Risoluzione dei problemi relativi al blocco del firewall ASA da parte della funzionalità di crittografia DNS di Umbrella Virtual Appliance

Sommario

Introduzione

In questo articolo viene descritto come risolvere i problemi relativi alla funzionalità DNScrypt di blocco del firewall ASA.

Panoramica

Cisco ASA Firewall può bloccare la funzionalità DNScrypt offerta da Umbrella Virtual Appliance. Di seguito è riportato il messaggio di avviso di 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

I messaggi di errore possono essere visualizzati anche nei log del firewall dell'ASA:

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

La crittografia DNSCrypt è progettata per proteggere il contenuto delle query DNS e, di conseguenza, impedisce ai firewall di eseguire l'ispezione dei pacchetti.

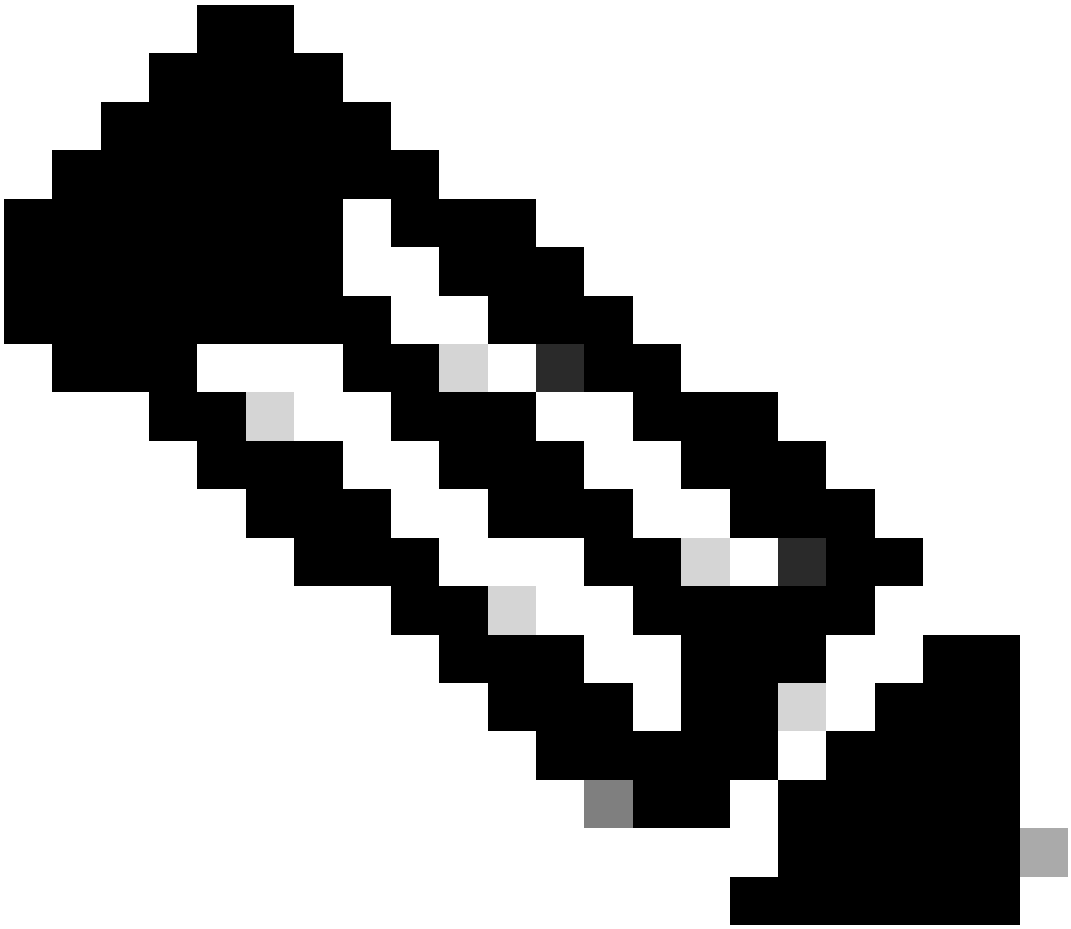
Causa

Questi errori non devono causare alcun impatto sulla risoluzione DNS per gli utenti.

L'appliance virtuale invia query di test per determinare la disponibilità di DNScrypt. Le query di test sono bloccate. Tuttavia, questi messaggi di errore indicano che l'appliance virtuale non aggiunge ulteriore sicurezza crittografando il traffico DNS della società.

Risoluzione

È consigliabile disabilitare l'ispezione dei pacchetti DNS per il traffico tra l'appliance virtuale e i resolver DNS Umbrella. Anche se questa operazione disabilita la registrazione e l'ispezione del protocollo sull'appliance ASA, migliora la sicurezza consentendo la crittografia DNS.



Nota: Questi comandi vengono forniti solo come guida e si consiglia di consultare un esperto Cisco prima di apportare qualsiasi modifica a un ambiente di produzione. Tenere presente questo difetto anche sull'appliance ASA potrebbe influire sul DNS su TCP, il che può causare problemi anche con DNSCrypt:
Supporto ispezione DNS CSCsm90809 per DNS su TCP

Eccezioni ispezione pacchetti - Comandi IOS

1. Creare un nuovo ACL chiamato 'dns_inspect' con regole per negare il traffico a 208.67.222.222 e 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. Rimuovere i criteri di ispezione DNS correnti sull'appliance ASA. Ad esempio:

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

3. Creare una mappa delle classi corrispondente all'ACL creato nel passaggio 1:

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

4. Configurare una mappa dei criteri in global_policy. Deve corrispondere alla mappa delle classi creata nel passaggio 3. Abilitare l'ispezione DNS.

