Fehlerbehebung: ASA-Firewall blockiert DNS-Skript-Funktionalität von der virtuellen Umbrella Appliance

Inhalt

Einleitung

In diesem Artikel wird die Fehlerbehebung bei der ASA-Firewall beschrieben, die die DNScrypt-Funktion blockiert.

Überblick

Die Cisco ASA Firewall kann die von der Umbrella Virtual Appliance gebotene DNScrypt-Funktion blockieren. Daraus ergibt sich die folgende Umbrella Dashboard-Warnung:

> 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

Diese Fehlermeldungen sind auch in den ASA-Firewall-Protokollen zu finden:

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

Die DNSCrypt-Verschlüsselung wurde entwickelt, um den Inhalt Ihrer DNS-Abfragen zu schützen und verhindert so auch, dass Firewalls eine Paketprüfung durchführen.

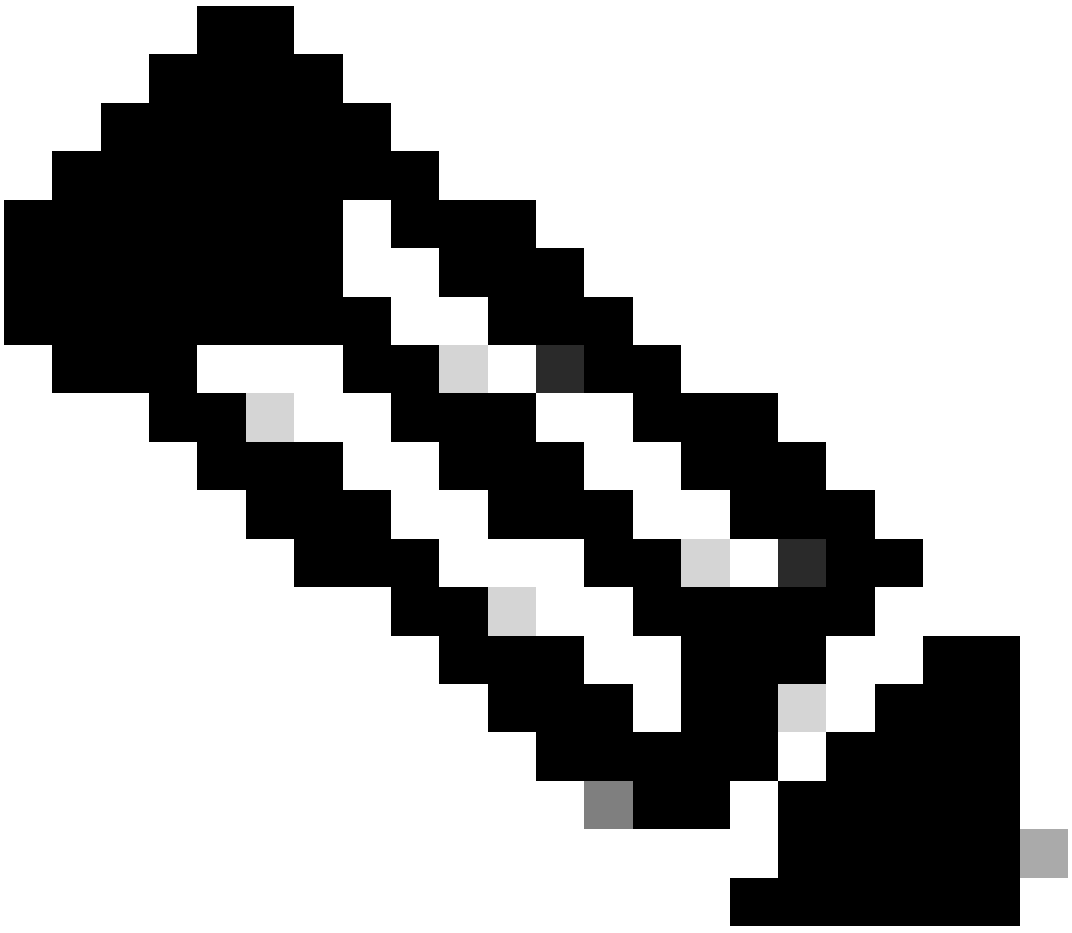
Ursache

Diese Fehler dürfen keine Auswirkungen auf die DNS-Auflösung haben, die auf Benutzer zutreffen.

Die virtuelle Appliance sendet Testabfragen, um die Verfügbarkeit von DNScrypt zu ermitteln. Diese Testabfragen werden blockiert. Diese Fehlermeldungen weisen jedoch darauf hin, dass die virtuelle Appliance keine zusätzliche Sicherheit bietet, indem sie den DNS-Datenverkehr Ihres Unternehmens verschlüsselt.

Auflösung

Wir empfehlen, die DNS-Paketprüfung für den Datenverkehr zwischen der virtuellen Appliance und den DNS-Resolvern von Umbrella zu deaktivieren. Dadurch werden zwar die Protokollierung und Protokollprüfung auf der ASA deaktiviert, die Sicherheit wird jedoch durch die Möglichkeit der DNS-Verschlüsselung erhöht.



Anmerkung: Diese Befehle dienen lediglich als Anleitung. Es wird empfohlen, einen Experten von Cisco zu Rate zu ziehen, bevor Änderungen an der Produktionsumgebung vorgenommen werden.
Beachten Sie diesen Fehler auch bei ASA. kann sich auf DNS über TCP auswirken, was ebenfalls Probleme mit DNSCrypt verursachen kann:

CSCsm90809 DNS-Inspektionsunterstützung für DNS über TCP

Ausnahmen bei der Paketprüfung - IOS-Befehle

1. Erstellen Sie eine neue ACL mit dem Namen "dns_inspect" mit Regeln zum Verweigern von Datenverkehr an die Adressen 208.67.222.222 und 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. Entfernen Sie die aktuelle DNS-Inspektionsrichtlinie auf der ASA. Beispiele:

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

3. Erstellen Sie eine Klassenzuordnung, die mit der in Schritt #1 erstellten ACL übereinstimmt:

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

4. Konfigurieren Sie unter "global_policy" eine Richtlinienzuordnung. Dies muss mit der in Schritt #3 erstellten Klassenzuordnung übereinstimmen. Aktivieren Sie die DNS-Inspektion.

