Umbrella Virtual Appliance에서 DNScyrpt 기능을 차단하는 ASA 방화벽 문제 해결

목차

소개

이 문서에서는 DNScrypt 기능을 차단하는 ASA 방화벽의 문제를 해결하는 방법에 대해 설명합니다 .

개요

Cisco ASA 방화벽은 Umbrella Virtual Appliance에서 제공하는 DNScrypt 기능을 차단할 수 있습니다. 이렇게 하면 Umbrella Dashboard 경고가 표시됩니다.

> DNS queries forwarded by this VA to OpenDNS are not encrypted. For more information, and steps to resolve, please visit: https://support.opendns.com /entries/57607634#dnscrypt-disabled

이러한 오류 메시지는 ASA 방화벽 로그에서도 확인할 수 있습니다.

```
Dropped UDP DNS request from inside:192.168.1.1/53904 to outside-fiber:208.67.220.220/53; label length
```

DNSCrypt 암호화는 DNS 쿼리의 내용을 보호하도록 설계되었으므로 방화벽에서 패킷 검사를 수행하지 못하도록 차단합니다.

원인

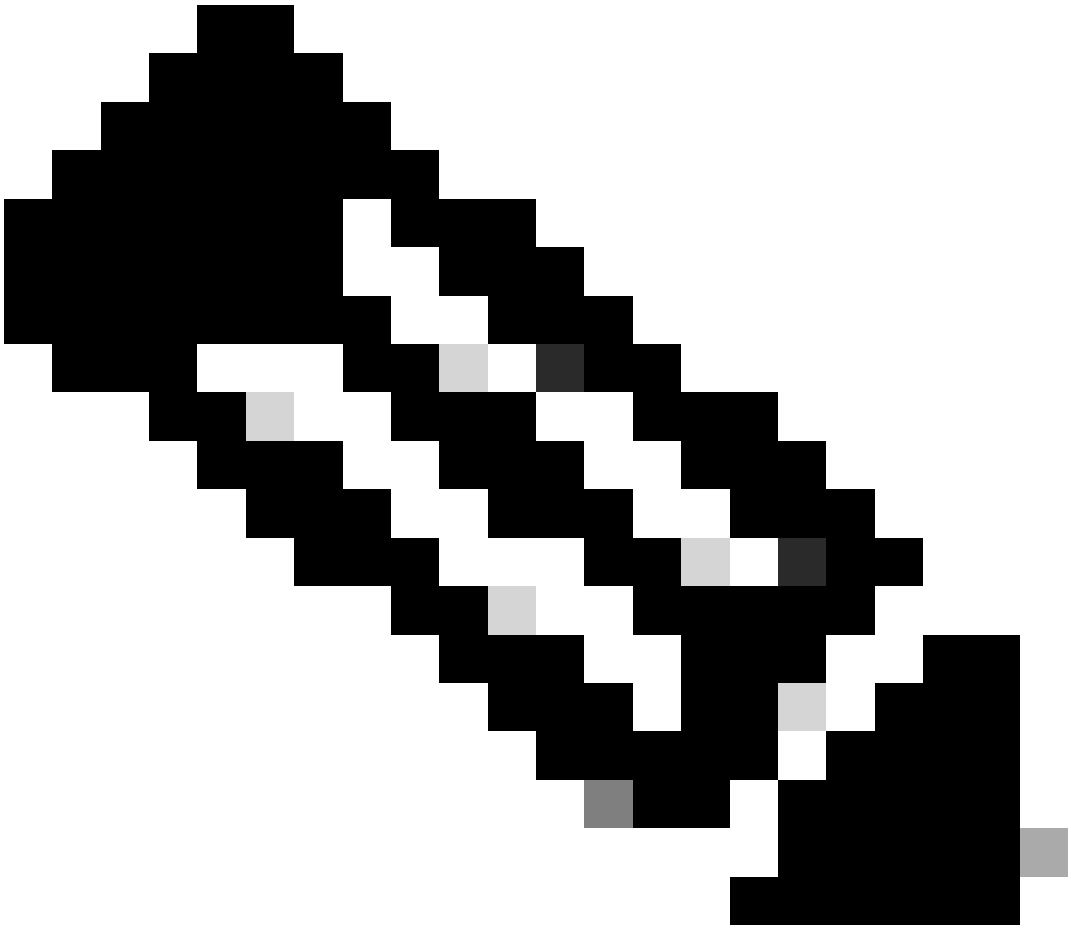
이러한 오류로 인해 사용자가 DNS 확인에 영향을 주지 않아야 합니다.

가상 어플라이언스는 DNScrypt의 가용성을 확인하기 위해 테스트 쿼리를 전송하며, 이는 차단된 테스트 쿼리입니다. 그러나 이러한 오류 메시지는 Virtual Appliance가 회사의 DNS 트래픽을 암호

화하여 추가 보안을 추가하지 않고 있음을 나타냅니다.

해결

가상 어플라이언스와 Umbrella의 DNS 리졸버 간 트래픽에 대해 DNS 패킷 검사를 비활성화하는 것이 좋습니다. 이렇게 하면 ASA에서 로깅 및 프로토콜 검사가 비활성화되지만 DNS 암호화를 허용하여 보안이 향상됩니다.



참고: 이러한 명령은 지침으로만 제공되며 프로덕션 환경을 변경하기 전에 Cisco 전문가와 상담하는 것이 좋습니다.
또한 ASA의 이러한 결함도 DNSCrypt에 문제가 발생할 수 있는 DNS over TCP에 영향을 줄 수 있습니다.
CSCsm90809 TCP를 통한 DNS 검사 지원

패킷 검사 예외 - IOS 명령

1. 208.67.222.222 및 208.67.220.220에 대한 트래픽을 거부하는 규칙을 사용하여 'dns_inspect'라는 새 ACL을 생성합니다.
   <#root>

```
access-list dns_inspect extended deny udp host <Appliance IP> host 208.67.220.220 eq domain
access-list dns_inspect extended deny tcp host <Appliance IP> host 208.67.220.220 eq domain
access-list dns_inspect extended deny udp host <Appliance IP> host 208.67.222.222 eq domain
access-list dns_inspect extended deny tcp host <Appliance IP> host 208.67.222.222 eq domain
access-list dns_inspect extended permit udp any any eq domain
access-list dns_inspect extended permit tcp any any eq domain


For VA 2.2.0, please also add our 3rd and 4th resolver IPs which are also enabled for encrypt


access-list dns_inspect extended deny udp host <Appliance IP> host 208.67.220.222 eq domain
access-list dns_inspect extended deny tcp host <Appliance IP> host 208.67.220.222 eq domain
access-list dns_inspect extended deny udp host <Appliance IP> host 208.67.222.220 eq domain
access-list dns_inspect extended deny tcp host <Appliance IP> host 208.67.222.220 eq domain
```

2. ASA에서 현재 DNS 검사 정책을 제거합니다. 예를 들면 다음과 같습니다.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)#  class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

3. #1단계에서 생성한 ACL과 일치하는 클래스 맵을 만듭니다.

```
class-map dns_inspect_cmap
 match access-list dns_inspect
```

4. global_policy 아래에서 policy-map을 구성합니다. #3단계에서 만든 클래스 맵과 일치해야 합니다. DNS 검사를 사용하도록 설정하십시오.