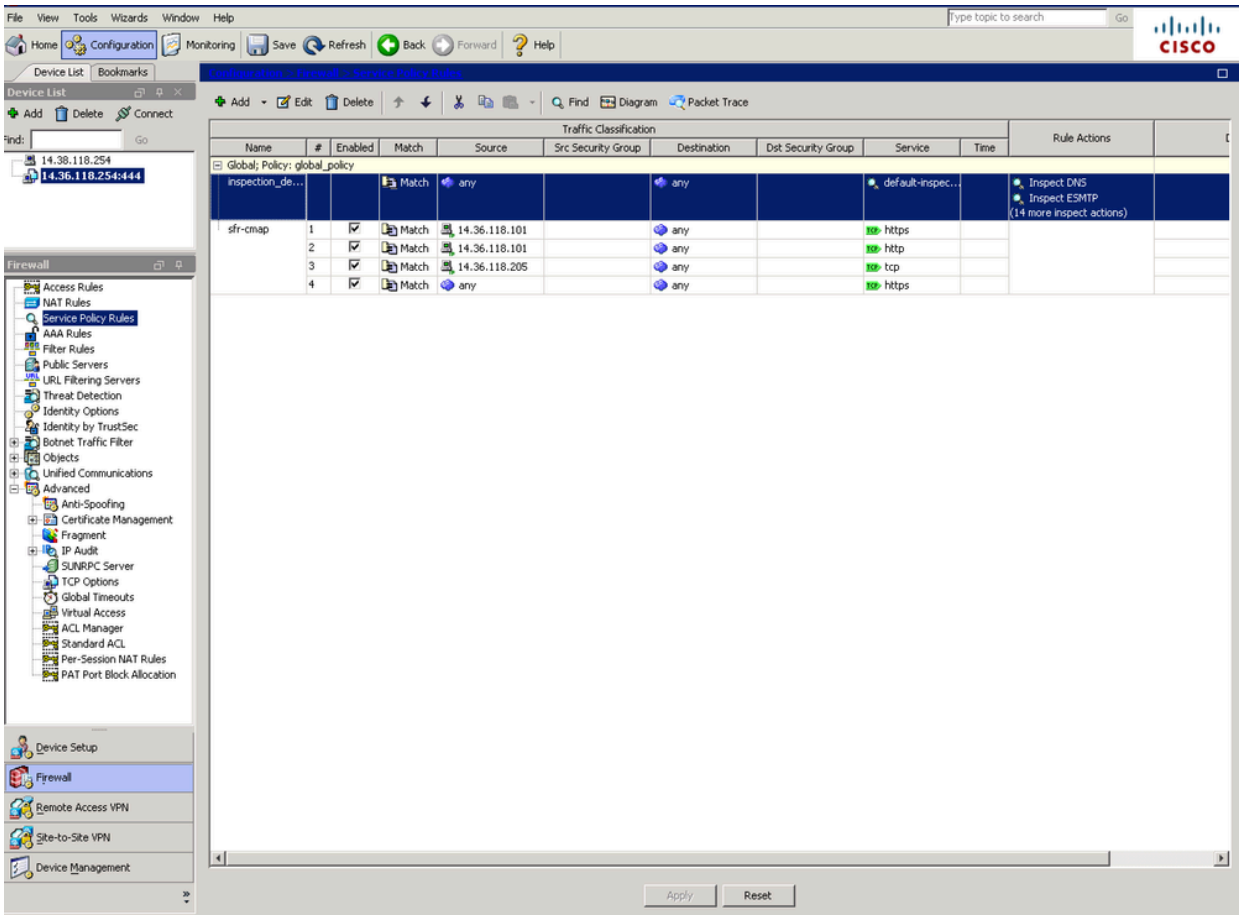
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. Dopo aver abilitato la funzione, è possibile verificare se il traffico sta raggiungendo le esclusioni eseguendo:

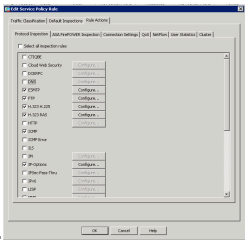
```
sh access-list dns_inspect
```

Eccezioni ispezione pacchetti - Interfaccia ASDM

1. Disabilitare innanzitutto l'ispezione dei pacchetti DNS, se applicabile. Questa operazione viene eseguita in Configurazione > Firewall > Regole dei criteri di servizio.

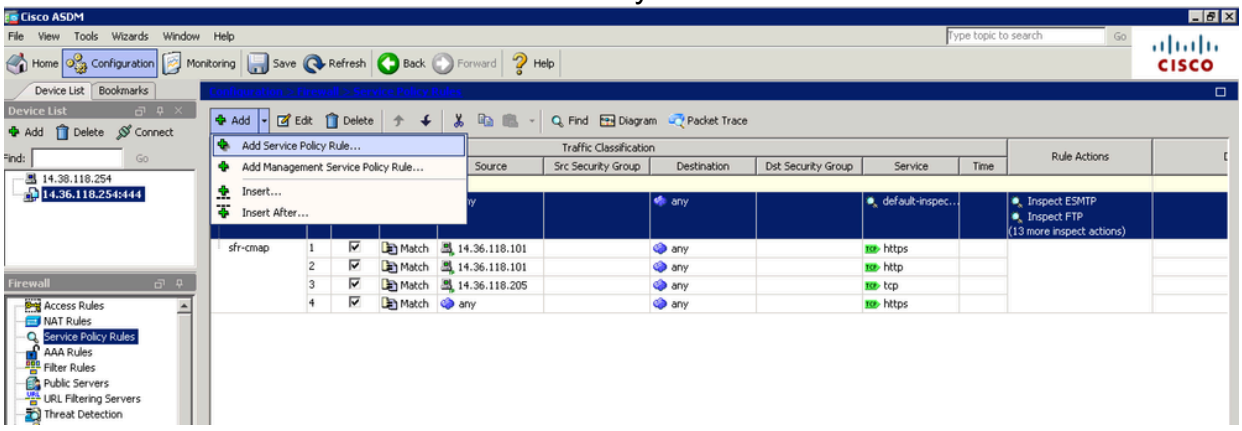


2. Nell'esempio, l'ispezione DNS è abilitata nella classe Criteri globali e 'selection_default'. Evidenziarlo e fare clic su Modifica. Nella nuova finestra

