

Bloccare il DNS con l'intelligence di sicurezza utilizzando Firepower Management Center

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurare un elenco DNS personalizzato con i domini che si desidera bloccare e caricare nell'FMC](#)

[Aggiungere un nuovo criterio DNS con l'azione configurata su 'dominio non trovato'](#)

[Assegnare i criteri DNS ai criteri di controllo di accesso](#)

[Verifica](#)

[Prima dell'applicazione dei criteri DNS](#)

[Dopo l'applicazione dei criteri DNS](#)

[Configurazione opzionale di Sinkhole](#)

[Verifica che Sinkhole funzioni](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la procedura per aggiungere un elenco DNS (Domain Name System) a un criterio DNS in modo da poterlo applicare con Security Intelligence (SI).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione Cisco ASA55XX Threat Defense
- Configurazione di Cisco Firepower Management Center

Componenti usati

- Cisco ASA5506W-X Threat Defense (75) versione 6.2.3.4 (build 42)
- Cisco Firepower Management Center per VMWare Versione del software: 6.2.3.4 (build 42) Sistema operativo: Cisco Fire Linux OS 6.2.3 (build13)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzionalità di Security Intelligence blocca il traffico da o verso indirizzi IP, URL o nomi di dominio con reputazione non valida. In questo documento, lo stato attivo è la blacklist dei nomi di dominio.

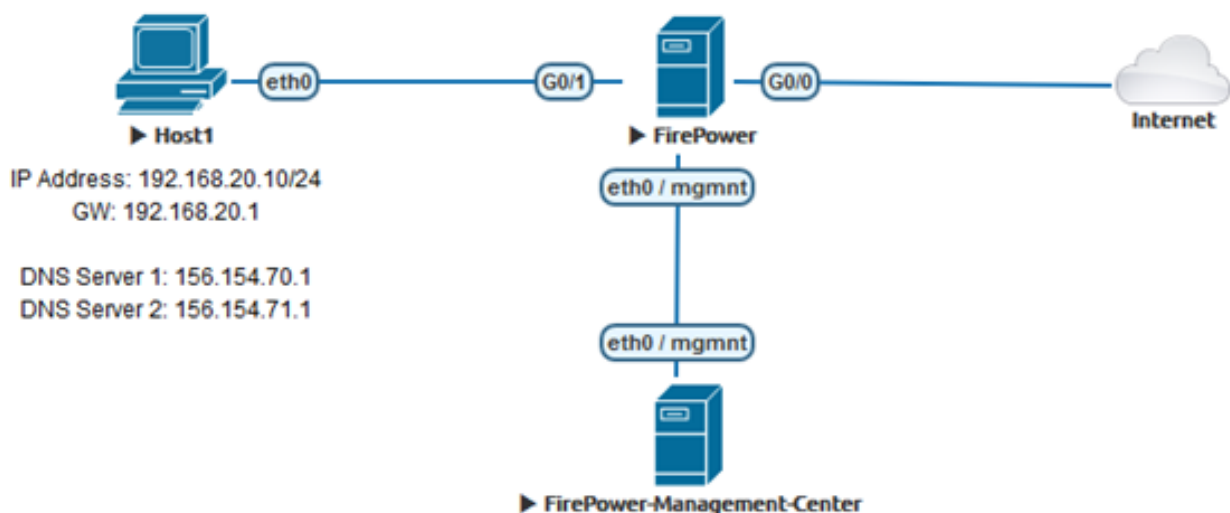
Nell'esempio è stato utilizzato il blocco 1 dominio:

- cisco.com

È possibile utilizzare il filtro URL per bloccare alcuni di questi siti, ma il problema è che l'URL deve corrispondere esattamente. D'altra parte, la lista nera di DNS con SI può focalizzare l'attenzione su domini come "cisco.com" senza doversi preoccupare di sottodomini o cambiamenti di URL.

Alla fine di questo documento, viene mostrata anche una configurazione Sinkhole opzionale.

