Solución de problemas de firewall ASA que bloquea la funcionalidad DNScyrpt desde el dispositivo virtual Umbrella

Contenido

Introducción

Overview

Causa

Resolución

- Excepciones de inspección de paquetes - Comandos IOS
- Excepciones de inspección de paquetes - Interfaz ASDM

Más información

Introducción

En este artículo se describe cómo solucionar problemas de firewall ASA que bloquean la funcionalidad DNScrypt.

Overview

El firewall Cisco ASA puede bloquear la funcionalidad DNScrypt que ofrece el dispositivo virtual Umbrella. Esto da como resultado esta advertencia del Panel de Umbrella:

> 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

Estos mensajes de error también se pueden ver en los registros del firewall ASA:

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

El cifrado DNSCrypt está diseñado para proteger el contenido de las consultas DNS y, como tal, también impide que los firewalls realicen la inspección de paquetes.

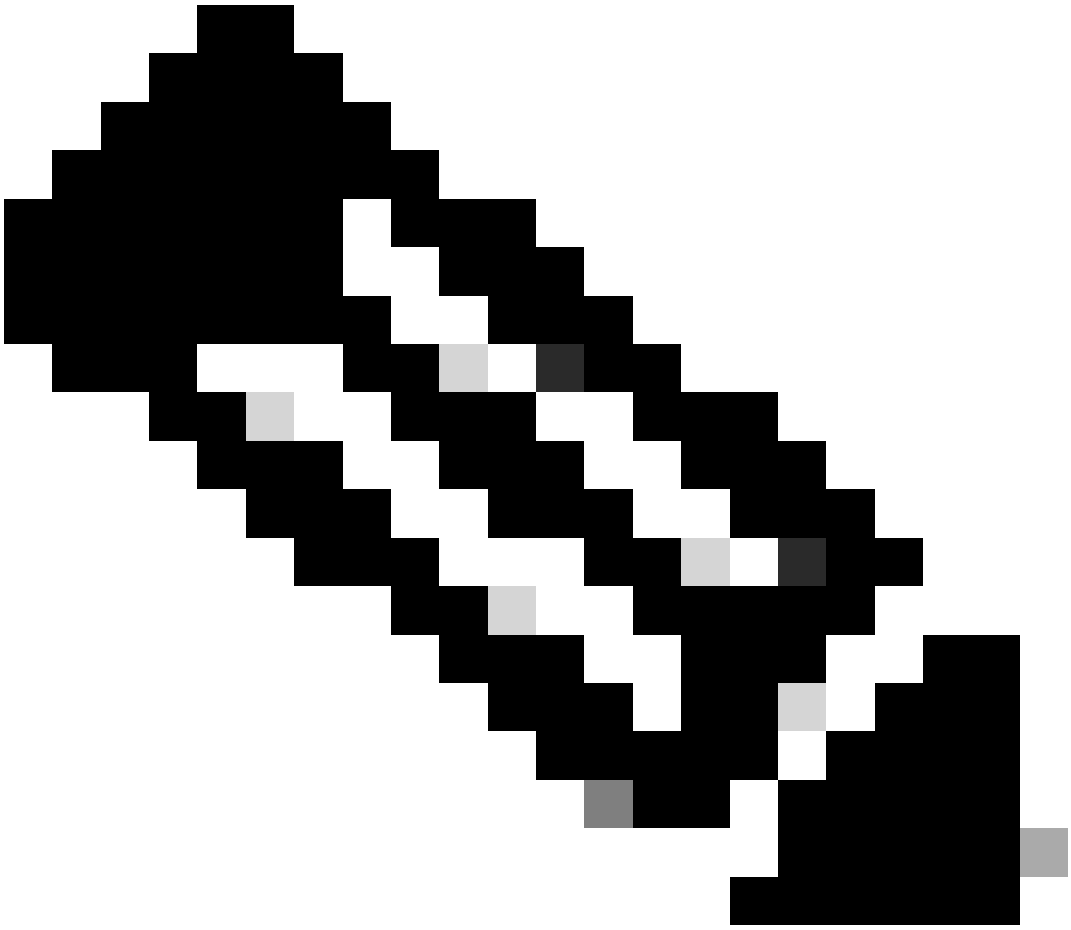
Causa

Estos errores no deben causar ningún impacto en los usuarios con la resolución de DNS.

El dispositivo virtual envía consultas de prueba para determinar la disponibilidad de DNScrypt y son esas consultas de prueba las que se bloquean. Sin embargo, estos mensajes de error indican que el dispositivo virtual no agrega seguridad adicional mediante el cifrado del tráfico DNS de su empresa.

Resolución

Se recomienda deshabilitar la inspección de paquetes DNS para el tráfico entre el dispositivo virtual y los resolvers DNS de Umbrella. Aunque esto inhabilita el registro y la inspección de protocolo en el ASA, mejora la seguridad al permitir el cifrado DNS.



Nota: Estos comandos se proporcionan solo como guía y se recomienda consultar a un experto de Cisco antes de realizar cambios en un entorno de producción.
También tenga en cuenta este defecto en ASA puede afectar a DNS sobre TCP, lo que también puede causar problemas con DNSCrypt:
CSCsm90809 Compatibilidad con inspección de DNS para DNS sobre TCP

Excepciones de inspección de paquetes - Comandos IOS

1. Cree una nueva ACL llamada 'dns_inspect' con reglas para negar el tráfico a 208.67.222.222 y 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. Elimine la política de inspección de DNS actual en el ASA. Por ejemplo:

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

3. Cree un mapa de clase que coincida con la ACL creada en el Paso #1:

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

4. Configure un policy-map bajo global_policy. Debe coincidir con el mapa de clase creado en el paso #3. Active la inspección de DNS.

