Umbrella仮想アプライアンスからのDNScyrpt機能をブロックするASAファイアウォールのトラブルシューティング

内容

はじめに

この記事では、DNScrypt機能をブロックするASAファイアウォールをトラブルシューティングする方法について説明します。

概要

Cisco ASAファイアウォールは、Umbrella仮想アプライアンスが提供するDNScrypt機能をブロックできます。この結果、次のUmbrellaダッシュボード警告が表示されます。

> 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

次のエラーメッセージは、ASAファイアウォールのログでも確認できます。

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

DNSCrypt暗号化は、DNSクエリの内容を保護するように設計されているため、ファイアウォールによるパケットインスペクションの実行も阻止されます。

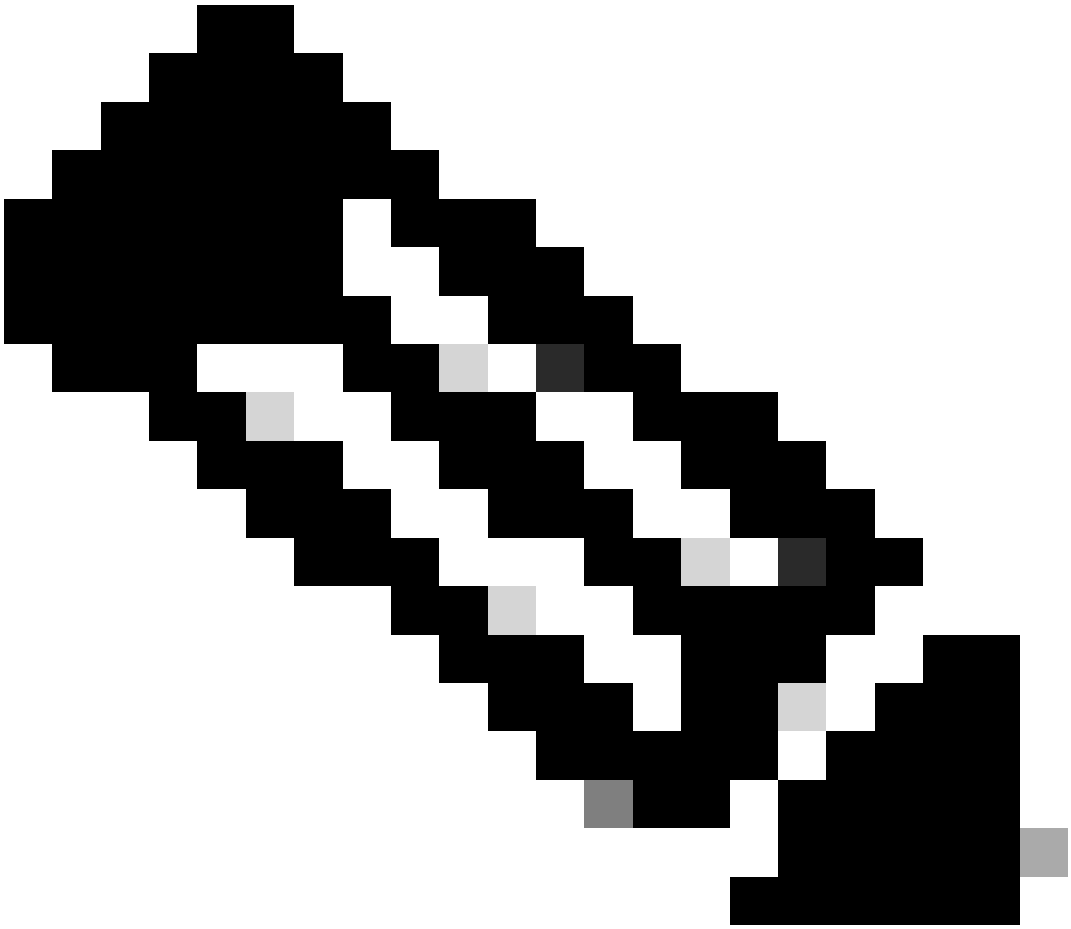
原因

これらのエラーが発生しても、DNS解決にユーザが影響を受けることはありません。

仮想アプライアンスは、テストクエリを送信してDNScryptの可用性を判断します。ブロックされるのは、テストクエリです。ただし、これらのエラーメッセージは、仮想アプライアンスが企業のDNSトラフィックを暗号化してセキュリティを強化していないことを示しています。

解決方法

仮想アプライアンスとUmbrellaのDNSリゾルバ間のトラフィックに対しては、DNSパケットインスペクションを無効にすることを推奨します。これによりASAでのロギングとプロトコルインスペクションは無効になりますが、DNS暗号化を許可することでセキュリティが強化されます。



注：これらのコマンドは説明のみを目的としているため、実稼働環境を変更する前にシスコの専門家に相談することを推奨します。
また、ASAでは、この不具合に注意してください はTCP上のDNSに影響を与える可能性があり、DNSCryptの問題を引き起こす可能性もあります。
CSCsm90809:DNS over TCPのDNSインスペクションサポート

パケット検査の例外 – IOSコマンド

1. 208.67.222.222および208.67.220.220へのトラフィックを拒否するルールを使用して、「dns_inspect」という名前の新しいACLを作成します。
   <#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. ASAの現在のDNSインスペクションポリシーを削除します。例：