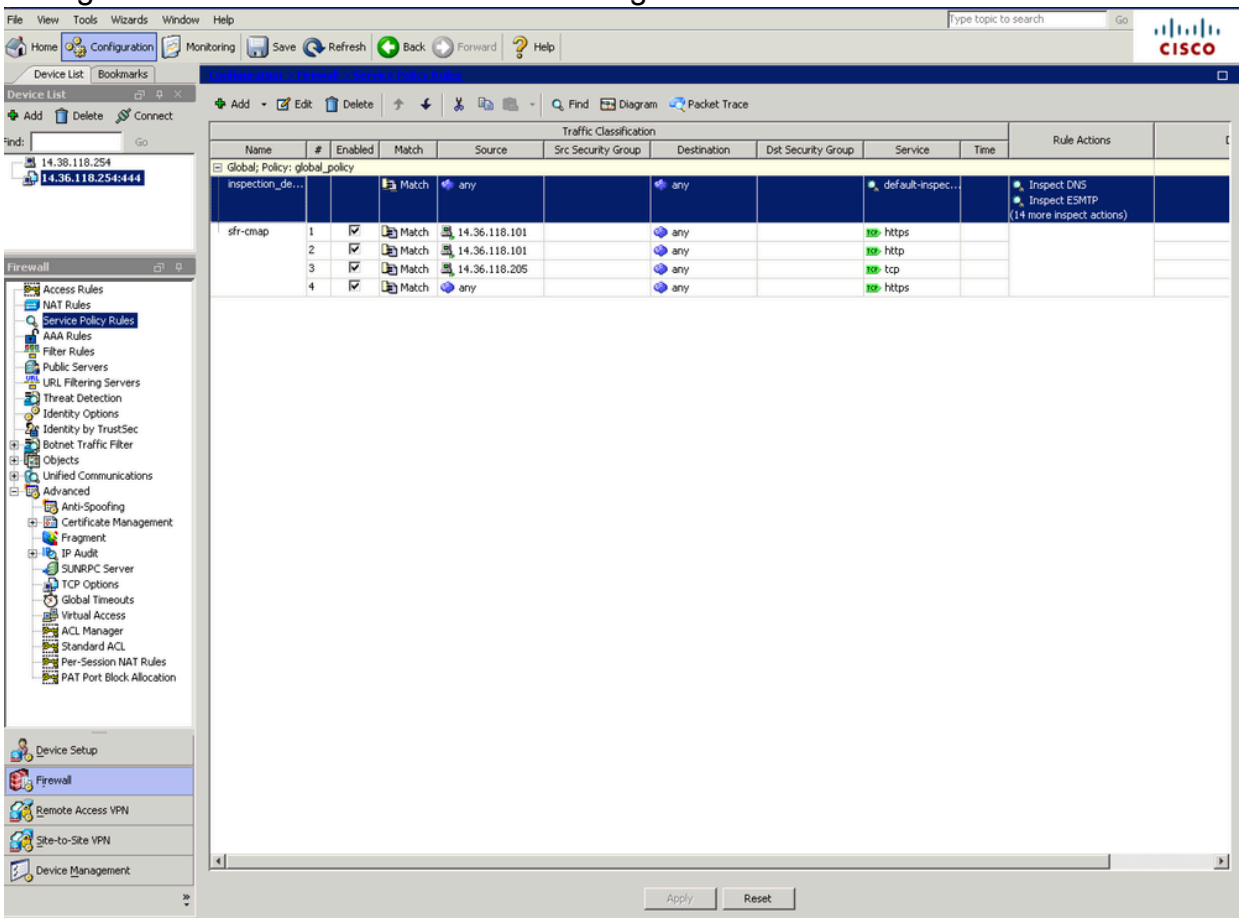
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. Wenn diese Funktion aktiviert ist, können Sie überprüfen, ob der Datenverkehr die Ausschlüsse erreicht:

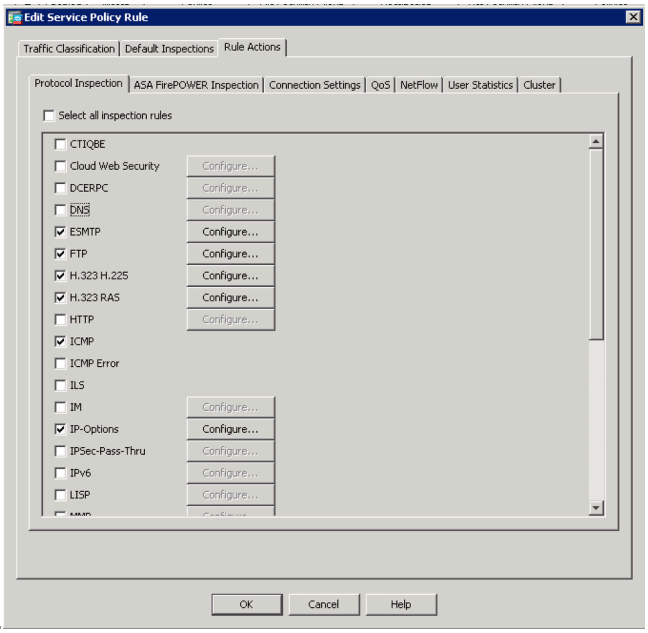
```
sh access-list dns_inspect
```

Ausnahmen bei der Paketprüfung - ASDM-Schnittstelle

1. Deaktivieren Sie zunächst ggf. die DNS-Paketprüfung. Dies geschieht unter Konfiguration > Firewall > Dienstrichtlinienregeln.

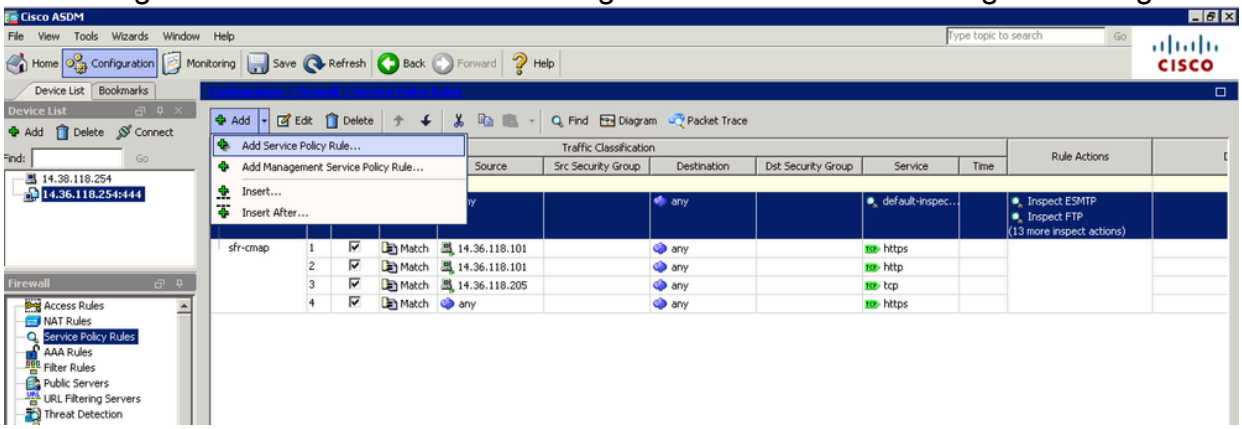


2. In diesem Beispiel ist die DNS-Inspektion unter der Klasse "Global Policy" und "inspection_default" aktiviert. Markieren Sie es und klicken Sie auf Bearbeiten. Deaktivieren Sie im neuen Fenster das Kontrollkästchen für "DNS" auf der Registerkarte "Rule Action" (Regelaktion).