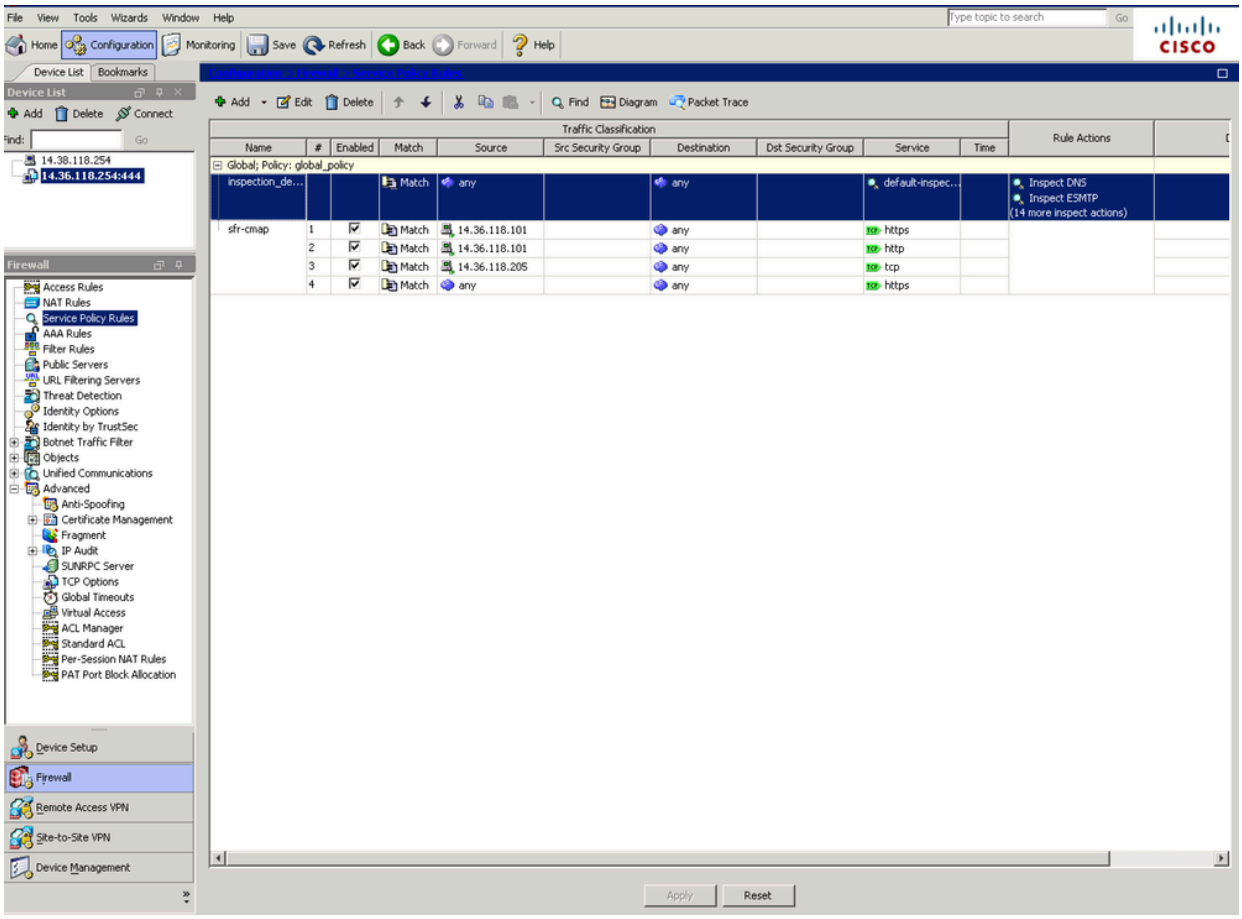
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. Una vez habilitada, puede verificar que el tráfico está alcanzando las exclusiones ejecutando:

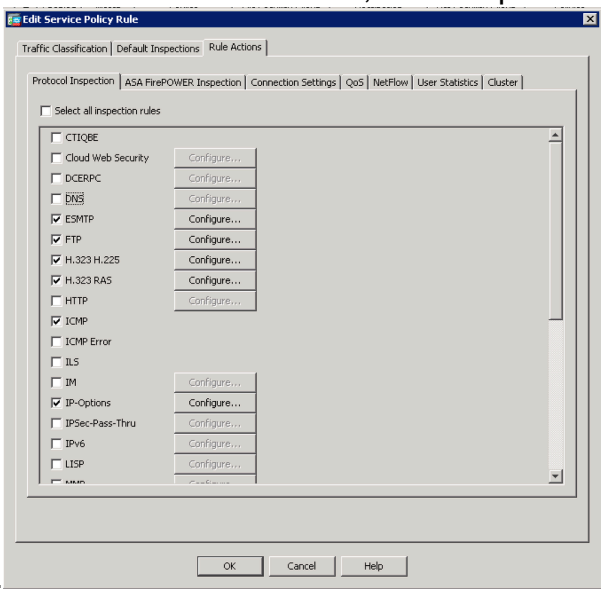
```
sh access-list dns_inspect
```

Excepciones de inspección de paquetes - Interfaz ASDM

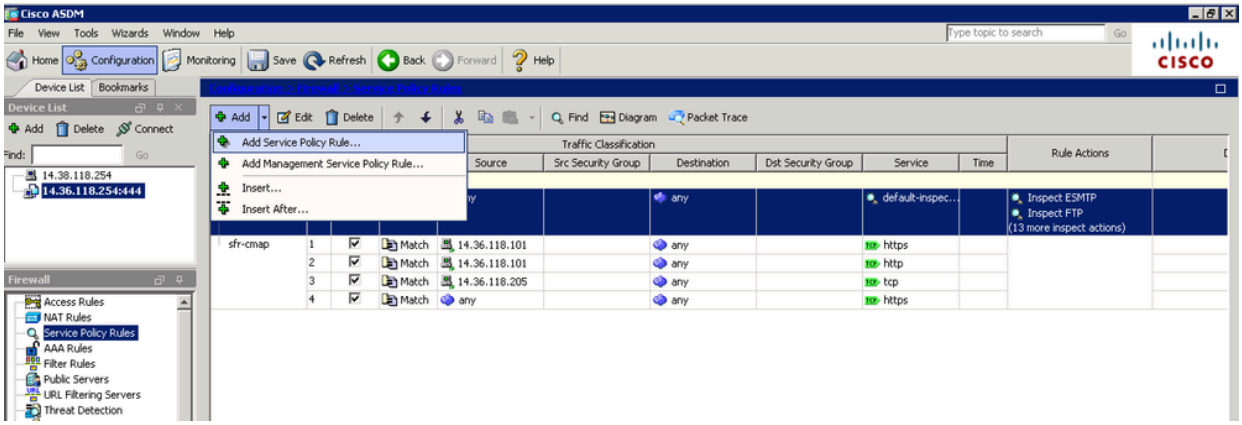
1. Deshabilite primero cualquier inspección de paquetes DNS si corresponde. Esto se hace en Configuration > Firewall > Service Policy Rules.



