

Firepower Management Centerを使用したセキュリティインテリジェンスによるDNSのブロック

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[ブロックするドメインを使用してカスタムDNSリストを設定し、リストをFMCにアップロードします](#)

[\[action configured to 'domain not found'\]を使用して新しいDNSポリシーを追加します](#)

[アクセスコントロールポリシーへのDNSポリシーの割り当て](#)

[確認](#)

[DNSポリシーの適用前](#)

[DNSポリシーの適用後](#)

[シンクホールの設定 \(オプション \)](#)

[Sinkholeが動作していることを確認します](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Security Intelligence(SI)で適用できるように、ドメインネームシステム(DNS)リストをDNSポリシーに追加する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASA55XX Threat Defenseの設定
- Cisco Firepower Management Centerの設定

使用するコンポーネント

- Cisco ASA5506W-X Threat Defense(75)バージョン6.2.3.4 (ビルド42)
- Cisco Firepower Management Center for VMWare ソフトウェア バージョン : 6.2.3.4 (build 42)OS : Cisco Fire Linux OS 6.2.3 (ビルド13)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

セキュリティインテリジェンスは、既知の不正なレピュテーションを持つIPアドレス、URL、またはドメイン名との間のトラフィックをブロックすることによって機能します。このドキュメントでは、主にドメイン名のブラックリスト化を取り上げています。

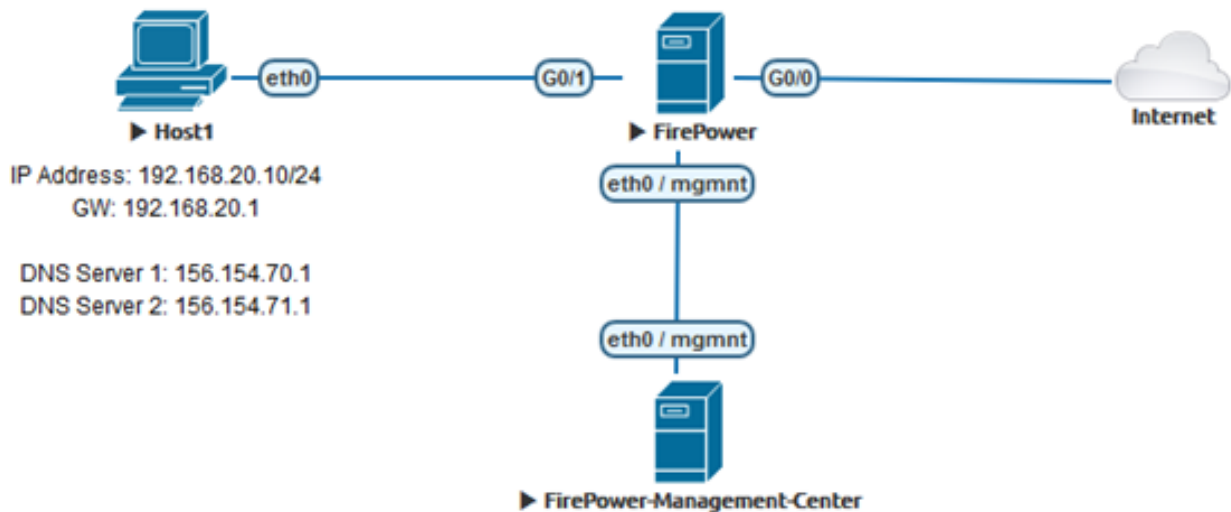
この例では、ブロック1ドメインを使用しています。

- cisco.com

URLフィルタリングを使用してこれらのサイトの一部をブロックすることもできますが、問題は、URLが完全に一致している必要があることです。一方、SIを使用したDNSブラックリストは、サブドメインやURLの変更を心配することなく、「cisco.com」のようなドメインに焦点を当てることができます。