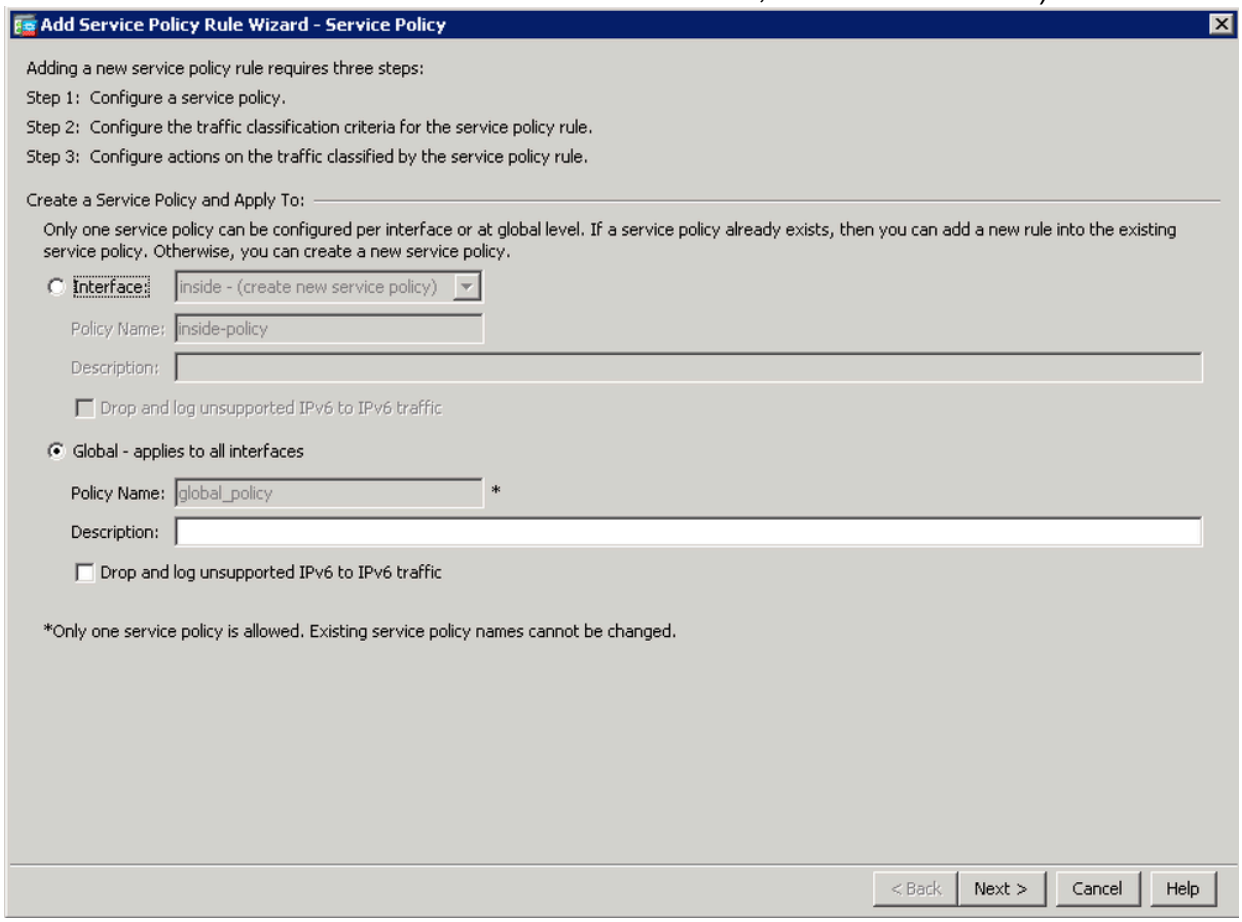


3. Jetzt können Sie die DNS-Überprüfung mit zusätzlichen Datenverkehrsausnahmen

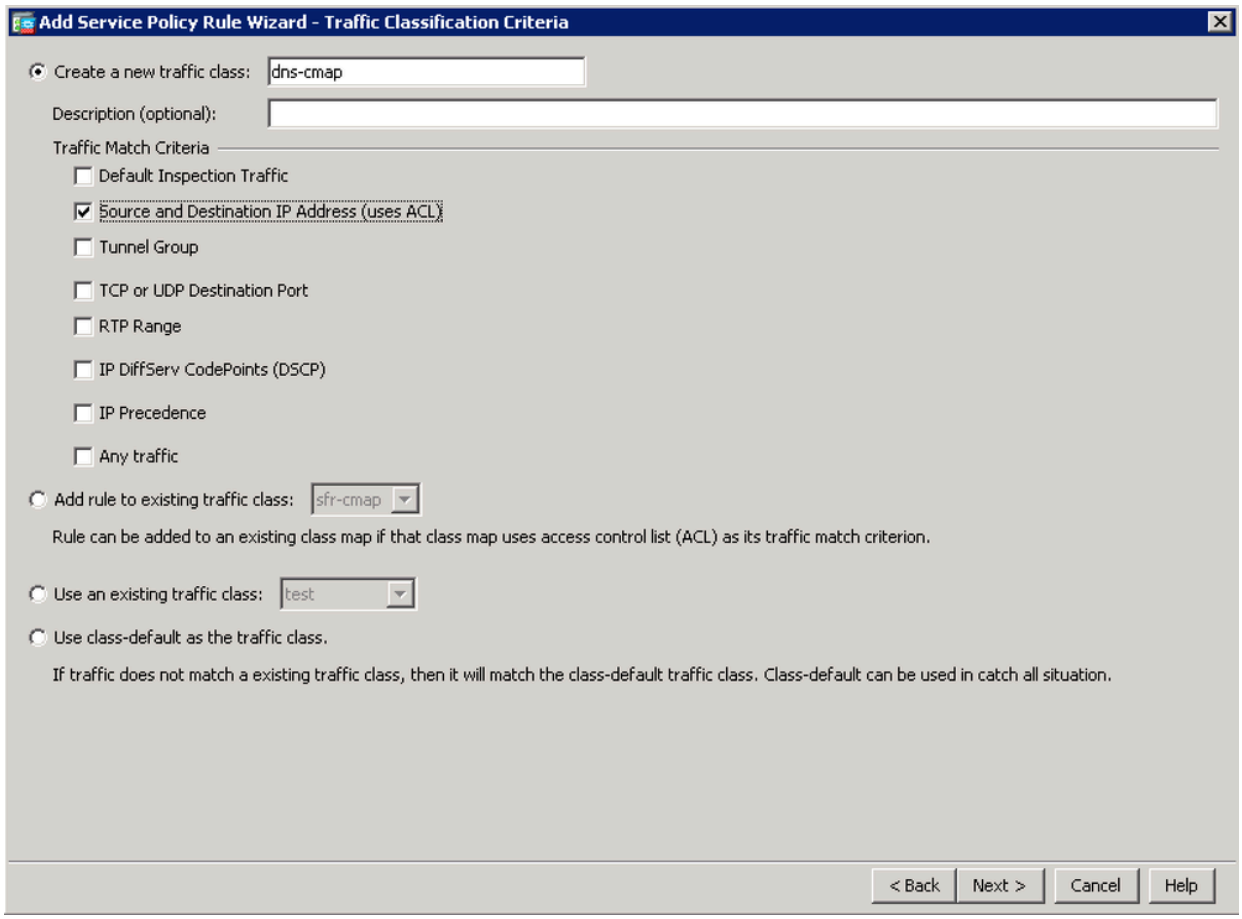
neu konfigurieren. Klicken Sie auf Hinzufügen > Servicerichtlinien-Regel hinzufügen...