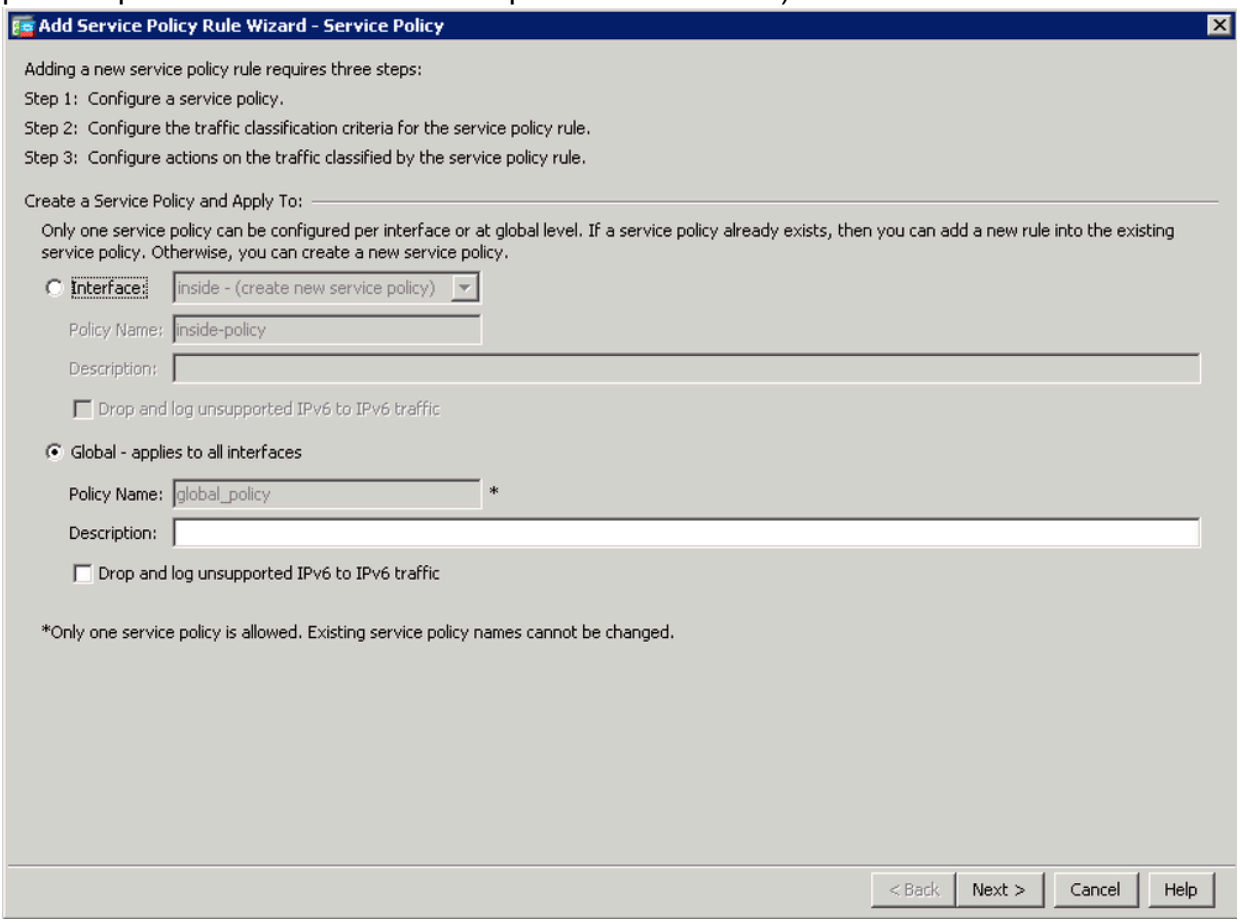
2. En el ejemplo, la inspección de DNS se habilita en la clase de política global e 'inspection_default'. Resáltela y haga clic en Edit. En la nueva ventana, desmarque la casilla de 'DNS' en la ficha "Acción de regla".



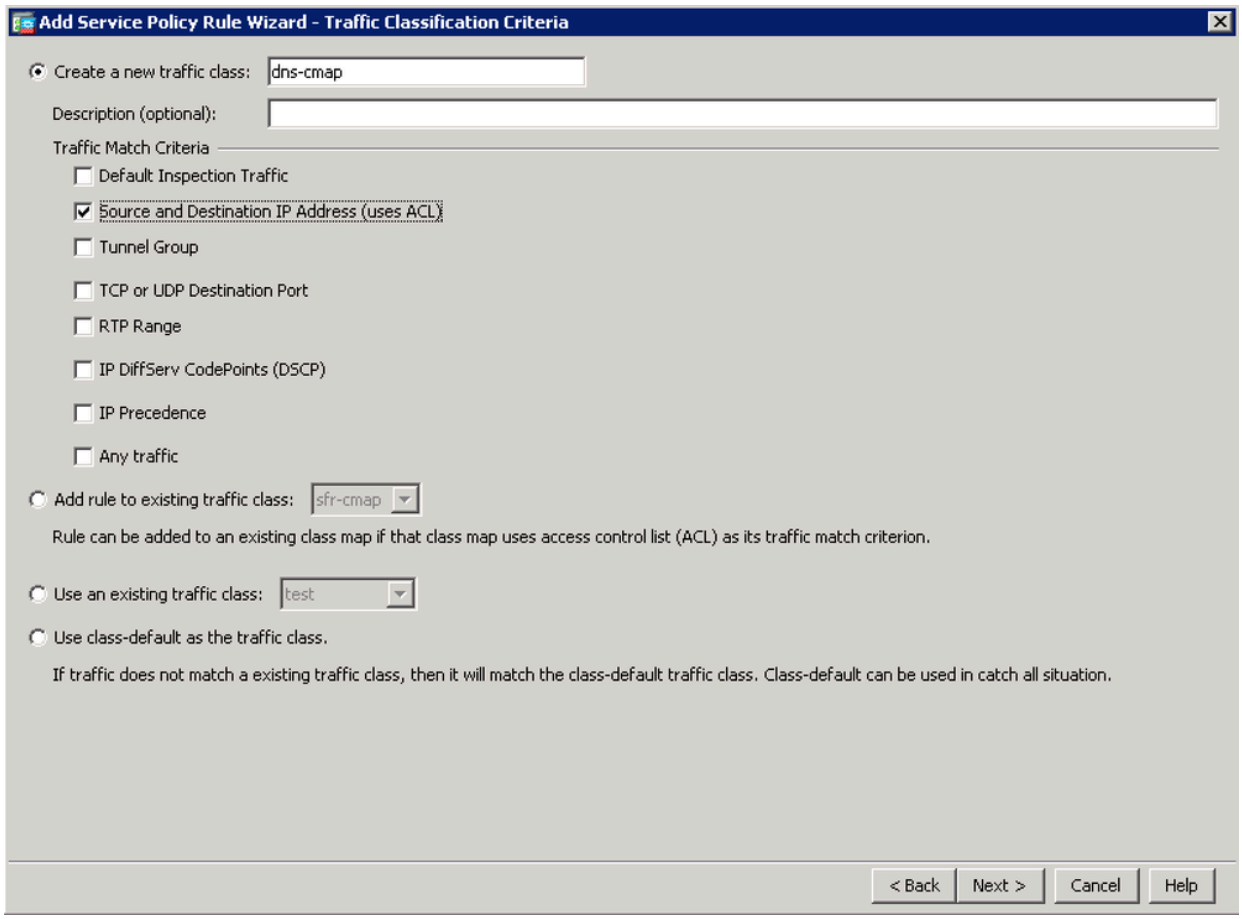
3. Ahora puede volver a configurar la inspección de DNS, esta vez con exenciones de tráfico adicionales. Haga clic en Add > Add Service Policy Rule...



