Firepower Management Center를 사용하여 보안 인텔리전스로 DNS 차단

목차

소개

이 문서에서는 DNS 정책에 DNS(Domain Name System) 목록을 추가하여 SI(Security Intelligence)를 사용하여 적용할 수 있는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA55XX Threat Defense 구성
- Cisco Firepower Management Center 컨피그레이션

사용되는 구성 요소

- Cisco ASA5506W-X Threat Defense(75) 버전 6.2.3.4(빌드 42)
- VMWare용 Cisco Firepower Management Center 소프트웨어 버전:6.2.3.4(빌드 42)OS:Cisco Fire Linux OS 6.2.3(빌드13)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

보안 인텔리전스는 알려진 잘못된 평판이 있는 IP 주소, URL 또는 도메인 이름 간 또는 간 트래픽을 차단하여 작동합니다.이 문서에서는 도메인 이름 블랙리스팅이 주요 초점입니다.

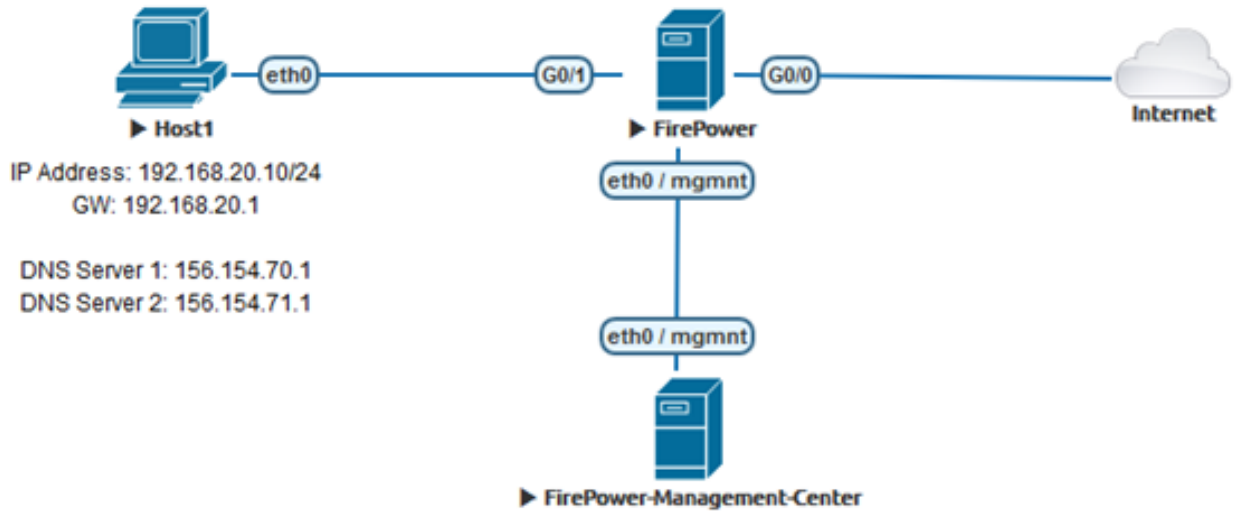
사용된 예에서는 1 도메인을 차단합니다.

- cisco.com

URL 필터링을 사용하여 이러한 사이트 중 일부를 차단할 수 있지만 문제는 URL이 정확히 일치해야 한다는 것입니다.반면, SI를 사용하는 DNS 블랙리스트는 하위 도메인이나 URL의 변경에 대해 걱정할 필요 없이 "cisco.com"과 같은 도메인에 집중할 수 있습니다.

이 문서의 끝에는 선택적인 Sinkhole 컨피그레이션도 표시됩니다.

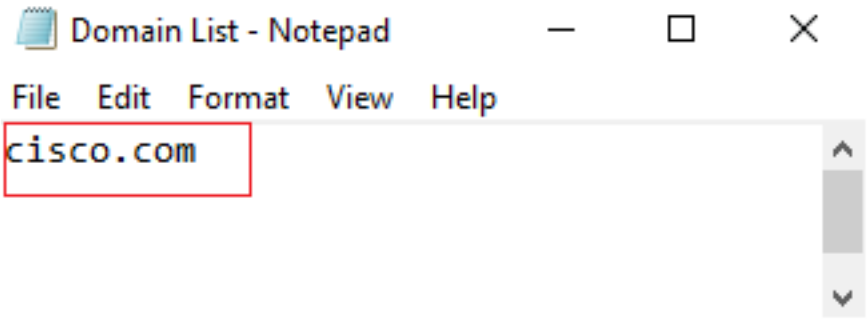
네트워크 다이어그램



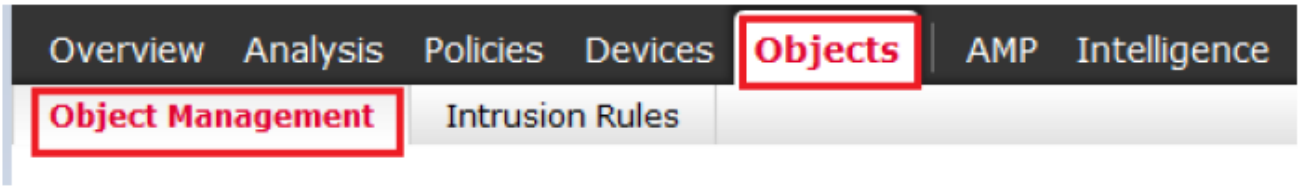
구성

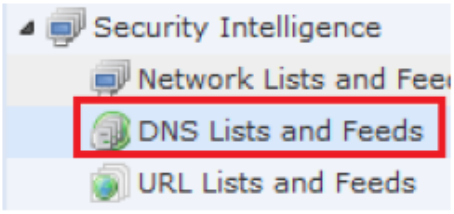
차단할 도메인으로 사용자 지정 DNS 목록을 구성하고 FMC에 목록 업로드

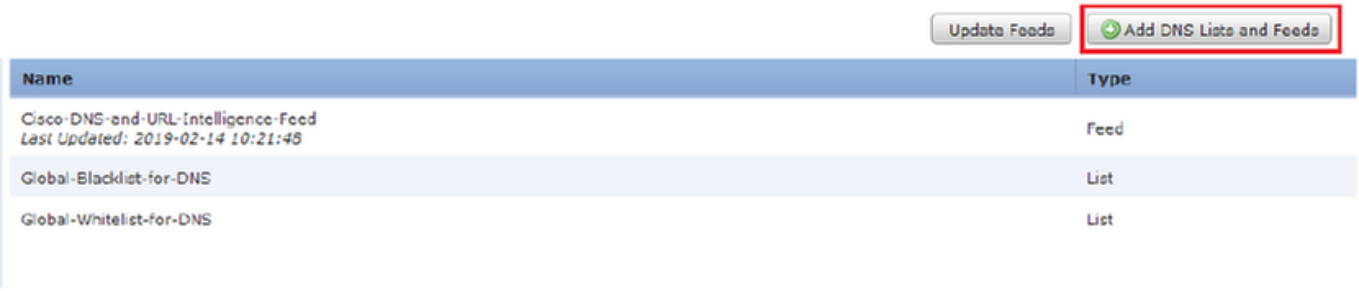
1단계. 차단할 도메인으로 .txt 파일을 만듭니다.컴퓨터에 .txt 파일을 저장합니다.



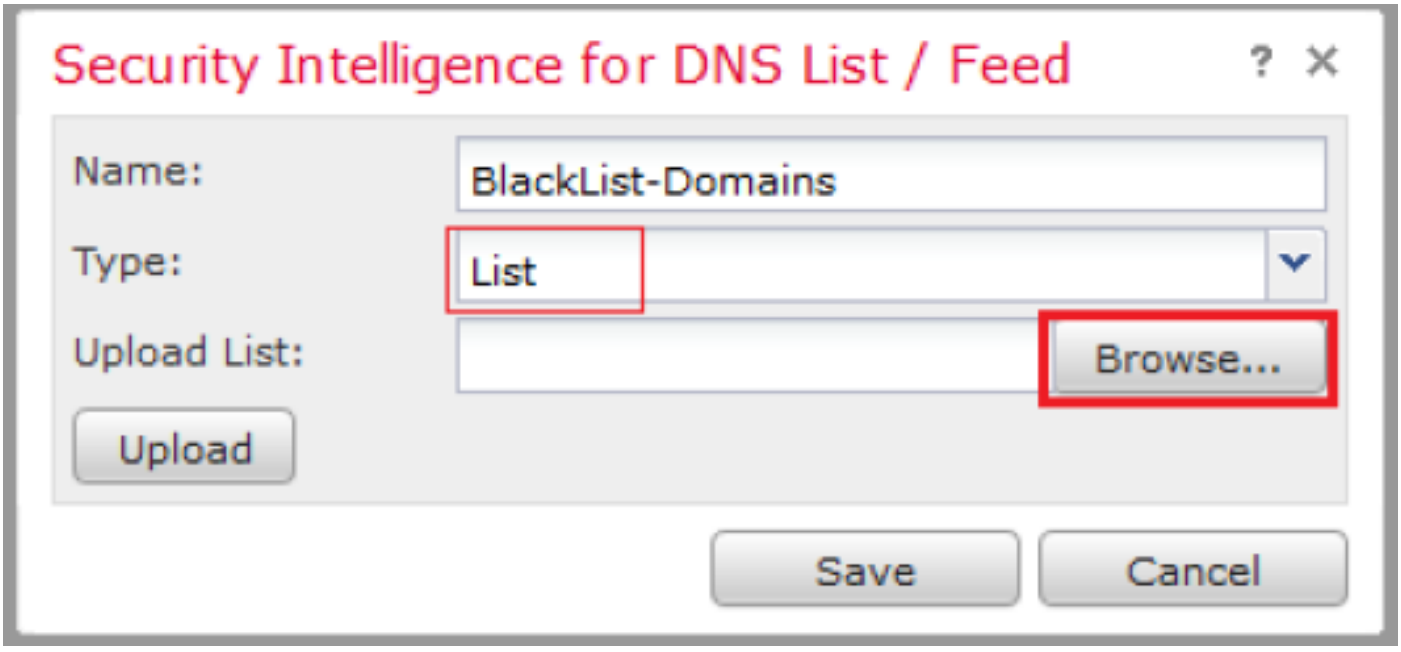
2단계. FMC에서 Object >> Object Management >> DNS Lists and Feeds >> Add DNS List and Feeds로 이동합니다.