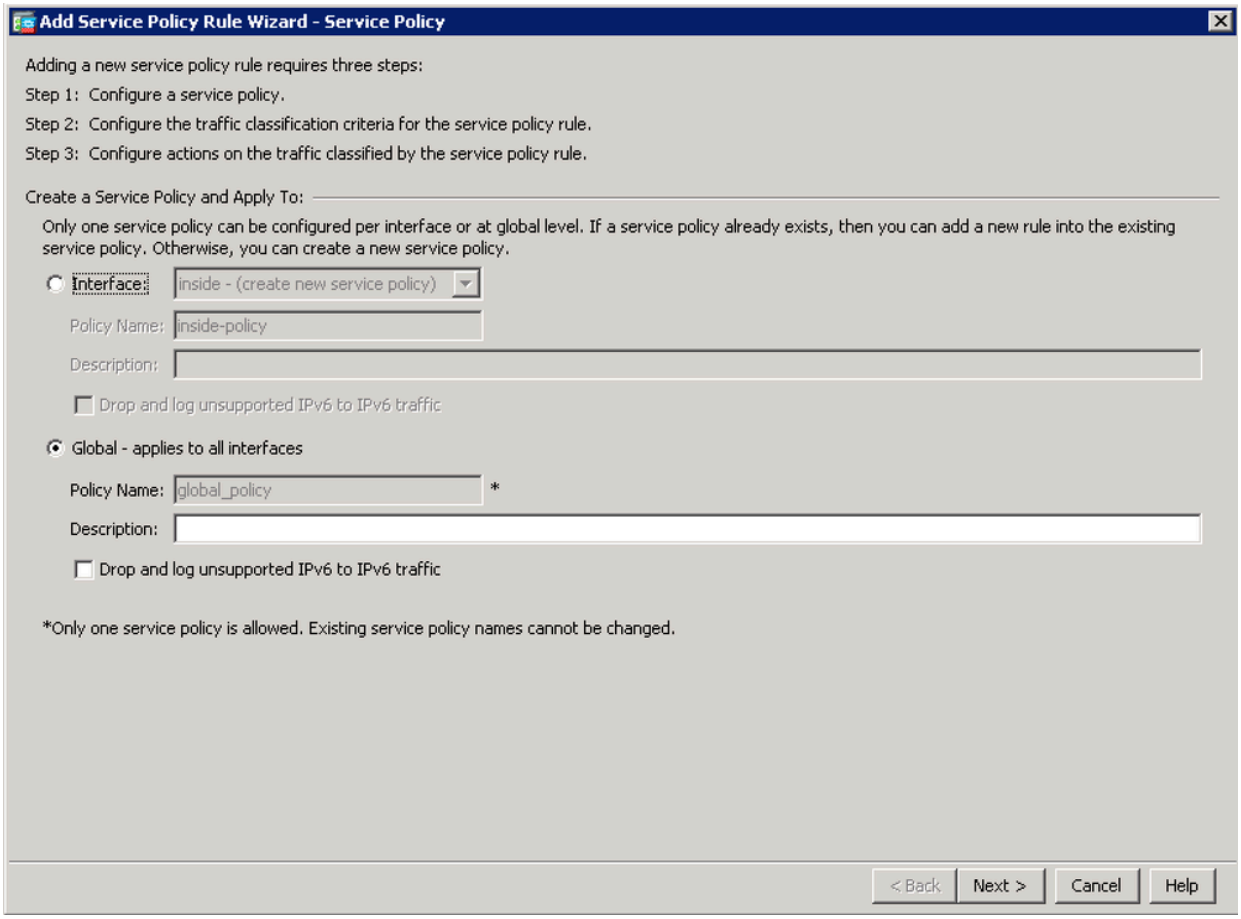


deselezionare la casella relativa a 'DNS' nella scheda "Azione regola".

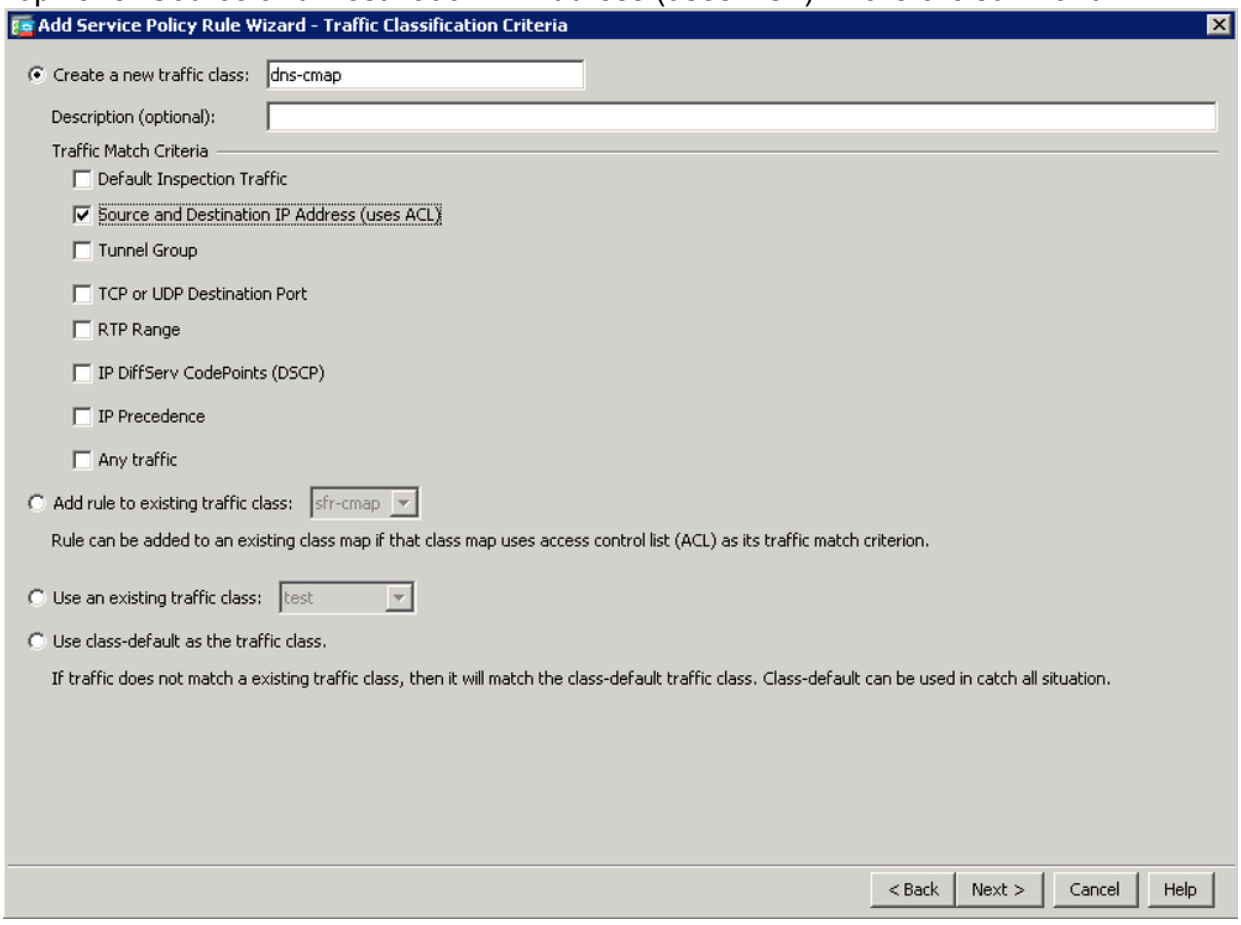
3. È ora possibile riconfigurare l'ispezione DNS, questa volta con ulteriori esenzioni dal traffico. Fare clic su Add > Add Service Policy Rule...