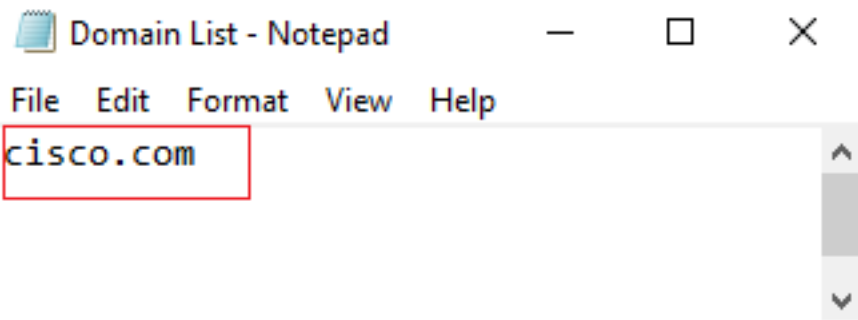
Esempio di rete



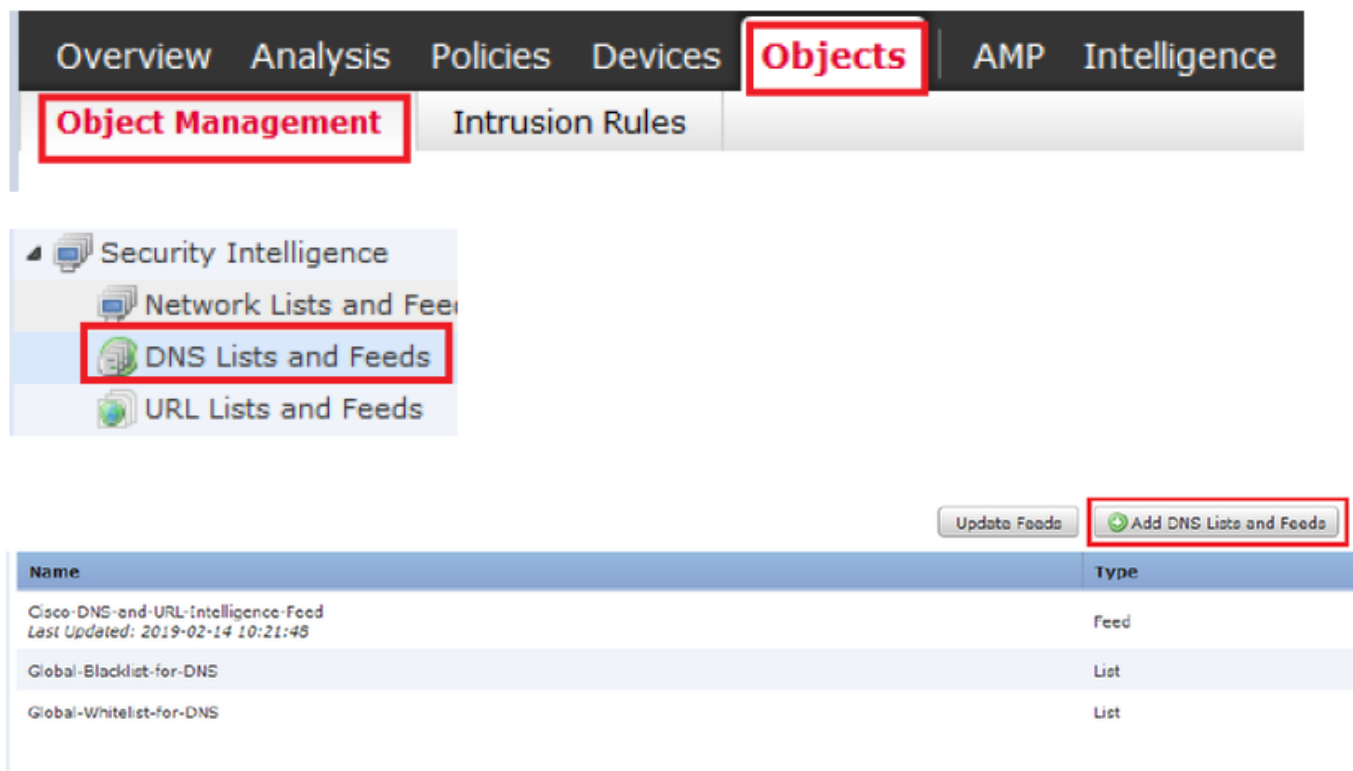
Configurazione

Configurare un elenco DNS personalizzato con i domini che si desidera bloccare e caricare nell'FMC

Passaggio 1. Creare un file txt con i domini che si desidera bloccare. Salvare il file .txt sul computer:



Passaggio 2. In FMC passare a Oggetto >> Gestione oggetti >> Elenchi e feed DNS >> Aggiungi elenco e feed DNS.



Passaggio 3. Creare un elenco denominato "BlackList-Domains", il tipo deve essere list e il file .txt con i domini in questione deve essere caricato come mostrato nelle immagini:

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

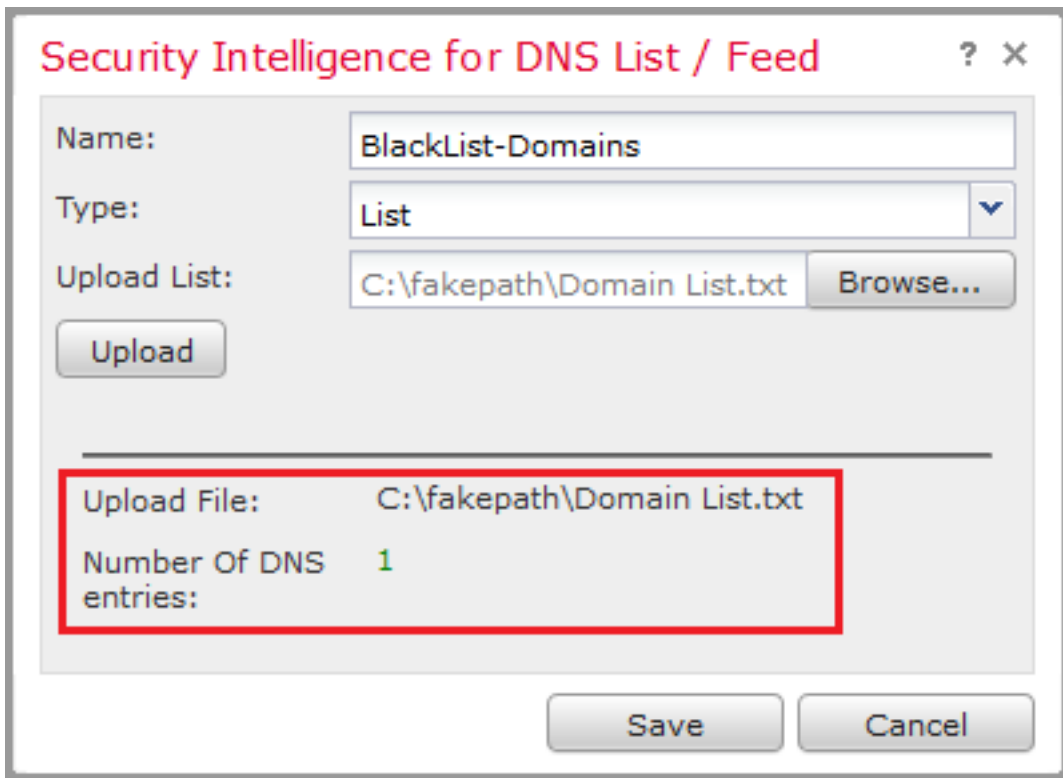
Type: List

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

Upload

Save Cancel

*Notare che quando si carica il file .txt, il numero di voci DNS dovrebbe leggere tutti i domini. Nell'esempio, un totale di 1:

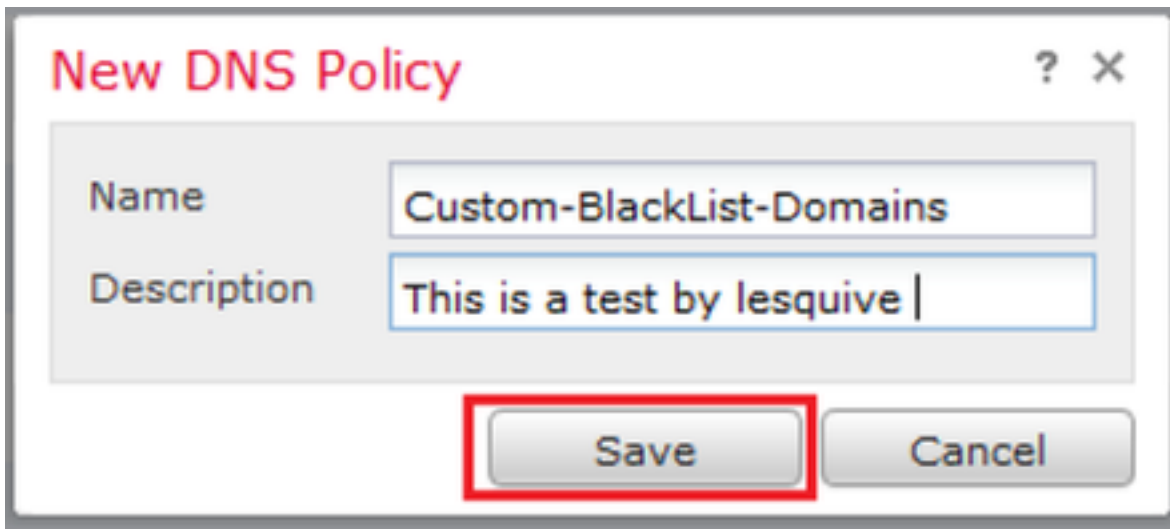


Aggiungere un nuovo criterio DNS con l'azione configurata su 'dominio non trovato'