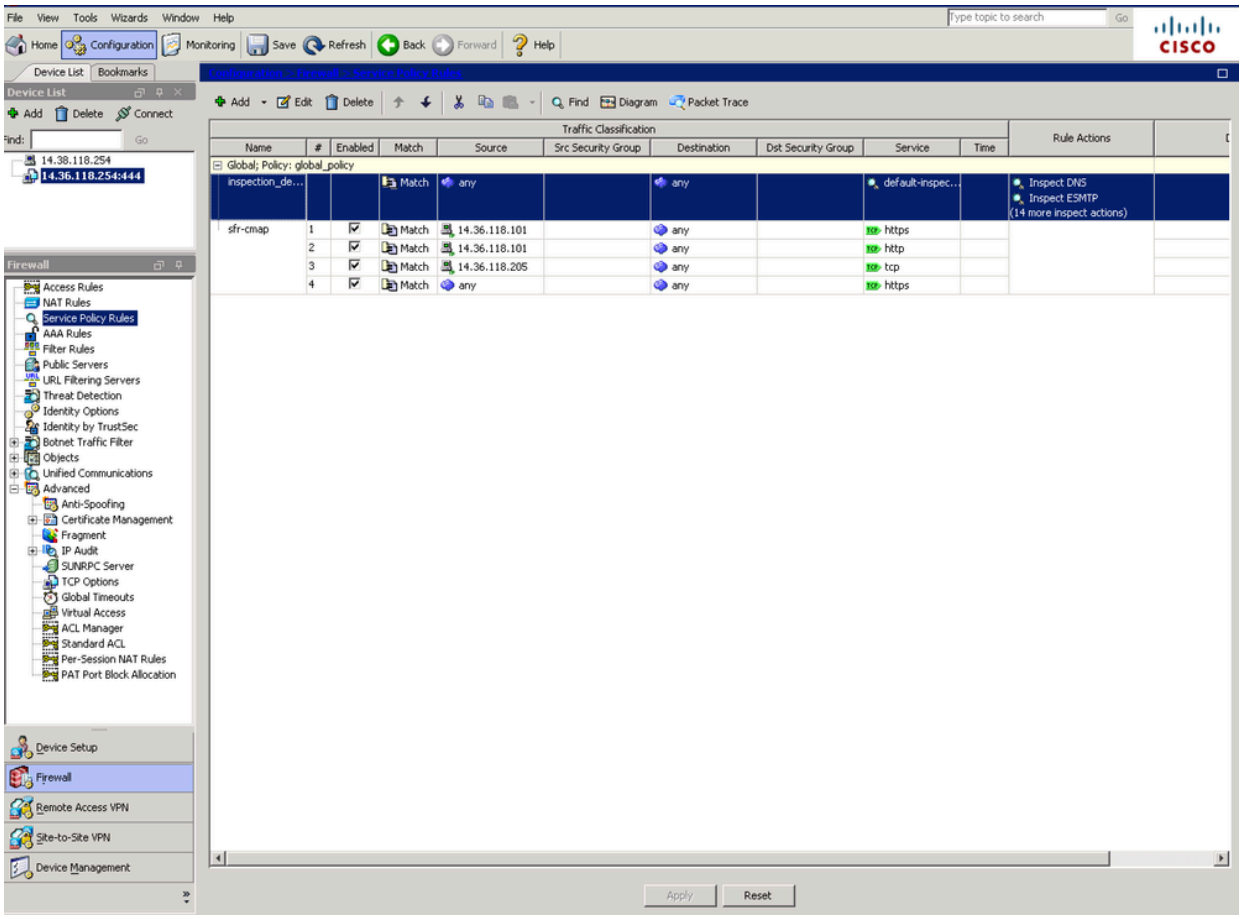
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. 활성화되면 다음을 실행하여 트래픽이 제외에 도달했는지 확인할 수 있습니다.

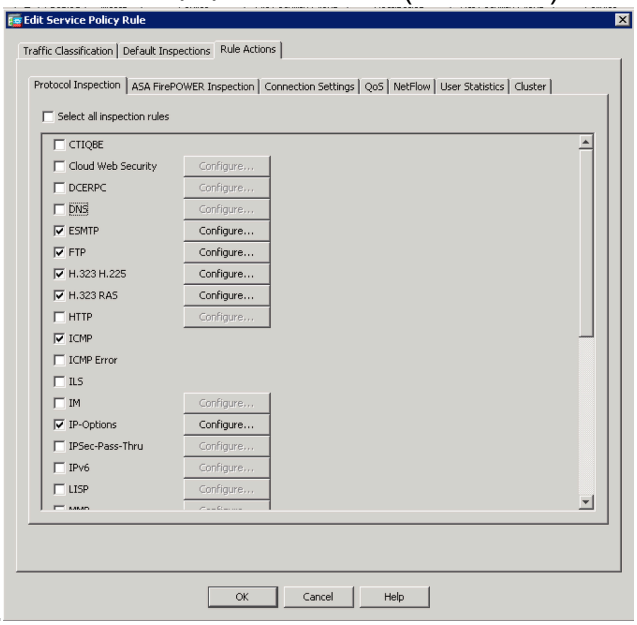
```
sh access-list dns_inspect
```

패킷 검사 예외 - ASDM 인터페이스

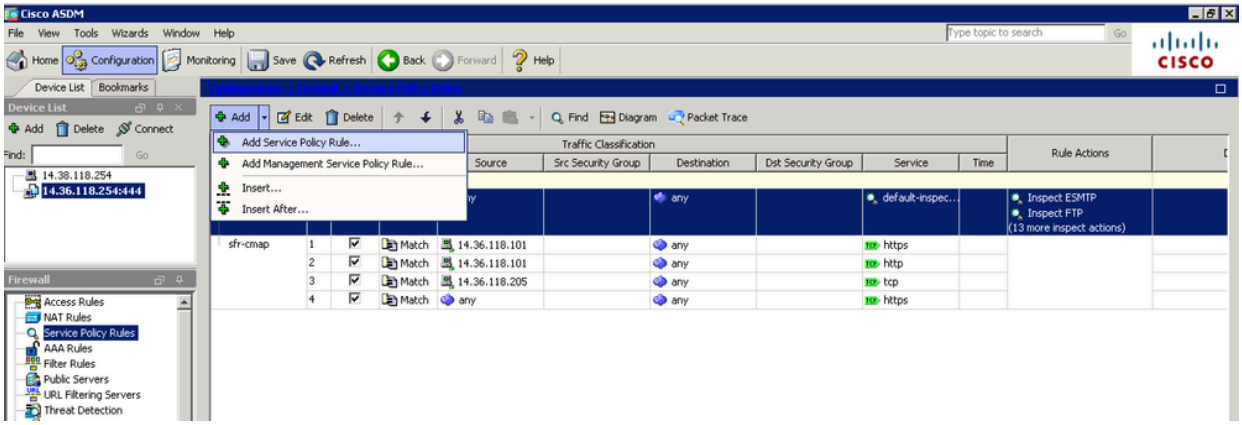
1. 해당되는 경우 먼저 DNS 패킷 검사를 비활성화합니다.이 작업은 Configuration(컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)에서 수행됩니다.



