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 <u>新增一個新的DNS策略,該策略的「操作配置為未找到域」</u> 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



FirePower-Management-Center

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:

🧾 Domain List - Notepad					—	\times
File	Edit	Format	View	Help		
ciso	co.co	m				^
						- L.

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:

Security Intelli	gence fo	r DNS List / Feed	? ×
Name:	BlackList	-Domains	
Type:	List		~
Upload List:		Brow	se
Upload			
		Save Car	ncel

Security Intelli	gence for DNS List / Feed ? ×
Name:	BlackList-Domains
Type:	List
Upload List:	C:\fakepath\Domain List.txt Browse
Upload	
	Save Cancel

*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:

Name:	BlackList-Domains	
Туре:	List	~
Upload List:	C:\fakepath\Domain List.txt	Browse
Upload File:	C:\fakepath\Domain List.txt	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:

Overview Analy	sis Policies	Devices Objec	ts AMP Intell	gence	
Access Control > I	DNS Networ	k Discovery Ap	plication Detectors	Correlation	Actions 🔻
Access Control					
Intrusion					
Malware & File					
DNS					
Identity					
SSL					
Prefilter					

Object Management	Access C	ontrol	Import/Export
Compare	Policies	٢	Add DNS Policy



步驟2.新增DNS規則,如下圖所示:

Ci Thi Rul	Jstom-BlackList-Domains I is a test by lesquive es					🔚 Sava 🛛 😢 d	Cancel
						🔾 Add D	NS Rule
	Name	Source Zones	Source Networks	VLAN Tags	DNS Lists	Action	
wh	telist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	08
Bla	klist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	J 8

Add Rule



Add Rule



Add Rule

Add Rule			? ×
Name Block bad domains	Enabled		
Action 🎇 Domain Not Found		¥	
Zones Networks VLAN Tags DNS			
Available Networks 🖸	٢	Source Networks (1)	
Search by name or value		📄 lesquive-network	Û
IPv6-to-1Pv4-Relay-Anycast	^	00	
💭 jvillalt-Inside			
lesquive-inside-network			
lesquive-network		to	
Manuel-Inside-NET			
Marco_PAT			
Retwork_Marco	_		
Dutside-Isaac			
pat-hugo		Entor on VD address	
Pat Marco	v	Enter an IP address	Add
			Add Cancel

7 ×

Add Rule

Name Back bad domains	C Enabled		
Action 🐞 Domain Not Found		*	
Zones Networks VLAN Tags DNS			
DNS Lists and Feeds	٥	Selected Items (1)	
Search by name or value		BlackList-Domains	9
I DNS Phishing	^		
DNS Response			
(DNS Spam			
DNS Suspicious	Add to Rule		
DNS Tor_exit_node			
3.8.8.8			
BlackList-Domains			
B Global-Blacklist-for-DNS			
C Global-Whitelist-for-DNS			
(test	¥		
			Add Cancel

Ru	Rules						
						🔇 Add Df	NS Rule
#	Name	Source Zo	Source Networks	VLAN Ta	DNS Lists	Action	
Wh	itelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	a 🕄
Bla	cklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	J 8
3	Block bad domains	🚠 lesquive-INS:	👼 lesquive-network	any	BlackList-Domains	Sinkhole	J 🗍

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。



lesquive-policy

Enter Description

Prefilter Policy: Default Prefilter Policy			SSL Policy: None	Identity Policy: None		
					Ta Inheritan	ce Settings 📑 Policy Assignments (1)
Rules	Security Intelligence	HTTP Responses	Advanced			
Availa	ble Objects 👶	Available Zone	∺s Ĉ		DNS Policy Custom-BlackList-Domains	V / []

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:

C:1.	Administrator: C:\Windows\System32\cmd.exe 📃 🖃 💌
	WINS Proxy Enabled : No DNS Suffix Search List : cr_security.lab
Et	hernet adapter Local Area Connection 2:
2	Connection-specific DNS Suffix .: Description Intel(R) PRO/1000 MT Network Connection #
	Physical Address. : <td:< td=""> <td:< td=""> <td:< td=""></td:<></td:<></td:<>
	Submet Hask
	DNS Servers : 156.154.70.1 156.154.71.1 NotBICC over Topip : Enabled
Et	hernet adapter DONT TOUCH !!!:
	Connection-specific DNS Suffix . : Description : Intel(R) PRO/1000 MT Network Connection 🔻

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:

6 *	Local Area Connection	2						-
File	Edit View Go	Capture Analyze	Statistics	: Telephony V	Mireless To	ools l	Help	
4	🔳 🧟 💿 📗 🛅	X 🖸 I S 🗢	⇒ 🖻 👔		ର୍ବ୍ବ			
	udp.stream eq 41							🔀 📥 💌 Ekpre
No.	Time	Source		Destination	P	otocol	Length	Irfo
T*	3510 22.702417	192.168.20.1	.0	156.154.70.1	0	NS	69	9 Standard query 0x0004 A cisco.com
<u> </u>	3515 22.746661	156, 154, 70, 1		192,168,20,18	, L	ND	271	. Standard query response 0x0004 A cisco.com A 72.185.4.
⊳	Frame 3515:	271 bytes	on wir	e (2168 bi	ts), 21	71 by	/tes c	captured (2168 bits) on interface Ø
⊳	Ethernet II	, Src: Cisc	o_cd:3	a:fb (00:f	e:c8:c0	1:3a	:fb),	Dst: Vmware_3e:58:0d (00:0c:29:3e:58:0d
\triangleright	Internet Pr	otocol Vers	ion 4,	Src: 156.	154.70	1,[)st: 1	192.168.20.10
\triangleright	User Datagr	am Protocol	, Src	Port: 53,	Dst Por	•t: 4	19399	
4	Domain Name	System (re	sponse)				
	Transact:	ion ID: ØxØ	004					
	Þ Flags: Ø	x8180 Stand	ard que	ery respon	se, No	erro	or .	
	Question	s: 1						
	Answer R	Rs: 1						
	Authority	y RRs: 3						
	Addition	al RRs: 6						
	Oueries							_
	Answers							
	▲ cisco.	.com: type	A, clas	ss IN, add	r 72.10	3.4.	185	
	Nan	ne: cisco.c	om					
	Tvr	e: A (Host	Addres	s) (1)				
	cla	ass: IN (0x	0001)	-, (-,				
	Tin	ne to live:	2573					
	Dat	a length:	4					
	Ado	ress: 72.1	63.4.18	35				
		•						

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。



步驟4.封包擷取顯示來自FTD(而不是DNS伺服器)的回應。

4	*Local Area Connectio	n 2							
File	e Edit View Go	Capture Analyze Stati:	tics Telephony Wireless	Tools	Help				
	📕 🛃 💿 🛄 📠	े 🕅 🖸 । ९ 🗢 🗢 🕾	🖗 🕹 🚍 🗐 ପ୍ ପ୍	Q. 🎹					
	udplistreamleg 13								
No.	Time	Source	Destination	Protocol	Length Info				
7	1617 11.205257	192.168.20.10	156.154.70.1	DNS	69 Standard	d query 0x0004 i	A cisco.com	n	_
4	1618 11.205928	156.154.70.1	192.168.20.10	DNS	69 Standard	d query response	≥ 0x0004 No	o such name A cisco.co	n
⊳F	-rame 1618:	69 bytes on wir	e (552 bits), 6	9 byte	s captured	(552 bits)	on inte	erface Ø	
⊳E	Ethernet II,	Src: Cisco cd:	3a:fb (00:fe:c8	:cd:3a	:fb), Dst:	Vmware Be:	58:0d ((00:0c:29:3e:58:	Ød)
▶ :	Internet Pro	tocol Version 4	. Src: 156.154.	70.1.	Dst: 192.16	8.20.10			
	lser Datagra	m Protocol, Src	Port: 53. Dst	Port:	50207				
21	Domain Name	Suctor (nocrore	-) -)		50207				
	Zunain Name	System (respons	e)						
	Iransacti	on ID: 0x0004							
	▷ Flags: Øx	8503 Standard q	uery response,	No suc	h name				
	Questions	: 1							
	Answer RR	s: 0							
	Authority	RRs: 0							
	Additiona	1 BB5: Ø							
	Dueries								
	P Quer res	Te. 16171							
	LKequest	TU: 101/]							
	[Time: 0.	000671000 secon	ds]						

