Block DNS with Security Intelligence using Firepower Management Center

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Network Diagram
Configure
Configure a custom DNS List with the domains we want to block and upload the list to FMC
Add a new DNS Policy with the 'action configured to 'domain not found'
Assign the DNS Policy to your Access Control Policy
Verify
Before the DNS Policy is Applied
After the DNS Policy is Applied
Optional Sinkhole Configuration
Verify Sinkhole is working
Troubleshoot

Introduction

This document describes the procedure to add a Domain Name System (DNS) List to a DNS Policy so that you can apply it with Security Intelligence (SI).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ASA55XX Threat Defense configuration
- Cisco Firepower Management Center configuration

Components Used

- Cisco ASA5506W-X Threat Defense (75) Version 6.2.3.4 (Build 42)
- Cisco Firepower Management Center for VMWare Software Version: 6.2.3.4 (build 42)OS: Cisco Fire Linux OS 6.2.3 (build13)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Security Intelligence works by blocking traffic to or from IP addresses, URLs, or domain names that have a known bad reputation. In this document, the main focus is domain name blacklisting.

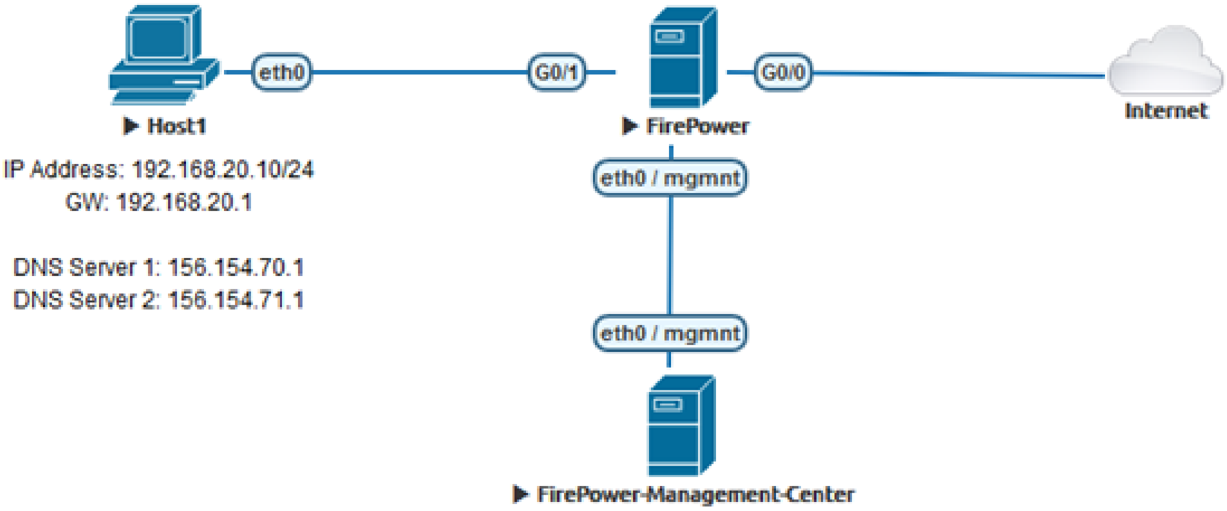
The example used blocks 1 domain:

- cisco.com

You could use URL filtering to block some of these sites, but the problem is that the URL must be an exact match. On the other hand, DNS blacklisting with SI can focus on domains like “cisco.com” without the need to worry about any sub-domains or changes in URL.

At the end of this document, an optional Sinkhole configuration is also demonstrated.

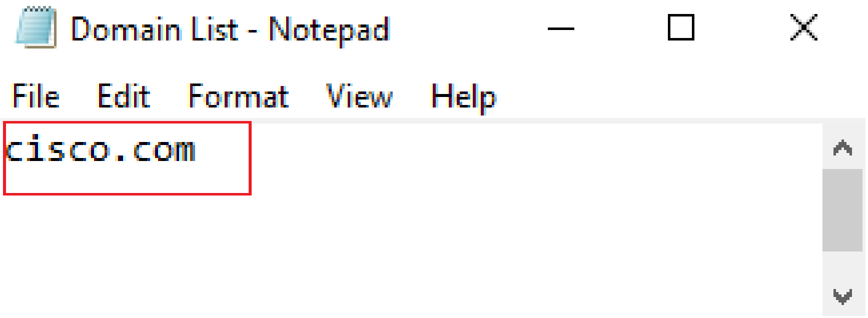
Network Diagram


eth0
G0/1
G0/0
Host1
FirePower
Internet
IP Address: 192.168.20.10/24
GW: 192.168.20.1
DNS Server 1: 156.154.70.1
DNS Server 2: 156.154.71.1
eth0 / mgmnt
eth0 / mgmnt
FirePower-Management-Center

Configure

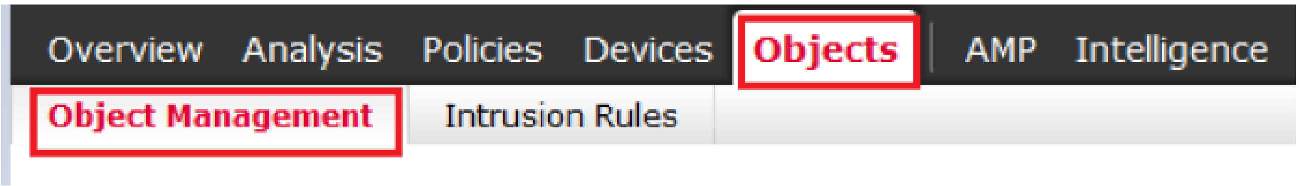
Configure a custom DNS List with the domains we want to block and upload the list to FMC

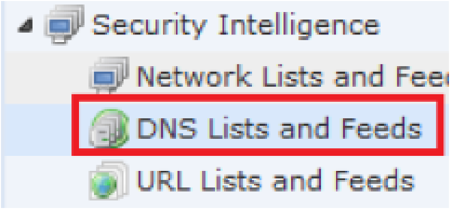
Step 1. Create a .txt file with the domains that you would like to block. Save the .txt file on your computer:

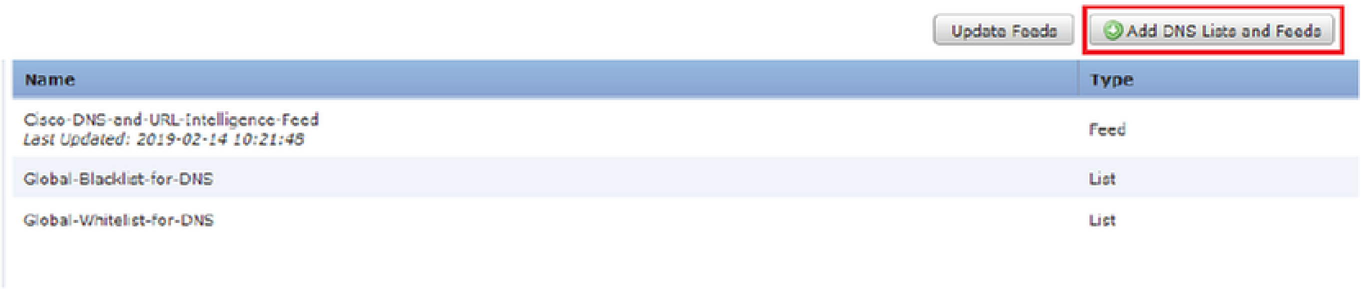


```
cisco.com
```

Step 2. In FMC navigate to Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds.

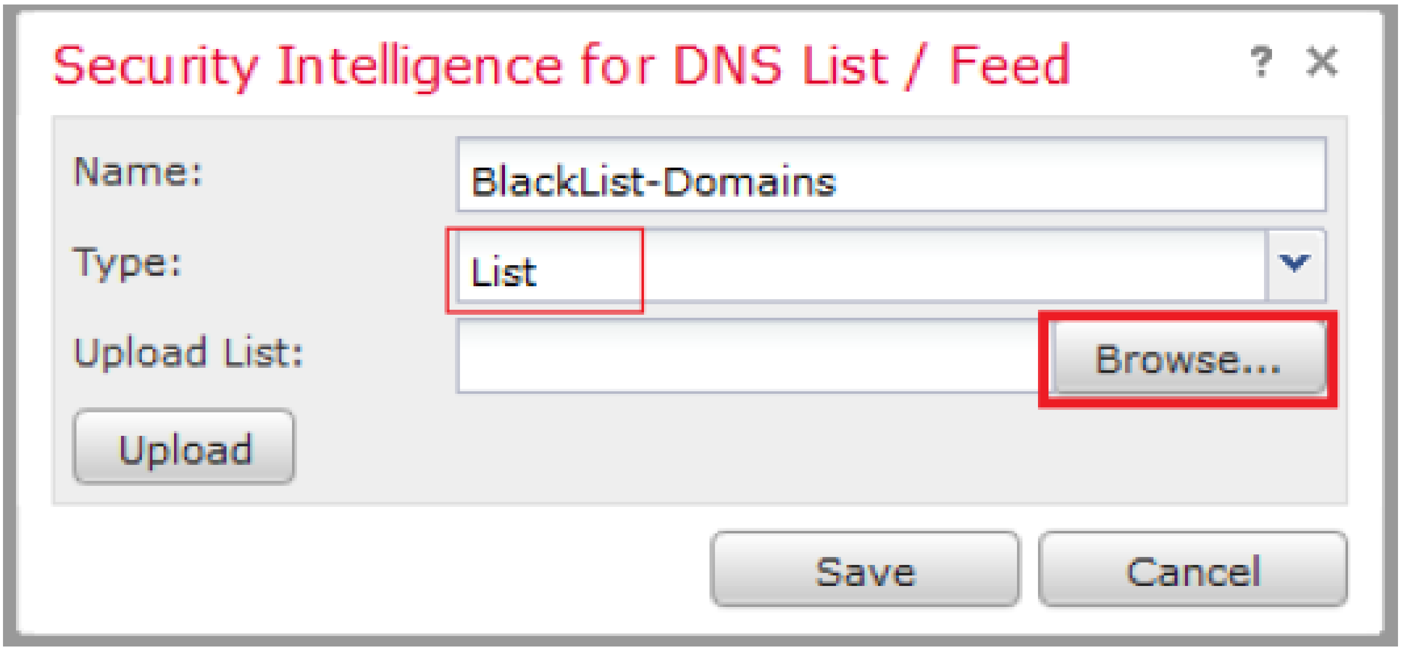






Name	Type
Cisco-DNS-and-URL-Intelligence-Feed *Last Updated: 2019-02-14 10:21:48*	Feed
Global-Blacklist-for-DNS	List
Global-Whitelist-for-DNS	List