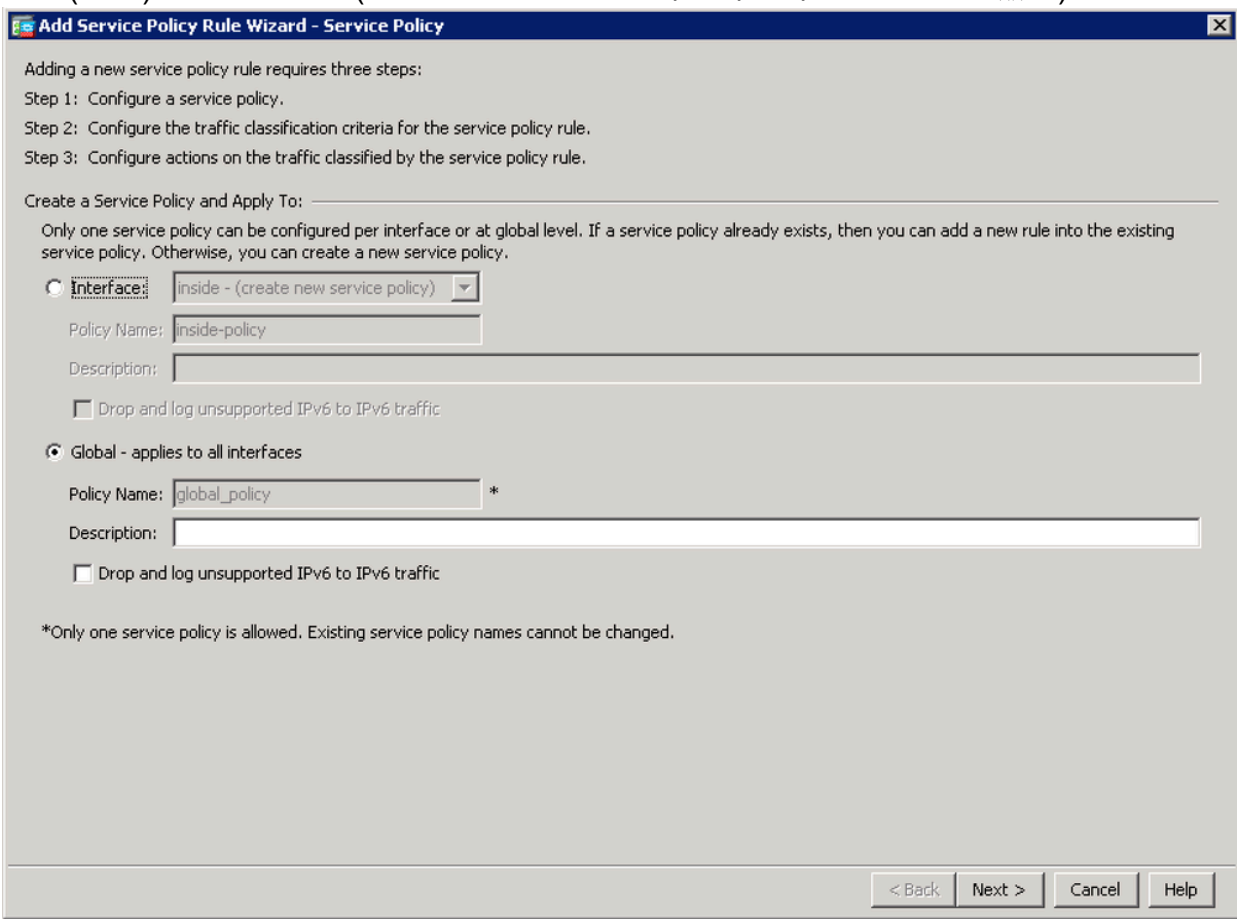
2. 이 예에서는 DNS 검사가 Global Policy 및 'inspection_default' 클래스 아래에서 활성화됩니다. 강조 표시하고 Edit(편집)를 클릭합니다. 새 창에서 "Rule Action(규칙 작업)" 탭 아래의 'DNS' 확인란의 선택을 취소합니다.



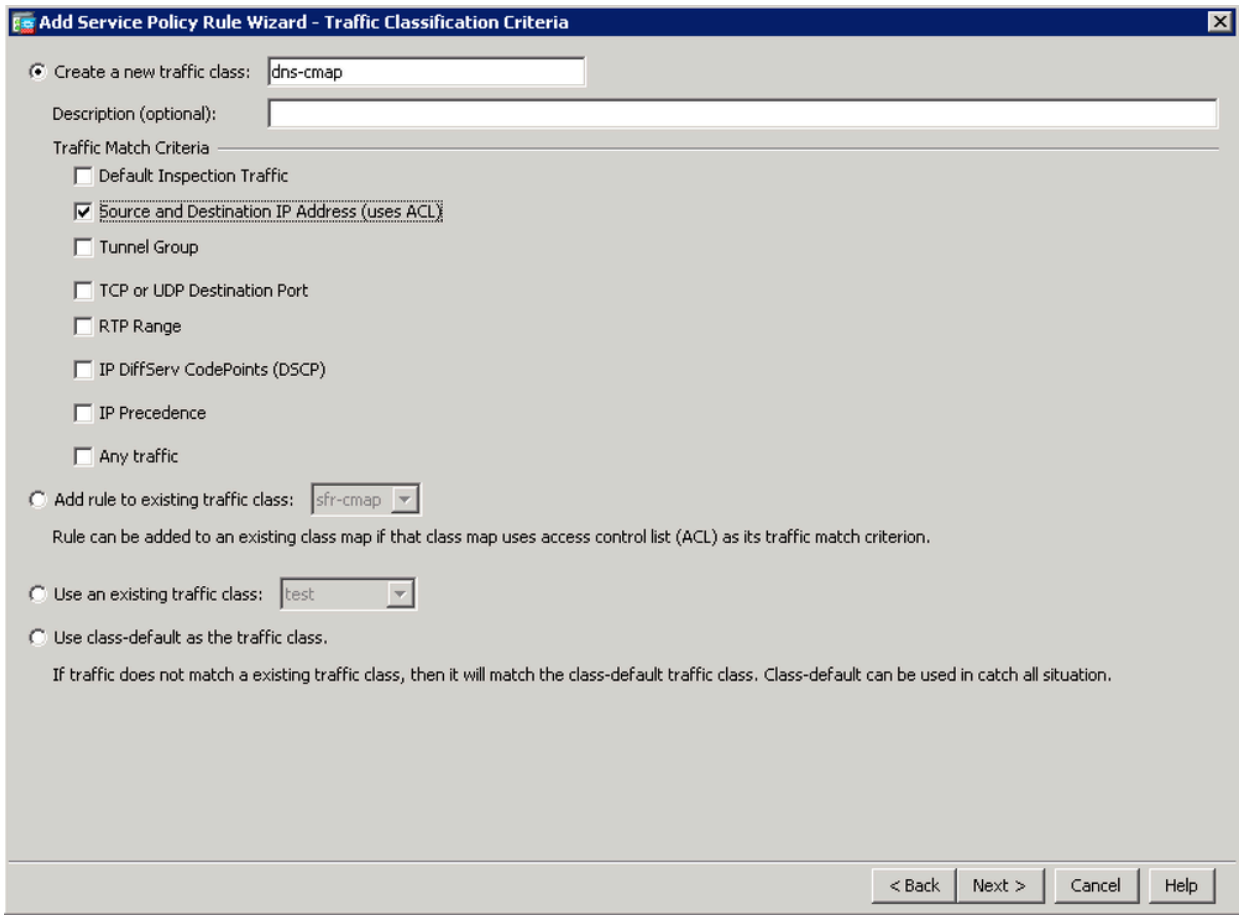
3. 이제 DNS 검사를 다시 구성할 수 있으며, 이번에는 트래픽 면제를 추가로 적용할 수 있습니다. Add(추가) > Add Service Policy Rule(서비스 정책 규칙 추가)...을 클릭합니다.



