排除ASA防火墙阻止Umbrella虚拟设备的DNScyrpt功能故障

目录

简介

本文介绍如何排除ASA防火墙阻止DNScrypt功能的故障。

概述

Cisco ASA防火墙可以阻止Umbrella虚拟设备提供的DNScrypt功能。这会导致此Umbrella Dashboard警告：

> 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

在ASA防火墙日志中也可以看到以下错误消息：

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

DNSCrypt加密旨在保护DNS查询的内容，因此也可以阻止防火墙执行数据包检测。

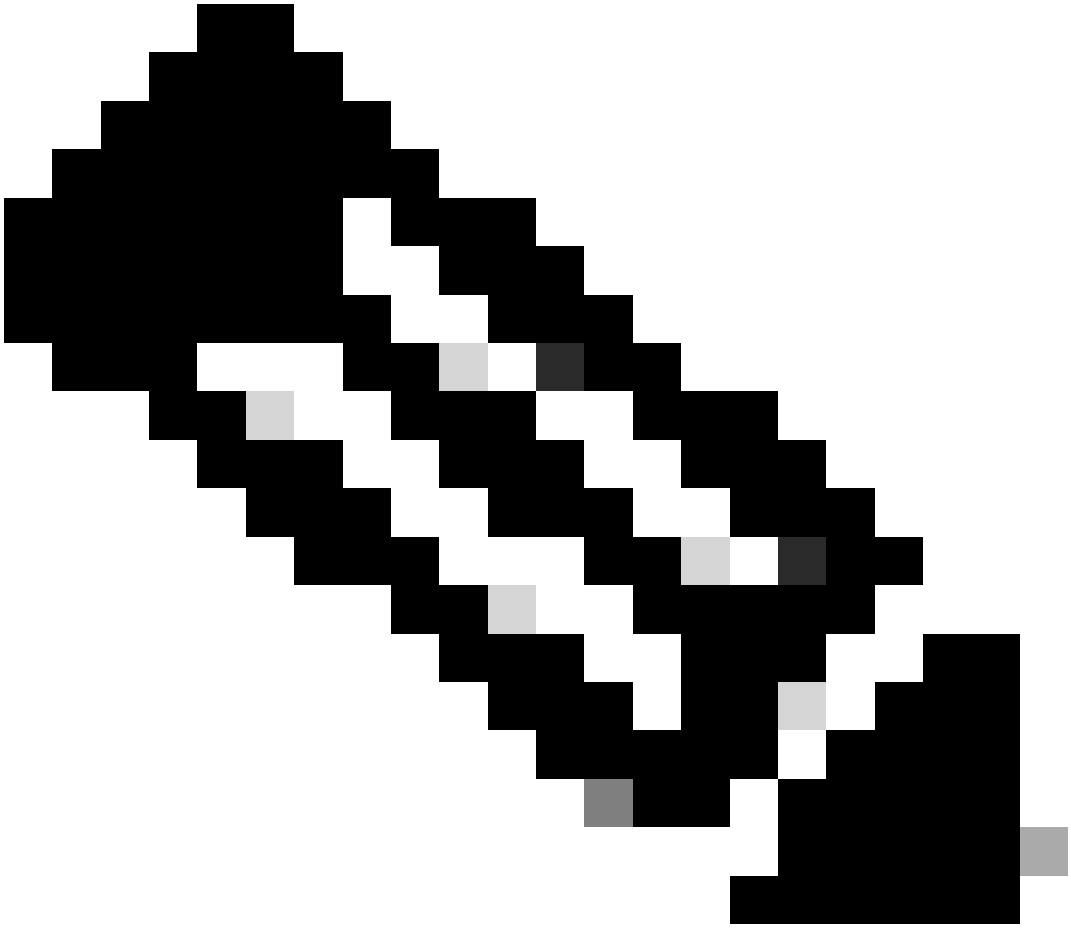
原因

这些错误不能导致任何用户面临DNS解析的影响。

虚拟设备发送测试查询以确定DNScrypt的可用性，而阻止的正是这些测试查询。但是，这些错误消息确实表明虚拟设备不会通过加密您公司的DNS流量来增加额外的安全性。

分辨率

我们建议对虚拟设备和Umbrella的DNS解析器之间的流量禁用DNS数据包检测。虽然这会禁用ASA上的日志记录和协议检查，但它通过允许DNS加密来增强安全性。



注意：这些命令仅供参考，建议在对生产环境进行任何更改之前咨询思科专家。
还要注意ASA上的此缺陷 可能会影响TCP上的DNS，这也会导致DNSCrypt出现问题：
CSCsm90809 DNS检测支持TCP上的DNS

数据包检测例外 — IOS命令

1. 创建名为“dns_inspect”的新ACL，其中包含的规则用于拒绝发往208.67.222.222和208.67.220.220的流量。
<#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. 删除ASA上的当前DNS检测策略。例如：

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

3. 创建与步骤1中创建的ACL匹配的类映#1:

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

4. 在global_policy下配置策略映射。这必须与步骤10中创建的类映射匹#3。启用DNS检测。

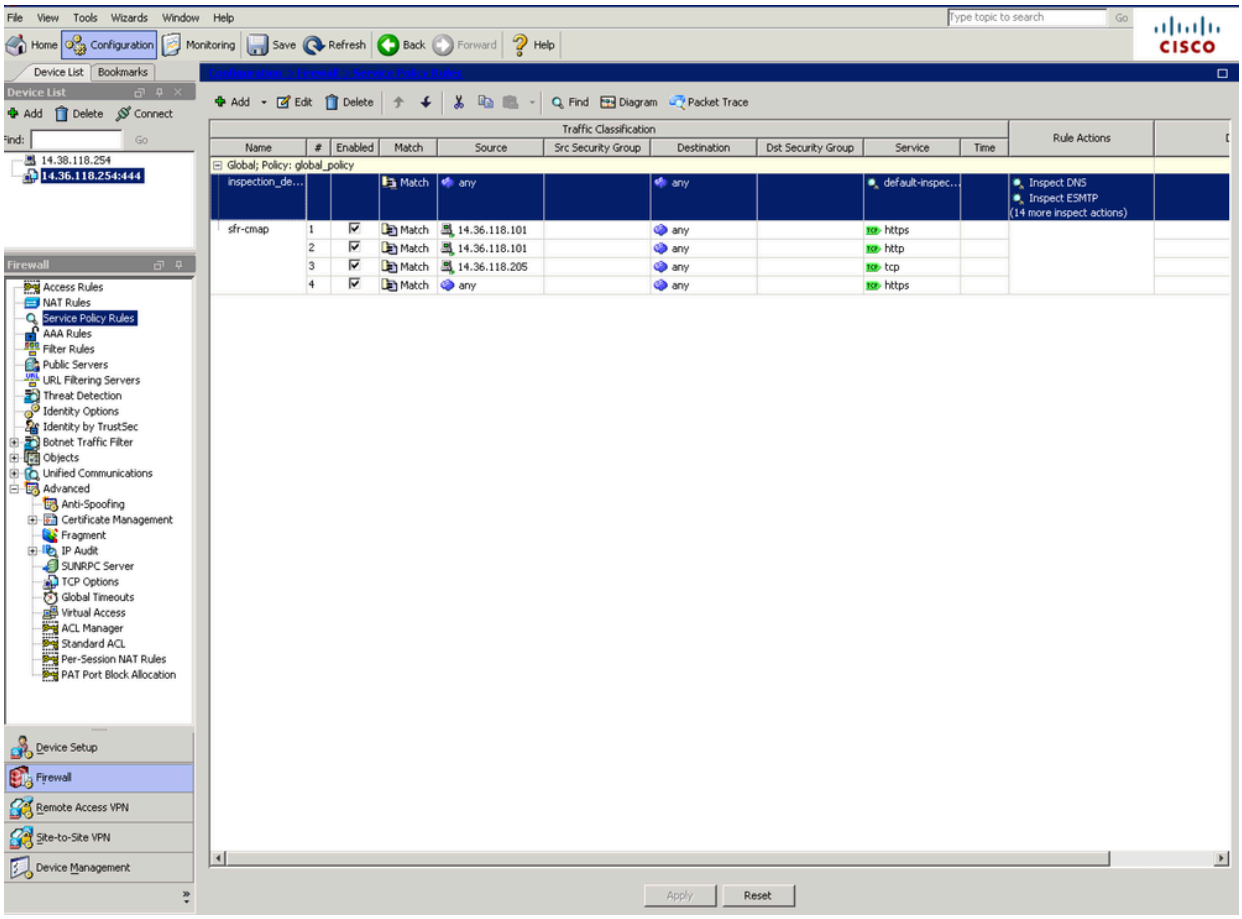
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. 启用后，您可以通过运行以下命令来验证流量是否正在达到例外情况：