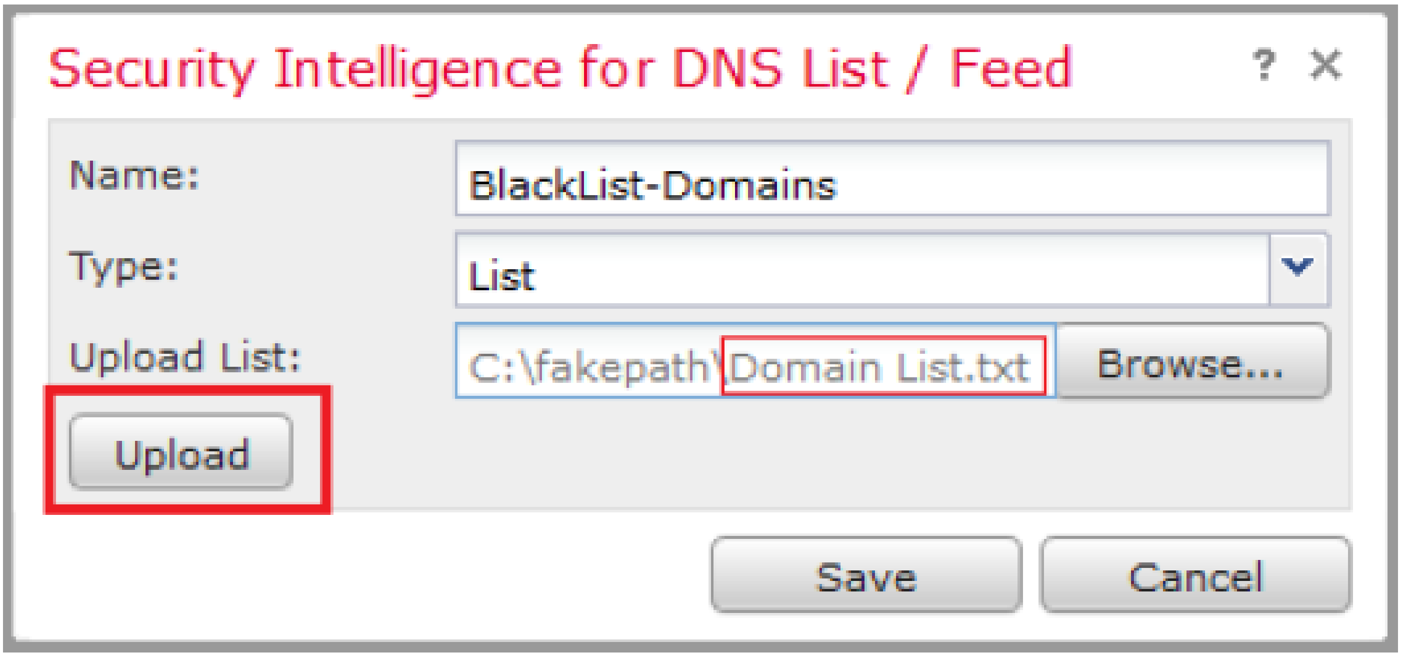
Step 3. Create a list called “BlackList-Domains”, the type should be list and the .txt file with the domains in question should be uploaded as seen in the images:



Name: BlackList-Domains

Type: List

Upload List:



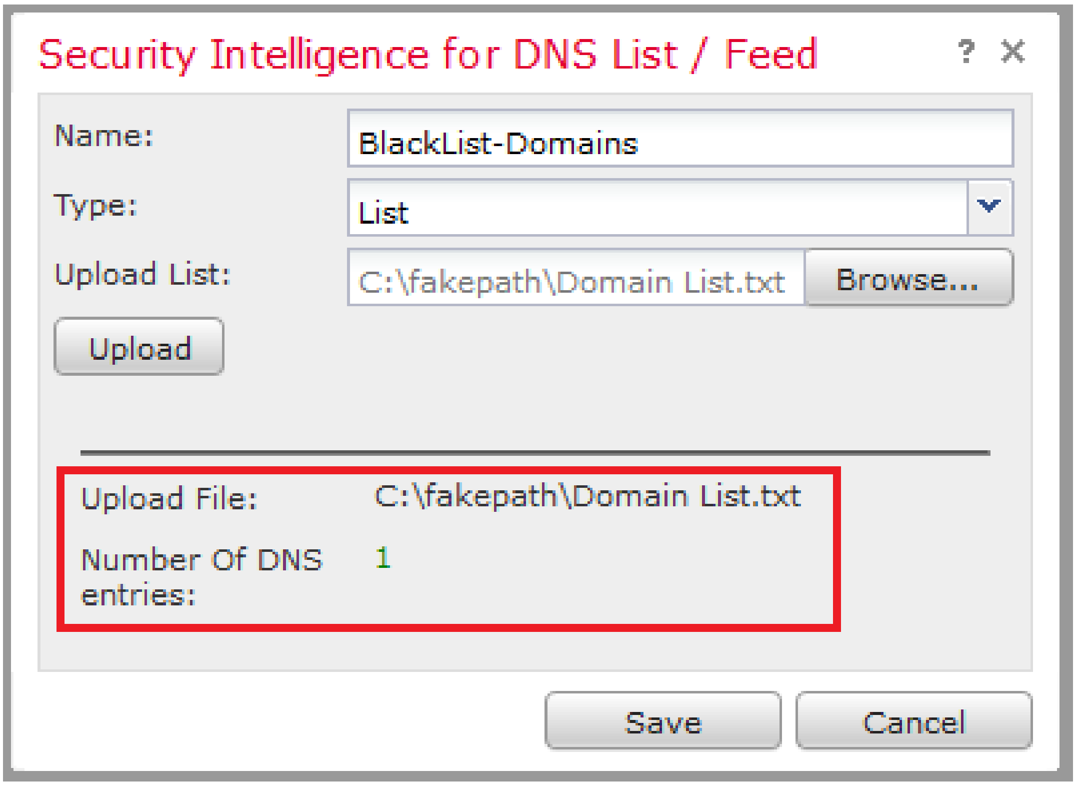
Security Intelligence for DNS List / Feed

Name: BlackList-Domains

Type: List

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

*Notice that when you upload the .txt file, the Number of DNS entries should read all domains. In this example, a total of 1:



Security Intelligence for DNS List / Feed

Name: BlackList-Domains

Type: List

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

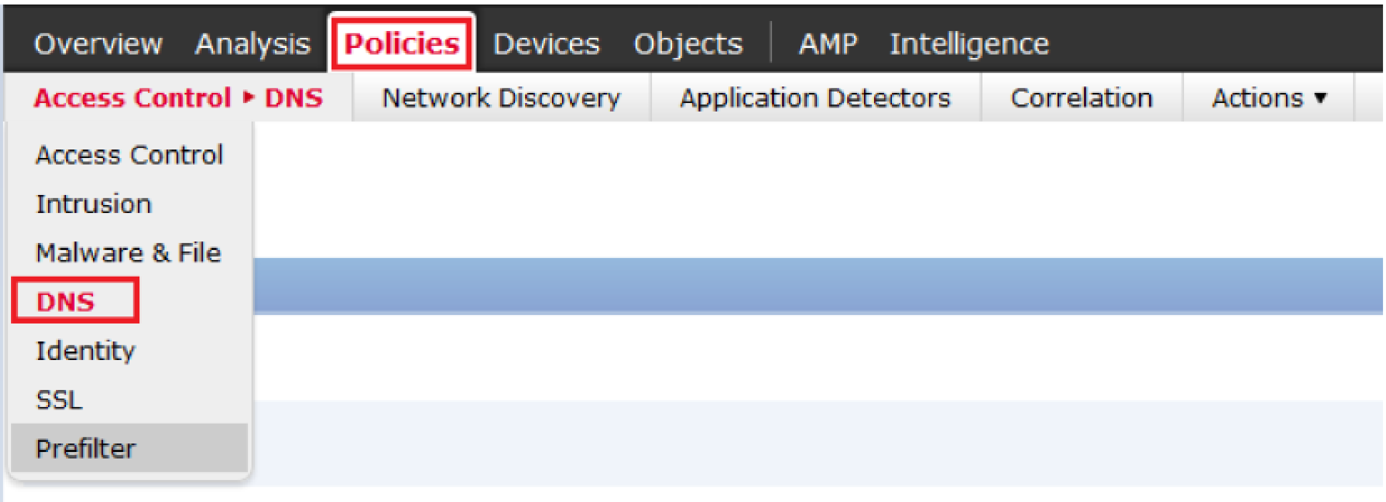
Upload File: C:\fakepath\Domain List.txt

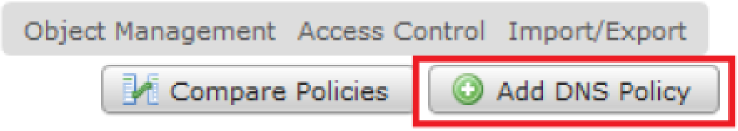
Number Of DNS entries: 1

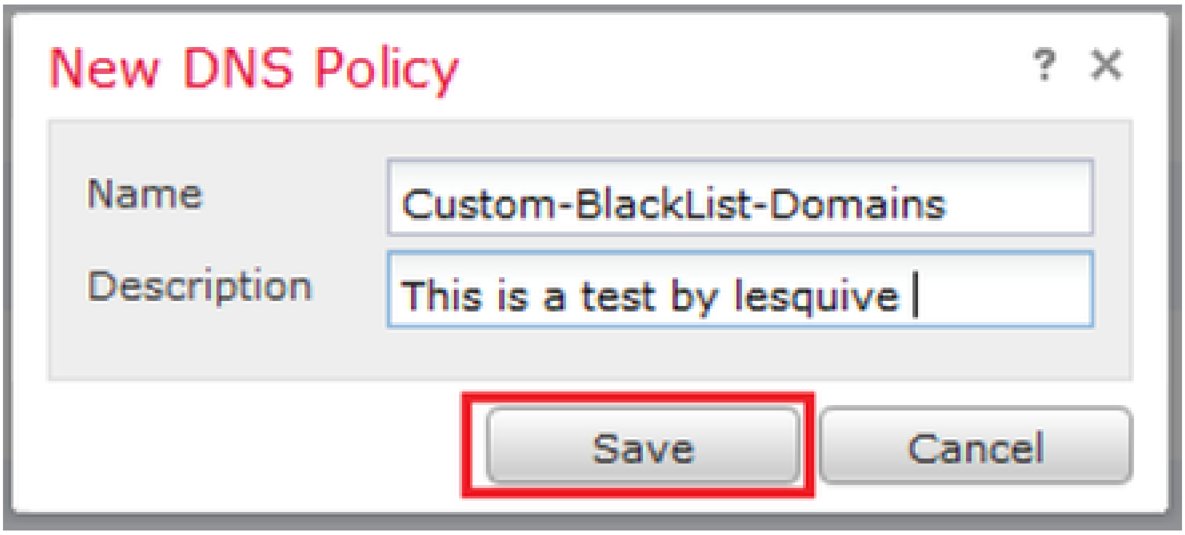
Add a new DNS Policy with the 'action configured to 'domain not found'

*Ensure you add a source zone, source network, and DNS List.

