Problemen oplossen ASA Firewall blokkeren DNScrypt Functionaliteit van de Umbrella Virtual Appliance

Inhoud

Inleiding

In dit artikel wordt beschreven hoe u problemen kunt oplossen met de ASA Firewall die de DNScrypt-functionaliteit blokkeert.

Overzicht

De Cisco ASA Firewall kan de DNScrypt-functionaliteit blokkeren die wordt aangeboden door de Umbrella Virtual Appliance. Dit resulteert in deze waarschuwing voor het Umbrella Dashboard:

> 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

Deze foutmeldingen zijn ook te zien in de ASA firewall logs:

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

DNSCrypt-codering is ontworpen om de inhoud van uw DNS-query's te beschermen en voorkomt als zodanig ook dat firewalls pakketinspecties uitvoeren.

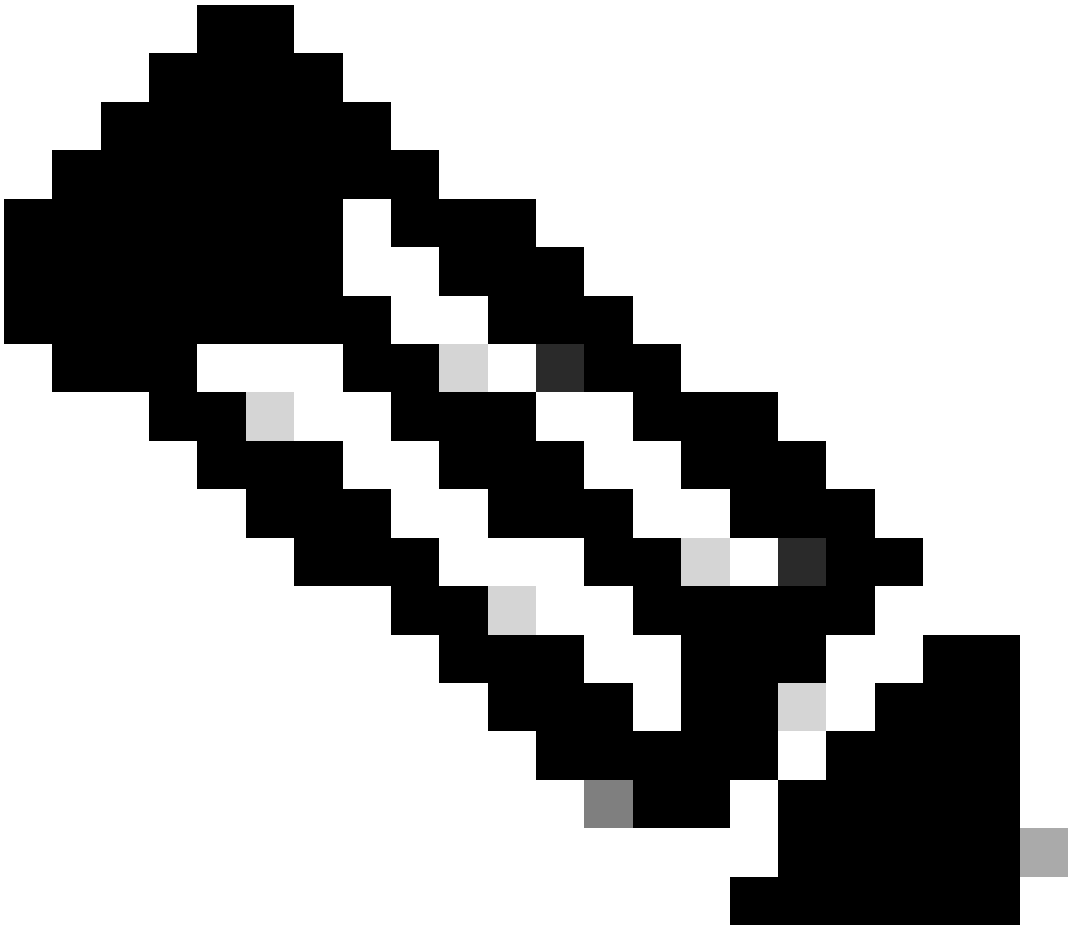
Oorzaak

Deze fouten mogen geen gevolgen hebben voor gebruikers die te maken hebben met de DNS-resolutie.

De Virtual Appliance verzendt testquery's om de beschikbaarheid van DNScrypt te bepalen en het zijn die testquery's die worden geblokkeerd. Deze foutmeldingen geven echter aan dat het virtuele apparaat geen extra beveiliging toevoegt door het DNS-verkeer van uw bedrijf te coderen.

resolutie

We raden aan om de DNS-pakketcontrole uit te schakelen voor verkeer tussen de Virtual Appliance en de DNS-resolvers van Umbrella. Hoewel dit de registratie en protocolinspectie op de ASA uitschakelt, verbetert het de beveiliging door DNS-codering toe te staan.



Opmerking: deze opdrachten worden alleen ter begeleiding gegeven en het wordt aanbevolen dat een Cisco-expert wordt geraadpleegd voordat wijzigingen in een productieomgeving worden aangebracht.
Wees je ook bewust van dit defect op ASA kan invloed hebben op DNS via TCP, wat ook problemen met DNSCrypt kan veroorzaken:
CSCsm90809 DNS-inspectieondersteuning voor DNS via TCP

Uitzonderingen voor pakketinspectie – IOS-opdrachten

1. Maak een nieuwe ACL genaamd 'dns_inspect' met regels om verkeer te weigeren naar 208.67.222.222 en 208.67.220.220.
   <#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. Verwijder het huidige DNS-inspectiebeleid op de ASA. Voorbeeld:

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

3. Maak een klassenoverzicht dat overeenkomt met de ACL die is gemaakt in stap #1:

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

4. Configureer een beleidskaart onder global_policy. Dit moet overeenkomen met de klassenindeling die is gemaakt in stap #3. DNS-inspectie inschakelen.