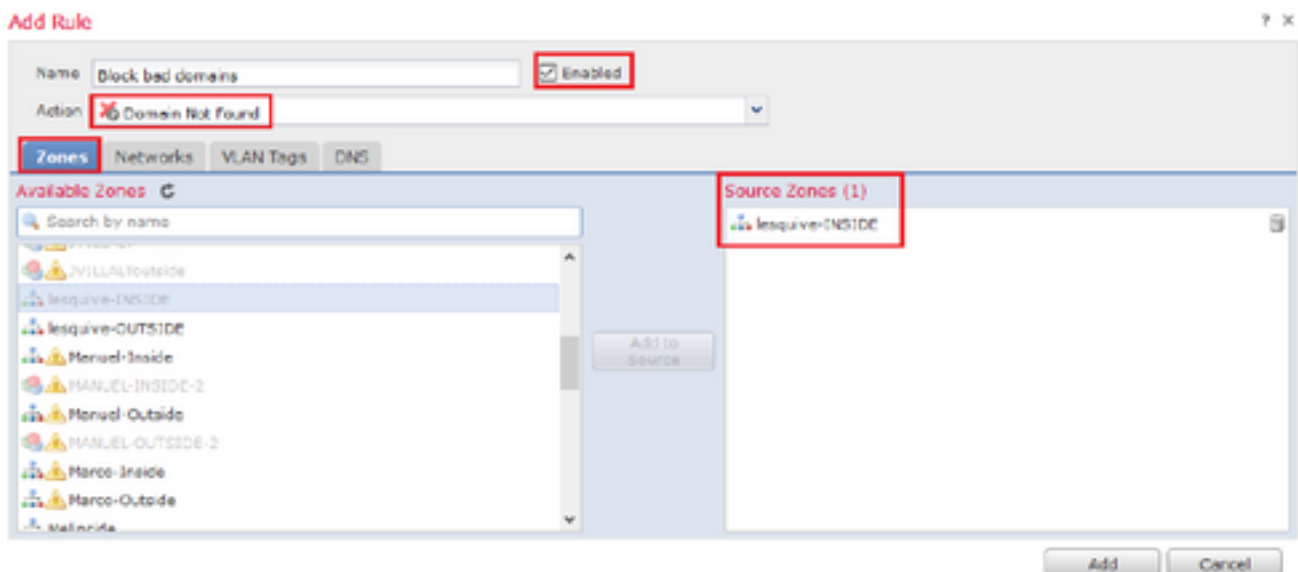
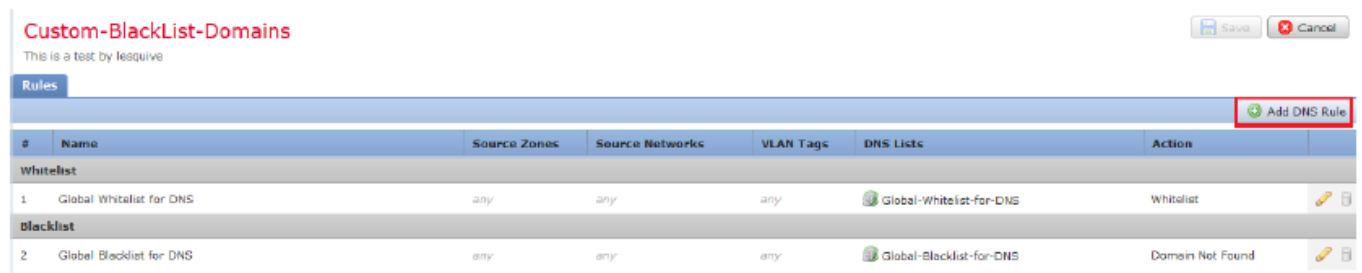
*Assicurarsi di aggiungere una zona di origine, la rete di origine e l'elenco DNS.

Passaggio 1. Passare a Criteri >> Controllo di accesso >> DNS >> Aggiungi criterio DNS:





Passaggio 2. Aggiungere una regola DNS come mostrato nell'immagine:



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

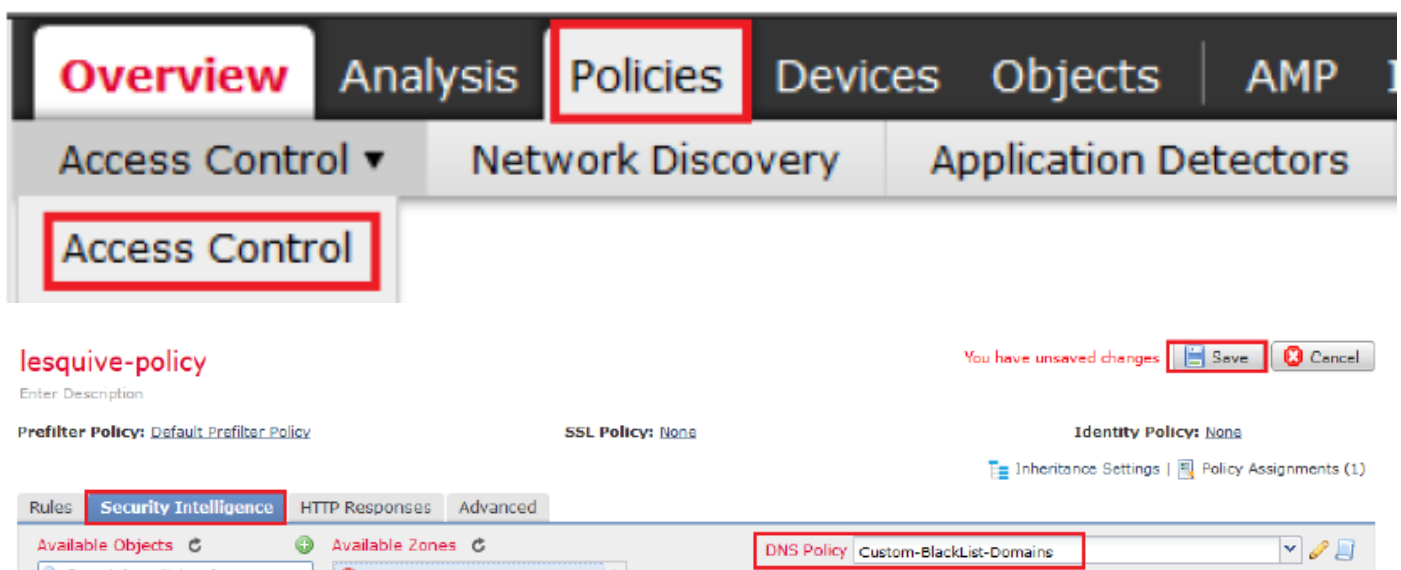
| Rules | | | | | | | Add DNS Rule |
|------------------|--------------------------|--------------|------------------|------------|--------------------------|------------------|---|
| # | Name | Source Zo... | Source Networks | VLAN Ta... | DNS Lists | Action | |
| Whitelist | | | | | | | |
| 1 | Global 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 |   |