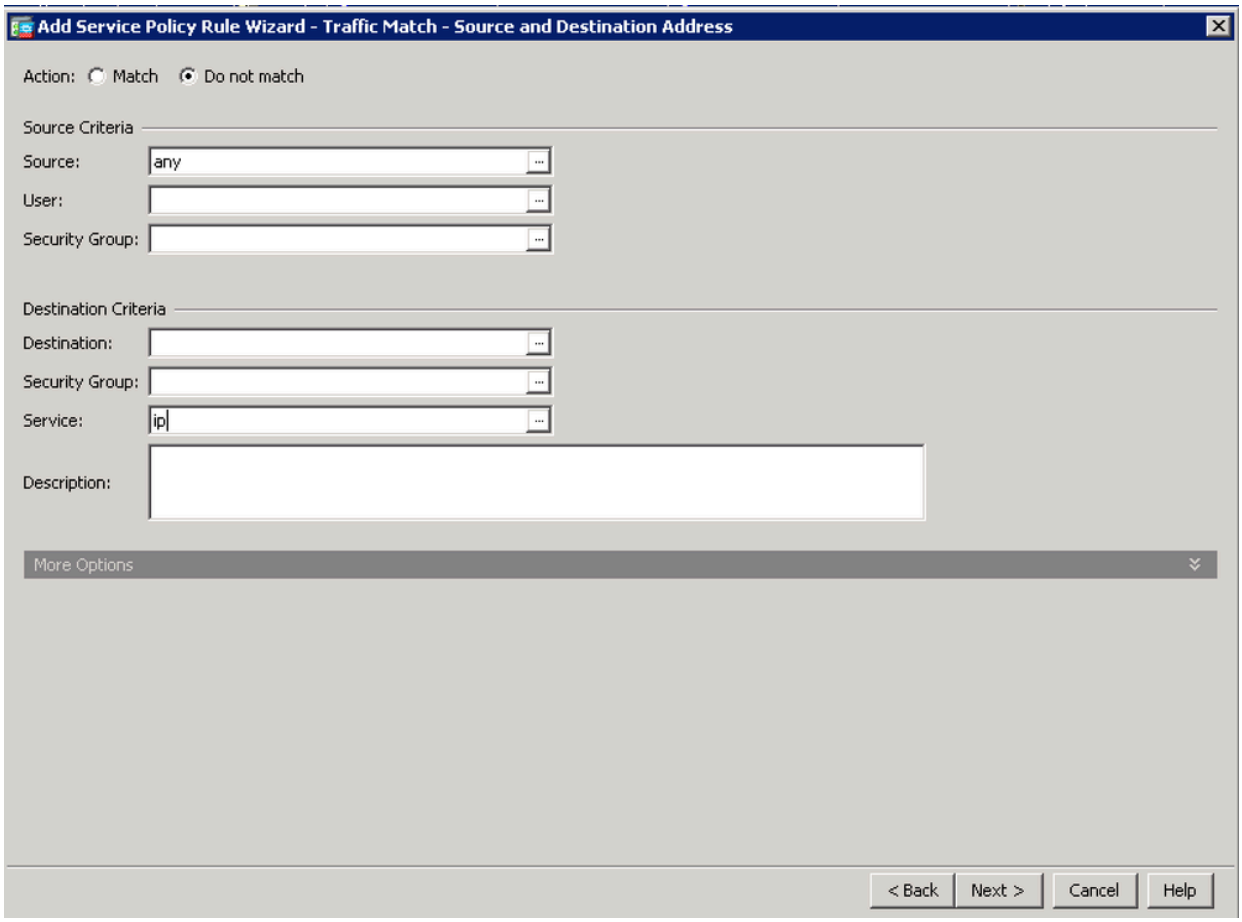
4. "Global - Applies to all interfaces(전역 - 모든 인터페이스에 적용됨)"를 선택하고 Next(다음)를 클릭합니다(원하는 경우 특정 인터페이스에도 적용할 수 있음).



