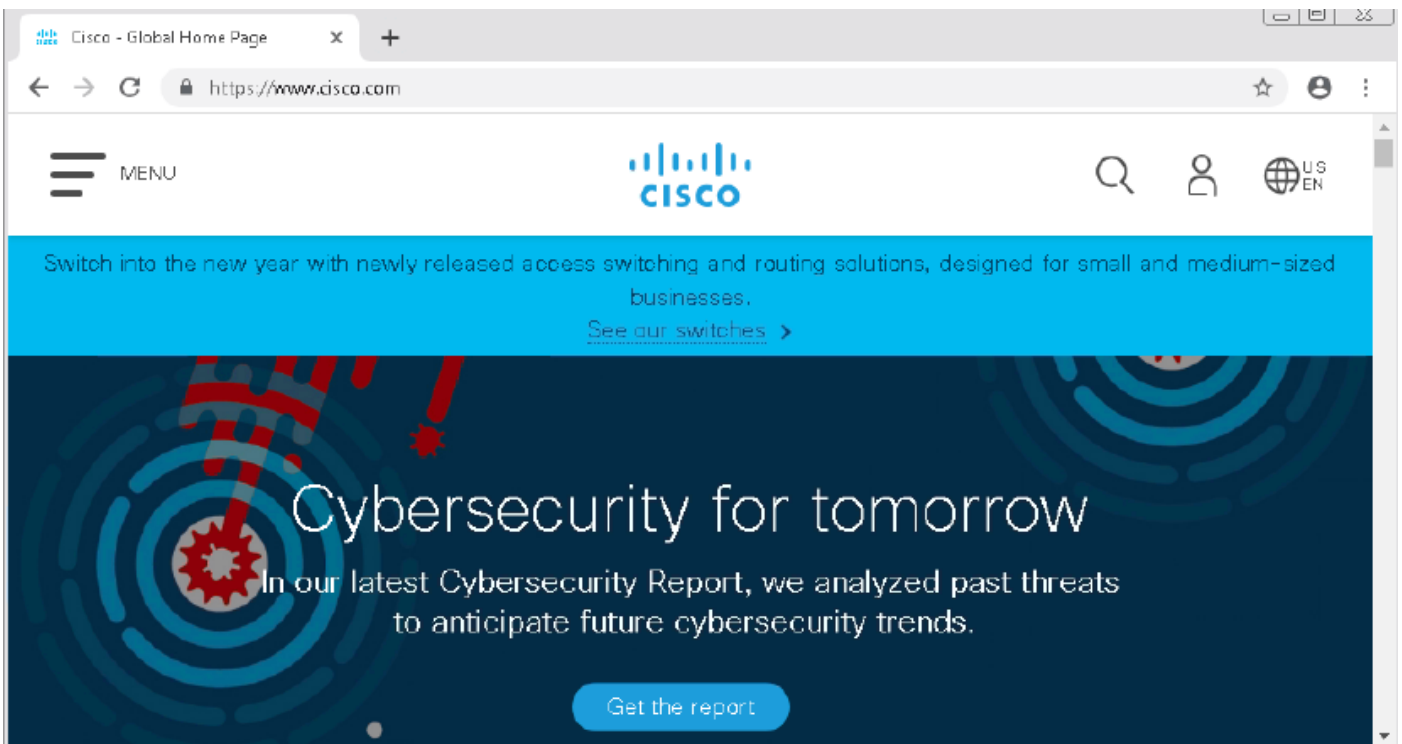
Ethernet adapter Local Area Connection 2:

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
```

Schritt 2: Bestätigen Sie, dass Sie zur Cisco.com-Website navigieren können (siehe Bild):



Schritt 3: Mit Paketerfassung bestätigen, dass DNS korrekt aufgelöst wurde:

The screenshot shows a network capture in Wireshark. The top pane displays a table of captured 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 bottom pane shows the details of the selected packet (Frame 3515):

- 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

Nachdem die DNS-Richtlinie angewendet wurde

Schritt 1: Löschen Sie den DNS-Cache auf Ihrem Host mit dem Befehl `ipconfig /flushdns`.