Informazioni importanti sull'ordine delle regole:

- La lista bianca globale è sempre la prima e ha la precedenza su tutte le altre regole.
- La regola Whitelist DNS discendenti viene visualizzata solo in distribuzioni multidominio, in domini non foglia. È sempre seconda e ha la precedenza su tutte le altre regole tranne la lista bianca globale.
- La sezione Whitelist precede la sezione Blacklist; le regole delle liste bianche hanno sempre la precedenza su altre regole.
- La lista nera globale è sempre la prima nella sezione Lista nera e ha la precedenza su tutte le altre regole di controllo e lista nera.
- La regola delle liste nere DNS discendenti viene visualizzata solo in distribuzioni multidominio, in domini non foglia. Si trova sempre al secondo posto nella sezione Lista nera e ha la precedenza su tutte le altre regole di controllo e lista nera ad eccezione della lista nera globale.
- La sezione blacklist contiene le regole di controllo e blacklist.
- Quando si crea una regola DNS per la prima volta, la posizione del sistema si trova per ultima nella sezione Whitelist se si assegna un'azione Whitelist, oppure per ultima nella sezione Blacklist se si assegna qualsiasi altra azione

Assegnare i criteri DNS ai criteri di controllo di accesso

Andare a Criteri >> Controllo di accesso >> Criteri per FTD >> Security Intelligence >> Criteri DNS e aggiungere i Criteri creati.



The screenshot shows the 'Policies' tab selected in the top navigation bar. Below it, the 'Access Control' sub-tab is active. The main content area shows the configuration for a policy named 'lesquive-policy'. At the bottom, the 'Rules' section is expanded to 'Security Intelligence', and a 'DNS Policy' is assigned to 'Custom-BlackList-Domains'. A 'Save' button is highlighted in red, indicating unsaved changes.

Al termine, assicurarsi di distribuire tutte le modifiche.

Verifica

Prima dell'applicazione dei criteri DNS

Passaggio 1. Verificare le informazioni relative al server DNS e all'indirizzo IP sul computer host come illustrato nell'immagine:

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

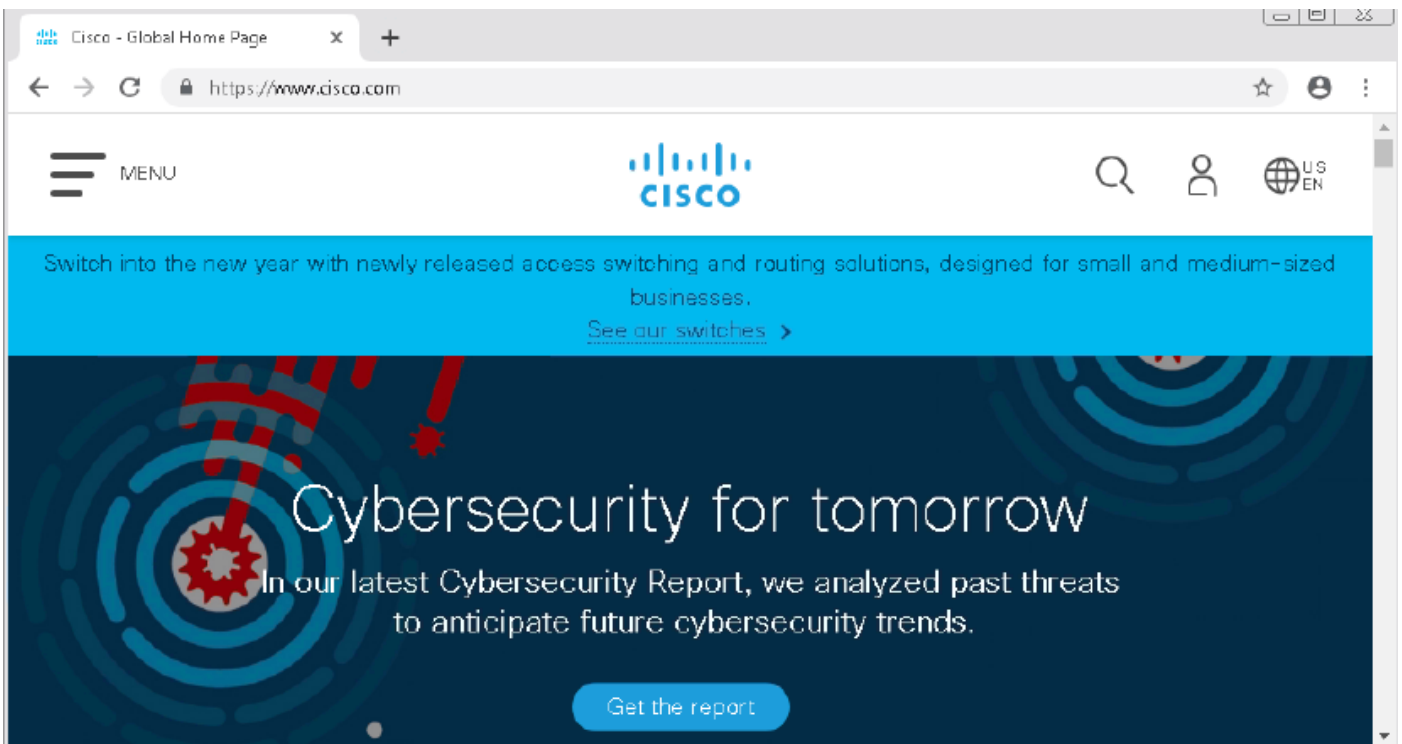
Ethernet adapter Local Area Connection 2:

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:a9aa: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
```

Passaggio 2. Confermare che sia possibile passare a cisco.com come mostrato nell'immagine:



Passaggio 3. Verificare con le acquisizioni di pacchetti che il DNS sia risolto correttamente:

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets. Packet 3510 is a DNS standard query from source 192.168.20.10 to destination 156.154.70.1 for the domain cisco.com. Packet 3515 is the corresponding standard query response from 156.154.70.1 to 192.168.20.10, containing the IP address 72.163.4.185 for cisco.com.

The bottom pane shows the detailed view of packet 3515, highlighting the 'Answers' section:

- 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

Dopo l'applicazione dei criteri DNS

Passaggio 1. Cancellare la cache DNS sull'host con il comando `ipconfig /flushdns`.

```

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

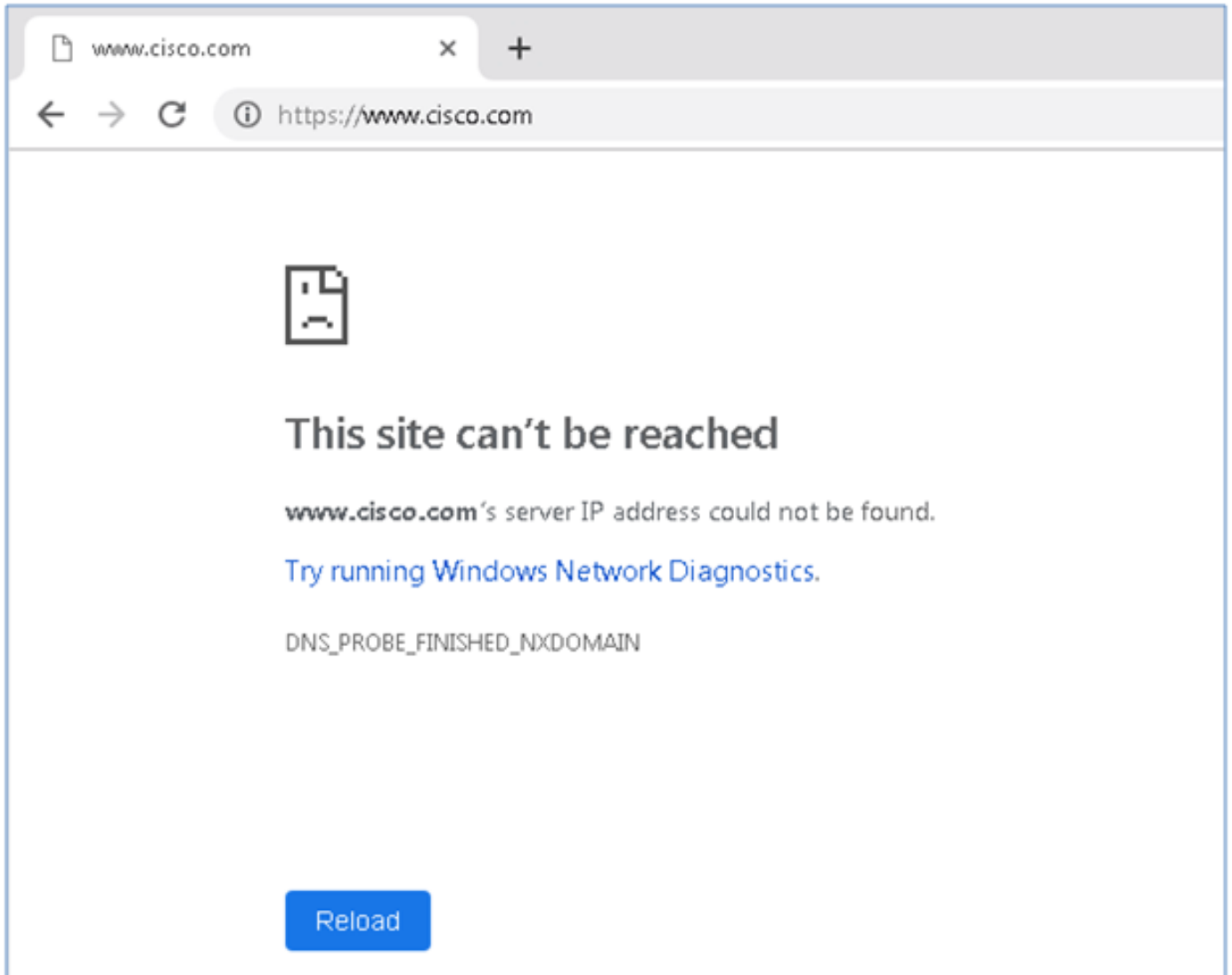
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>_
  
```

Passaggio 2. Passare al dominio in questione con un browser Web. Non dovrebbe essere raggiungibile:



Passaggio 3. Provare a utilizzare **nslookup** nel dominio cisco.com. La risoluzione dei nomi non riesce.