このドキュメントの最後に、オプションのSinkhole設定も示します。

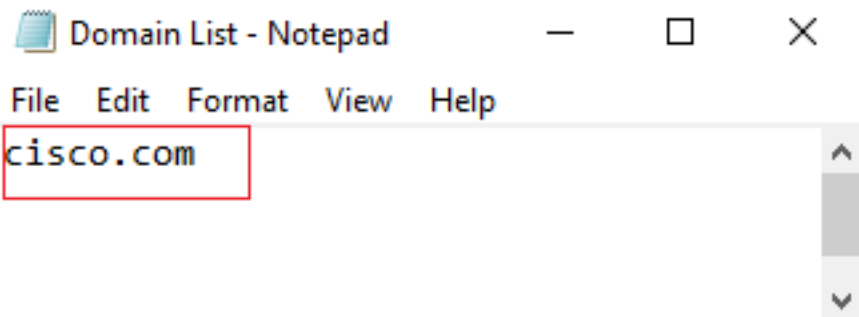
ネットワーク図



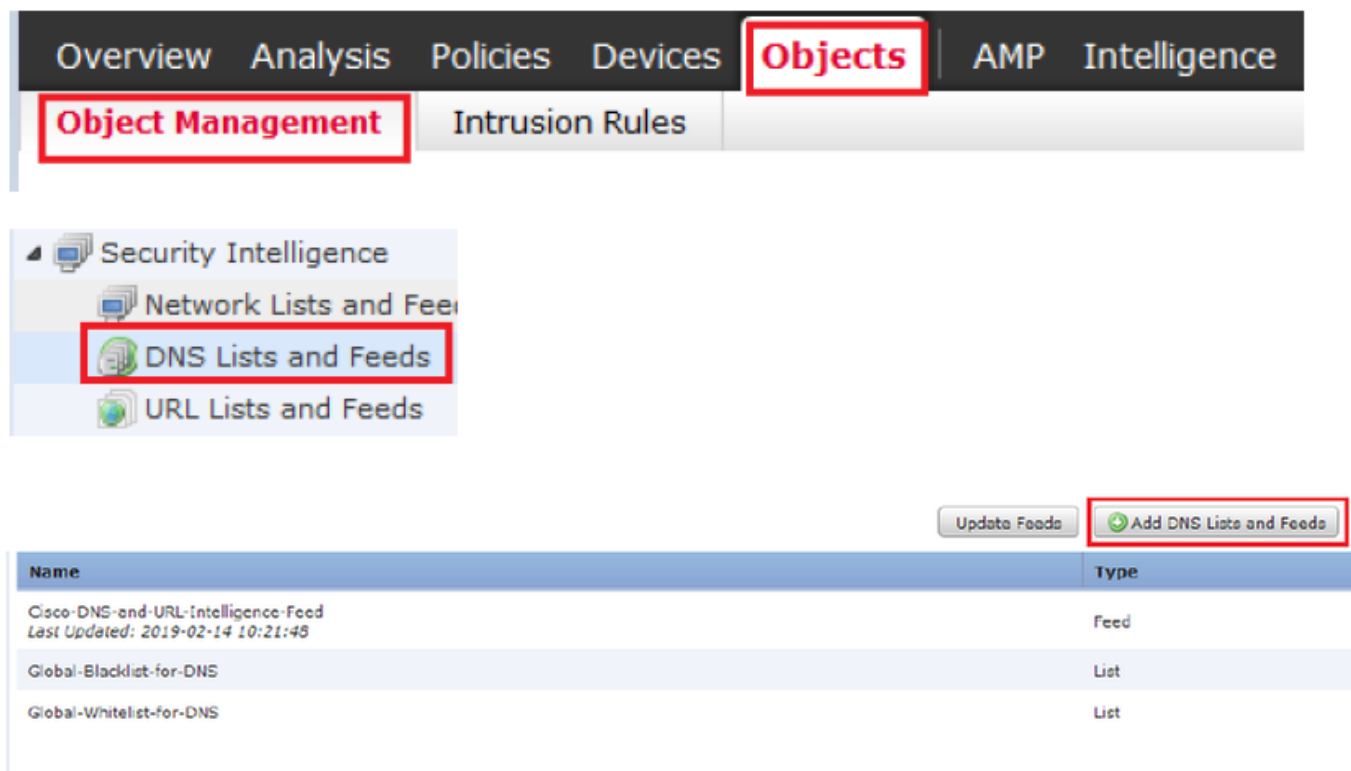
設定

ブロックするドメインを使用してカスタムDNSリストを設定し、リストをFMCにアップロードします

ステップ1：ブロックするドメインを含む.txtファイルを作成します。コンピュータに.txtファイルを保存します。



ステップ2:FMCで、[Object] > [Object Management] >> [DNS Lists and Feeds] >> [Add DNS List and Feeds]に移動します。



ステップ3:「BlackList-Domains」という名前のリストを作成します。タイプはlistであり、問題のドメインを含む.txtファイルは、次の図に示すようにアップロードする必要があります。

