

使用Firepower管理中心阻止具有安全情报的DNS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[使用要阻止的域配置自定义DNS列表，并将列表上传到FMC](#)

[添加新的DNS策略，其中“action configured to 'domain not found'”](#)

[将DNS策略分配到访问控制策略](#)

[验证](#)

[应用DNS策略之前](#)

[应用DNS策略后](#)

[可选Sinkhole配置](#)

[验证Sinkhole是否正常工作](#)

[故障排除](#)

简介

本文档介绍将域名系统(DNS)列表添加到DNS策略以便您能将其应用于安全情报(SI)的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco ASA55XX威胁防御配置
- 思科Firepower管理中心配置

使用的组件

- 思科ASA5506W-X威胁防御(75)版本6.2.3.4 (内部版本42)
- 适用于VMWare的思科Firepower管理中心 软件版本:6.2.3.4 (内部版本42) 操作系统：思科 Fire Linux OS 6.2.3(build13)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全情报的工作方式是阻止流入或流出IP地址、URL或域名的流量，这些流量具有已知的不良信誉。在本文档中，主要重点是域名黑名单。

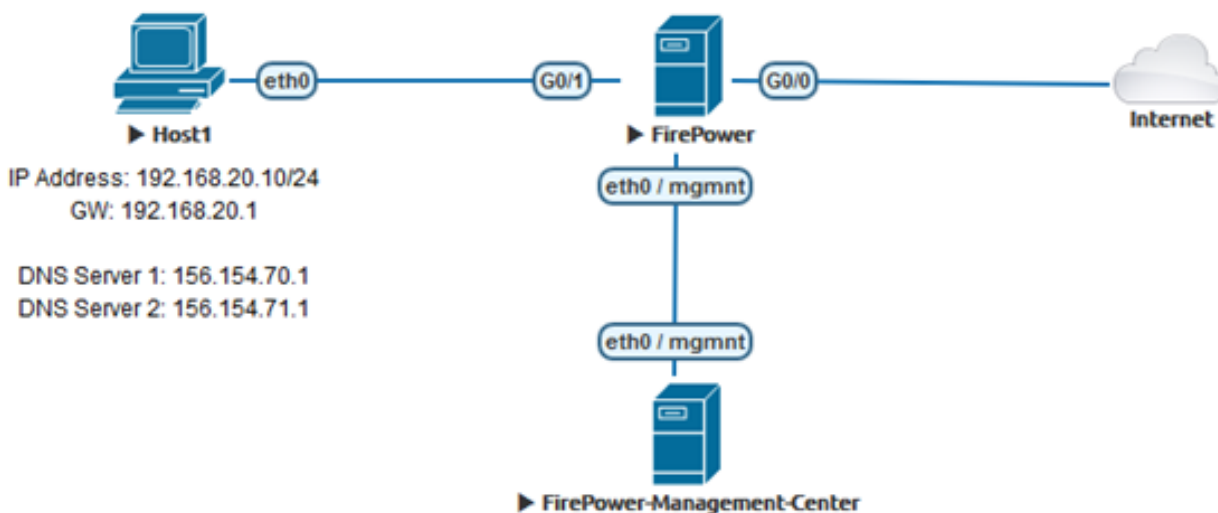
示例使用块1域：

- cisco.com

您可以使用URL过滤来阻止其中一些站点，但问题是URL必须完全匹配。另一方面，SI的DNS黑名单可以专注于“cisco.com”等域，而无需担心任何子域或URL更改。

本文档末尾还演示了可选的Sinkhole配置。

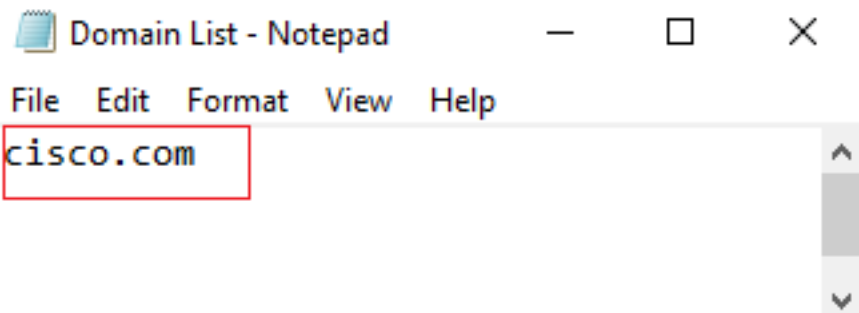
网络图



配置

使用要阻止的域配置自定义DNS列表，并将列表上传到FMC

步骤1.使用要阻止的域创建.txt文件。将.txt文件保存在计算机上：



步骤2.在FMC中，导航至Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds。

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management Intrusion Rules

Security Intelligence

- Network Lists and Feeds
- DNS Lists and Feeds**
- URL Lists and Feeds

Update Feeds **Add DNS Lists and Feeds**

Name	Type
Cisco-DNS-and-URL-Intelligence-Feed <i>Last Updated: 2019-02-14 10:21:48</i>	Feed
Global-Blacklist-for-DNS	List
Global-Whitelist-for-DNS	List