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:

<pre>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 IP address: 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 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 192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Got end of flow event from hardware with flags 0000000 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 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 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 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 DNS SI shared mem lookup returned 1 for cisco.com.cr_security.lab 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.cr_security.lab 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 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 UNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 UNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 UNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 UNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 UNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1</pre>
<pre>Please specify a client IP address: Please specify a client port: Please specify a server IP address; 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 A5 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 A5 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 A5 1 I 0 Got end of flow event from hardware with flags 0000000 192.168.20.10-61374 > 156.154.70.1-53 17 A5 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 A5 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 A5 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 A5 1 I 1 DNS SI shared mem lookup for cisco.com.cr_security.lab 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Skirping Science first with inffs 1 -> 0, vlan 0 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain</pre>
<pre>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 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 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 for cisco.com.cr_security.lab 192.166.20.10-61374 > 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 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 192.166.20.10-61374 > 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 192.166.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Starting SrcZone first with intfs 1 -> 0, vian 0 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 1, id 1 action Allow 192.166.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.166.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain</pre>
<pre>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 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 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 192.160.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab 192.160.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup returned 1 for cisco.com 192.160.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup returned 1 for cisco.com 192.160.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipring SroZone first with intfs 1 -> 0, vian 0 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 1, id 1 action Allow 192.166.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.160.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain</pre>
<pre>Please specify a server port: Montroring firewall engine debug messages 192.168.20.10-61373 > 156.154.70.1-53 17 A5 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.or_security.lab 192.168.20.10-61373 > 156.154.70.1-53 17 A5 1 I 0 Skipping DNS rule lookup for cisco.com.or_security.lab since we've already gotten a response 192.168.20.10-61373 > 156.154.70.1-53 17 A5 1 I 0 Got end of flow event from hardware with flags 0000000 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 DNS SI shared mem lookup returned 0 for cisco.com.or_security.lab 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 DNS SI shared mem lookup returned 0 for cisco.com.or_security.lab 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 DNS SI shared mem lookup returned 0 for cisco.com.or_security.lab 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup for cisco.com.or_security.lab since we've already gotten a response 192.168.20.10-61374 > 156.154.70.1-53 17 A5 1 I 1 Skipping DNS rule lookup for cisco.com.or_security.lab since we've already gotten a response 192.160.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Got end of flow event from hardware with flags 00000000 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Starting SrcDone first with intfs 1 -> 0, vlan 0 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 1, id 1 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain</pre>
<pre>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 0000000 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 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 DNS SI shared mem lookup for cisco.com.cr_security.lab 192.166.20.10-61374 > 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 192.166.20.10-61374 > 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 192.166.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 0000000 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, vian 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 NKDemain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NKDemain</pre>
