

# FirePOWER Management Center مداخلتساب DNS رطح Center

## تايتوتحمل

[قمدقمل](#)

[قيساسال تابلطمل](#)

[تابلطمل](#)

[قمدختسمل تانوكمل](#)

[قيساسا تامولعم](#)

[قكبش لل يطيطختل مسرل](#)

[نويوتل](#)

[FMC ل اوليحتو قمتاق ل رطح ديرن يتل تالاجمل مداخلتساب قصصخم DNS قمتاق نويوت](#)

['دوجوم ريغ لاجمل' ل نويوت مت يذل عارجال' مداخلتساب ديچ DNS چهن قفاضا](#)

[كب صاخل لوصولاب مكحتل چهنل DNS چهن نويوت](#)

[قحصلا نم ققحتل](#)

[DNS چهن قيبطت لبق](#)

[DNS چهن قيبطت دع](#)

[قيرايتخال StackSlot قاطب قئيهت](#)

[لحول لمع نم دكات](#)

[اهخالص او عاطخال فاشكتسا](#)

## قمدقمل

كنكمي يتح DNS چهن ل (DNS) لاجمل مسا ماظن قمتاق قفاضا عارجل دننتمل اذه فصوي (SI) نامال تامولعم مداخلتساب اوقيبطت

## قيساسال تابلطمل

### تابلطمل

قيلال عيضاوملاب قفرعم كيديل نوكت ناب Cisco قيصوت

- Cisco ASA55XX ديدهتل دض عافدل نويوت
- Cisco قكركشل عباتل FireSIGHT قراذ زكرم نويوت

### قمدختسمل تانوكمل

- Cisco ASA5506W-X Threat Defense (75)، رادصل (Build 42) 6.2.3.4
- ليعشتل ماظن (42 قينب) 6.2.3.4: جم انربل رادصل VMWare ل Cisco Firepower قراذ زكرم  
Cisco Fire Linux OS 6.2.3 (Build13)

قصاخ قيلمعم قئيب ي ق دوجومل قزهجال نم دننتمل اذه ي ق دراول تامولعمل عاشنل مت تناك اذ (يضارتفا) حوسمم نويوتب دننتمل اذه ي ق قمدختسمل قزهجال عيمج تادب رما يال لمحمل ريثاتل لل كمهف نم دكات ف، ليعشتل دي ق كتكبش

## ةيساسأ تامولعم

أ URL نېوانع وأ IP نېوانع ىلإ وأ نم رورملا ةكرح رظح قيرط نع Security Intelligence لمعي يسئرلا زيكرتلا نوكي، دنتسمل اذه في .ةفورعم ةئيس ةعمس اهل يتلا تالاجملا عامسأ .ءادوسلا ةمئاقلا في لاجملا مسا جاردا وه

