

使用Firepower管理中心阻止具有安全情報的DNS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[使用要阻止的域配置自定義DNS清單並將清單上傳到FMC](#)

[新增一個新的DNS策略，該策略的「操作配置為未找到域」](#)

[將DNS策略分配給您的訪問控制策略](#)

[驗證](#)

[應用DNS策略之前](#)

[應用DNS策略之後](#)

[可選的Sinkhole配置](#)

[驗證Sinkhole工作正常](#)

[疑難排解](#)

簡介

本檔案介紹將網域名稱系統(DNS)清單新增到DNS原則中的程式，以便您可以將其套用到安全情報(SI)。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA55XX威脅防禦配置
- Cisco Firepower管理中心配置

採用元件

- Cisco ASA5506W-X威脅防禦(75)版本6.2.3.4 (內部版本42)
- 適用於VMWare的Cisco Firepower管理中心 軟體版本：6.2.3.4 (內部版本42) 作業系統：
Cisco Fire Linux OS 6.2.3(build13)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

安全情報通過阻止流向或來自具有已知不良信譽的IP地址、URL或域名的流量來工作。本文檔主要關注域名黑名單。

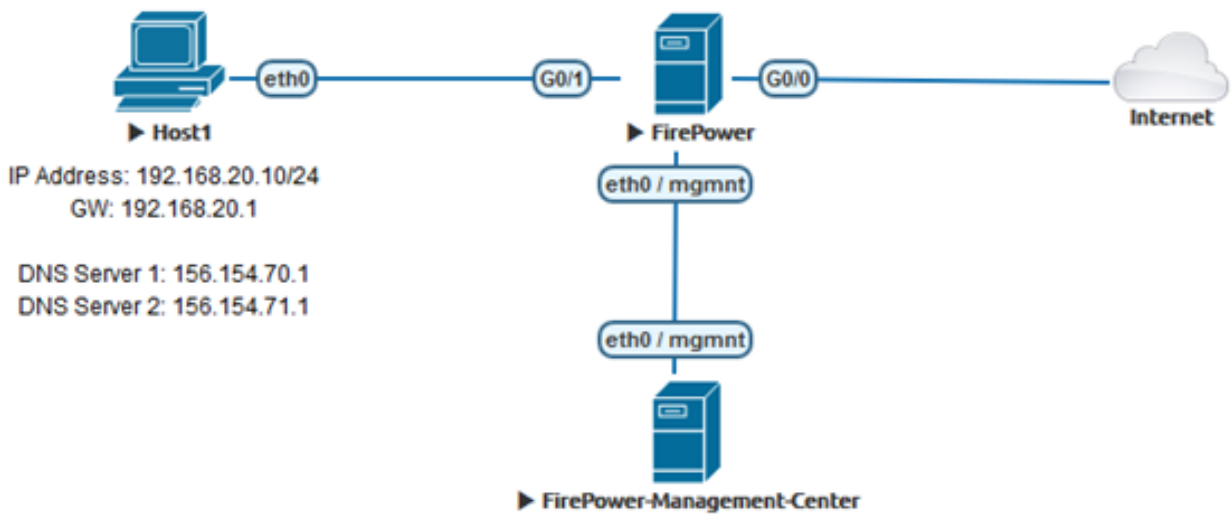
使用的示例塊1域：

- cisco.com

您可以使用URL過濾來封鎖其中一些網站，但問題在於URL必須完全匹配。另一方面，使用SI的DNS黑名單可以專注於像「cisco.com」這樣的域，而無需擔心任何子域或URL更改。