```
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: rdnst1.ultradns.net
Address: 156.154.70.1

> cisco.com
Server: rdnst1.ultradns.net
Address: 156.154.70.1

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

Passaggio 4. Le acquisizioni dei pacchetti mostrano una risposta dall'FTD, anziché dal server DNS.

The screenshot shows a network traffic capture in Wireshark. The top pane displays a table of captured packets:

| 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 |

The bottom pane shows the details of the selected packet (Frame 1618):

- 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]

Passaggio 5. Eseguire i debug nella CLI FTD: il sistema supporta firewall-engine-debug e specifica il protocollo UDP.

```
>
> 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
```

*Debug quando cisco.com corrisponde:

```
> system support firewall-engine-debug

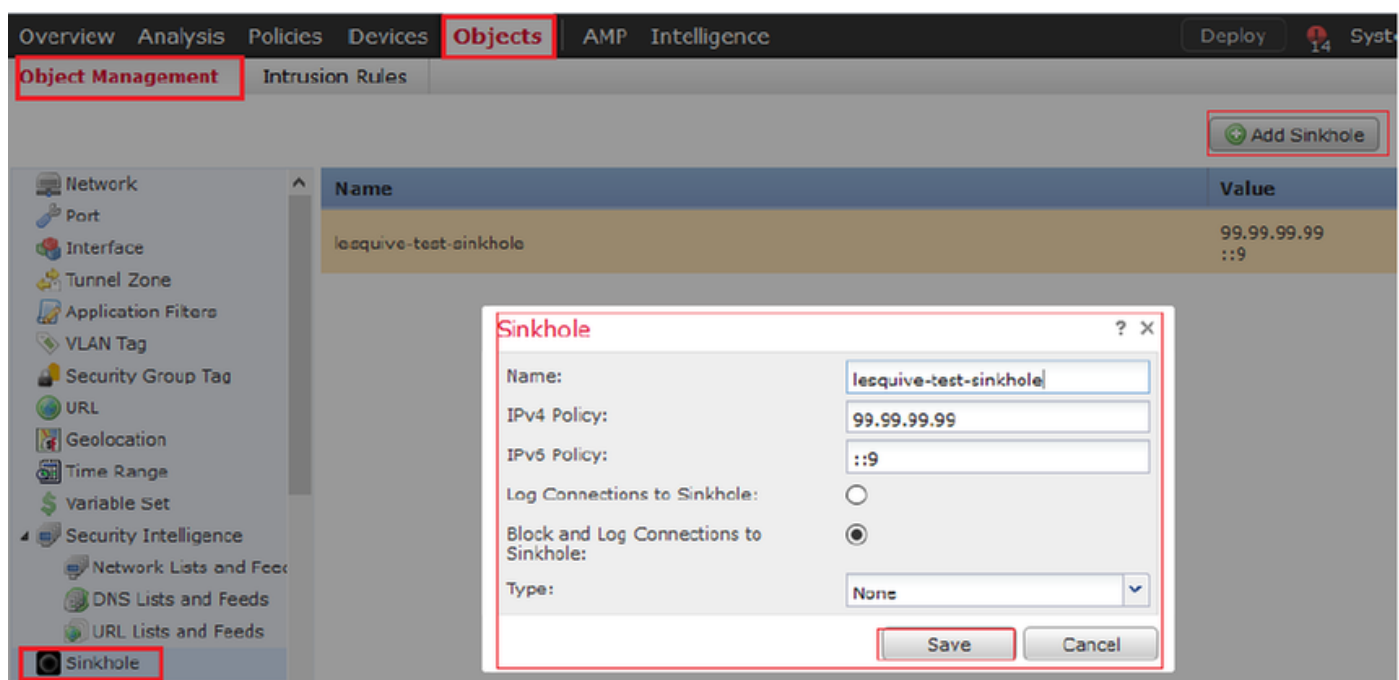
Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

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
```