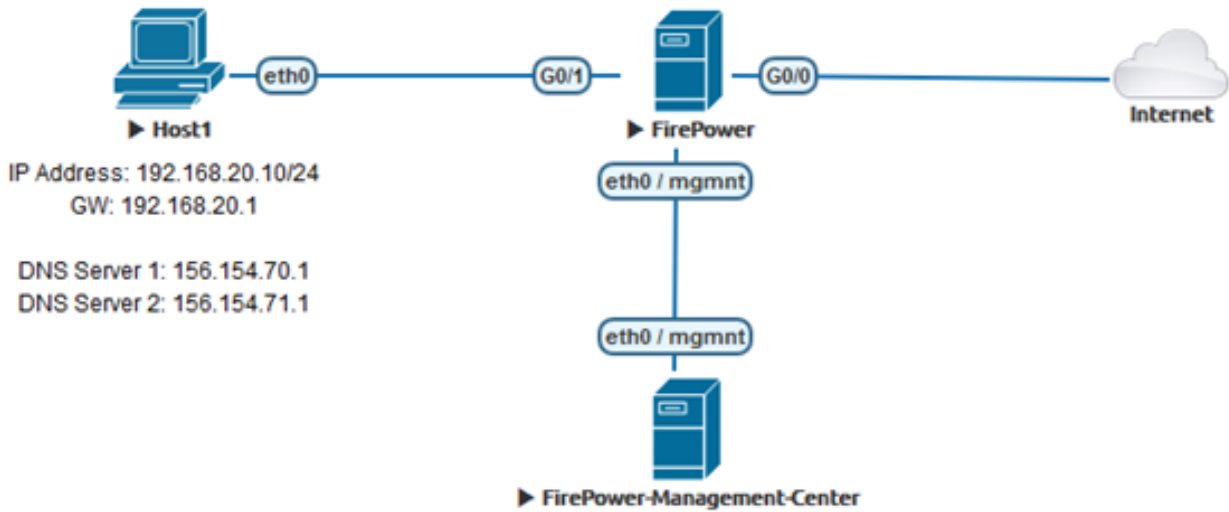
لاجملا 1 لتك لاثملا مدختسأ

- cisco.com

نأ بجي URL نأ يه ةلكشملا نكلو، عقاوملا هذه ضعب رظحل URL ةيفصت مادختسا كنكمي تالاجم ىلع عم DNS ل ءادوسلا ةمئاقلا زكرت نأ نكمي، ىرخأ ةيحان نمو .امامت اقباطم نوكي URL في تاريغت وأ ةيعرف تالاجم يا لوح قلقلا ىلإ ةجالحا نود "cisco.com" لثم

يرايتخ Sinkhole ةقاطب نيوكت حيصوت اضيأ متي، دنتسمل اذه ةياهن في

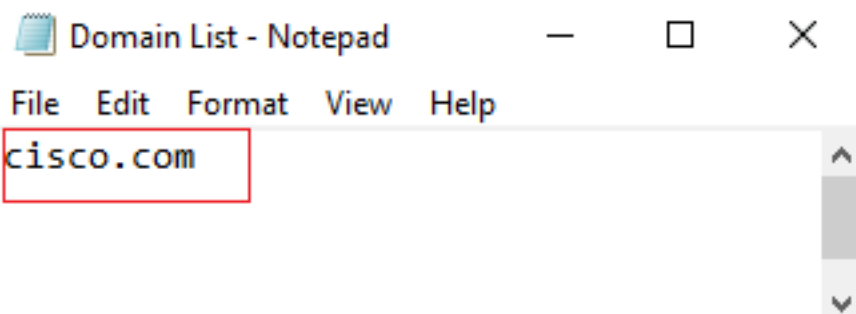
## ةكبشلال يطيختلا مسرلا



## نيوكتلا

ةمئاقلا رظح ديرن يتلا تالاجملا مادختساب ةصصخم DNS ةمئاق نيوكت FMC ىلإ اهليحتو

ىلع .txt فلم ظفح .اهرظح ديرت يتلا تالاجملا مادختساب .txt .فلم ءاشناب مق 1. ةوطخلا كبساح:



ةفاضإ >> بي و زومو DNS مئاوق >> نئاكلا ةرادإ >> نئاك ىلا لقتنا ، FMC ي ف 2. ةوطخلا بي و زومو DNS ةمئاوق .

The screenshot shows the Cisco Security Intelligence Center (SIC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' menu is expanded, showing 'Object Management' and 'Intrusion Rules'. Under 'Object Management', there is a sub-menu with 'Security Intelligence', 'Network Lists and Feeds', 'DNS Lists and Feeds', and 'URL Lists and Feeds'. The 'DNS Lists and Feeds' sub-menu is selected. In the main content area, there are two buttons: 'Update Feeds' and 'Add DNS Lists and Feeds'. Below the buttons is a table with the following data:

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

بجي و ةمئاوق عونلا نوكي نأ بجي و ، "BlackList-Domains" ىمست ةمئاوق ءاشناب مق 3. ةوطخلا روصلال ي ف حضوم وه امك ةينعملال تالاجملا عم .txt فلم ليحت

The screenshot shows the 'Security Intelligence for DNS List / Feed' dialog box. The 'Name' field is filled with 'BlackList-Domains'. The 'Type' dropdown menu is set to 'List'. The 'Upload List' field is empty, and the 'Browse...' button is highlighted. There are 'Upload', 'Save', and 'Cancel' buttons at the bottom of the dialog.

**Security Intelligence for DNS List / Feed** ? X

Name: BlackList-Domains

Type: List

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

Upload

Save Cancel

لثاملا اذه يف .تالاجملا عيجم DNS تالخدإ ددع أرقى نأ بجي ،.txt . فلم ليحت دنع هنا طحال\*  
 1: يلامج