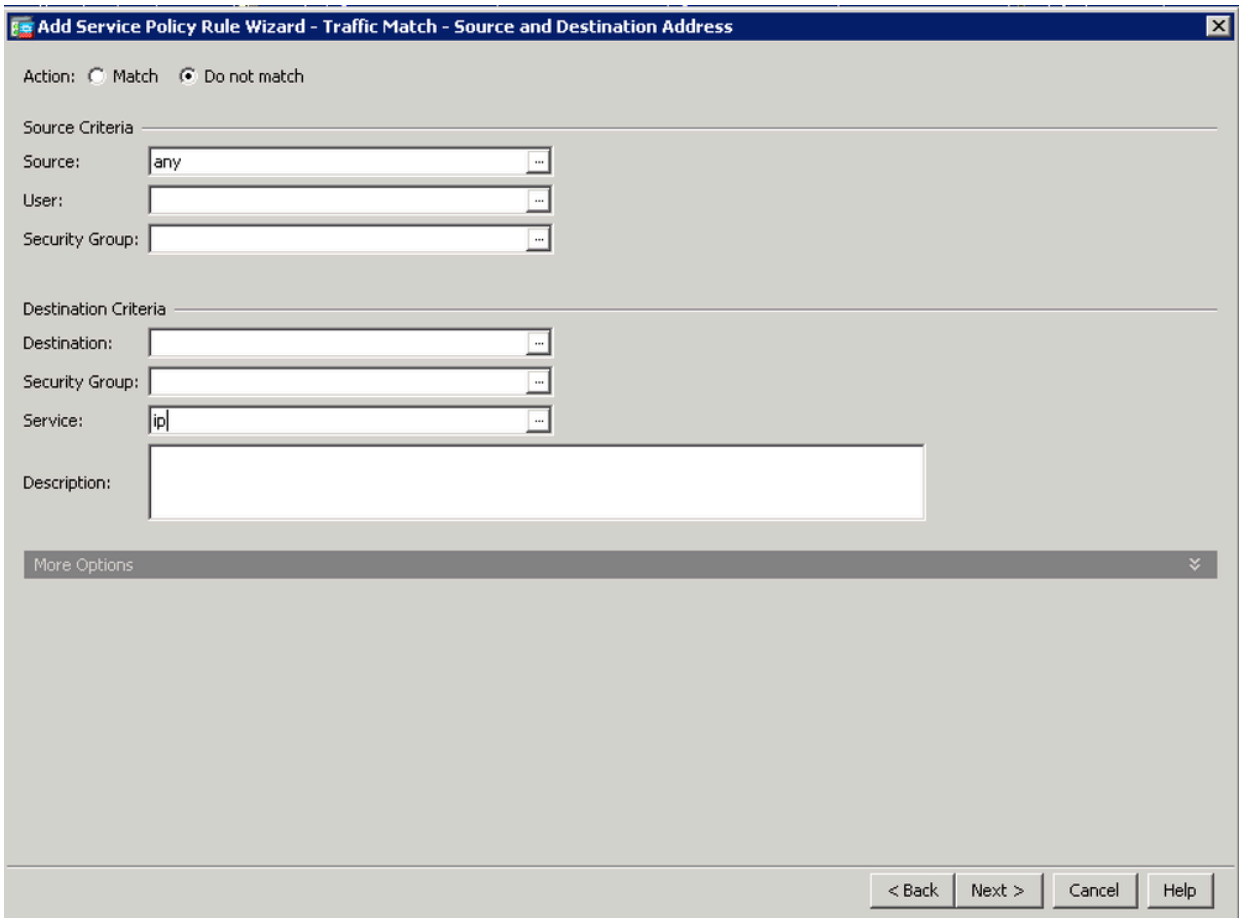
4. Seleccione "Global - Se aplica a todas las interfaces" y haga clic en Next (también puede aplicar esto a una interfaz específica si lo desea).