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

3. 手順#1で作成したACLと一致するクラスマップを作成します。

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

4. global_policyでポリシーマップを設定します。これは、ステップ#3で作成したクラスマップと一致している必要があります。DNSインスペクションを有効にします。

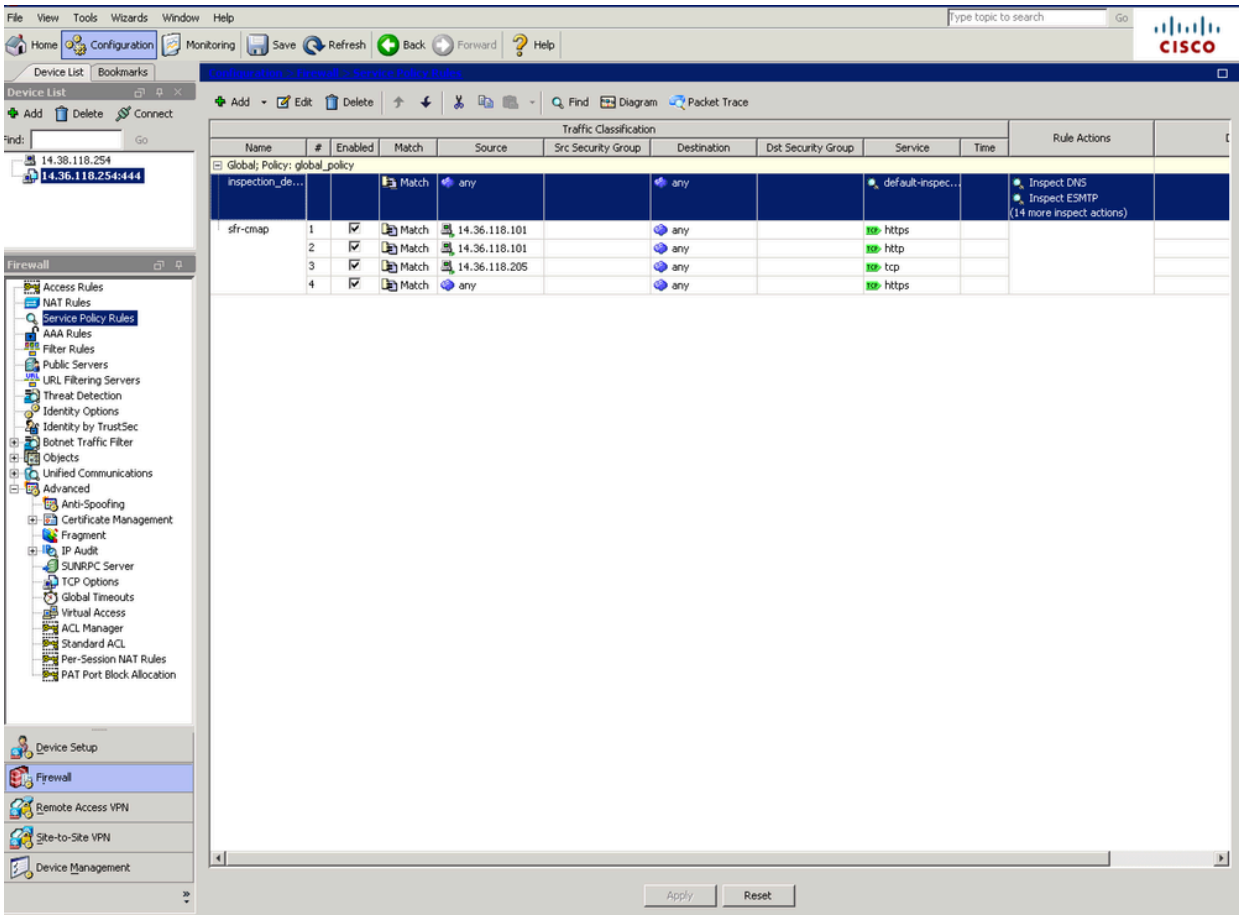
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. 有効にすると、次のコマンドを実行して、トラフィックが除外に一致していることを確認できます。

