使用Firepower管理中心阻止具有安全情報的DNS

目錄

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。

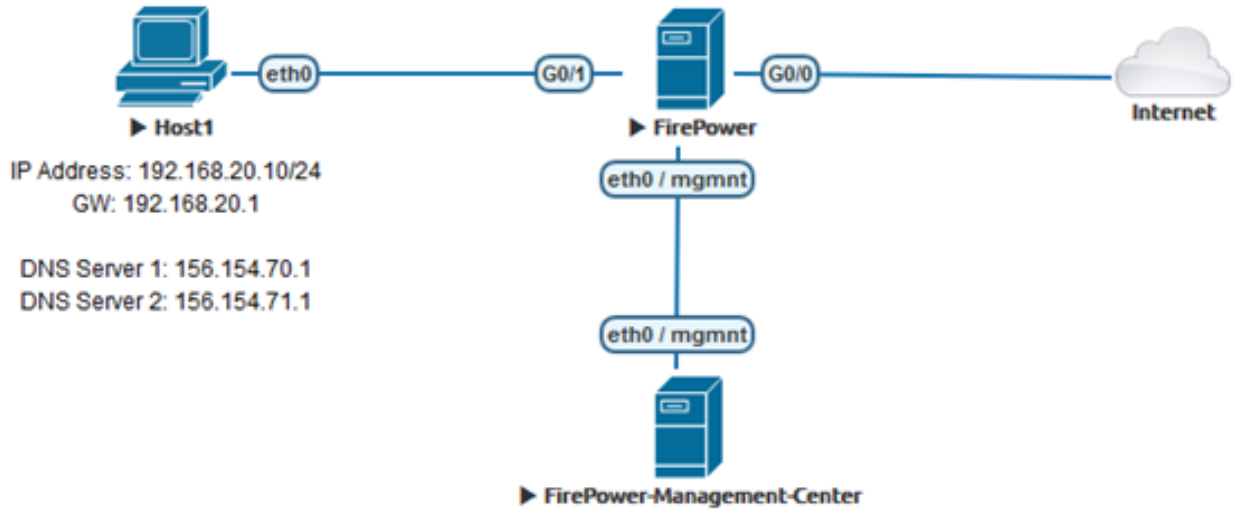
使用的示例塊1域：

- 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。

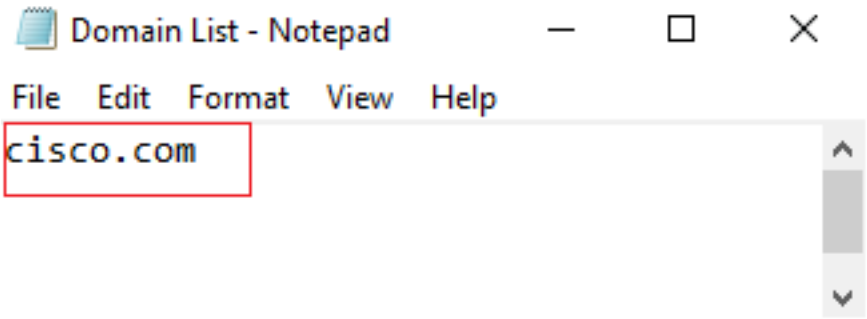
網路圖表



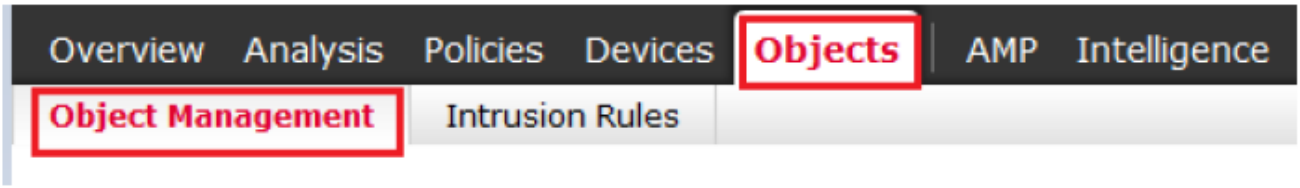
設定

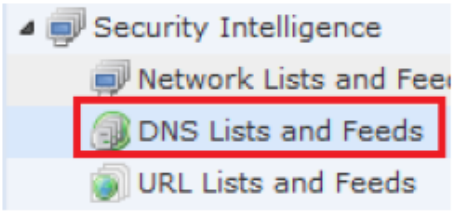
使用要阻止的域配置自定義DNS清單並將清單上傳到FMC

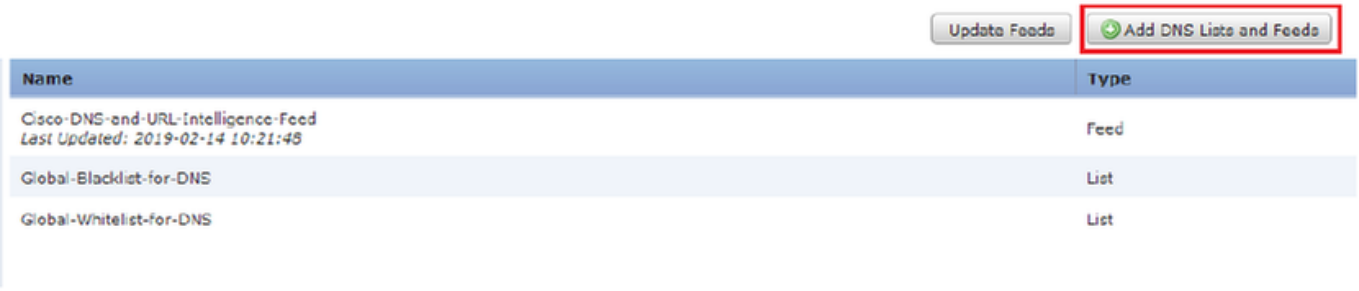
步驟1.使用您要阻止的域建立.txt檔案。在電腦上儲存.txt檔案：



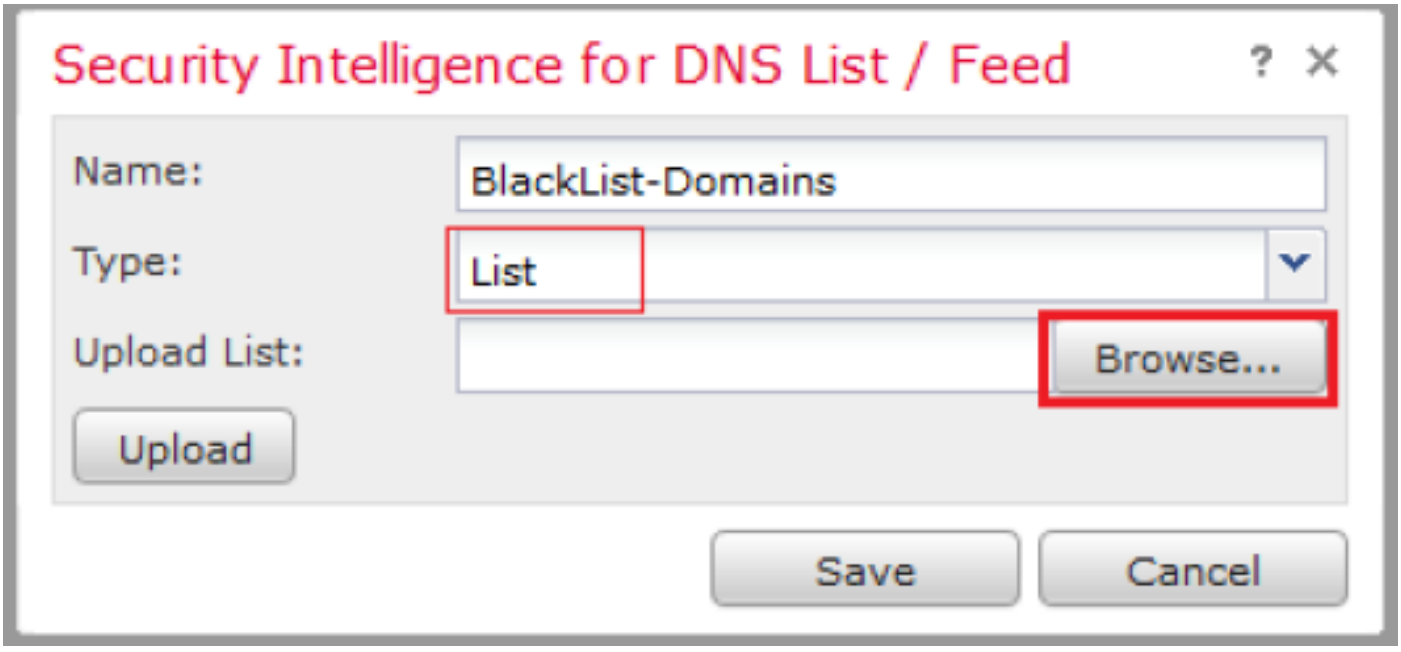
步驟2.在FMC中，導航到Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds。