**Security Intelligence for DNS List / Feed** ? X

Name: BlackList-Domains

Type: List

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

Upload

---

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

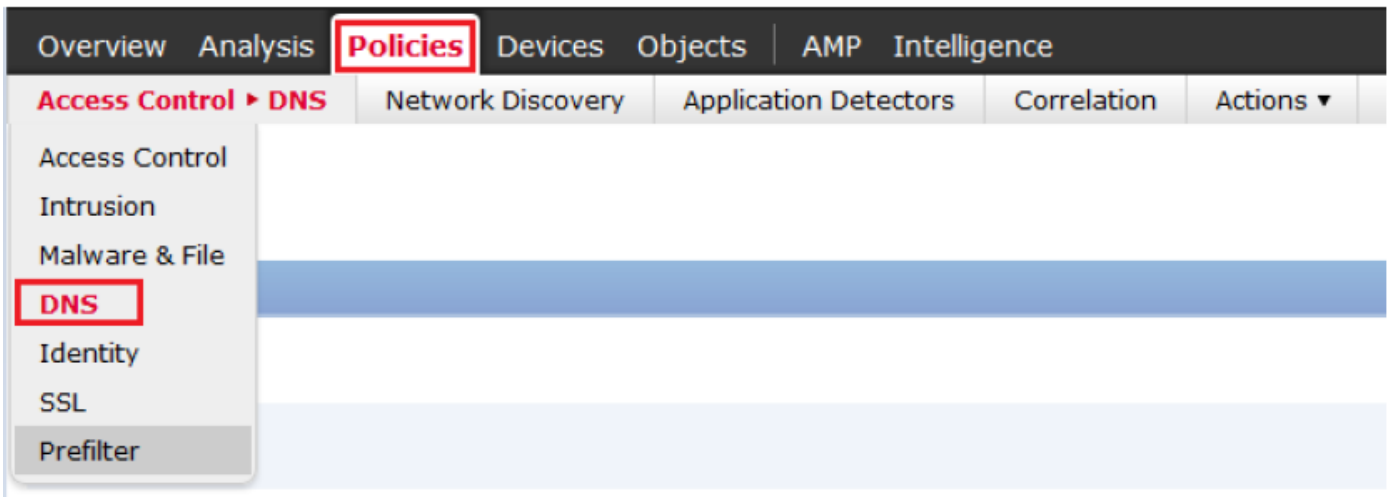
Number Of DNS entries: 1

Save Cancel

'دوجوم ريغ لاجملا' ل هنيوكت مت يذلا عارجلا' مادختساب ديجم DNS جهن ةفاضل

DNS ةمئاقو ردصم ةكبش و ردصم ةقطنم ةفاضل نم دكأت\*

DNS: ةسايس ةفاضل >> DNS >> لوصول يف مكحتلا >> تاسايسلا ل لقتنا . 1 ةوطخلا



Object Management Access Control Import/Export



### New DNS Policy

Name: Custom-BlackList-Domains

Description: This is a test by lesquive |

**Save** Cancel

ةروصولا يف رهظي امك DNS ةدعاق ةفاضلا 2. ةوطخلا

Custom-BlackList-Domains  
This is a test by lesquive

Save Cancel

Rules **+ Add DNS Rule**

#	Name	Source Zones	Source Networks	VLAN Tags	DNS Lists	Action	
<b>Whitelist</b>							
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	
<b>Blacklist</b>							
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	

### Add Rule

? x

Name:   Enabled

Action:

**Zones** | Networks | VLAN Tags | DNS

Available Zones

- Search by name
- JVILLALToutside
- lesquive-INSIDE
- lesquive-OUTSIDE
- Manuel-Inside
- MANUEL-INSIDE-2
- Manuel-Outside
- MANUEL-OUTSIDE-2
- Marco-Inside
- Marco-Outside
- Melincide

Source Zones (1)

- lesquive-INSIDE

Add to Source

Add Cancel

### Add Rule

? x

Name:   Enabled

Action:

**Zones** | Networks | VLAN Tags | DNS

Available Zones

- Search by name
- JVILLALToutside
- lesquive-INSIDE
- lesquive-OUTSIDE
- Manuel-Inside
- MANUEL-INSIDE-2
- Manuel-Outside
- MANUEL-OUTSIDE-2
- Marco-Inside
- Marco-Outside
- Melincide

Source Zones (1)

- lesquive-INSIDE

Add to Source

Add Cancel

### Add Rule

? x

Name:   Enabled

Action:

**Networks** | Zones | VLAN Tags | DNS

Available Networks

- Search by name or value
- IPv6-to-IPv4-Relay-Anycast
- jvillalt-Inside
- lesquive-inside-network
- lesquive-network
- Manuel-Inside-NET
- Marco\_PAT
- Network\_Marco
- Outside-isaac
- pat-hugo
- Pat\_Marco

Source Networks (1)