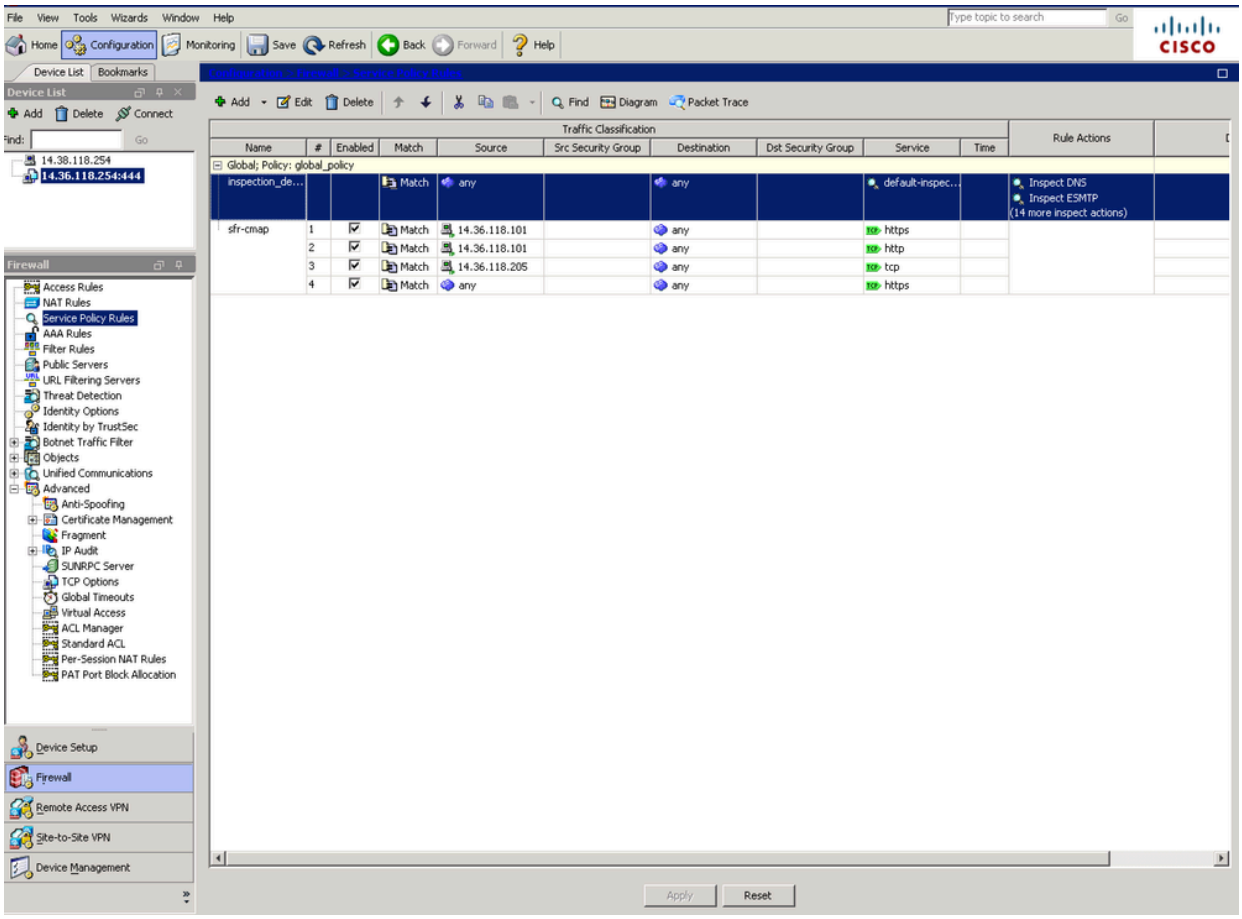
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. Als deze optie is ingeschakeld, kunt u controleren of het verkeer de uitsluitingen raakt door het volgende uit te voeren:

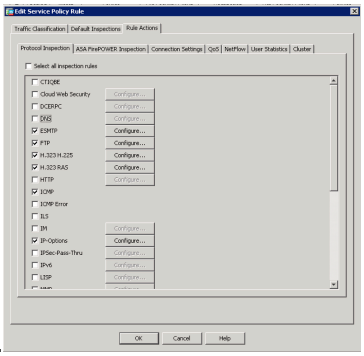
```
sh access-list dns_inspect
```

Uitzonderingen voor pakketinspectie – ASDM-interface

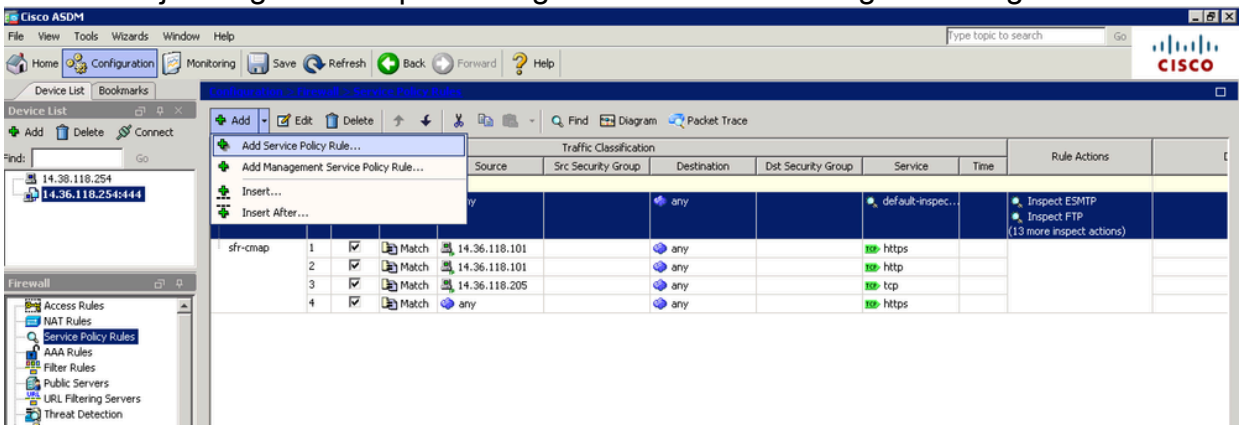
1. Schakel eerst een DNS-pakketinspectie uit, indien van toepassing.Dit gebeurt in Configuratie > Firewall > Servicebeleidsregels.