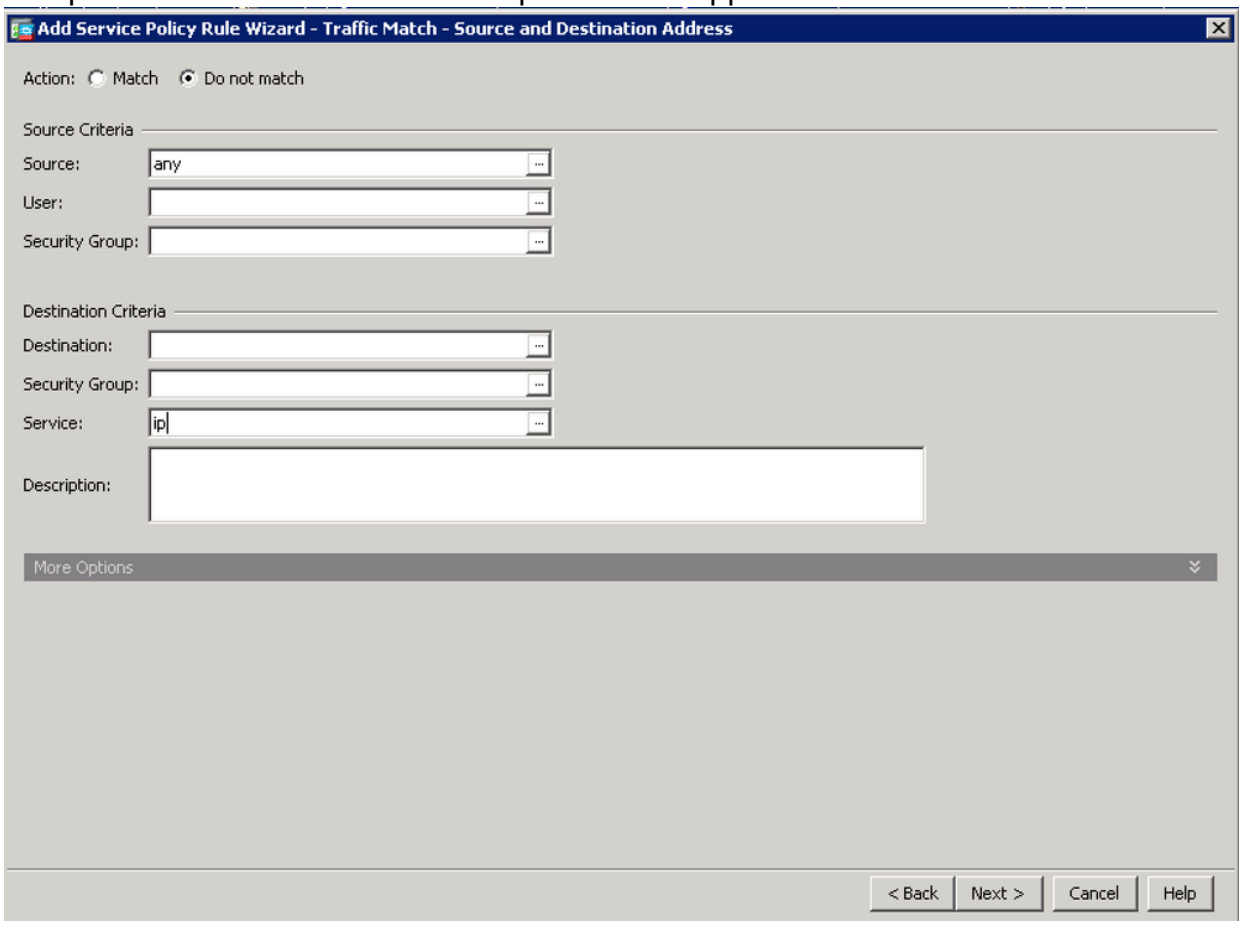
4. Selezionare "Global - Applies to all interfaces" e fare clic su Next (applicabile anche a un'interfaccia specifica).



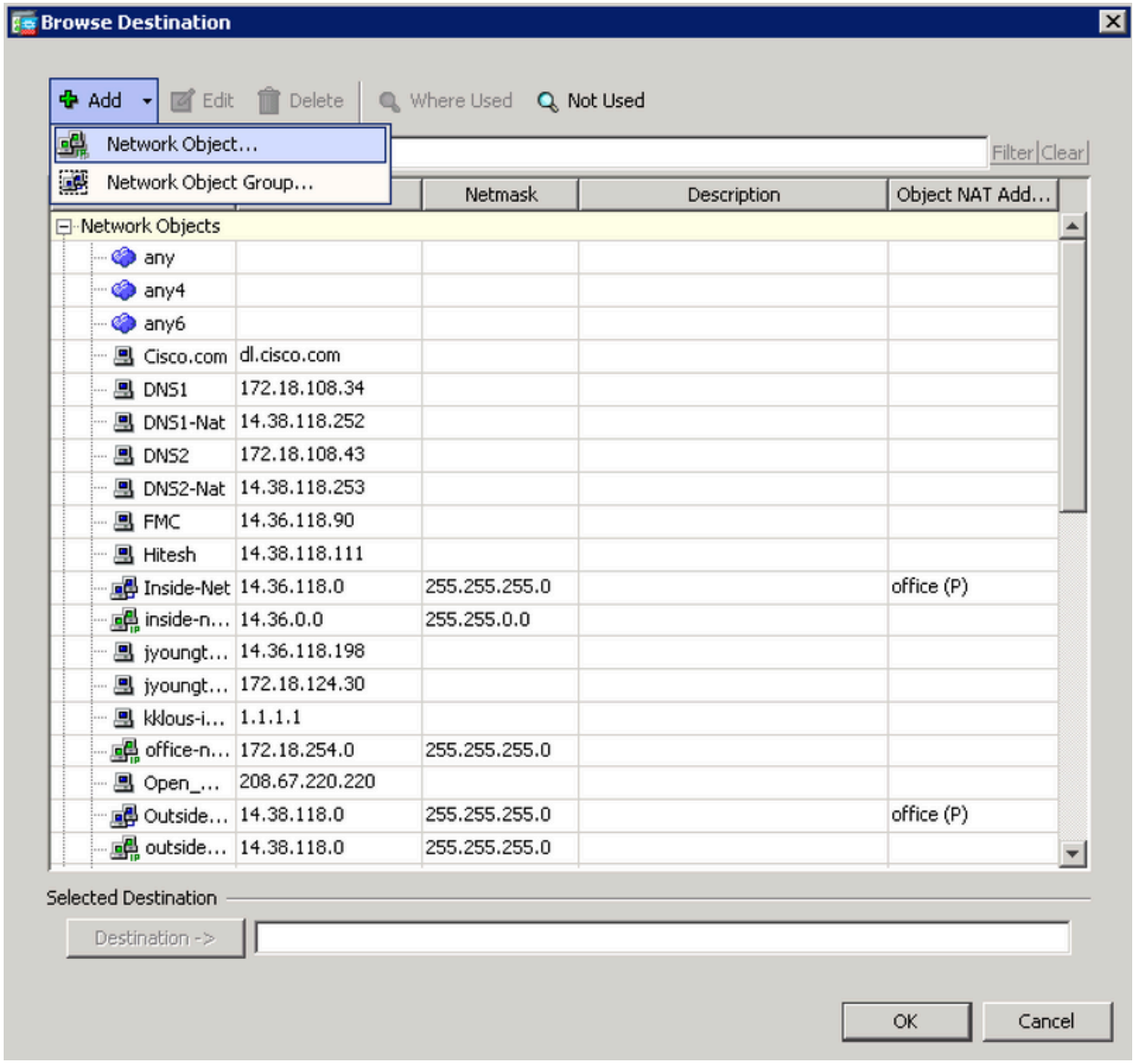
5. Assegnare un nome alla mappa di classe (ad esempio 'dns-cmap') e selezionare l'opzione "Source and Destination IP Address (uses ACL)". Fare clic su Avanti.