- lesquive-network

Add to Source

Enter an IP address  Add

Add Cancel

## Add Rule

? x

Name:   Enabled

Action:

Zones Networks VLAN Tags **DNS**

DNS Lists and Feeds

- DNS Phishing
- DNS Response
- DNS Spam
- DNS Suspicious
- DNS Tor\_exit\_node
- 0.0.0.0
- BlackList-Domains**
- Global-Blacklist-for-DNS
- Global-Whitelist-for-DNS
- test

Add to Rule

Selected Items (1)

- BlackList-Domains

Add Cancel

Rules

+ Add DNS Rule

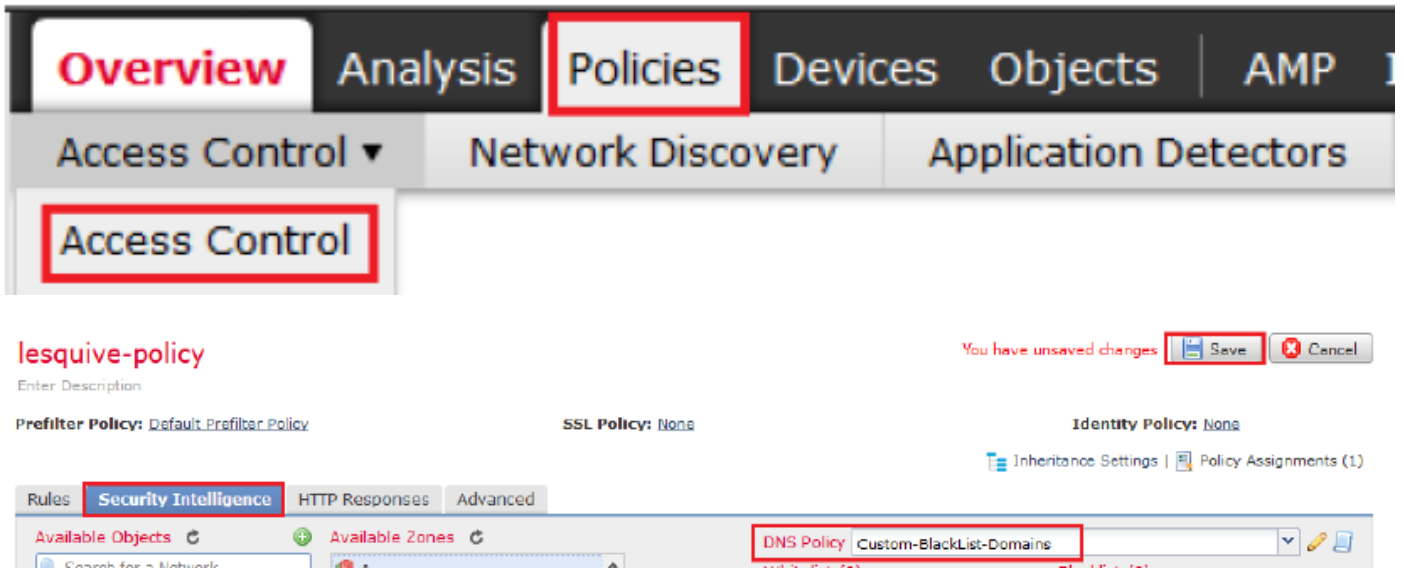
#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action	
Whitelist							
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist	
Blacklist							
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found	
3	Block bad domains	lesquive-INS	lesquive-network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

ةدعاقلا بيترت لوح ةمهم تامولم

- ىرخألا دعاقولا عيمج قبسيو لوالا وه ضيبألا ملالعل نوكي ام امئاد.
- ،تالاجملا ةددعتم رشنلا تايلمع يف طقف Descendant DNS Whitelists ةدعاق رهظت ،ىرخألا دعاقولا عيمج قبسيو يناثلا زكرملا نوكي ام امئاد .ةقرولا ةعباتلا ريغ تالاجملا ةمئلعل اعاضيبلا ةدعاقلا ادع ام
- امئاد اعاضيبلا مئاقولا دعاقو نوكو ،ءادوسلا ةمئاقلا مسق ضيبألا مسق قبسي ىرخأ دعاقو ىلع ةيقبسا
- ذأتو ءادوسلا ةمئاقلا مسق يف لوالا يه ةمئلعل ءادوسلا ةمئاقلا نوك ام امئاد ،ىرخألا ءادوسلا ةمئاقلا واشاشلا دعاقو عيمج ىلع ةيولوالا
- ،تالاجملا ةددعتم رشنلا تايلمع يف طقف عباتلا DNS ل ءادوسلا مئاقولا ةدعاق رهظت ،مسق يف ةيوناثلا ةبترملا يف نوك ام امئاد .ةقرولا ةعباتلا ريغ تالاجملا يف ةمئاقلا ادع ام ىرخألا ءادوسلا ةمئاقلا واشاشلا دعاقو عيمج قبستو ءادوسلا ةمئاقلا ةمئلعل ءادوسلا
- .BlackList و Monitor دعاقو ىلع ءادوسلا ةمئاقلا مسق يوتحي
- تمق اذا ضيبألا مسقلا يف ماظنلا عضوم يقبي ،الو DNS ةدعاق ءاشناب موقت ام دنع ةيلمع يئيعتب تمق اذا ءادوسلا ةمئاقلا مسق يف رخأ ،أو WhiteList ةيلمع نييعتب ىرخأ