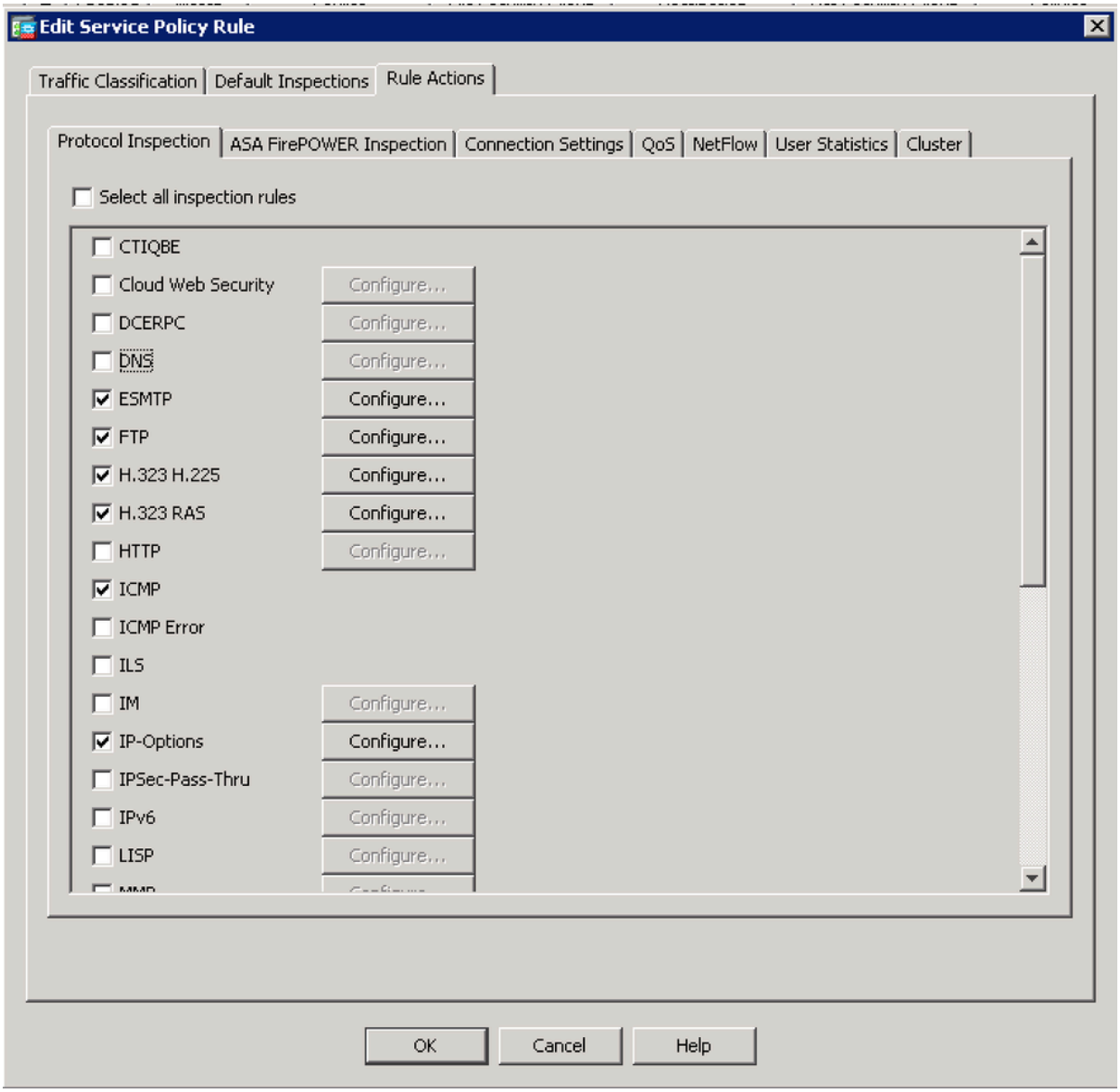
```
sh access-list dns_inspect
```

パケット検査の例外 – ASDMインターフェイス

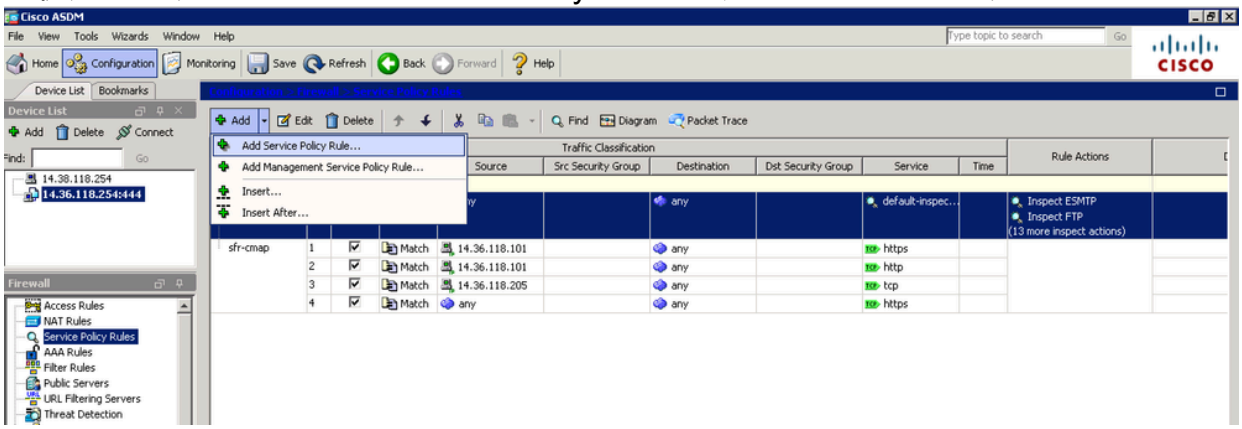
1. 必要に応じて、まずDNSパケットインスペクションを無効にします。これは、Configuration > Firewall > Service Policy Rulesで行います。