在本文檔末尾還演示了可選的Sinkhole配置。

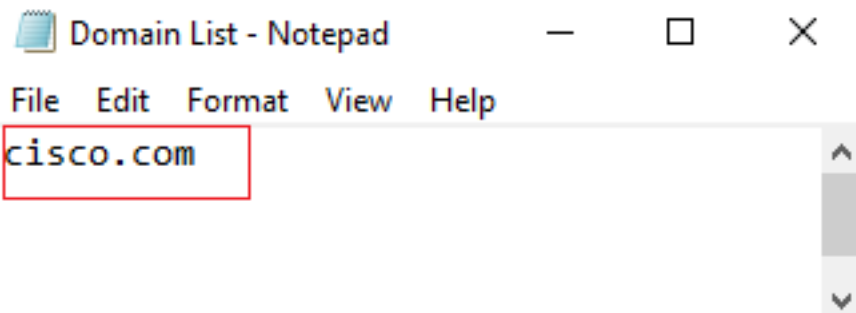
網路圖表



設定

使用要阻止的域配置自定義DNS清單並將清單上傳到FMC

步驟1.使用您要阻止的域建立.txt檔案。在電腦上儲存.txt檔案：



步驟2.在FMC中，導航到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

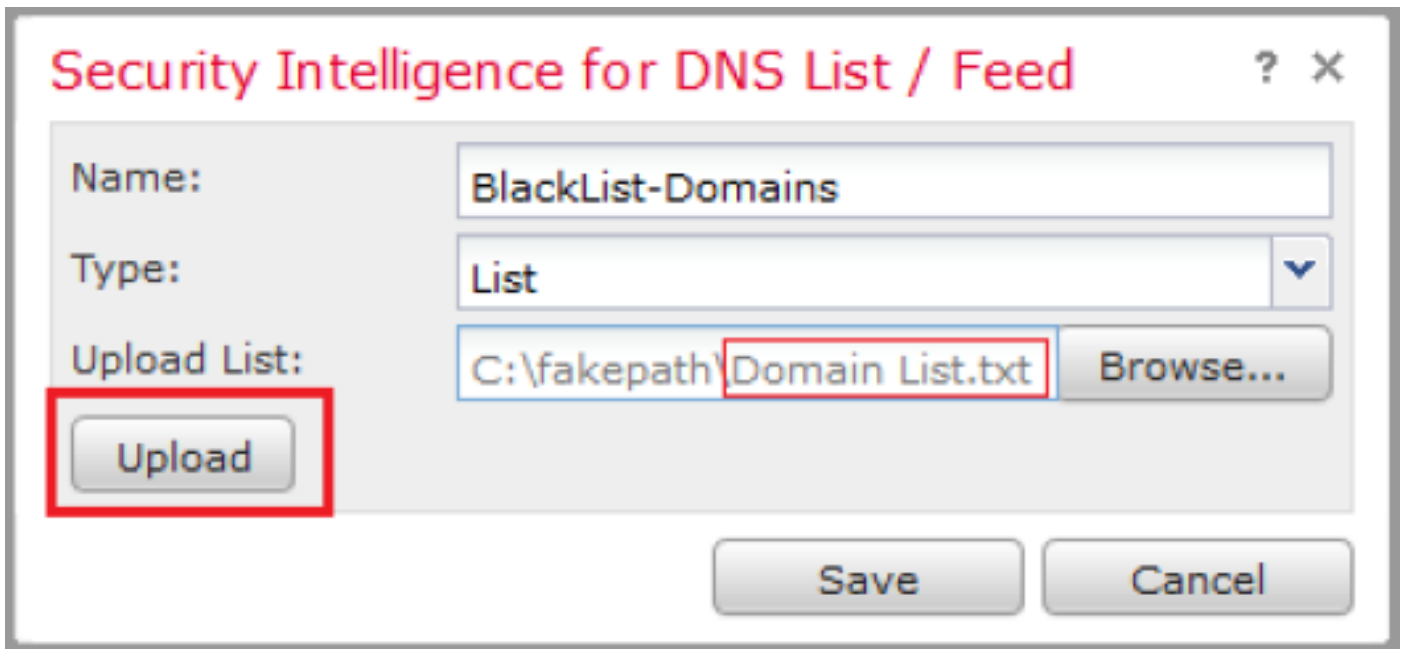
步驟3.建立一個名為「BlackList-Domains」的清單，型別應為list，並且上傳帶有相關域的.txt檔案，如下圖所示：

Security Intelligence for DNS List / Feed ? X

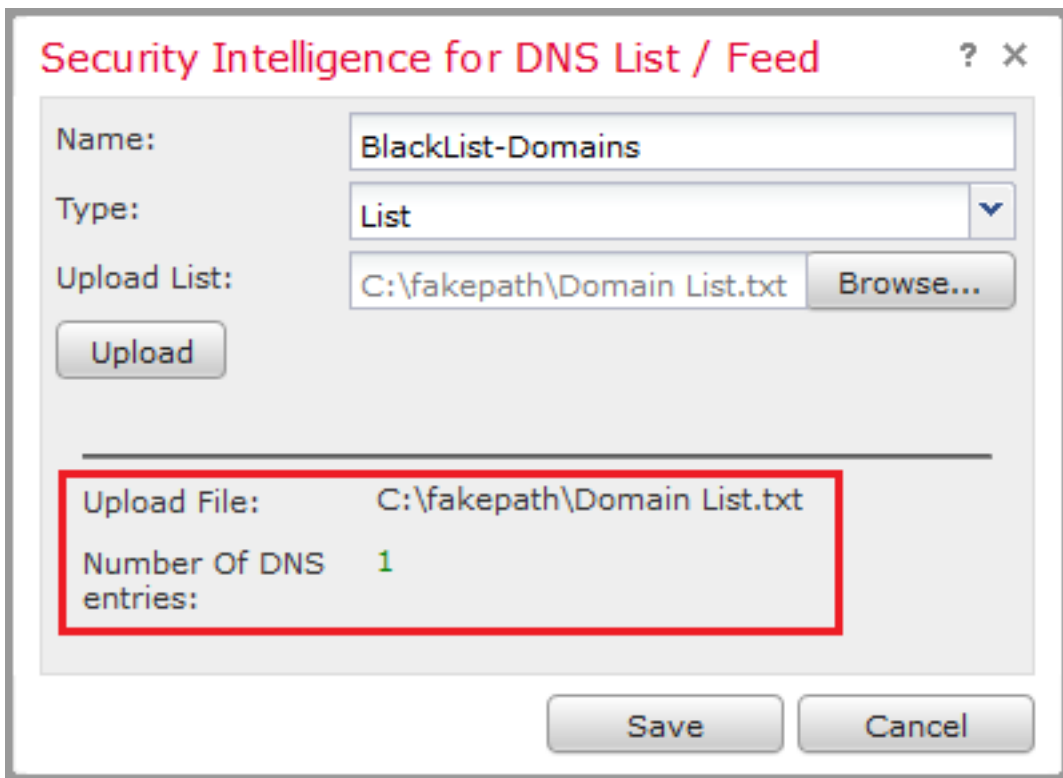
Name:

Type: ▼

Upload List: **Browse...**



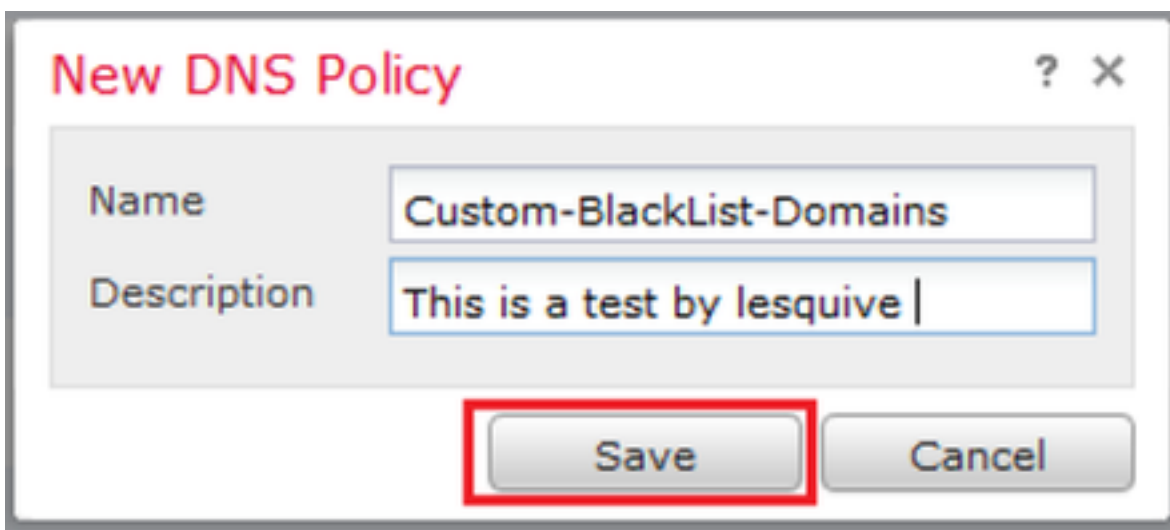
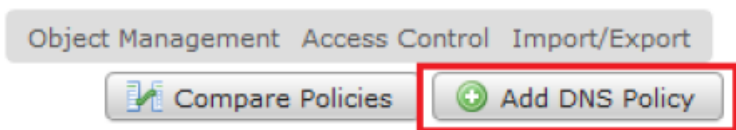
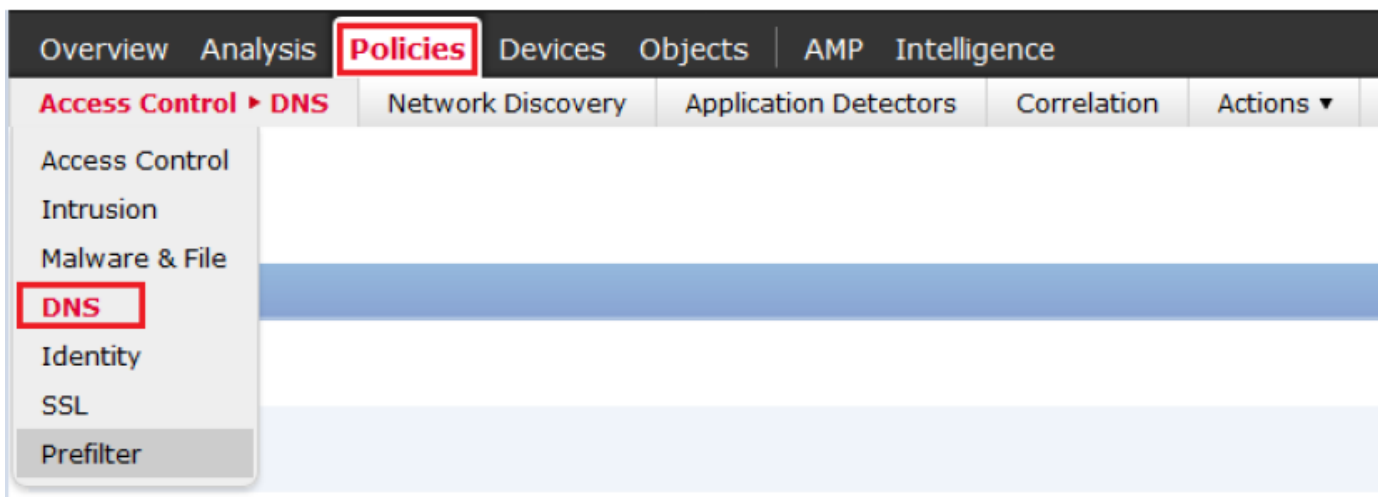
*請注意，上傳.txt檔案時，DNS條目數量應讀取所有域。在此範例中，一共為1:



新增一個新的DNS策略，該策略的「操作配置為未找到域」

*確保新增源區域、源網路和DNS清單。

步驟1. 導航到Policies >> Access Control >> DNS >> Add DNS Policy:



步驟2.新增DNS規則，如下圖所示：



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

Add Rule

Name: Beck 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
- 0.0.0.0
- BlackList-Domains**
- Global-Blacklist-for-DNS
- Global-Whitelist-for-DNS
- test

Selected Items (1)

- BlackList-Domains

Add to Rule

Add Cancel

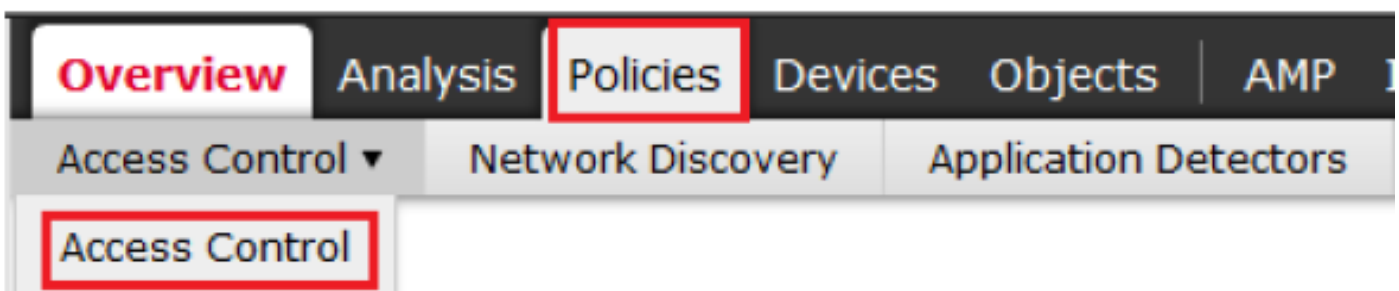
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action	
Whitelist							
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	
Blacklist							
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	
3	Block bad domains	lesquive-INS	lesquive-network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

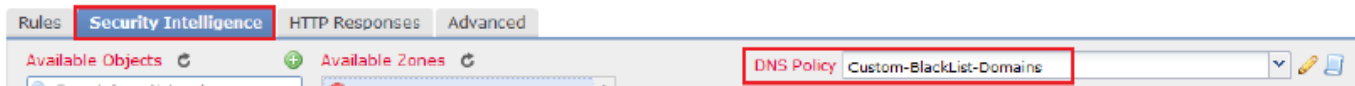
有關規則順序的重要資訊：

- 全域性白名單始終是第一個並優先於所有其他規則。
- 子體DNS白名單規則僅在多域部署和非枝葉域中顯示。它始終是次要，優先於除全域性白名單之外的所有其他規則。
- 「白名單」部分位於「黑名單」部分之前；白名單規則始終優先於其他規則。
- 全域性黑名單始終位於「黑名單」部分的首位，優先於其他所有監控規則和黑名單規則。
- 子體DNS黑名單規則僅在多域部署和非枝葉域中顯示。它始終位於「黑名單」部分的第二位，並且優先於除「全域性黑名單」之外的所有其他監控規則和黑名單規則。
- 「黑名單」部分包含監控規則和黑名單規則。
- 當您首次建立DNS規則時，如果分配了白名單操作，則系統位置位於白名單部分的最後；如果分配了任何其他操作，則系統位置位於黑名單部分的最後