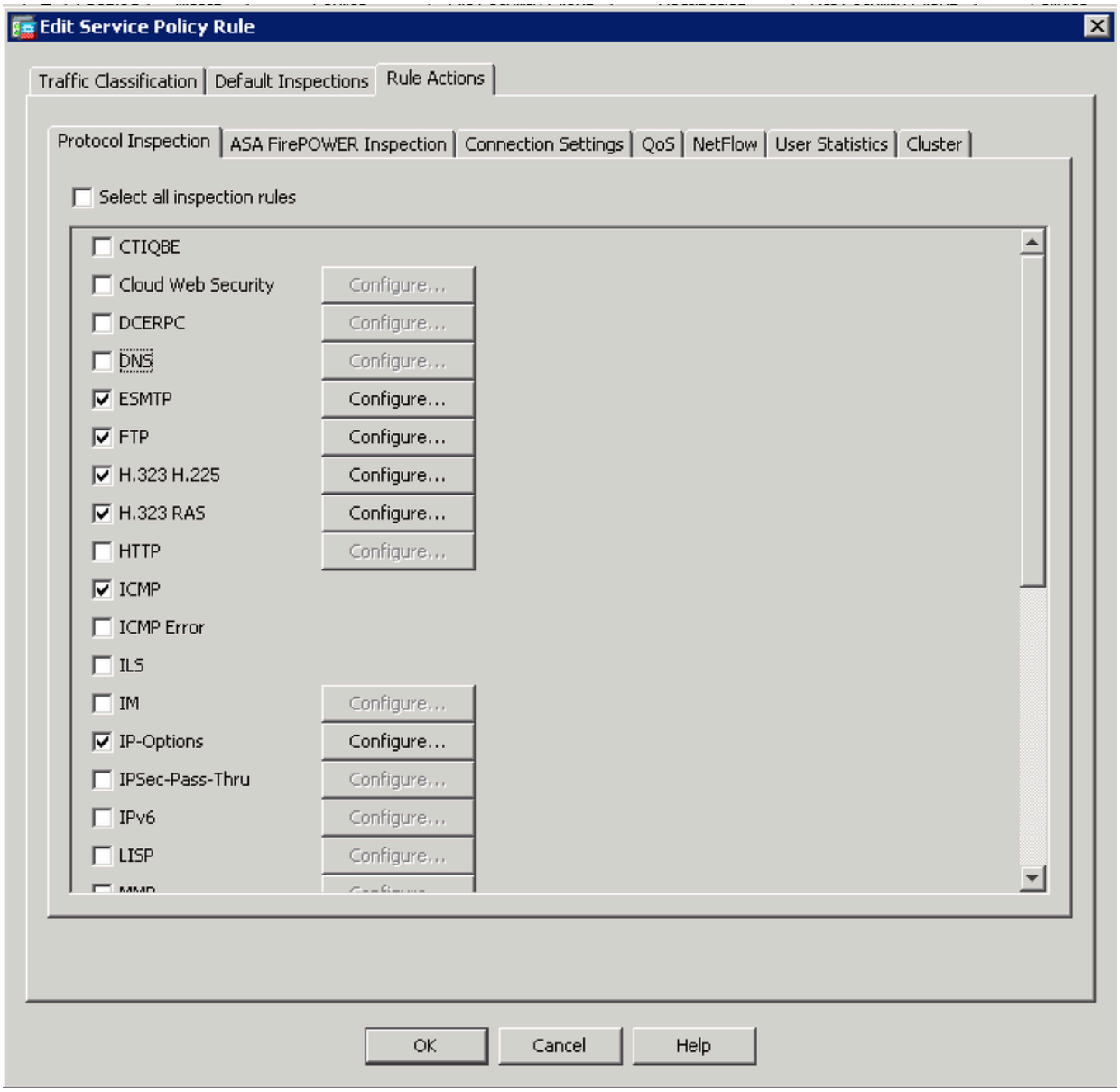
```
sh access-list dns_inspect
```

数据包检测例外 — ASDM接口

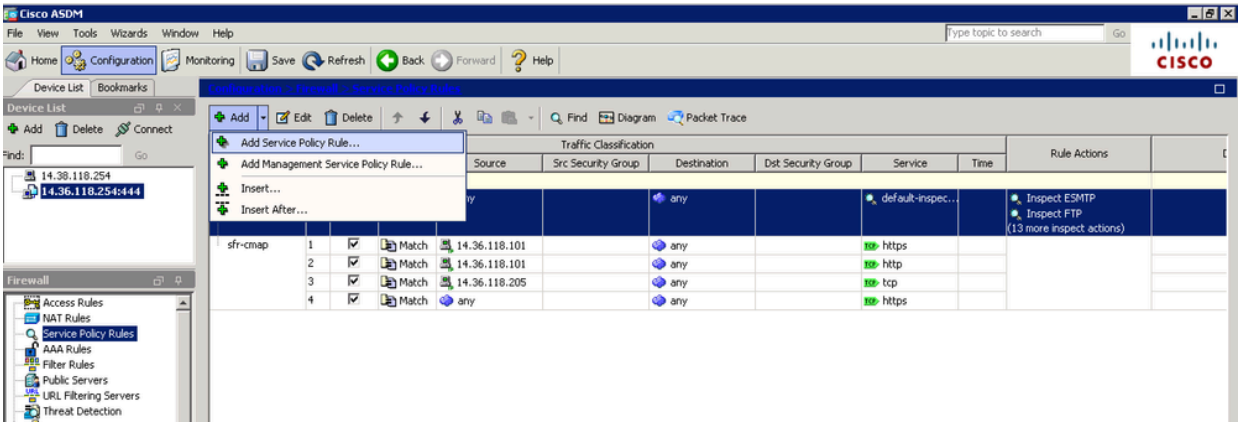
1. 首先禁用任何DNS数据包检测（如果适用）。此操作在Configuration > Firewall > Service Policy Rules中完成。



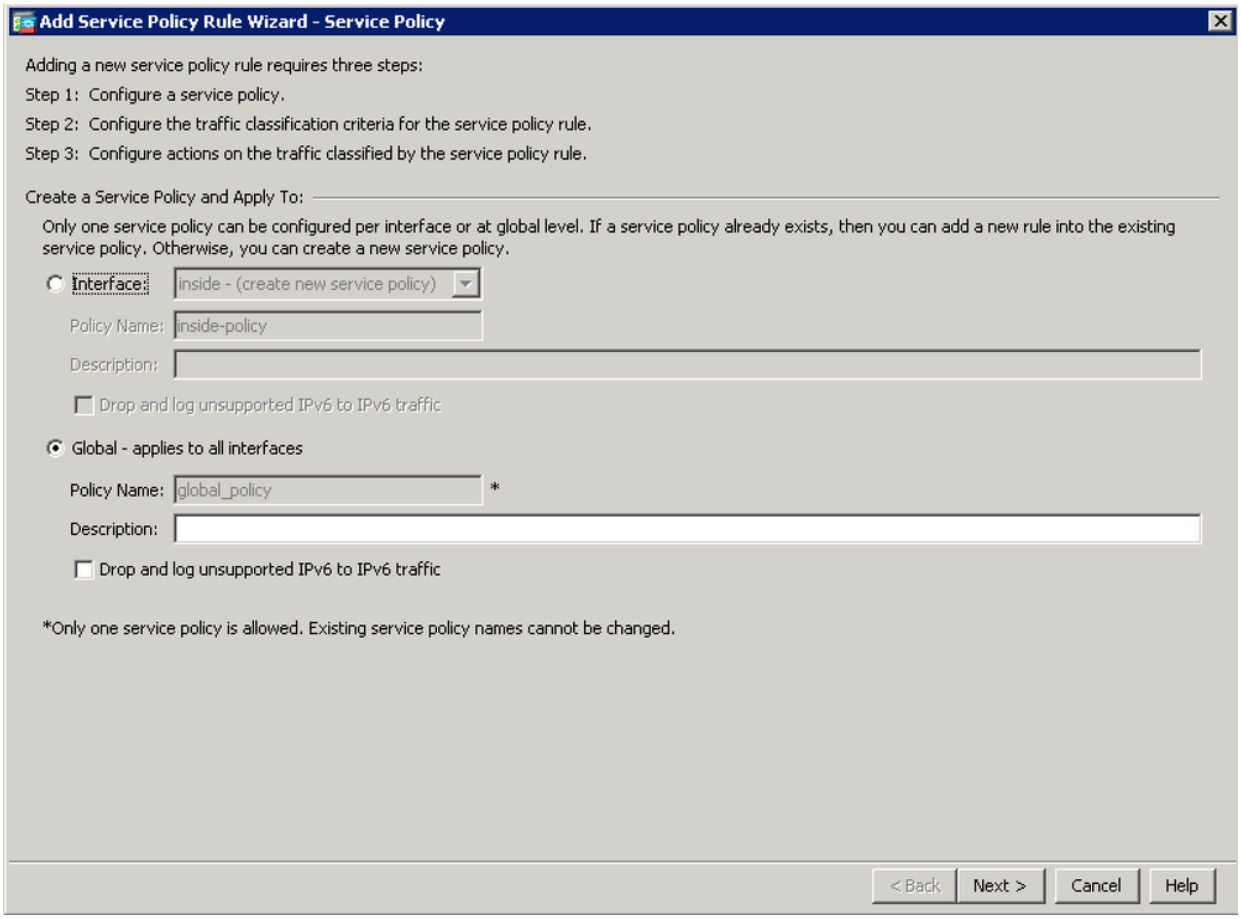
2. 在本示例中，DNS检测在Global Policy和“inspection_default”类下启用。突出显示它并单击Edit。在新窗口中，取消选中“Rule Action”（规则操作）选项卡下的“DNS”(DNS)复选框。