Step 1. Navigate to Policies >> Access Control >> DNS >> Add DNS Policy:





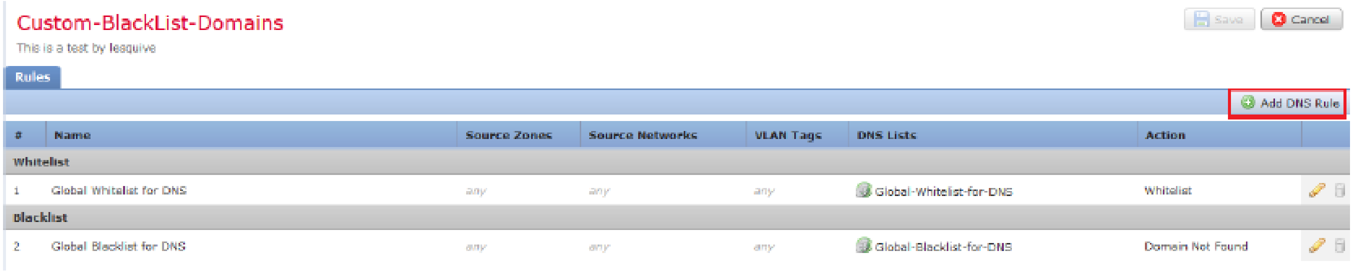


New DNS Policy

Name: Custom-BlackList-Domains

Description: This is a test by lesquive

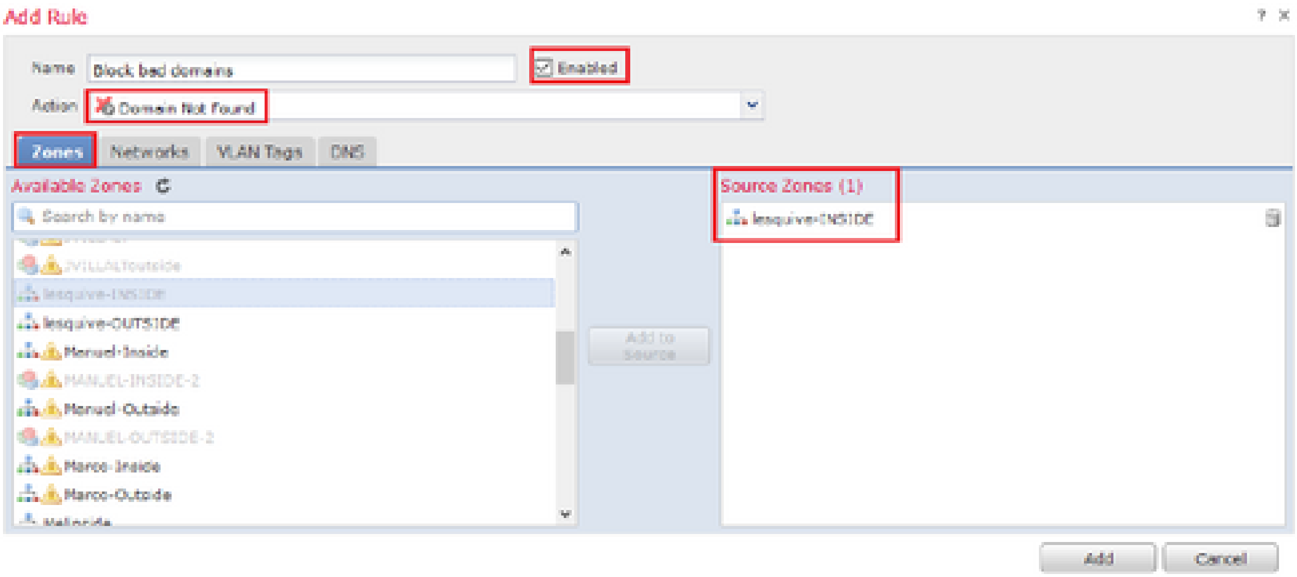
Step 2. Add A DNS rule as seen in the image:



Custom-BlackList-Domains

This is a test by lesquive

#	Name	Source Zones	Source Networks	VLAN Tags	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



Add Rule

Name: Block bad domains ☑ Enabled

Action: Domain Not Found

Zones | Networks | VLAN Tags | DNS

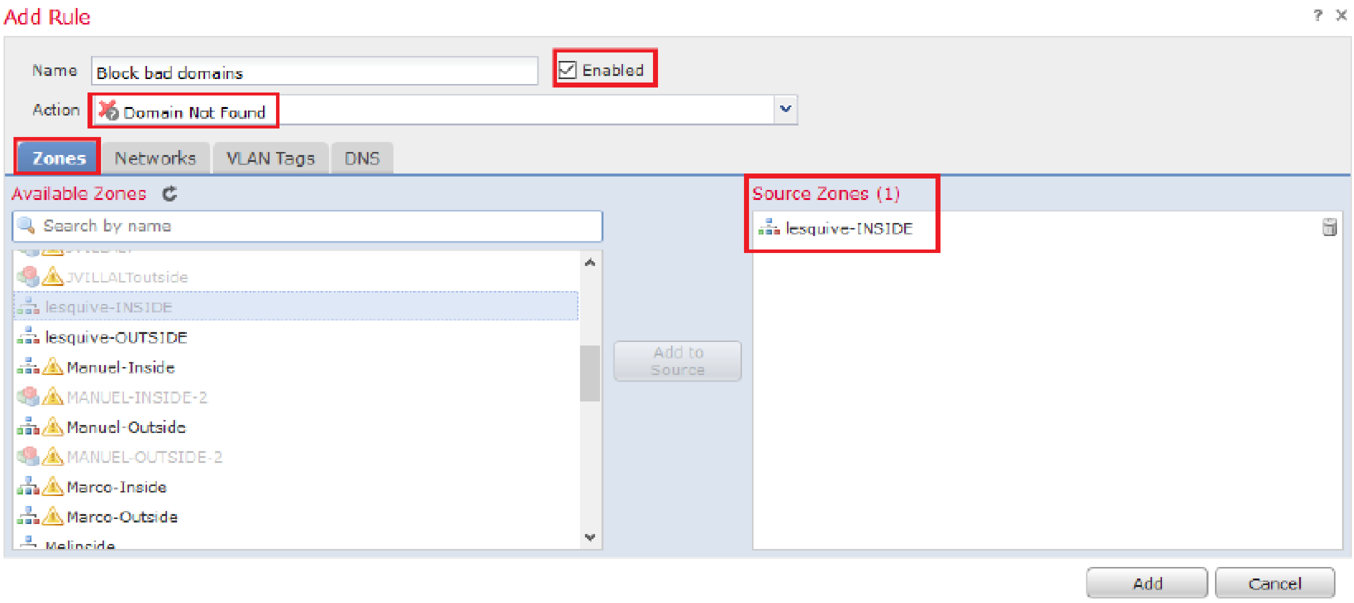
Available Zones

Search by name

- JVILLALToutside
- lesquive-INSIDE
- lesquive-OUTSIDE
- Manuel-Inside
- MANUEL-INSIDE-2
- Manuel-Outside
- MANUEL-OUTSIDE-2
- Marco-Inside
- Marco-Outside
- Melinside

Source Zones (1)

- lesquive-INSIDE



Add Rule

Name: Block bad domains ☑ Enabled

Action: Domain Not Found

Zones | Networks | VLAN Tags | DNS

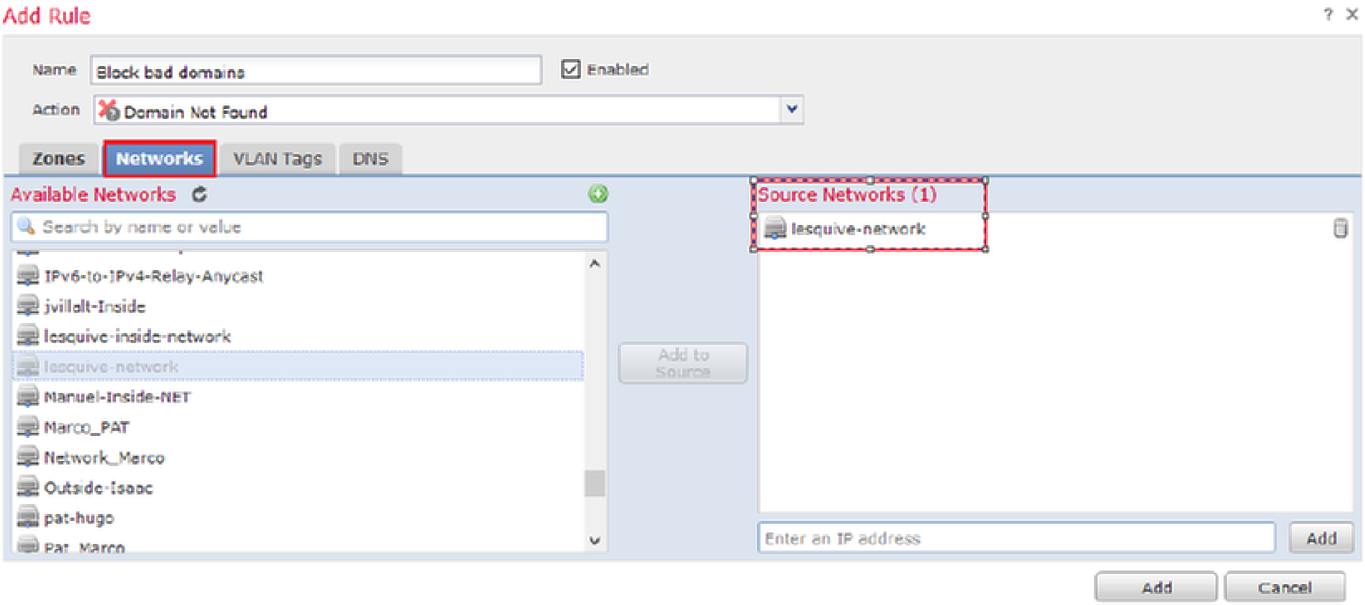
Available Zones

Search by name

- JVILLALToutside
- lesquive-INSIDE
- lesquive-OUTSIDE
- Manuel-Inside
- MANUEL-INSIDE-2
- Manuel-Outside
- MANUEL-OUTSIDE-2
- Marco-Inside
- Marco-Outside
- Melinside

Source Zones (1)