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

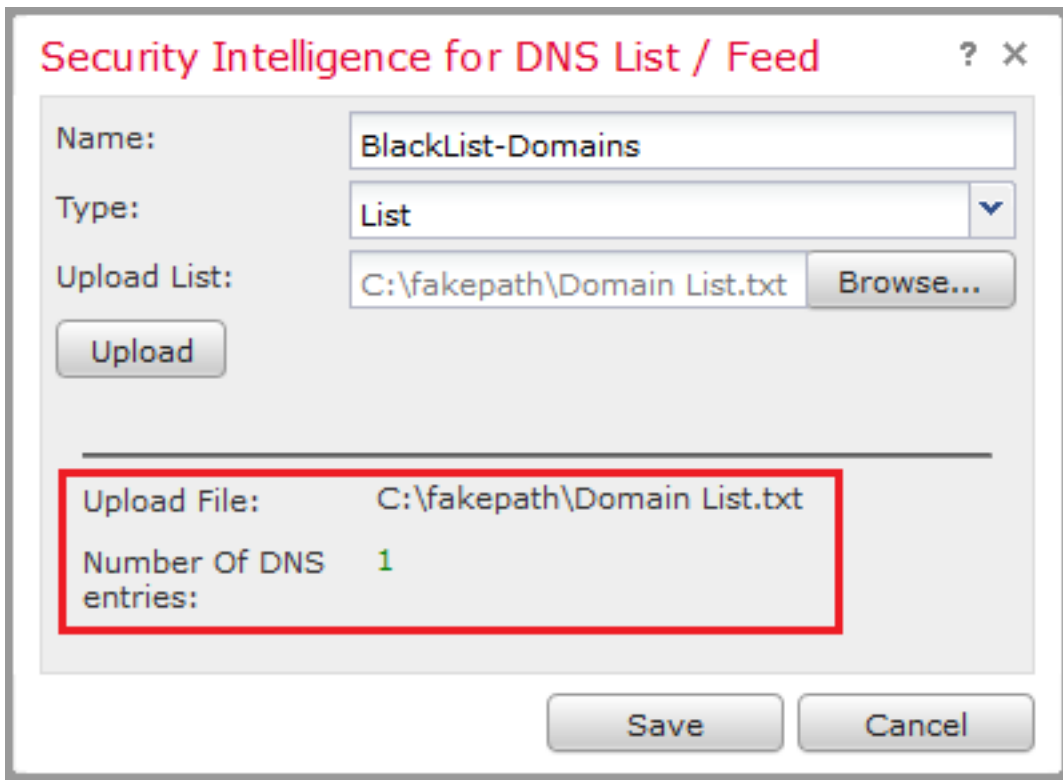
Type: List

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

Upload

Save Cancel

*.txtファイルをアップロードすると、[Number of DNS entries]はすべてのドメインを読み取ります。この例では、合計が1です。

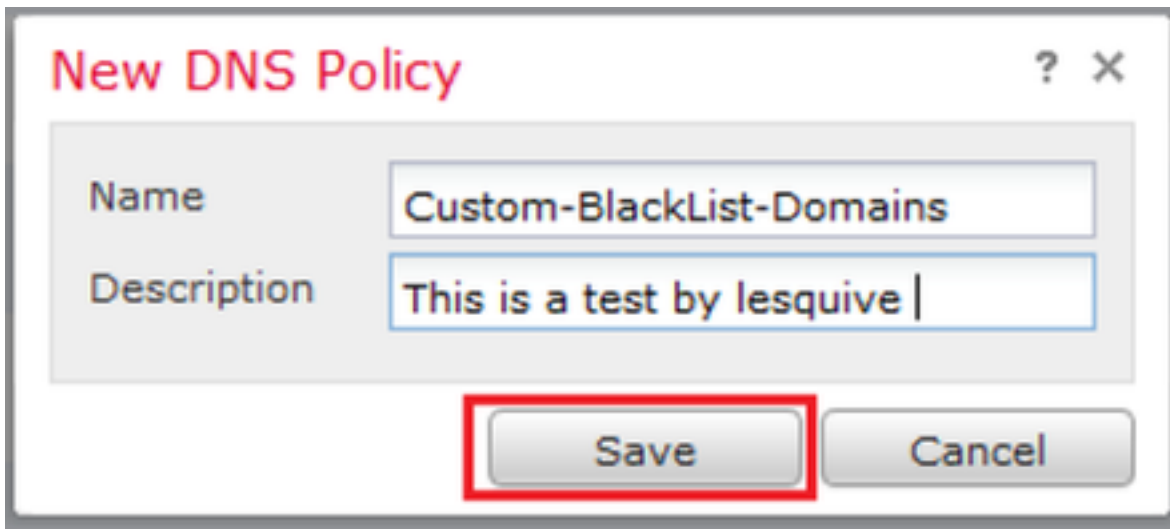


[action configured to 'domain not found']を使用して新しいDNSポリシーを追加します

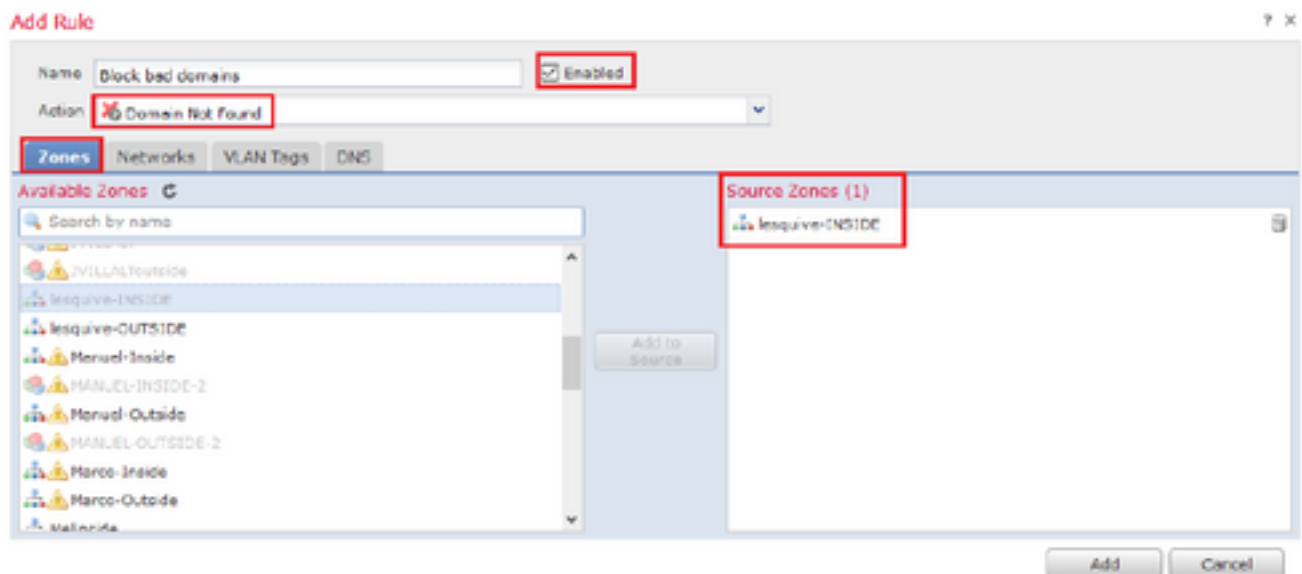
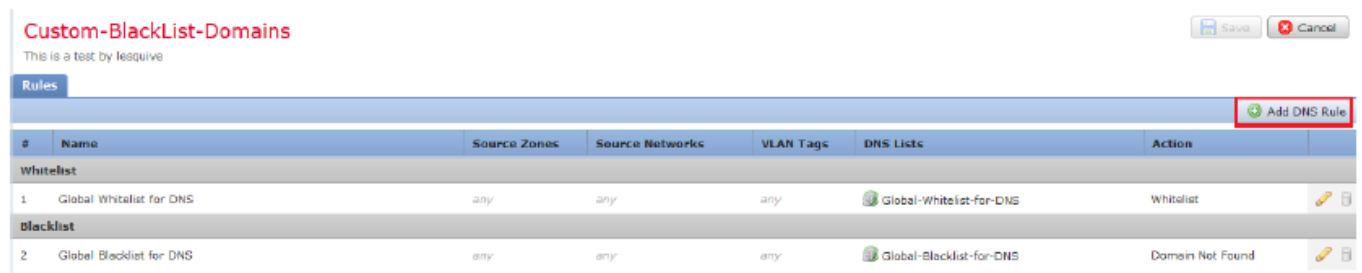
*ソースゾーン、ソースネットワーク、およびDNSリストを追加してください。

ステップ1:[Policies] >> [Access Control] >> [DNS] >> [Add DNS Policy]に移動します。





ステップ2 : 図に示すように、DNSルールを追加します。



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

ルールの順序に関する重要な情報：