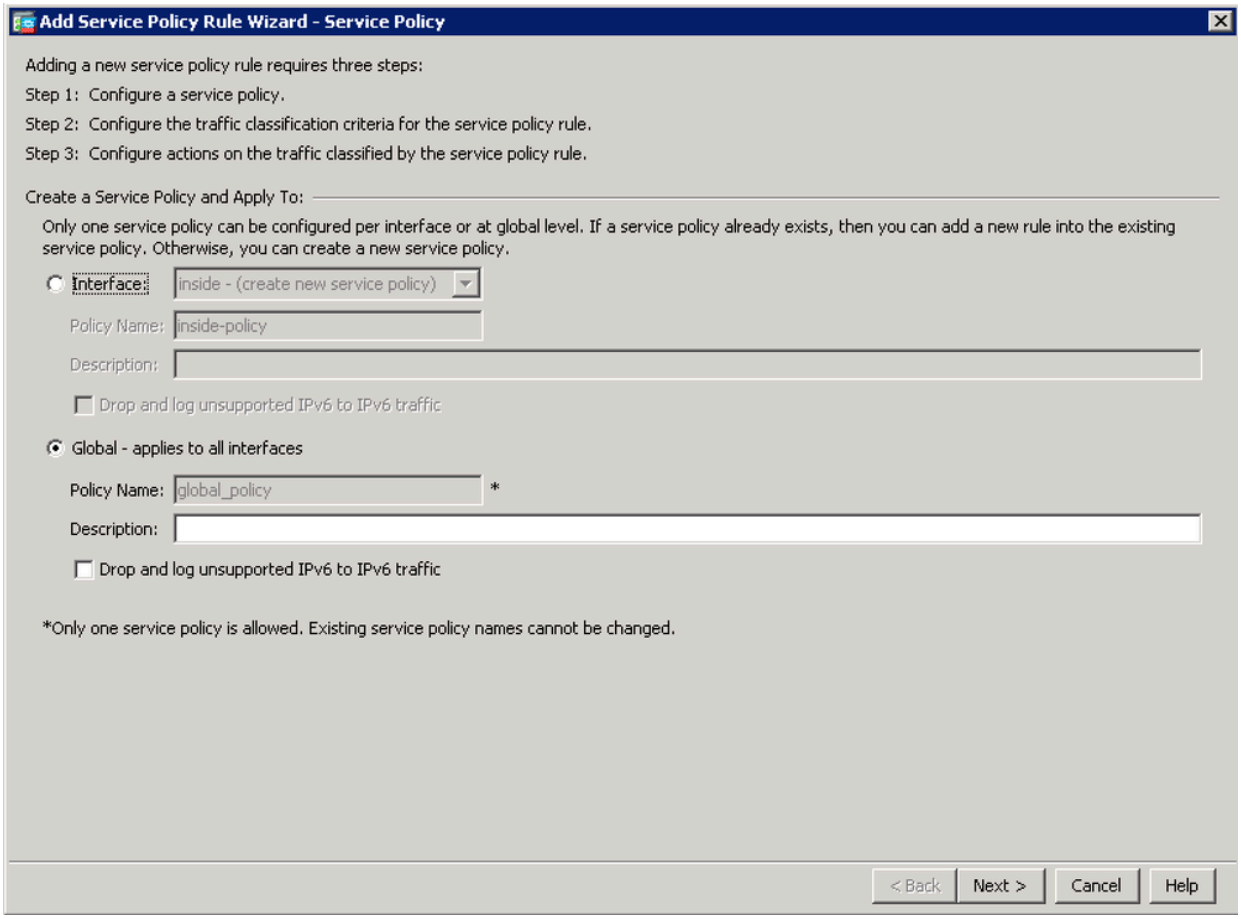
2. この例では、グローバルポリシーと「inspection_default」クラスでDNSインスペクションが有効になっています。これを強調表示して、Editをクリックします。新しいウィンドウで、「Rule Action」タブの下の「DNS」のチェックボックスをオフにします。