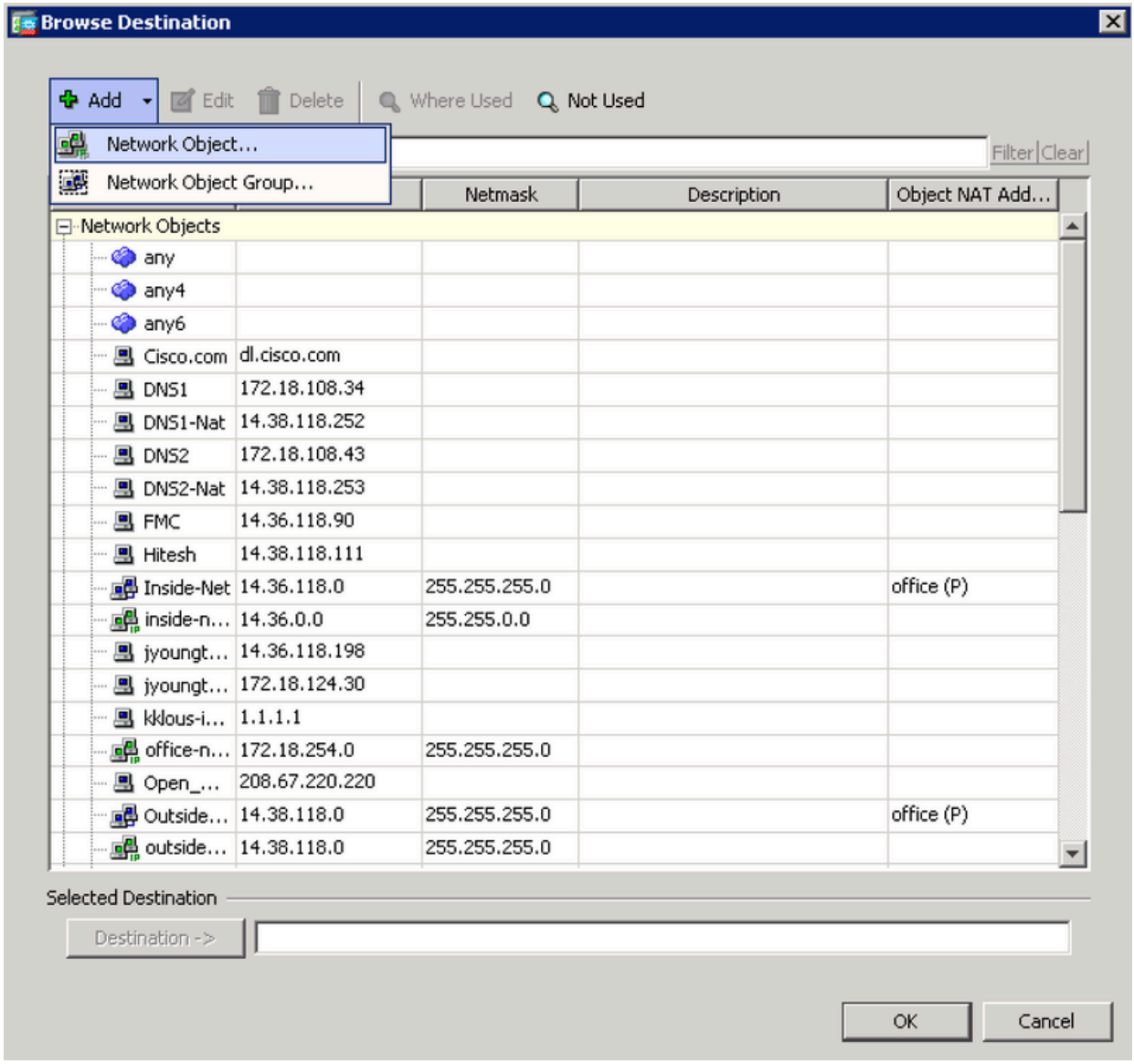
5. 클래스 맵에 이름을 지정하고(예: 'dns-cmap') "Source and Destination IP Address (uses ACL)(소스 및 대상 IP 주소(ACL 사용))" 옵션을 선택합니다. Next(다음)를 클릭합니다..

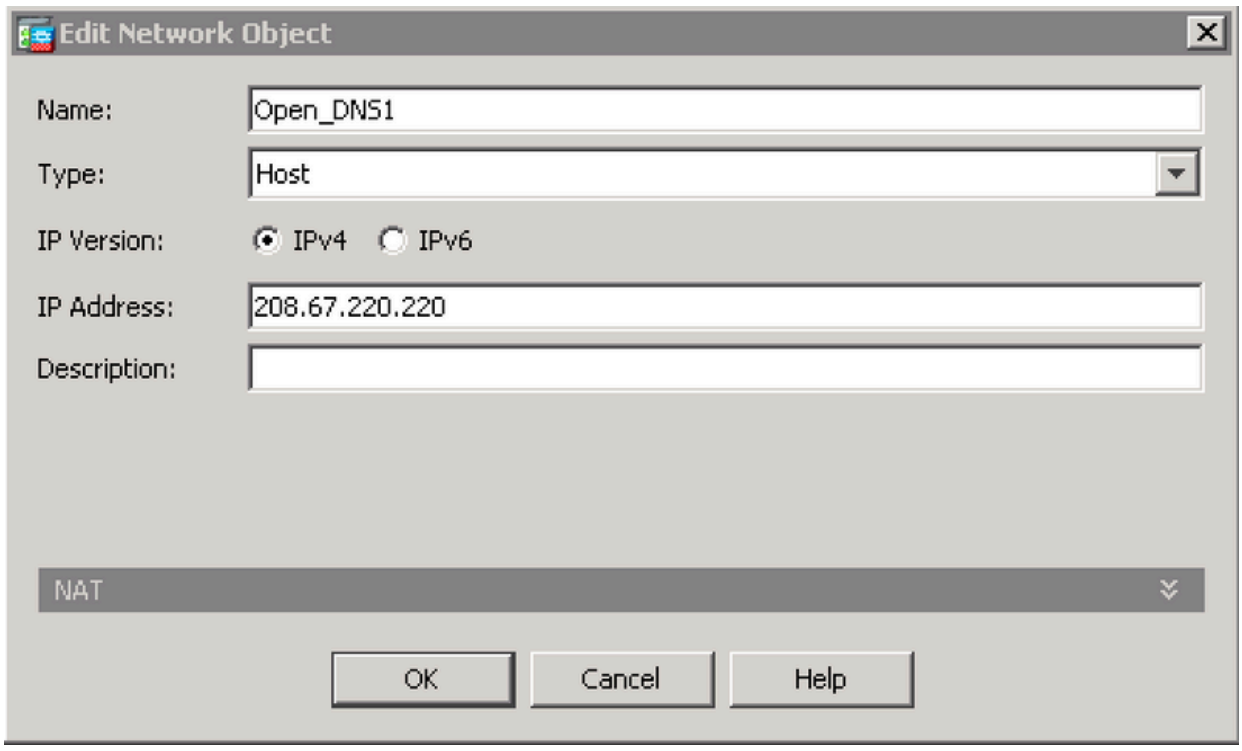


6. "Do not match" 작업을 사용하여 검사하지 않을 트래픽을 구성하는 것으로 시작합니다. Source의 경우 'any' 옵션을 사용하여 Umbrella의 DNS 서버로 향하는 모든 트래픽을 제외할 수 있습니다. 또는 특정 가상 어플라이언스 IP 주소만 제외하도록 여기서 네트워크 개체 정의를 생성할 수 있습니다.