- グローバルホワイトリストは常に最初にあり、他のすべてのルールよりも優先されます。
- 子孫DNSホワイトリスト規則は、非リーフドメインのマルチドメイン展開でのみ表示されます。これは常に2番目であり、グローバルホワイトリスト以外のすべてのルールよりも優先されます。
- Blacklistセクションの前にWhitelistセクションがあります。ホワイトリストのルールは、常に他のルールよりも優先されます。
- グローバルブラックリストは、常に[ブラックリスト(Blacklist)]セクションの最初にあり、他のすべてのモニタおよびブラックリストのルールよりも優先されます。
- 子孫DNSブラックリスト規則は、非リーフドメインのマルチドメイン展開でのみ表示されます。これは常に[ブラックリスト(Blacklist)]セクションの2番目であり、グローバルブラックリスト以外のすべてのモニタおよびブラックリストのルールよりも優先されます。
- [ブラックリスト(Blacklist)]セクションには、モニタおよびブラックリストのルールが含まれています。
- DNSルールを初めて作成する場合、システム位置は[ホワイトリスト]セクションの最後に表示されます (ホワイトリストのアクションを割り当てた場合)。

アクセスコントロールポリシーへのDNSポリシーの割り当て

[Policies] >> [Access Control] >> [The Policy for your FTD] >> [Security Intelligence] >> [DNS Policy]に移動し、作成したポリシーを追加します。