- lesquive-INSIDE



Add Rule

Name: Block bad domains ☑ Enabled

Action: Domain Not Found

Zones | Networks | VLAN Tags | DNS

Available Networks

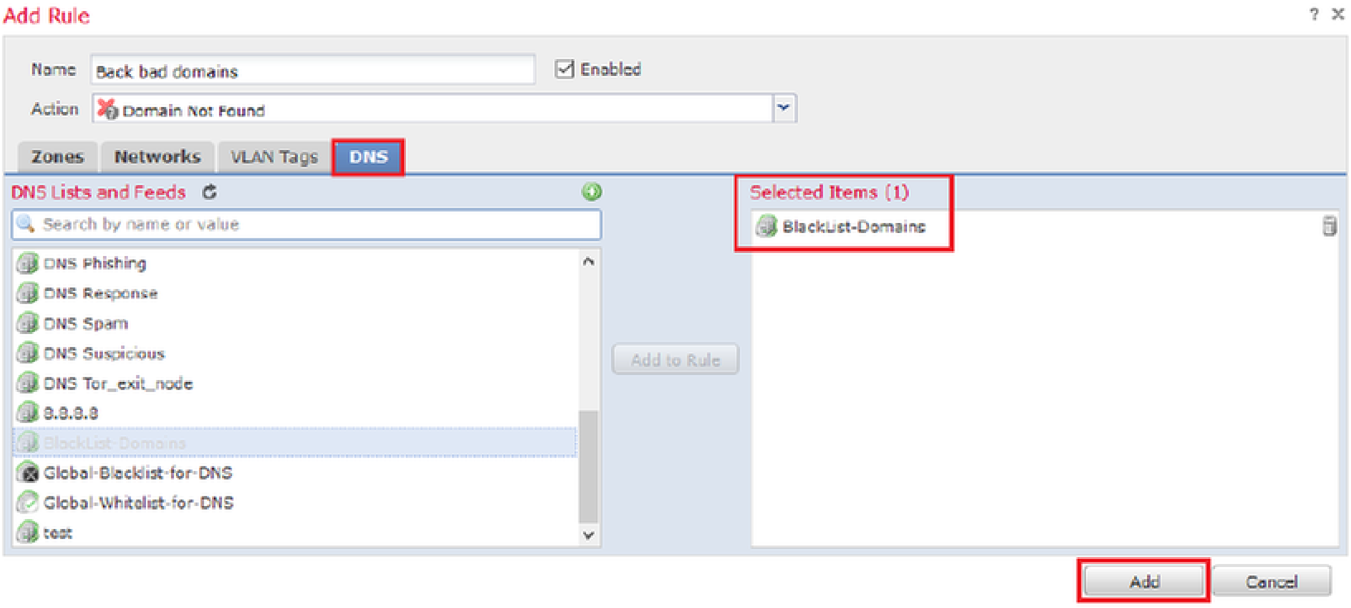
Search by name or value

- IPv6-to-IPv4-Relay-Anycast
- jvillalt-Inside
- lesquive-inside-network
- lesquive-network
- Manuel-Inside-NET
- Marco_PAT
- Network_Marco
- Outside-Isaac
- pat-hugo
- Pat_Marco

Source Networks (1)

- lesquive-network

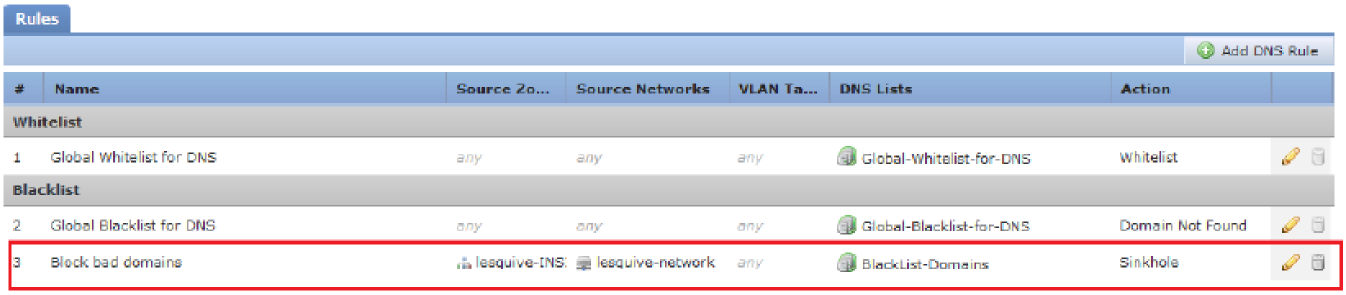
Enter an IP address



Add Rule

Name: Back bad domains ☑ Enabled

Action: Domain Not Found



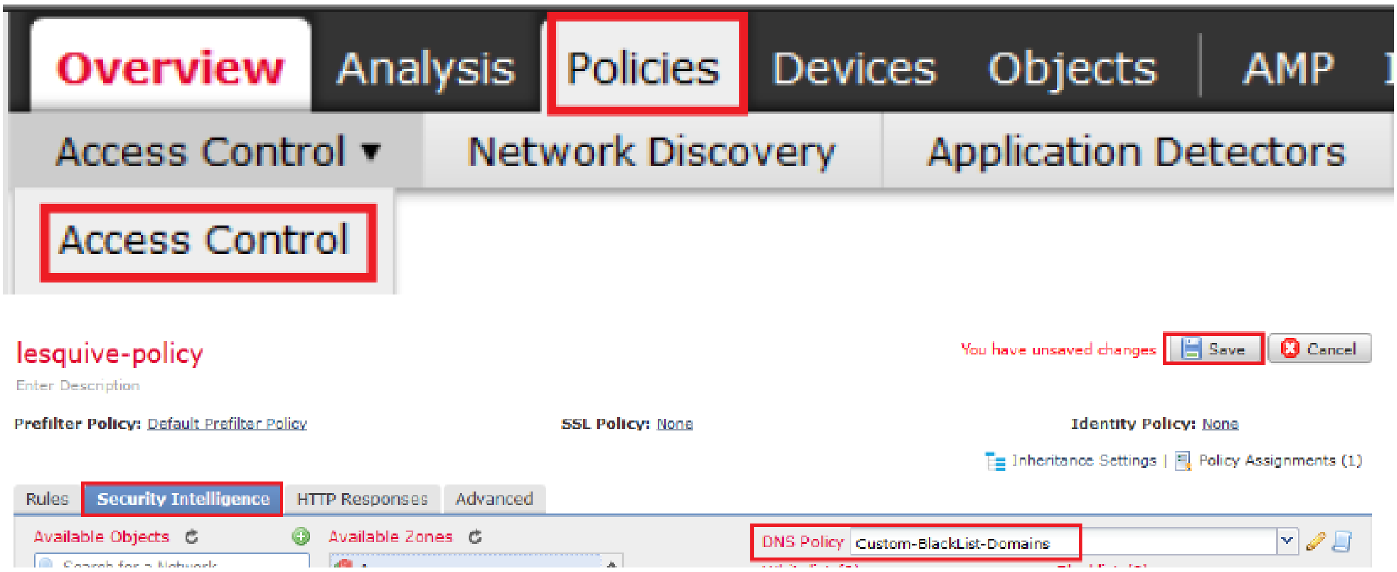
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Block bad domains	lesquive-INS:	lesquive-network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

Important information on rule order:

- The Global Whitelist is always first and takes precedence over all other rules.
- The Descendant DNS Whitelists rule only appears in multi-domain deployments, in non-leaf domains. It is always second and takes precedence over all other rules except the Global Whitelist.
- The Whitelist section precedes the Blacklist section; whitelist rules always take precedence over other rules.
- The Global Blacklist is always first in the Blacklist section and takes precedence over all other Monitor and blacklist rules.
- The Descendant DNS Blacklists rule only appears in multi-domain deployments, in non-leaf domains. It is always second in the Blacklist section and takes precedence over all other Monitor and blacklist rules except the Global Blacklist.
- The Blacklist section contains Monitor and blacklist rules.
- When you first create a DNS rule, the system position sit last in the Whitelist section if you assign a Whitelist action, or last in the Blacklist section if you assign any other action

Assign the DNS Policy to your Access Control Policy

Go to Policies >> Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy and add the Policy you created.



lesquive-policy

Enter Description

You have unsaved changes Save Cancel

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Inheritance Settings | Policy Assignments (1)

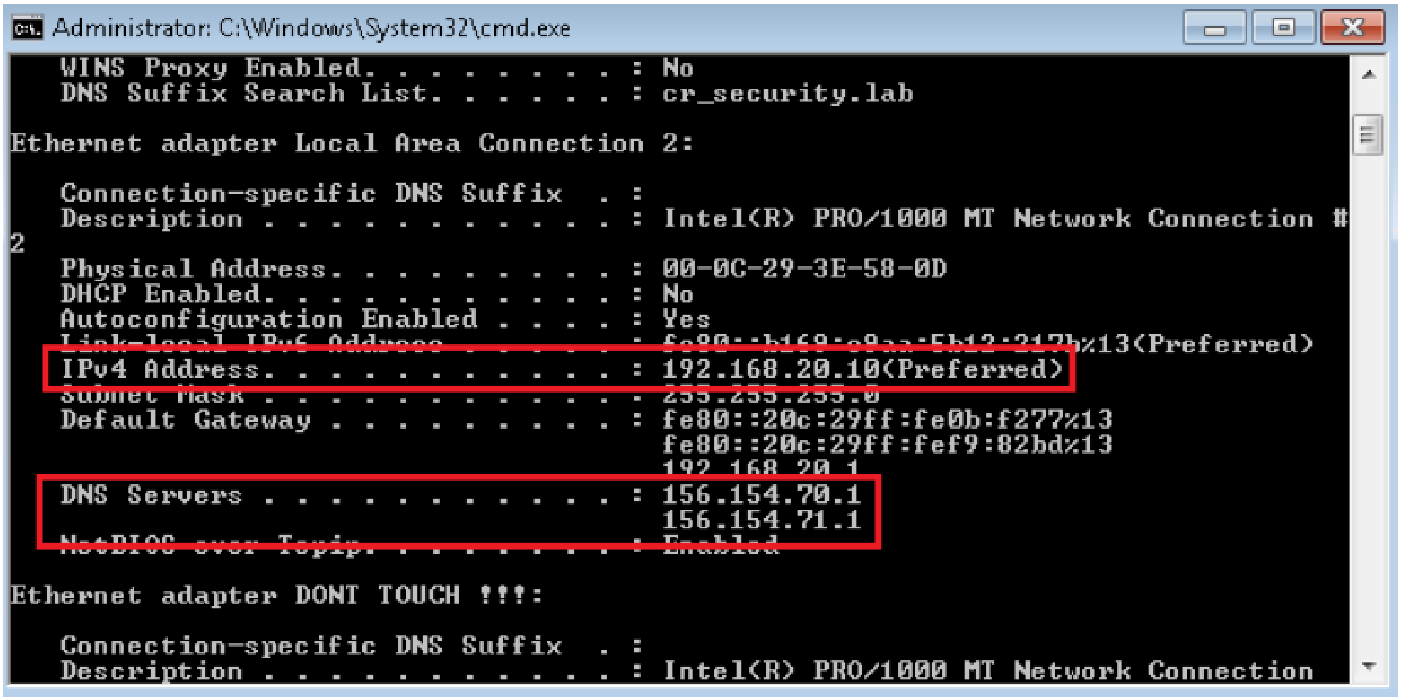
DNS Policy: Custom-BlackList-Domains

Ensure you deploy all changes when finished.