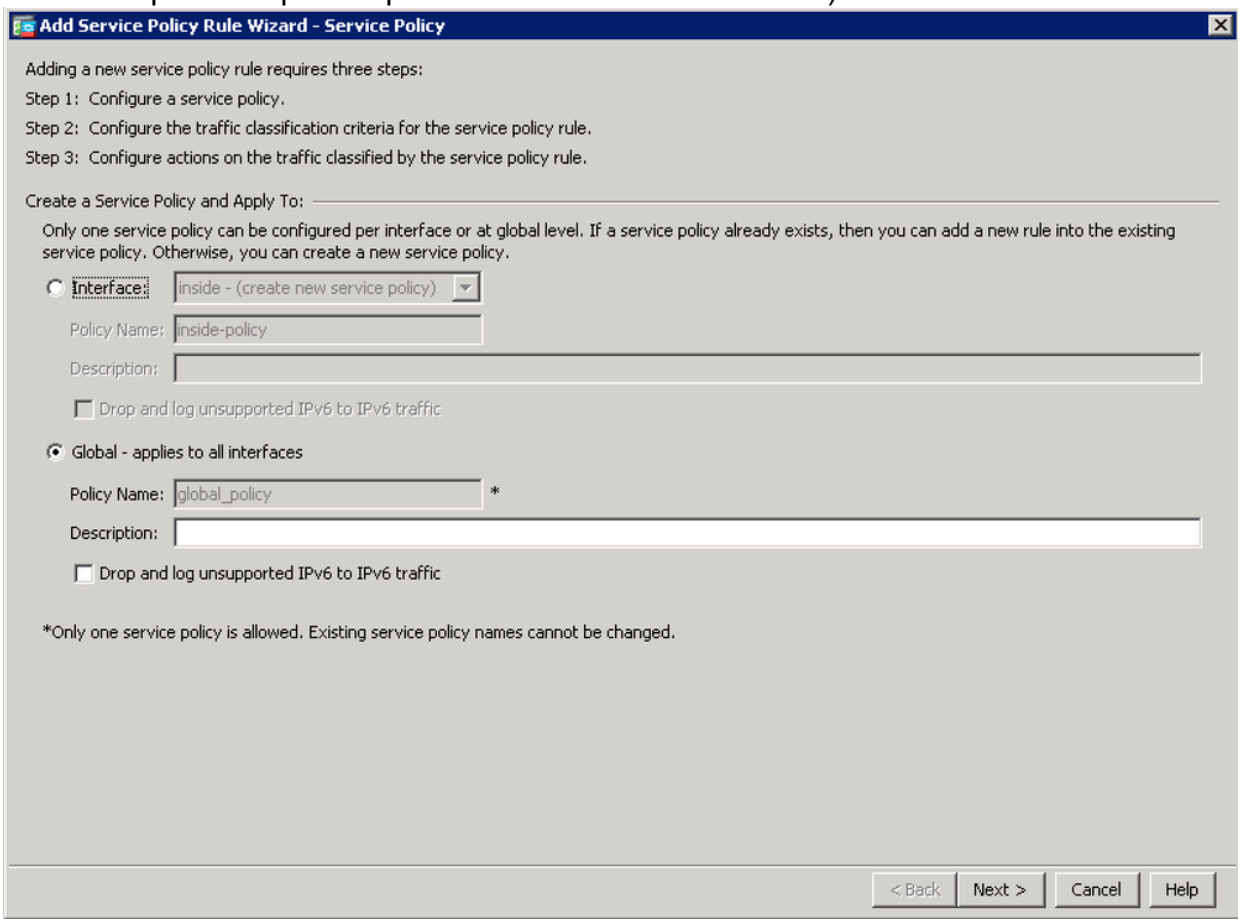
2. In het voorbeeld is de DNS-inspectie ingeschakeld onder de klasse Global Policy en 'inspection_default'. Markeer het en klik op Bewerken. Schakel in het nieuwe venster het selectievakje voor 'DNS' uit onder het tabblad 'Regelactie'.



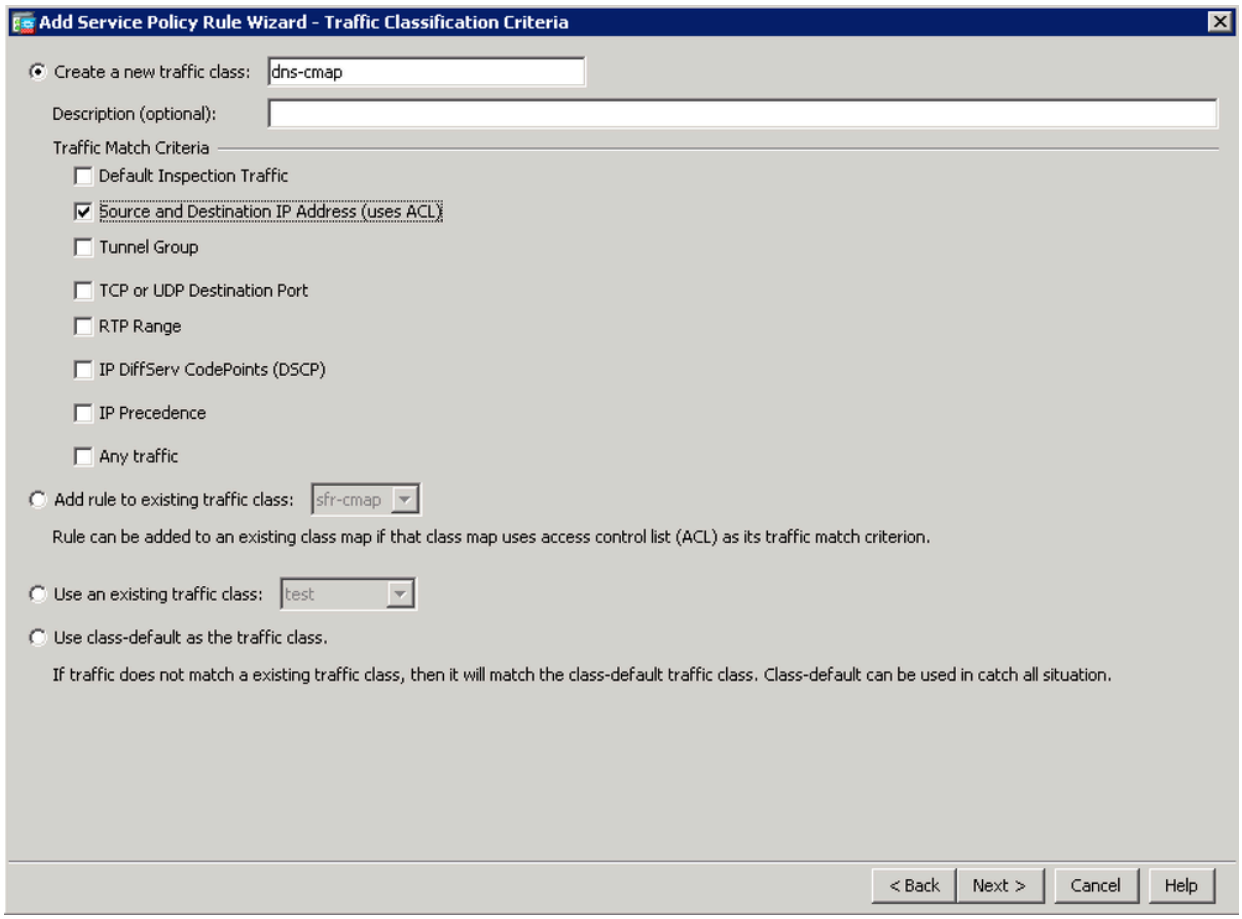
3. Nu kunt u de DNS-inspectie opnieuw configureren, dit keer met extra verkeersvrijstellingen. Klik op Toevoegen > Servicebeleidsregel toevoegen...