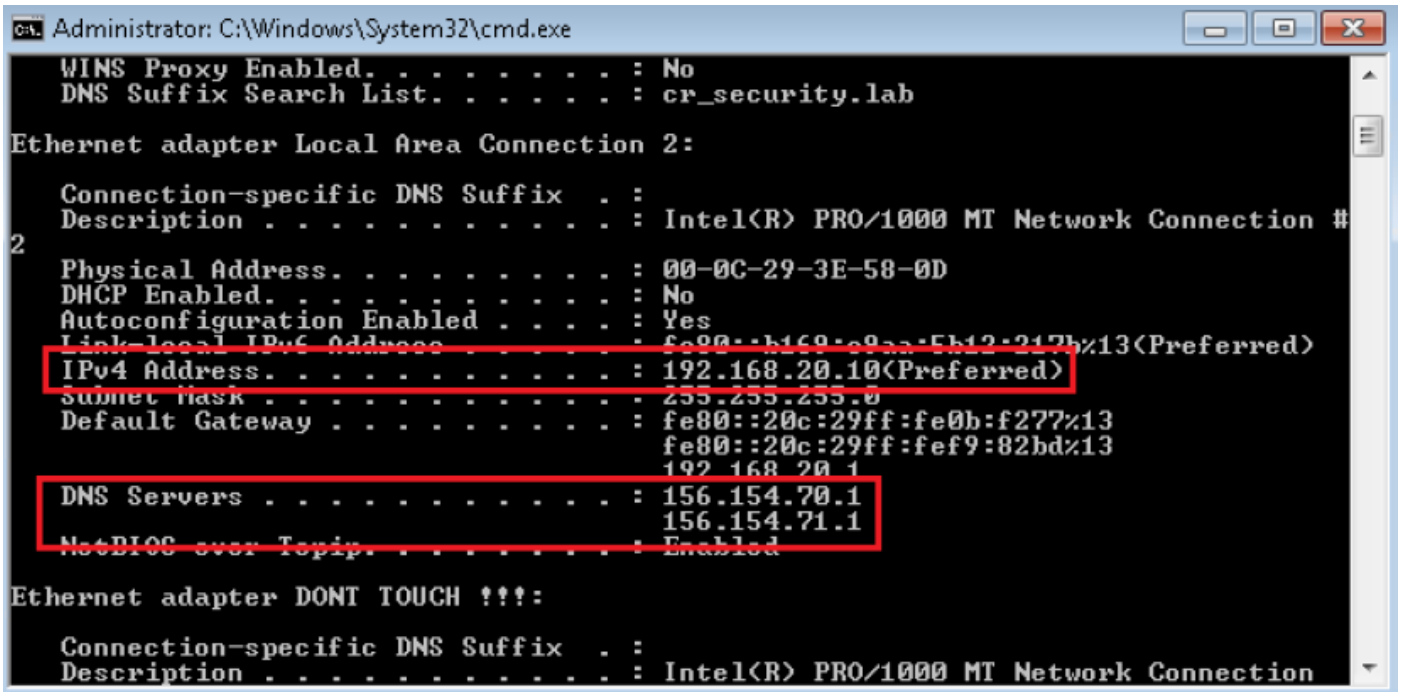
The screenshot shows the configuration page for a policy named 'lesquive-policy'. The navigation path is: Overview > Analysis > Policies > Devices > Objects > AMP > Access Control > Network Discovery > Application Detectors > Access Control. The 'Access Control' tab is selected. The policy configuration shows 'Prefilter Policy: Default Prefilter Policy', 'SSL Policy: None', and 'Identity Policy: None'. Under the 'Rules' section, the 'Security Intelligence' tab is active, and the 'DNS Policy' is set to 'Custom-BlackList-Domains'. A 'Save' button is visible, indicating unsaved changes.

完了したら、すべての変更を必ず導入してください。

確認

DNSポリシーの適用前

ステップ1：図に示すように、ホストマシンのDNSサーバとIPアドレス情報を確認します。



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

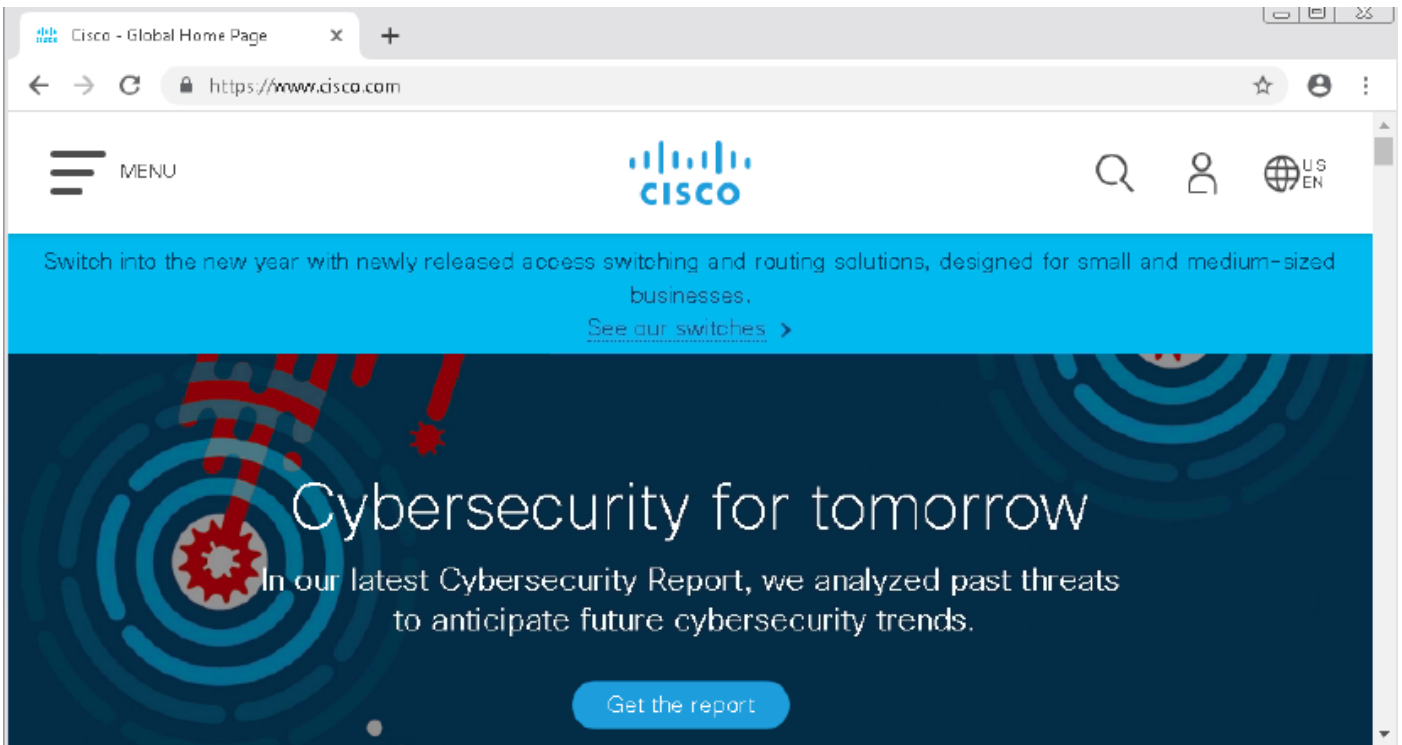
Ethernet adapter Local Area Connection 2:

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:c9aa-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
```

ステップ2：次の図に示すように、cisco.comに移動できることを確認します。



ステップ3：パケットキャプチャで、DNSが正しく解決されていることを確認します。

The screenshot shows a Wireshark capture of network traffic on 'Local Area Connection 2'. The packet list pane shows two 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 packet details pane for packet 3515 shows the following structure:

- 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

DNSポリシーの適用後

ステップ1: ipconfig /flushdns コマンドを使用して、ホストのDNSキャッシュをクリアします。

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

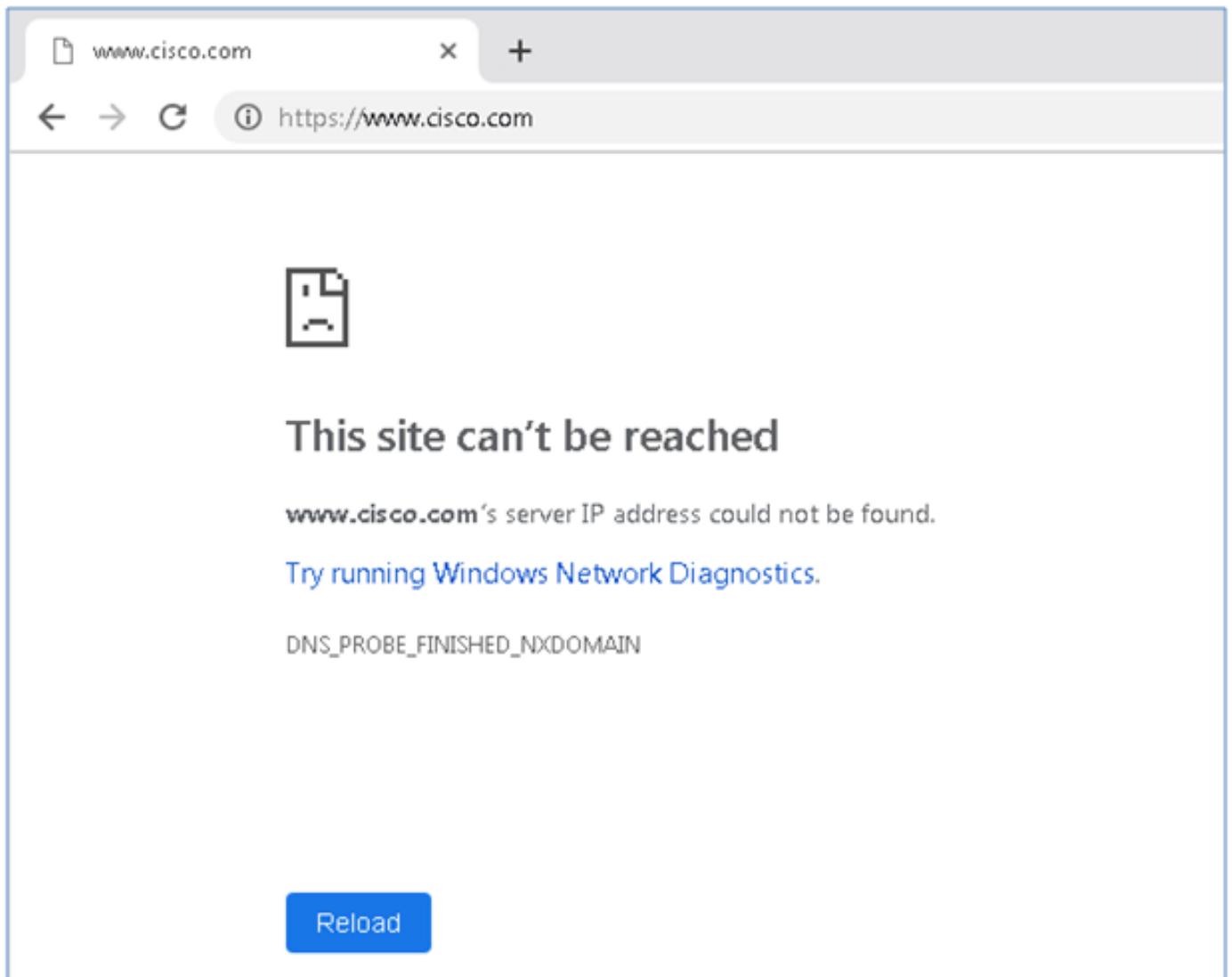
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
```