將DNS策略分配給您的訪問控制策略

轉至Policies >> Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy並新增您建立的策略。



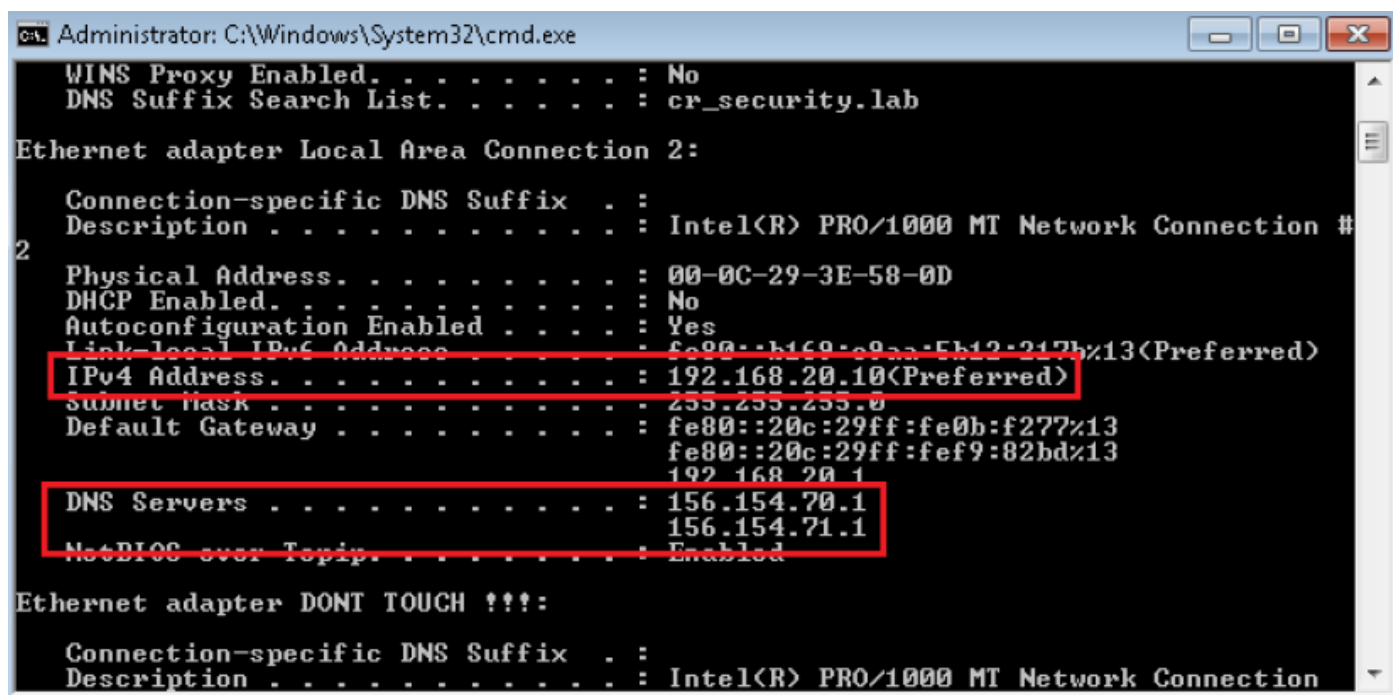


確保完成時部署所有更改。

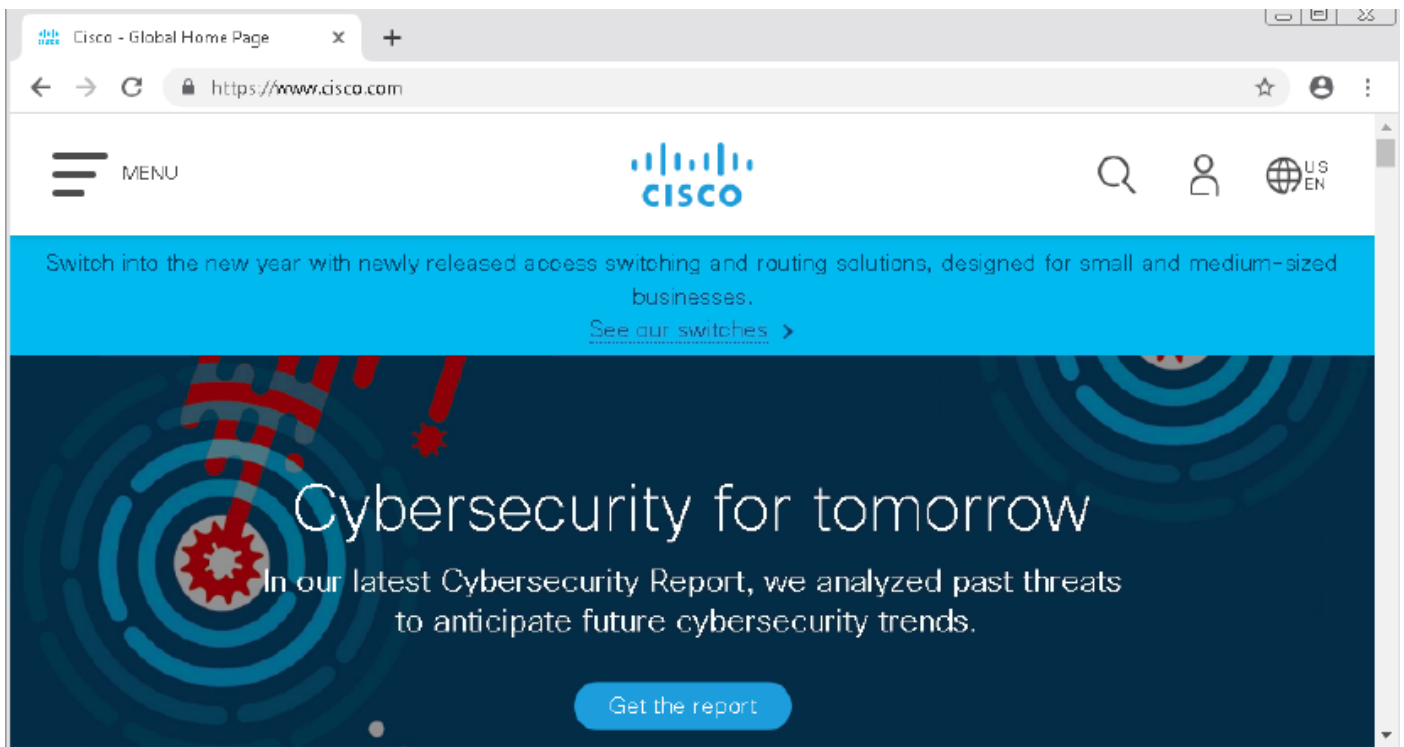
驗證

應用DNS策略之前

步驟1.檢查主機上的DNS伺服器 and IP地址資訊，如下圖所示：



步驟2.確認您可以導覽至cisco.com，如下圖所示：



步驟3.使用資料包捕獲確認DNS已正確解析：

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets. Packet No. 3515 is selected, and its details are shown in the bottom pane. The packet is a DNS Standard