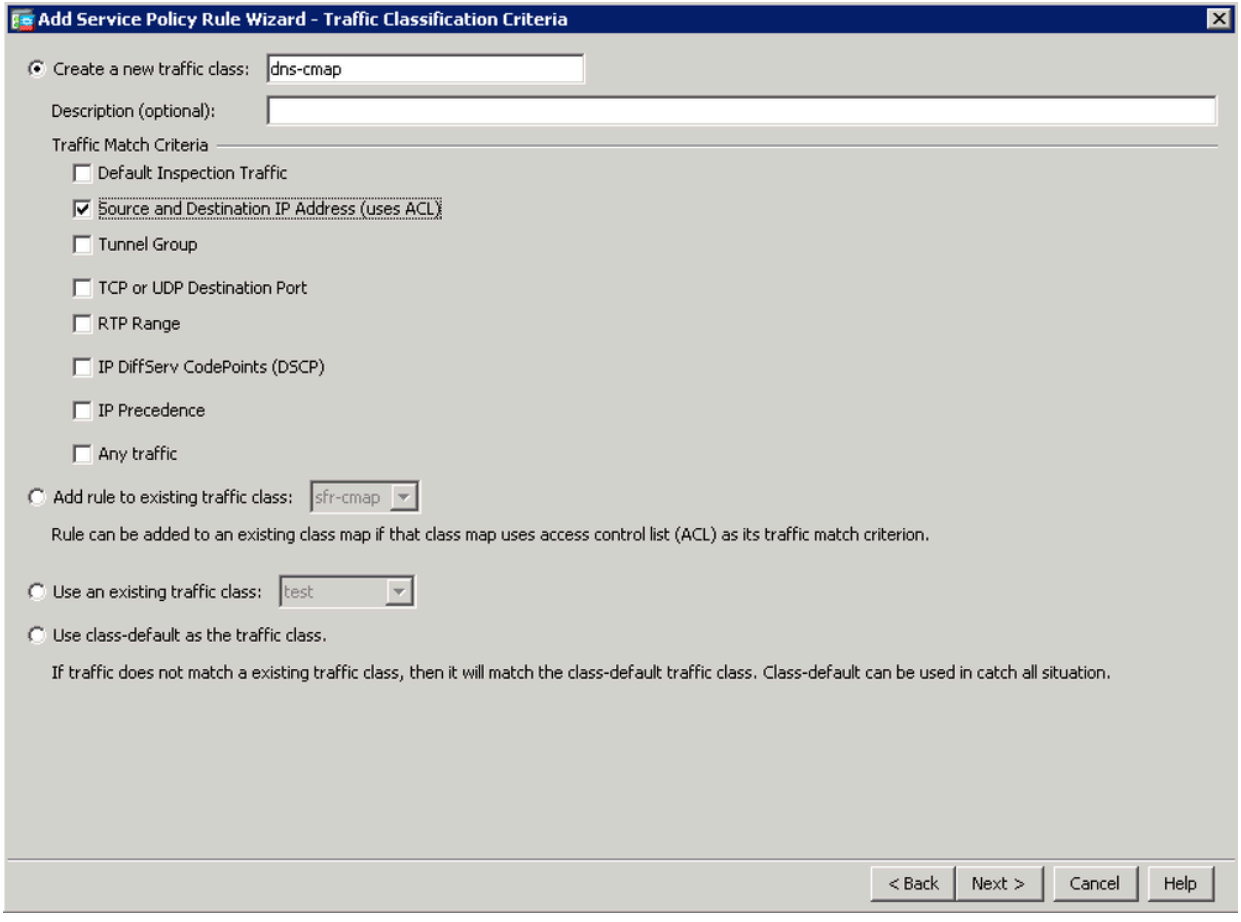
3. 现在，您可以重新配置DNS检测，此次额外免除流量。单击Add > Add Service Policy Rule...



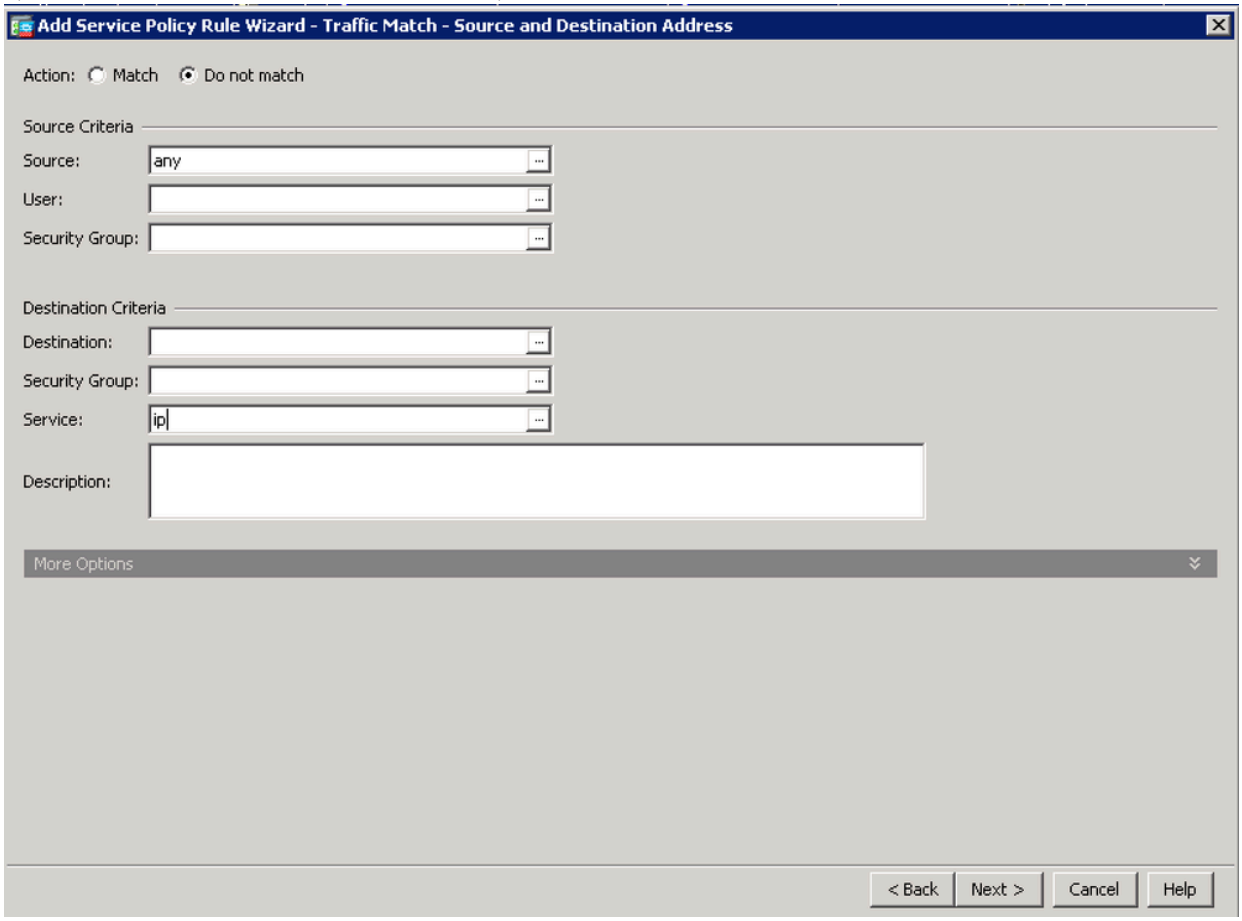
4. 选择“全局 — 应用于所有接口”，然后单击下一步（如果需要，您也可以将此功能应用于特定接口）。



