Dépannage du pare-feu ASA bloquant la fonctionnalité de chiffrement DNS à partir de l'appliance virtuelle Umbrella

Table des matières

Introduction

Cet article décrit comment dépanner le pare-feu ASA bloquant la fonctionnalité DNScrypt.

Aperçu

Le pare-feu Cisco ASA peut bloquer la fonctionnalité DNScrypt offerte par l'appareil virtuel Umbrella. Cela entraîne cet avertissement de tableau de bord de parapluie :

> 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

Ces messages d'erreur peuvent également être vus dans les journaux du pare-feu ASA :

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

Le cryptage DNSCrypt est conçu pour protéger le contenu de vos requêtes DNS et, en tant que tel, empêche également les pare-feu d'effectuer l'inspection des paquets.

Motif

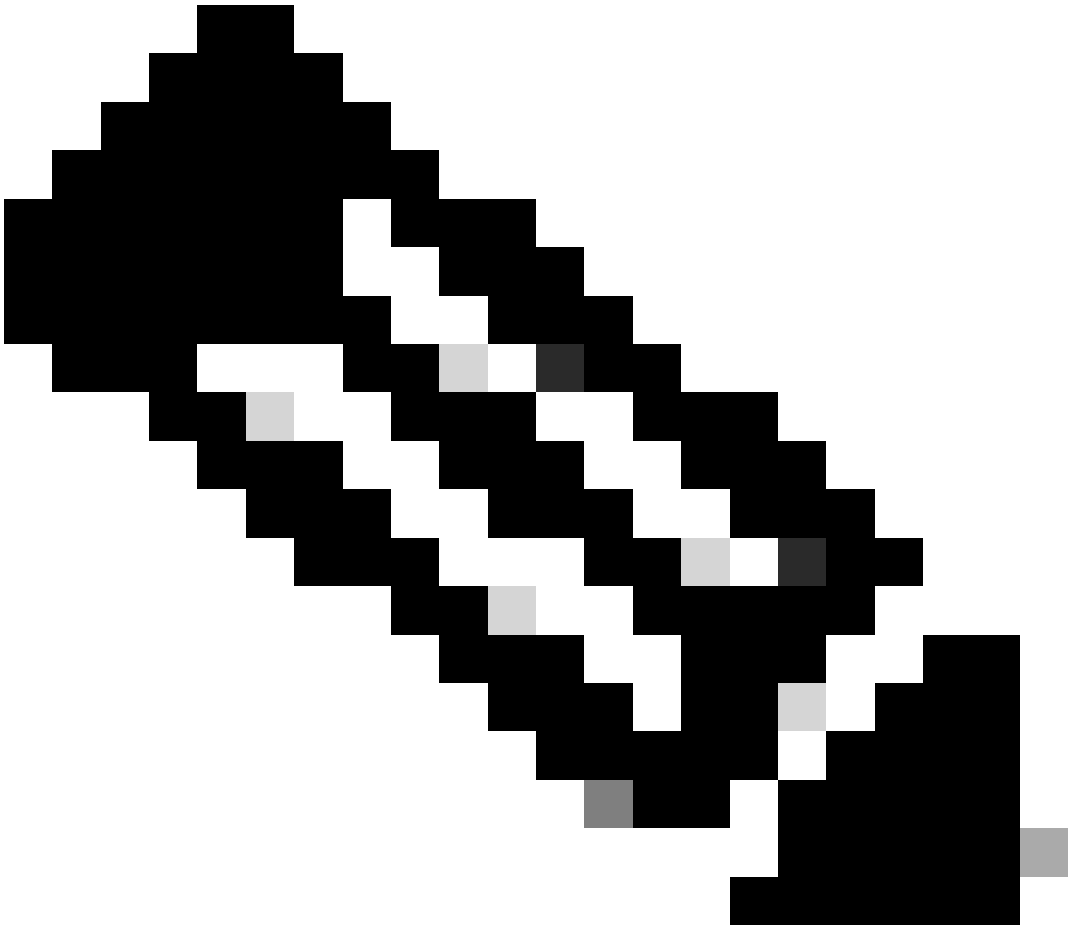
Ces erreurs ne doivent pas avoir d'impact sur la résolution DNS pour les utilisateurs.

L'appliance virtuelle envoie des requêtes de test pour déterminer la disponibilité de DNScrypt et ce

sont ces requêtes de test qui sont bloquées. Cependant, ces messages d'erreur indiquent que l'appliance virtuelle n'ajoute pas de sécurité supplémentaire en chiffrant le trafic DNS de votre entreprise.

Résolution

Nous vous recommandons de désactiver l'inspection des paquets DNS pour le trafic entre l'appliance virtuelle et les résolveurs DNS d'Umbrella. Bien que cela désactive la journalisation et l'inspection de protocole sur l'ASA, cela améliore la sécurité en autorisant le chiffrement DNS.



Remarque : Ces commandes sont fournies à titre indicatif uniquement et il est recommandé de consulter un expert Cisco avant d'apporter des modifications à un environnement de production.
Notez également ce défaut sur ASA pourrait affecter DNS sur TCP, ce qui peut également entraîner des problèmes avec DNSCrypt :
CSCsm90809 Prise en charge de l'inspection DNS pour DNS sur TCP

Exceptions d'inspection des paquets - Commandes IOS

1. Créez une nouvelle liste de contrôle d'accès appelée « dns_inspect » avec des règles pour refuser le trafic vers 208.67.222.222 et 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. Supprimez la stratégie d'inspection DNS actuelle sur l'ASA. Exemple :

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

3. Créez une carte de classe correspondant à la liste de contrôle d'accès créée à l'étape #1 :

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

4. Configurez un policy-map sous global_policy. Cela doit correspondre à la carte de classe créée à l'étape #3. Activez l'inspection DNS.