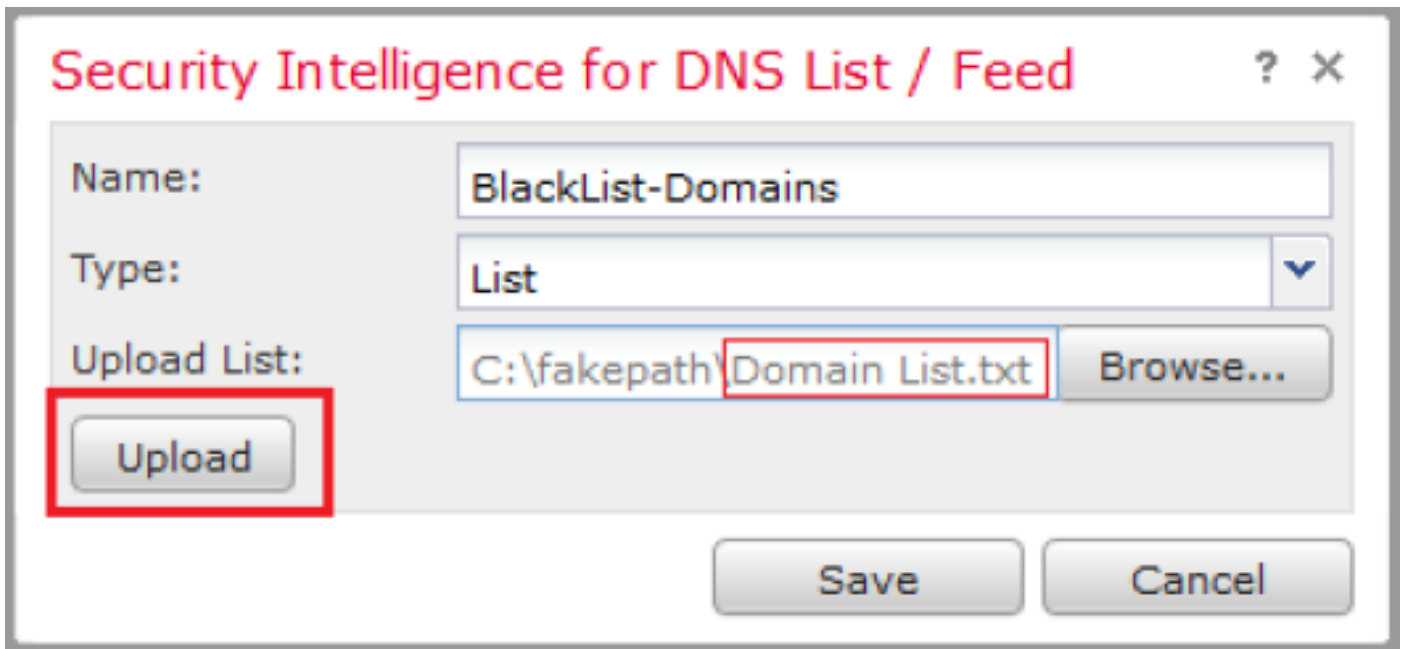
步骤3.创建名为“BlackList-Domains”的列表，该类型应为list，并且应上传包含相关域的.txt文件，如图所示：