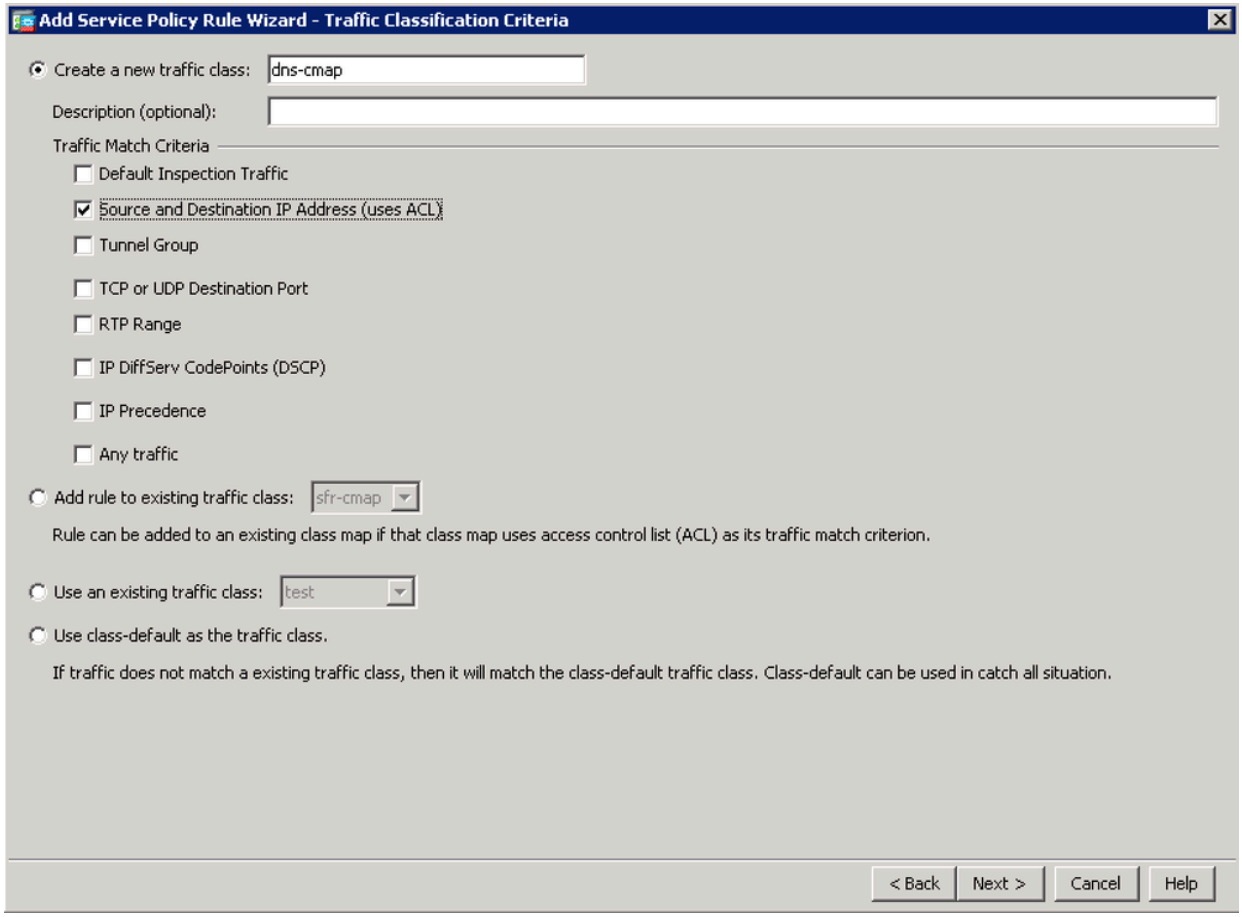
3. これで、DNSインスペクションを再設定できます。今回は、追加のトラフィック除外を使用します。Add > Add Service Policy Rule...の順にクリックします。



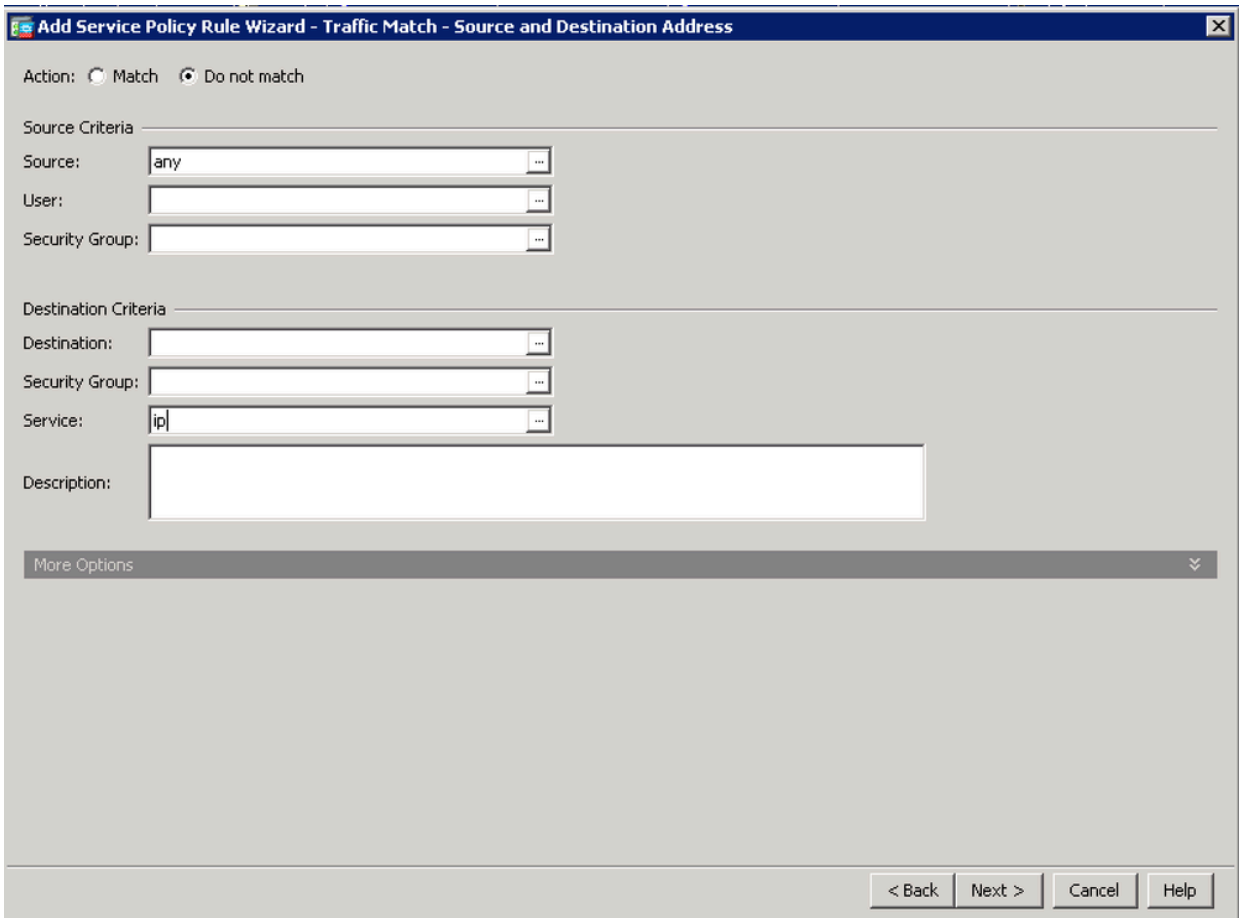
4. 「Global - Applies to all interfaces」を選択し、Nextをクリックします（必要に応じて、特定のインターフェイスに適用することもできます）。