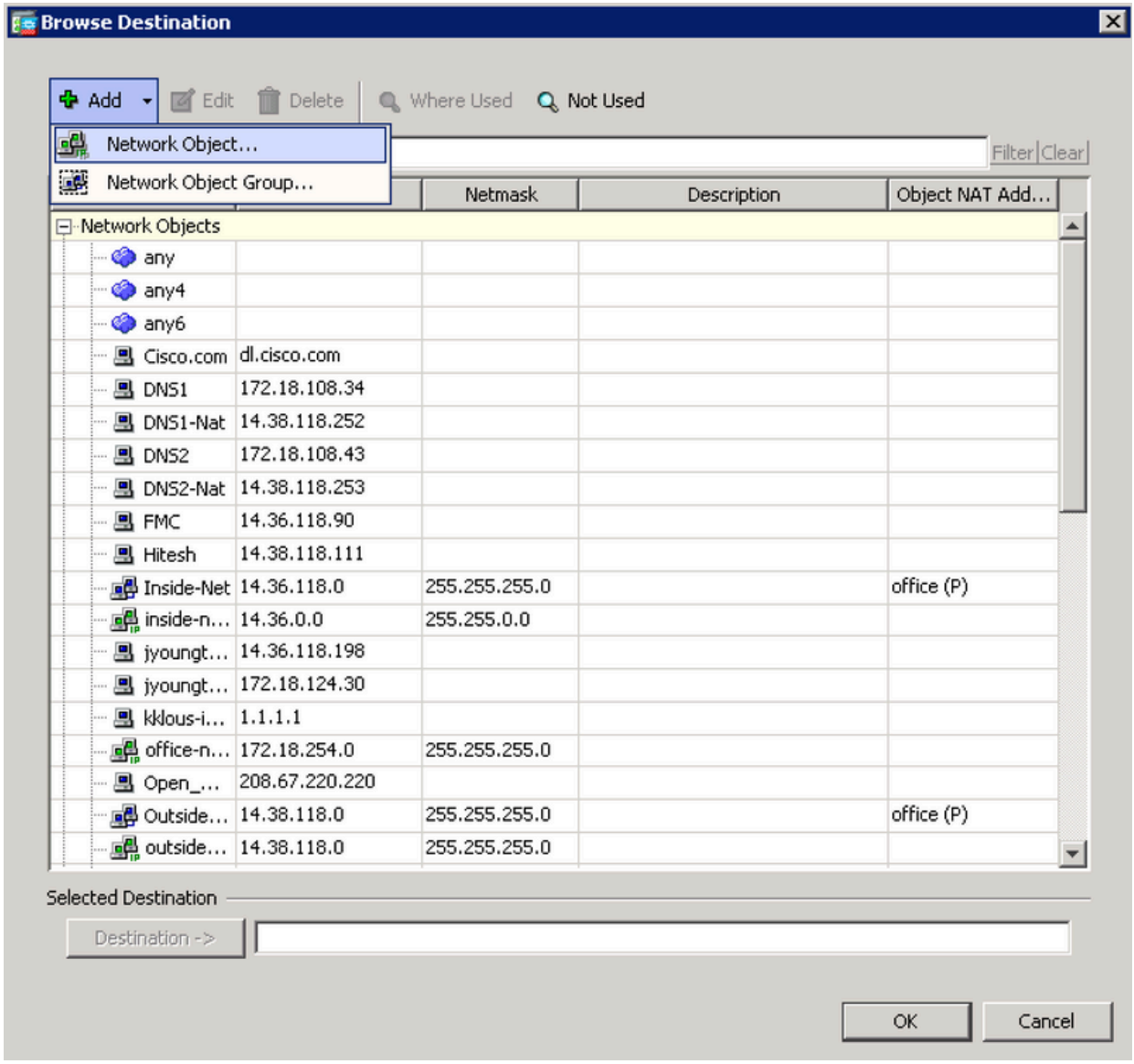
5. Asigne un nombre al mapa de clase (por ejemplo, 'dns-cmap') y active la opción "Dirección IP de origen y destino (utiliza ACL)". Haga clic en Next (Siguiente).

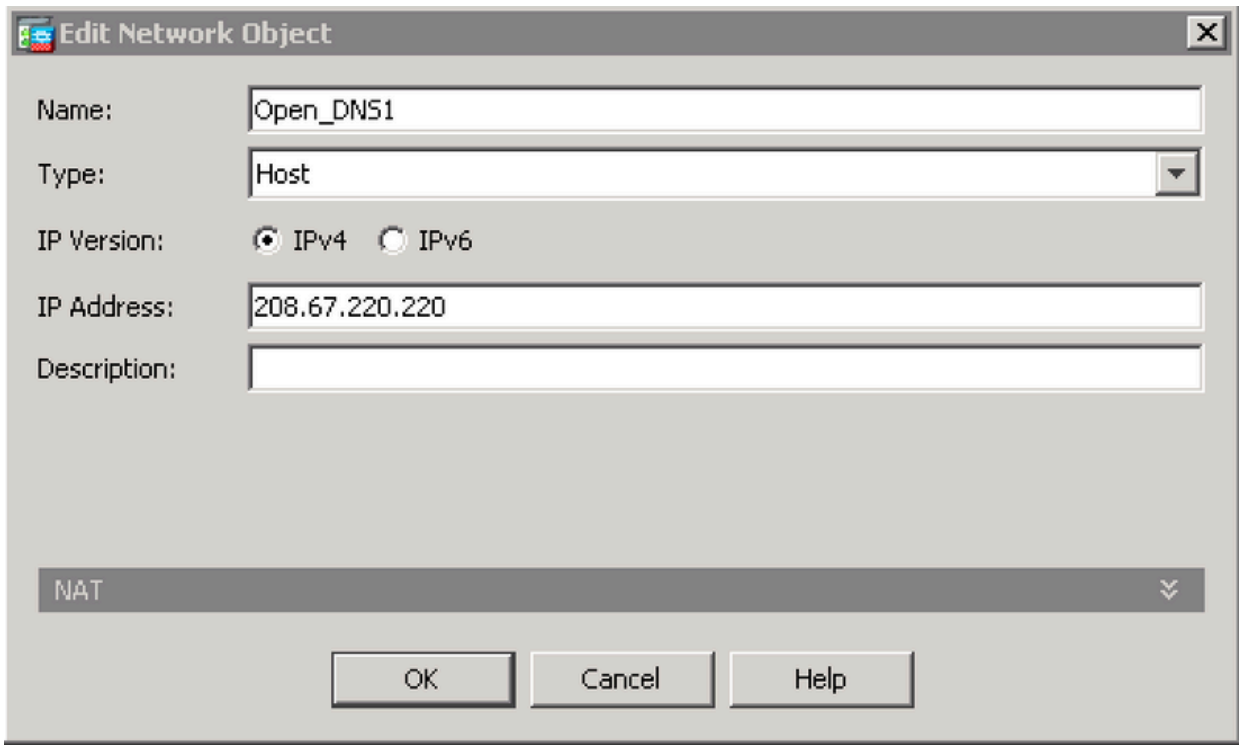


6. Comience por configurar el tráfico que no desea que se inspeccione mediante la acción "No coincidir".
   Para Source, puede utilizar la opción 'any' para eximir todo el tráfico destinado a los servidores DNS de Umbrella. También puede crear aquí una definición de objeto de red para eximir únicamente la dirección IP específica del dispositivo virtual.