Verify

Before the DNS Policy is Applied

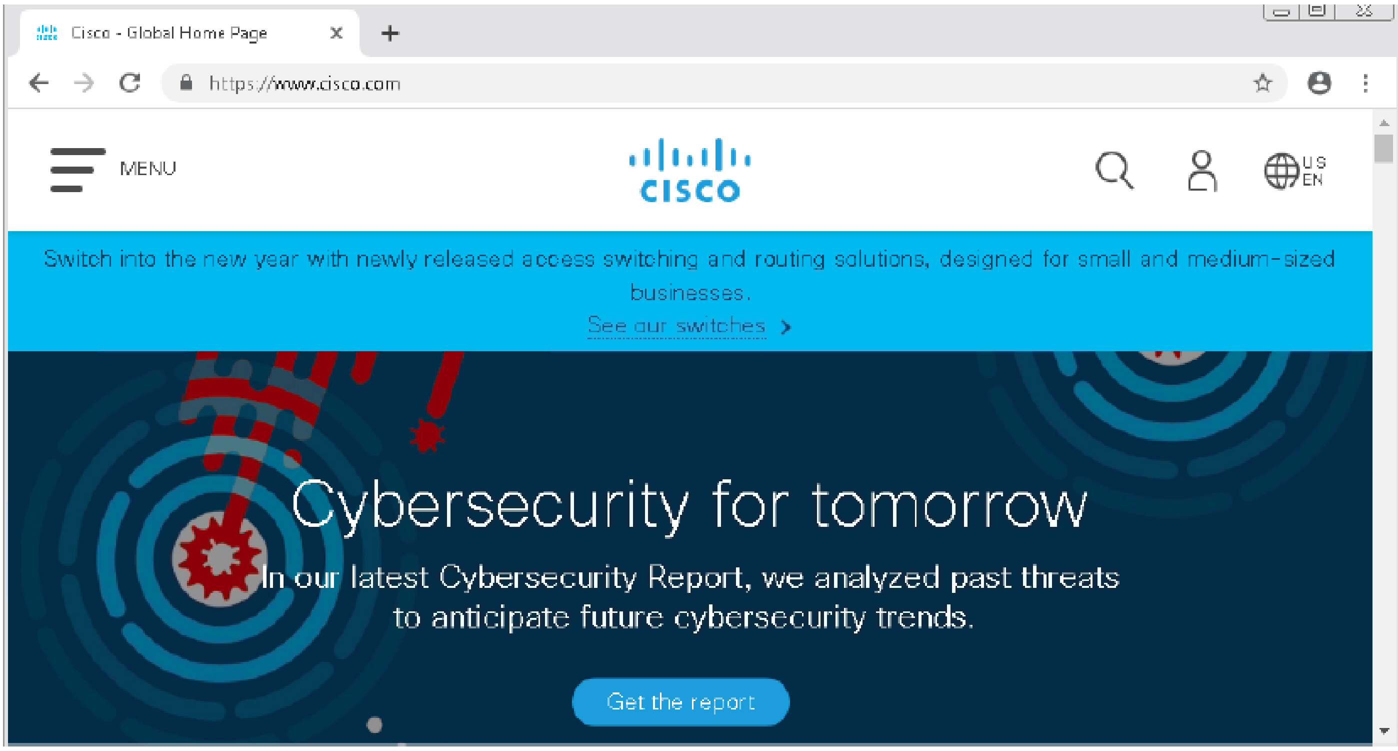
Step 1. Check the DNS server and IP address information on your host machine as seen in the image:



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
```

Step 2. Confirm you can navigate to cisco.com as seen in the image:

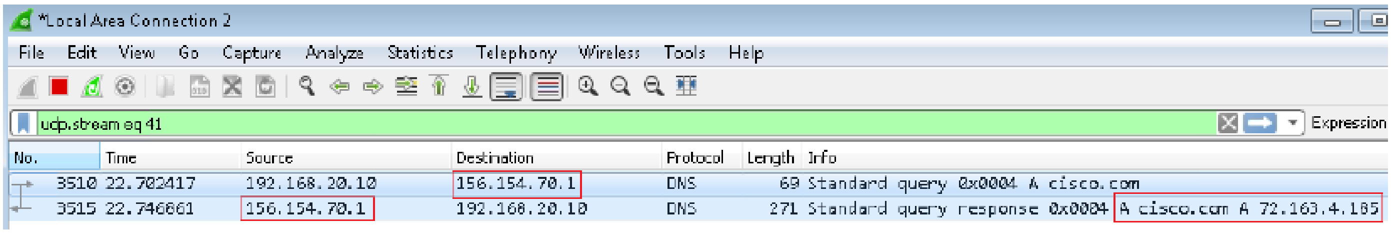


Switch into the new year with newly released access switching and routing solutions, designed for small and medium-sized businesses.
See our switches >

Cybersecurity for tomorrow

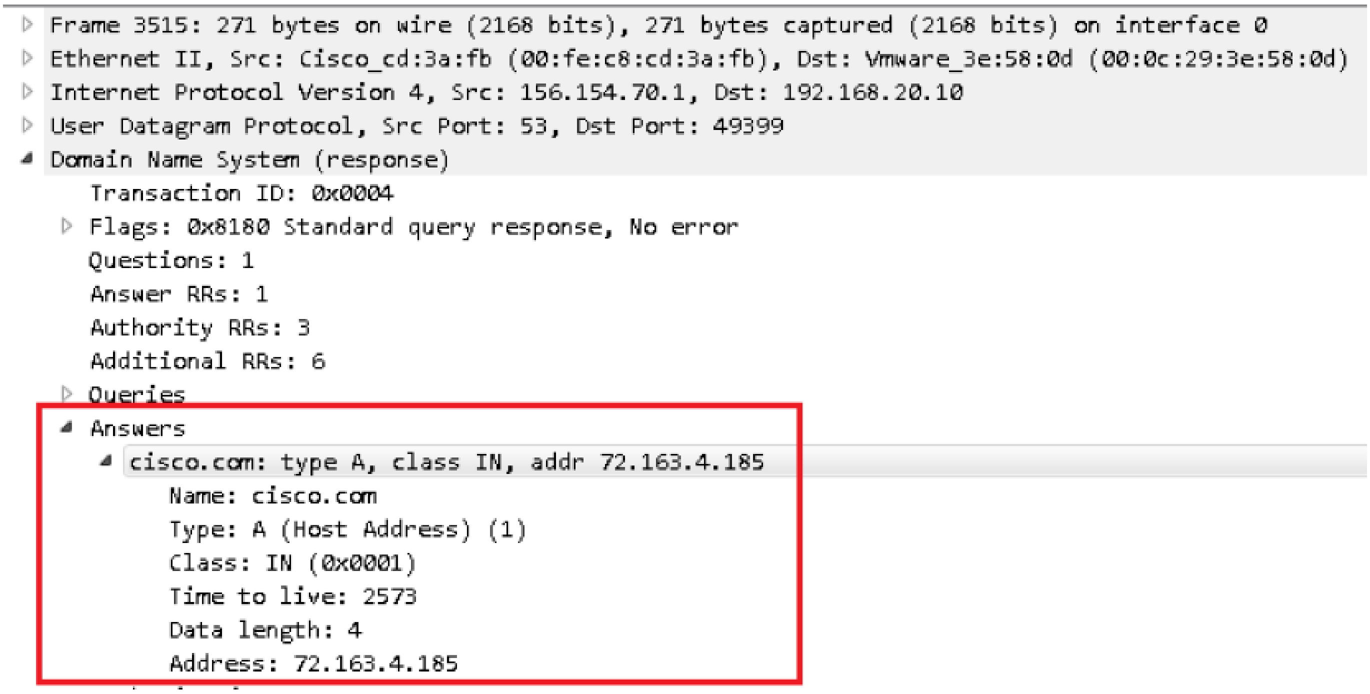
In our latest Cybersecurity Report, we analyzed past threats to anticipate future cybersecurity trends.

Step 3. Confirm with packet captures that DNS is resolved correctly:


*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression

```
udp.stream eq 41
```

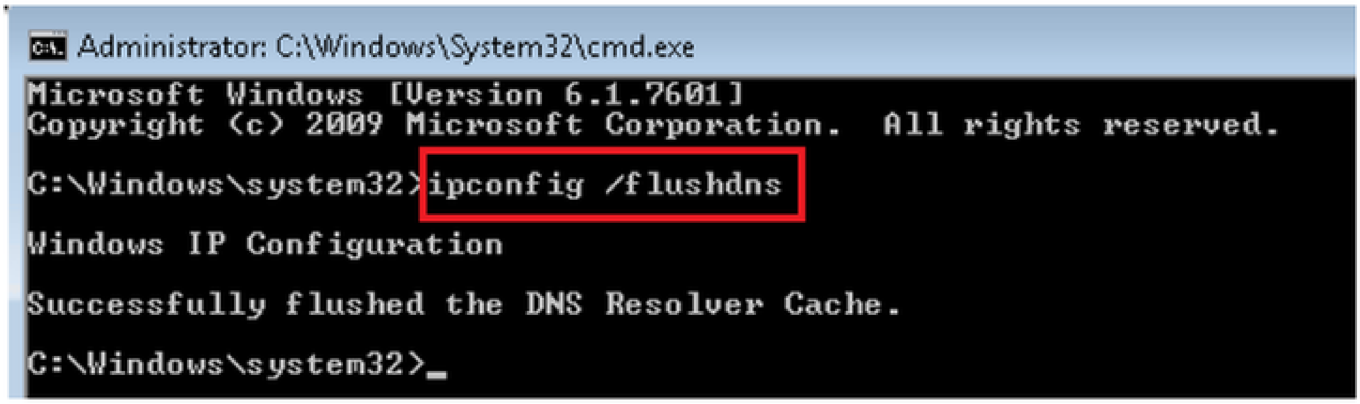
No.	Time	Source	Destination	Protocol	Length	Info
3510	22.702417	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0004 A cisco.com
3515	22.746861	156.154.70.1	192.168.20.10	DNS	271	Standard query response 0x0004 A cisco.com A 72.163.4.185



```
▷ 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
```

After the DNS Policy is Applied

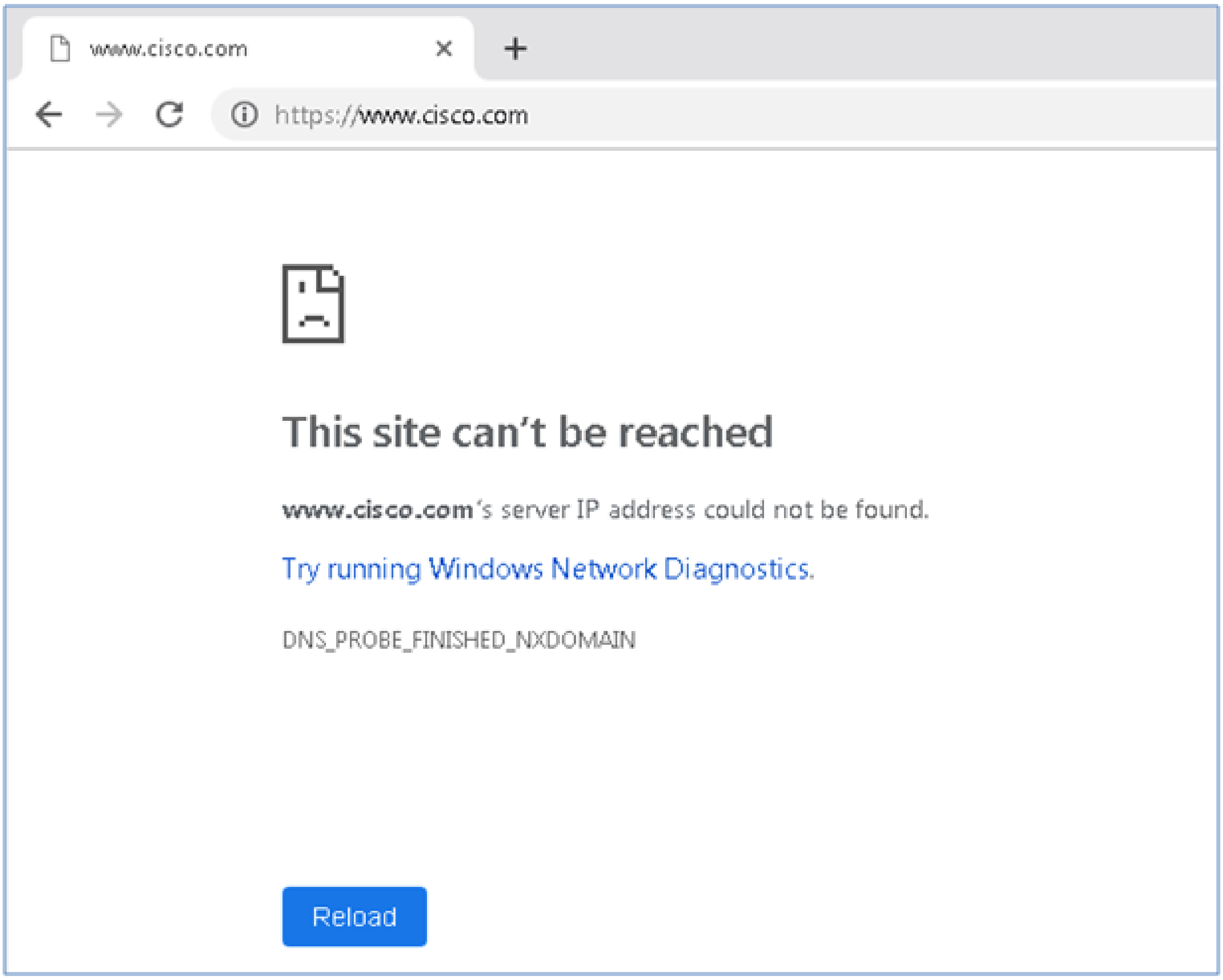
Step 1. Clear DNS cache on your host with the command **ipconfig /flushdns.**



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>_
```