query response from 156.154.70.1 to 192.168.20.1. The response contains one answer for 'cisco.com' with IP address 72.163.4.185. The details pane for the answer is highlighted with a red box.

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
  
```

應用DNS策略之後

步驟1.使用命令ipconfig /flushdns清除主機上的DNS快取。

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

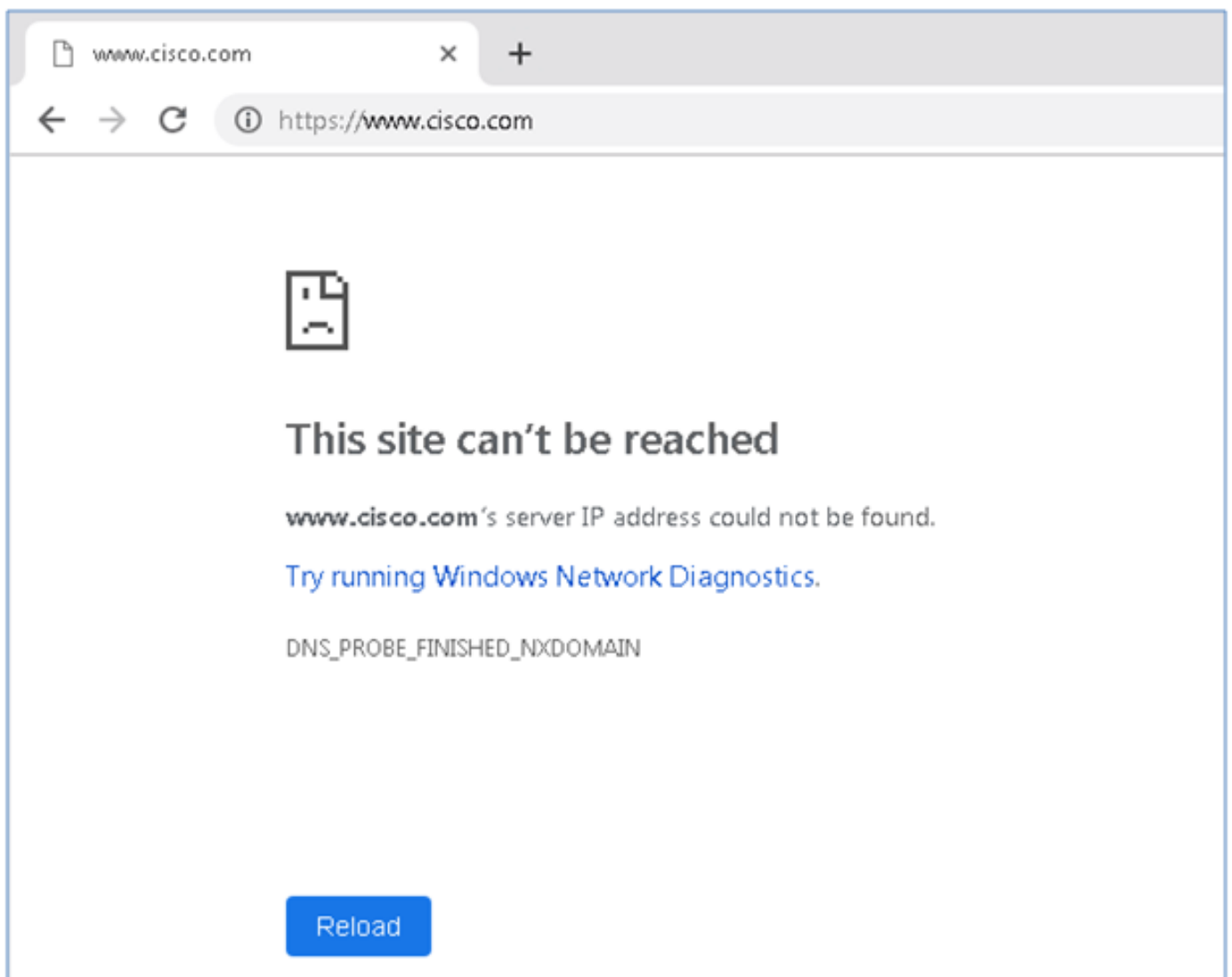
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
```