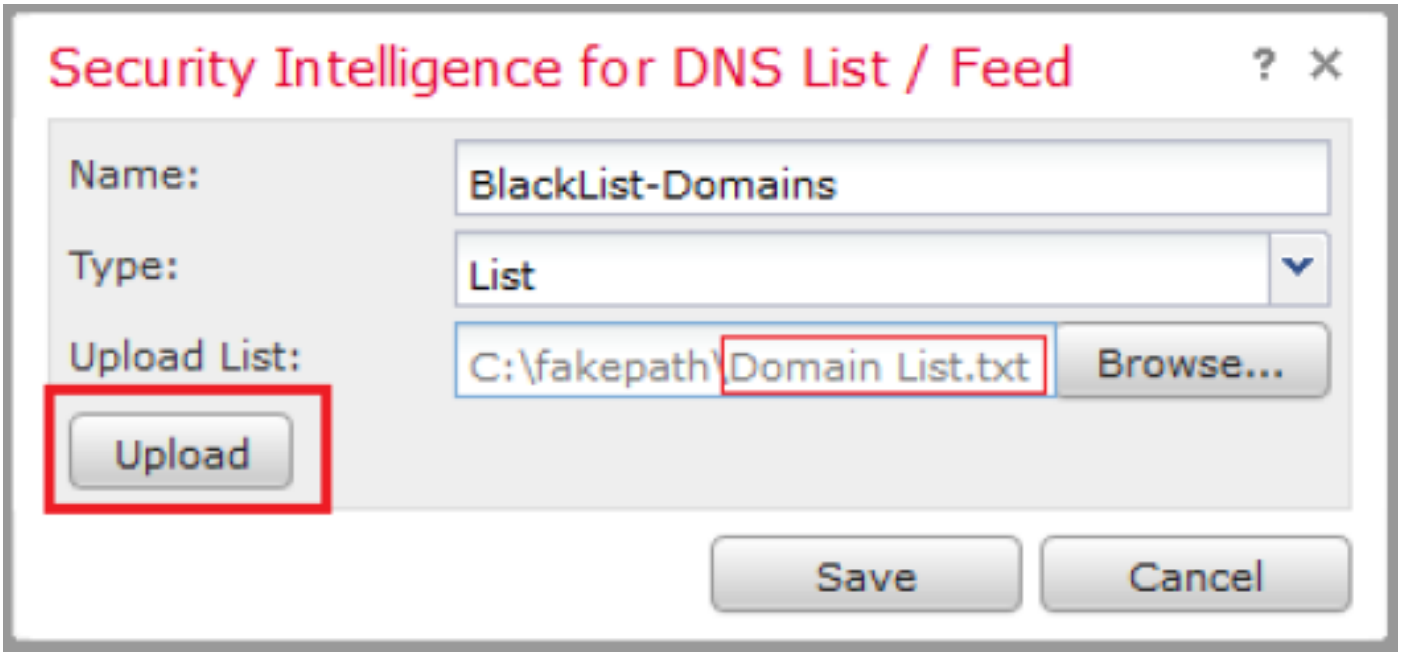




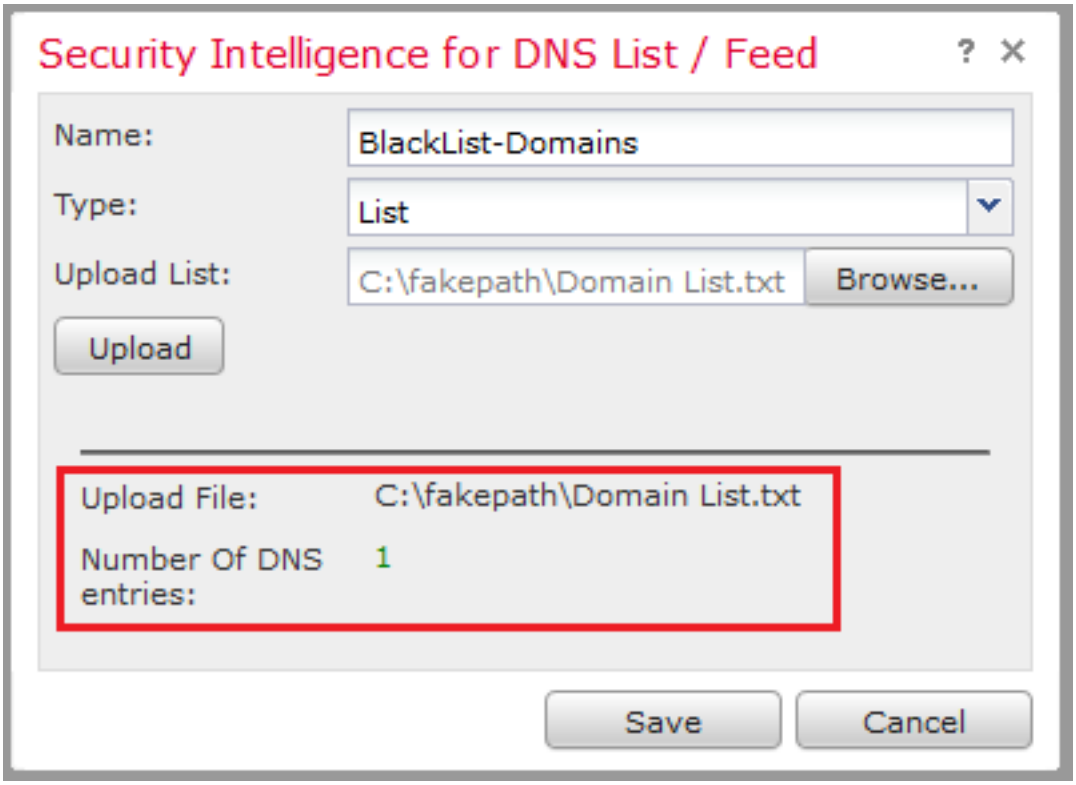


3단계. "BlackList-Domains"라는 목록을 만듭니다. 다음 이미지에 표시된 대로 유형이 나열되어야 하며 해당 도메인이 포함된 .txt 파일을 업로드해야 합니다.





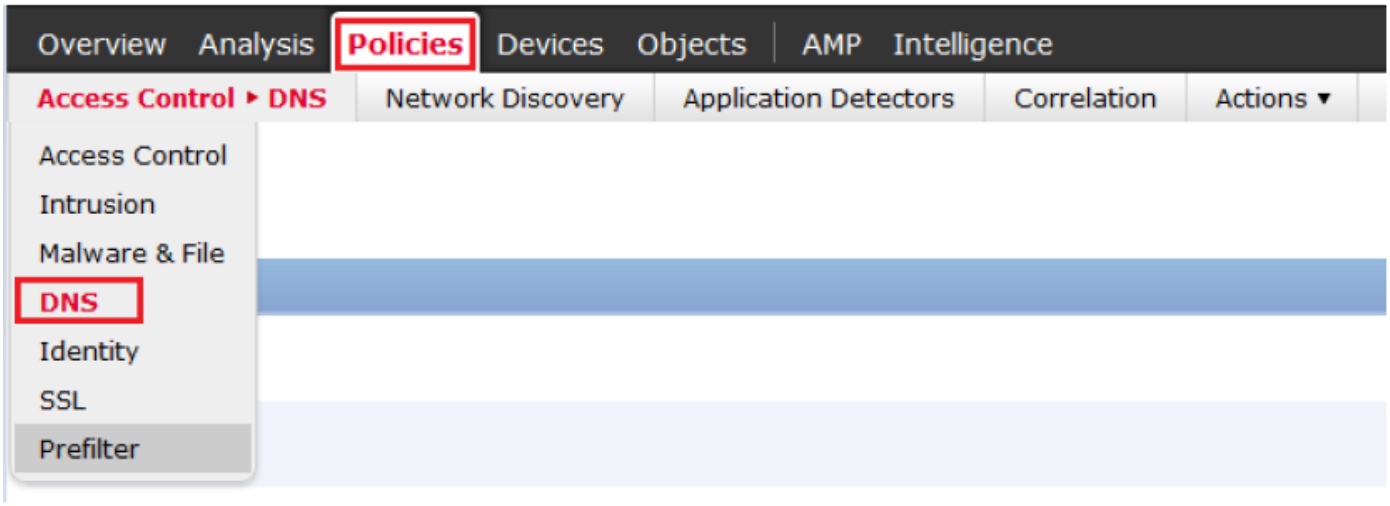
*.txt 파일을 업로드할 때 Number of DNS entries는 모든 도메인을 읽어야 합니다.이 예에서는 총 1:

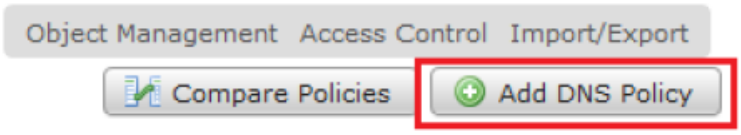


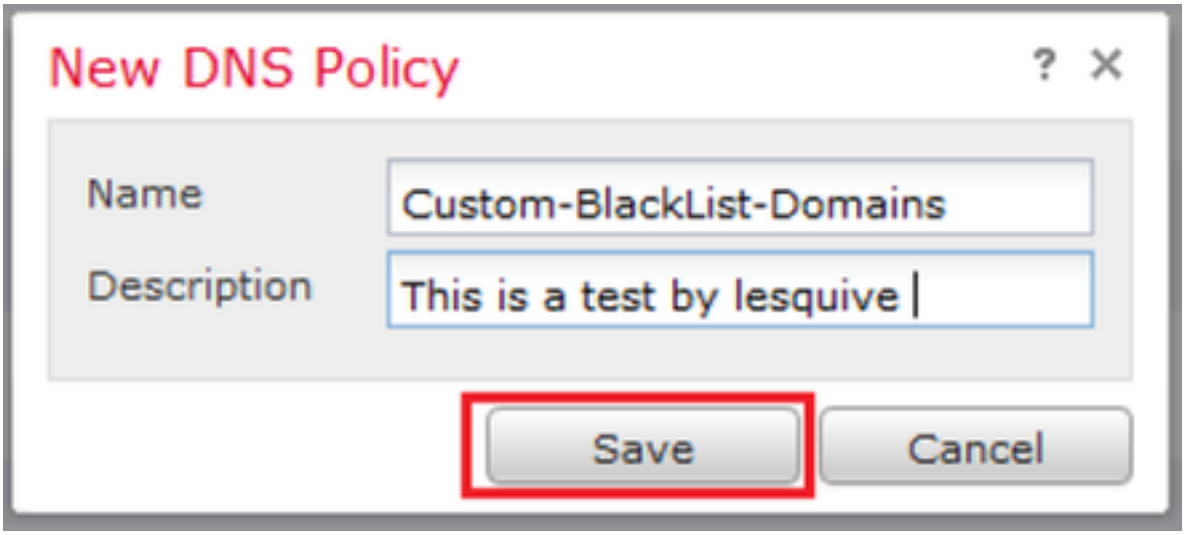
'도메인을 찾을 수 없음'으로 구성된 작업으로 새 DNS 정책 추가

*소스 영역, 소스 네트워크 및 DNS 목록을 추가해야 합니다.

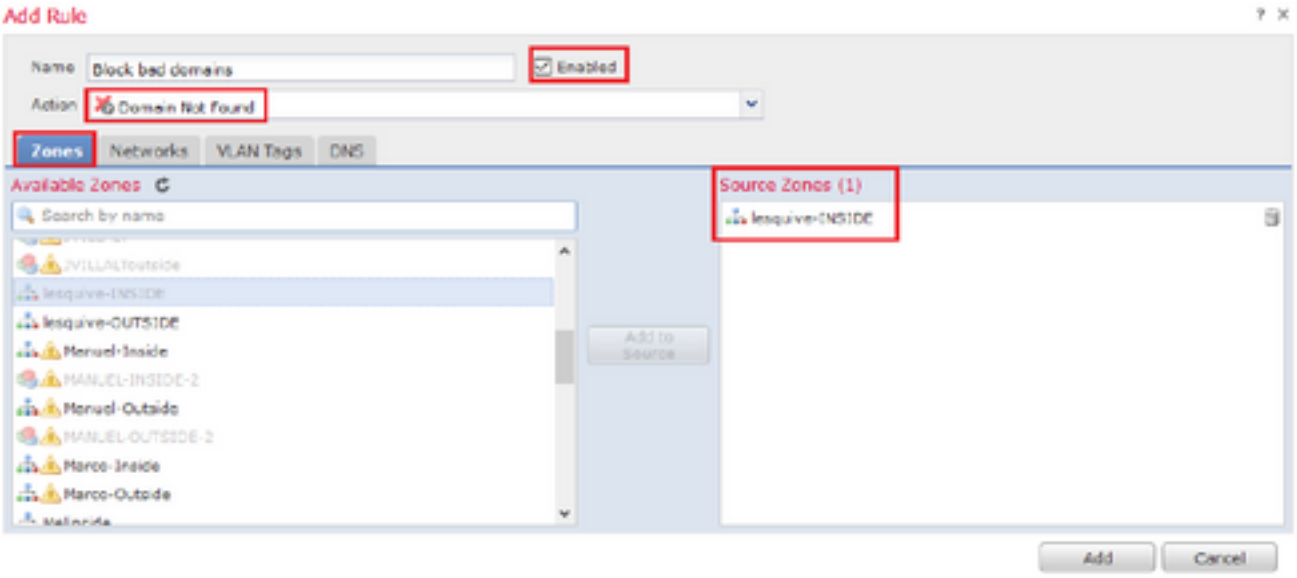
1단계. Policies(정책) >> Access Control(액세스 제어) >> DNS >> Add DNS Policy(DNS 정책 추가)로 이동합니다.