Step 2. Navigate to the domain in question with a web browser. It should be unreachable:



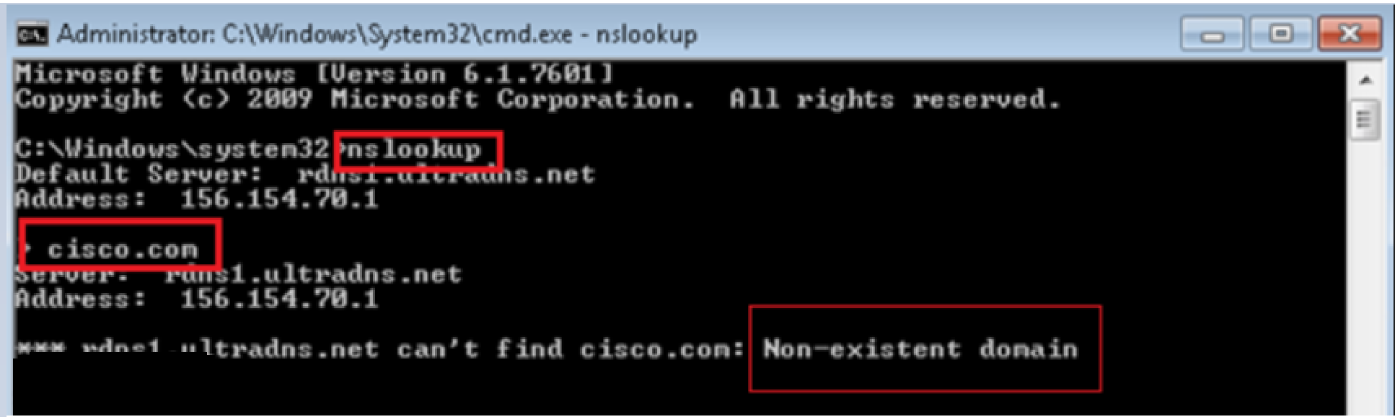
This site can't be reached

www.cisco.com's server IP address could not be found.

Try running Windows Network Diagnostics.

DNS_PROBE_FINISHED_NXDOMAIN

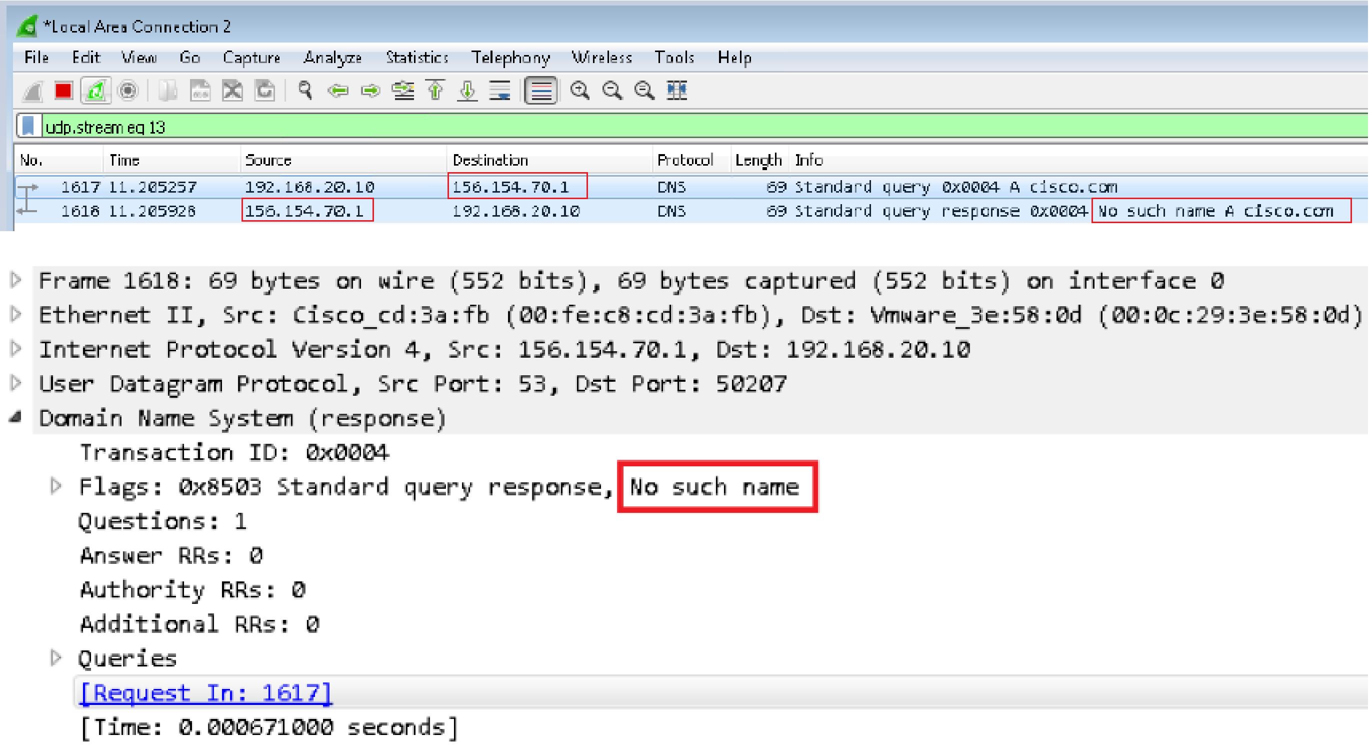
Step 3. Try to issue **nslookup** on the domain cisco.com. The name resolution fails.



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

*** rdns1.ultradns.net can't find cisco.com: Non-existent domain
```

Step 4. Packet captures show a response from the FTD, instead of the DNS server.



*Local Area Connection 2

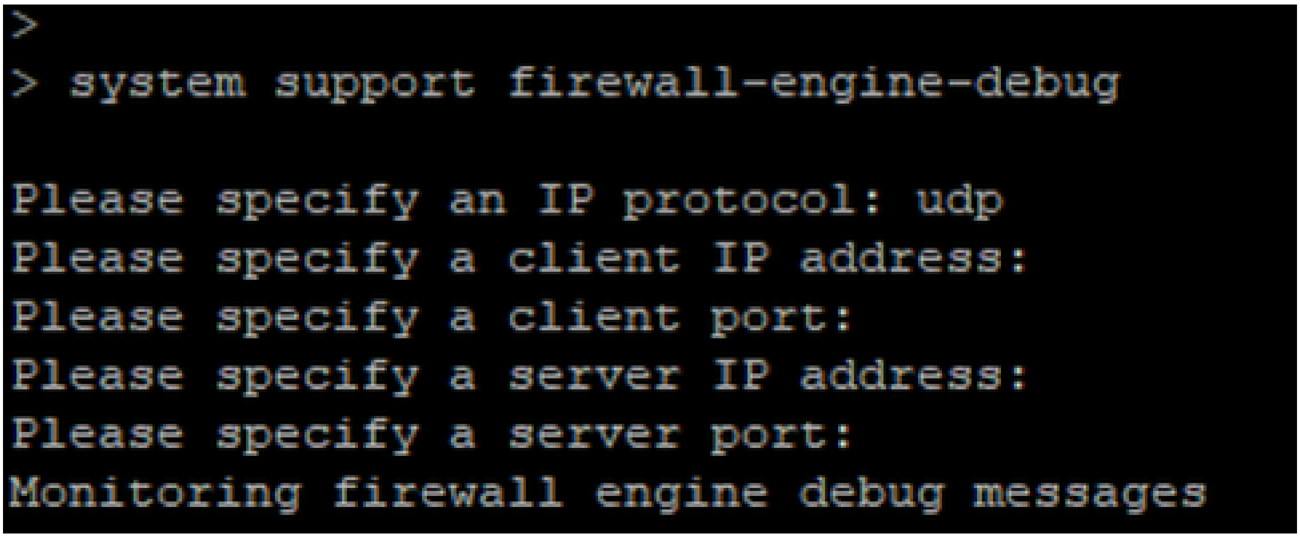
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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
```

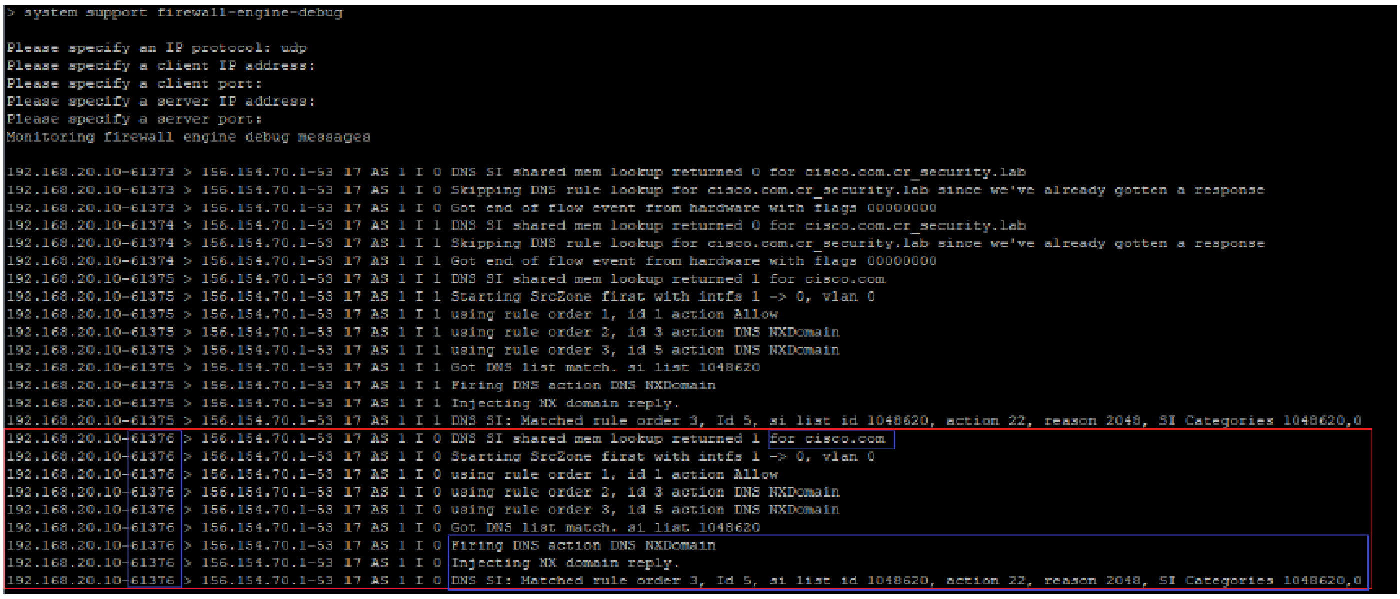
```
▷ Frame 1618: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
▷ Ethernet II, Src: Cisco_cd:3a:fb (00:fe:c8:cd:3a:fb), Dst: Vmware_3e:58:0d (00:0c:29:3e:58:0d)
▷ Internet Protocol Version 4, Src: 156.154.70.1, Dst: 192.168.20.10
▷ User Datagram Protocol, Src Port: 53, Dst 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]
```