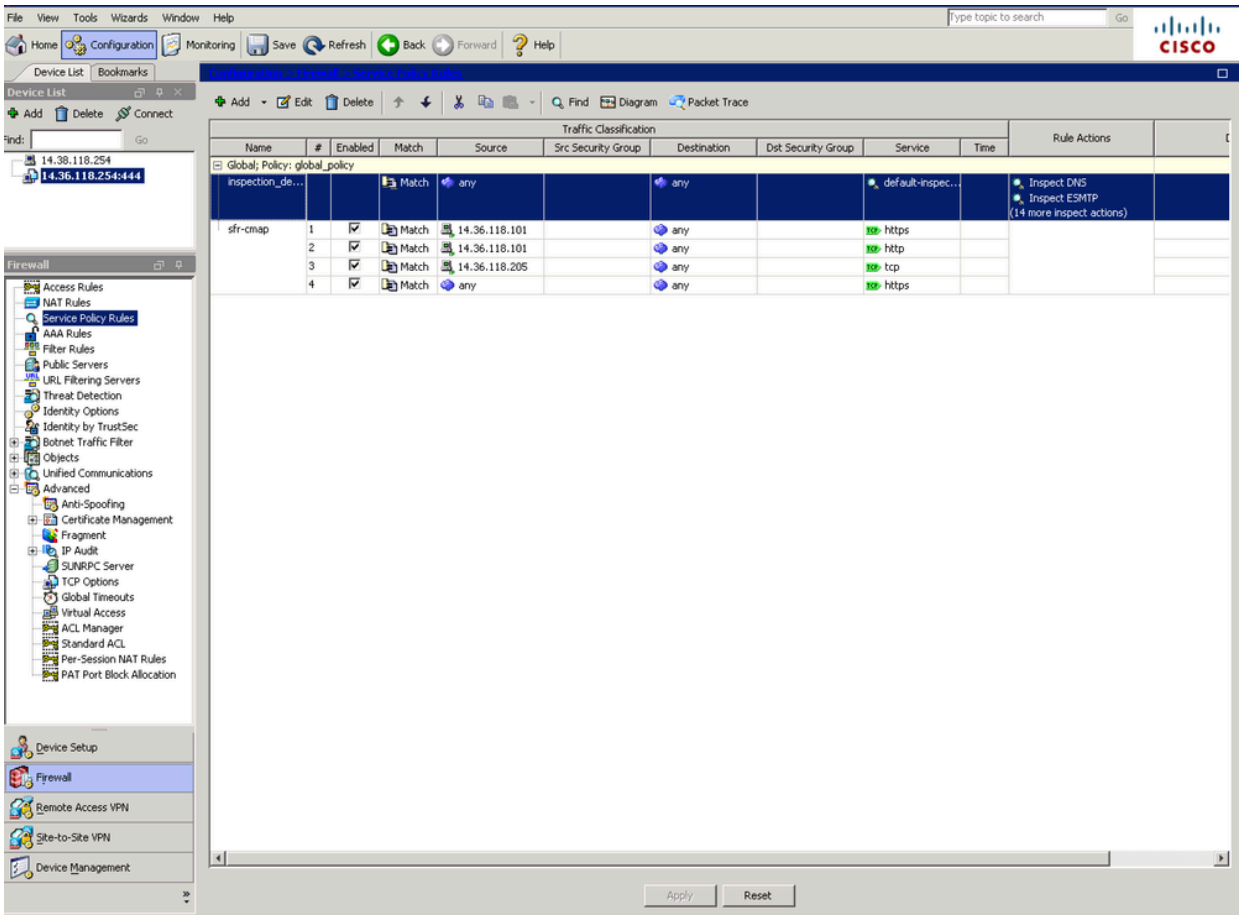
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. Une fois activé, vous pouvez vérifier que le trafic atteint les exclusions en exécutant :

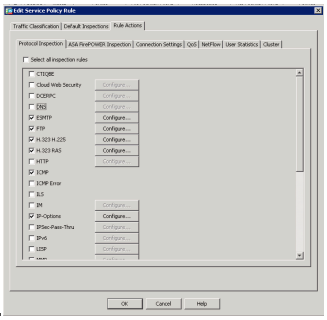
```
sh access-list dns_inspect
```

Exceptions d'inspection de paquet - Interface ASDM

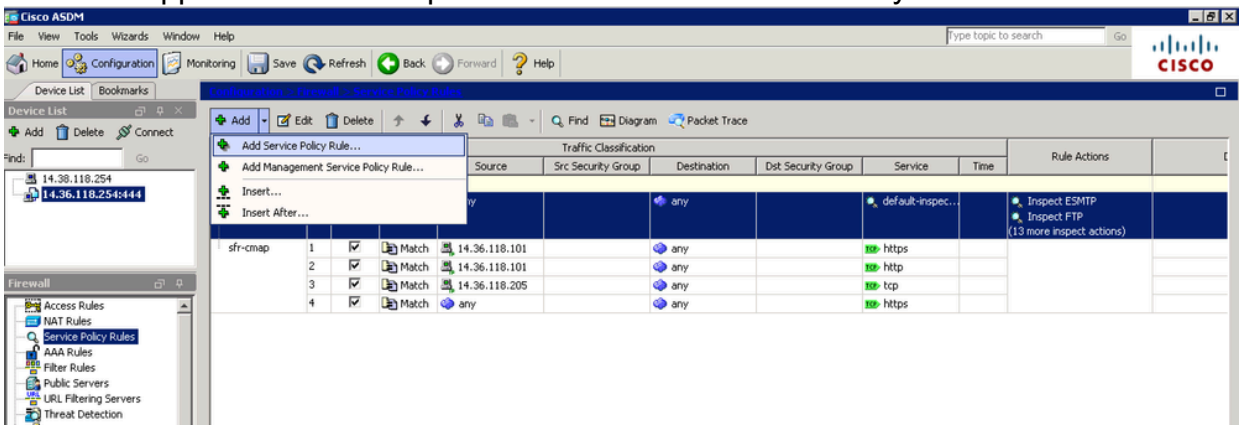
1. Commencez par désactiver toute inspection de paquet DNS, le cas échéant.Ceci est fait dans Configuration > Firewall > Service Policy Rules.