<pre>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 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 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 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com 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 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 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 2, id 3 action DNS NXDomain</pre>
<pre>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 0000000 192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup for cisco.com.cr_security.lab 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 192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 0000000 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 0000000 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 0000000 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 0000000 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Starting SroZone first with intfs 1 -> 0, vian 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 2, id 3 action DNS NXDomain</pre>
<pre>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 Sot end of flow event from hardware with flags 0000000 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 Skipping DNS rule lookup 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 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Skipping Science 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 NKDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NKDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NKDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NKDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NKDomain</pre>
<pre>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 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response 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 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 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 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 Using rule order for the flow with flags 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 2, id 3 action DNS NXDomain 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 2, id 3 action DNS NXDomain 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 2, id 4 for the DNE NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 4 for the DNE NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 4 for the DNE NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 4 for the DNE NXDOMain 193.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 4 for the DNE NXDOMain 193.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 4 for the DNE</pre>
<pre>192.168.20.10-61374 > 156.154.70.1-53 17 A3 1 I 1 DN3 SI shared mem lookup returned 0 for cisco.com.cr security.lab 192.168.20.10-61374 > 156.154.70.1-53 17 A3 1 I 1 Skipping DN3 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 A3 1 I 1 Got end of flow event from hardware with flags 00000000 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 DN3 SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 DN3 SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 DN3 SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 1, id 1 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DN3 NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DN3 NXDomain</pre>
<pre>192.168.20.10-61374 > 156.154.70.1-53 17 A3 1 I 1 Skipping DNS rule lookup for cisco.com.or security.lab since we've already gotten a response 192.168.20.10-61374 > 156.154.70.1-53 17 A3 1 I 1 Got end of flow event from hardware with flags 00000000 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 DNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 Sot end of flow event from hardware with flags 0000000 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 Sot end of flow event from hardware with flags 00000000 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 Starting SrcZone first with intfs 1 -> 0, vian 0 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 1, id 1 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NKDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NKDomain</pre>
<pre>192.168.20.10-61374 > 156.154.70.1-53 17 A3 1 I 1 Got end of flow event from hardware with flags 00000000 192.168.20.10-61375 > 156.154.70.1-53 17 A3 1 I 1 DNS SI shared mem lookup returned 1 for cisc.com 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 Starting SrcZone first with intfs 1 -> 0, vlan 0 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 1, id 1 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain 192.168.20.10-61375 > 156.154.70.1-53 17 A5 1 I 1 using rule order 2, id 5 action DNS NXDomain</pre>
192.168.20.10-61375 > 156.154.70.1-53 17 Å3 1 I 1 DNS SI shared mem lookup returned 1 for cisco.com 192.168.20.10-61375 > 156.154.70.1-53 17 Å5 1 I 1 Starting SrcZone first with intfs 1 -> 0, vlan 0 192.168.20.10-61375 > 156.154.70.1-53 17 Å5 1 I 1 using rule order 1, id 1 action Allow 192.168.20.10-61375 > 156.154.70.1-53 17 Å5 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 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 192.68.20.10-61375 > 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 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 A5 1 I 1 using rule order 2, id 3 action DNS NXDomain
101 100 10 CLIPTE & LEG
192.166.20.10-613/5 > 156.154.70.1-53 17 AS 1 1 1 using rule order 5, 10 5 action DNS NADOMAIN
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got DWS 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。