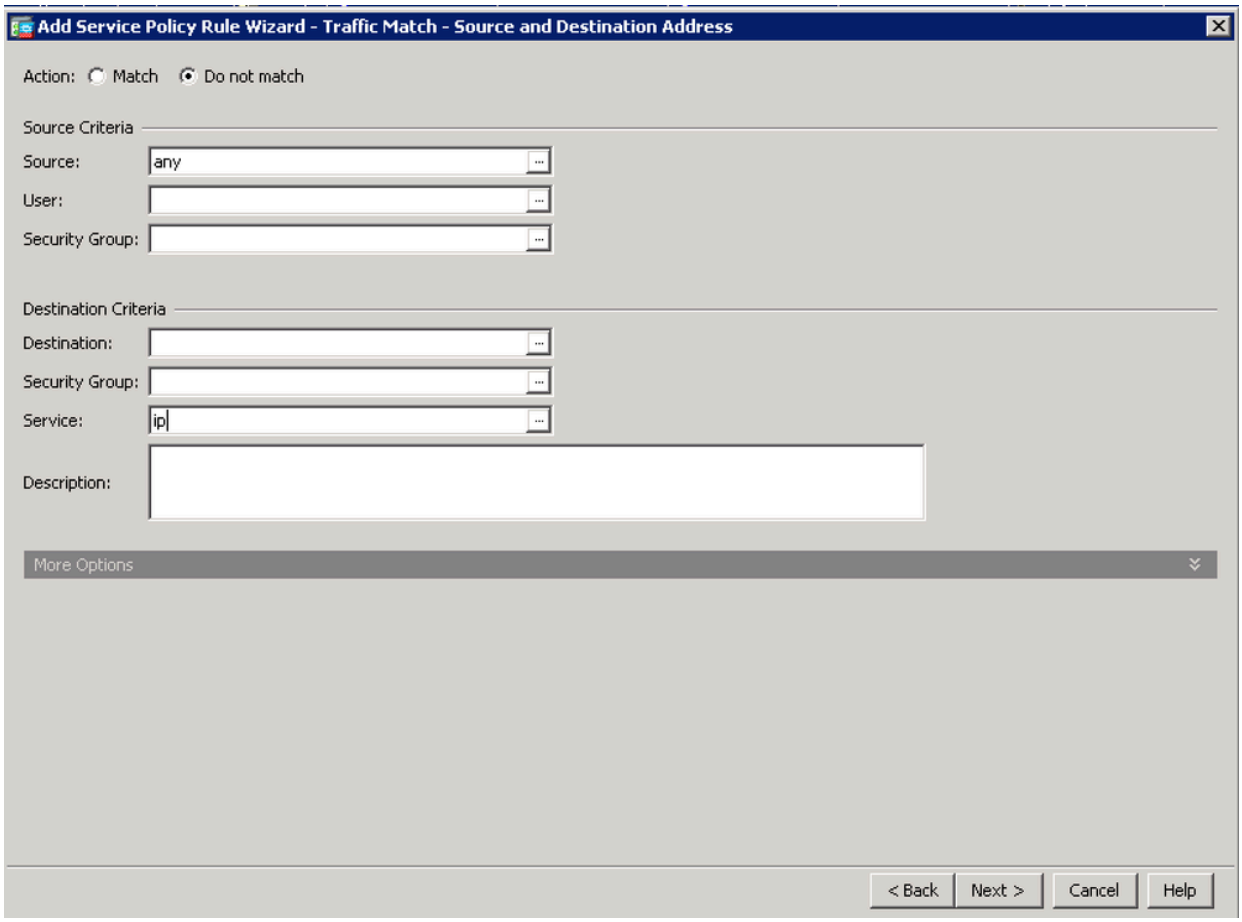
4. Selecteer "Algemeen - van toepassing op alle interfaces" en klik op Volgende (u kunt dit ook toepassen op een specifieke interface als u dat wilt).