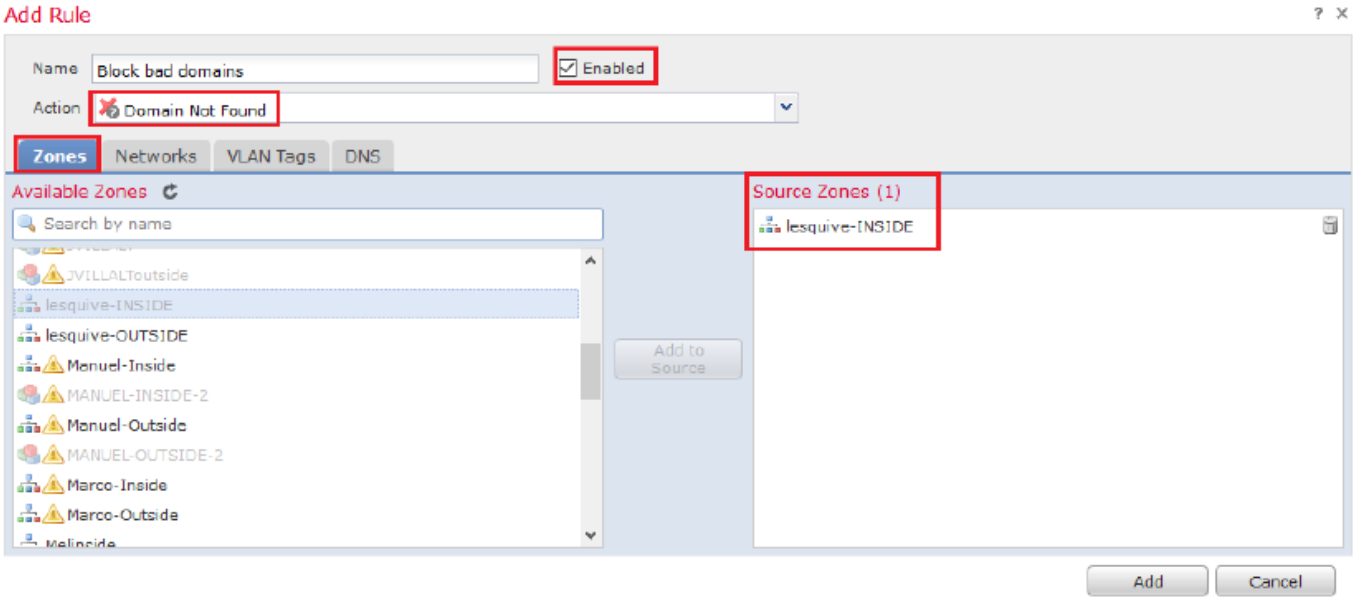


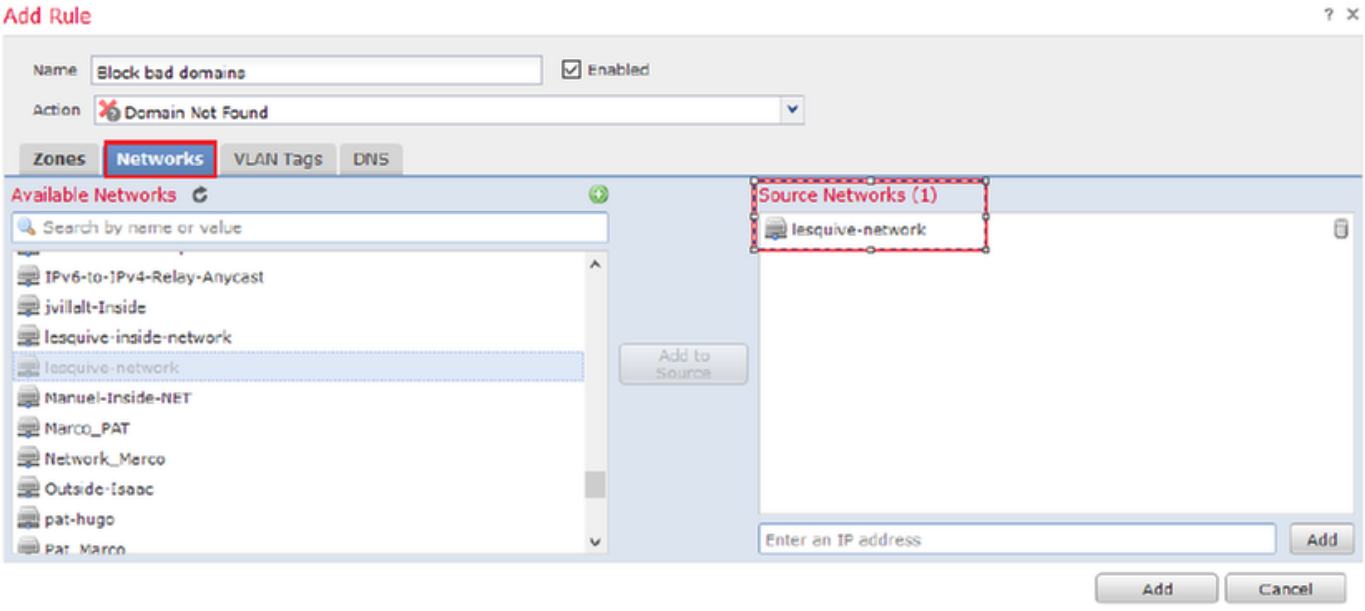


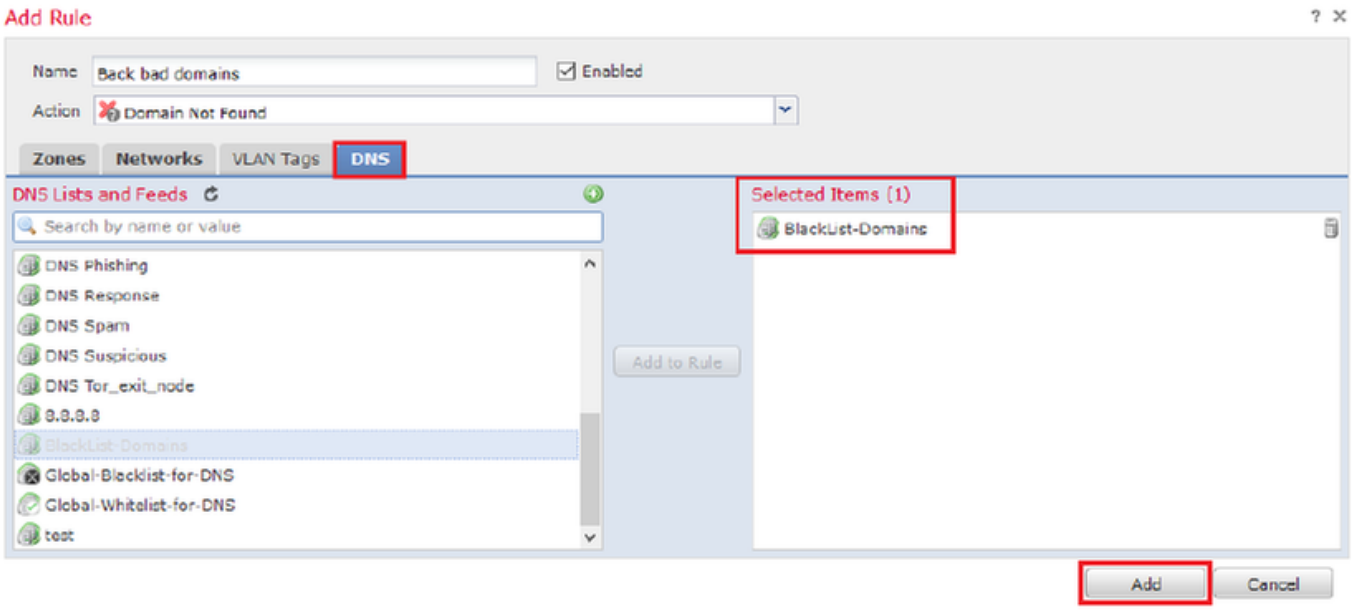


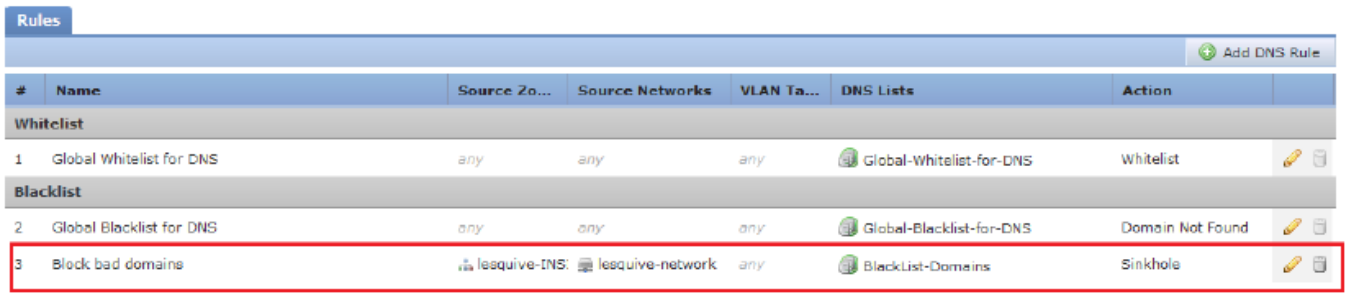
2단계. 이미지에 표시된 대로 DNS 규칙을 추가합니다.


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-OUTSIDE
Manuel-Inside
Manuel-Outside
Marco-Inside
Marco-Outside
Source Zones (1)
lesquive-INSIDE
Add to Source
Add
Cancel


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-INSIDE
lesquive-OUTSIDE
Manuel-Inside
MANUEL-INSIDE-2
Manuel-Outside
MANUEL-OUTSIDE-2
Marco-Inside
Marco-Outside
Source Zones (1)
lesquive-INSIDE
Add to Source
Add
Cancel


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
Source Networks (1)
lesquive-network
Add to Source
Enter an IP address
Add
Add
Cancel



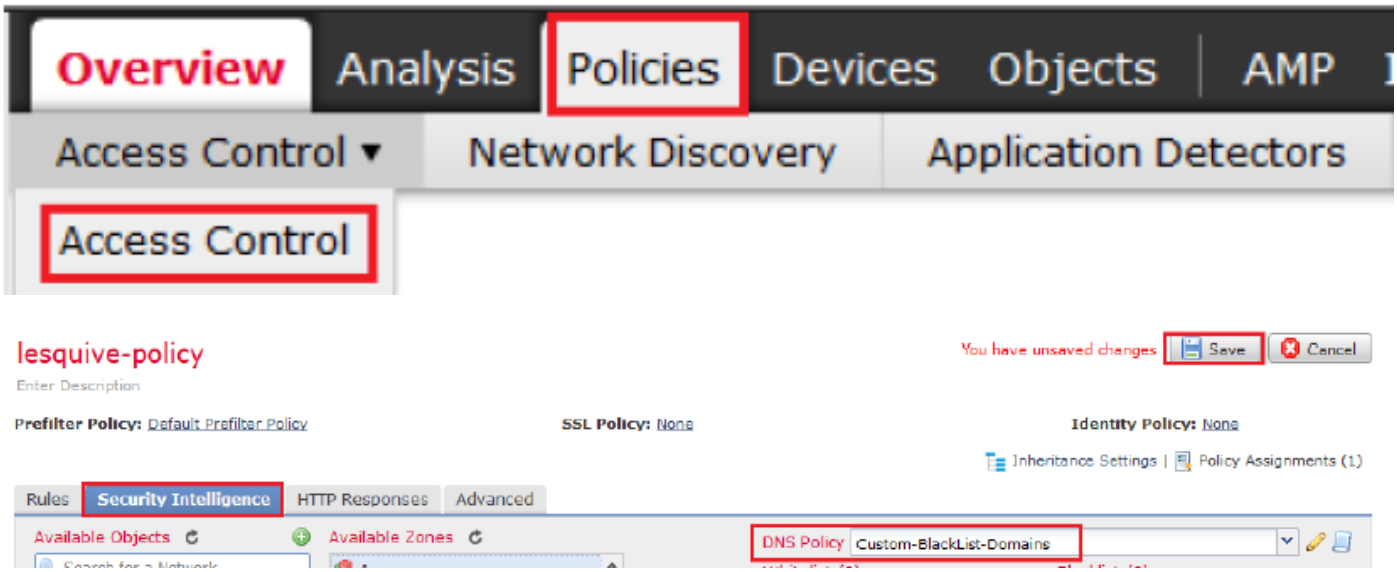


규칙 순서에 대한 중요 정보:

- 전역 화이트리스트는 항상 먼저 실행되며 다른 모든 규칙보다 우선합니다.
- Descendant DNS Whitelists 규칙은 다중 도메인 구축의 비 리프 도메인에만 나타납니다.항상 두 번째이며 전역 화이트리스트를 제외한 다른 모든 규칙보다 우선합니다.
- Whitelist 섹션이 Blacklist 섹션 앞에 있습니다.화이트리스트 규칙은 항상 다른 규칙보다 우선합니다.
- Global Blacklist는 항상 Blacklist(블랙리스트) 섹션에서 첫 번째로 수행되며 다른 모든 Monitor(모니터) 및 Blacklist(블랙리스트) 규칙보다 우선합니다.
- Descendant DNS Blacklists(하위 DNS 블랙리스트) 규칙은 다중 도메인 구축의 비 리프 도메인에만 나타납니다.이는 항상 Blacklist(블랙리스트) 섹션에서 두 번째이며 Global Blacklist(전역 블랙리스트)를 제외한 다른 모든 Monitor(모니터) 및 Blacklist(블랙리스트) 규칙보다 우선합니다.
- Blacklist 섹션에는 Monitor 및 Blacklist 규칙이 포함되어 있습니다.
- DNS 규칙을 처음 생성할 때 Whitelist(화이트리스트) 작업을 할당하면 시스템 위치가 Whitelist(화이트리스트) 섹션의 맨 마지막에 배치되고, 다른 작업을 할당하면 Blacklist(블랙리스트) 섹션의 맨 마지막에 배치됩니다.