步驟2.使用Web瀏覽器導航至相關域。應該無法連線：



步驟3.嘗試在域cisco.com上發出nslookup。名稱解析失敗。

```
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

www.ultra1.ultradns.net can't find cisco.com: Non-existent domain
```

步驟4.封包擷取顯示來自FTD (而不是DNS伺服器) 的回應。

```
*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]
```

步驟5.在FTD CLI中執行偵錯：系統支援firewall-engine-debug並指定UDP協定。

```
>
> 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
```

*與cisco.com匹配時的調試：

```
> system support firewall-engine-debug

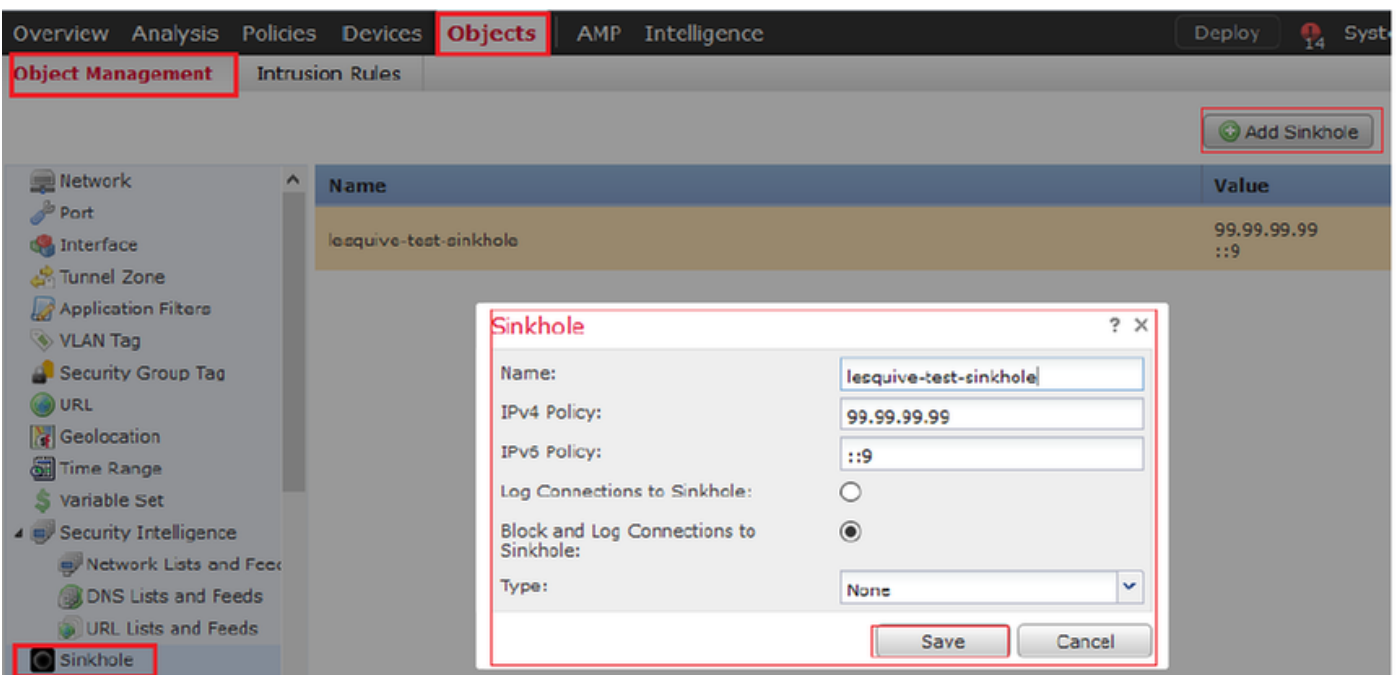
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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
```