## كب صاخلا لوصولاب مكحتلا جهنل DNS جهن نييعت

ءاكذ >> كب صاخلا FTD ب صاخلا جهنلا >> لوصولا يف مكحتلا >> تاسايسلا ىلا لقتنا هءاشنأ يذلا جهنلا فضاو DNS جهن >> نامألا



ءاهتنالال دنع ءاربيغءال ءفاك رشن نم دءاء.

## ءءصلا نم ققءءال

### DNS ءهن قيبءء لبء

بي ءءصوم وه امك بيضءال زاهءال لىء IP ءاونءو DNS مءاءءامولءم نم ققءء 1. ءوءءال ءرءصلا:

```

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

Ethernet adapter Local Area Connection 2:

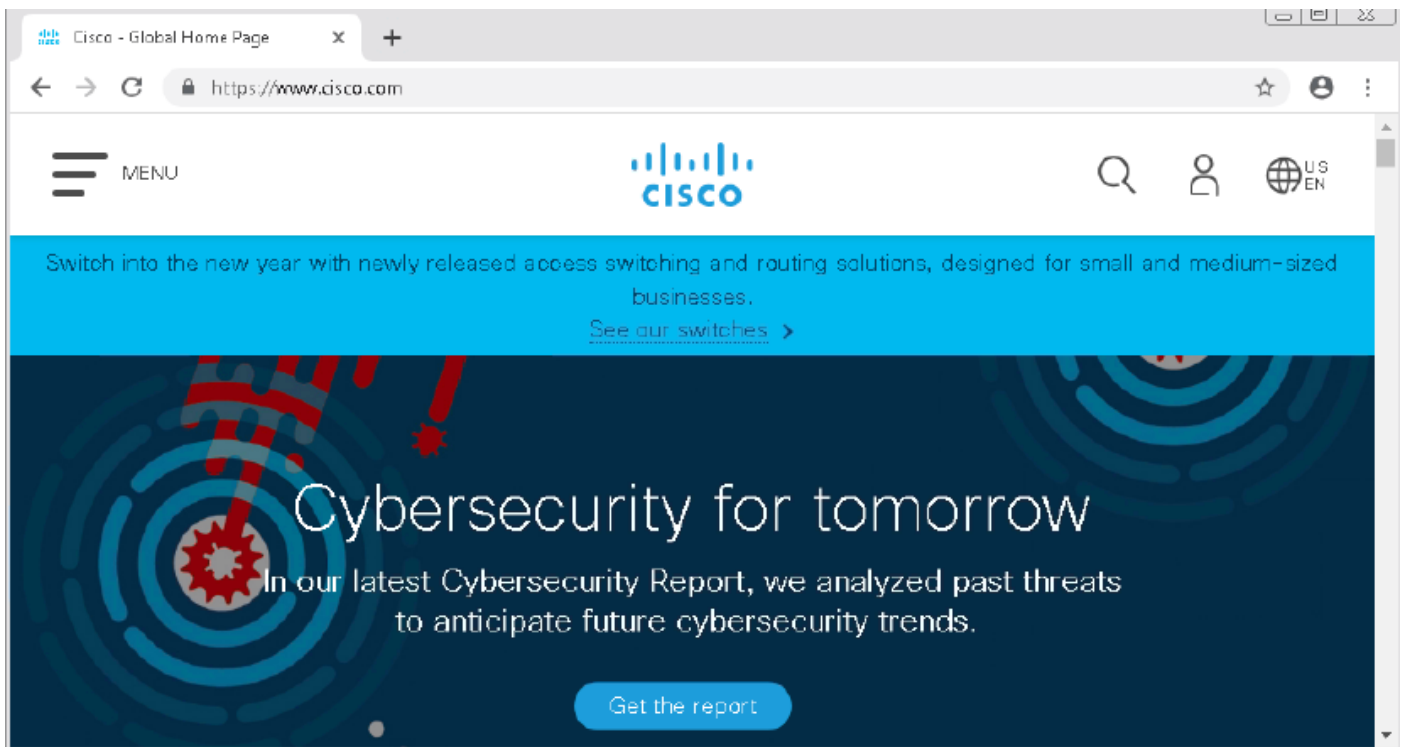
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #
2
Physical Address. . . . . : 00-0C-29-3E-58-0D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b168:e9aa:5b12:217b%13(Preferred)
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
  