ステップ2: Webブラウザを使用して、対象のドメインに移動します。到達不能であるはずですが。



ステップ3 : ドメインcisco.comでnslookupを発行してみます。名前解決が失敗する。

```
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

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

ステップ4 : パケットキャプチャは、DNSサーバではなくFTDからの応答を示します。

The screenshot shows a Wireshark capture of a UDP stream. The packet list pane shows two packets: packet 1617 is a standard query for 'A cisco.com' from 192.168.20.10 to 156.154.70.1; packet 1618 is a standard query response from 156.154.70.1 to 192.168.20.10. The packet details pane for packet 1618 shows a Domain Name System (response) with Transaction ID 0x0004. The flags are 0x8503, indicating a standard query response. The message is 'No such name A cisco.com'. The queries section shows a link to the request in packet 1617, with a time of 0.000671000 seconds.

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

▶ 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]

ステップ5:FTD CLIでデバッグを実行します。システムはfirewall-engine-debugをサポートし、UDPプロトコルを指定します。

```
>  
> 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
```

*cisco.comが一致した場合のデバッグ：

```
> system support firewall-engine-debug

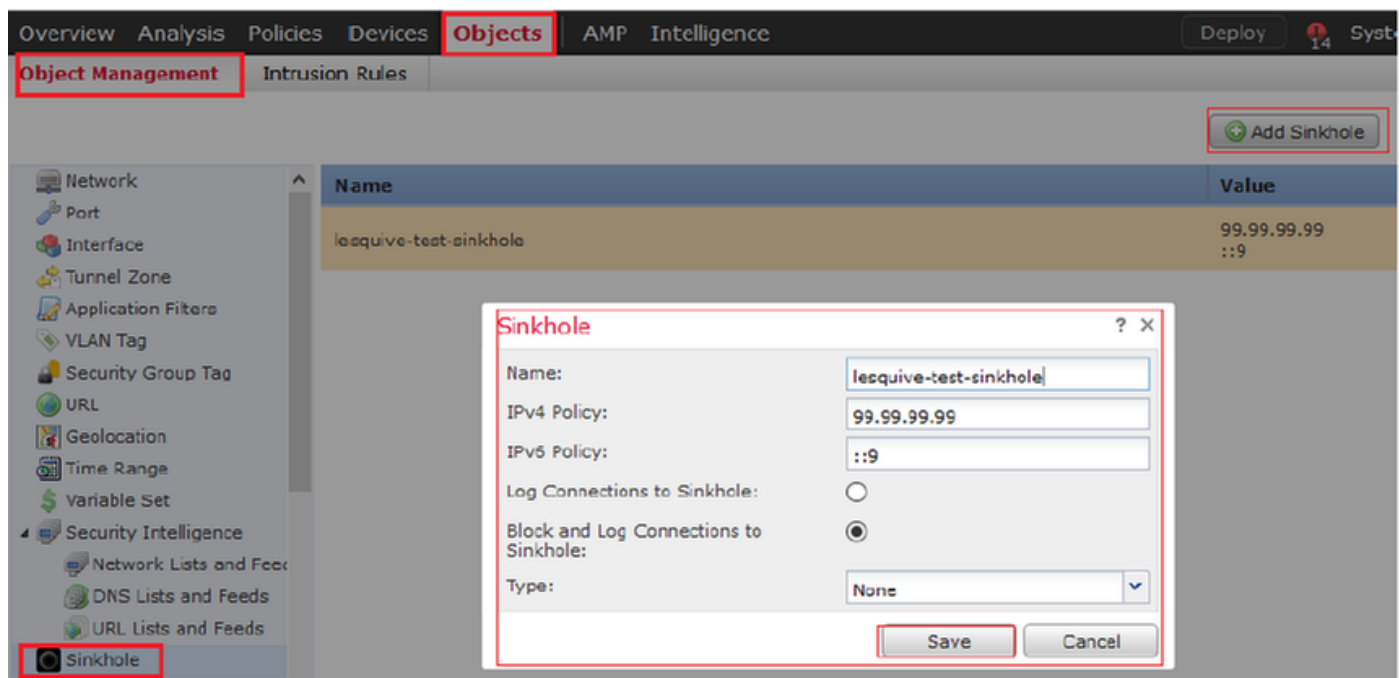
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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
```

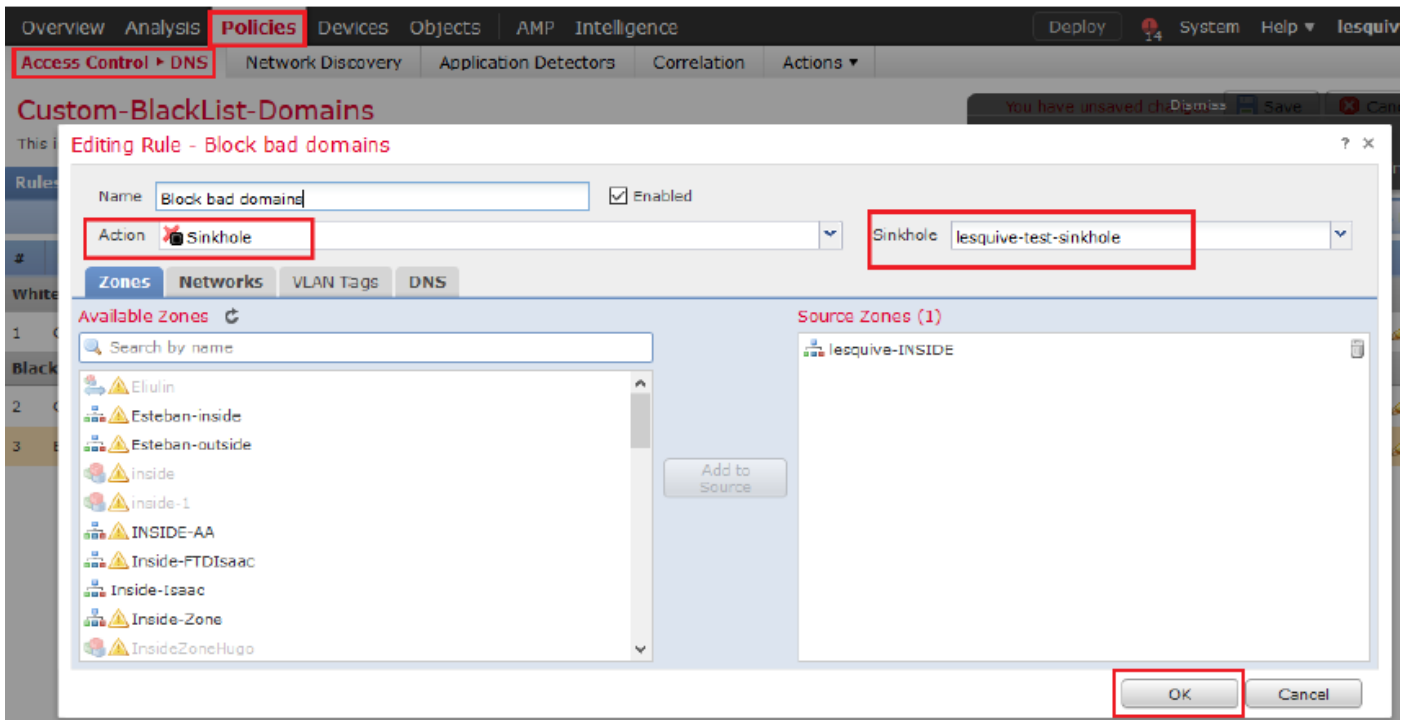
シンクホールの設定 (オプション)

DNSシンクホールは、誤った情報を提供するDNSサーバです。ブロックしているドメインのDNSクエリに対する「No such name」DNS応答を返す代わりに、偽のIPアドレスを返します。