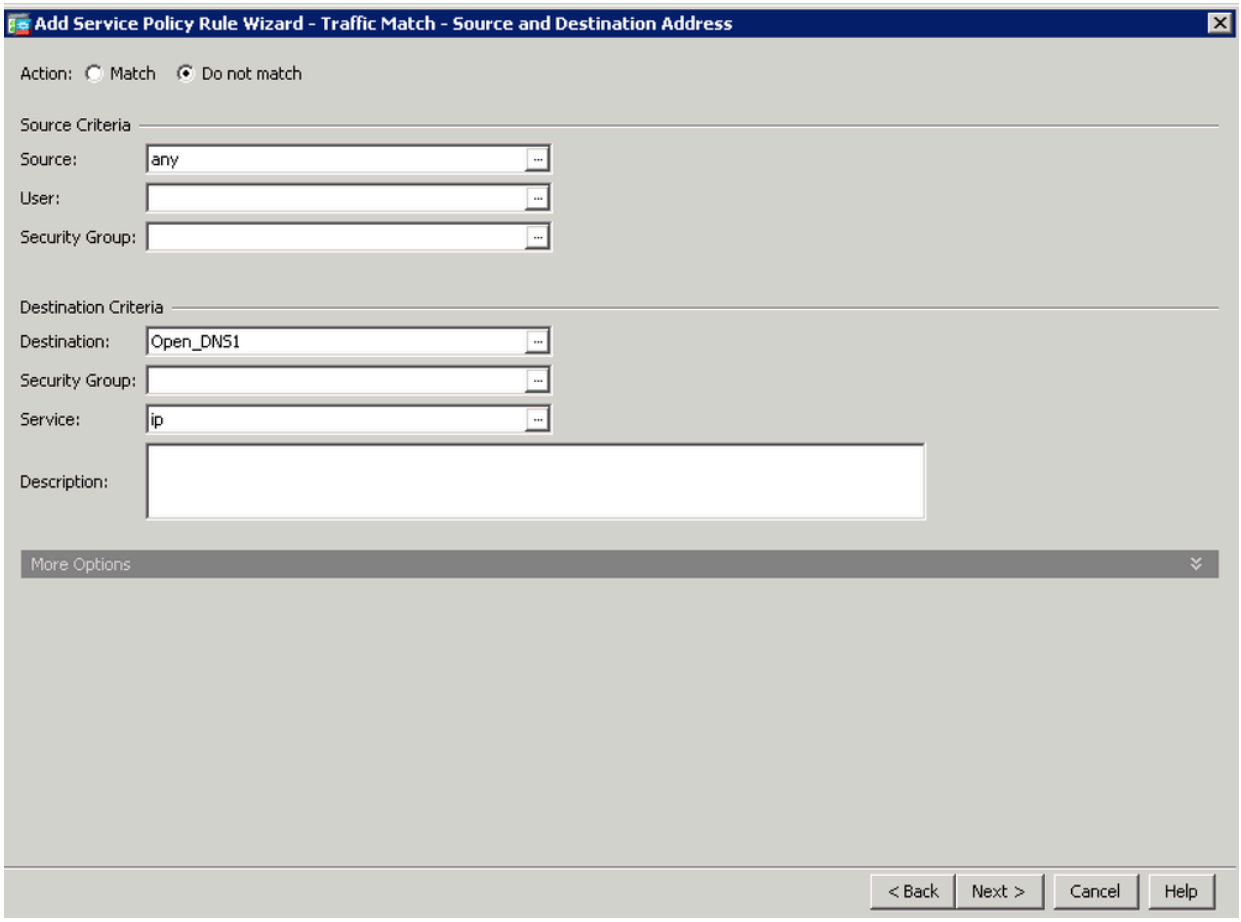


7. Destination 필드에서...를 클릭합니다. 다음 창에서 Add(추가) > Network Object(네트워크 개체)를 클릭하고 IP 주소가 '208.67.222.222'인 개체를 만듭니다. IP 주소가 '208.67.220.220'인 개체를 만들려면 이 단계를 반복합니다.

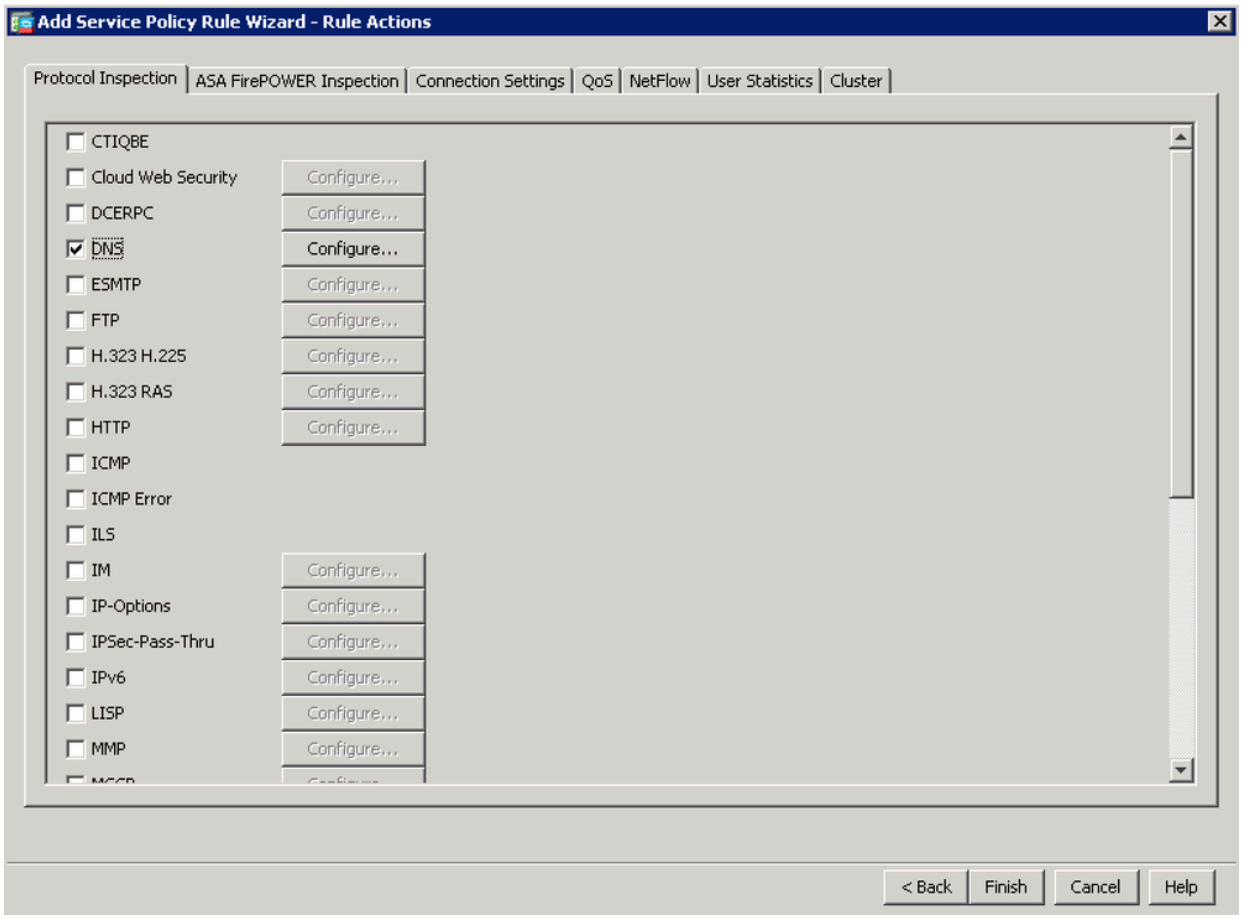

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90
Hitesh 14.38.118.111
Inside-Net 14.36.118.0 255.255.255.0 office (P)
inside-n... 14.36.0.0 255.255.0.0
jyoungt... 14.36.118.198
jyoungt... 172.18.124.30
kklous-i... 1.1.1.1
office-n... 172.18.254.0 255.255.255.0
Open_... 208.67.220.220
Outside... 14.38.118.0 255.255.255.0 office (P)
outside... 14.38.118.0 255.255.255.0
Selected Destination
Destination ->
OK
Cancel