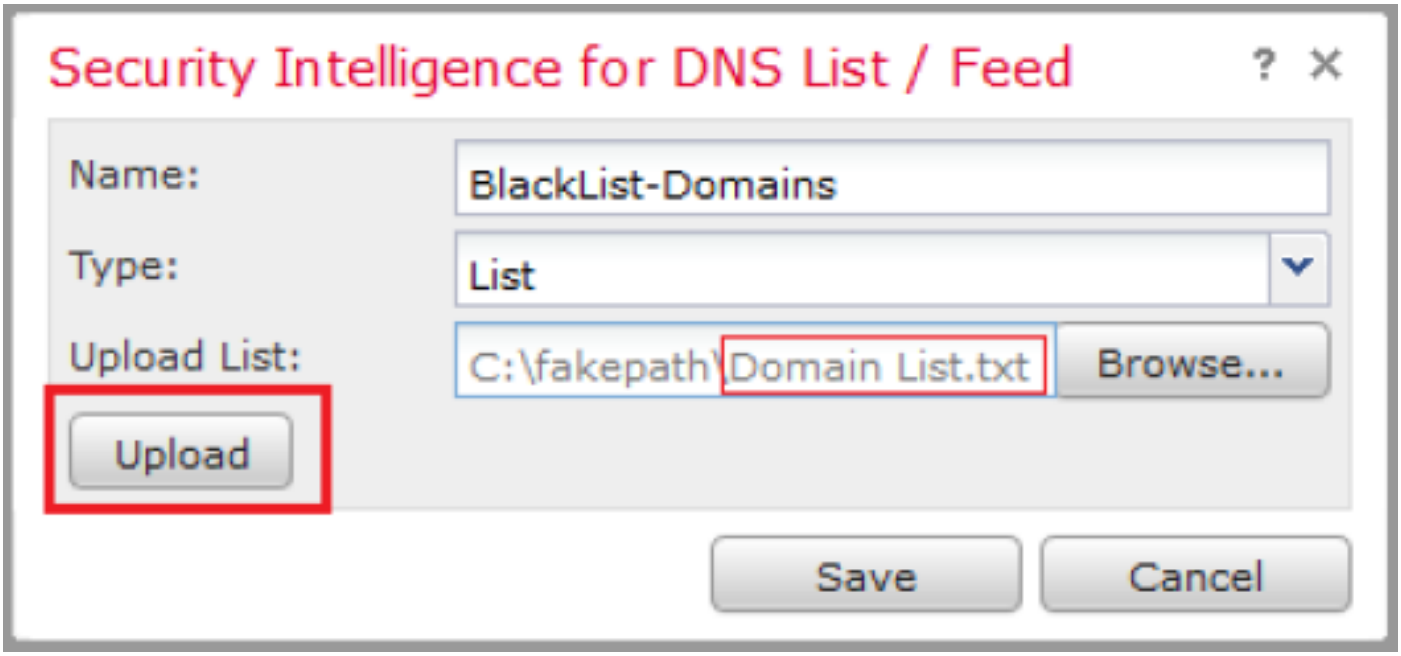




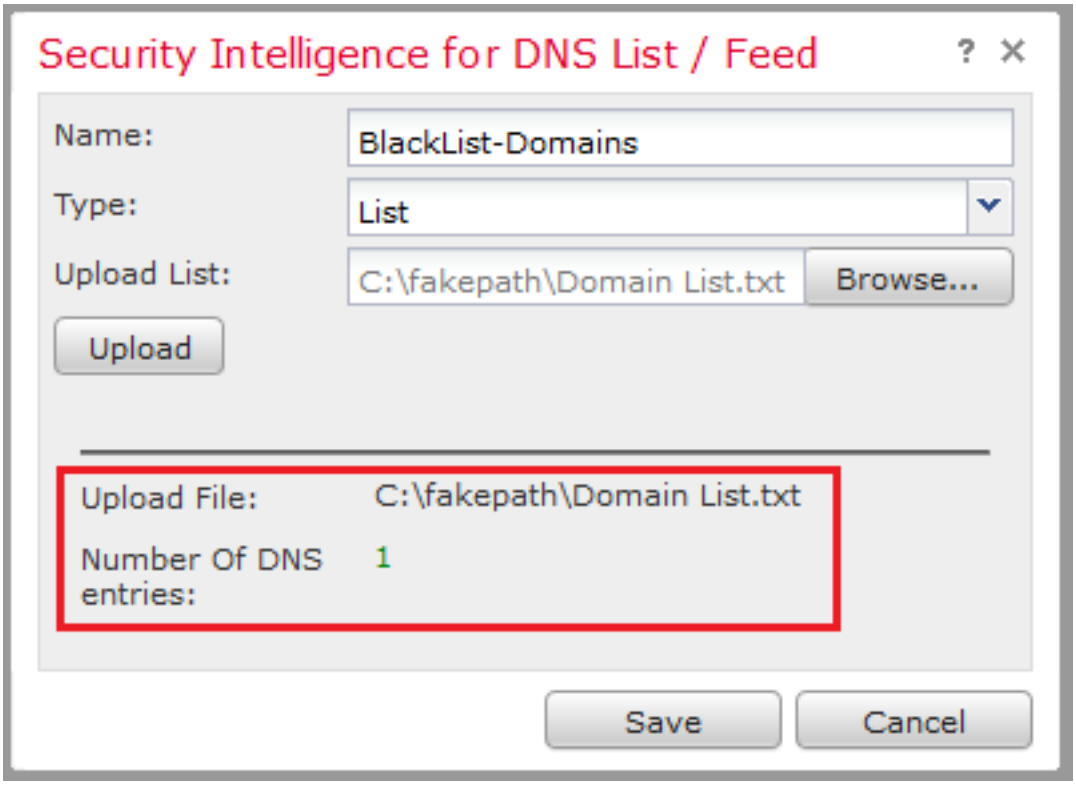


步驟3.建立一個名為「BlackList-Domains」的清單，型別應為list，並且上傳帶有相關域的.txt檔案，如下圖所示：





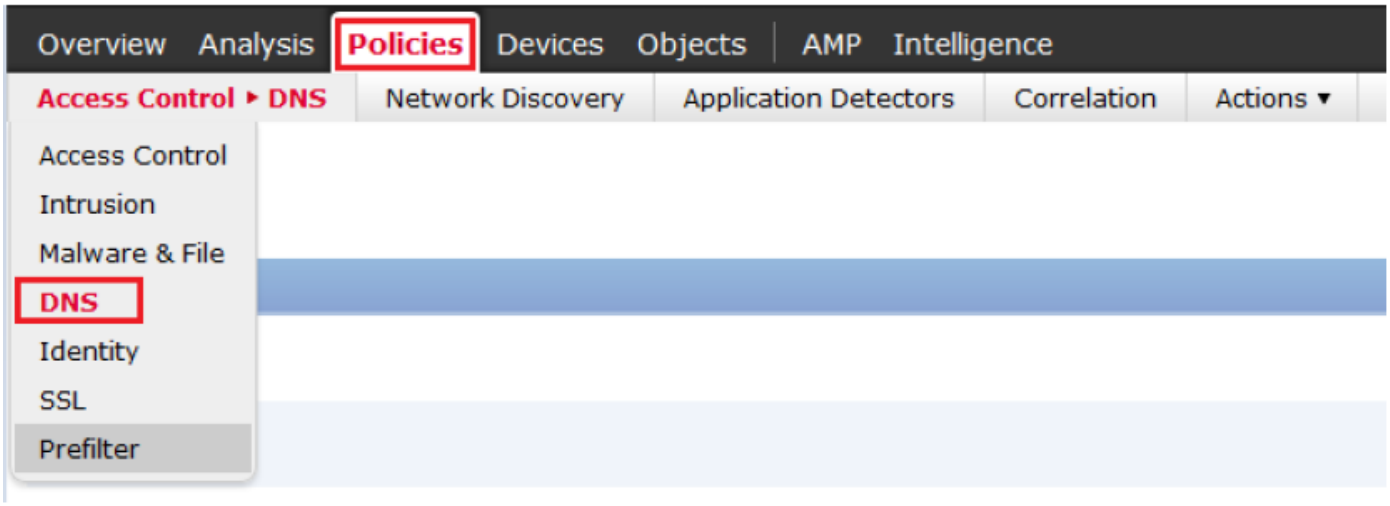
*請注意，上傳.txt檔案時，DNS條目數量應讀取所有域。在此範例中，一共為1:

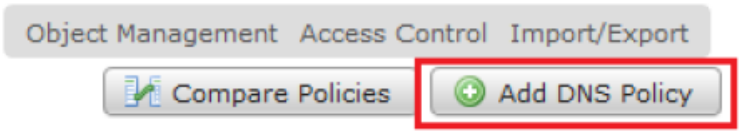


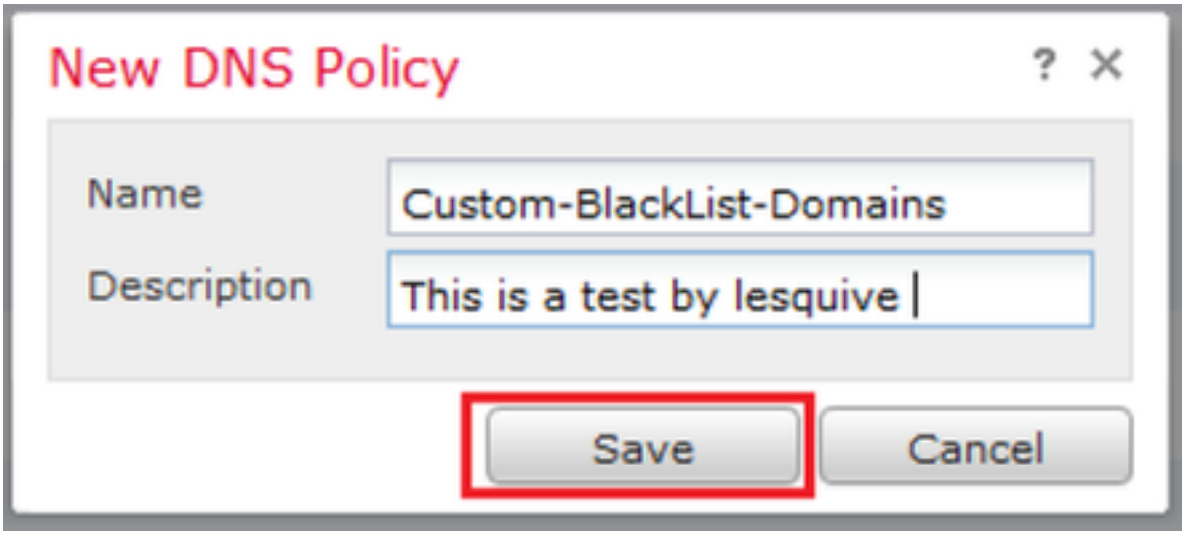
新增一個新的DNS策略，該策略的「操作配置為未找到域」

*確保新增源區域、源網路和DNS清單。

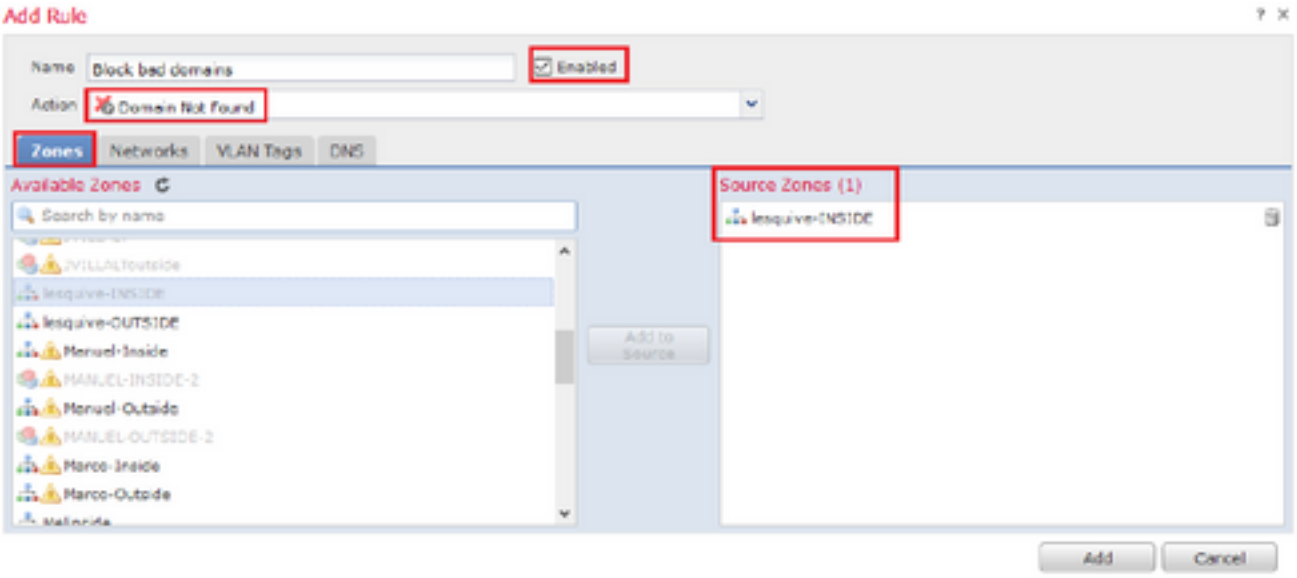
步驟1.導航到Policies >> Access Control >> DNS >> Add DNS Policy:

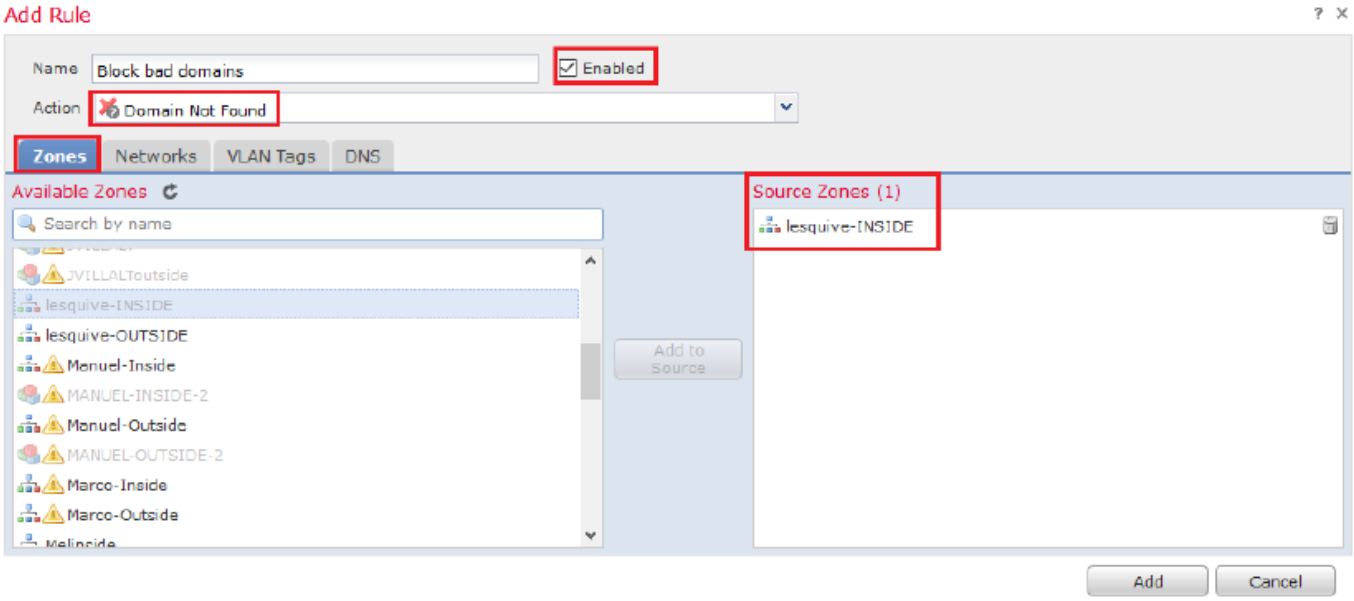


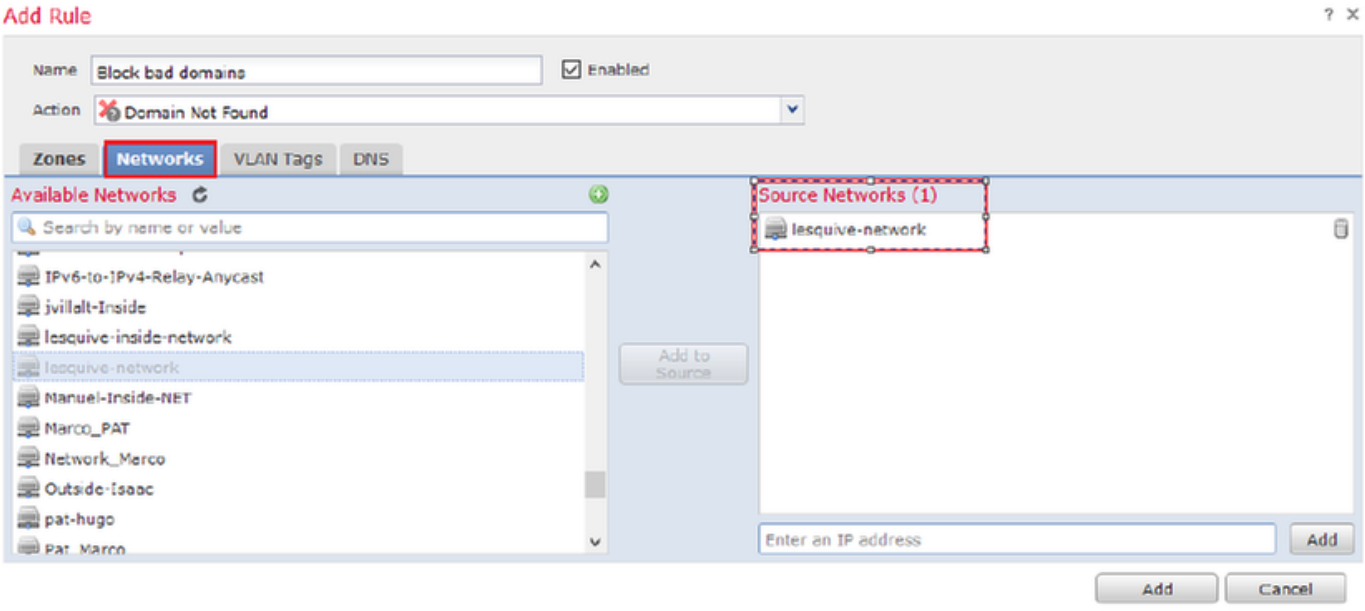


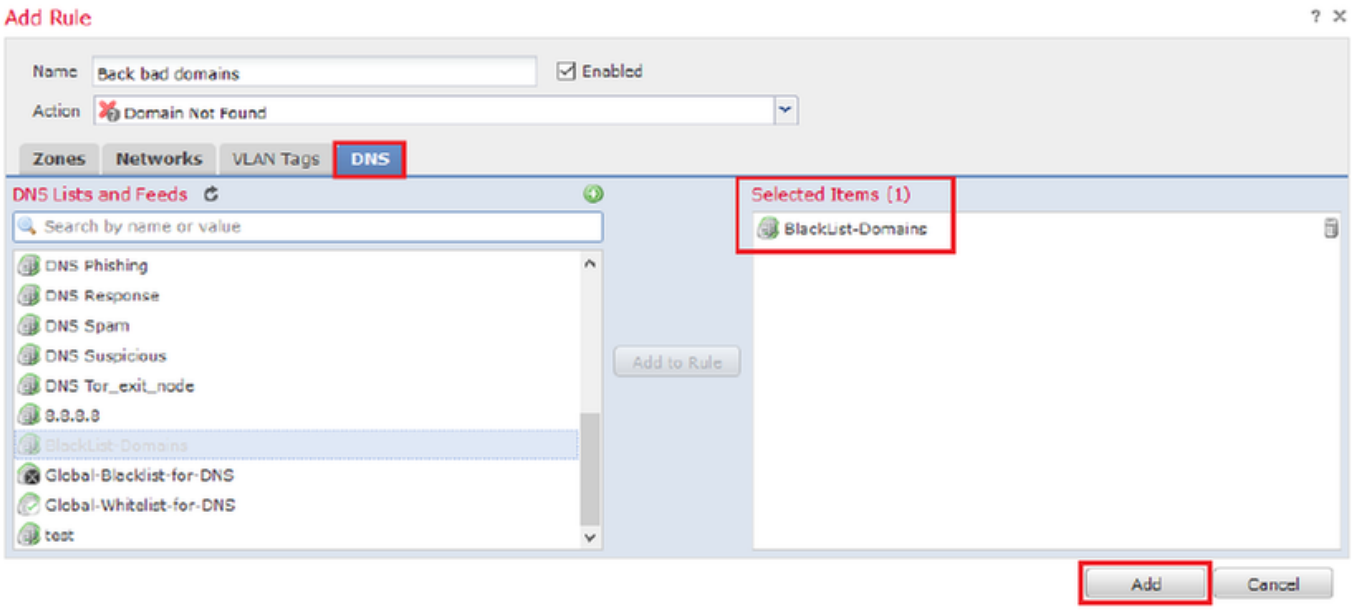


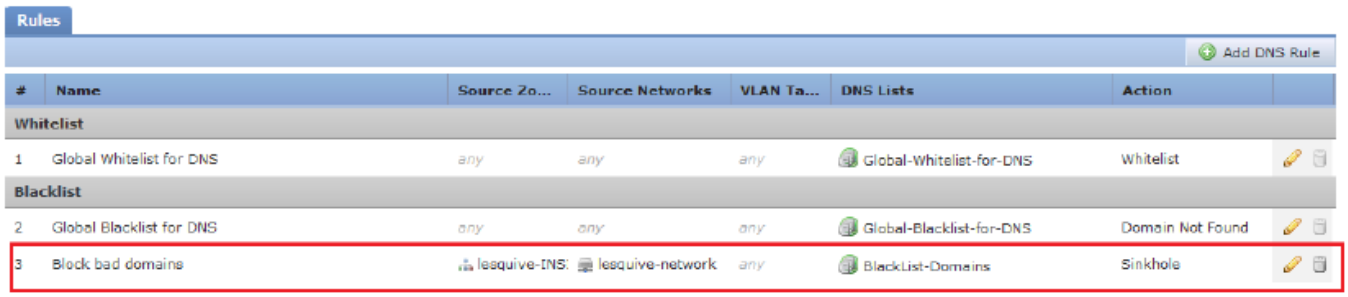
步驟2.新增DNS規則，如下圖所示：


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


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
Source Zones (1)
lesquive-INSIDE
Add to Source
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
Source Networks (1)
lesquive-network
Add to Source
Enter an IP address
Add
Add
Cancel