ステップ1:[Objects] >> [Object Management] >> [Sinkhole] >> [Add Sinkhole]に移動し、偽のIPアドレス情報を作成します。



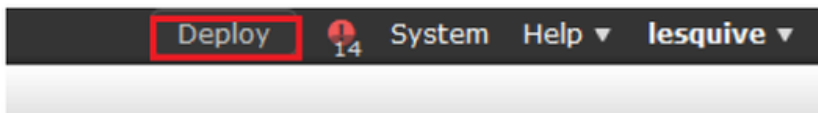
ステップ2:DNSポリシーにシンクホールを適用し、FTDに変更を導入します。



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



Sinkholeが動作していることを確認します

```
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

トラブルシューティング

[Analysis] > [Connections] >> [Security Intelligence Events]に移動し、DNSポリシーでロギングを有効にしている限り、SIによってトリガーされるすべてのイベントを追跡します。

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	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	USA	BlackList-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	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	USA	BlackList-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	BlackList-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	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	lesquive-OUTSIDE	50590 / 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	lesquive-OUTSIDE	62565 / udp	
↓	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	60136 / udp	
↓	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 / udp	

FMCによって管理されるFTDでは、`system support firewall-engine-debug`コマンドを使用することもできます。

```
>
> 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
```

パケットキャプチャは、DNS要求がFTDサーバに送信していることを確認するのに役立ちます。テスト時にローカルホストのキャッシュをクリアすることを忘れないでください。

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>_