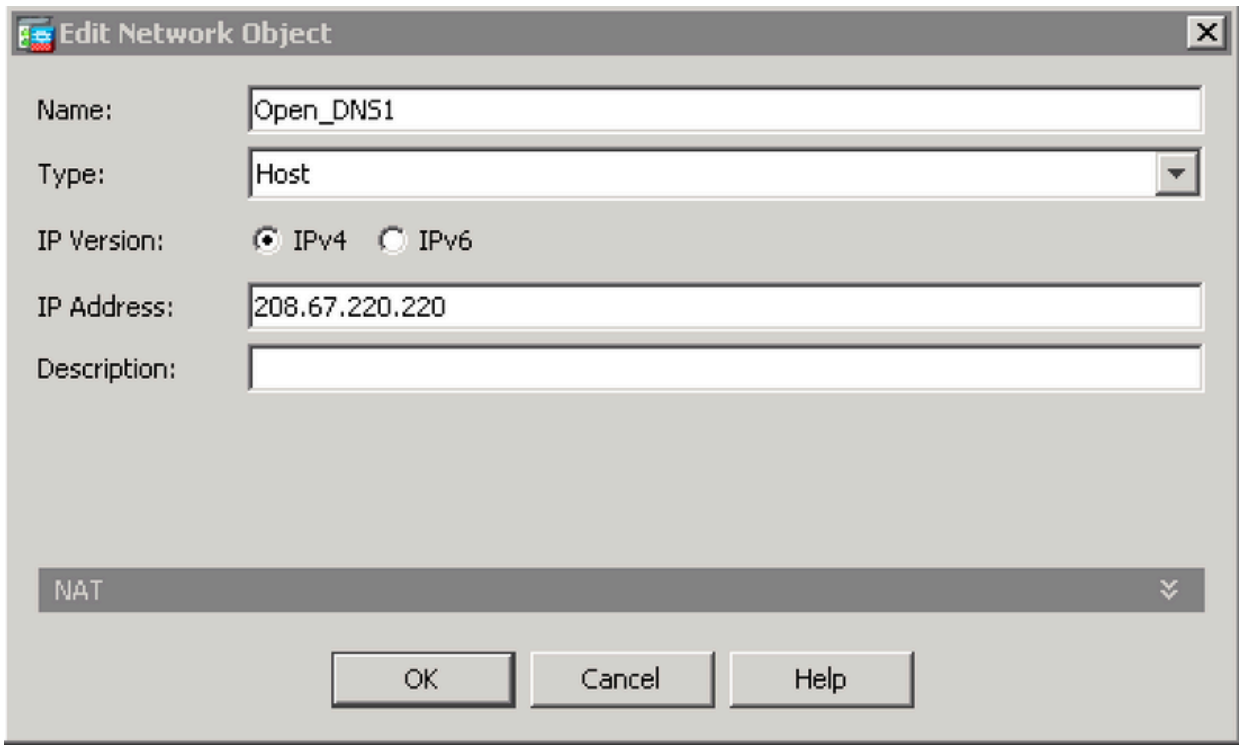


6. Iniziare configurando il traffico che non si desidera venga ispezionato utilizzando l'azione "Non corrispondenza".
   Per Source, è possibile utilizzare l'opzione 'any' per esentare tutto il traffico destinato ai server DNS di Umbrella. In alternativa, è possibile creare una definizione dell'oggetto di rete per esentare solo l'indirizzo IP specifico dell'appliance virtuale.