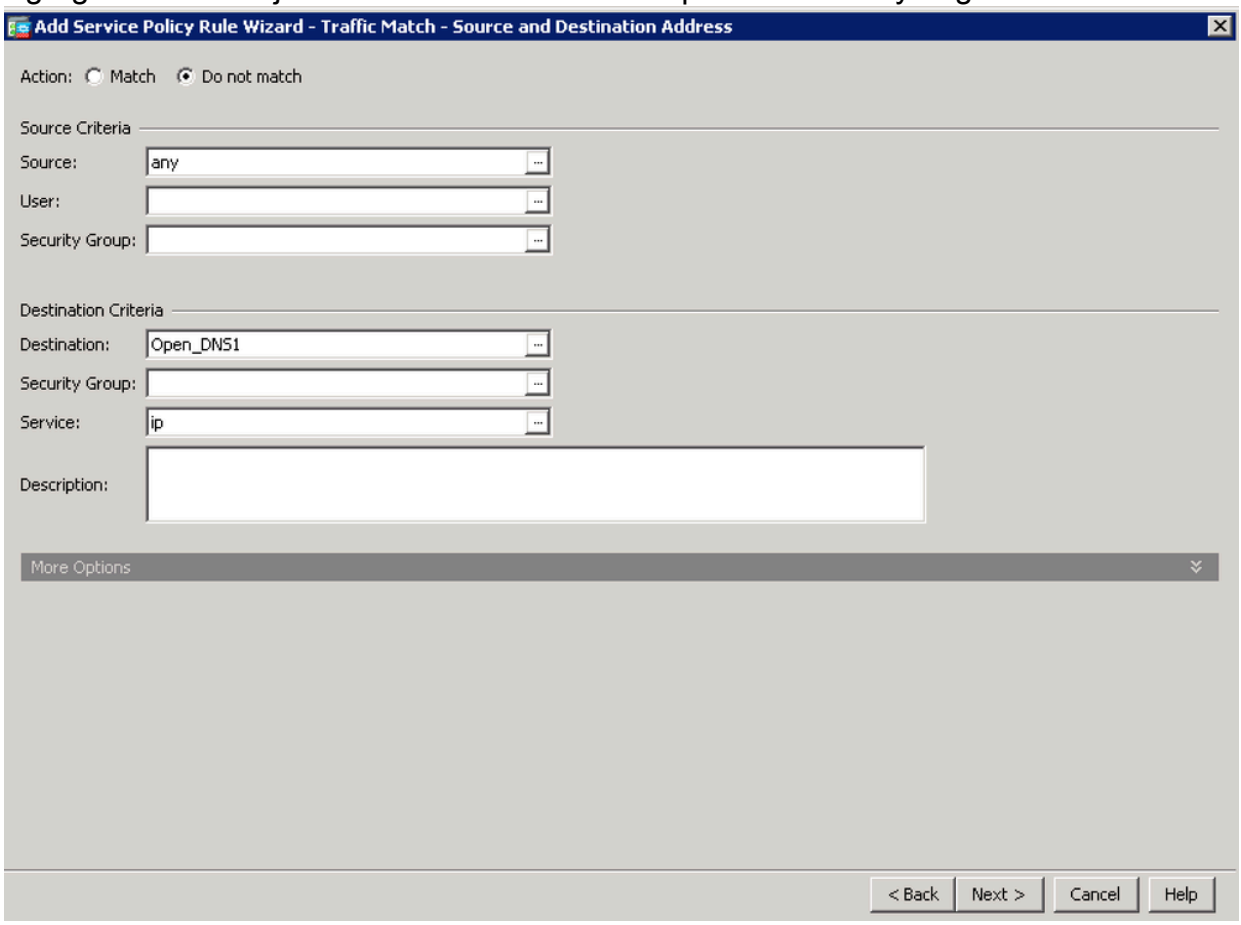


7. Haga clic en ... en el campo Destino. En la siguiente ventana, haga clic en Add > Network Object y cree un objeto con la dirección IP '208.67.222.222'. Repita este paso para crear un objeto con la dirección IP '208.67.220.220'.