```

ءرءصلا بي ءءصوم وه امك cisco.com لىءال لاقءءنالال كءكم بي هنأ نم دءاء 2. ءوءءال:





حیحص لكشب هلح مت DNS نأ مزحلا طاقثلا مادختساب ديكتألا 3. ةوطخل

No.	Time	Source	Destination	Protocol	Length	Info
3510	22.702417	192.168.20.10	156.154.70.1	DNS	69	Standard query 0x0004 A cisco.com
3515	22.746661	156.154.70.1	192.168.20.10	DNS	271	Standard query response 0x0004 A cisco.com A 72.163.4.185

```

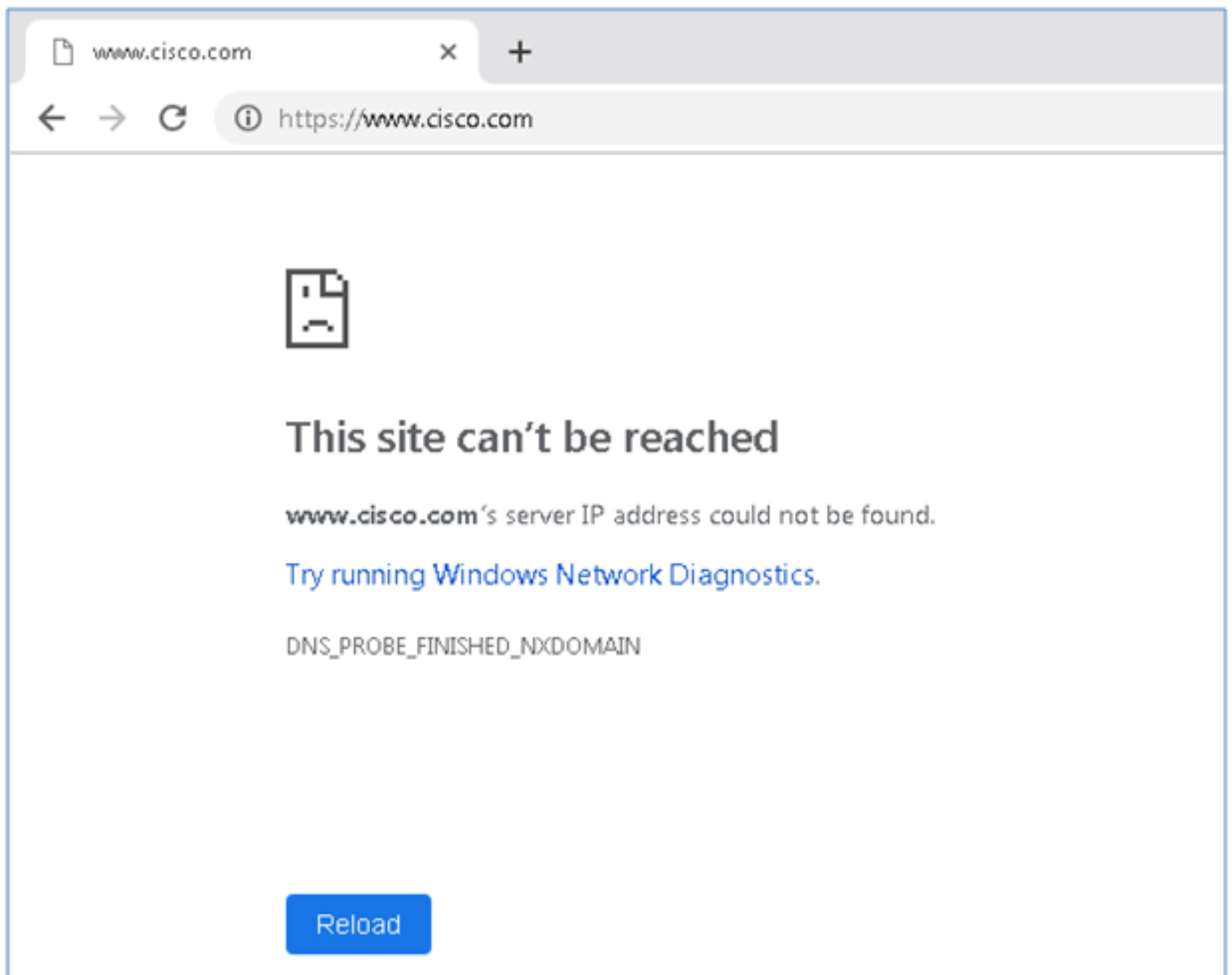
> Frame 3515: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface 0
> Ethernet II, Src: Cisco_cd:3a:fb (00:fe:c8:cd:3a:fb), Dst: Vmware_3e:58:0d (00:0c:29:3e:58:0d)
> Internet Protocol Version 4, Src: 156.154.70.1, Dst: 192.168.20.10
> User Datagram Protocol, Src Port: 53, Dst Port: 49399
  Domain Name System (response)
    Transaction ID: 0x0004
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 6
    Queries
      Answers
        cisco.com: type A, class IN, addr 72.163.4.185
          Name: cisco.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 2573
          Data length: 4
          Address: 72.163.4.185
  