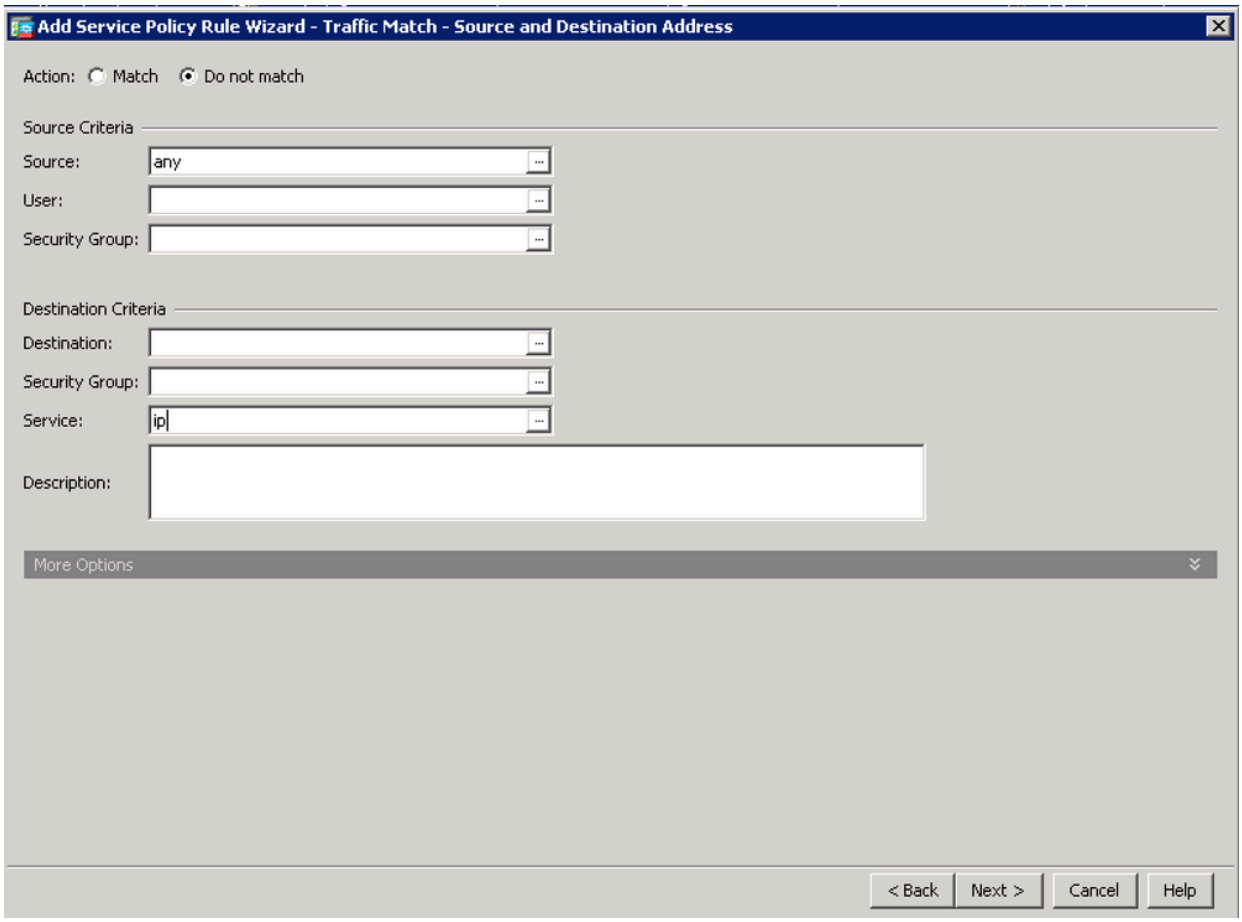
4. Wählen Sie "Global - Gilt für alle Schnittstellen" und klicken Sie auf Weiter (Sie können dies auch auf eine bestimmte Schnittstelle anwenden, wenn Sie möchten).