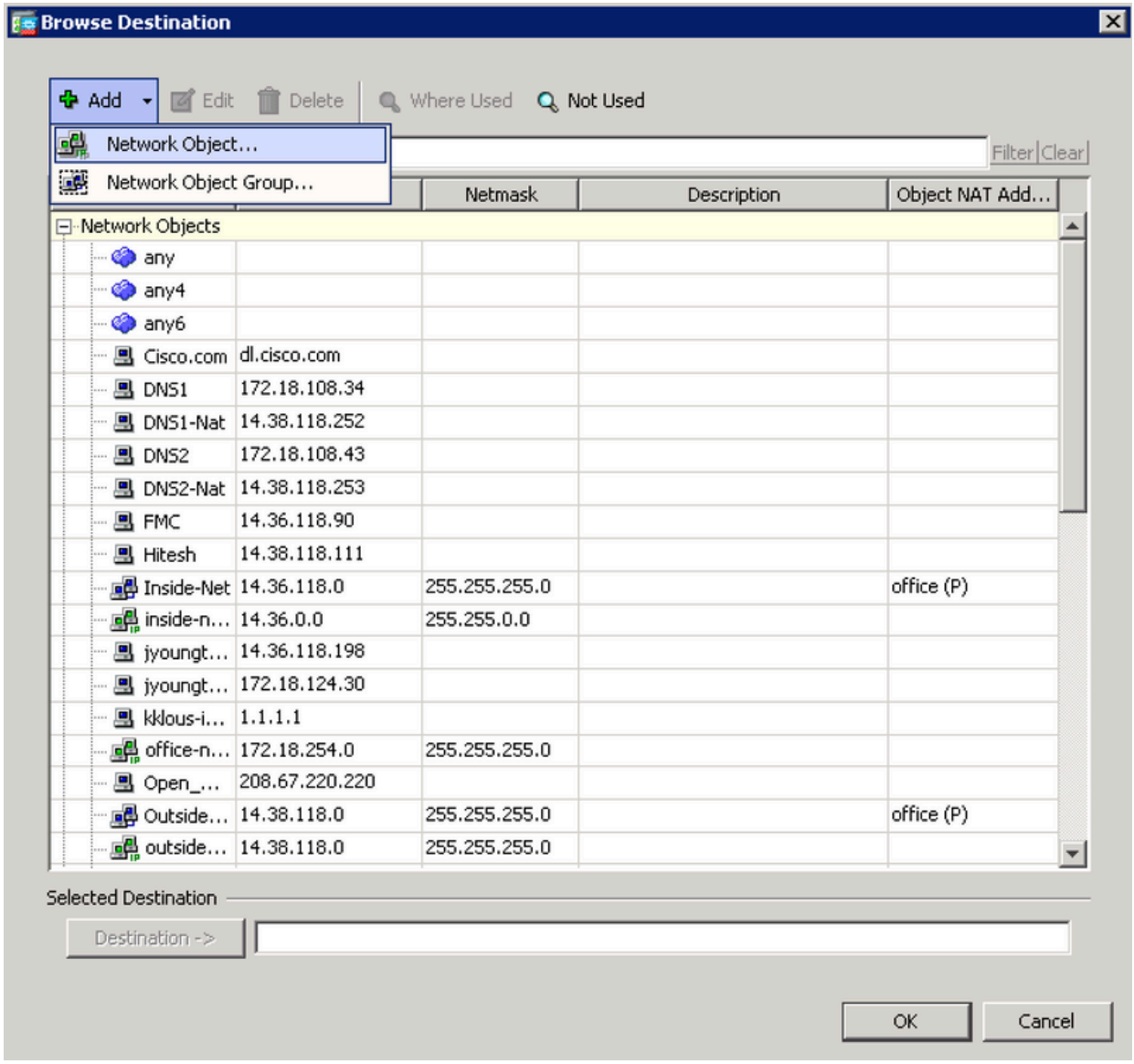
5. 为类映射指定名称（例如“dns-cmap”），并选中选项“源和目标IP地址（使用ACL）”。单击“下一步”.

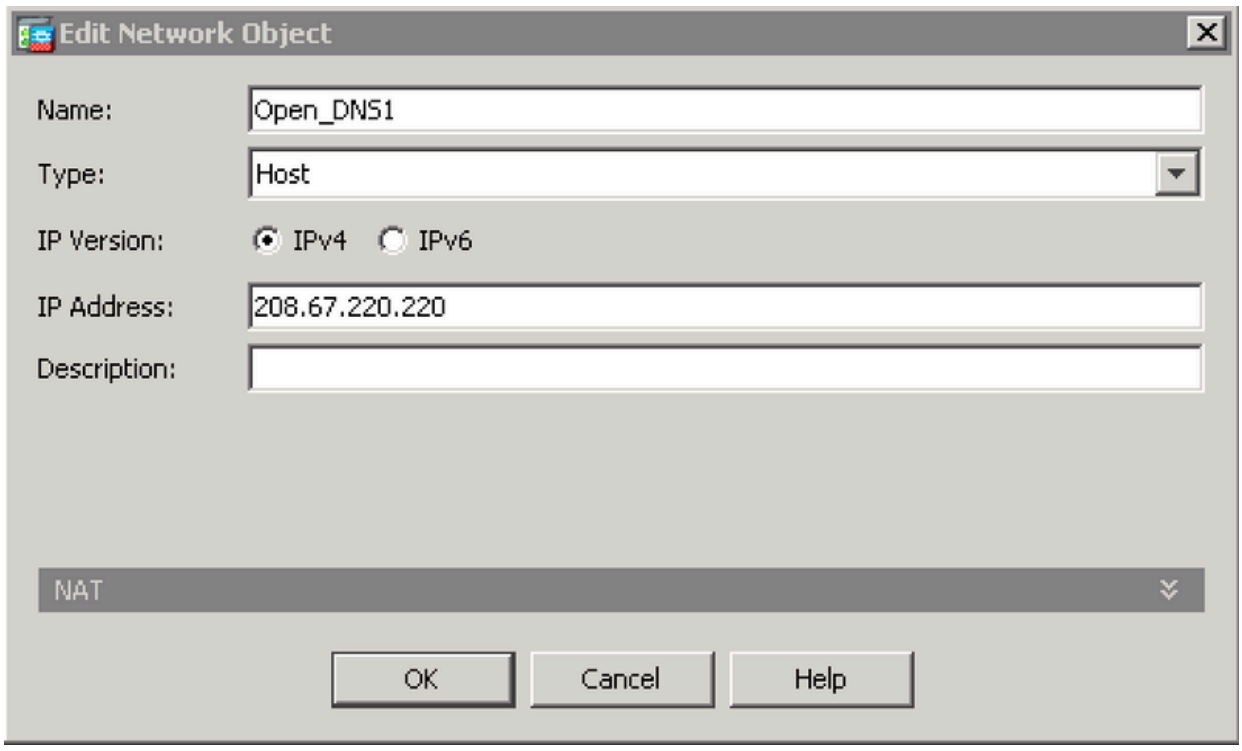


6. 首先使用“不匹配”操作配置您不希望检查的流量。
   对于Source，您可以使用“any”选项免除发往Umbrella的DNS服务器的所有流量。或者，您可以在此处创建网络对象定义，以仅免除特定虚拟设备IP地址。