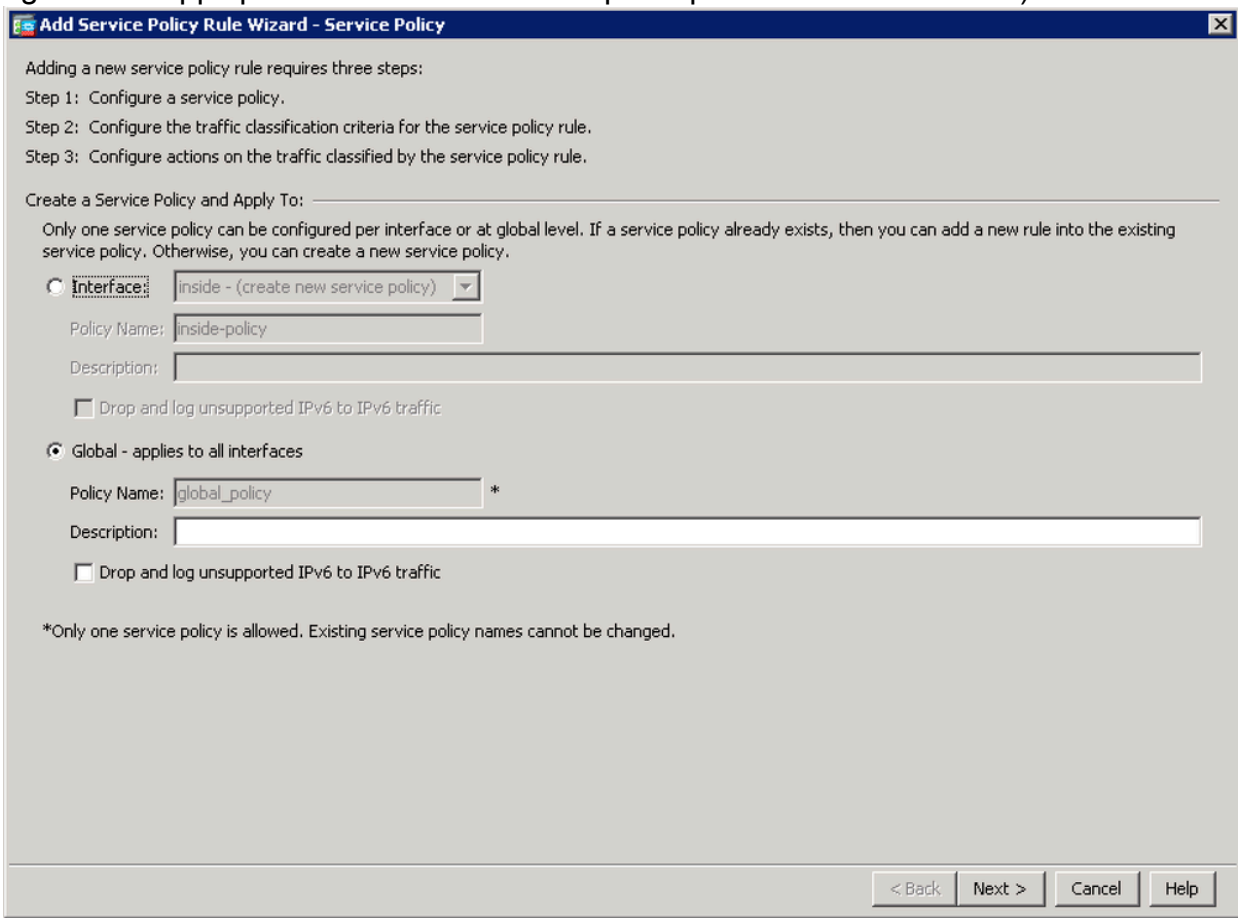
2. Dans l'exemple, l'inspection DNS est activée sous la politique globale et la classe « inspection_default ». Mettez-le en surbrillance et cliquez sur Edit. Dans la nouvelle fenêtre, décochez la case « DNS » sous l'onglet « Rule Action ».



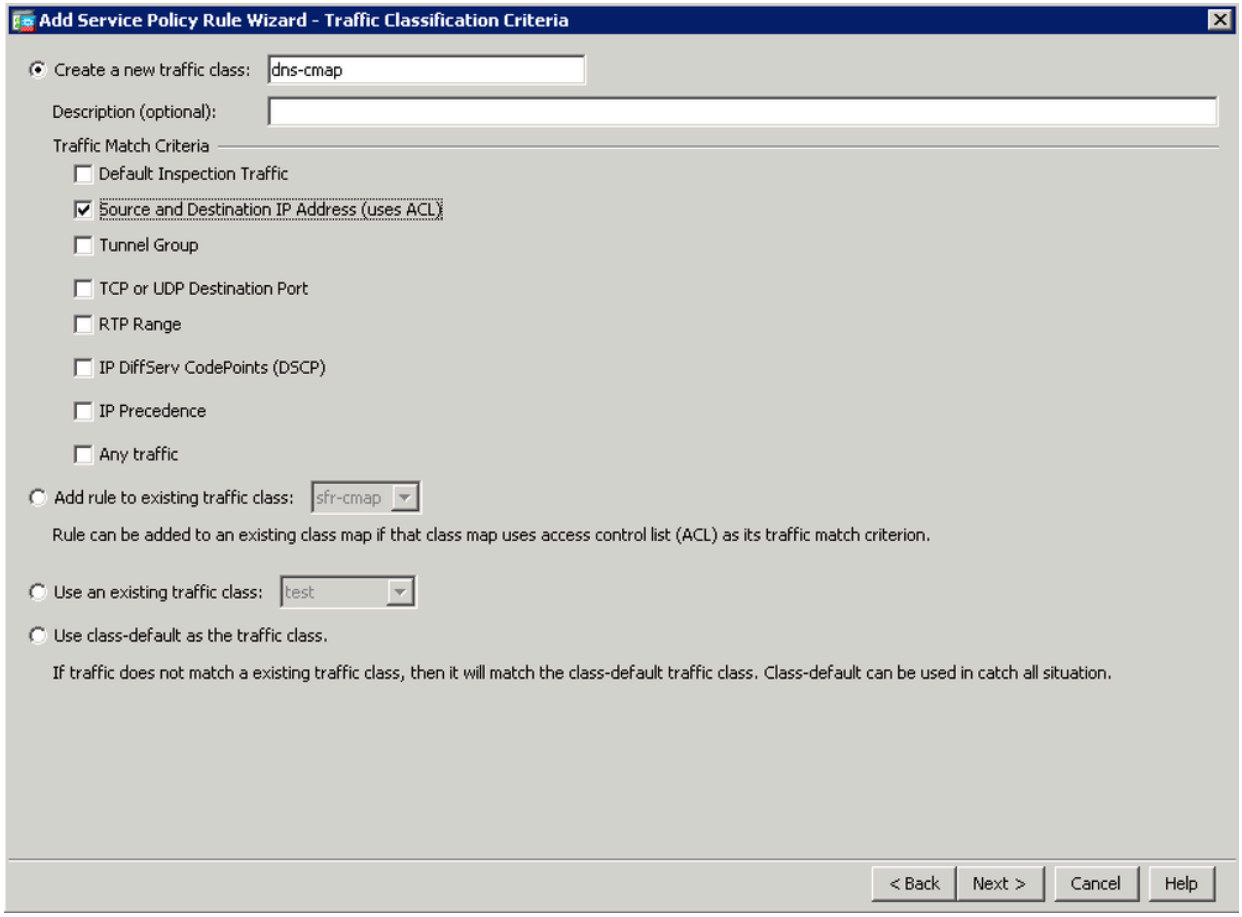
3. Vous pouvez maintenant reconfigurer l'inspection DNS, cette fois avec des exemptions de trafic supplémentaires. Cliquez sur Add > Add Service Policy Rule...