Overview Analysis	Policies	Devices	Objects	AMP	Intelligence			Deploy	ng Syst
Object Management	Intrusi	ion Rules							
								S Add	Sinkhole
Network	^	Name						Value	
J [®] Port								99,99,99	9,99
A Interface		lesquive-tes	t-sinkhole					::9	
and Tunnel Zone									
Application Filters			Sinkh	ole			? X		
📎 VLAN Tag				CTC.			_		
Security Group Tag			Name	:		lesquive-test-sinkhole			
URL			IPv4 P	Policy:		99.99.99.99			
Geolocation			IPv6 P	Policy:		::9			
Time Range			log C	opportion	s to Sinkholes	0			
Ş Variable Set			Log C		is to sinknole.	0			
4 Security Intelligence	•		Block	and Log (ole:	Connections to	۲			
Network Lists and	d Feer		Type:				~		
DNS Lists and Fee	eds		type.			None			
URL Lists and Fee	eds					Save Can	cel		
Sinkhole									

步驟2.將sinkhole套用到DNS原則,並將變更部署到FTD。

Over	rview Analysis Policies Devices Objects AMP Intelligence	Deploy 🧛 System Help	r lesquiv
Acce	ss Control > DNS Network Discovery Application Detectors Correlation	n Actions 🔻	
Cus	stom-BlackList-Domains	You have unsaved chalismiss 📃 Save	🛛 🐹 Can
This i	Editing Rule - Block bad domains		? ×
Rules #	Name Block bad domains I Enabled Action Conces Networks VLAN Tags DNS	Sinkhole lesquive-test-sinkhole	*
1 (Available Zones 🖸	Source Zones (1)	
Black	Search by name	esquive-INSIDE	1
2 C	A Eliulin Esteban-outside Inside Inside-1 Inside-FTDIsaac Inside-Isaac Inside-Isaac Inside-Isaac Inside-Isaac Inside-Isaac Inside-Isaac		
		OK Can	cel

ONS Rule
P 8
P 8
1 6



驗證Sinkhole工作正常



4	Local Area Connection	2			
File	Edit View Go	Capture Analyze Stati	stics Telephony Wireless	Tools I	Help
4	🔳 🔬 🖲] 🛅	🗙 🛅 । ९ 👳 🕾	🗄 🕸 🚍 🗐 Q, Q,	Q, 👥	
	p.addr192.168.20.10	B.B. dns			
No.	Time	Source	Destination	Protocol	xel Length Info
-*	3495 51.991370	192.168.28.18	156.154.70.1	DNS	85 Standard query 0x2002 A cisco.com.cr_security.lab
<u>م</u> لي	3500 52.070896	156.154.78.1	192.168.20.18	DNS	160 Standard query response 0x0002 No such name A cisco.com.cr_security.lab SOA a.root-servers.net
	3501 52.071268	192.168.28.10	156.154.70.1	DNS	85 Standard query 8x0003 AAAA cisco.com.cr_security.lab
	3507 52.123690	156.154.70.1	192.168.20.18	DNS	160 Standard query response 0x0003 No such name AAAA cisco.com.cr_security.lab SDA a.root-servers.m
	3508 52,123851	192.168.28.10	156.154.70.1	DNS	69 Standard query_ <u>000004 A cisco.com</u>
	3509 52,124678	156.154.78.1	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 2002025 AAAA clsco.com
	3511 52.128125	156.154.70.1	192.168.20.18	DNS	97 Standard query response 0x0005 A4AA cisco.com A4AA ::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:

Secur Security	acurity Intelligence Events (awitch workflow) surity Intelligence with Application Details > Table View of Security Intelligence Events Expending Expending													
No Search	lo Search Constraints (<u>Edit Search</u>)													
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 Por ICMP Type		
↓ □	2019-02-14 14:36:57		Sinkhole	DNS Block	192.168.20.10		is <u>156.154.70.1</u>	🔤 USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60548 / udp		
∔ 🗆	2019-02-14 14:36:57		Sinkhole	DNS Block	192.168.20.10		156.154.70.1	SA SEU SA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60547 / udp		
1	2019-02-14 14:36:52		Sinkhole	DNS Block	192.168.20.10		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		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		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		156.154.70.1	se USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60539 / udp		
1	2019-02-14 14:30:24		Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	🔤 USA	BlackList-Domaine	leaquive-INSIDE	lesquive-OUTSIDE	62087 / udp		
∔ □	2019-02-14 14:30:24		Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	SA USA	BlackList-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 🔤	BlackList-Domains	lesquive-INSIDE	leaguive-OUTSIDE	50590 / udo		
↓ □	2019-02-14 14:14:24		Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	SA USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	62565 / udo		
↓ □	2019-02-14 14:13:43		Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domaina	lesquive-INSIDE	leaguive-OUTSIDE	60136 / udo		
+ 🗆	2019-02-14 14:13:43		Domain Not Found	DNS Block	192.168.20.10		156.154.70.1	💴 USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	53647 / udo		

您也可以在由FMC管理的FTD上使用system support firewall-engine-debug命令。



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>_