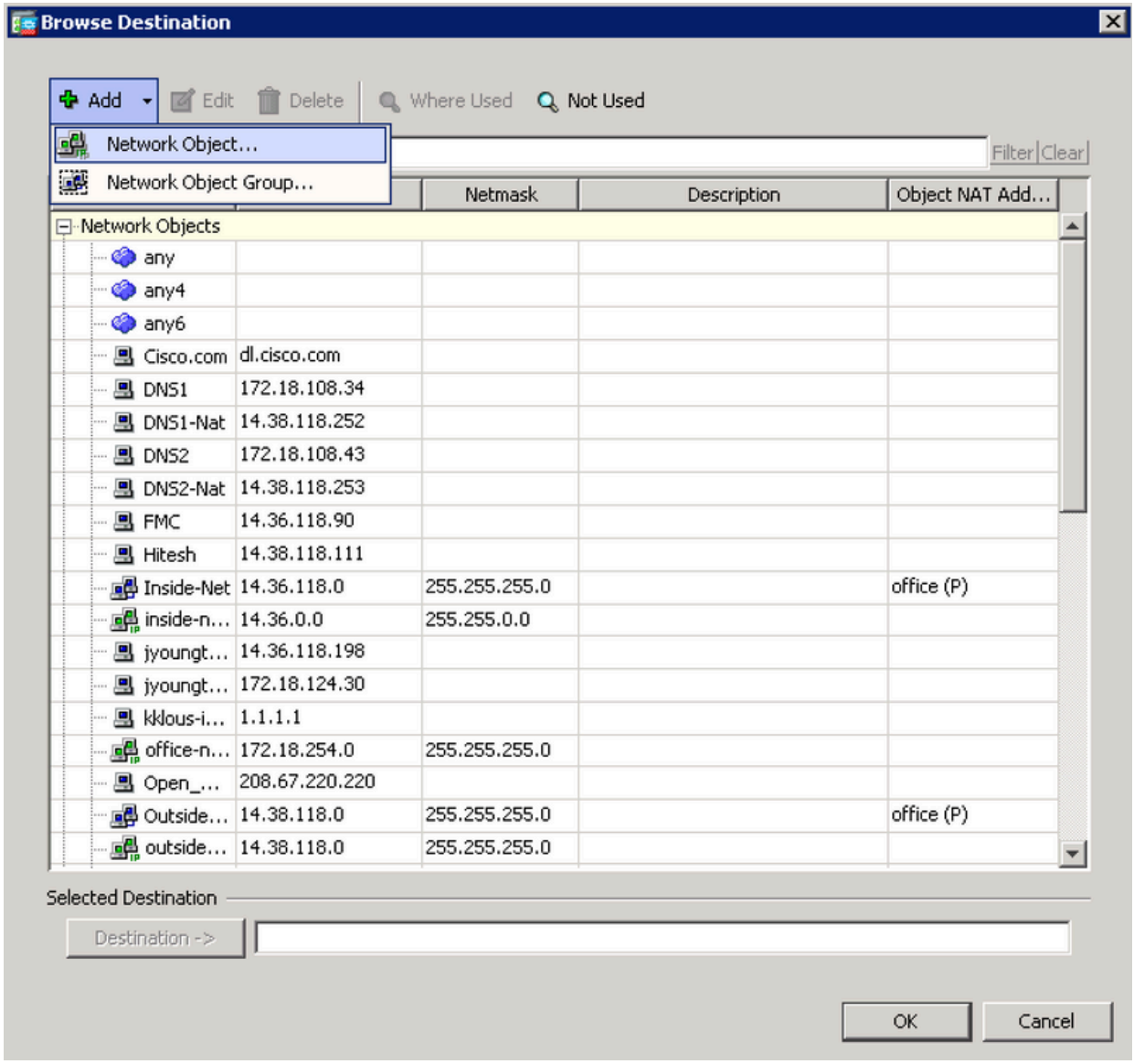
5. クラスマップに名前を付け（「dns-cmap」など）、「Source and Destination IP Address (uses ACL)」オプションにチェックマークを付けます。 [Next] をクリックします。.