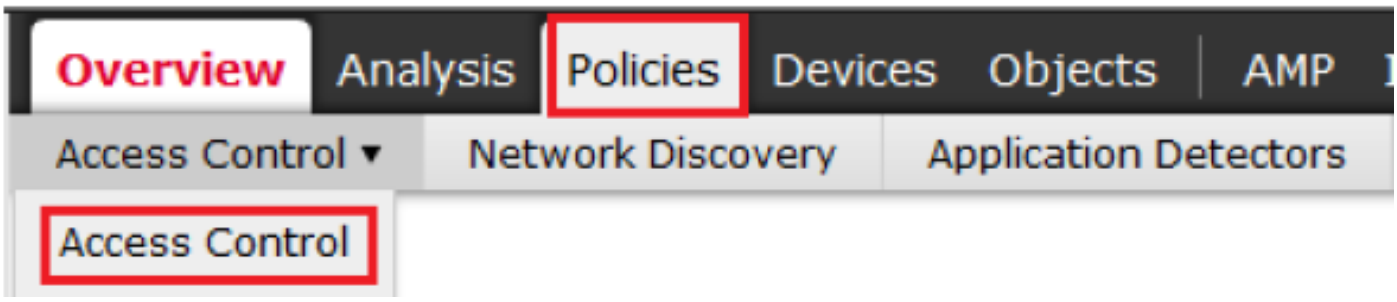


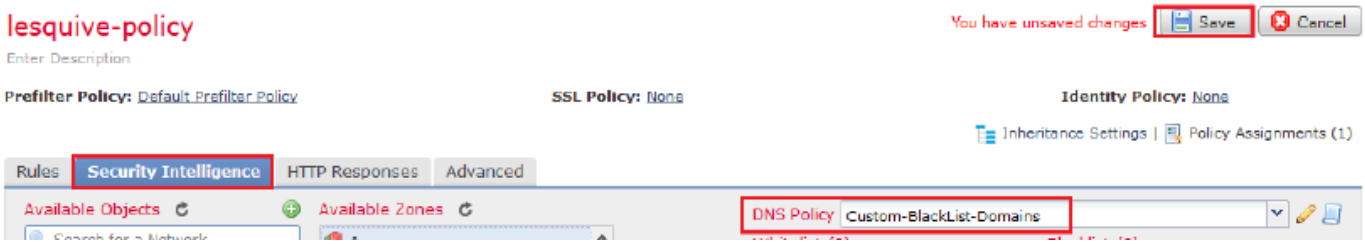
有關規則順序的重要資訊：

- 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。



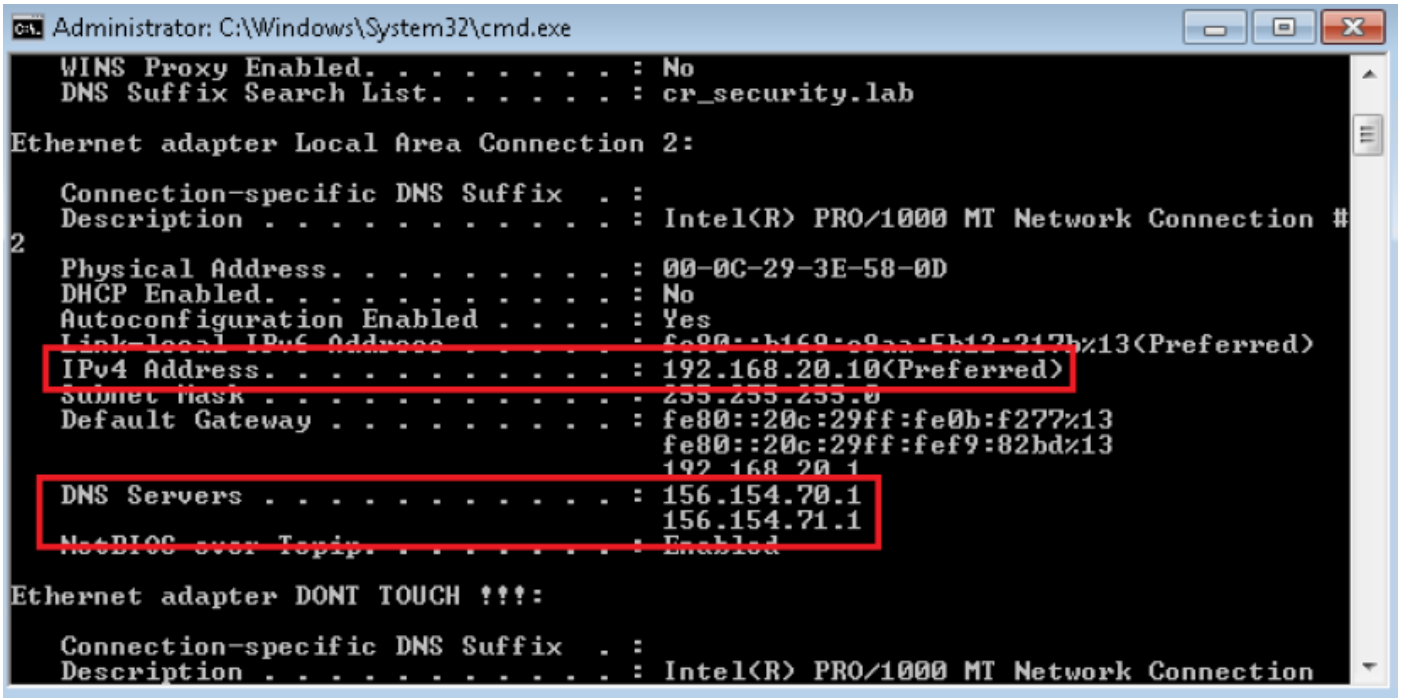


確保完成時部署所有更改。

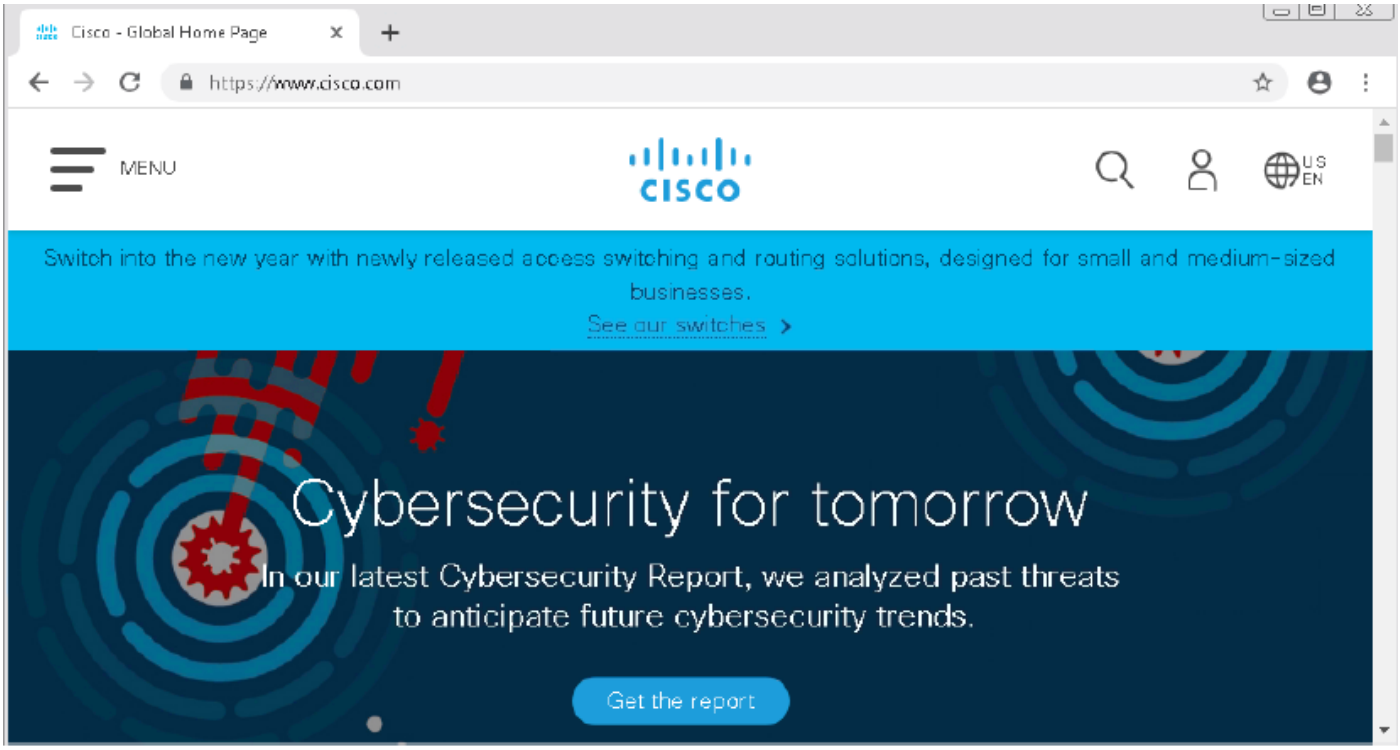
驗證

應用DNS策略之前

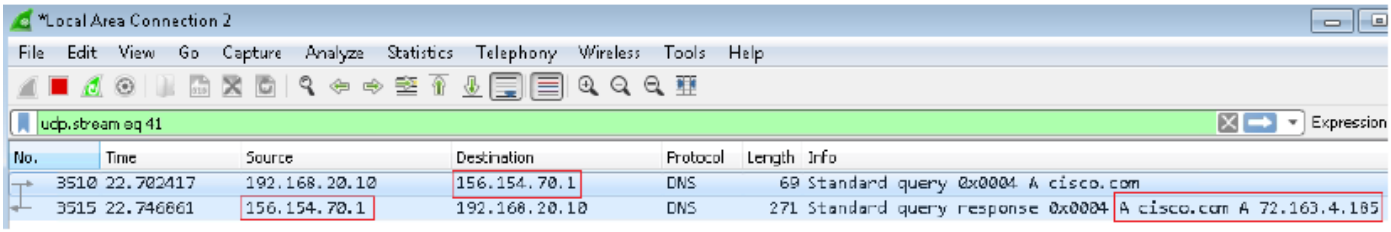