```

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

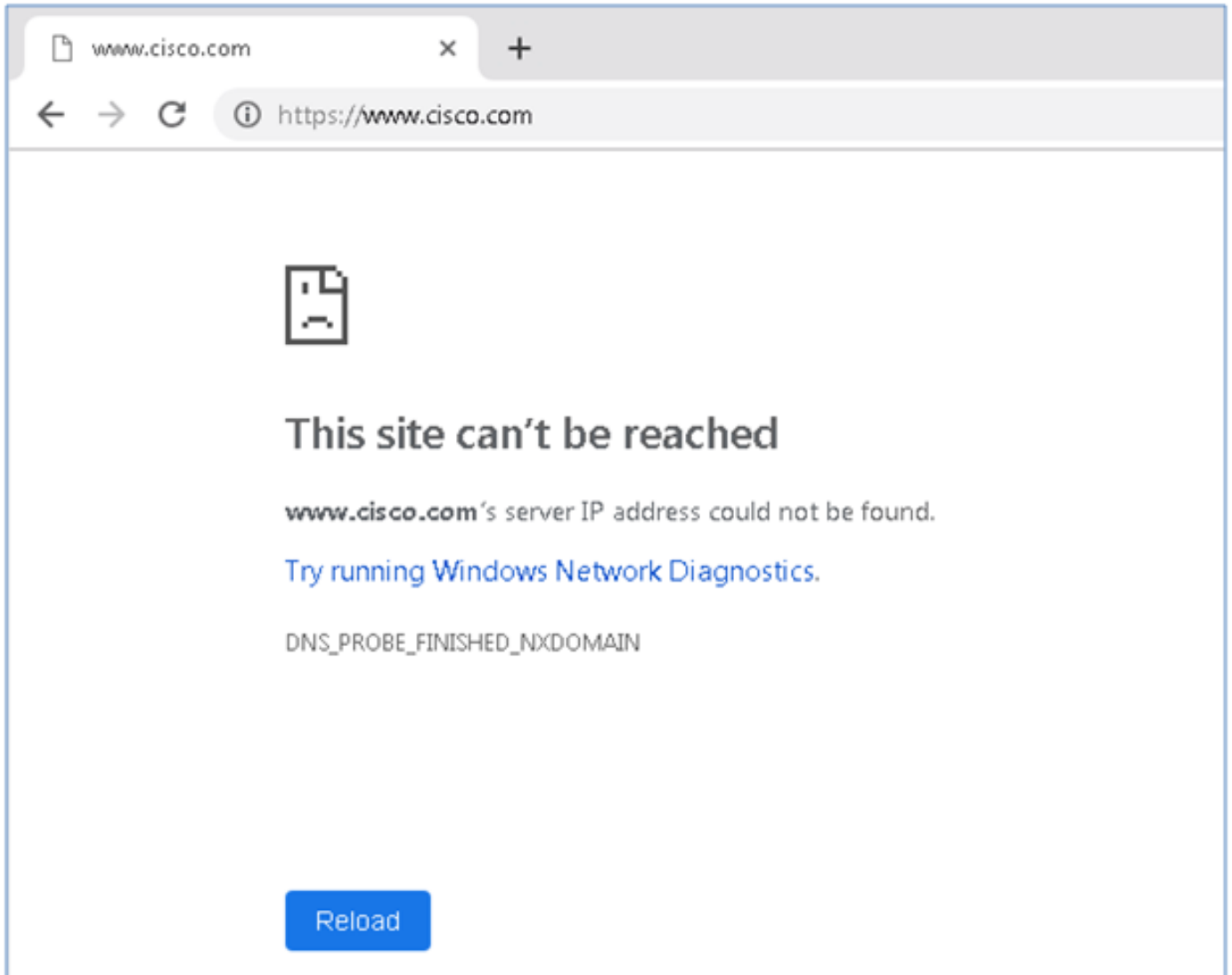
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
  
```

Schritt 2: Navigieren Sie mit einem Webbrowser zur betreffenden Domäne. Es sollte nicht erreichbar sein:



Schritt 3: Versuchen Sie, **nslookup** auf der Domäne cisco.com herauszugeben. Die Namensauflösung schlägt fehl.

```
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
```

Schritt 4: Paketerfassungen zeigen eine Antwort vom FTD an, nicht vom DNS-Server.

The screenshot shows a network traffic 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]

Schritt 5: Führen Sie das Debuggen in der FTD-CLI aus: System unterstützt Firewall-Engine-Debugging und legt UDP-Protokoll fest.