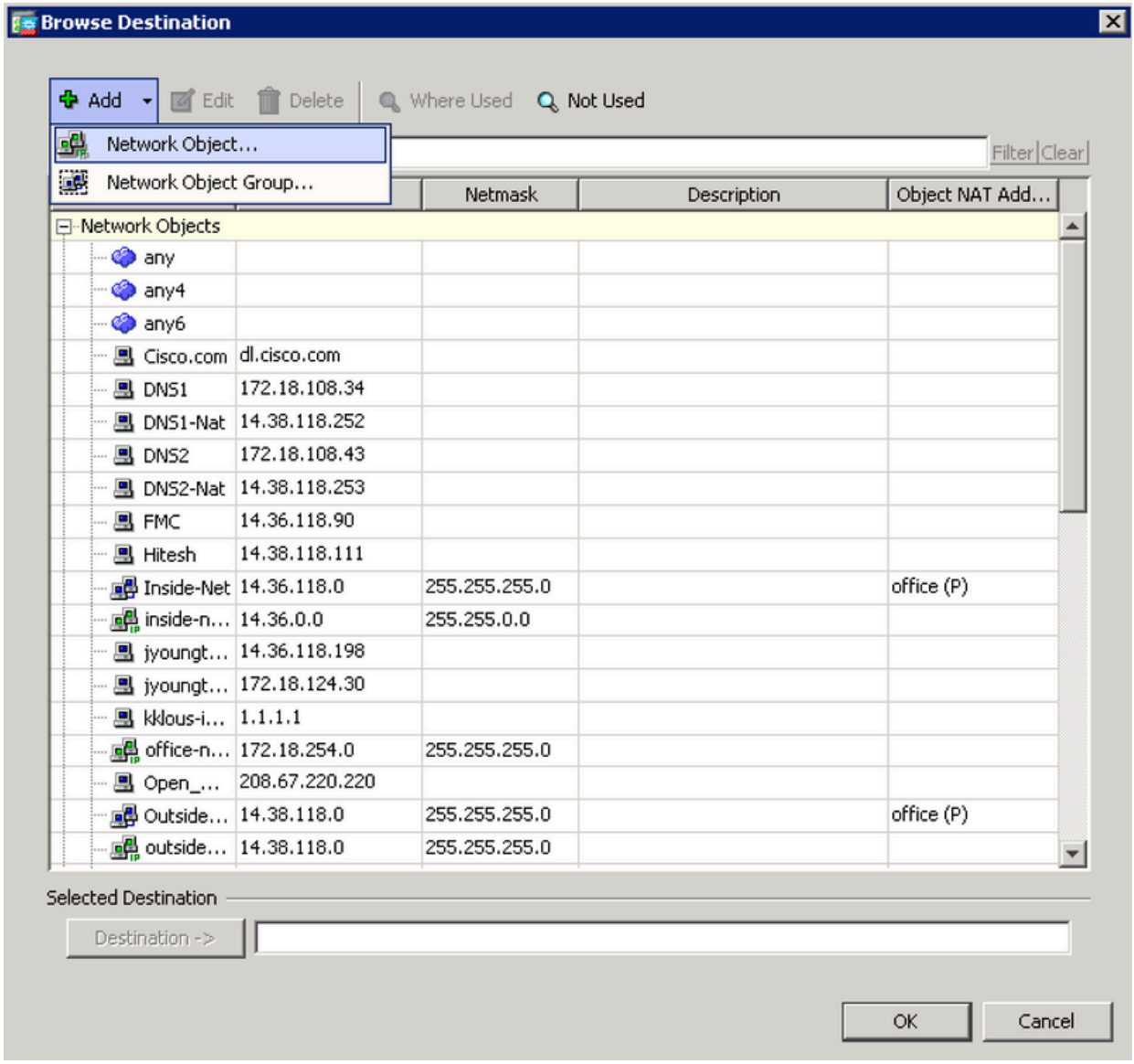
5. Geben Sie der Klassenzuordnung einen Namen (z. B. "dns-cmap"), und aktivieren Sie die Option "Quell- und Ziel-IP-Adresse (verwendet ACL)". Klicken Sie auf "Weiter".

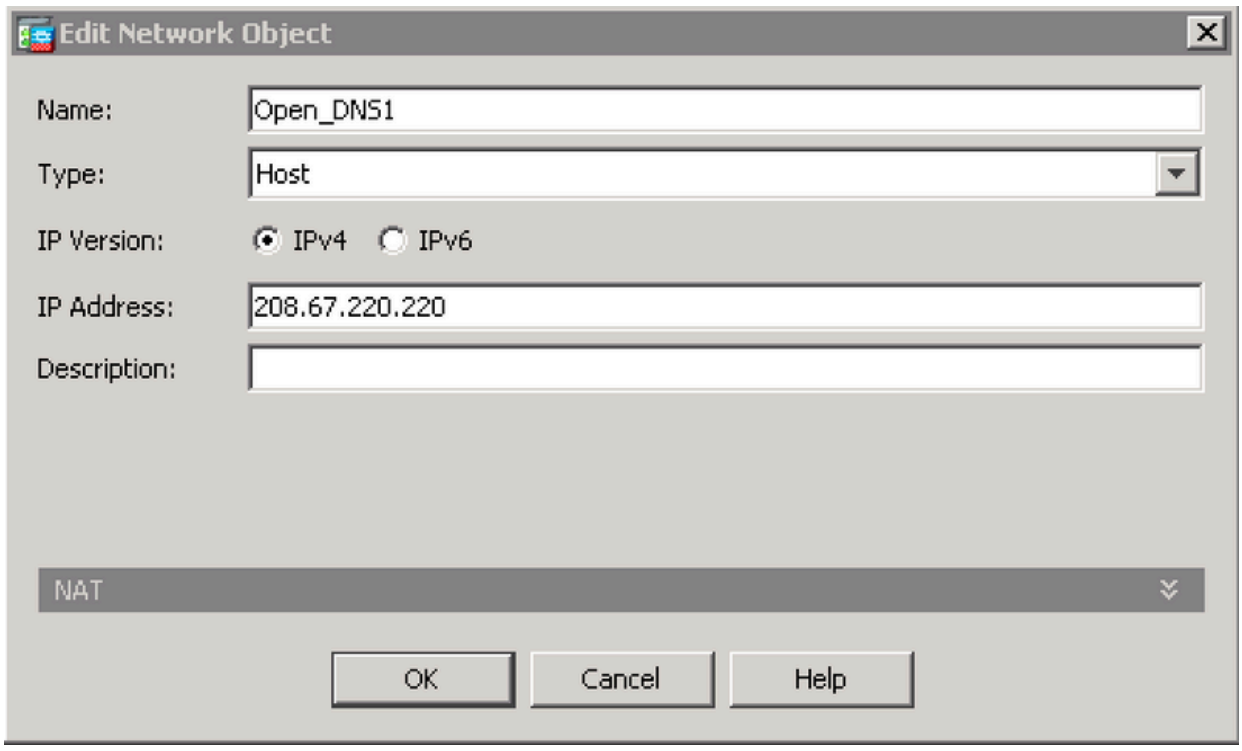


6. Konfigurieren Sie zunächst den Datenverkehr, der nicht überprüft werden soll. Verwenden Sie dazu die Aktion "Nicht übereinstimmen".
   Für Source (Quelle) können Sie die Option "any" verwenden, um den gesamten Datenverkehr, der an die DNS-Server von Umbrella gerichtet ist, auszunehmen. Alternativ können Sie hier eine Netzwerkobjektdefinition erstellen, um nur die spezifische IP-Adresse der virtuellen Appliance auszunehmen.