Security Intelligence for DNS List / Feed ? X

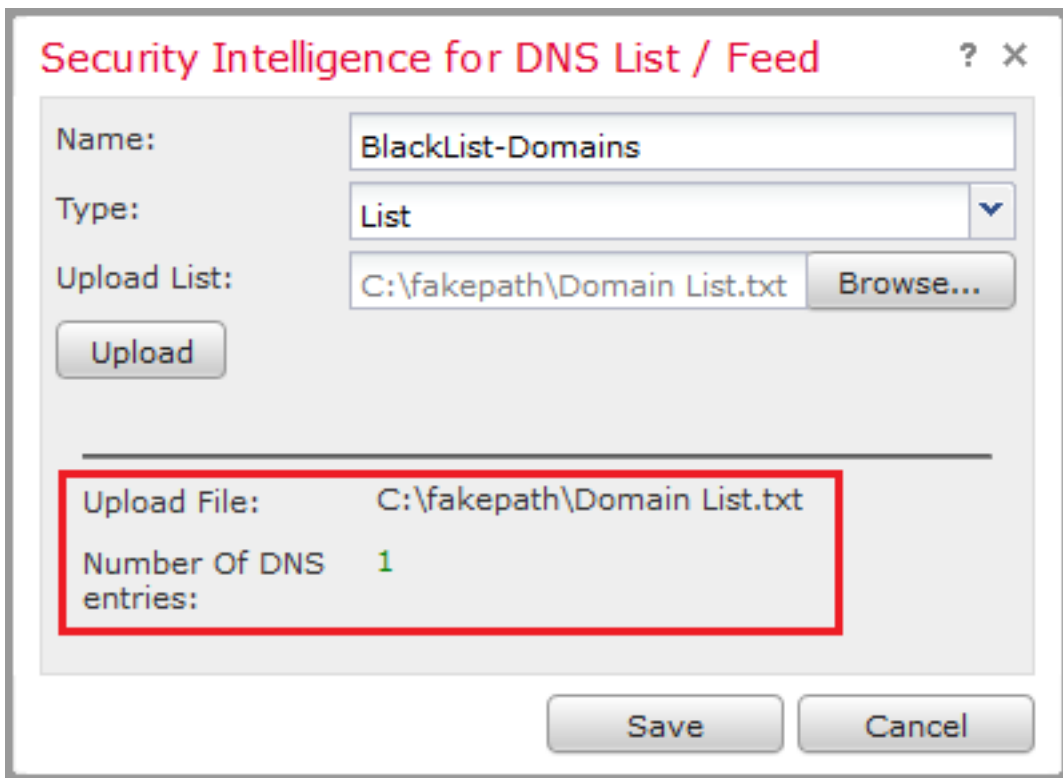
Name:

Type: ▼

Upload List: **Browse...**



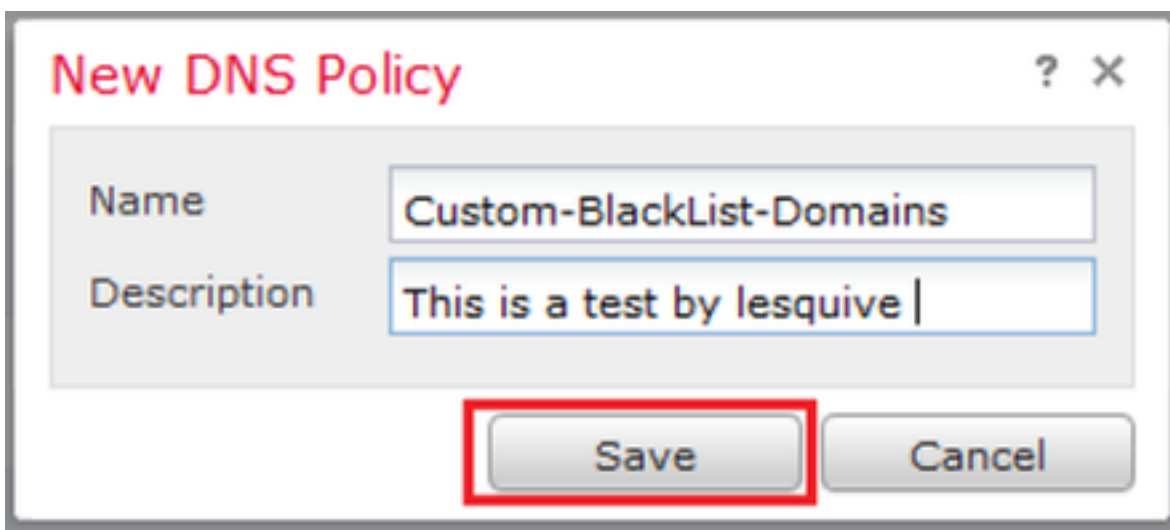
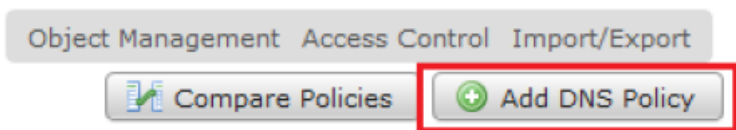
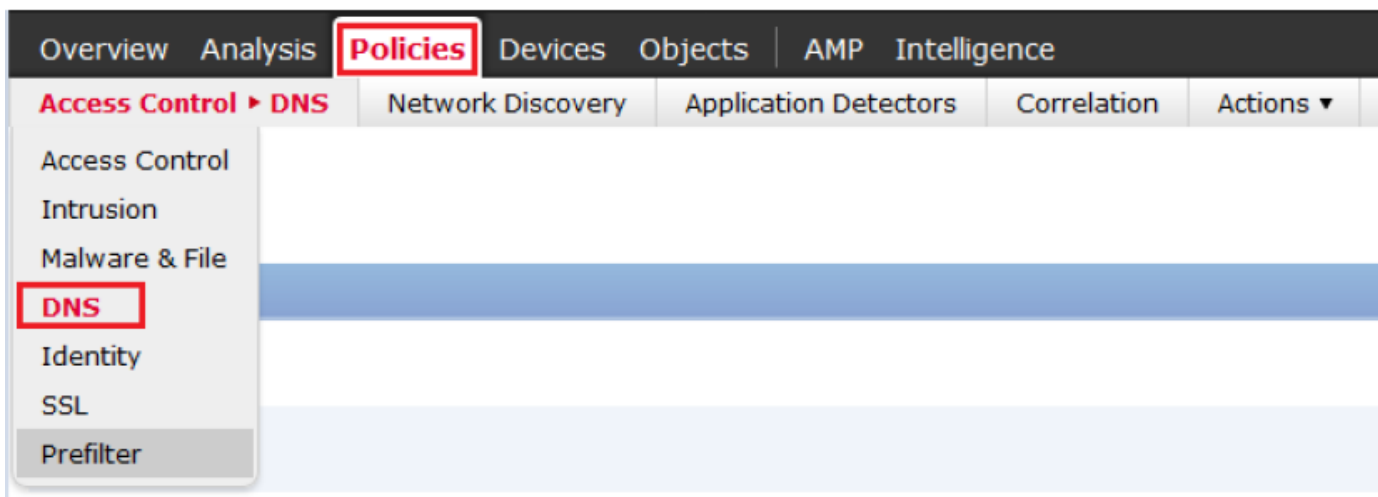
*请注意，上传.txt文件时，DNS条目数应读取所有域。在本例中，总数为1:



添加新的DNS策略，其中“action configured to 'domain not found'”

*确保添加源区域、源网络和DNS列表。

步骤1.导航至Policies >> Access Control >> DNS >> Add DNS Policy:



步骤2.添加DNS规则，如图所示：



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 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:

Networks | Zones | 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
- Pat_Marco

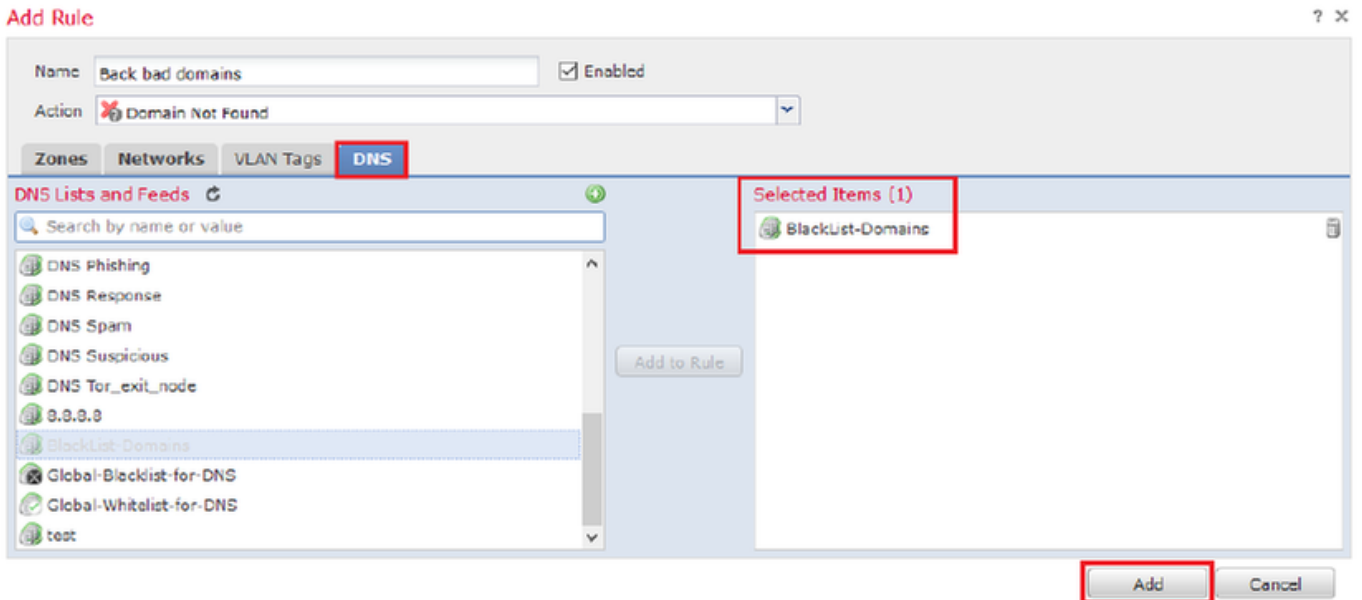
Source Networks (1)