步驟1.檢查主機上的DNS伺服器和IP地址資訊，如下圖所示：

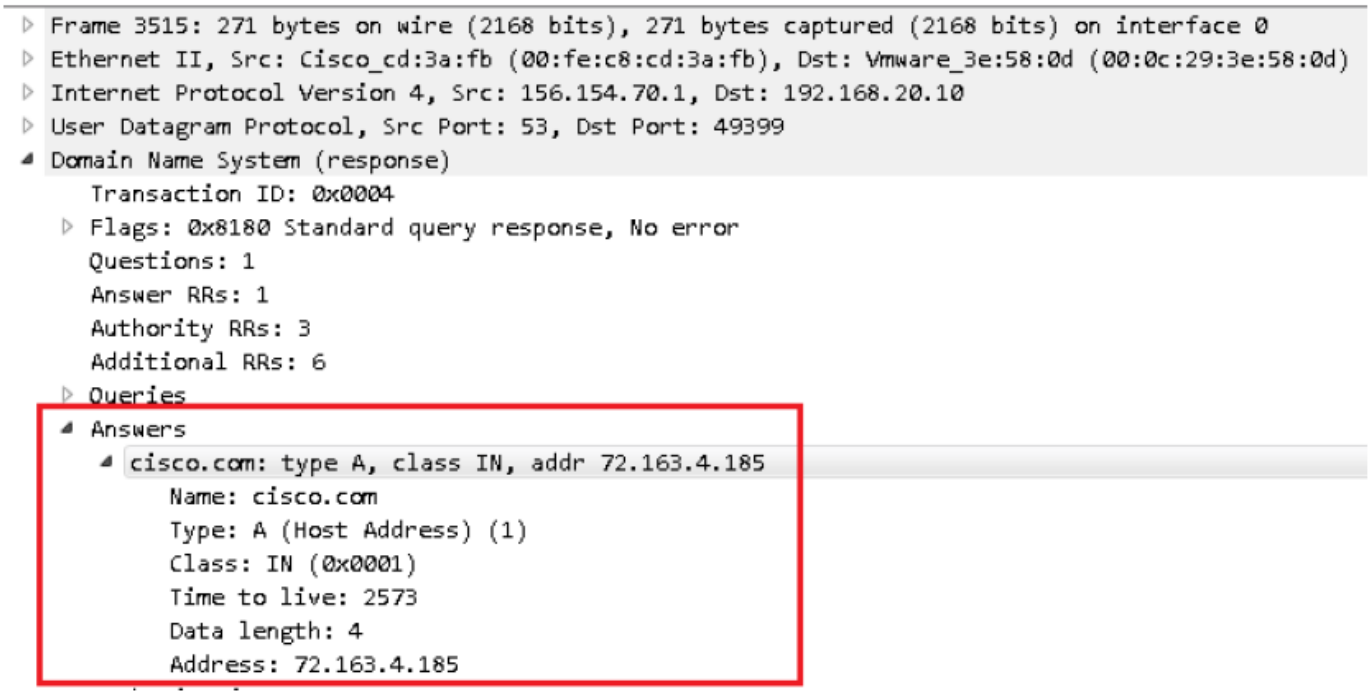


步驟2.確認您可以導覽至cisco.com，如下圖所示：



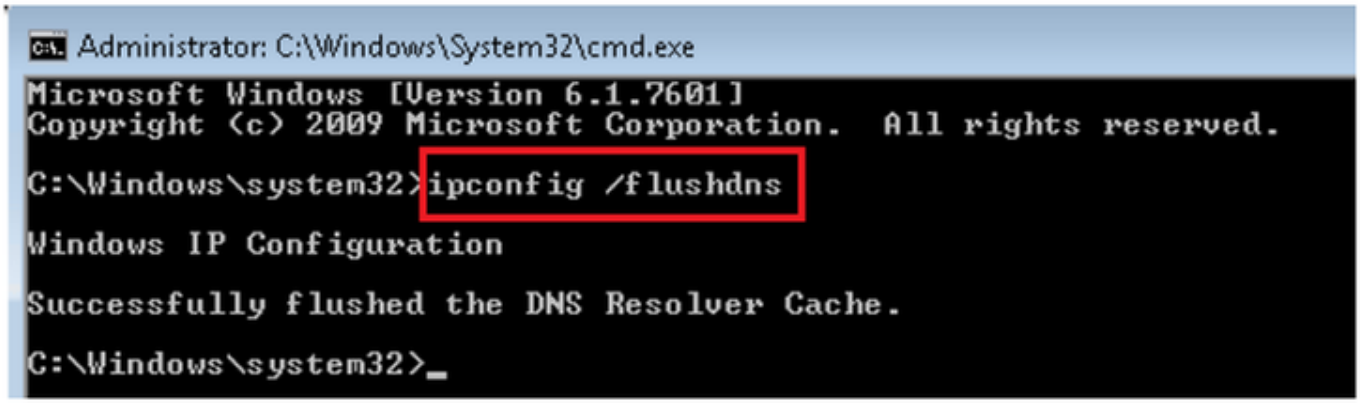
步驟3.使用資料包捕獲確認DNS已正確解析：



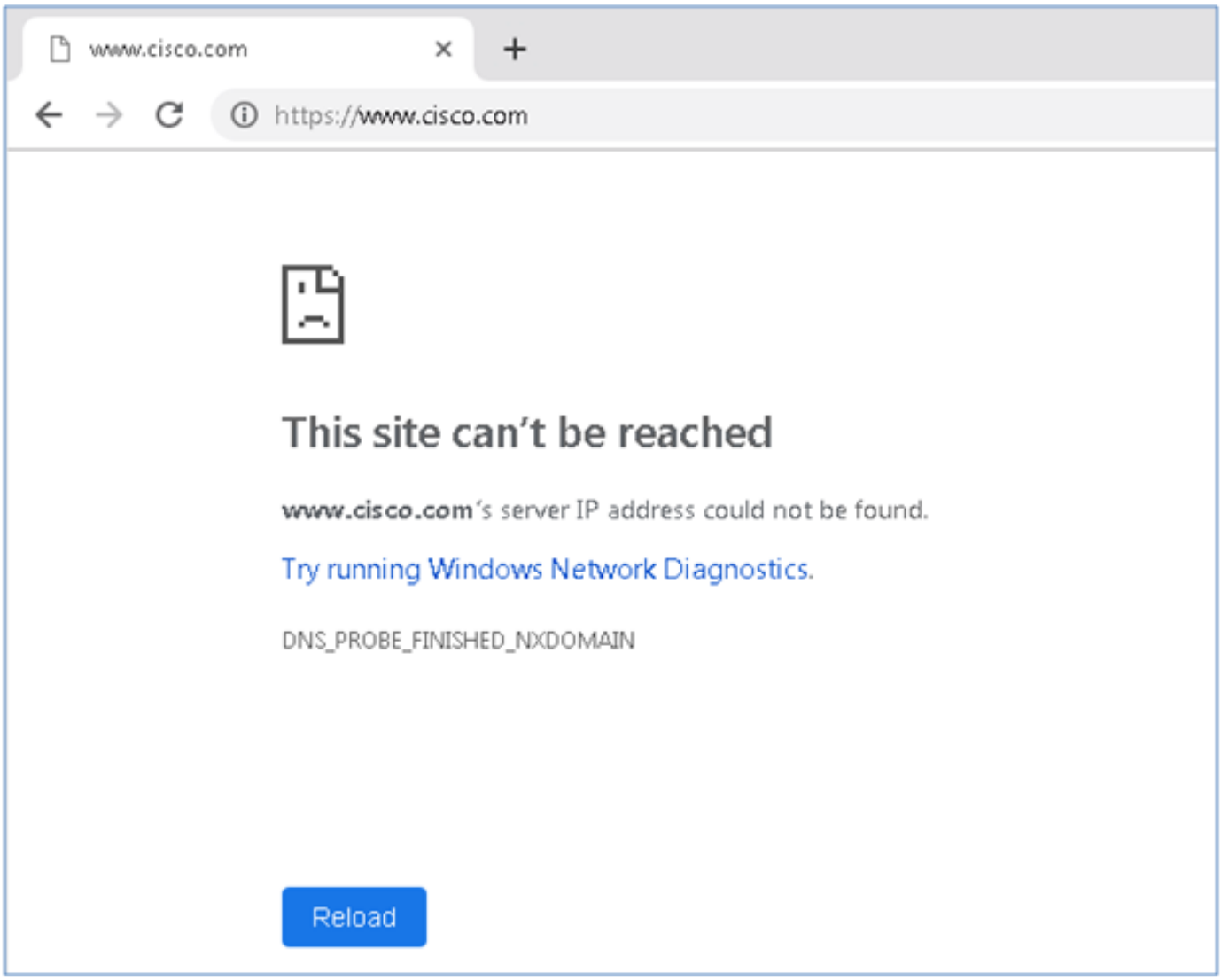


應用DNS策略之後

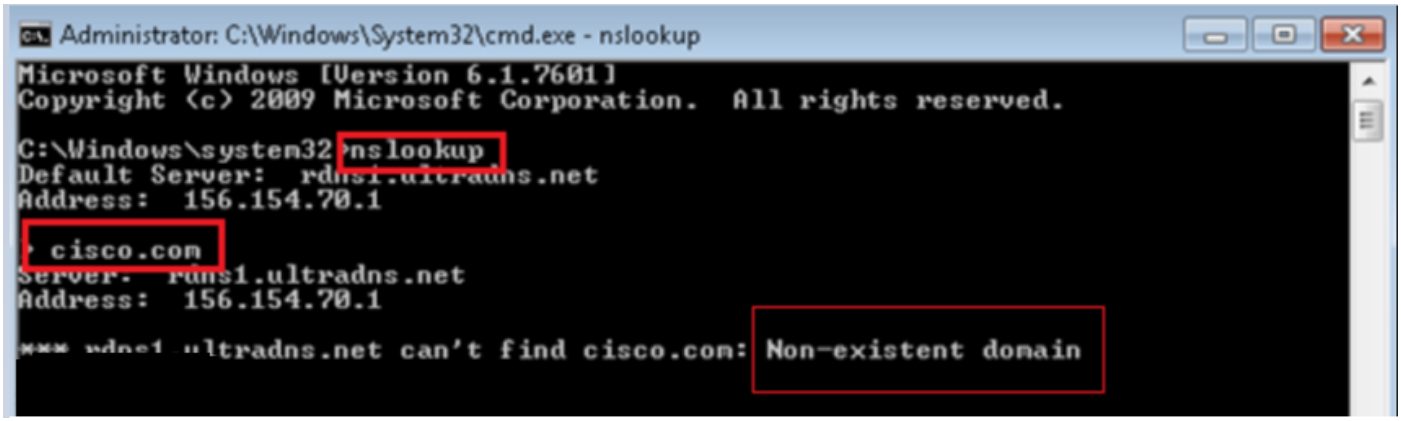
步驟1.使用命令**ipconfig /flushdns清除主機上的DNS快取。**