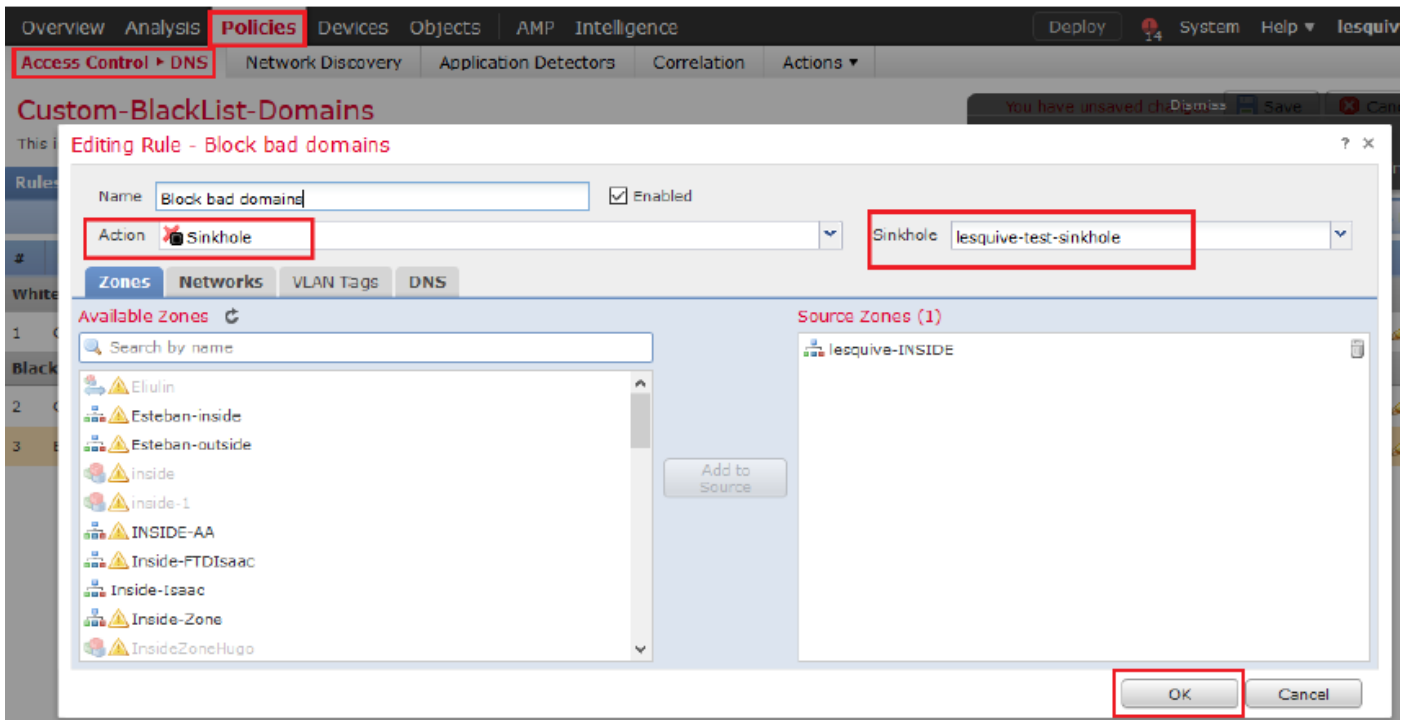
Configurazione opzionale di Sinkhole

Un sinkhole DNS è un server DNS che fornisce informazioni false. Anziché restituire una risposta DNS del tipo "Nessun nome" alle query DNS sui domini che si stanno bloccando, restituisce un indirizzo IP falso.

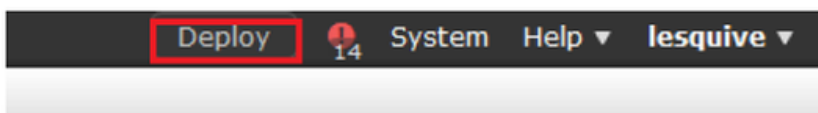
Passaggio 1. Passare a Oggetti >> Gestione oggetti >> Sinkhole >> Aggiungi sinkhole e creare le informazioni di indirizzo IP false.



Passaggio 2. Applicare il sinkhole ai criteri DNS e distribuire le modifiche a FTD.



| # | 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



Verifica che Sinkhole funzioni

```
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 |

Risoluzione dei problemi

Passare ad Analisi > Connessioni >> Eventi di Security Intelligence per tenere traccia di tutti gli eventi attivati da SI, purché sia stata abilitata la registrazione nei criteri DNS:

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 14:36:57 | | 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 | |

È inoltre possibile utilizzare il comando `system support firewall-engine-debug` sull'FTD gestito dal 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
```

Le acquisizioni dei pacchetti possono essere utili per confermare che le richieste DNS stanno arrivando al server FTD. Non dimenticare di cancellare la cache sull'host locale durante il test.

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>_