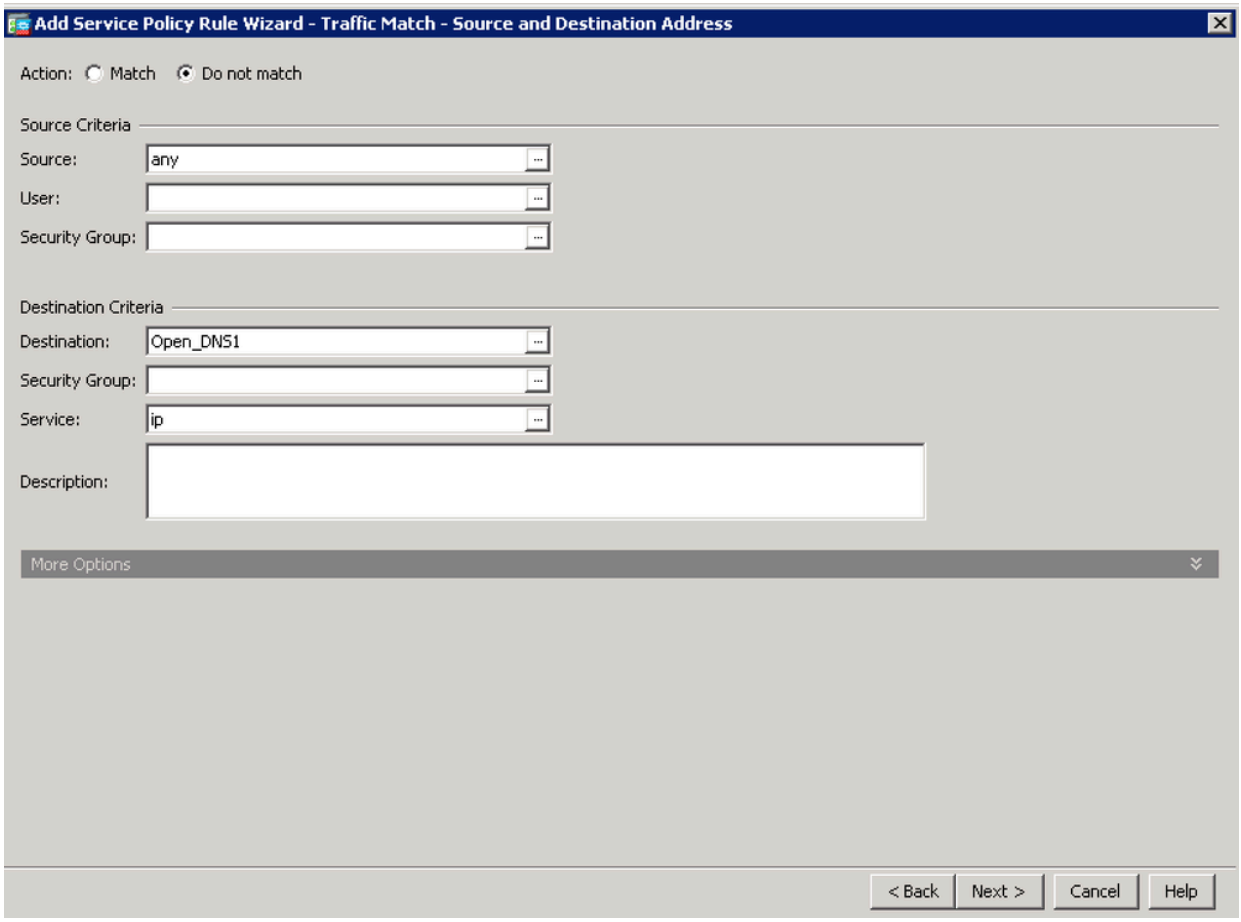


7. Klicken Sie im Feld Ziel auf .... Klicken Sie im nächsten Fenster auf Add > Network Object (Hinzufügen > Netzwerkobjekt), und erstellen Sie ein Objekt mit der IP-Adresse '208.67.222.222'. Wiederholen Sie diesen Schritt, um ein Objekt mit der IP-Adresse "208.67.220.220" zu erstellen.