```
>
> 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
```

* Debuggt, wenn cisco.com zugeordnet wird:

```

> 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

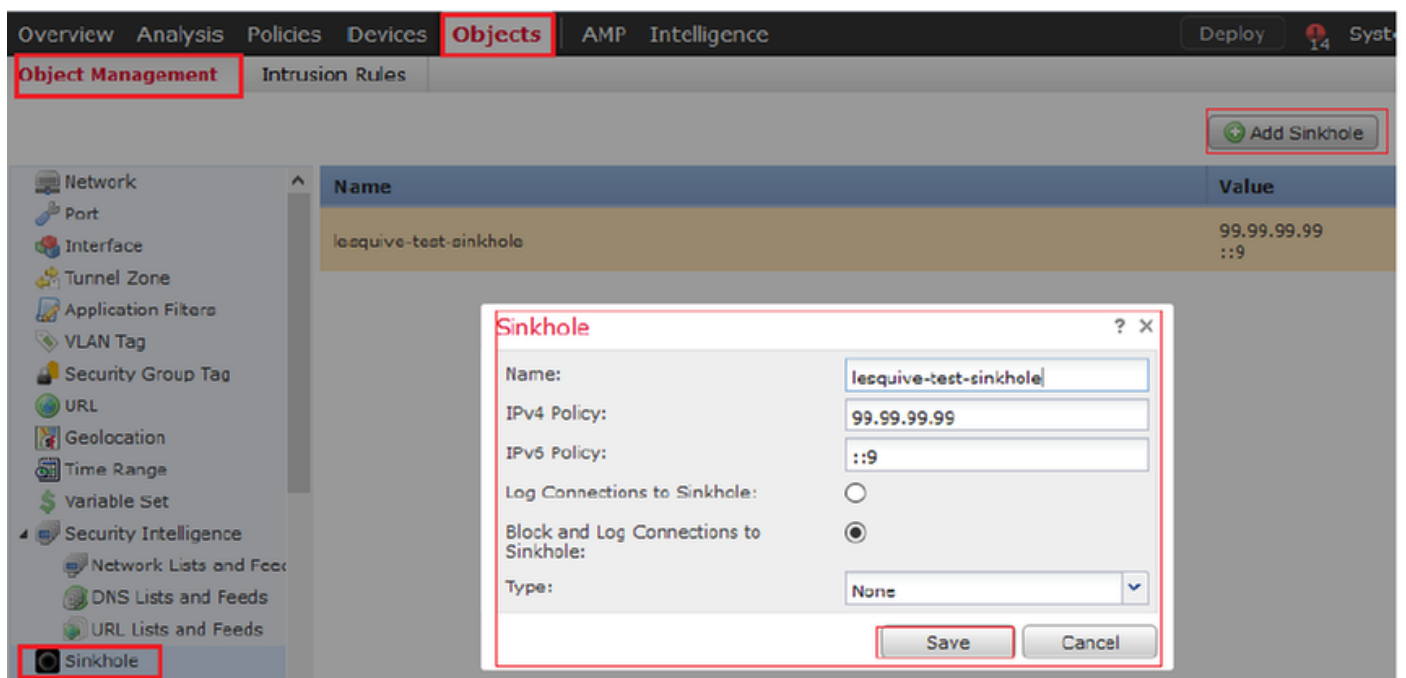
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.cr security.lab
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Skipping DNS rule lookup for cisco.com.cr security.lab since we've already gotten a response
192.168.20.10-61373 > 156.154.70.1-53 17 AS 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

```

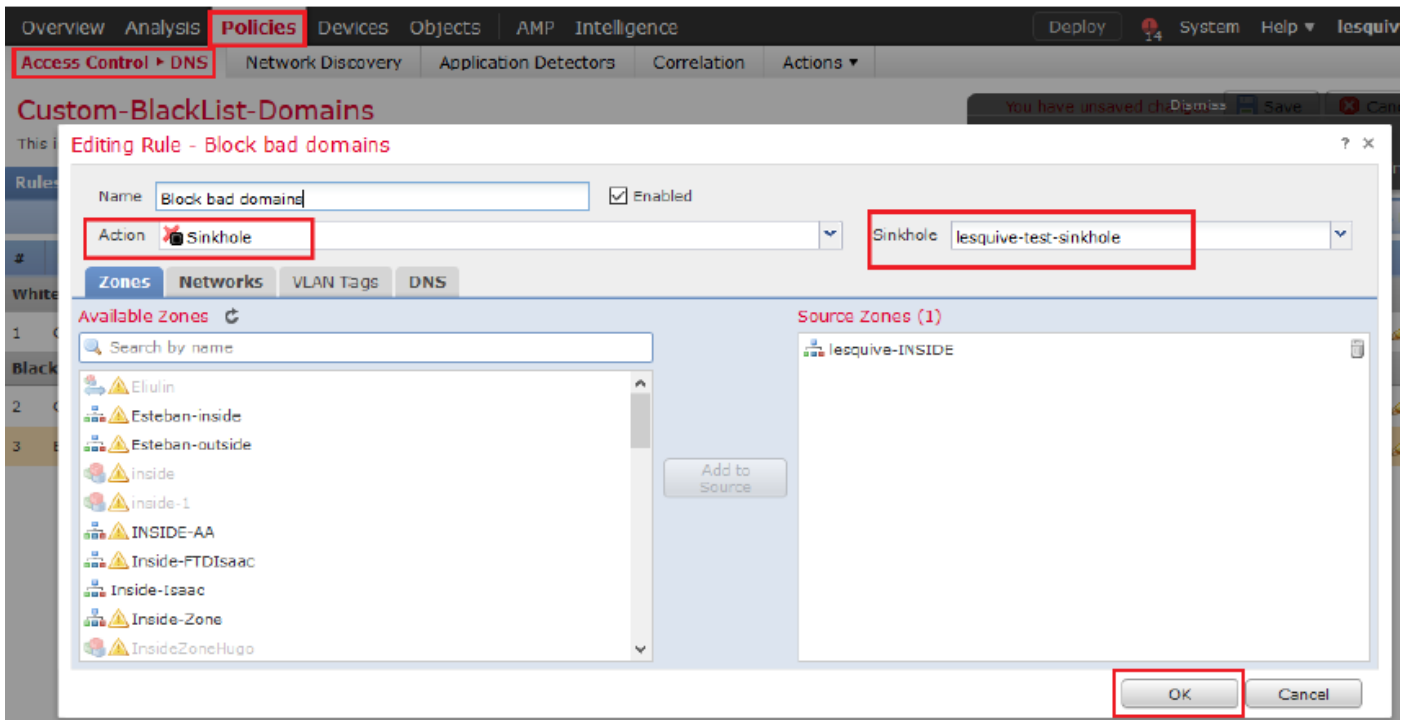
Optionale Sinkloch-Konfiguration

Ein DNS-sinkhole ist ein DNS-Server, der falsche Informationen bereitstellt. Anstatt eine DNS-Antwort "No such name" (Kein solcher Name) auf DNS-Anfragen an Domänen zurückzusenden, die Sie blockieren, gibt sie eine gefälschte IP-Adresse zurück.

Schritt 1: Navigieren Sie zu Objekte >> Objektverwaltung >> Sinkhole >> Sinkhole hinzufügen, und erstellen Sie die gefälschten IP-Adressinformationen.

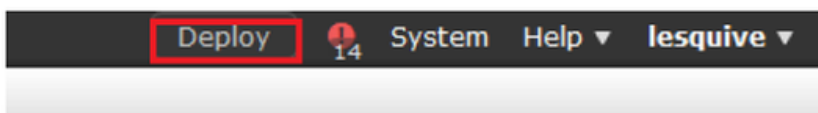


Schritt 2: Wenden Sie das Sprungloch auf Ihre DNS-Richtlinie an, und stellen Sie Änderungen in FTD bereit.



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



Überprüfen Sie, ob das Sinkloch funktioniert.

```
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

Fehlerbehebung

Navigieren Sie zu **Analysis > Connections >> Security Intelligence Events (Analyse >> Verbindungen >> Sicherheitsinformationsergebnisse)**, um alle von SI ausgelösten Ereignisse zu verfolgen, sofern Sie die Anmeldung in der DNS-Richtlinie aktiviert haben:

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	

Sie können den **Firewall-Engine-Debug-Befehl** zur **Systemunterstützung** auch auf dem vom FMC verwalteten FTD verwenden.

```
>
> 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
```

Paketerfassungen können hilfreich sein, um zu bestätigen, dass DNS-Anfragen an den FTD-Server gesendet werden. Vergessen Sie nicht, beim Testen den Cache auf Ihrem lokalen Host zu löschen.

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>_