```

## DNS جهن قيبت دع

رمال مادختساب كفيضم لىع DNS ل تقؤملا نيزختلا ةركاذ حسمب مق 1. ةوطخل  
/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>_
```

ىل لوصول نوکي نأ دبالو .بيو ضرعت سم مادخت ساب ينعمل لاجملا ىل لقتنا 2. ةوطخل  
نكم ريغ تامولعمل هذه:



مسالال ليلحت لشف . cisco.com لاجملا ىلع nslookup رادصا لواح 3. ةوطخل

```

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

C:\Windows\system32>nslookup
Default Server: rdns1.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdns1.ultradns.net
Address: 156.154.70.1

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

```

DNS مداخل نم ال د ب ، FTD نم ةباجتسا مزحلا روص رهظت 4. ةوطخل

The image shows a Wireshark capture of a DNS transaction. The packet list pane shows two packets: a standard query (No. 1617) and a standard query response (No. 1618). The response packet contains the text 'No such name A cisco.com'. The packet details pane for packet 1618 shows the Domain Name System (response) section with the following information:

- 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]

FTD CLI ف ءاطخأل احيصت ليغشت 5. ةوطخل engine-debug رادج ماطنلا معد : UDP لوكوتورب ديحتو

```

>
> 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 قباطت دن ءاطخأل احيصت\*:

```

> 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

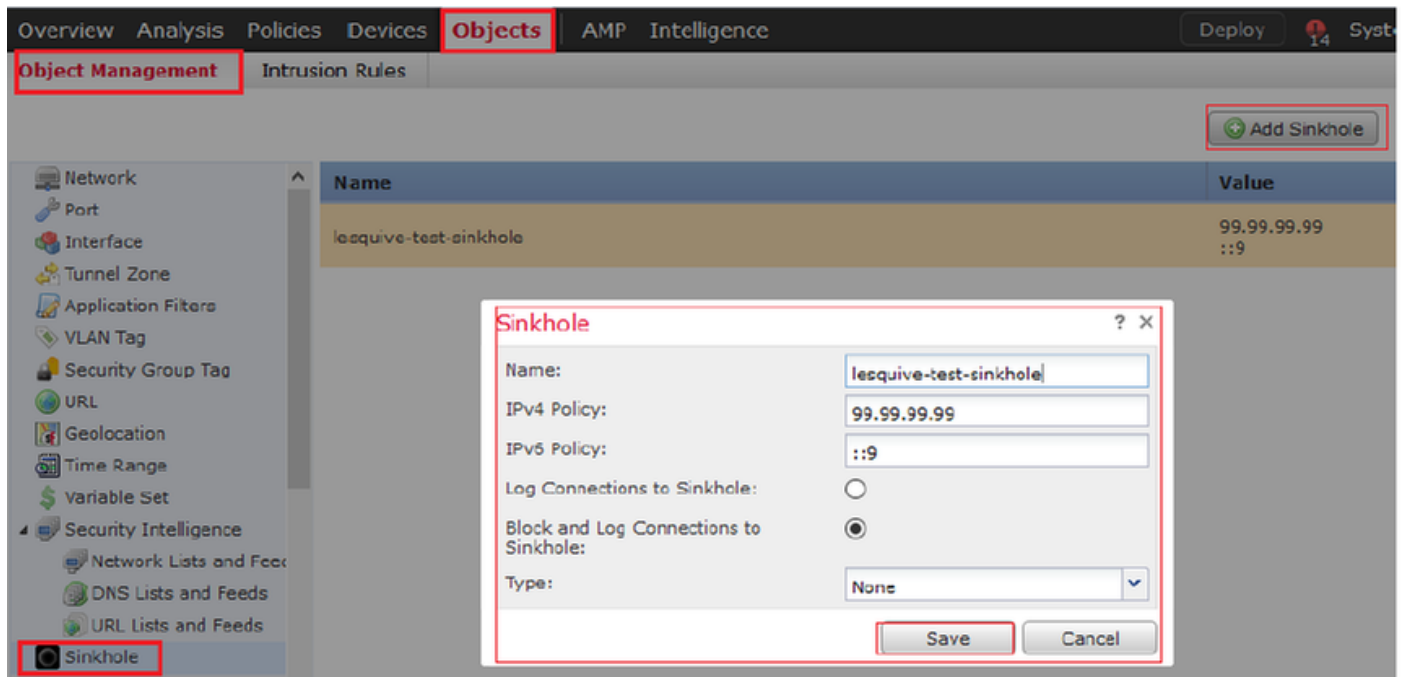
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.cr security.lab
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Skipping DNS rule lookup for cisco.com.cr security.lab since we've already gotten a response
192.168.20.10-61373 > 156.154.70.1-53 17 AS 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