액세스 제어 정책에 DNS 정책 할당

Policies >> Access Control >> The Policy for your FTD >> Security Intelligence >> DNS Policy로 이동하여 생성한 정책을 추가합니다.

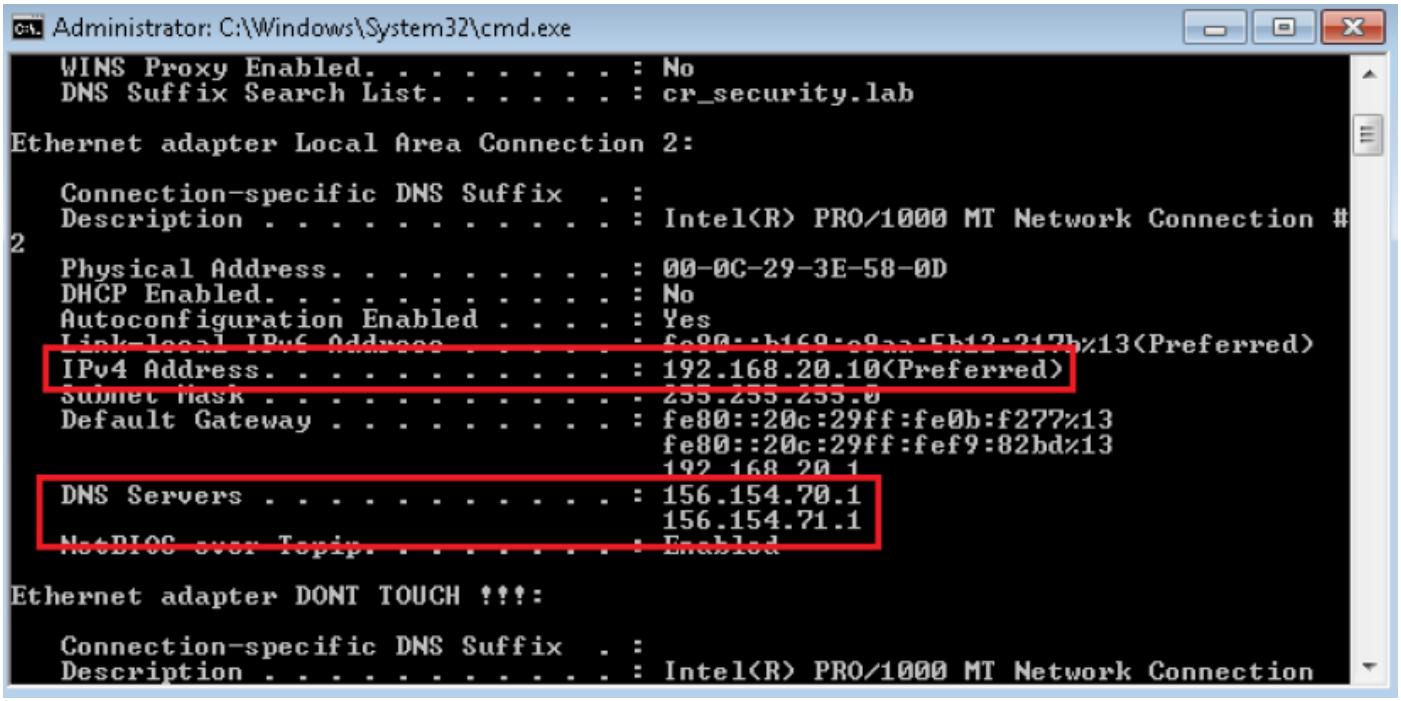


완료되면 모든 변경 사항을 구축합니다.

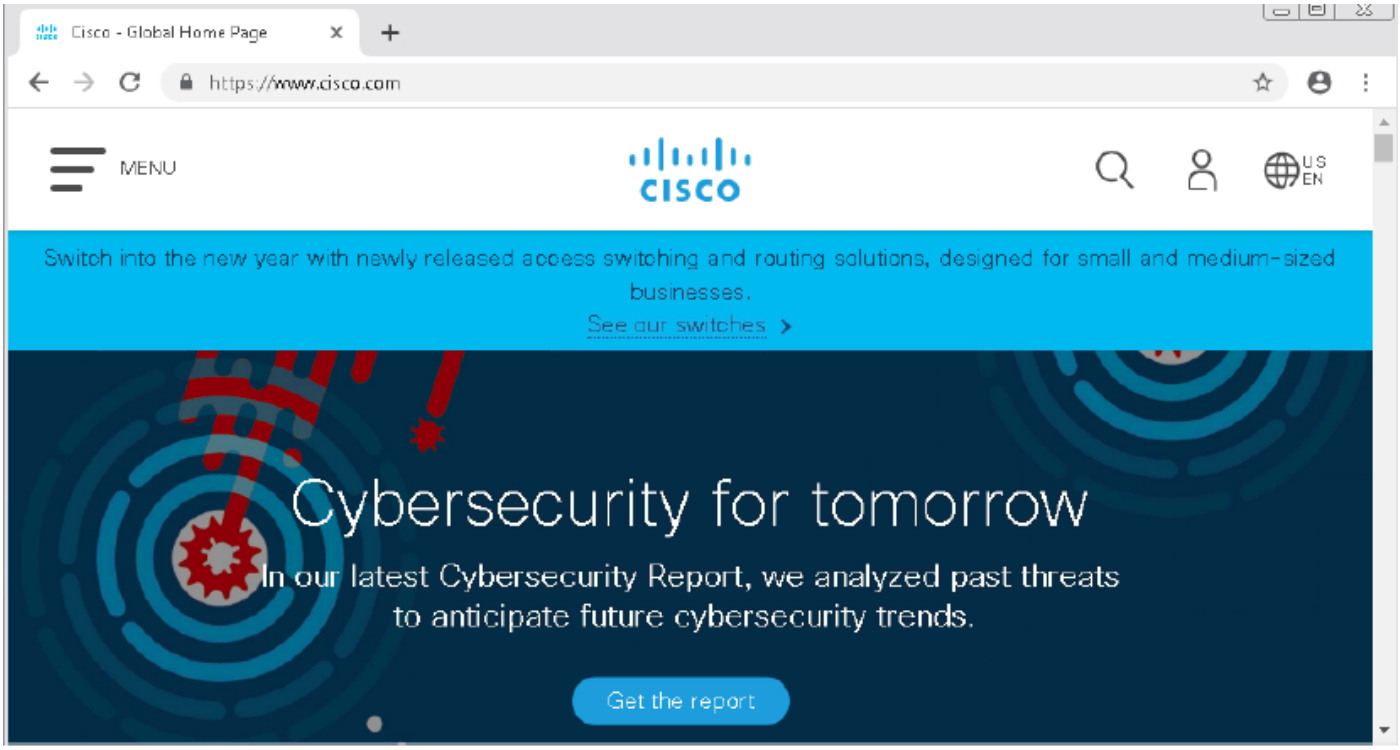
다음을 확인합니다.

DNS 정책을 적용하기 전

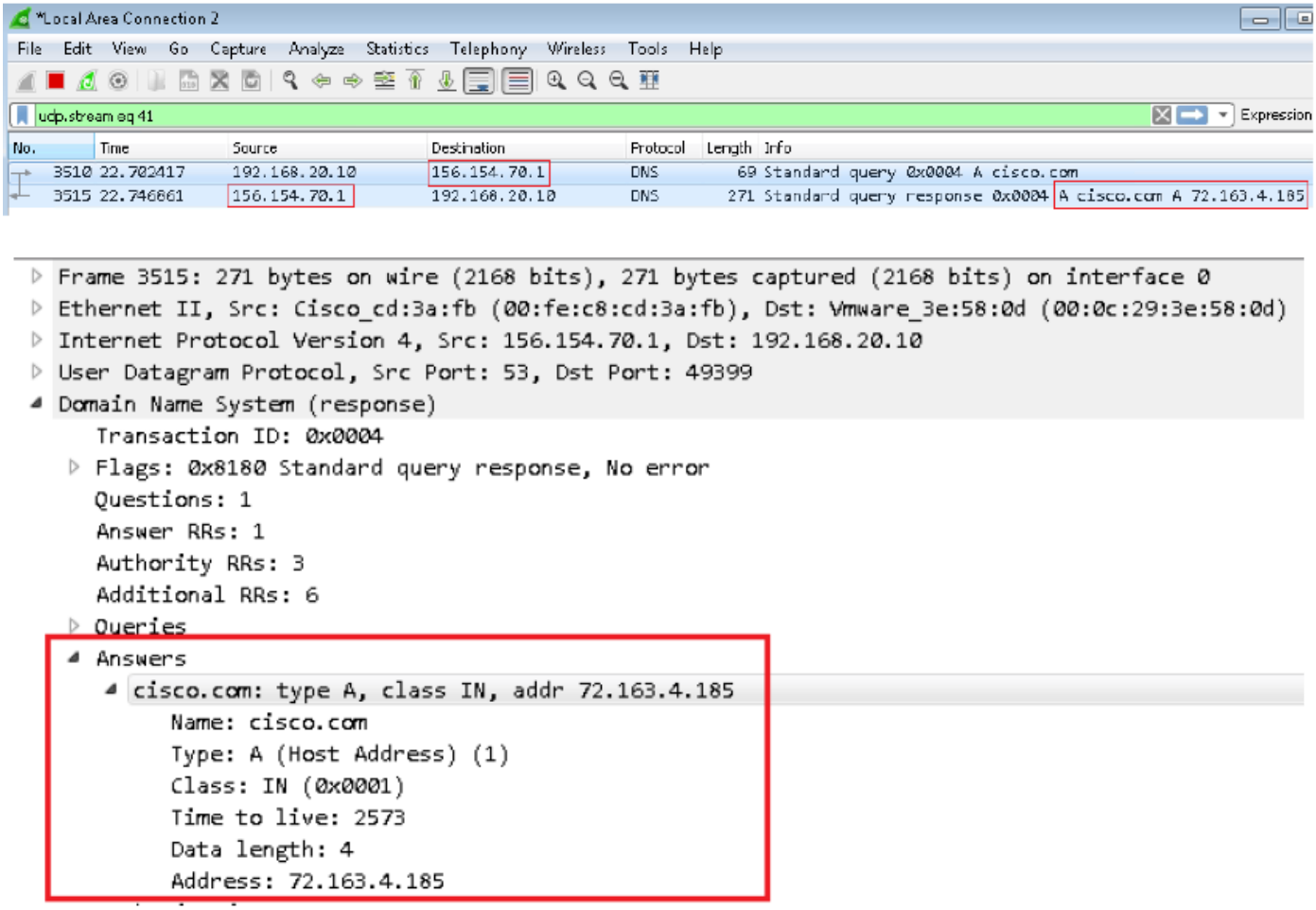
1단계. 이미지에 표시된 대로 호스트 시스템의 DNS 서버 및 IP 주소 정보를 확인합니다.