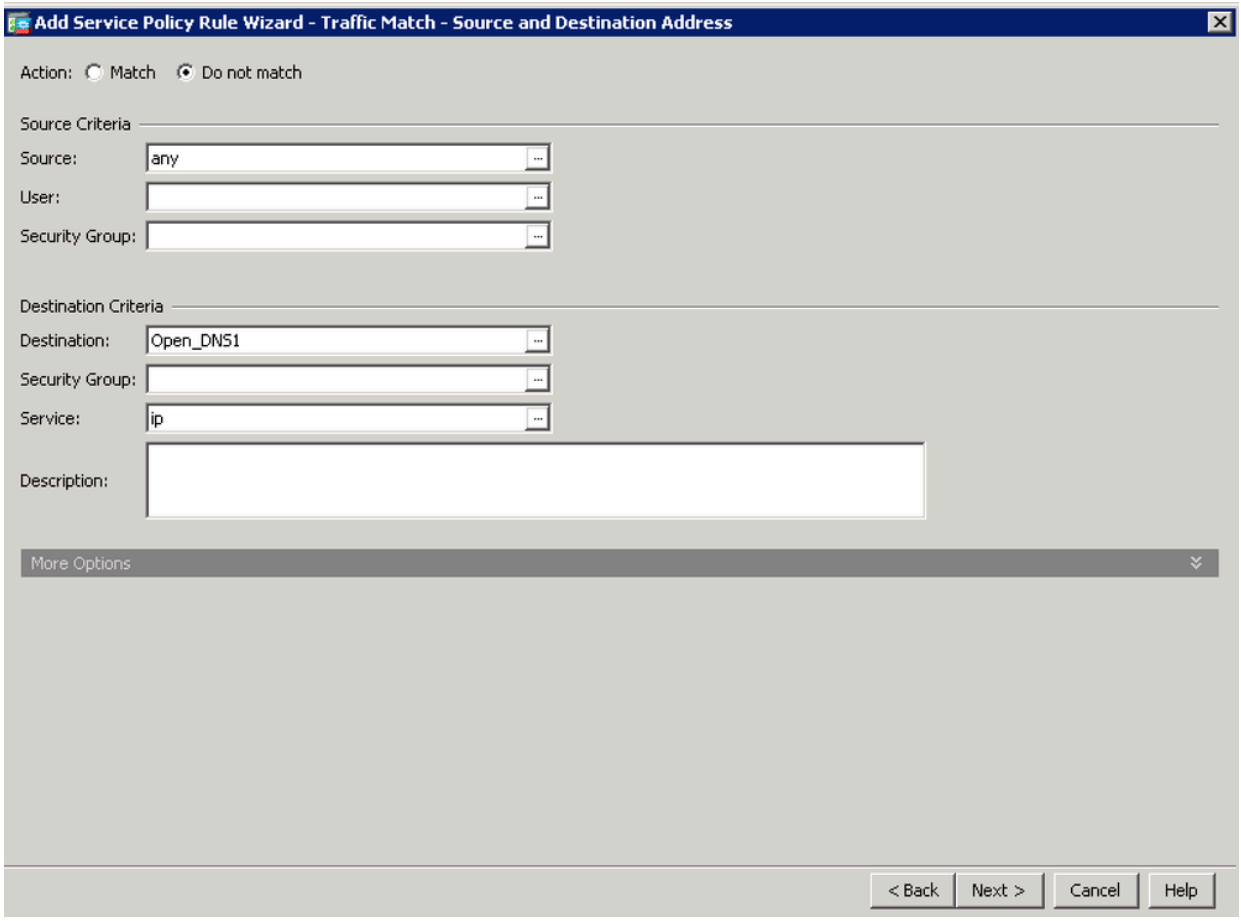


7. 单击Destination字段上的……。在下一个窗口中，单击Add > Network Object，并创建IP地址为“208.67.222.222”的对象。 重复此步骤，创建IP地址为“208.67.220.220”的对象。