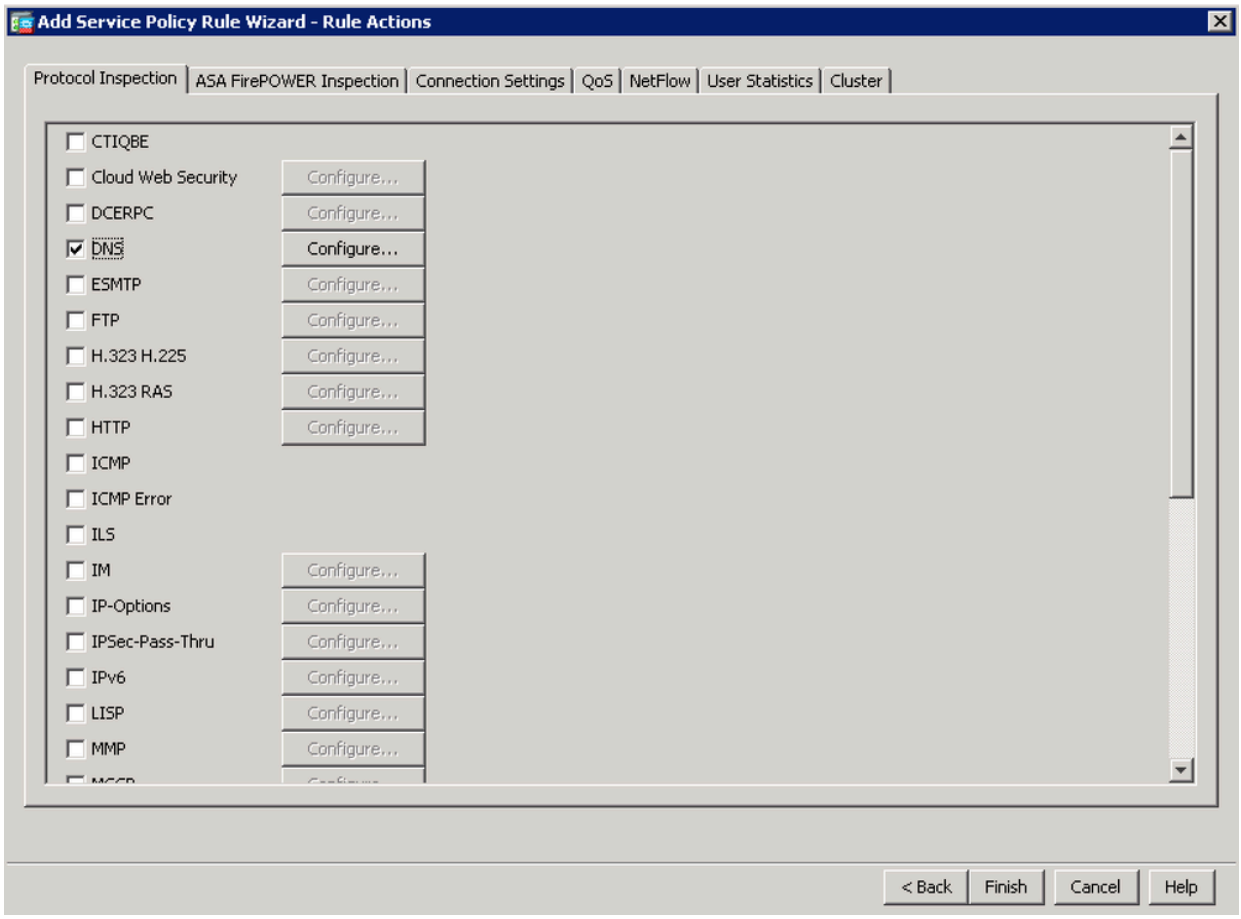

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

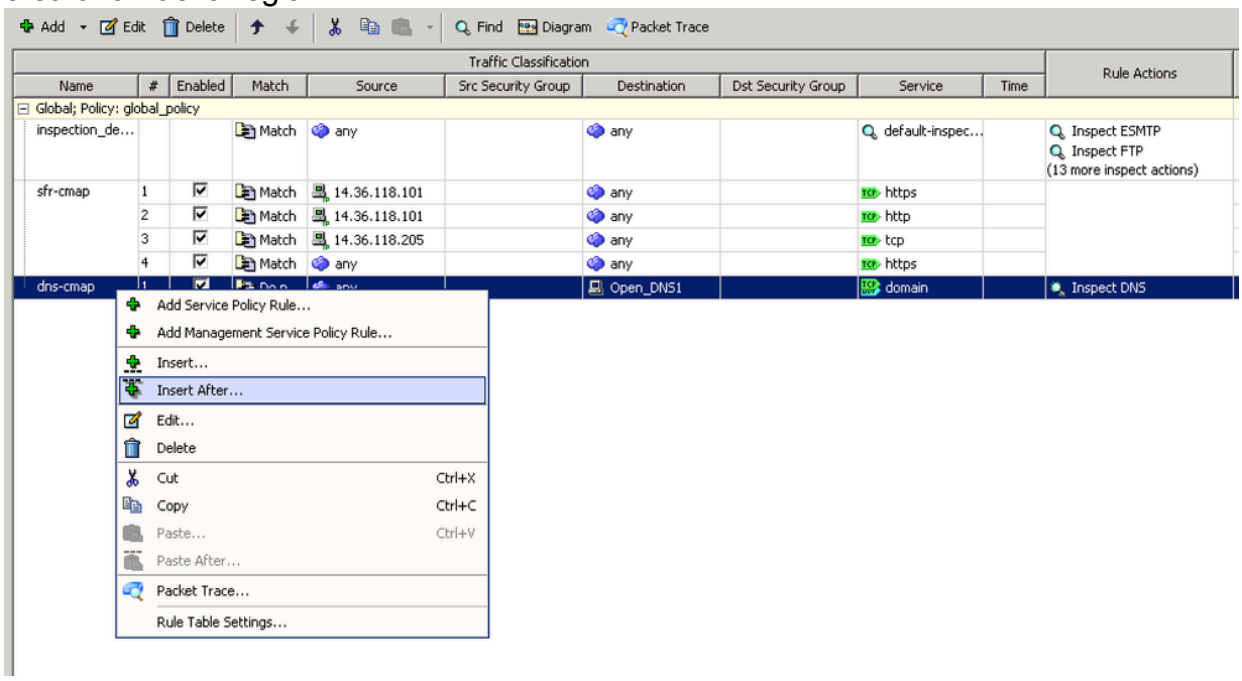
8. Agregue ambos objetos de red Umbrella al campo Destination y haga clic en OK.