Step 5. Run debugs in FTD CLI: system support firewall-engine-debug and specify UDP protocol.



```
>
> 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
```

*Debugs when cisco.com is matched:

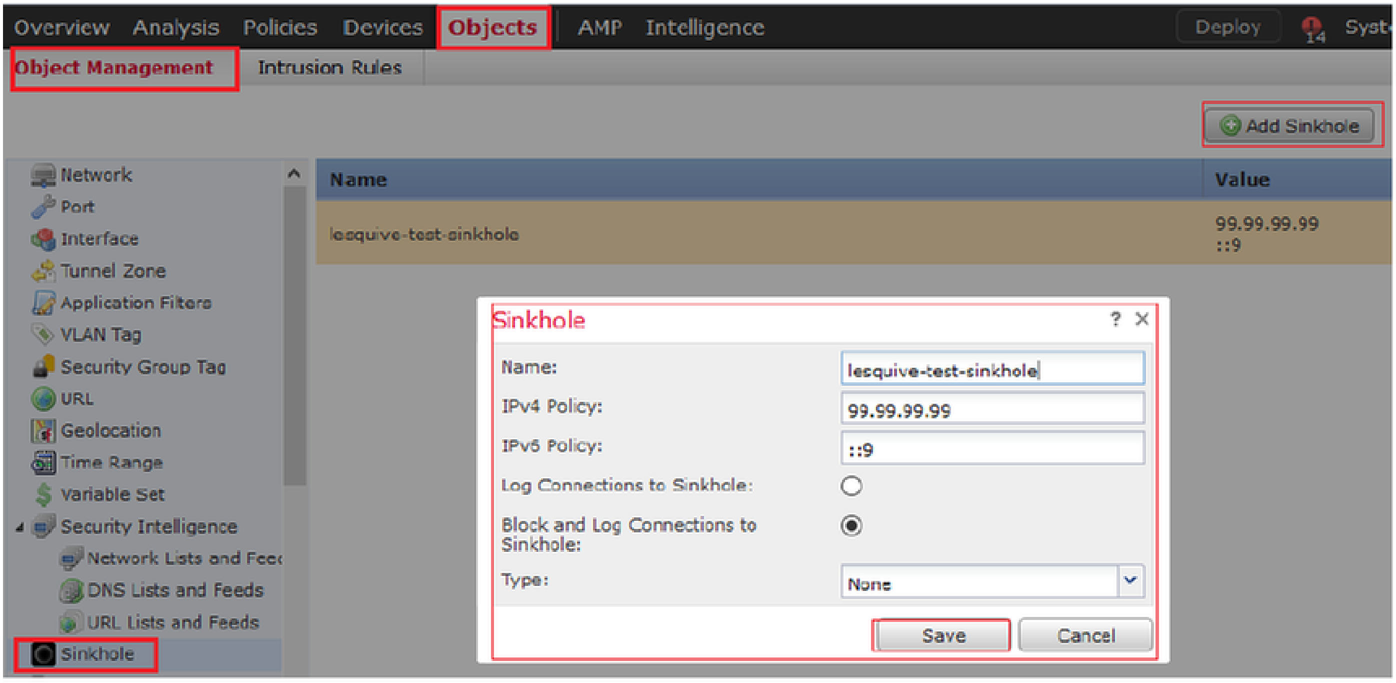


```
> system support firewall-engine-debug

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
```

Optional Sinkhole Configuration

A DNS sinkhole is a DNS server that provides false information. Instead of returning a “No such name” DNS response to DNS queries on domains you’re blocking, it returns a fake IP address.

Step 1. Navigate to Objects >> Object Management >> Sinkhole >> Add Sinkhole and create the fake IP address information.



Name	Value
lesquive-test-sinkhole	99.99.99.99 ::9

Name: lesquive-test-sinkhole

IPv4 Policy: 99.99.99.99

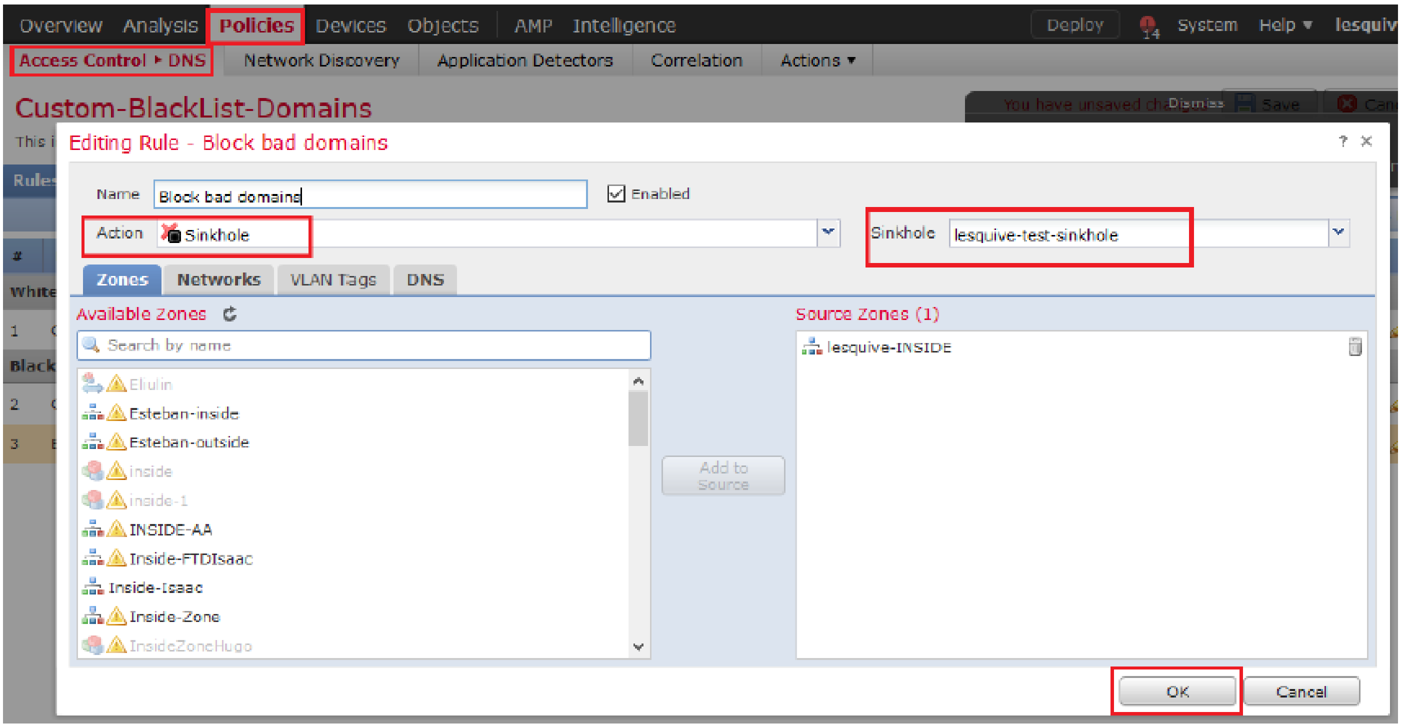
IPv6 Policy: ::9

Log Connections to Sinkhole: ○

Block and Log Connections to Sinkhole: ●

Type: None

Step 2. Apply the sinkhole to your DNS Policy and deploy changes to FTD.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy
System Help ▾ lesquiv
Access Control ▸ DNS
Network Discovery Application Detectors Correlation Actions ▾
You have unsaved ch Dismiss Save Cancel
Zones Networks VLAN Tags DNS
Add to Source
OK Cancel

Custom-BlackList-Domains

Editing Rule - Block bad domains

Name: Block bad domains ☑ Enabled

Action: Sinkhole

Sinkhole: lesquive-test-sinkhole

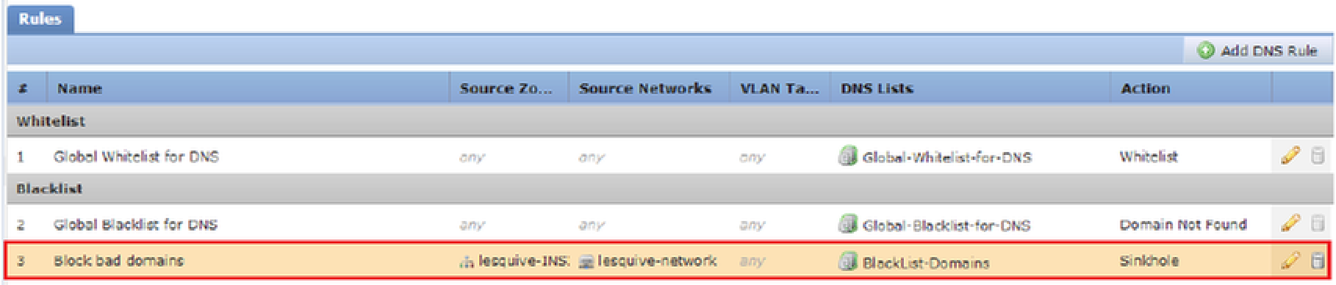
Available Zones

Search by name

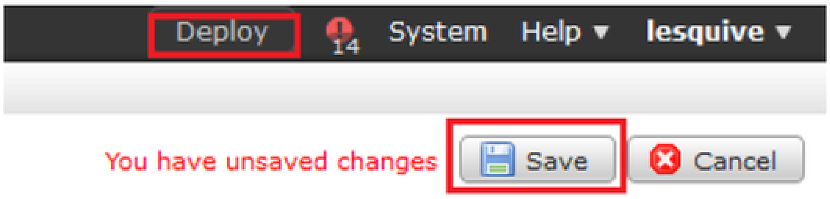
- Eliulin
- Esteban-inside
- Esteban-outside
- inside
- inside-1
- INSIDE-AA
- Inside-FTDIsaac
- Inside-Isaac
- Inside-Zone
- InsideZoneHugo