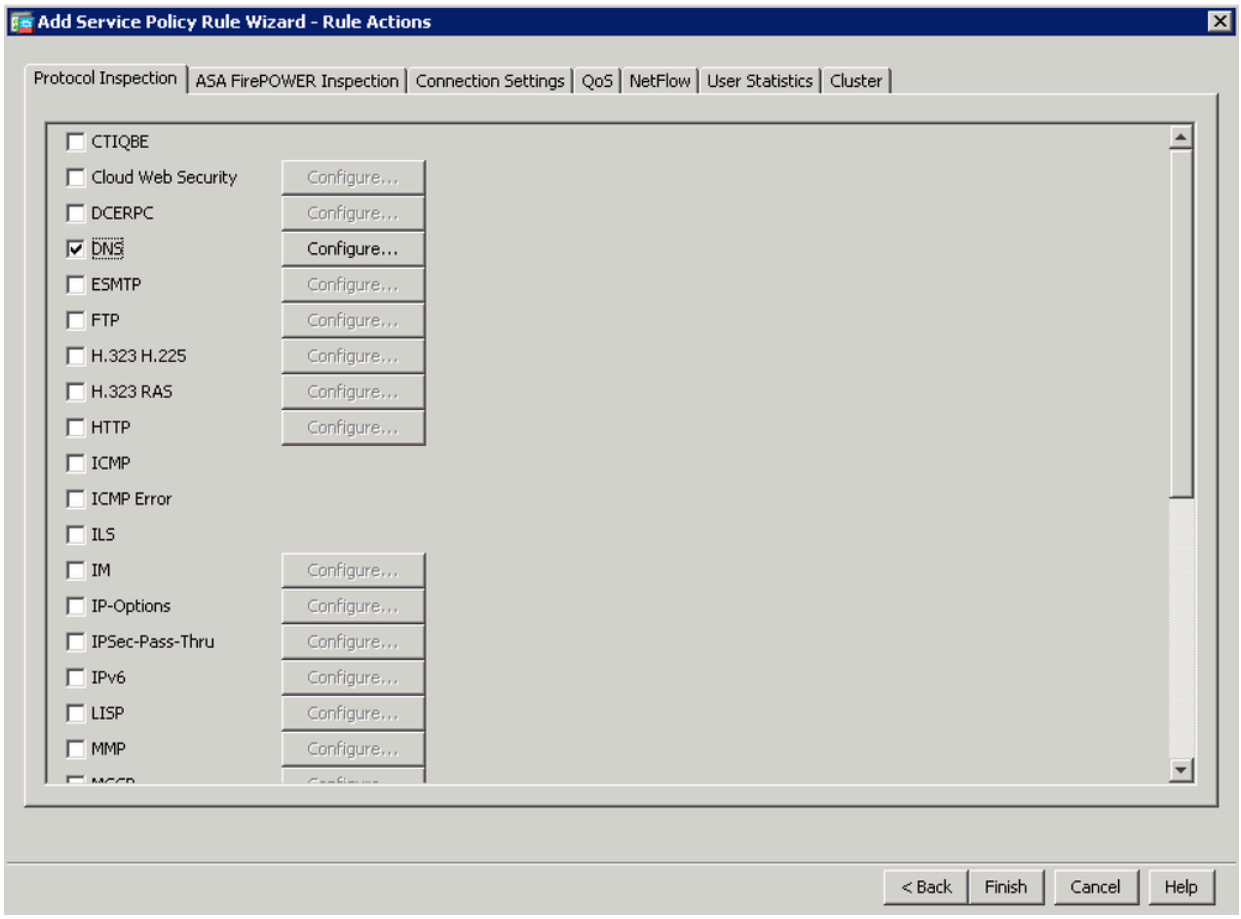

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

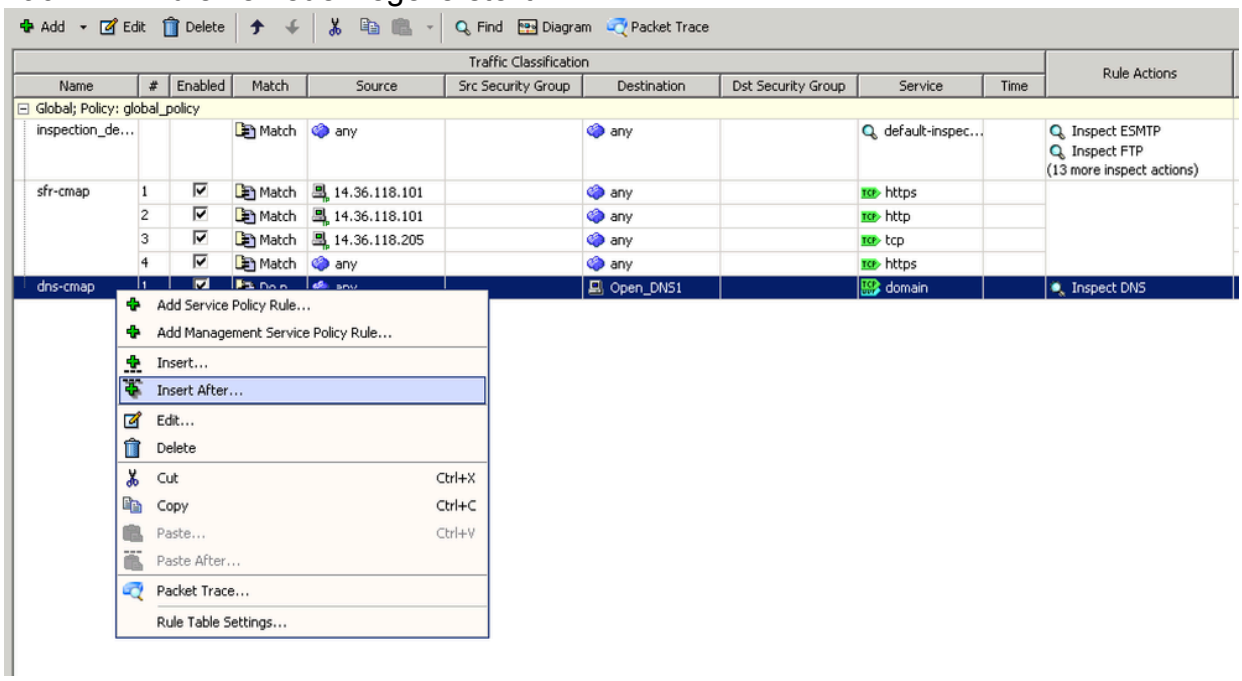
8. Fügen Sie beide Umbrella-Netzwerkobjekte dem Zielfeld hinzu, und klicken Sie auf OK.



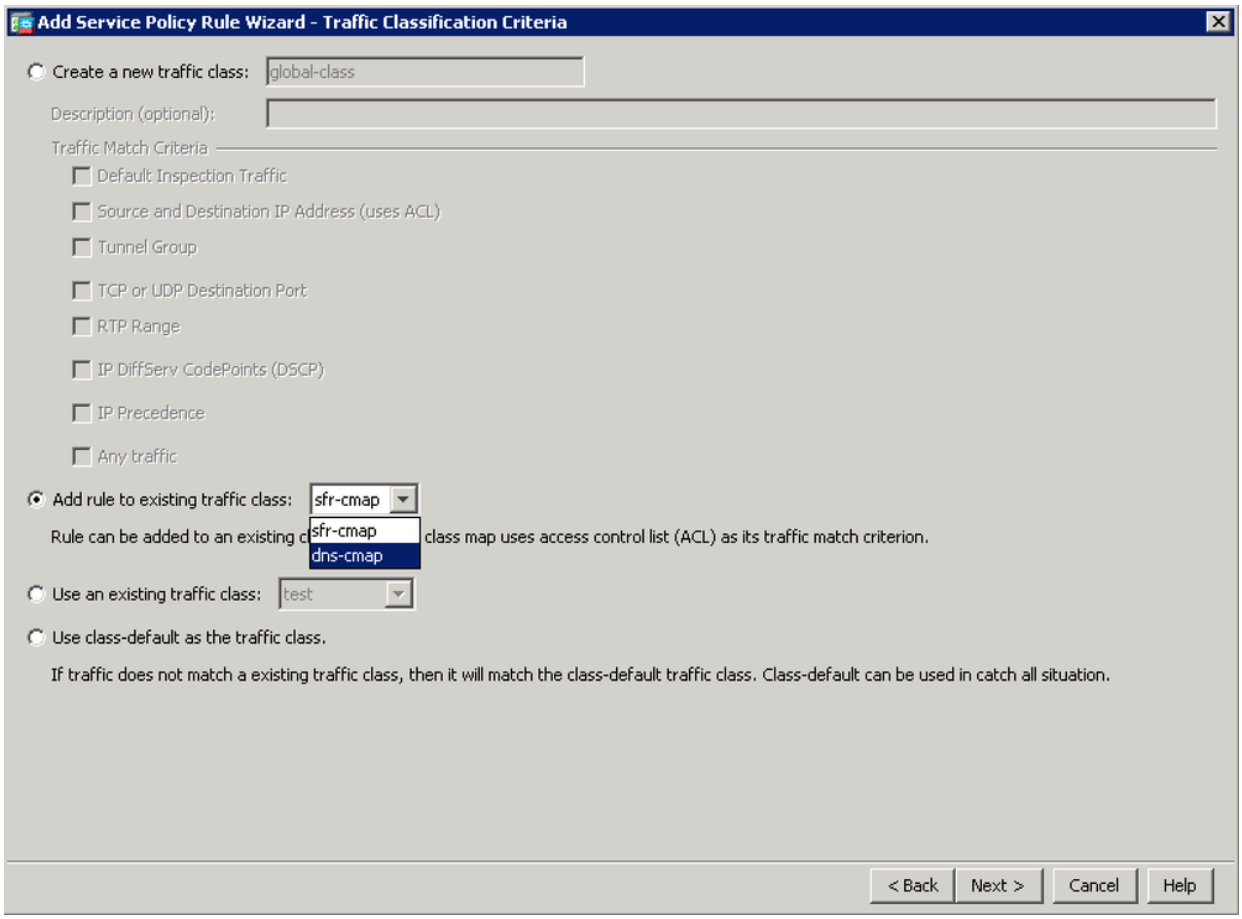
9. Aktivieren Sie im nächsten Fenster das Kontrollkästchen für "DNS", und klicken Sie auf Fertig stellen.