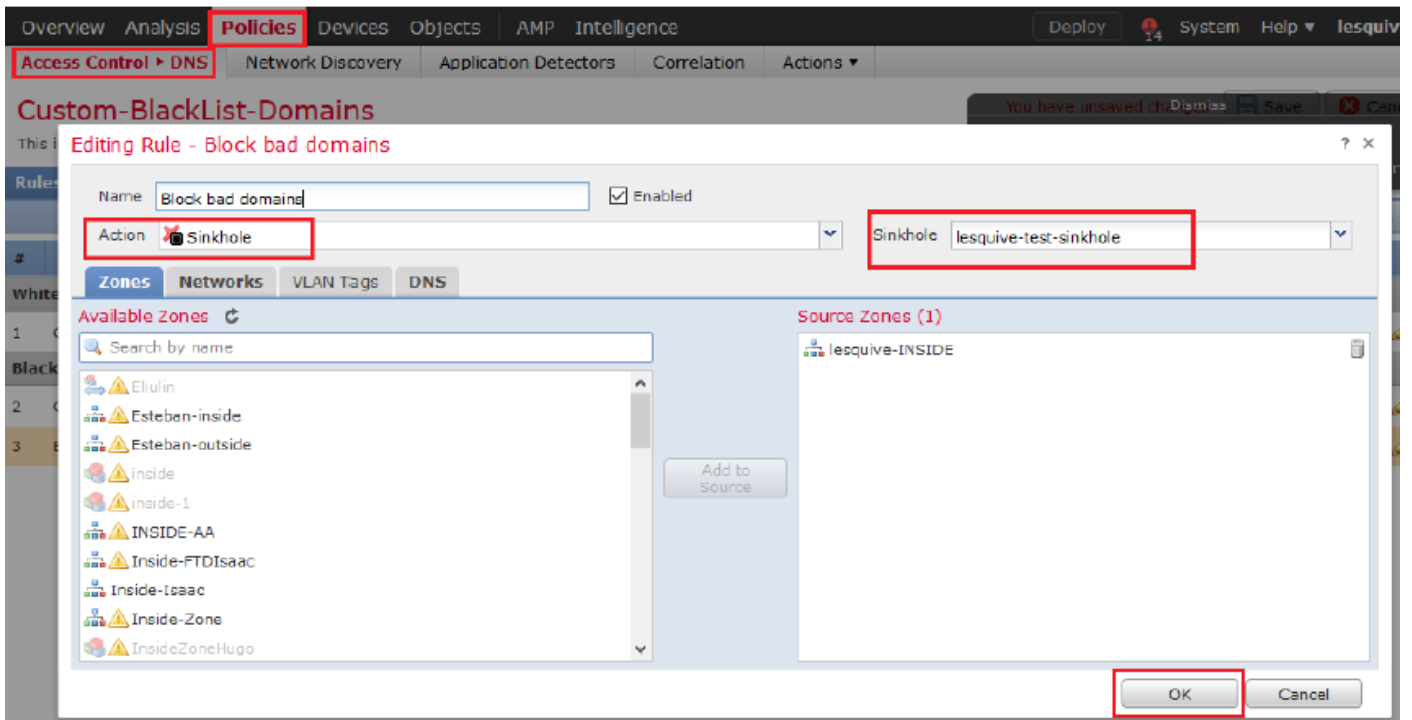
可選的Sinkhole配置

DNS sinkhole是提供虛假資訊的DNS伺服器。它不是對要阻止的域上的DNS查詢返回「無此類名稱」的DNS響應，而是返回一個假IP地址。

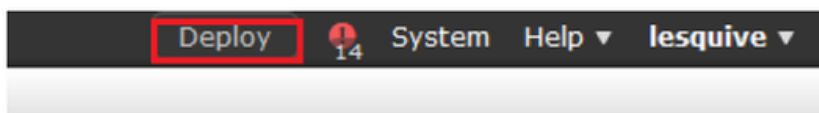
步驟1.導航到Objects > Object Management >> Sinkhole >> Add Sinkhole並建立虛假IP地址資訊。



步驟2.將sinkhole套用到DNS原則，並將變更部署到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



驗證Sinkhole工作正常

```

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 99.99.99.99
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

疑難排解

導航到 Analysis >> Connections >> Security Intelligence Events 以跟蹤 SI 觸發的所有事件，只要您已在 DNS 策略中啟用日誌記錄：

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 14:36:57		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	

您也可以由 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
```

封包擷取有助於確認 DNS 要求是否正在傳送至 FTD 伺服器。測試時不要忘記清除本地主機上的快取。

。

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>_