- lesquive-network

Add to Source

Enter an IP address Add

Add Cancel



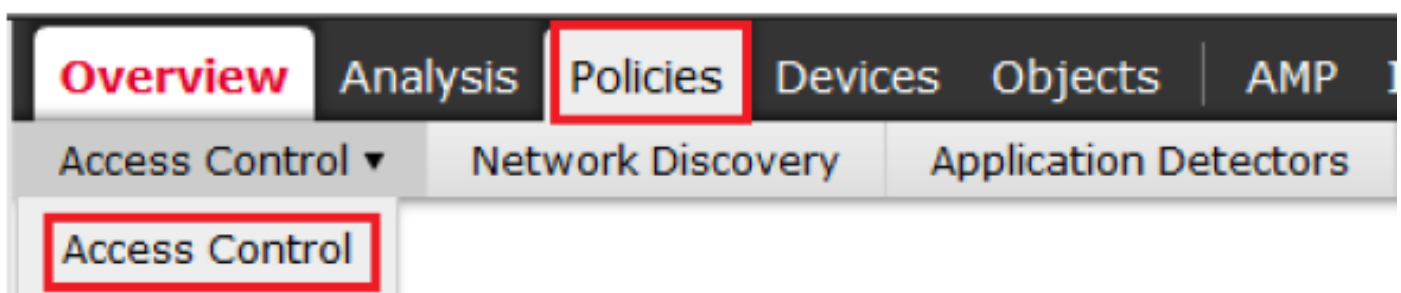
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Block bad domains	lesquive-INS	lesquive-network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

有关规则顺序的重要信息：

- 全局白名单始终优先于所有其他规则。
- 后代DNS白名单规则仅在非枝叶域的多域部署中显示。它始终是次要规则，优先于除全局白名单之外的所有其他规则。
- 白名单部分位于黑名单部分之前；白名单规则始终优先于其他规则。
- 全局黑名单始终在黑名单部分中处于首位，优先于所有其他监控和黑名单规则。
- 后代DNS黑名单规则仅在非枝叶域的多域部署中显示。它始终在黑名单部分中位列第二，优先于除全局黑名单之外的所有其他监控和黑名单规则。
- “黑名单”部分包含监控和黑名单规则。
- 首次创建DNS规则时，如果分配了白名单操作，则系统位置在白名单部分最后，如果分配了任何其他操作，则在黑名单部分最后

将DNS策略分配到访问控制策略

转至Policies >> Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy，然后添加您创建的策略。

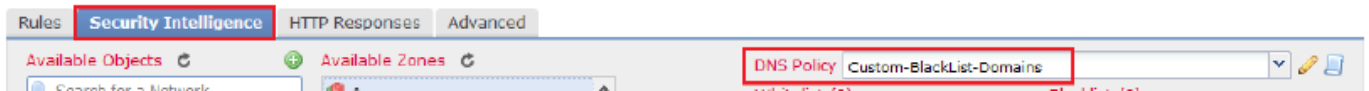


Enter Description

Prefilter Policy: Default_Prefilter_Policy

SSL Policy: None

Identity Policy: None

Inheritance Settings | Policy Assignments (1)

确保完成后部署所有更改。

验证

应用DNS策略之前

步骤1.检查主机上的DNS服务器和IP地址信息，如图所示：

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

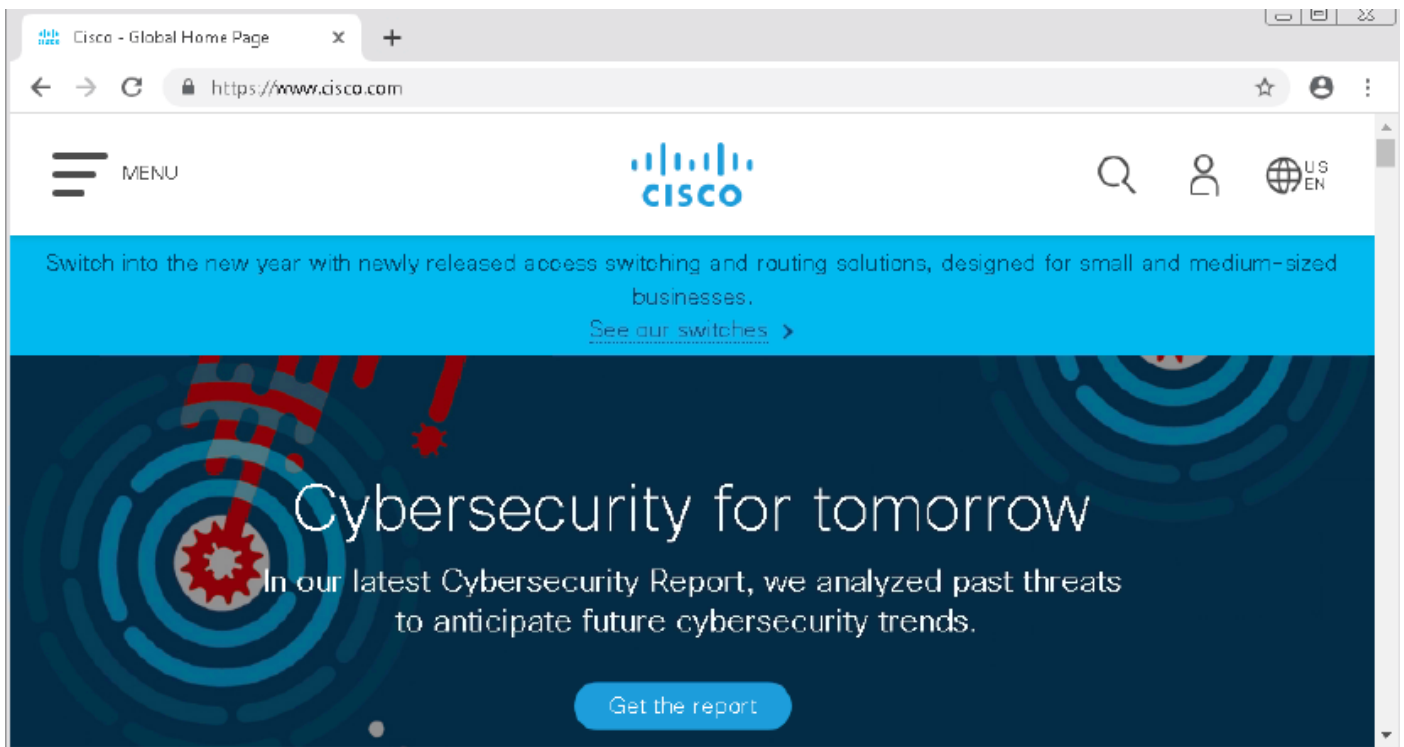
Ethernet adapter Local Area Connection 2:

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
```

步骤2.确认您可以导航至cisco.com，如图所示：



步骤3.使用数据包捕获确认DNS已正确解析：

*Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ucp.stream eq 41 Expression

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

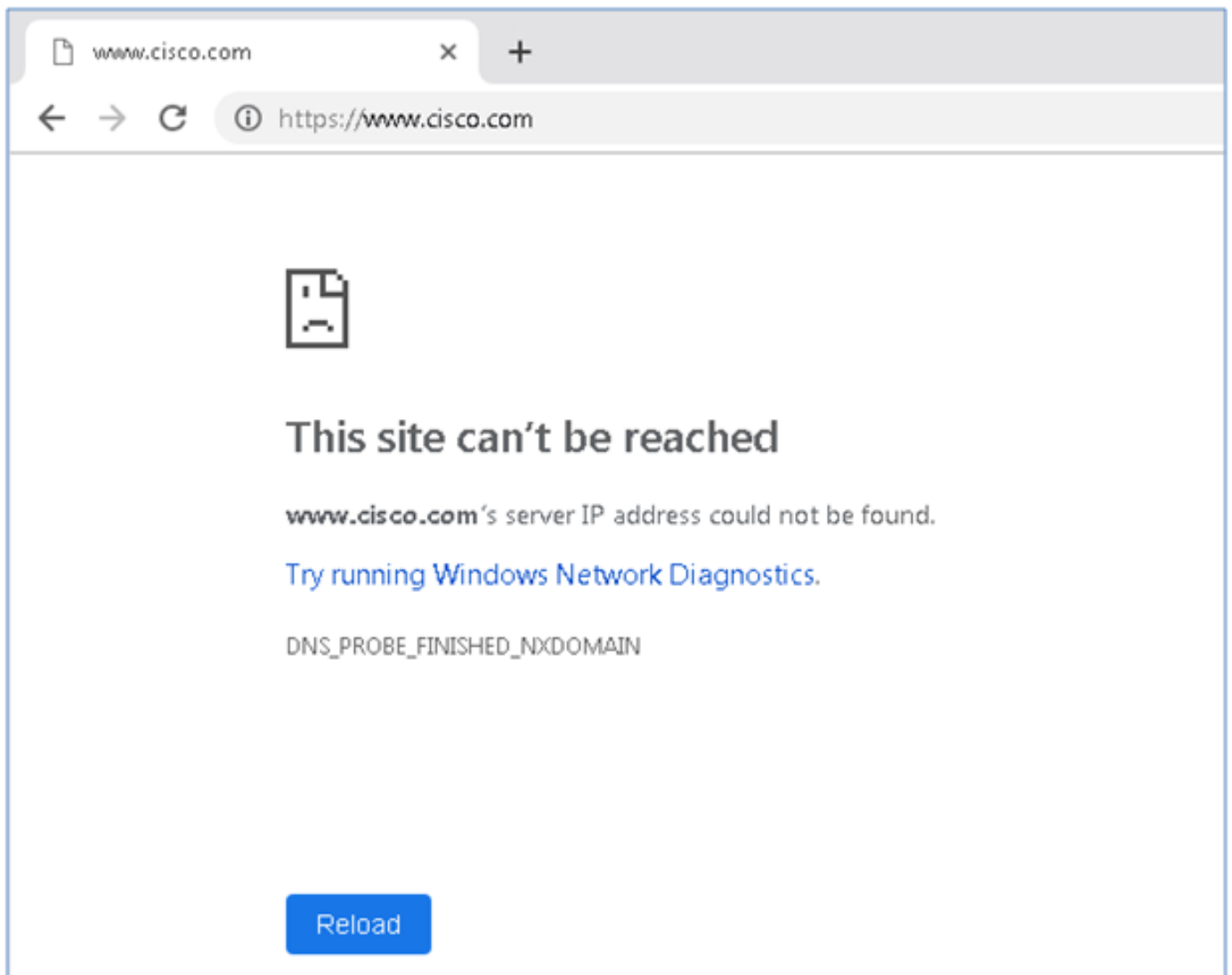
Address: 72.163.4.185

应用DNS策略后

步骤1.使用命令ipconfig /flushdns清除主机上的DNS缓存。