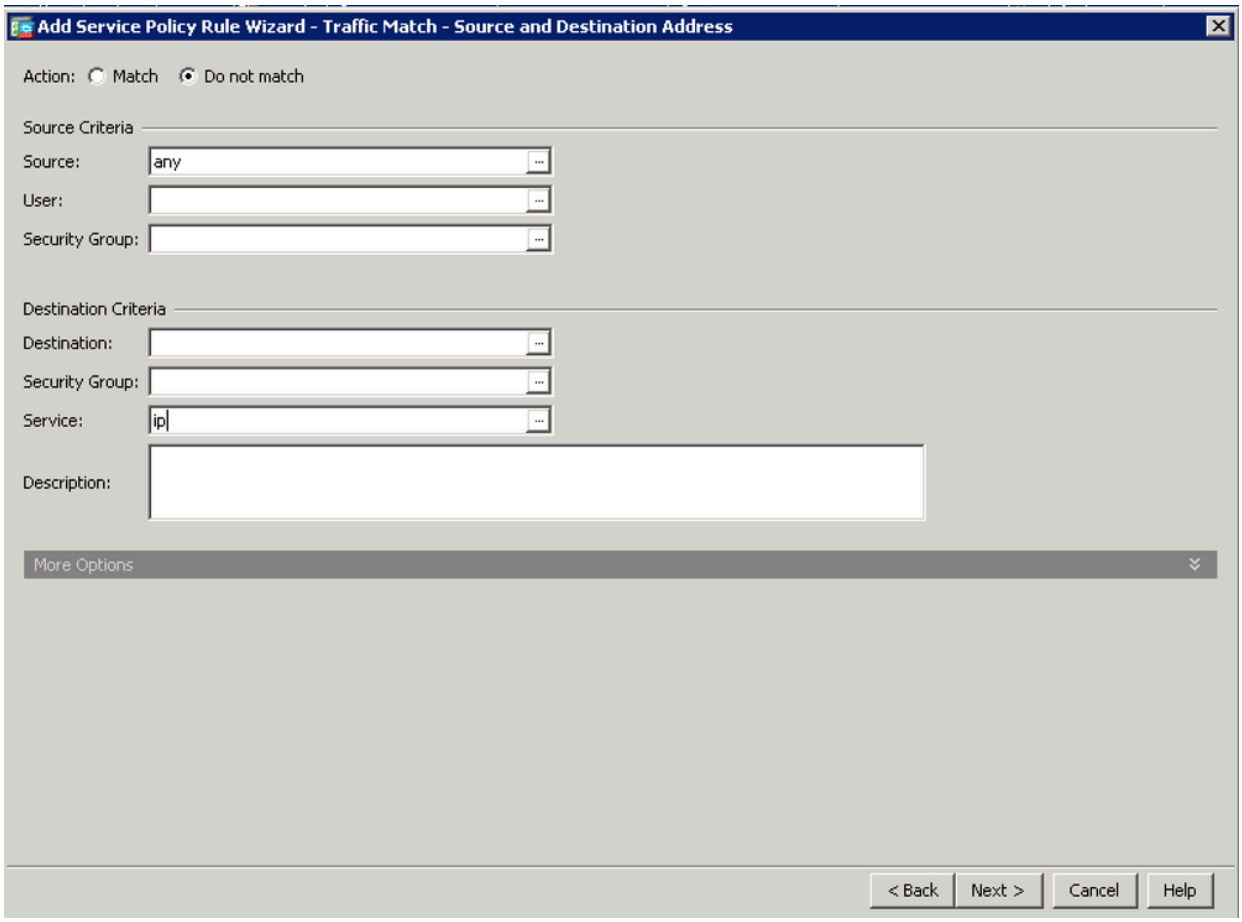
4. Sélectionnez "Global - Applies to all interfaces" et cliquez sur Next (vous pouvez également appliquer ceci à une interface spécifique si vous le souhaitez).



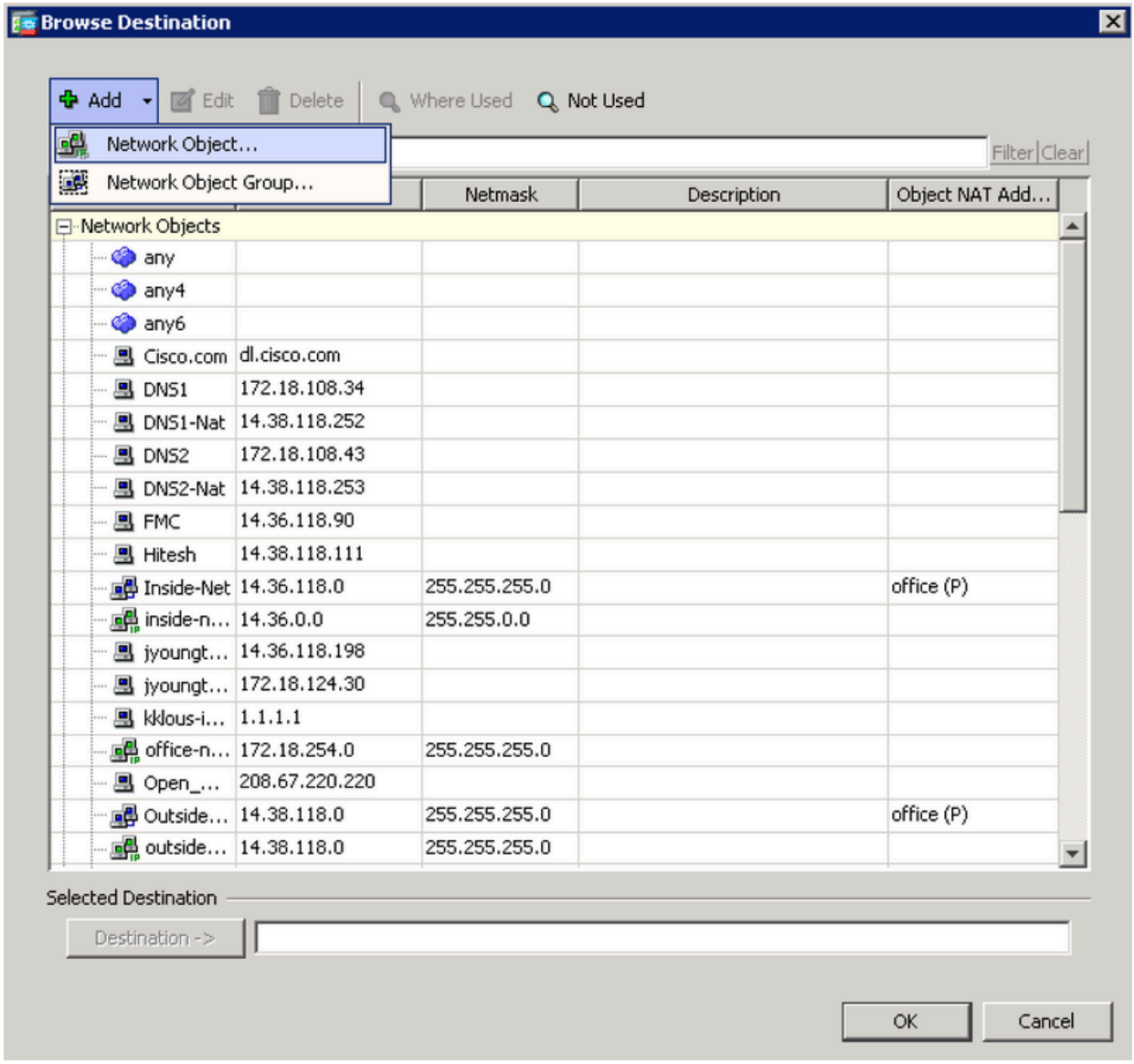
5. Attribuez un nom au class-map (par exemple 'dns-cmap') et cochez l'option "Adresse IP source et de destination (utilise ACL). Cliquez sur Suivant.