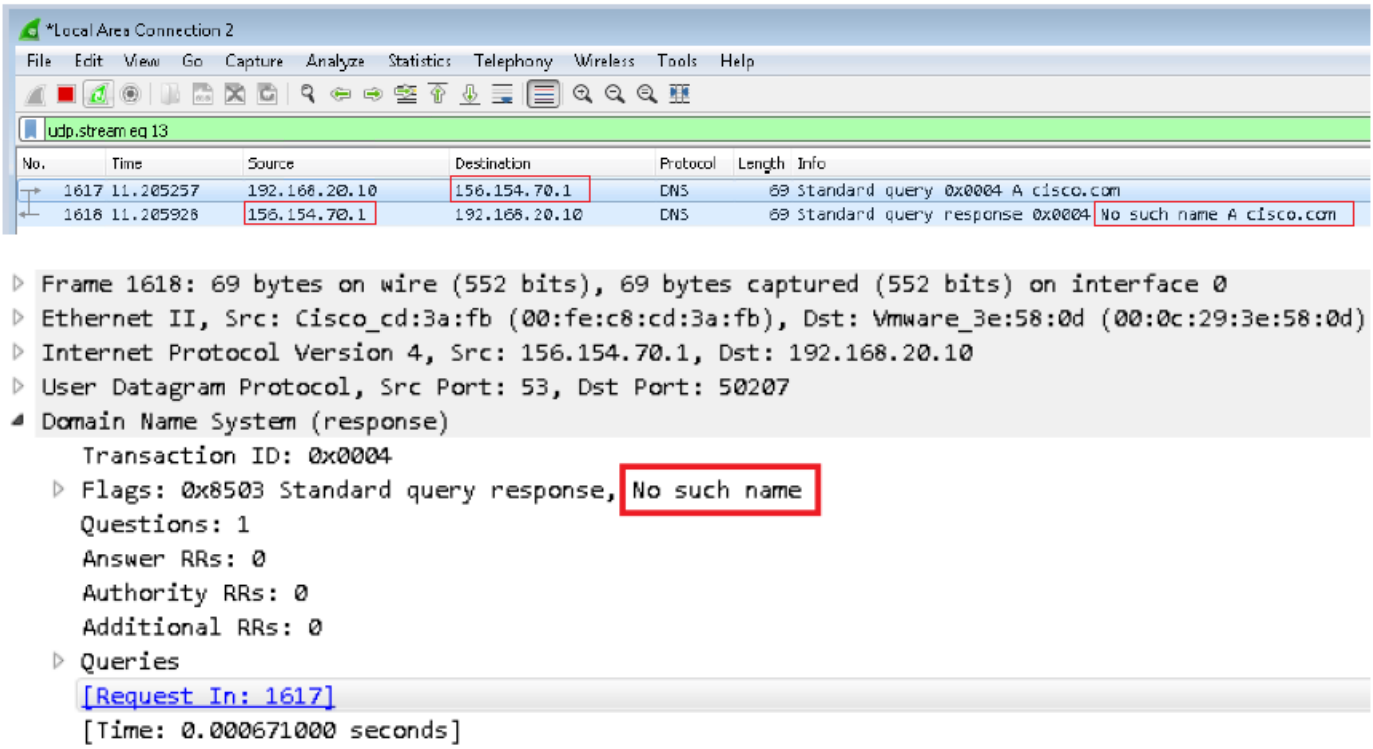
步驟2.使用Web瀏覽器導航至相關域。應該無法連線：



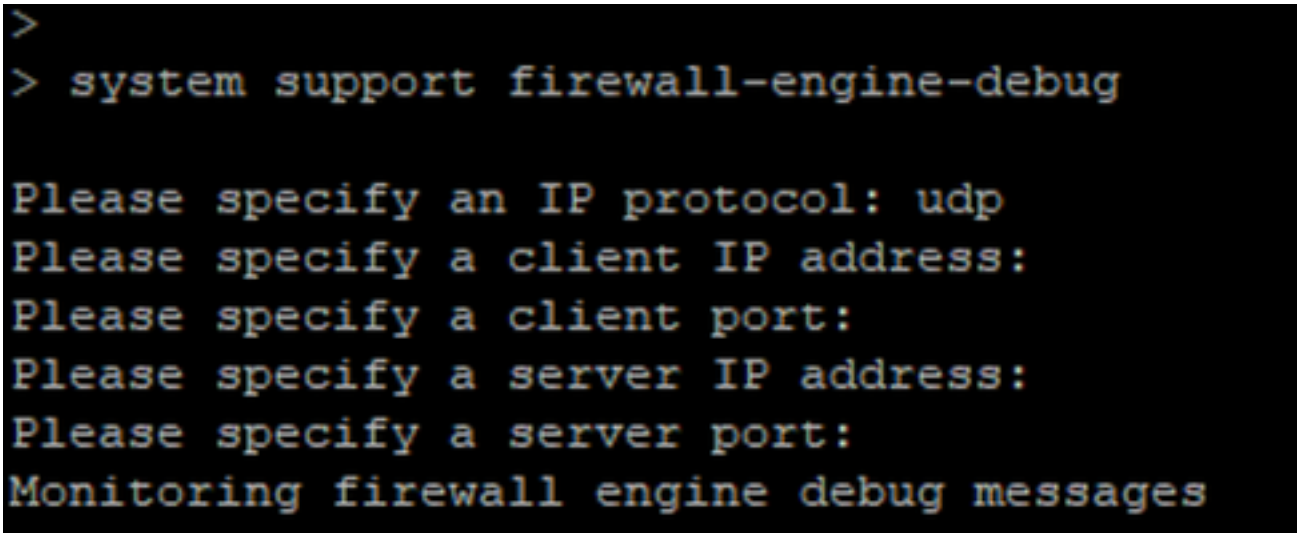
步驟3.嘗試在域cisco.com上發出**nslookup**。名稱解析失敗。



步驟4.封包擷取顯示來自FTD（而不是DNS伺服器）的回應。



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



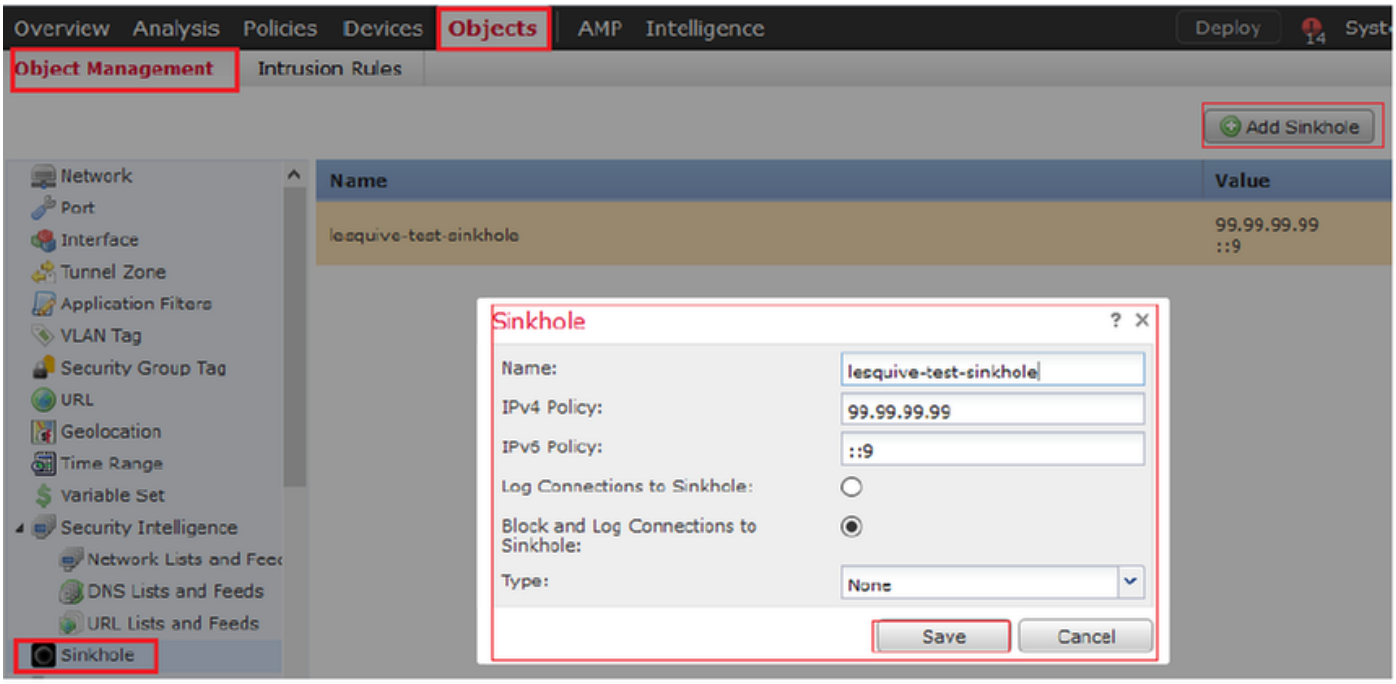
*與cisco.com匹配時的調試：

```
> 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 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
```