```
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>_
```

步骤2.使用Web浏览器导航至相关域。它应该不可达：



步骤3.尝试在域cisco.com上发出nslookup。名称解析失败。

```
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

www.rdnsl.ultradns.net can't find cisco.com: Non-existent domain
```

步骤4.数据包捕获显示来自FTD的响应，而不是DNS服务器的响应。

```
*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.stream eq 13
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 11.205928 156.154.70.1 192.168.20.10 DNS 69 Standard query response 0x0004 No such name A cisco.com

> 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]
```

步骤5.在FTD CLI中运行调试：系统支持firewall-engine-debug并指定UDP协议。

```
>
> 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
```

*匹配cisco.com时的调试：

```
> system support firewall-engine-debug

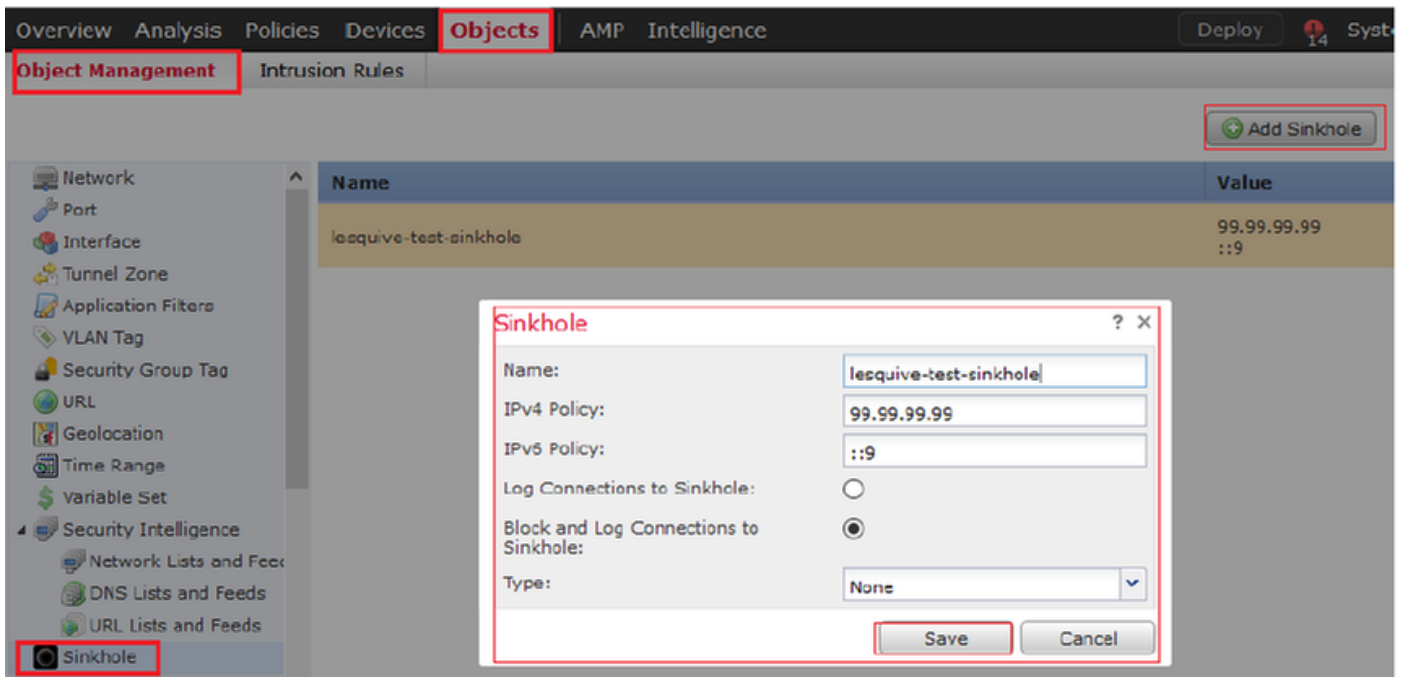
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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
```

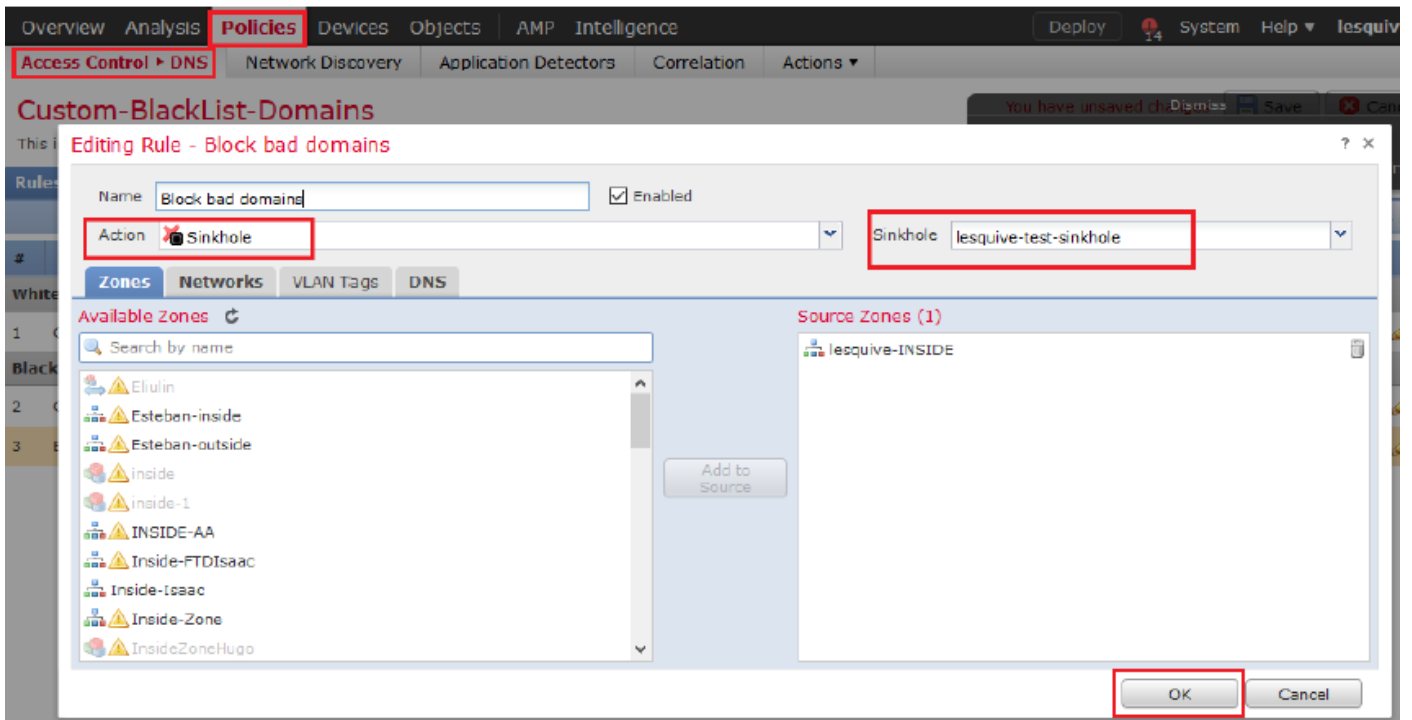
可选Sinkhole配置

DNS信洞是提供虚假信息的DNS服务器。它不会返回“无此名称”DNS响应，而是返回虚假IP地址，以响应您所阻止的域的DNS查询。