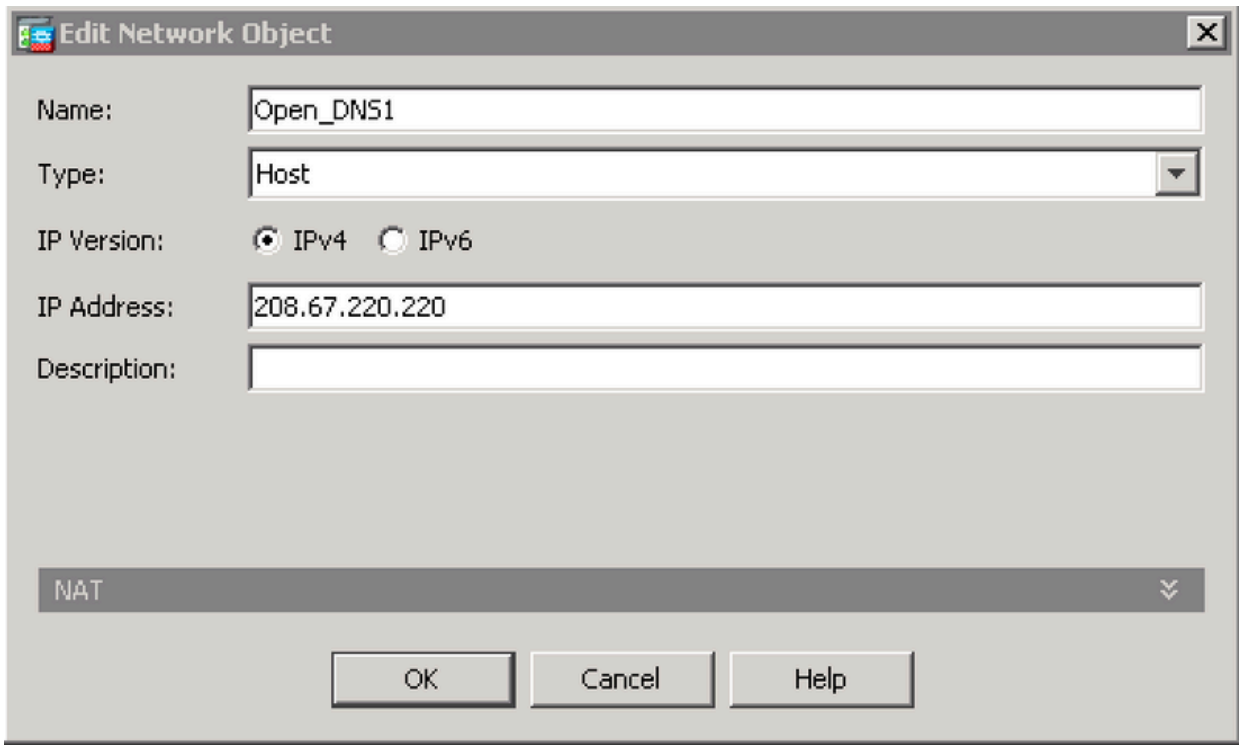


6. Commencez par configurer le trafic que vous ne souhaitez pas inspecter à l'aide de l'action « Ne pas correspondre ».
   Pour Source, vous pouvez utiliser l'option 'any' pour exempter tout le trafic destiné aux serveurs DNS d'Umbrella. Vous pouvez également créer une définition d'objet réseau ici pour exempter uniquement l'adresse IP spécifique de l'appliance virtuelle.