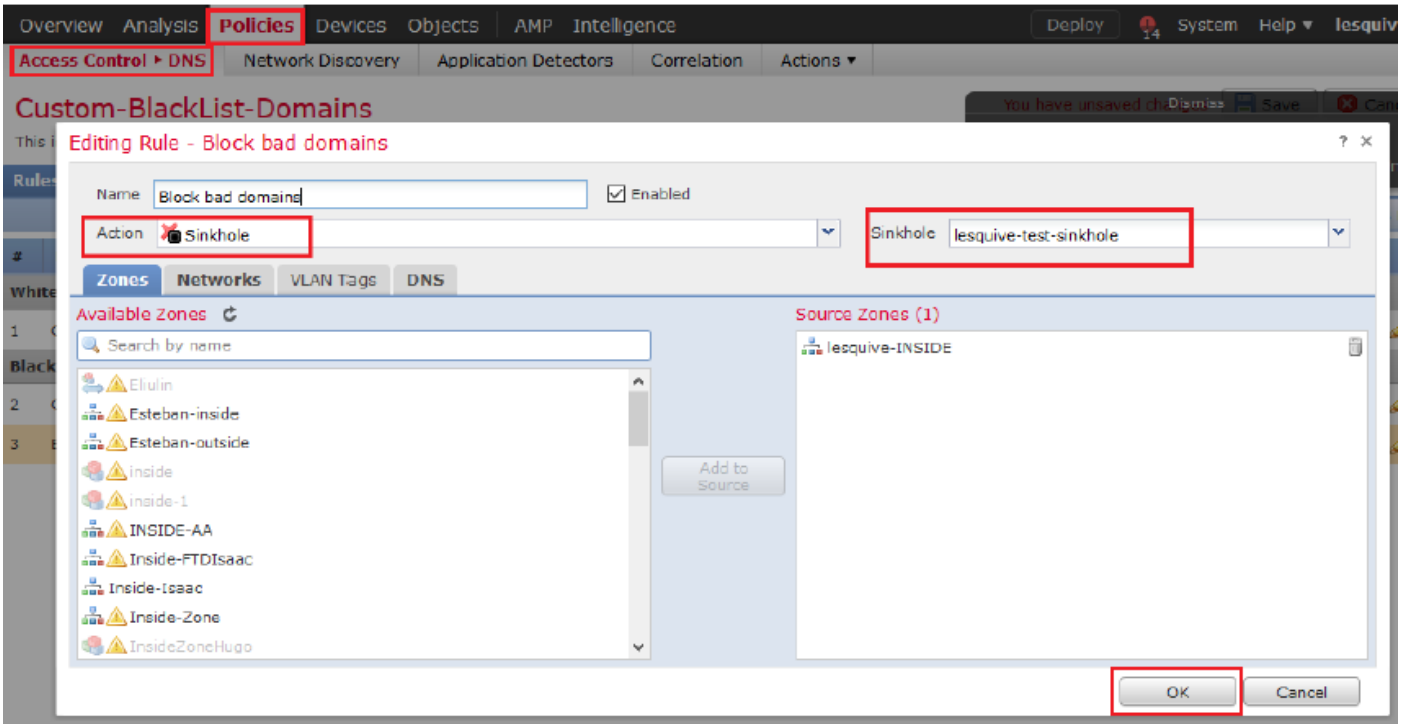
可選的Sinkhole配置

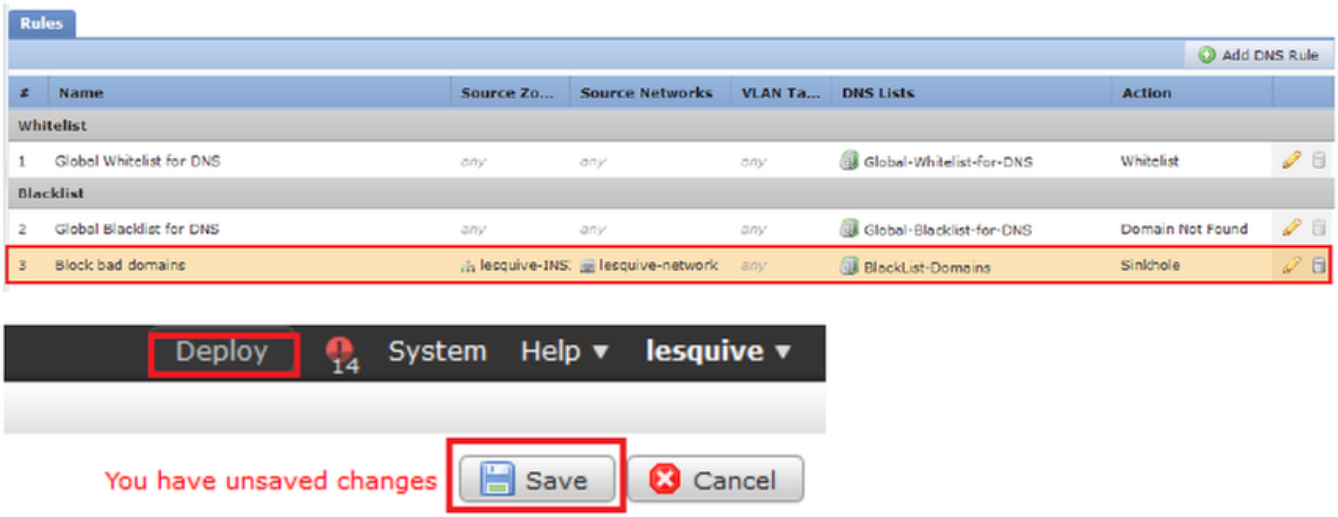
DNS sinkhole是提供虛假資訊的DNS伺服器。它不是對要阻止的域上的DNS查詢返回「無此類名稱」的DNS響應，而是返回一個假IP地址。

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

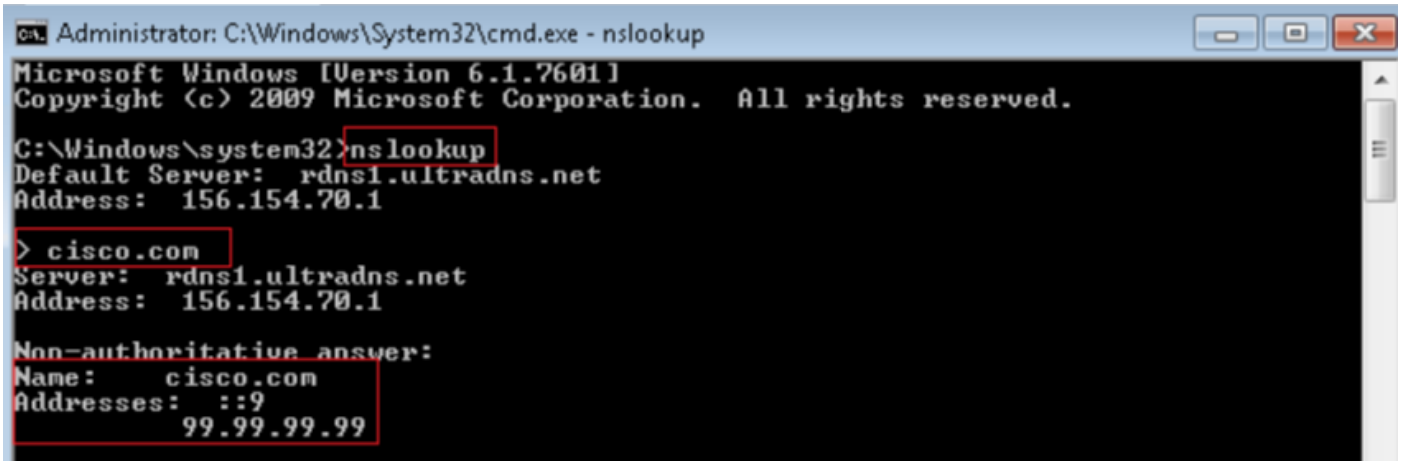


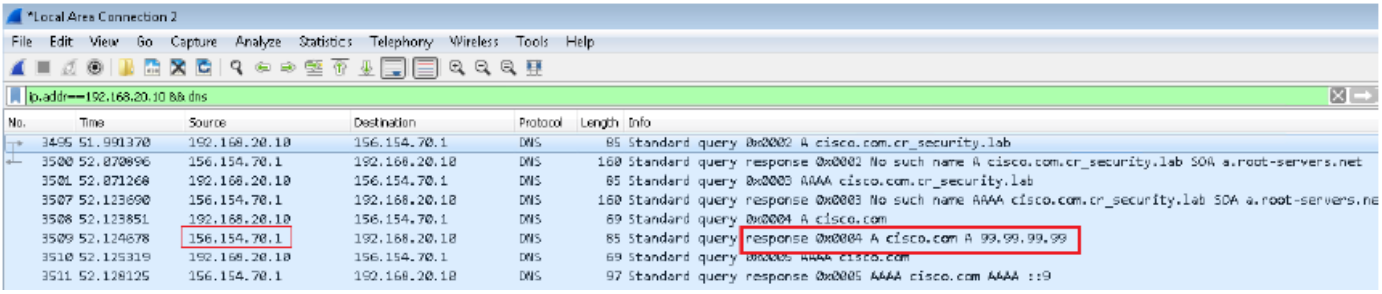
步驟2.將sinkhole套用到DNS原則，並將變更部署到FTD。





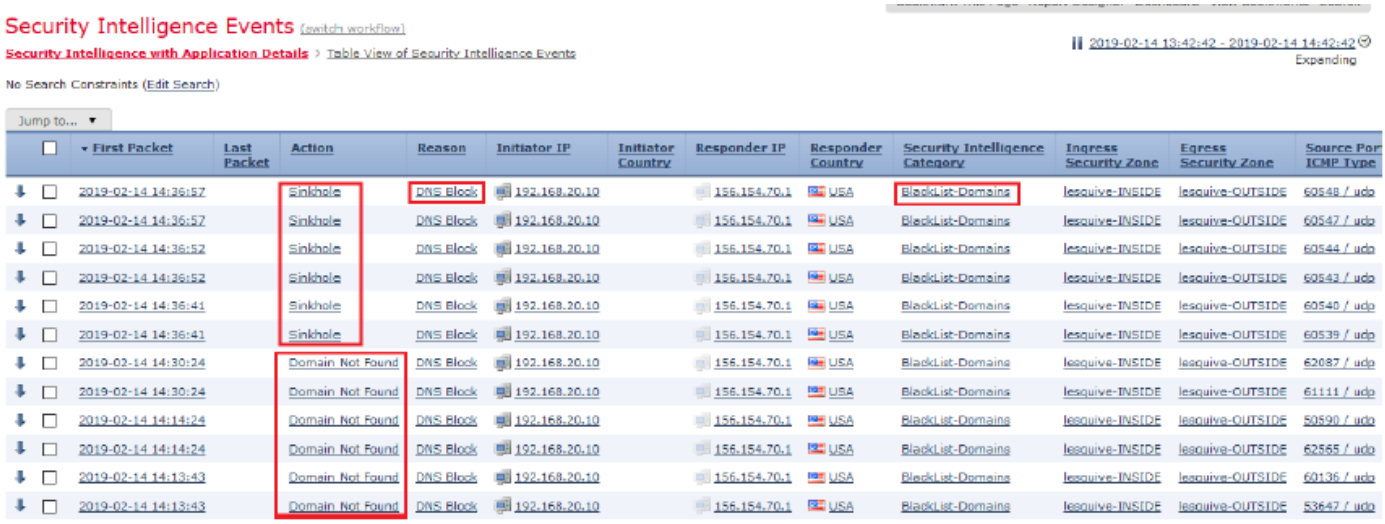
驗證Sinkhole工作正常





疑難排解

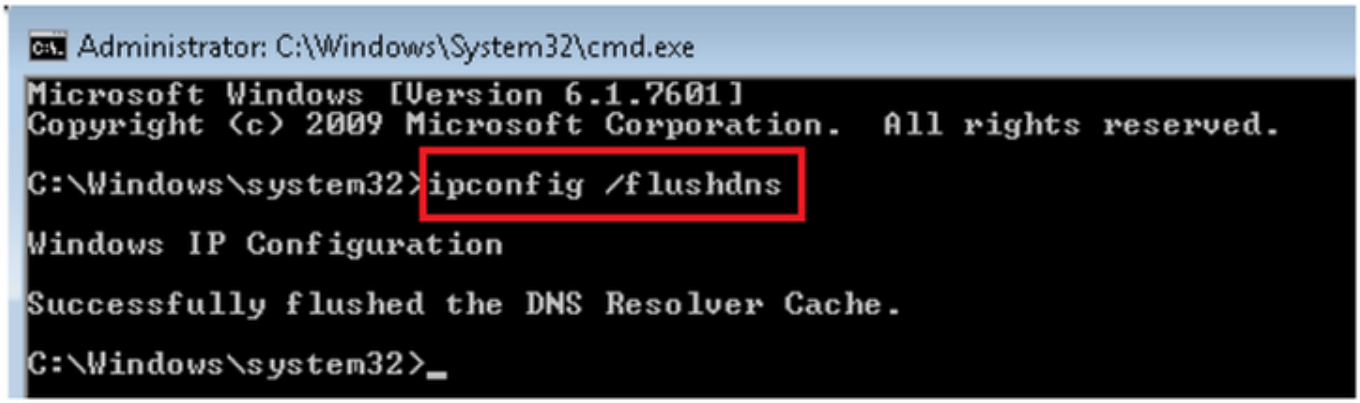
導航到Analysis >> Connections >> Security Intelligence Events以跟蹤SI觸發的所有事件，只要您已在DNS策略中啟用日誌記錄：



您也可以在由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>