Source Zones (1)

- lesquive-INSIDE

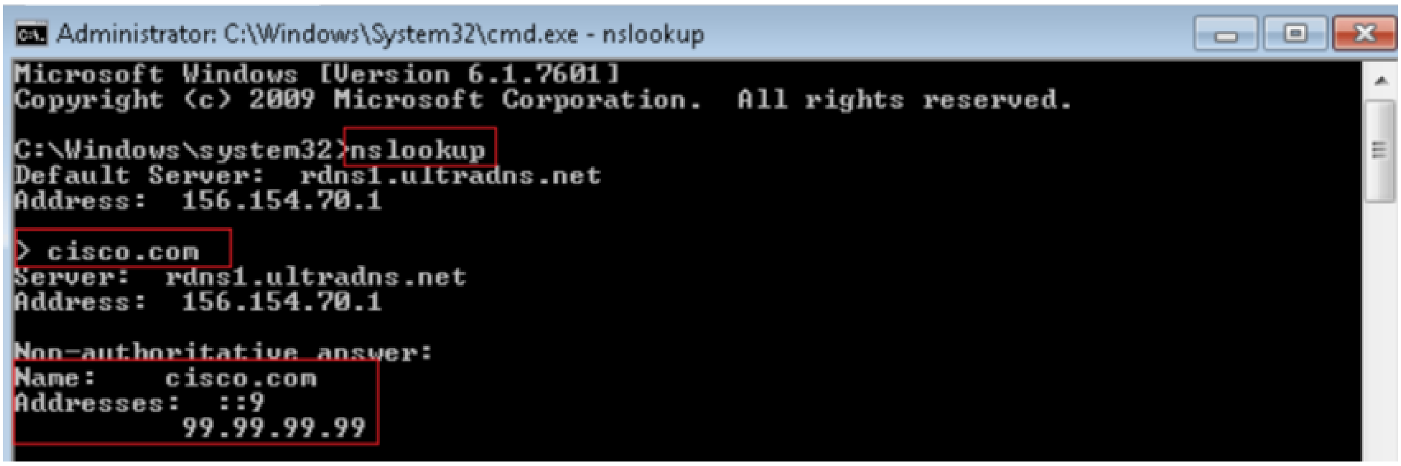


#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Block bad domains	lesquive-INS:	lesquive-network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

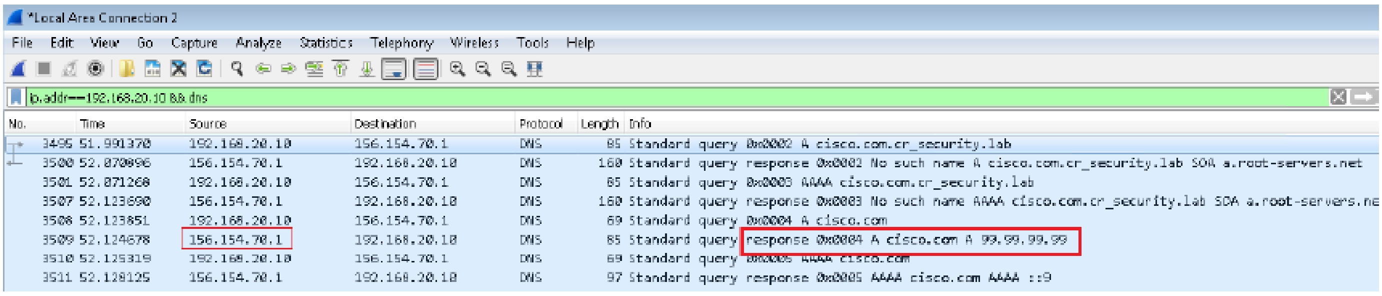


You have unsaved changes

Verify Sinkhole is working



```
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
```

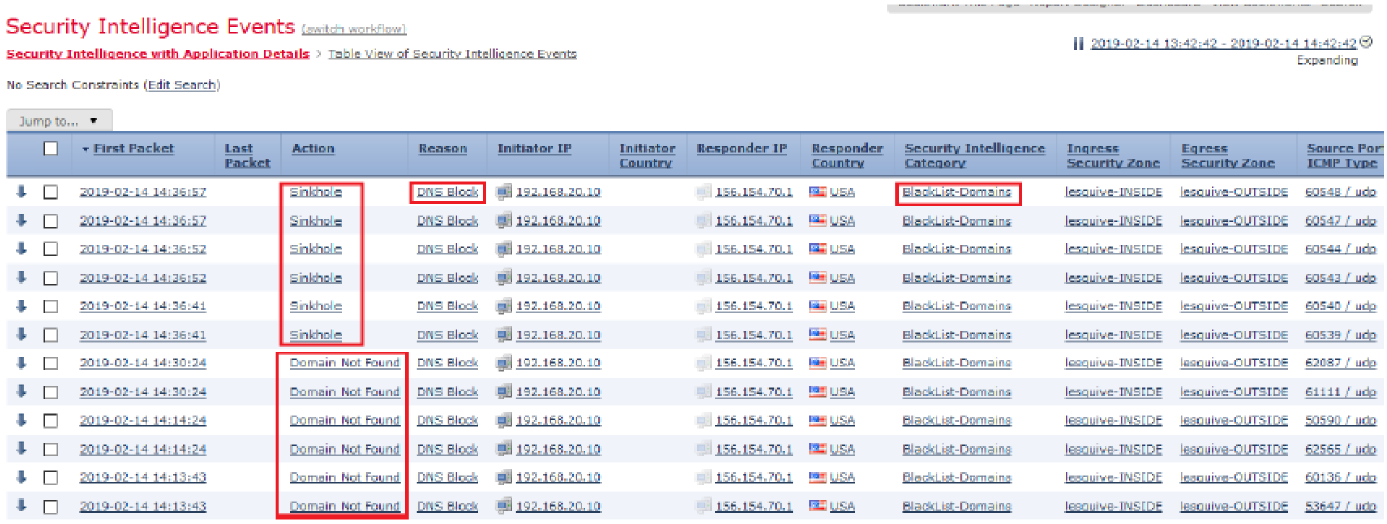

*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.20.10 && dns

```
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  52.070096   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  52.071260   192.168.20.10   156.154.70.1    DNS       85   Standard query 0x0003 AAAA cisco.com.cr_security.lab
3507  52.123690   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.ne
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
```

Troubleshoot

Navigate to Analysis >> Connections >> Security Intelligence Events to track all the events that are triggered by SI as long as you have enabled logging in the DNS Policy:


Security Intelligence Events (switch workflow)

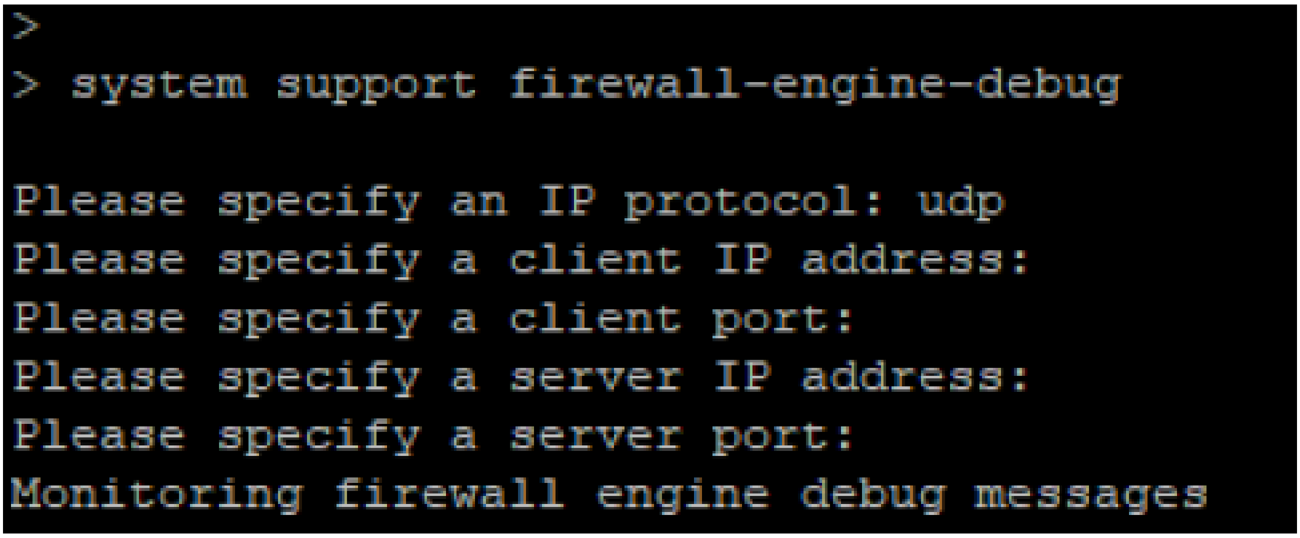
Security Intelligence with Application Details > Table View of Security Intelligence Events

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

No Search Constraints (Edit Search)

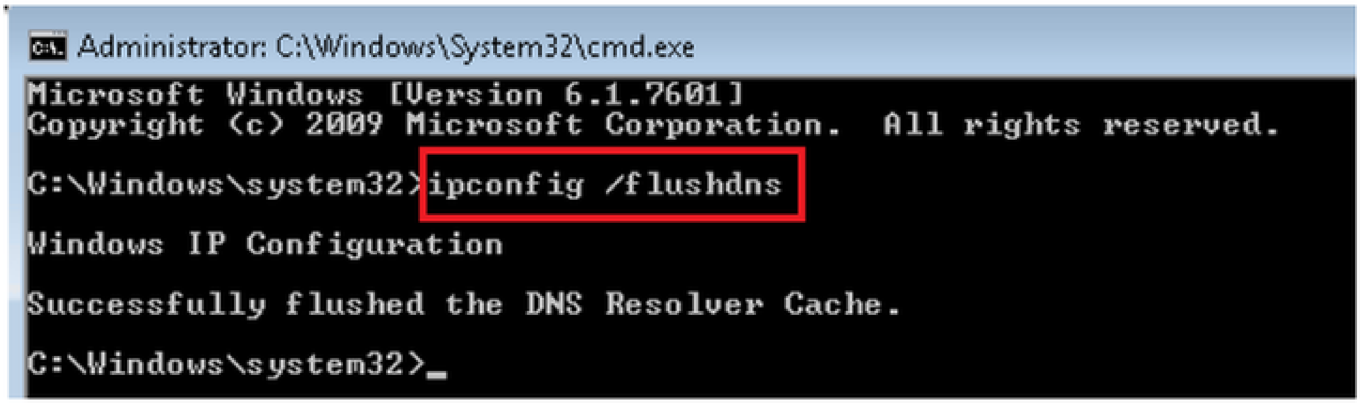
	□	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
⬇	□	2019-02-14 14:36:57		Sinkhole	DNS Block	192.168.20.10		156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	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

You can also use **system support firewall-engine-debug** command on the FTD that is managed by the FMC.



```
>
> 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
```

Packet captures can be helpful to confirm that DNS requests are making it to the FTD server. Don’t forget to clear the cache on your local host when testing.



```
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>_
```