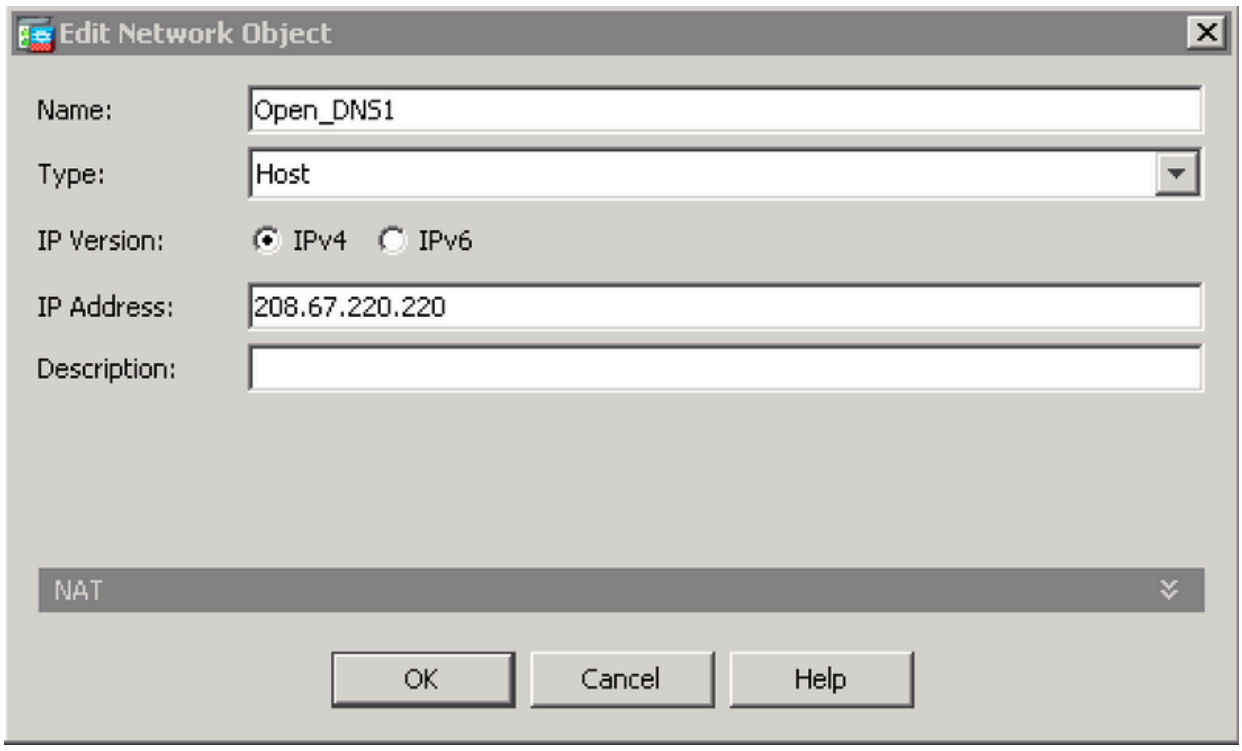


6. 最初に、「Do not match」アクションを使用して、検査を受けないようにするトラフィックを設定します。
   Sourceでは、オプション「any」を使用して、UmbrellaのDNSサーバ宛てのすべてのトラフィックを除外できます。または、ここでネットワークオブジェクト定義を作成して、特定の仮想アプライアンスのIPアドレスを除外することもできます。