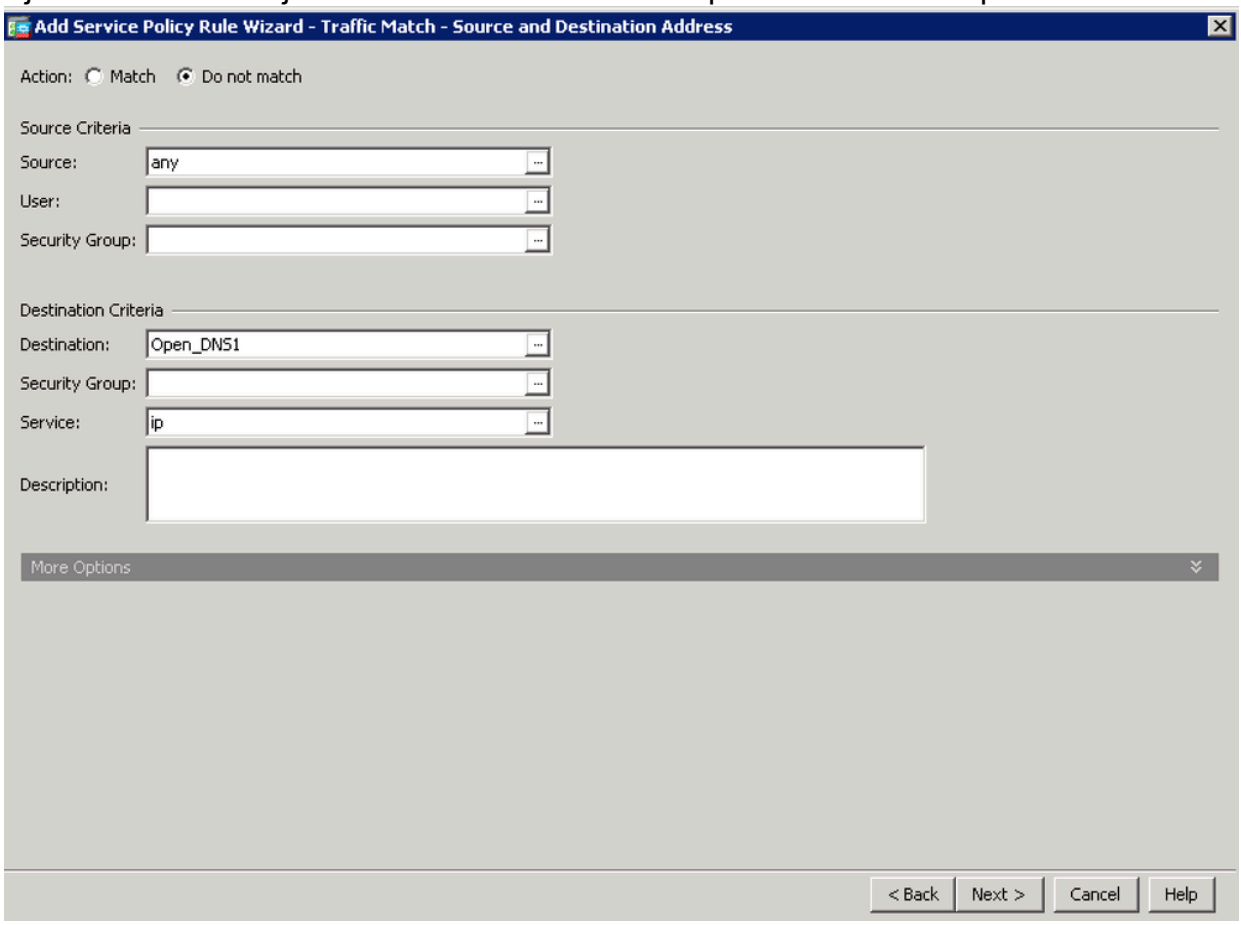


7. Cliquez sur ... dans le champ Destination. Dans la fenêtre suivante, cliquez sur Add > Network Object et créez un objet avec l'adresse IP '208.67.222.222'. Répétez cette étape pour créer un objet avec l'adresse IP « 208.67.220.220 ».