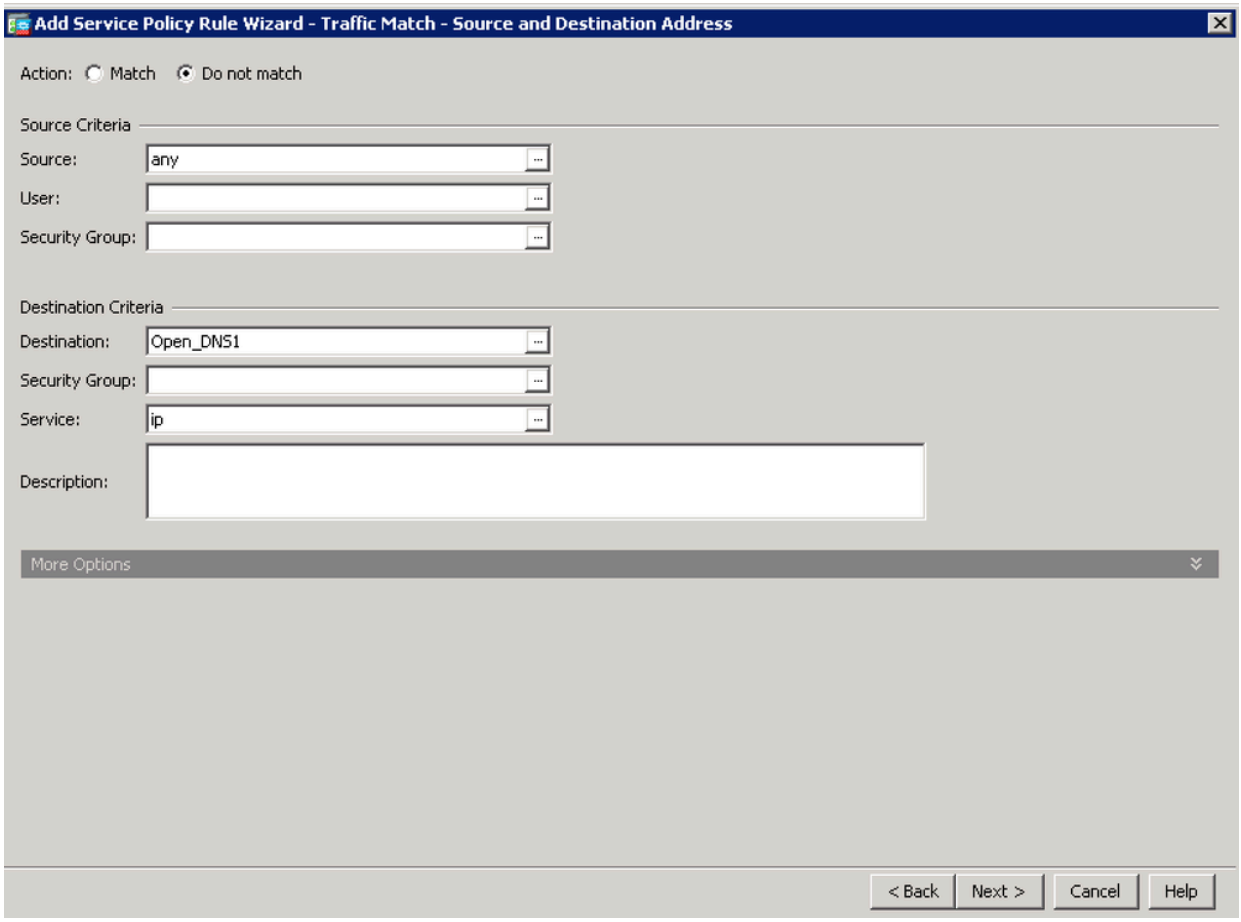


7. Fare clic su ... nel campo Destinazione. Nella finestra successiva, fare clic su Add > Network Object e creare un oggetto con l'indirizzo IP '208.67.222.222'. Ripetere questo passaggio per creare un oggetto con indirizzo IP '208.67.220.220'.