9. En la siguiente ventana, marque la casilla de 'DNS' y haga clic en Finish.

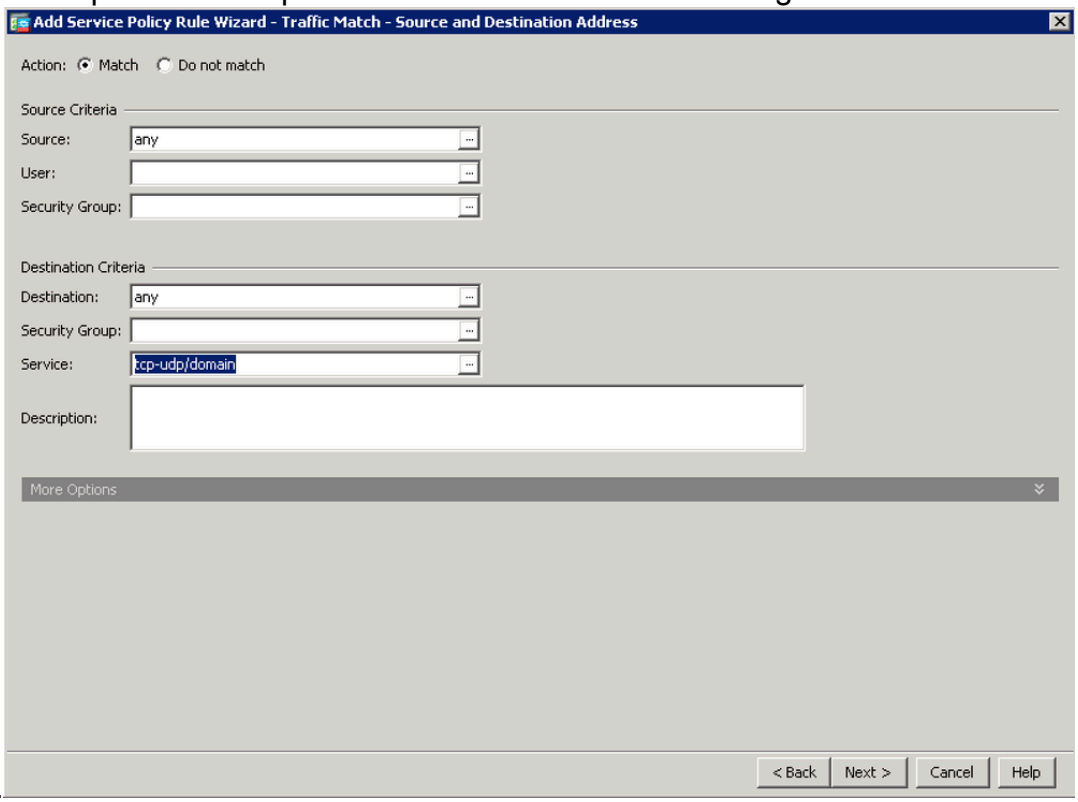


10. ASA ahora muestra la nueva política global para 'dns-cmap'. Ahora necesita configurar el tráfico restante que inspecciona el ASA. Esto se hace haciendo clic con el botón derecho del ratón en 'dns-cmap' y seleccionando la opción "Insertar después..." que crea una nueva regla.

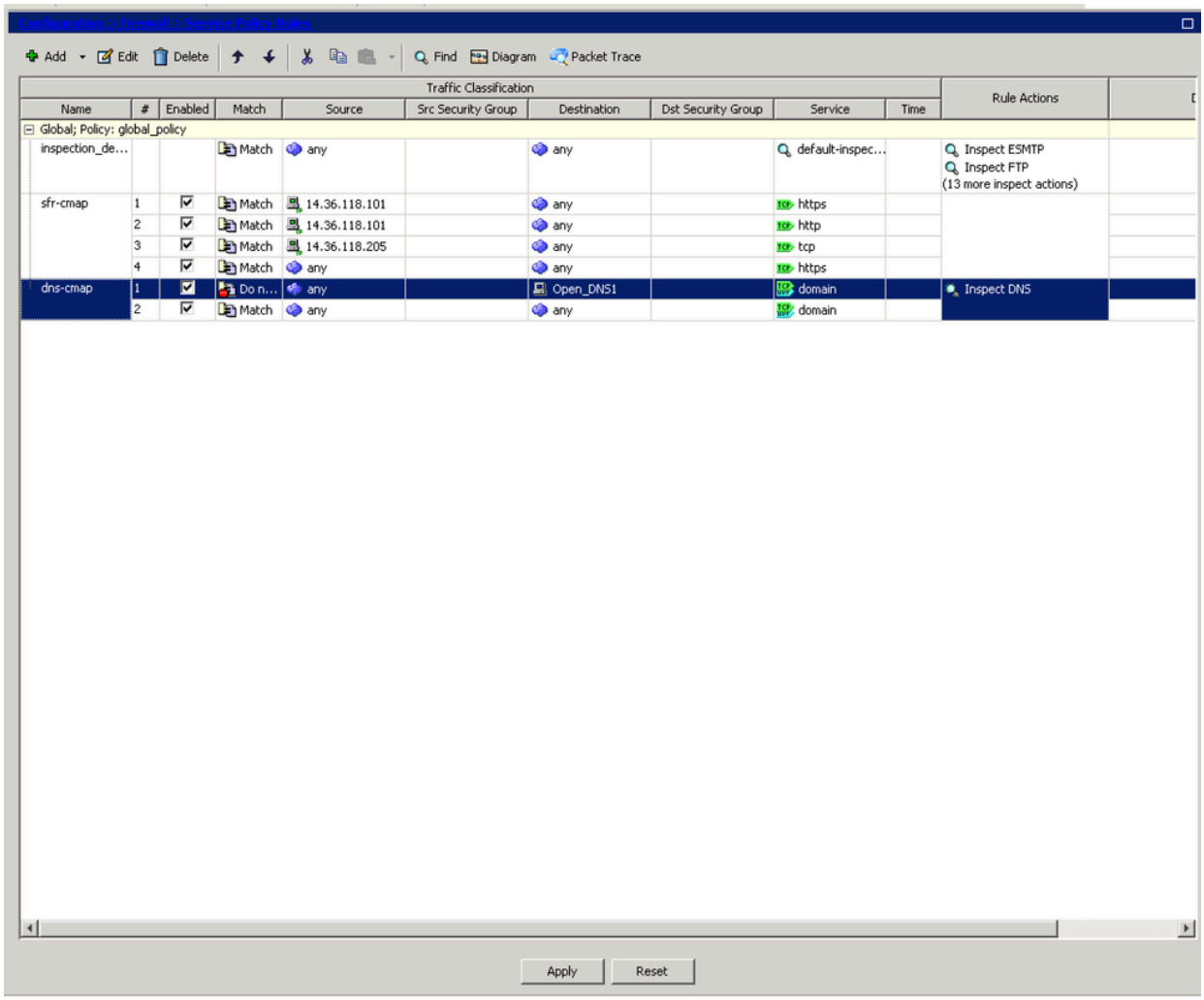


11. En la primera ventana, haga clic en Next y, a continuación, marque el botón de opción "Add rule to existing traffic class:" (Agregar regla a clase de tráfico existente). Seleccione 'dns-cmap' en el menú desplegable y, a continuación, haga clic en Next.

12. Deje la acción como 'Coincidir'. Elija el origen, el destino y el servicio del tráfico que está sujeto a la inspección de DNS. Aquí, por ejemplo, coincidimos el tráfico de cualquier cliente que va a cualquier servidor DNS TCP o UDP. Haga clic en Next (Siguiente).



13. Deje la opción 'DNS' marcada y haga clic en Finish.
14. Haga clic en Apply en la parte inferior de la ventana.



Más información

Si prefiere inhabilitar DNScrypt en lugar de configurar las exenciones de ASA, comuníquese con el soporte técnico de Umbrella.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).