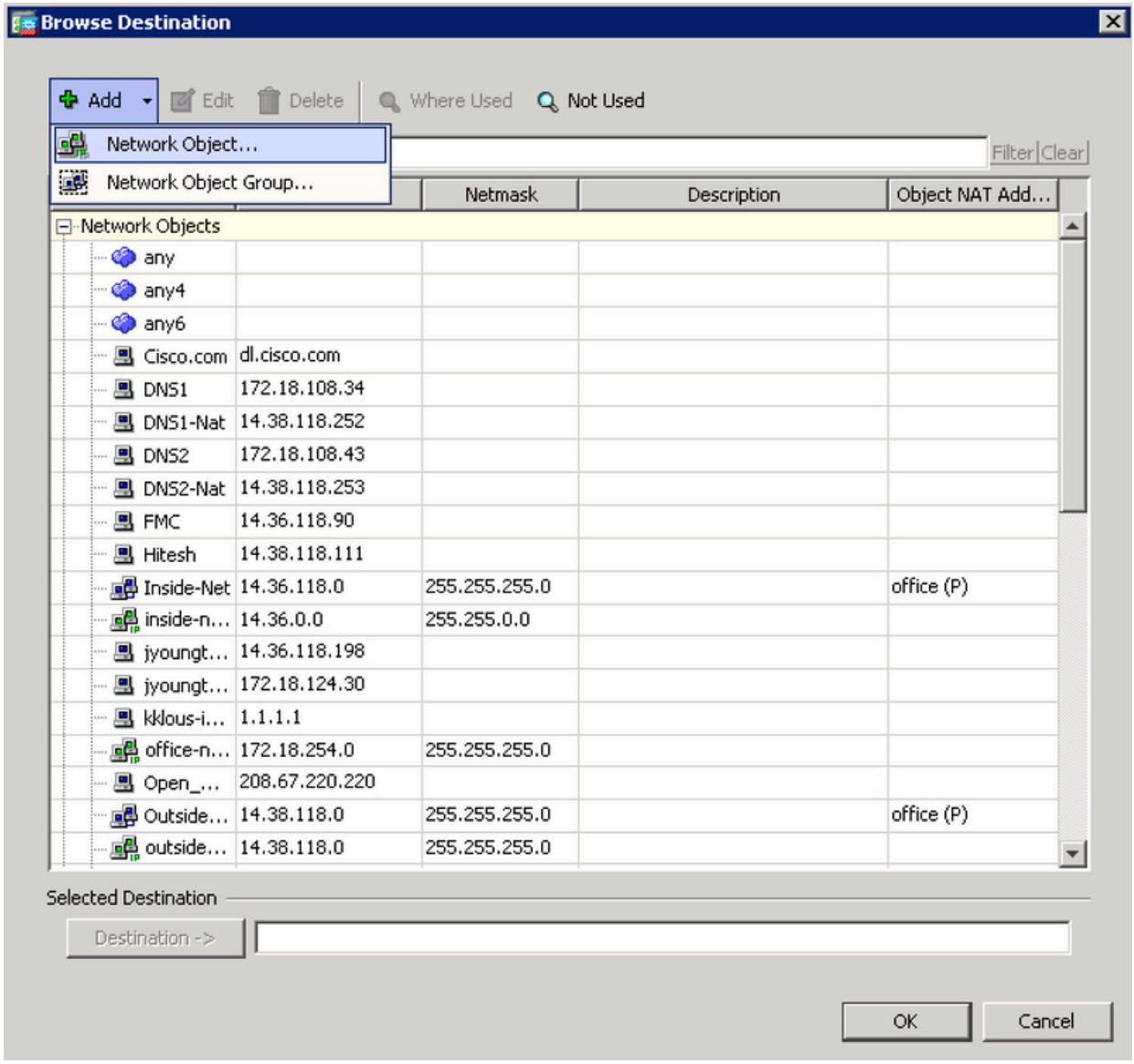
5. Geef een naam aan de class-map (bijvoorbeeld 'dns-cmap') en vink de optie "Source and Destination IP Address (uses ACL)" aan. Klik op Volgende.

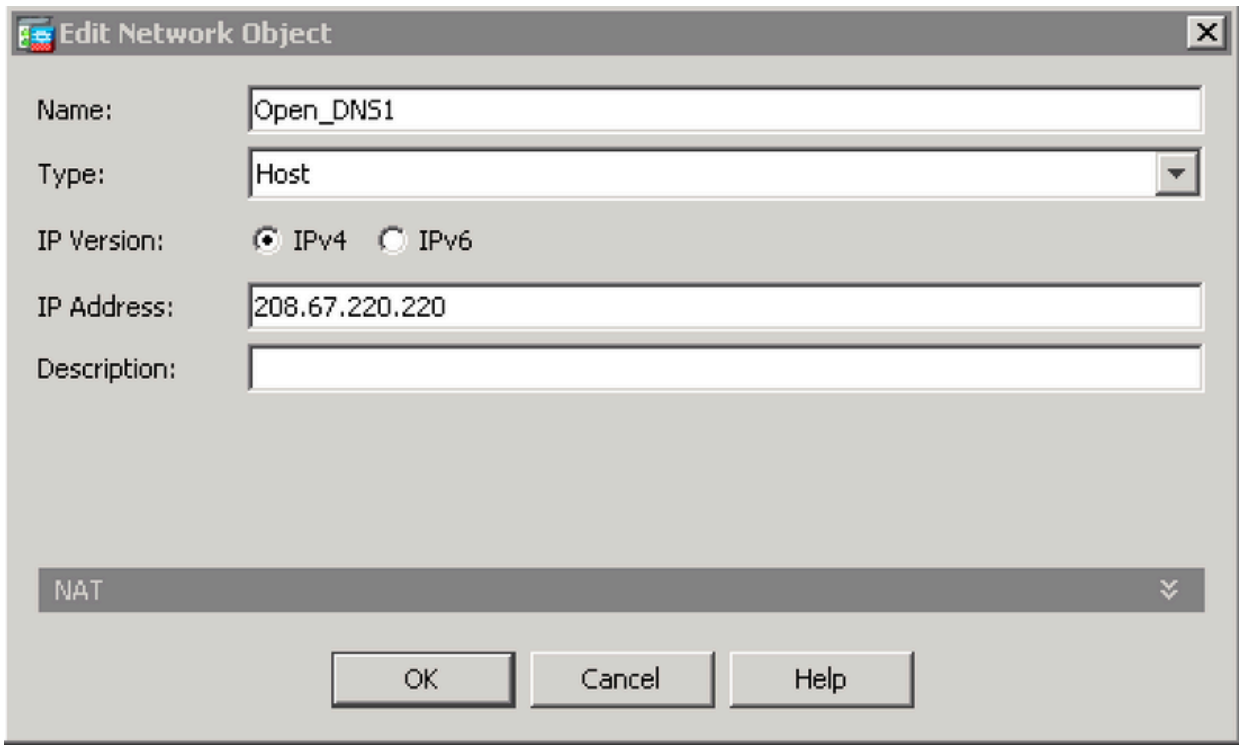


6. Begin met het configureren van het verkeer dat u niet wilt worden geïnspecteerd met behulp van de actie "Niet overeenkomen".
   Voor Source kunt u de optie 'any' gebruiken om al het verkeer dat bestemd is voor de DNS-servers van Umbrella vrij te stellen. Als alternatief kunt u hier een Network Object-definitie maken om alleen het specifieke IP-adres van het virtuele apparaat vrij te stellen.