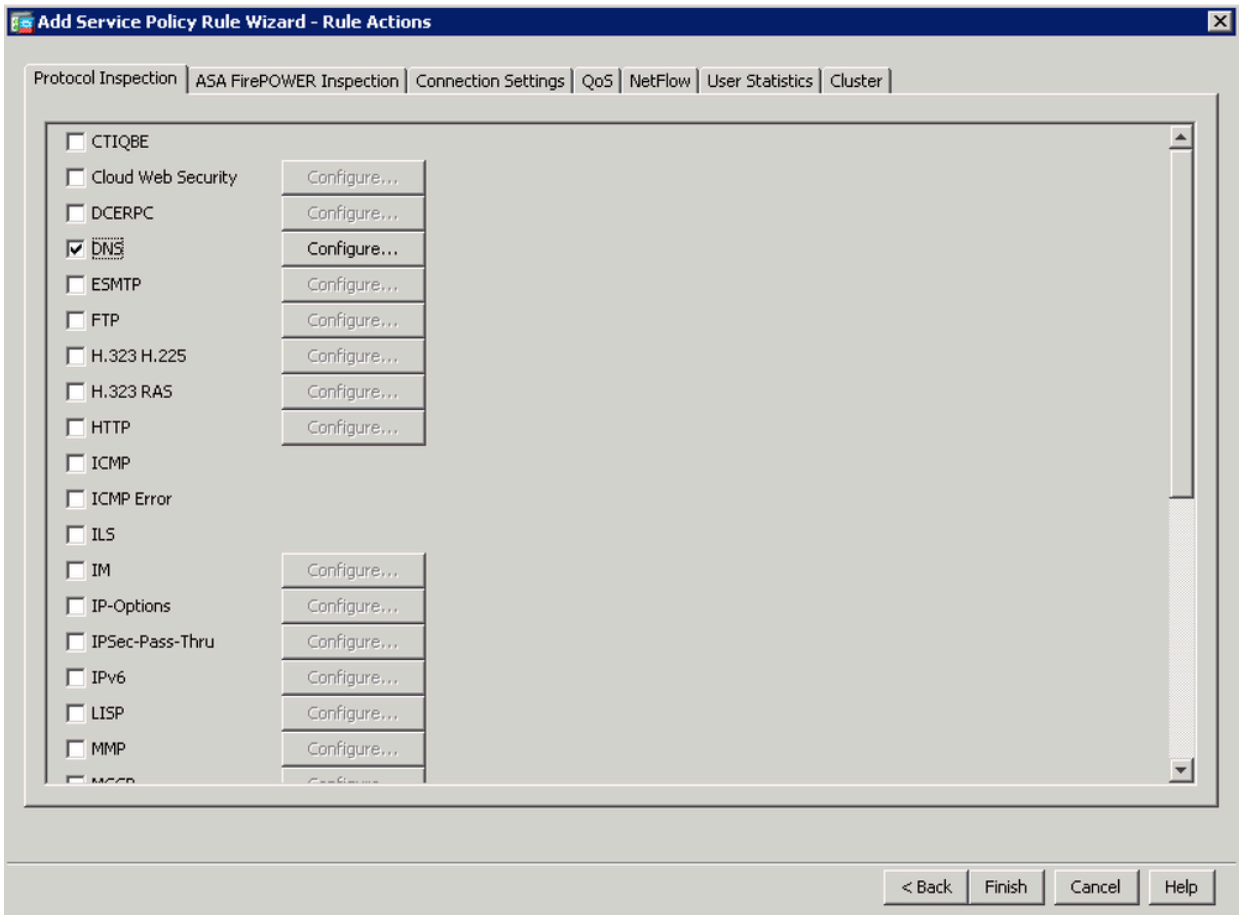

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

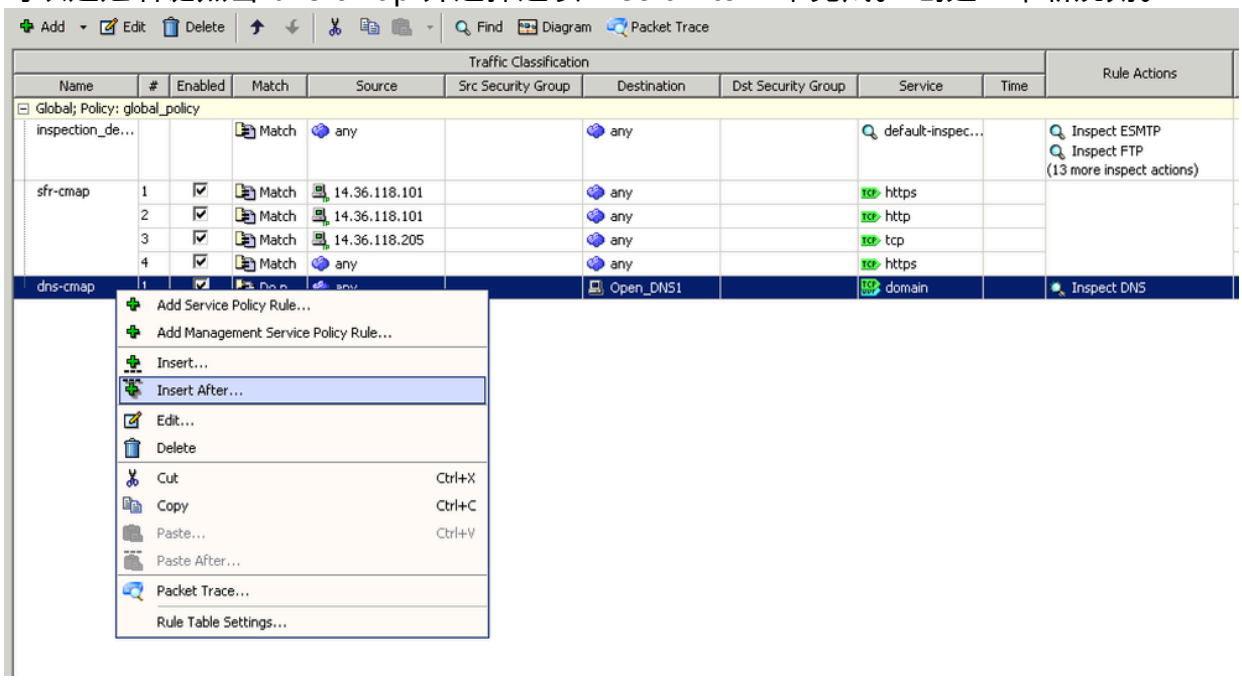
8. 将两个Umbrella网络对象添加到Destination字段，然后单击OK。