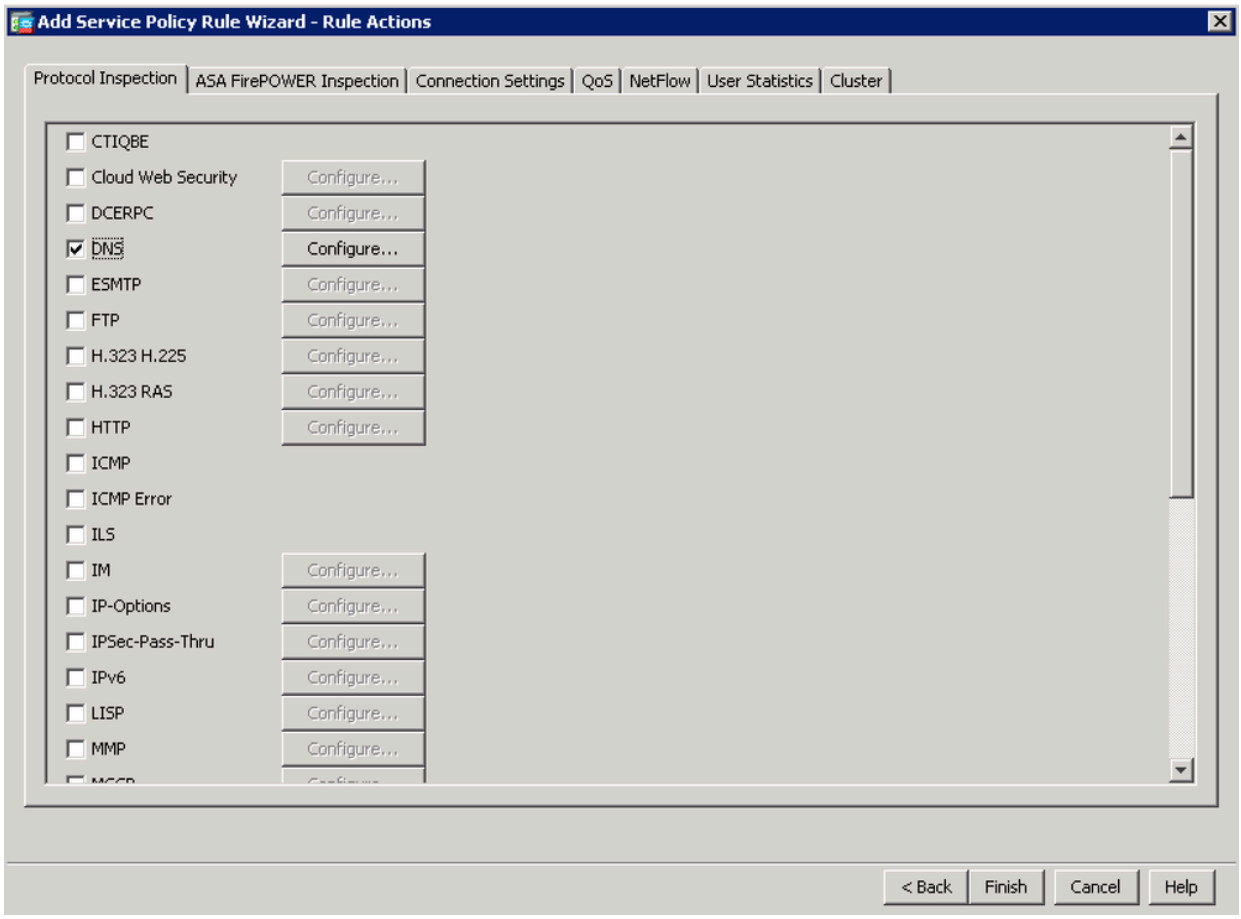

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

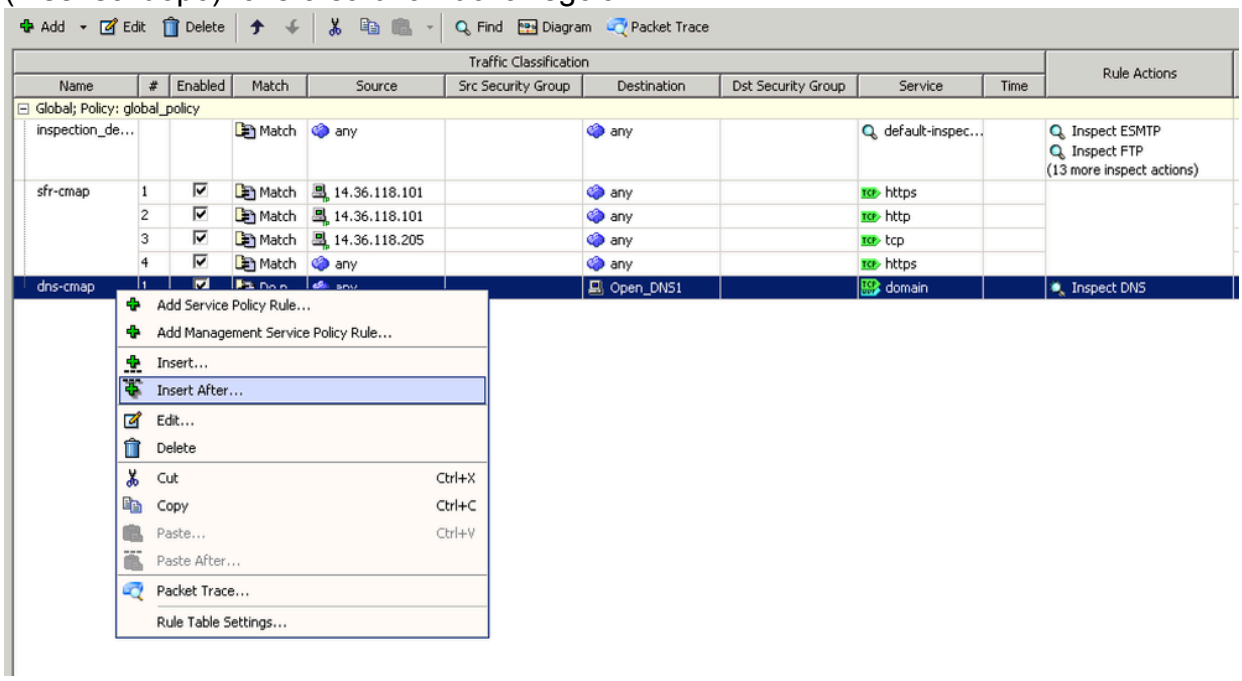
8. Aggiungere entrambi gli oggetti di rete Umbrella al campo Destinazione e fare clic su OK.



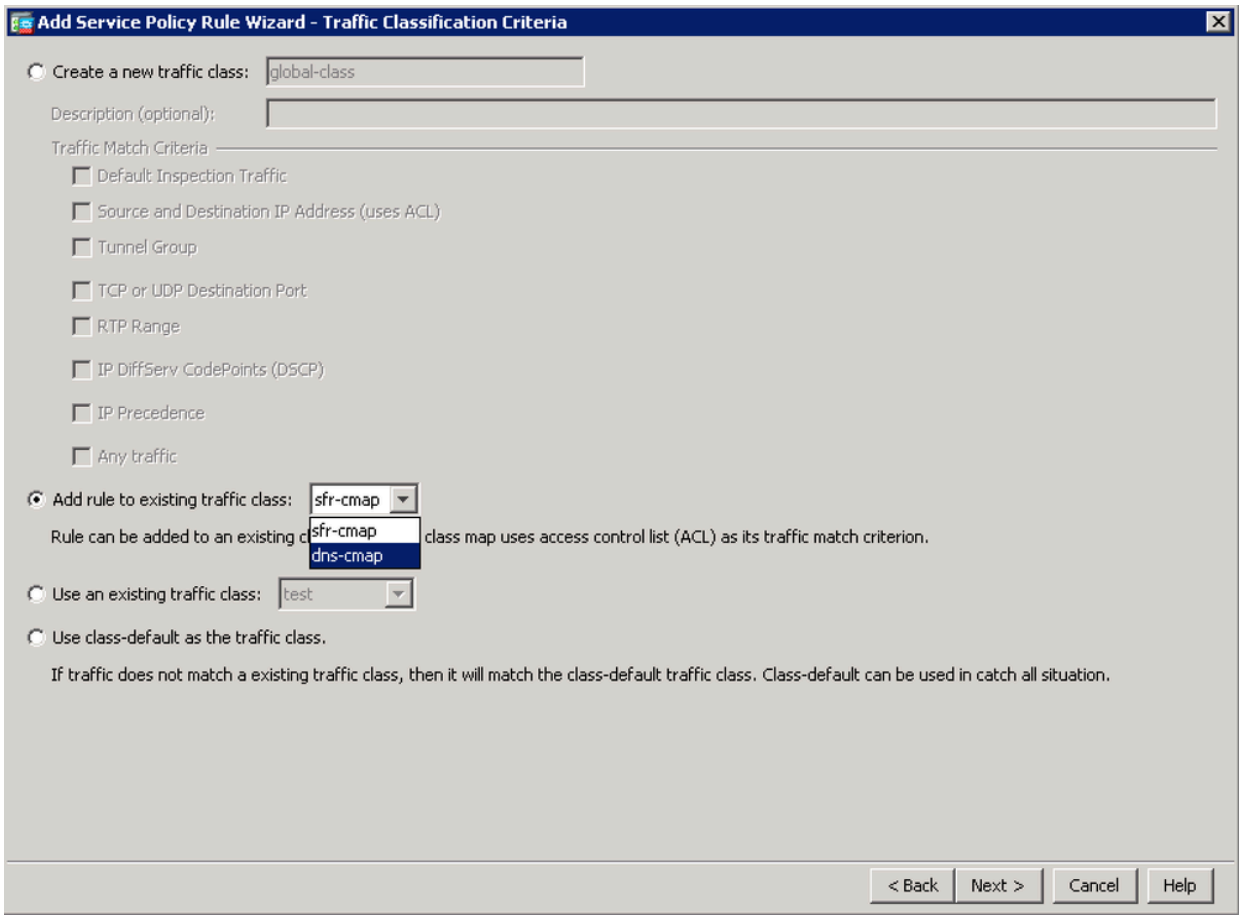
9. Nella finestra successiva selezionare la casella relativa a 'DNS' e fare clic su Fine.