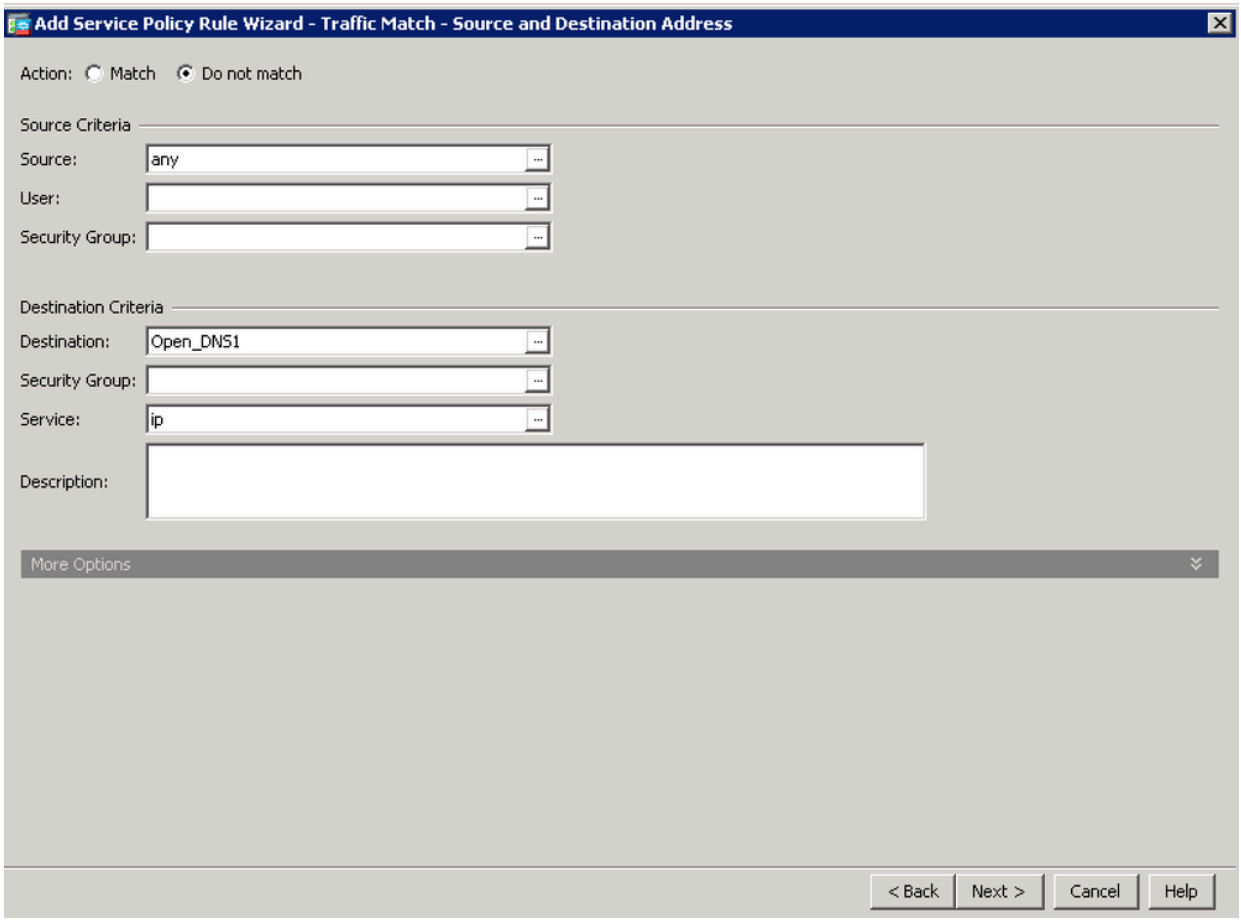


7. Klik ... in het veld Bestemming. Klik in het volgende venster op Toevoegen > Netwerkobject en maak een object met het IP-adres van '208.67.222.222'. Herhaal deze stap om een object te maken met een IP-adres van '208.67.220.220'.