步骤1.导航至“对象”>>“对象管理”>>“Sinkhole”>>“添加Sinkhole”并创建虚假的IP地址信息。



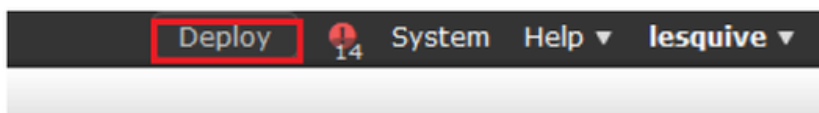
步骤2.将Sinkhole应用到DNS策略，并将更改部署到FTD。



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



验证Sinkhole是否正常工作

```
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

故障排除

导航至 Analysis >> Connections >> Security Intelligence Events，以跟踪SI触发的所有事件，只要您已在DNS策略中启用日志记录：

Security Intelligence Events [\[switch workflow\]](#)

Security Intelligence with Application Details > Table View of Security Intelligence Events

No Search Constraints (Edit Search)

2019-02-14 13:42:42 - 2019-02-14 14:42:42 Expanding

	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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-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	BlockList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	53647 / udp	

您还可以在FMC管理的FTD上使用system support firewall-engine-debug命令。

```
>
> 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
```

数据包捕获有助于确认DNS请求是否正在向FTD服务器发出。测试时，不要忘记清除本地主机上的缓存。

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>_