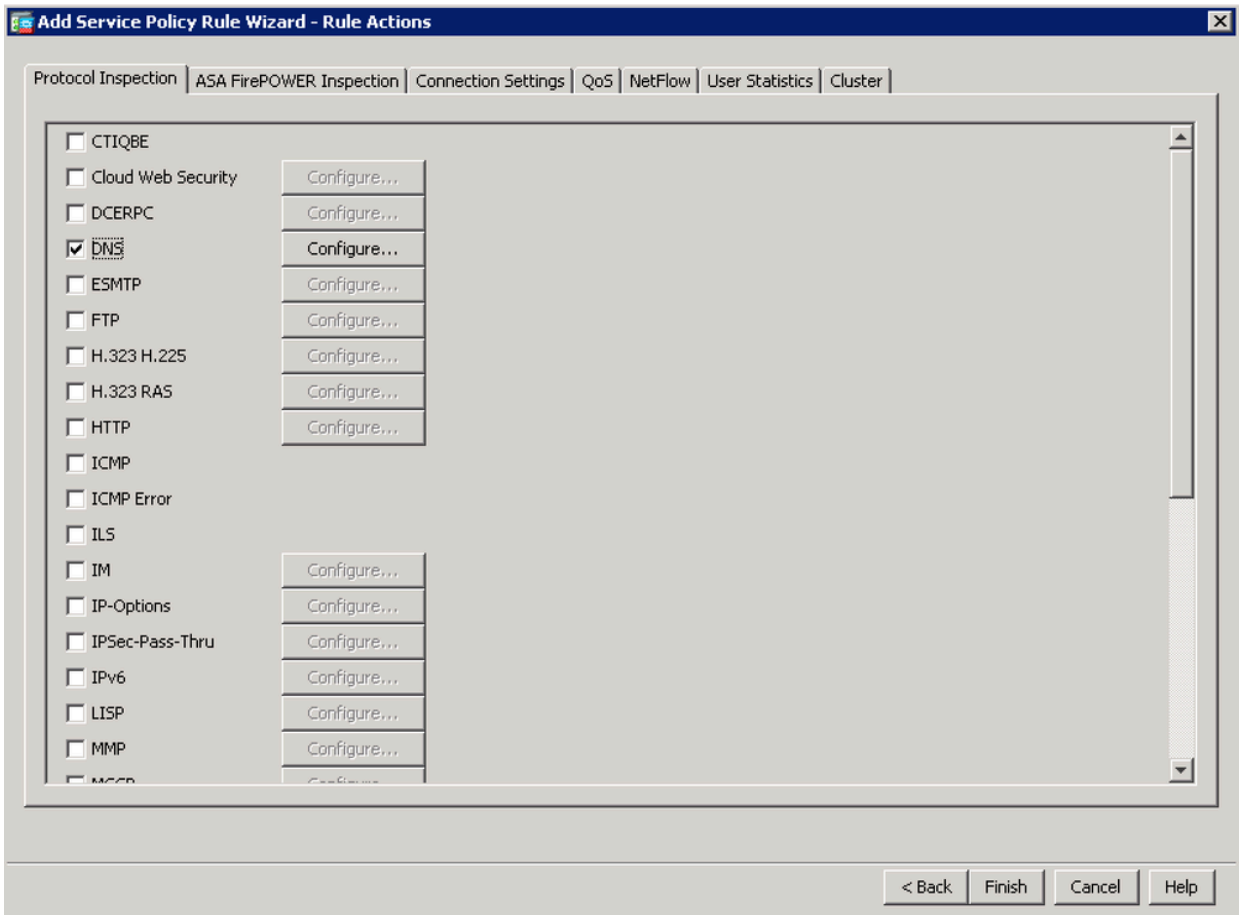

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

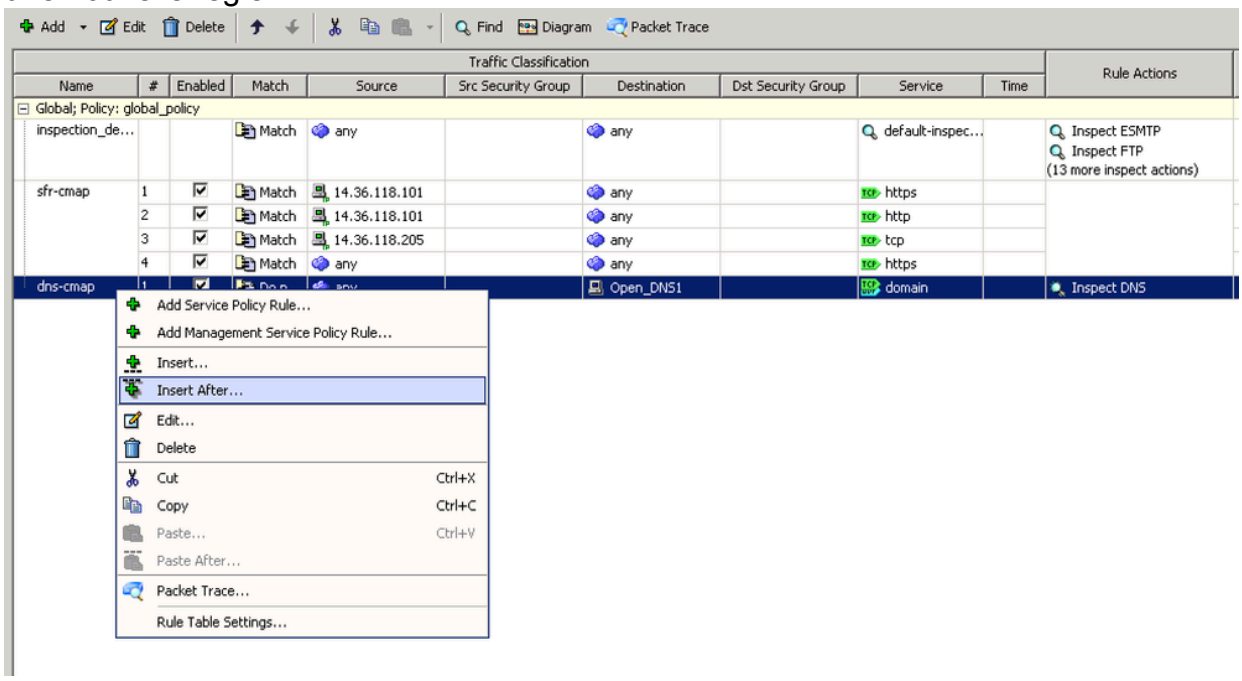
8. Ajoutez les deux objets réseau Umbrella au champ Destination et cliquez sur OK.



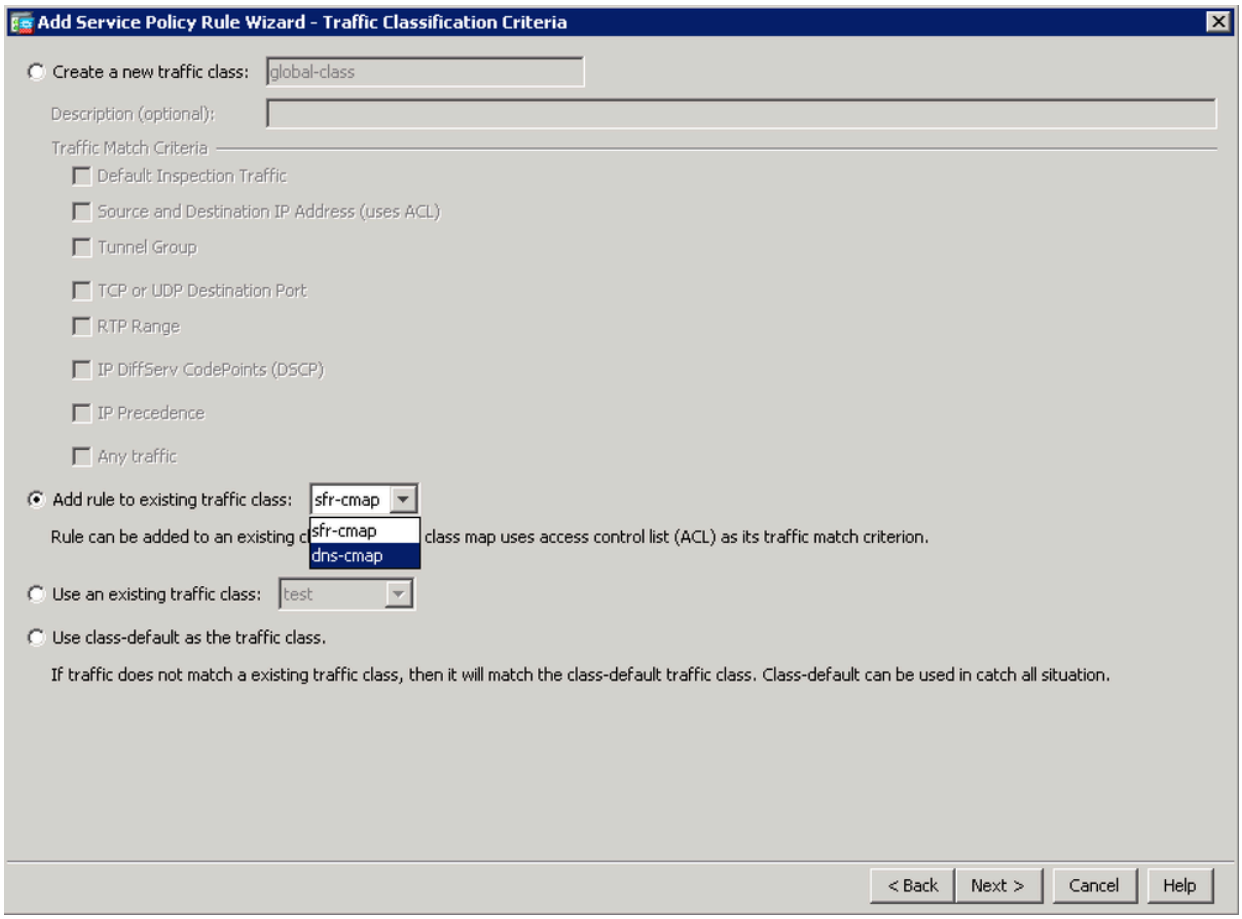
9. Dans la fenêtre suivante, cochez la case « DNS » et cliquez sur Finish.