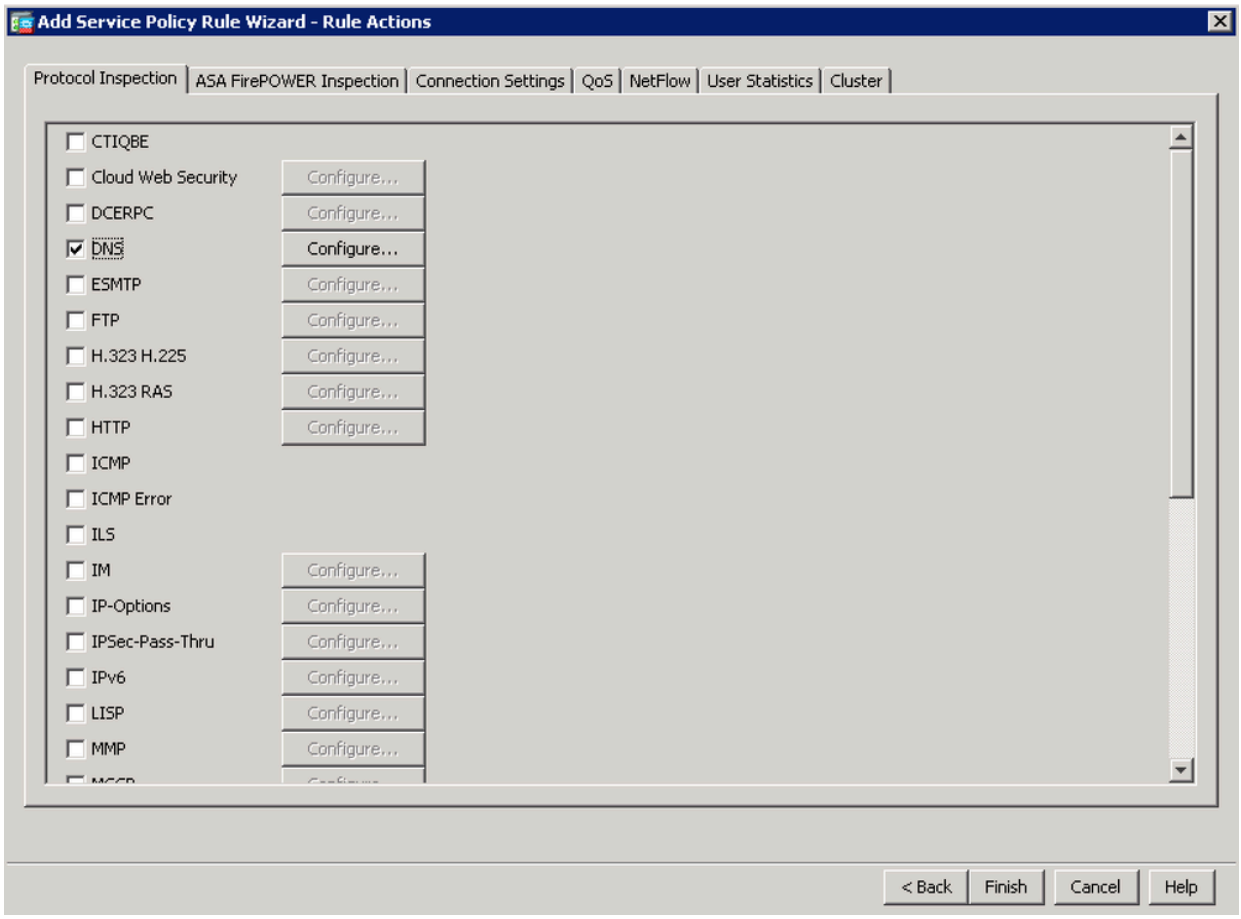

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90
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

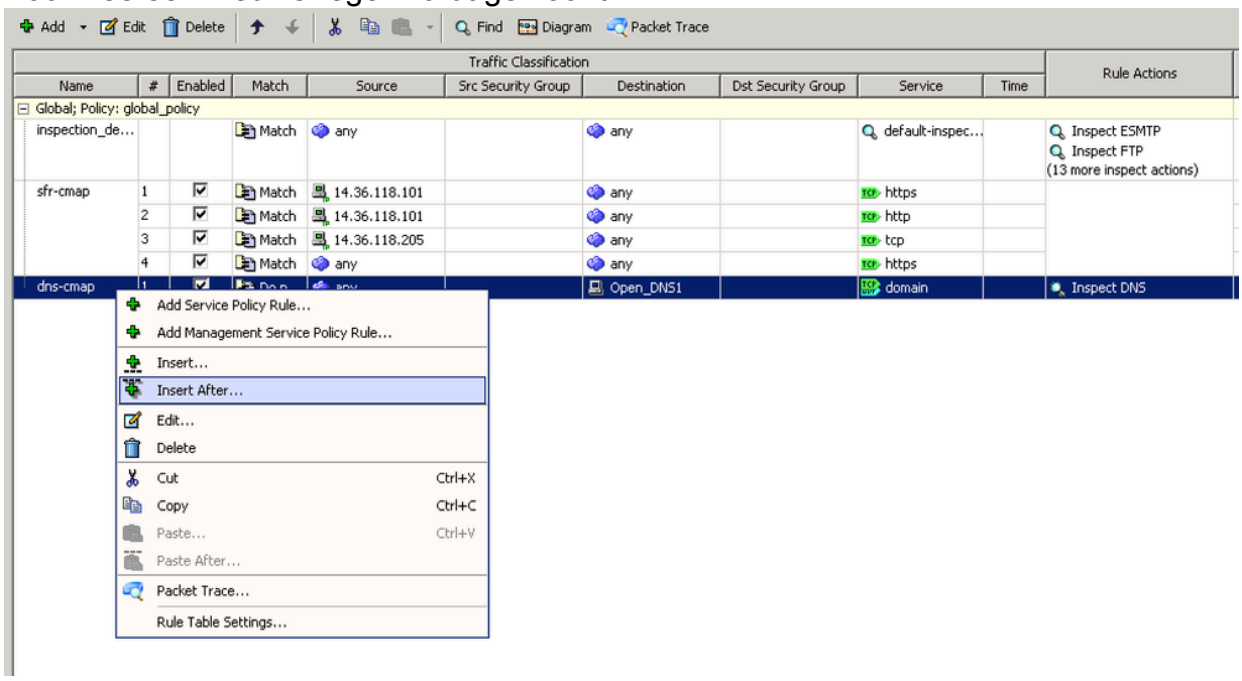
8. Voeg beide overkoepelende netwerkobjecten toe aan het veld Bestemming en klik op OK.



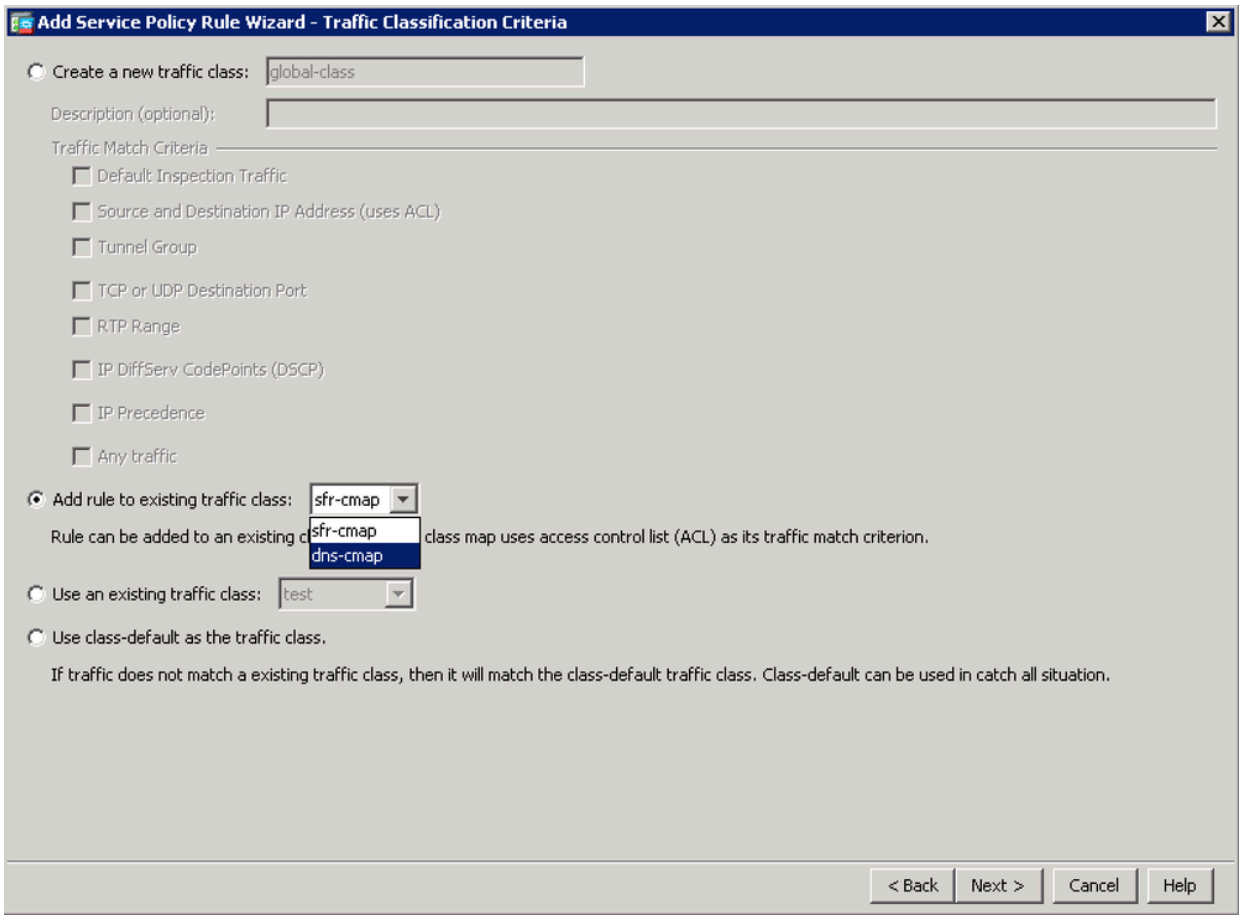
9. Schakel in het volgende venster het selectievakje voor 'DNS' in en klik op Voltooien.