2단계. 이미지에 표시된 대로 cisco.com으로 이동할 수 있는지 확인합니다.

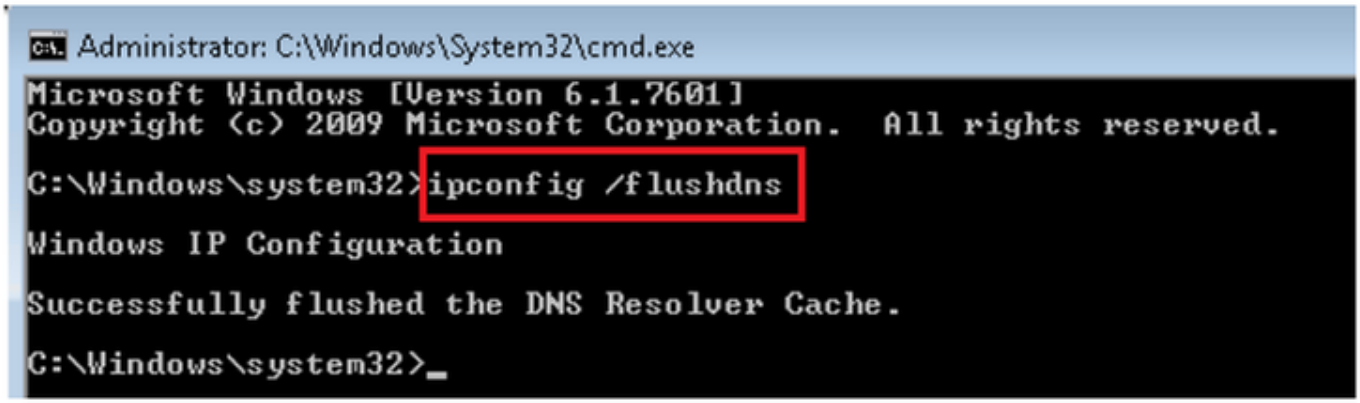


3단계. DNS가 올바르게 해결되었음을 패킷 캡처로 확인합니다.

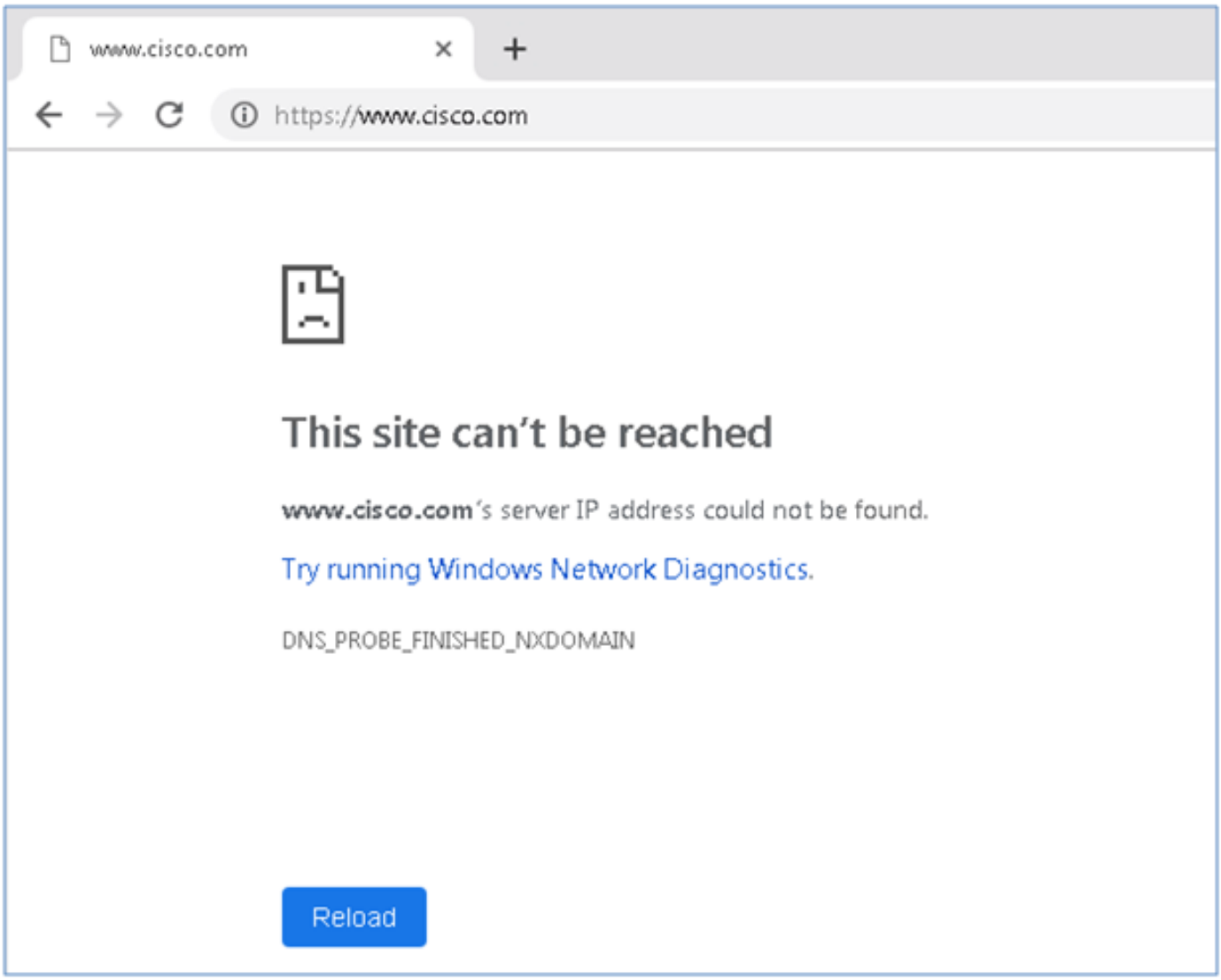


DNS 정책이 적용된 후

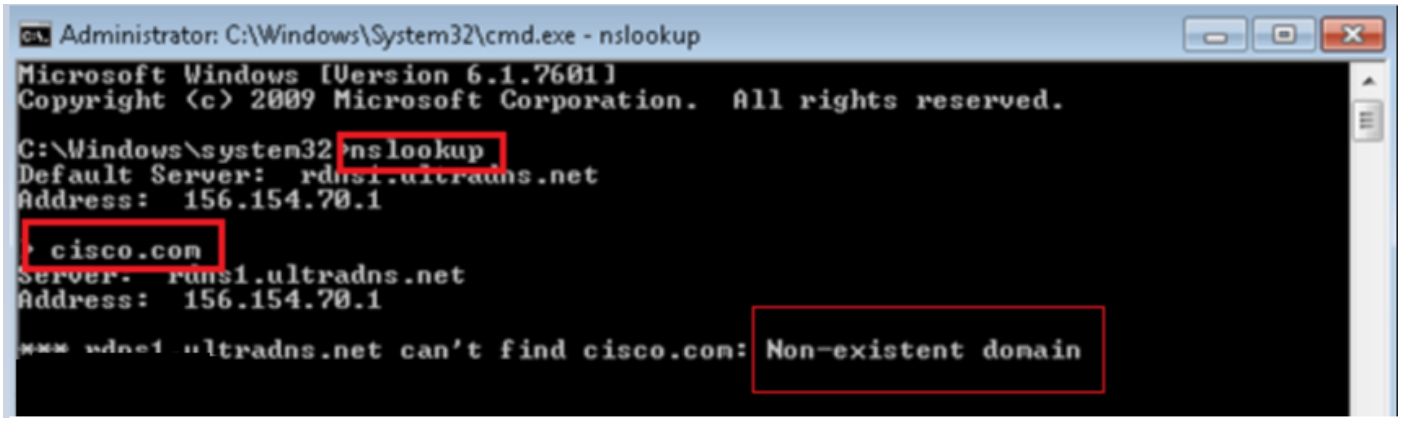
1단계. ipconfig /flushdns 명령을 사용하여 호스트에서 DNS 캐시를 지웁니다.