```

## تاريخي تخال StackSlot قواطب ةئيهت

اذه لثم نودب" DNS ةباجتسإ عاجرا نم ال دب . ةئطاخ تامولعم رفوي DNS مداخ وه DNS Sinkhole فيزم IP ناووع عجرت اهنإف ، اهرطحج موقت يتللا تالاجملا ىلع DNS تامالعتسا ىلإ "مسالا

ةيادبلا ةحتف فضا >> ةرئادل ةحتف >> تانئاكل ةرادا >> تانئاكل ىلإ لقتنا . 1 ةوطخل فيزملا IP ناووع تامولعم عاشناب مقو



FTD. ىلع تاريخي تخال رشنو DNS جهن ىلع يلفسلل بقثلا قيبطت . 2 ةوطخل

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 14 System Help lesquive

Access Control DNS Network Discovery Application Detectors Correlation Actions

### Custom-BlackList-Domains

Editing Rule - Block bad domains

Name: Block bad domains  Enabled

Action: Sinkhole Sinkhole: lesquive-test-sinkhole

Available Zones:

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

Source Zones (1): lesquive-INSIDE

OK Cancel

Rules

Add DNS Rule

#	Name	Source Zo...	Source Networks	VLAN Ta...	DNS Lists	Action
<b>Whitelist</b>						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
<b>Blacklist</b>						
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

Deploy 14 System Help lesquive

You have unsaved changes

Save Cancel

لحوال لمع نم دكأت

```

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

## اهحال صا و عا طخال فاشك ت سا

تالاصت | Analysis (لجحتال) > Connections >> Security Intelligence Events (تالاصت) | لقتنا ني كمتب تمق املاط SI ةطساوب اهلي غشت متي يتال ثا دخال اعيمج بقعتل (نامال تامولعم DNS: جهن لى لوخدلا ليجست

Security Intelligence Events [\[switch workflow\]](#)

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

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

No Search Constraints [\(Edit Search\)](#)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port	ICMP Type
↓	2019-02-14 14:36:52		Sinkhole	DNS Block	192.168.20.10	USA	156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	60548 / udp	
↓	2019-02-14 14:36:52		Sinkhole	DNS Block	192.168.20.10	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	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	USA	156.154.70.1	USA	BlackList-Domains	lesquive-INSIDE	lesquive-OUTSIDE	53647 / udp	

هتراد مت يذال FTD لى مع system support firewall-engine-debug رمال مادختسا اضي كنكمي ةطساوب 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
```

ال FTD م داخ ي ف اهلعجت DNS تابلط نأ دي كأتل ةدي فم مزحلا طاقتل تايلمع نوكت نأ نكمي رابخال دنع يلحمل فيضم ال لى مع تقومل نيختل ةركاذ حسم سنت



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>\_