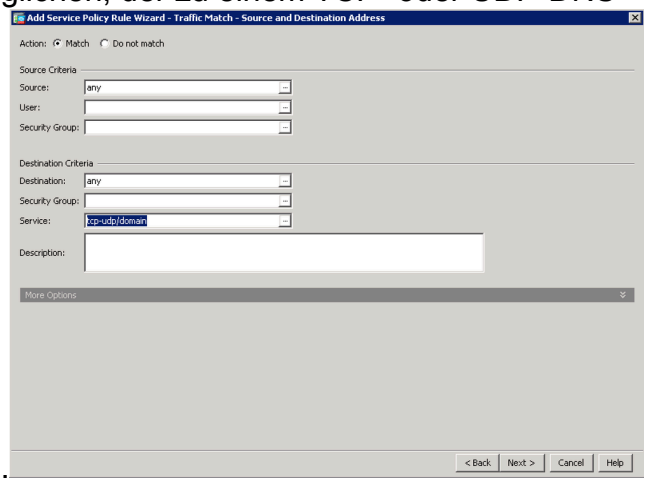
10. Die ASA zeigt jetzt die neue globale Richtlinie für "dns-cmap" an. Nun müssen Sie den verbleibenden Datenverkehr konfigurieren, der von der ASA überprüft wird. Dazu klicken Sie mit der rechten Maustaste auf 'dns-cmap' und wählen die Option "Einfügen nach...". wird eine neue Regel erstellt.



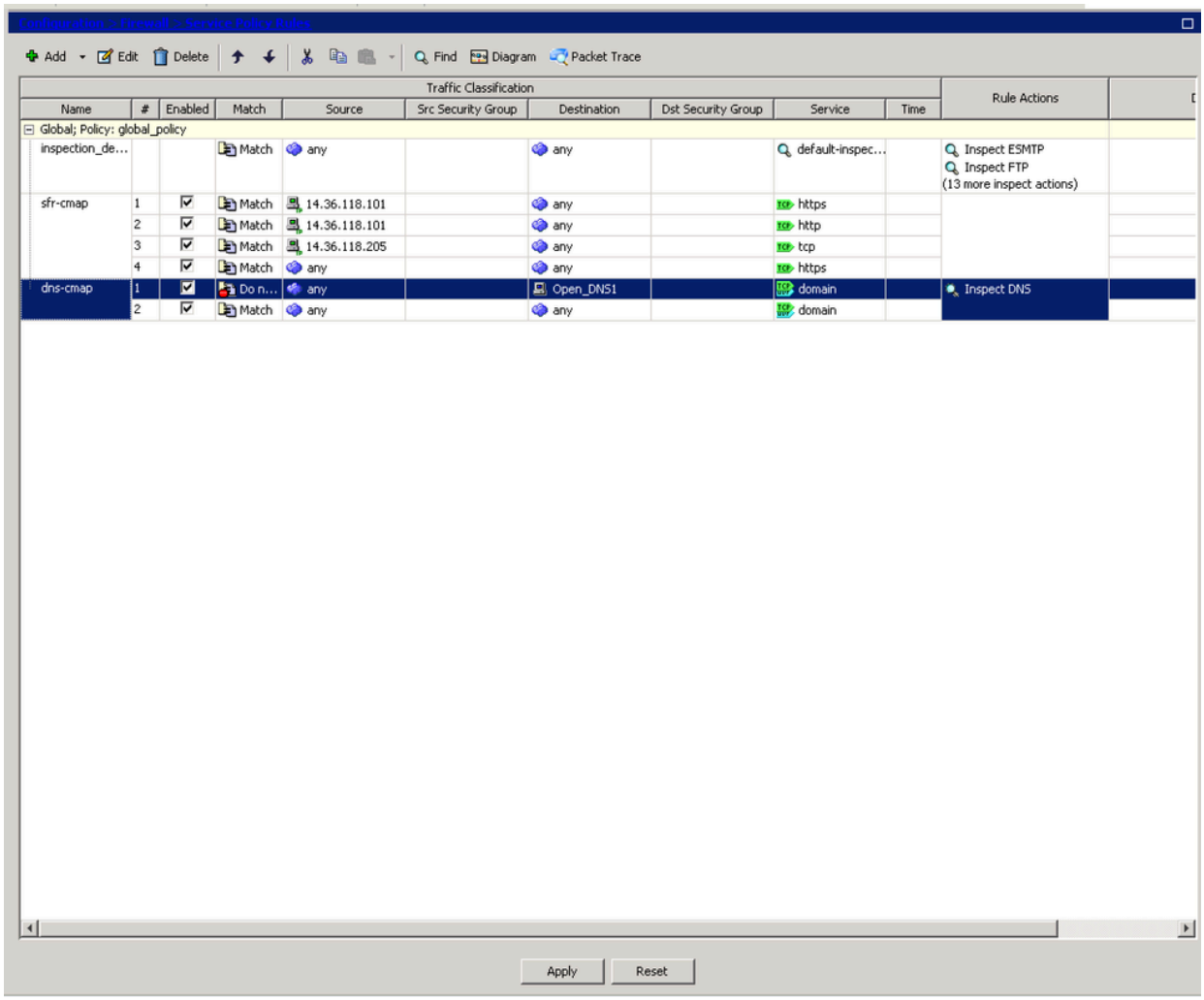
11. Klicken Sie im ersten Fenster auf "Weiter" und anschließend auf das Optionsfeld "Regel zu vorhandener Verkehrsklasse hinzufügen:". Wählen Sie "dns-cmap" aus dem Dropdown-Menü aus, und klicken Sie dann auf Weiter.



12. Belassen Sie die Aktion als 'Übereinstimmung'. Wählen Sie die Quelle, das Ziel und den Dienst für Datenverkehr aus, der der DNS-Überprüfung unterzogen wird. Hier wird z. B. Datenverkehr von einem Client abgeglichen, der zu einem TCP- oder UDP-DNS-Server geht. Klicken Sie auf Next (Weiter).



13. Lassen Sie die DNS-Option aktiviert, und klicken Sie auf Fertig stellen.
14. Klicken Sie unten im Fenster auf Apply (Anwenden).



Weitere Informationen

Wenn Sie DNScrypt deaktivieren möchten, statt ASA-Ausnahmen zu konfigurieren, wenden Sie sich an den Umbrella Support.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.