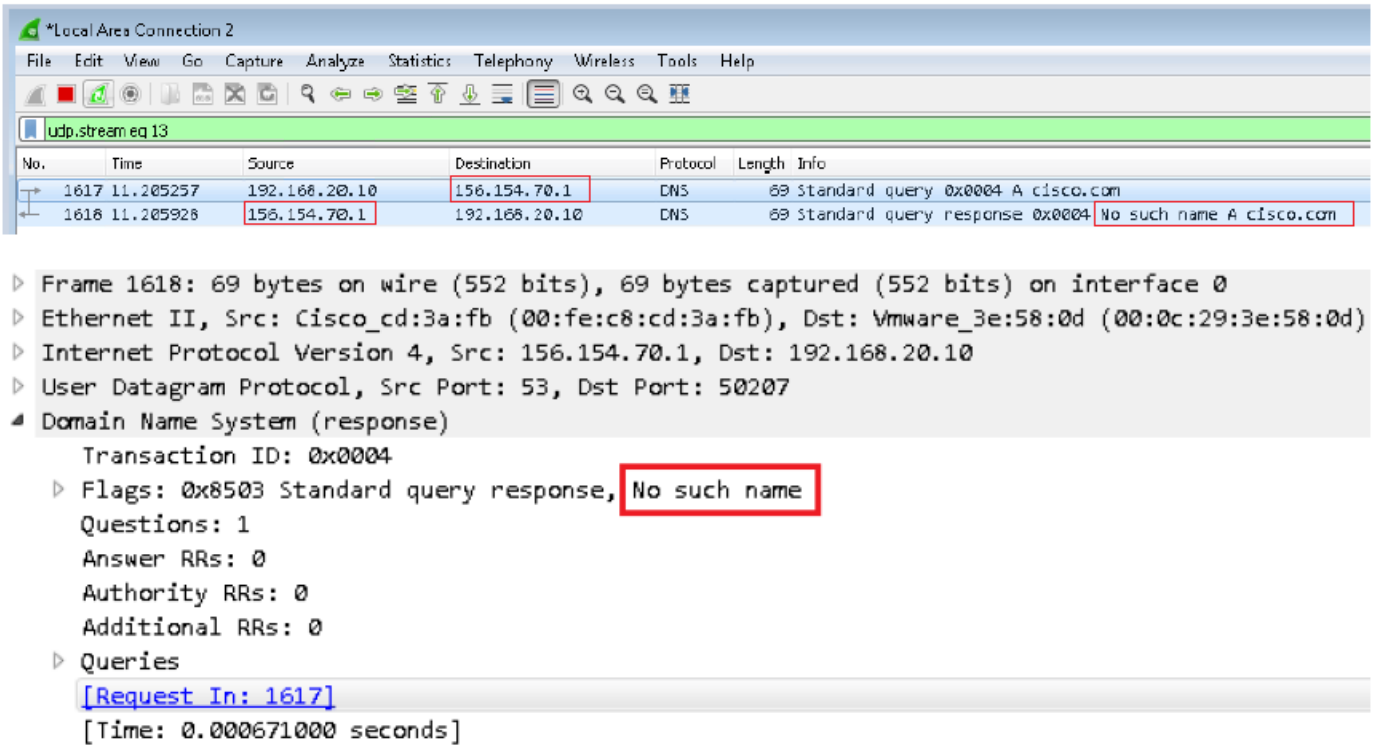
2단계. 웹 브라우저에서 해당 도메인으로 이동합니다.연결 불가 상태여야 합니다.



3단계. 도메인 cisco.com에서 nslookup을 실행합니다.이름 확인에 실패합니다.



4단계. 패킷 캡처는 DNS 서버 대신 FTD의 응답을 표시합니다.



5단계. FTD CLI에서 디버그를 실행합니다.시스템은 firewall-engine-debug를 지원하고 UDP 프로토콜을 지정합니다.

```
>
> 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
```

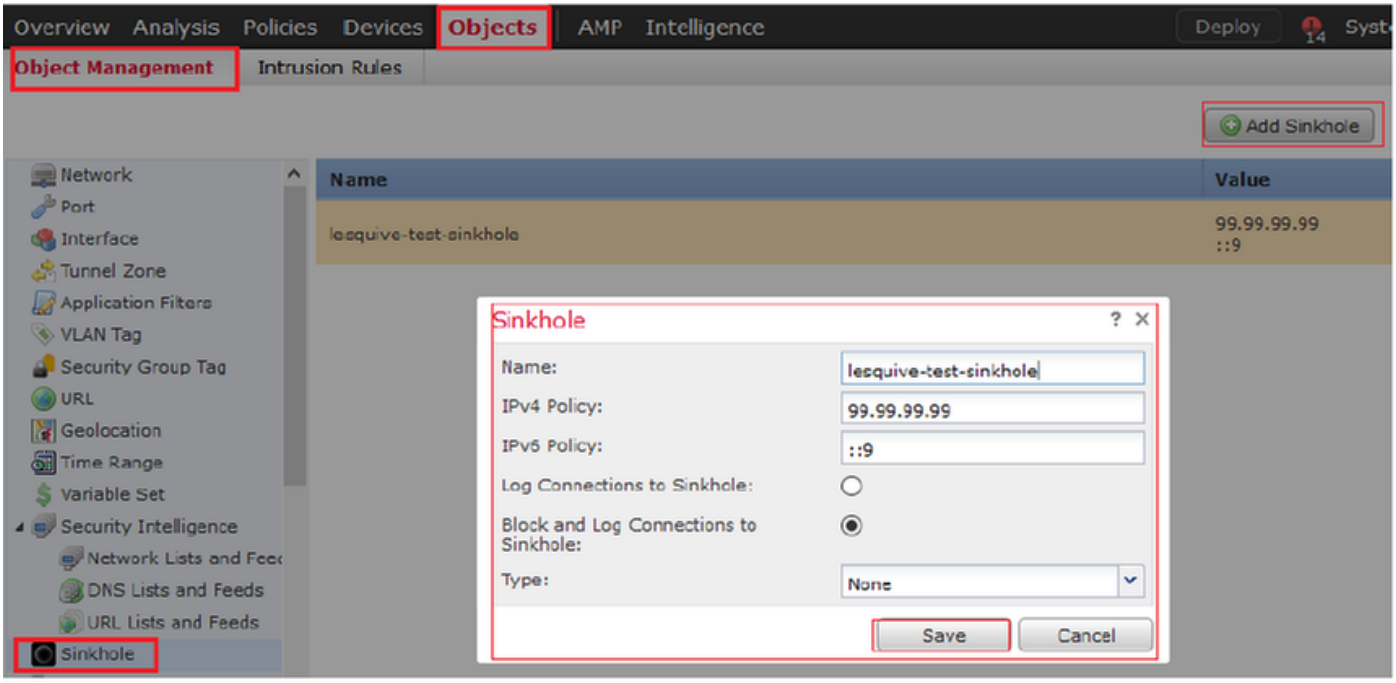
*cisco.com과 일치할 때 디버깅:

```
> 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
```