10. De ASA toont nu het nieuwe Global-Policy voor 'dns-cmap'. Nu moet u het resterende verkeer configureren dat wordt geïnspecteerd door de ASA. Dit wordt gedaan door met de rechtermuisknop op 'dns-cmap' te klikken en de optie 'Insert After...' te selecteren, waarmee een nieuwe regel wordt gemaakt.

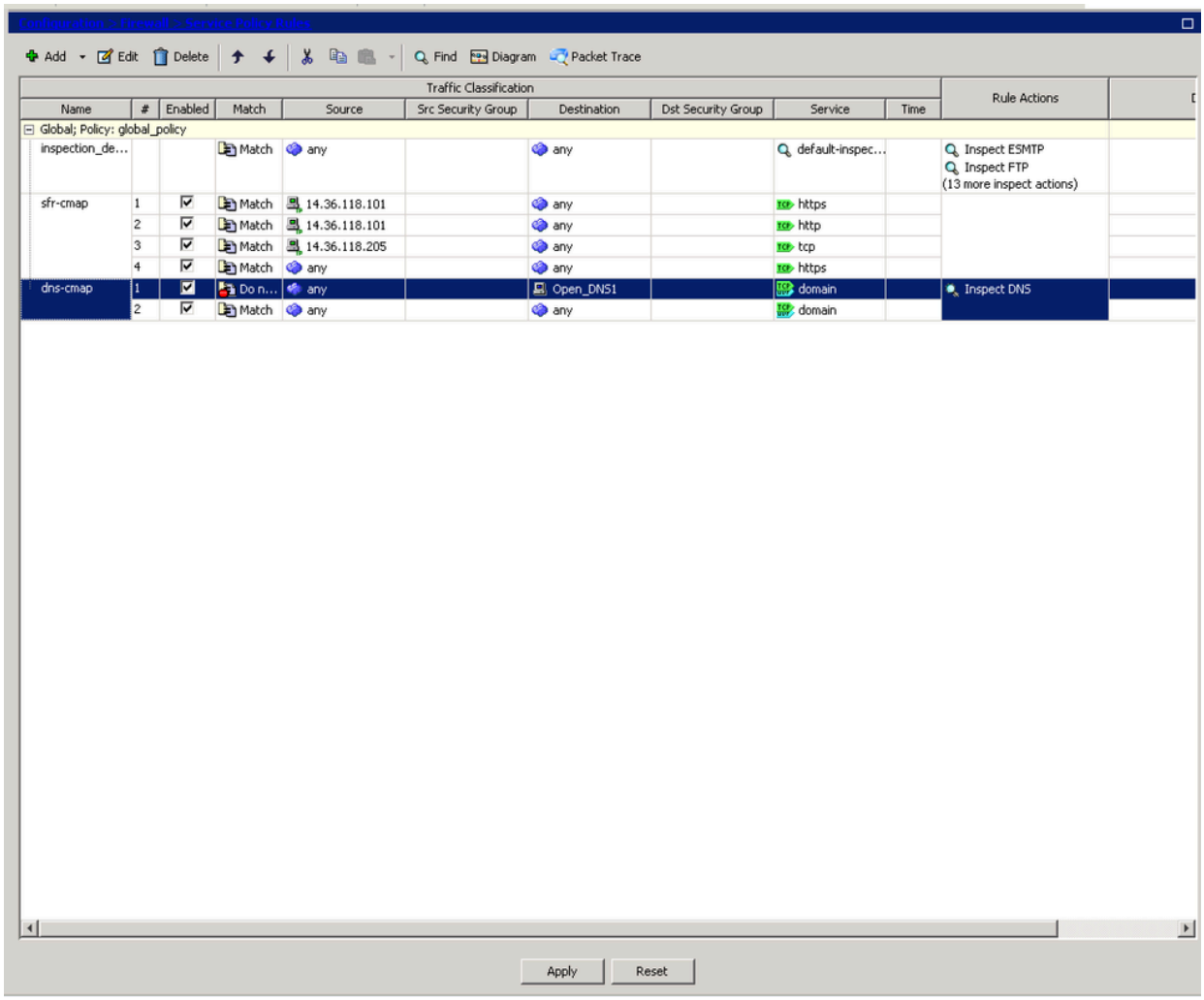


11. Klik in het eerste venster op Volgende en schakel vervolgens het keuzerondje "Regel toevoegen aan bestaande verkeersklasse:" in. Selecteer 'dns-cmap' in de vervolgkeuzelijst en klik vervolgens op Volgende.



12. Laat de actie achter als 'Match'. Kies de bron, bestemming en service van het verkeer dat onderworpen is aan DNS-inspectie. Hier vergelijken we bijvoorbeeld het verkeer van elke client die naar een TCP- of UDP DNS-server gaat. Klik op Next (Volgende).

13. Laat de optie 'DNS' ingeschakeld en klik op Voltooien.
14. Klik op Toepassen onderaan het venster.



Meer informatie

Als u DNScrypt liever uitschakelt dan ASA-vrijstellingen te configureren, neem dan contact op met Umbrella Support.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.