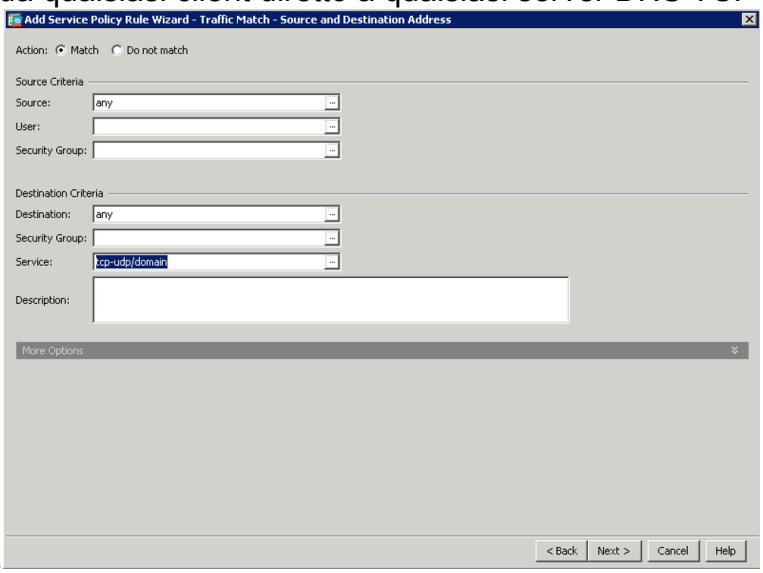
10. L'ASA mostra ora la nuova policy globale per 'dns-cmap'. A questo punto, è necessario configurare il traffico rimanente che viene ispezionato dall'ASA. A tale scopo, fare clic con il pulsante destro del mouse su 'dns-cmap' e selezionare l'opzione "Insert After..." (Inserisci dopo). che crea una nuova regola.



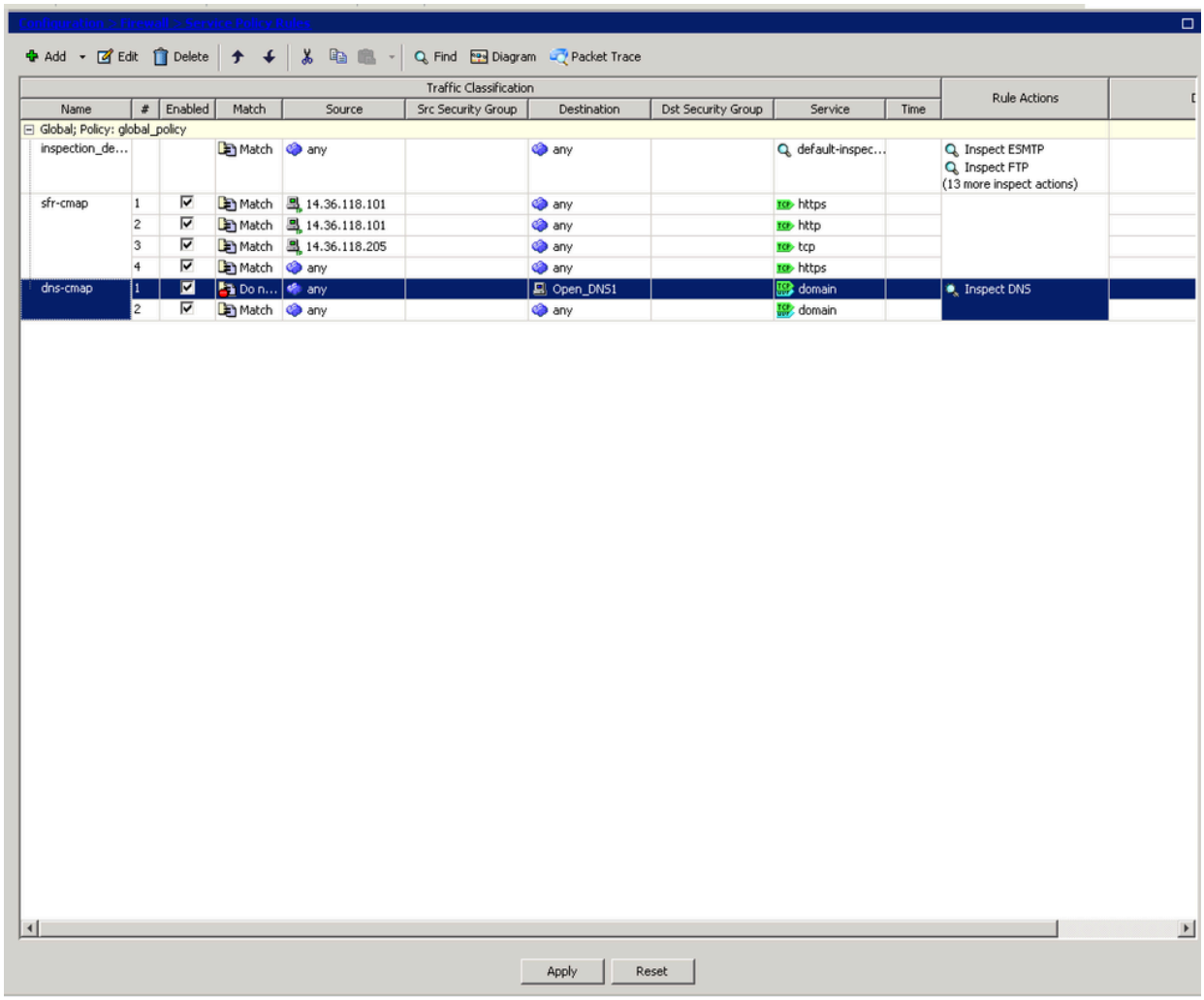
11. Nella prima finestra, fare clic su Next (Avanti), quindi selezionare il pulsante di opzione "Add rule to existing traffic class:" (Aggiungi regola alla classe traffico esistente). Selezionare 'dns-cmap' dall'elenco a discesa e fare clic su Avanti.



12. Lasciare l'azione come 'Corrispondenza'. Scegliere l'origine, la destinazione e il servizio del traffico soggetto a ispezione DNS. In questo caso, ad esempio, viene confrontato il traffico proveniente da qualsiasi client diretto a qualsiasi server DNS TCP o UDP. Fare clic su Next (Avanti).



13. Lasciare selezionata l'opzione 'DNS' e fare clic su Fine.
14. Fare clic su Apply (Applica) nella parte inferiore della finestra.



Ulteriori informazioni

Se si preferisce disabilitare DNScrypt anziché configurare le esenzioni ASA, contattare il supporto Umbrella.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).