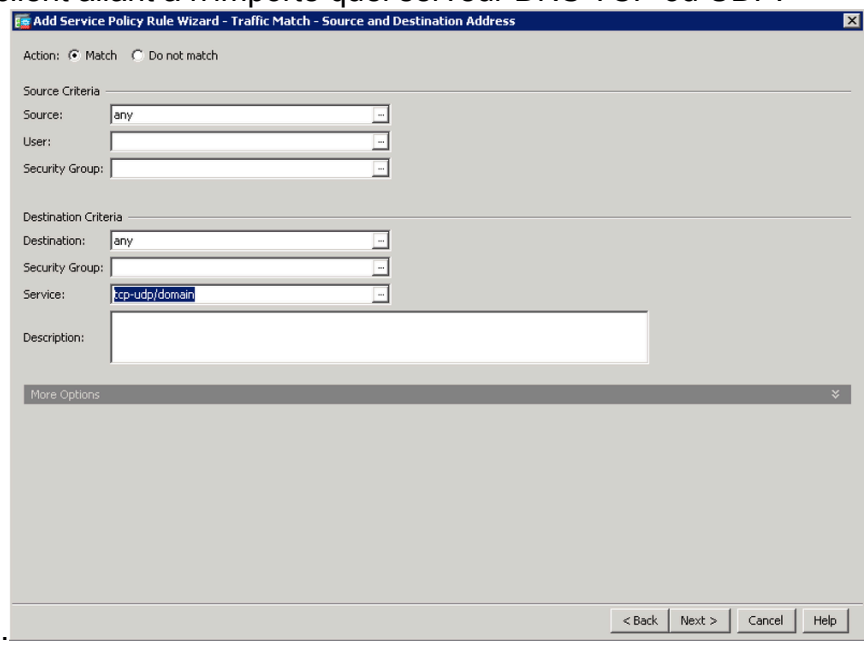
10. L'ASA affiche maintenant la nouvelle politique globale pour « dns-cmap ». Maintenant, vous devez configurer le trafic restant qui est inspecté par l'ASA. Pour ce faire, cliquez avec le bouton droit sur 'dns-cmap' et sélectionnez l'option "Insérer après..." qui crée une nouvelle règle.



11. Dans la première fenêtre, cliquez sur Next et sur puis cochez la case d'option « Add rule to existing traffic class: ». Sélectionnez « dns-cmap » dans la liste déroulante, puis cliquez sur Next.

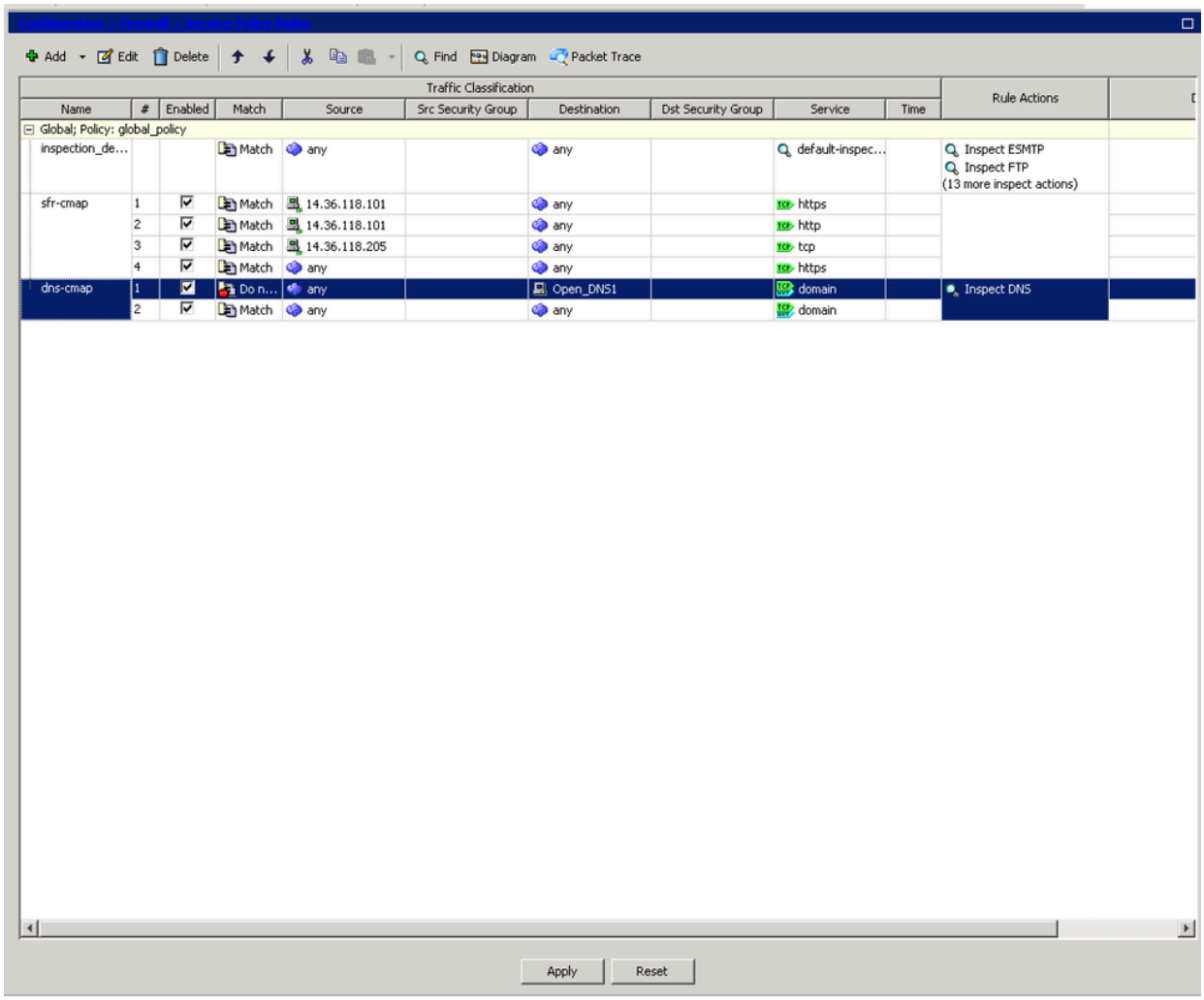


12. Laissez l'action « Correspondance ». Choisissez la source, la destination et le service du trafic qui est soumis à l'inspection DNS. Ici, par exemple, nous faisons correspondre le trafic de n'importe quel client allant à n'importe quel serveur DNS TCP ou UDP.



Cliquez sur Next (Suivant).

13. Laissez l'option « DNS » cochée et cliquez sur Finish.
14. Cliquez sur Apply en bas de la fenêtre.



Informations complémentaires

Si vous préférez désactiver DNScrypt plutôt que de configurer des exemptions ASA, contactez le support d'Umbrella.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.