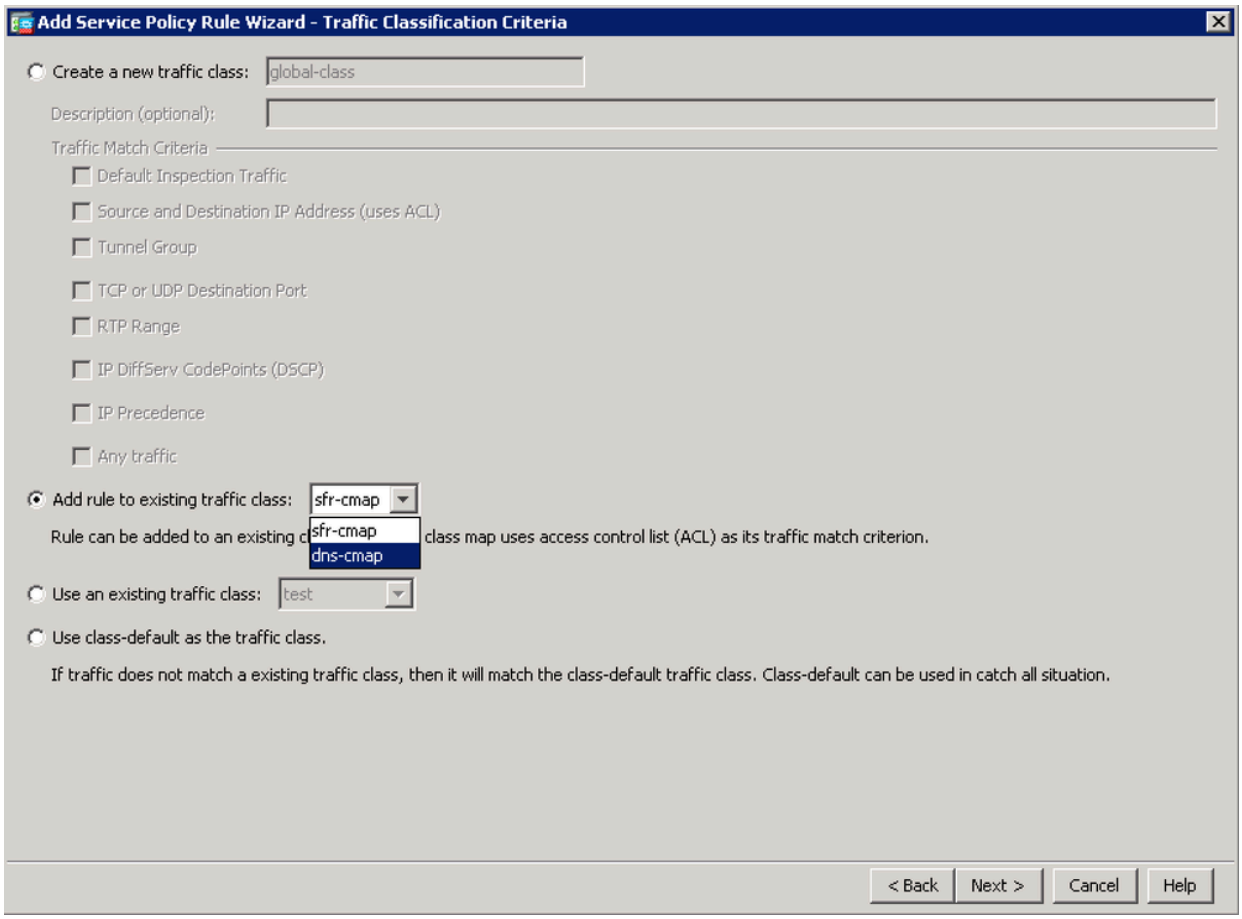
9. 在下一个窗口中，选中“DNS”复选框，然后单击Finish。



10. ASA现在显示“dns-cmap”的新全局策略。 现在，您需要配置由ASA检查的剩余流量。这可以通过右键点击“dns-cmap”并选择选项“Insert After..”来完成。 创建一个新规则。

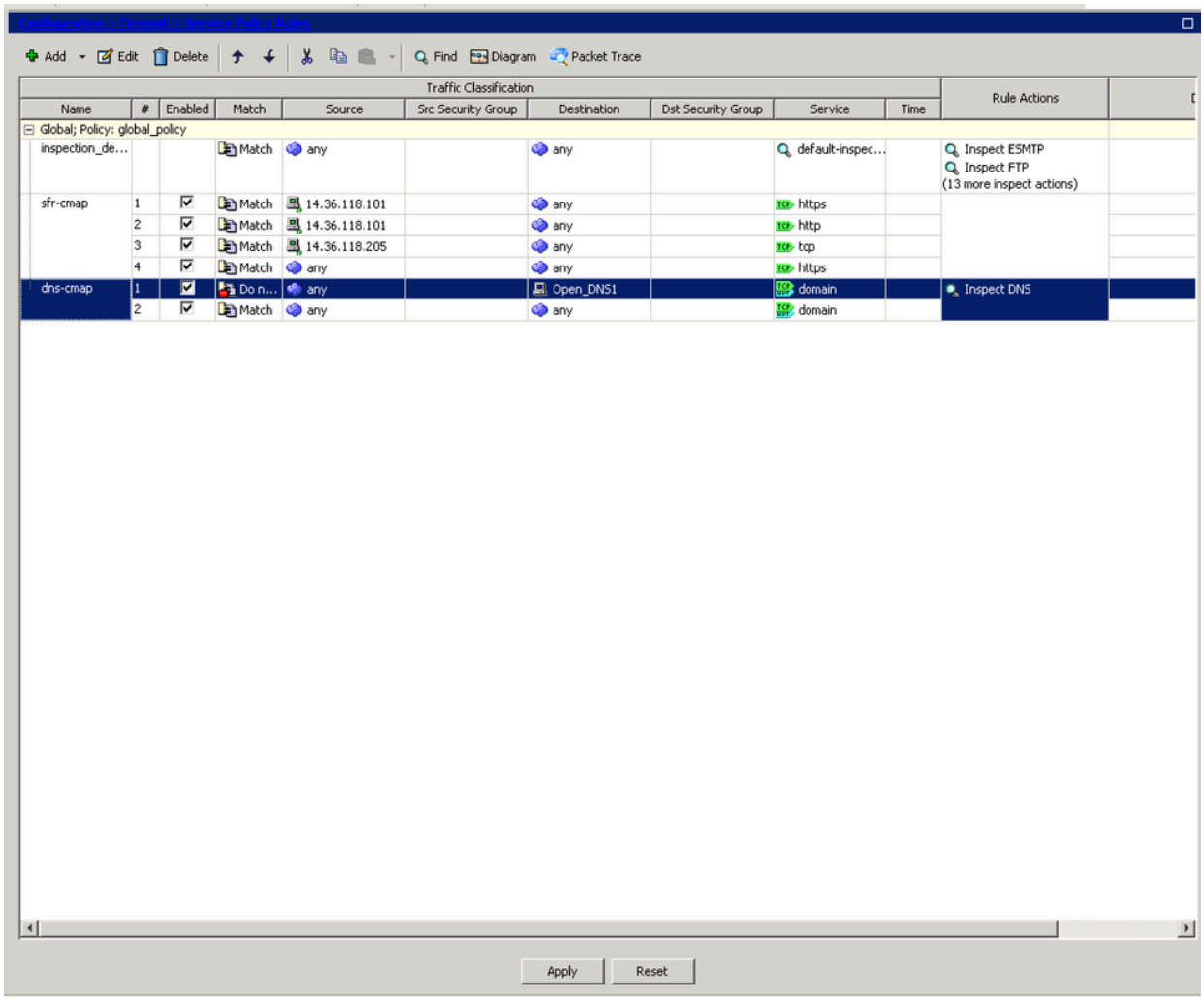


11. 在第一个窗口中单击Next，然后选中“Add rule to existing traffic class：”单选按钮。从下拉菜单中选择“dns-cmap”，然后单击Next。



12. 将Action保留为Match。 选择接受DNS检查的流量的源、目标和服务。例如，在此处，我们将匹配来自任何客户端的流量传输到任何TCP或UDP DNS服务器。单击 Next。

13. 选中“DNS”选项，然后单击Finish。
14. 单击窗口底部的Apply。



更多信息

如果您希望禁用DNScrypt而不是配置ASA免除，请联系Umbrella支持。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。