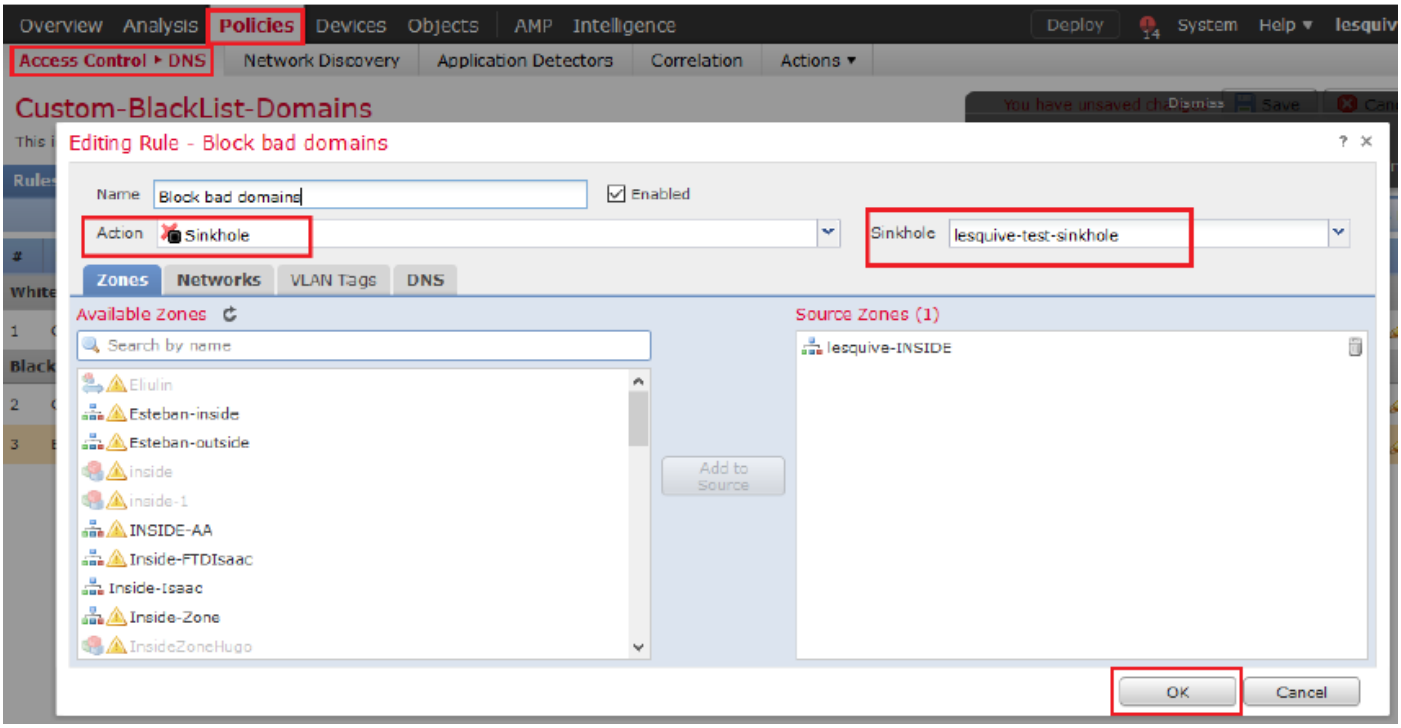
선택적 싱크홀 컨피그레이션

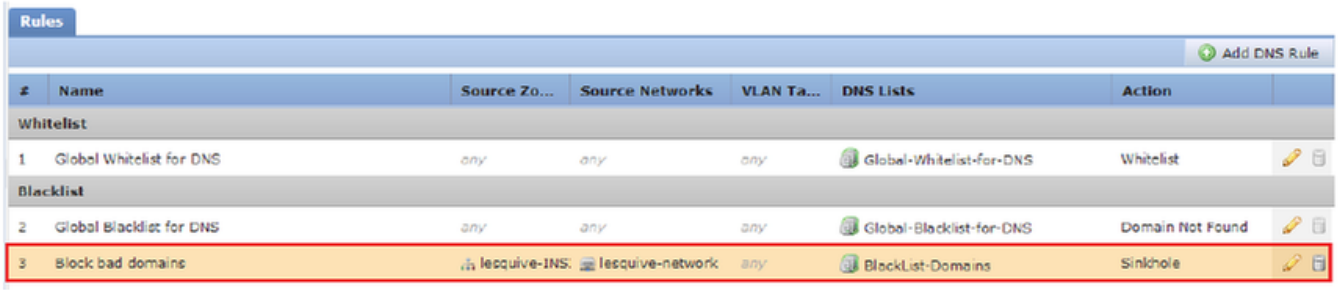
DNS 싱크홀은 잘못된 정보를 제공하는 DNS 서버입니다.차단 중인 도메인의 DNS 쿼리에 대해 "해당 이름 없음" DNS 응답을 반환하는 대신 위조 IP 주소를 반환합니다.

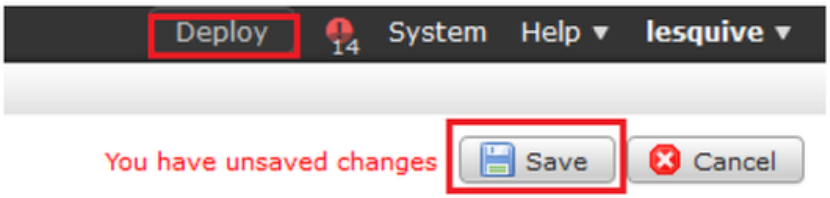
1단계. Objects >> Object Management >> Sinkhole >> Add Sinkhole으로 이동하고 위조 IP 주소 정보를 생성합니다.



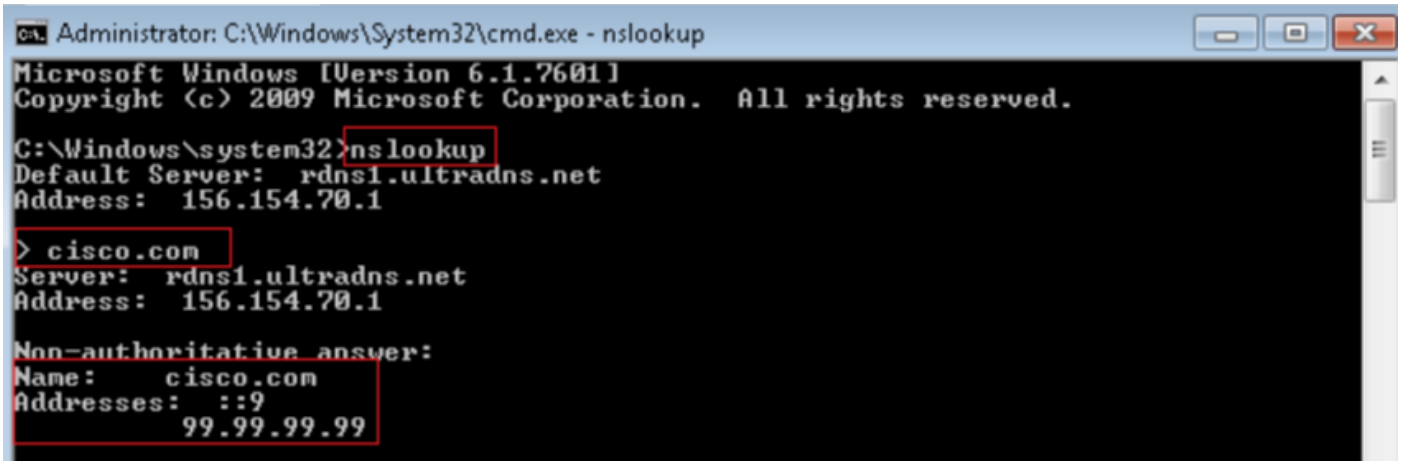
2단계. 싱크홀을 DNS 정책에 적용하고 FTD에 변경 사항을 구축합니다.

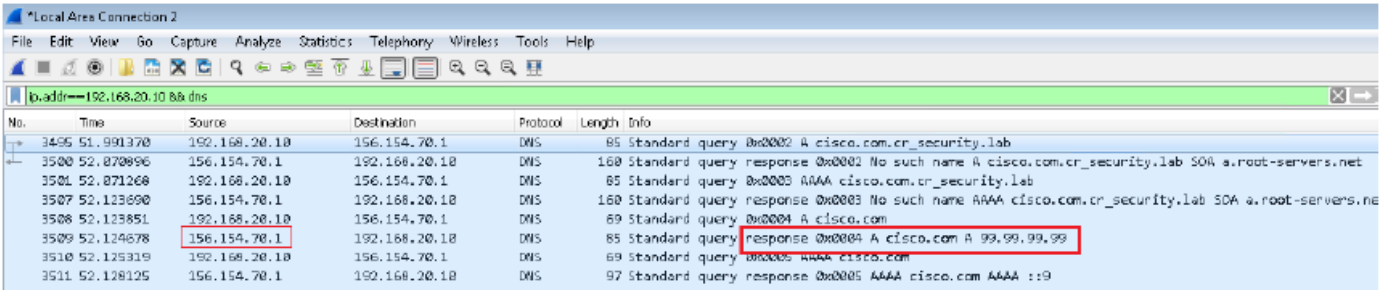






싱크홀이 작동하는지 확인





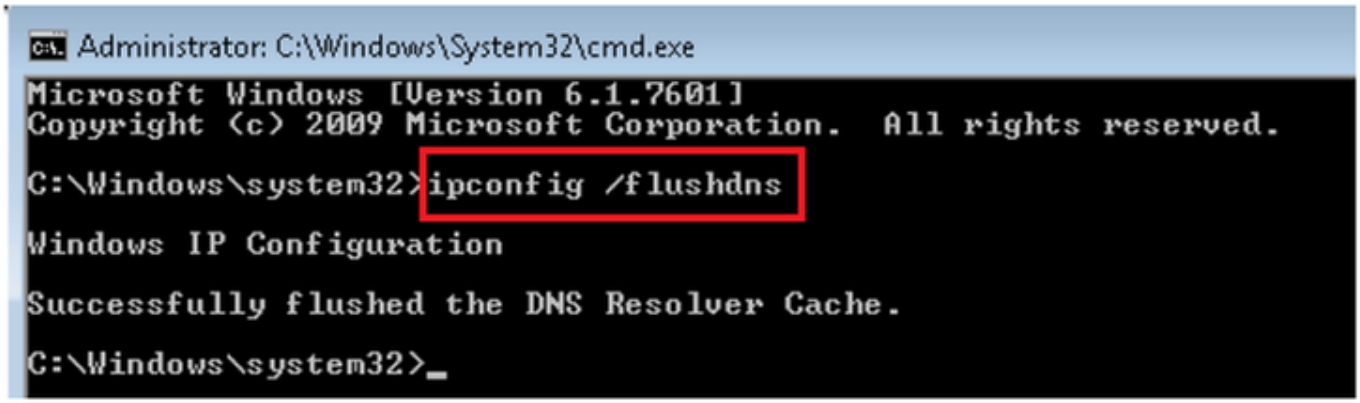
문제 해결

DNS 정책에서 로깅을 활성화한 경우 Analysis >> Connections >> Security Intelligence Events로 이동하여 SI에 의해 트리거되는 모든 이벤트를 추적합니다.

또한 FMC에서 관리하는 FTD에서 **system support firewall-engine-debug** 명령을 사용할 수 있습니다.

```
>
> 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
```

패킷 캡처는 DNS 요청이 FTD 서버로 전송되는지 확인하는 데 도움이 될 수 있습니다.테스트할 때 로컬 호스트의 캐시를 지우는 것을 잊지 마십시오.


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>