Edit Network Object
Name: Open_DNS1
Type: Host
IP Version: IPv4 IPv6
IP Address: 208.67.220.220
Description:
NAT
OK
Cancel
Help

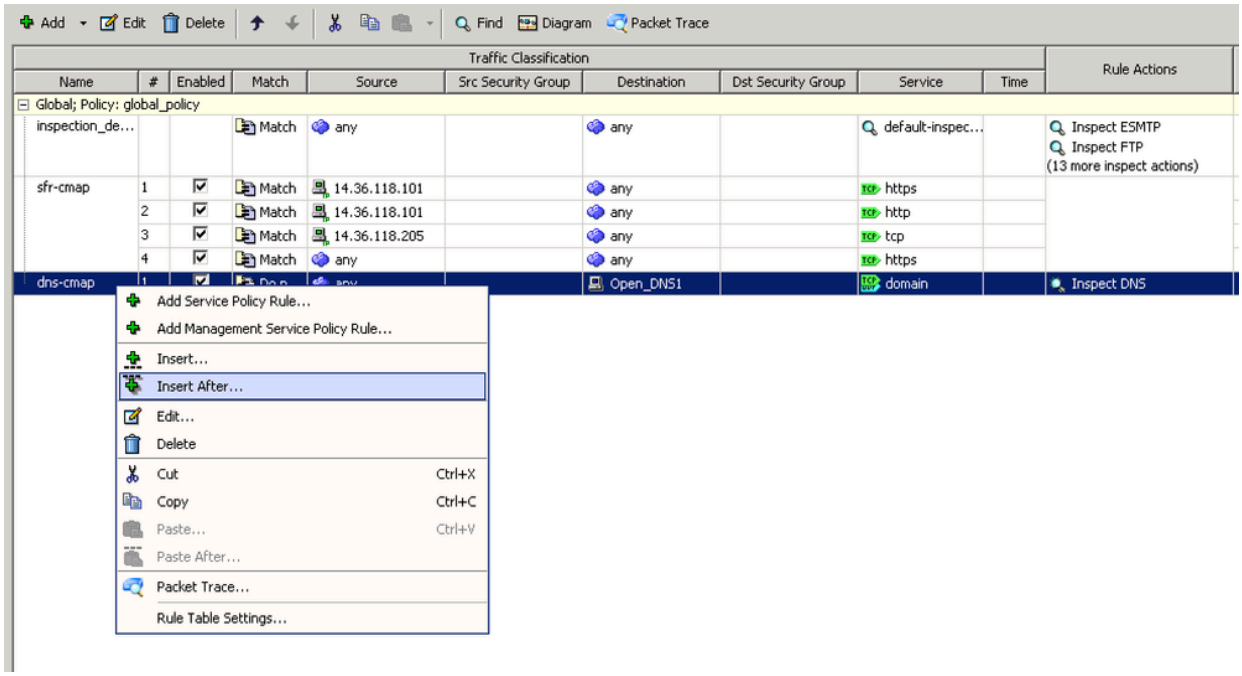
8. 두 Umbrella 네트워크 객체를 모두 Destination(대상) 필드에 추가하고 OK(확인)를 클릭합니다.



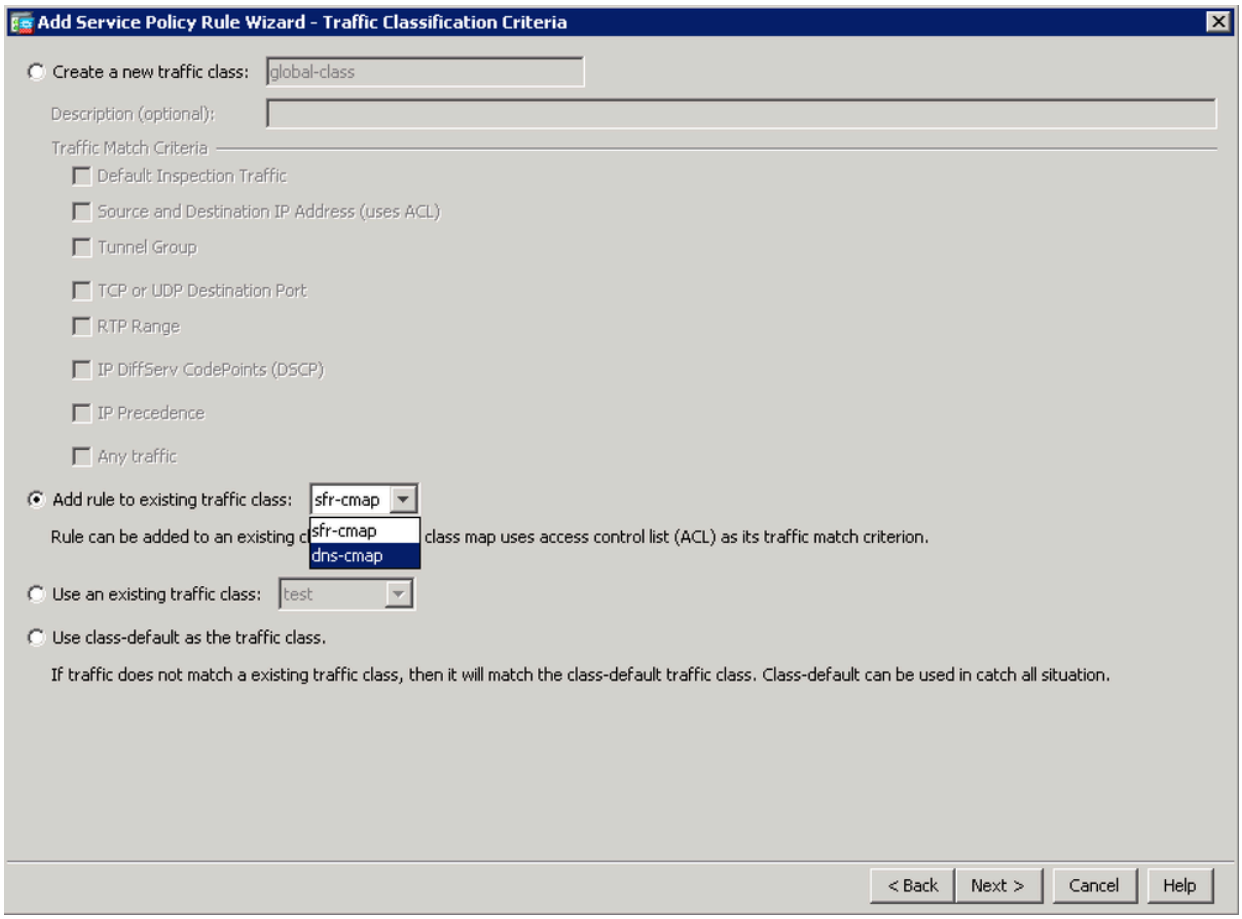
9. 다음 창에서 'DNS' 상자를 선택하고 Finish(마침)를 클릭합니다.



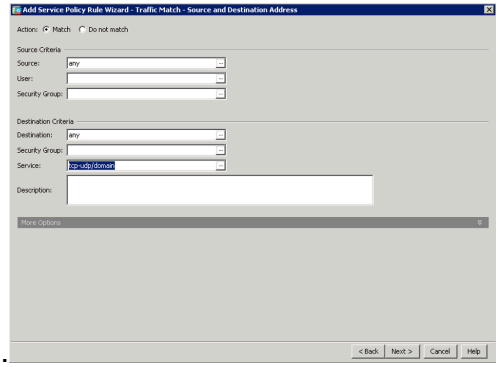
10. 이제 ASA에 'dns-cmap'에 대한 새로운 전역 정책이 표시됩니다. 이제 ASA에서 검사하는 나머지 트래픽을 구성해야 합니다. 이는 'dns-cmap'을 마우스 오른쪽 버튼으로 클릭하고 "Insert After..." 옵션을 선택하여 수행합니다. 새 규칙을 생성합니다.



11. 첫 번째 창에서 Next(다음)를 클릭한 다음 "Add rule to existing traffic class(기존 트래픽 클래스에 규칙 추가):" 라디오 버튼을 선택합니다. 드롭다운에서 'dns-cmap'을 선택하고 Next(다음)를 클릭합니다.

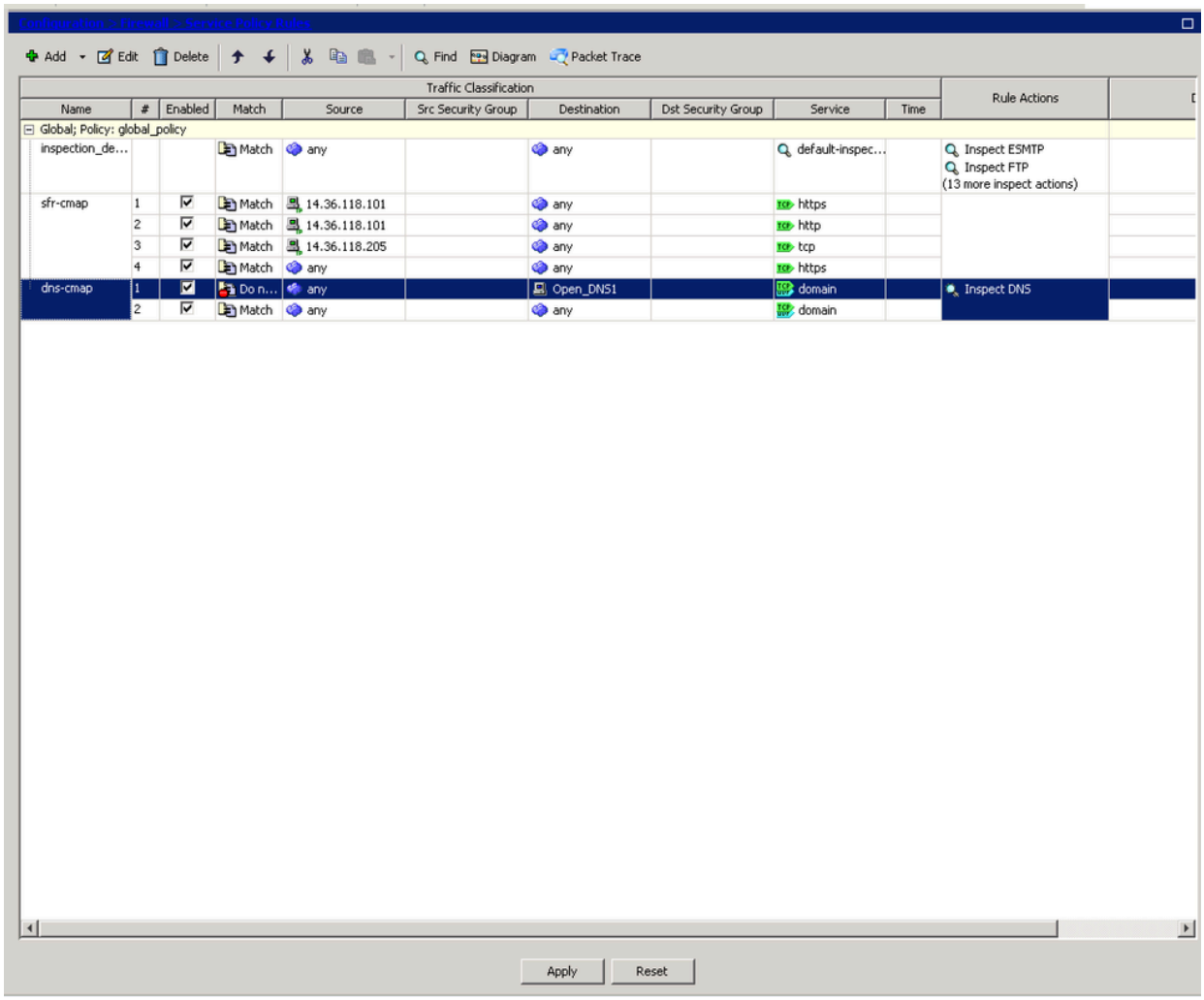


12. 작업을 'Match'로 둡니다. DNS 검사의 대상이 되는 트래픽의 Source, Destination 및 Service를 선택합니다. 예를 들어, TCP 또는 UDP DNS 서버로 이동하는 모든 클라이언



트의 트래픽을 매칭합니다. Next(다음)를 클릭합니다.

13. 'DNS' 옵션을 선택한 상태로 두고 Finish(마침)를 클릭합니다.
14. 창 하단에서 Apply(적용)를 클릭합니다.



추가 정보

ASA 면제를 구성하는 대신 DNScrypt를 비활성화하려면 Umbrella 지원에 문의하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.