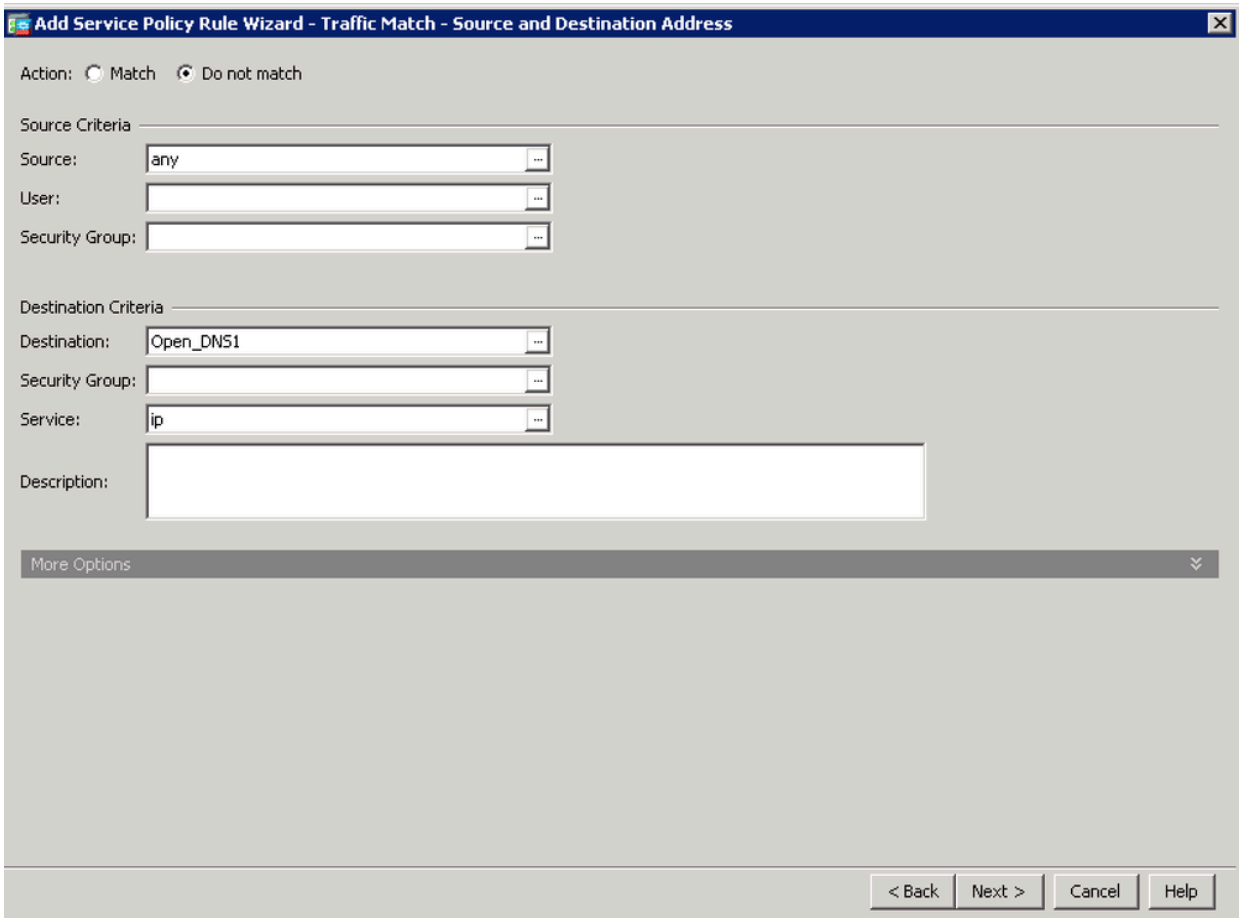


7. Destinationフィールドで...をクリックします。次のウィンドウでAdd > Network Objectの順にクリックし、「208.67.222.222」というIPアドレスを持つオブジェクトを作成します。 この手順を繰り返して、IPアドレスが「208.67.220.220」のオブジェクトを作成します。

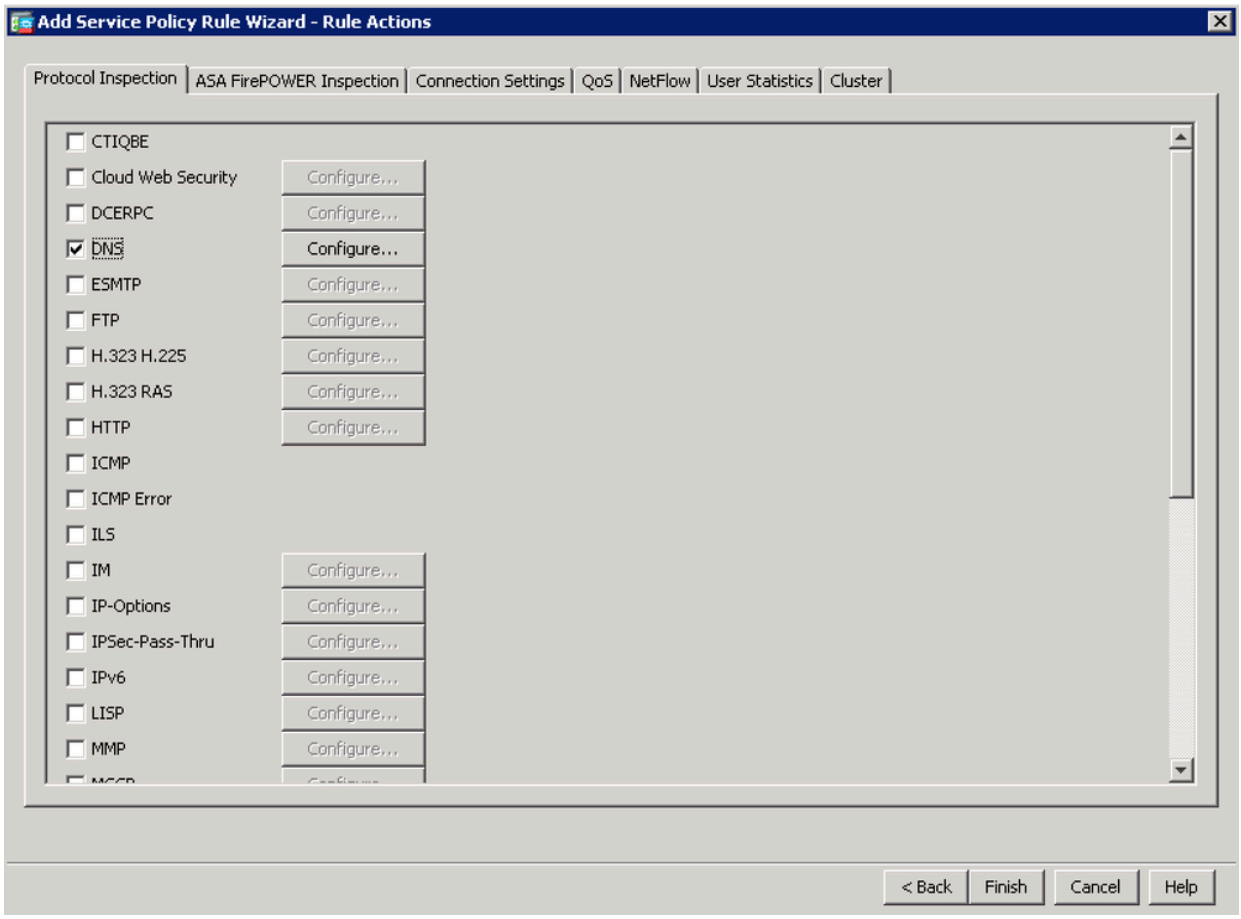

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90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

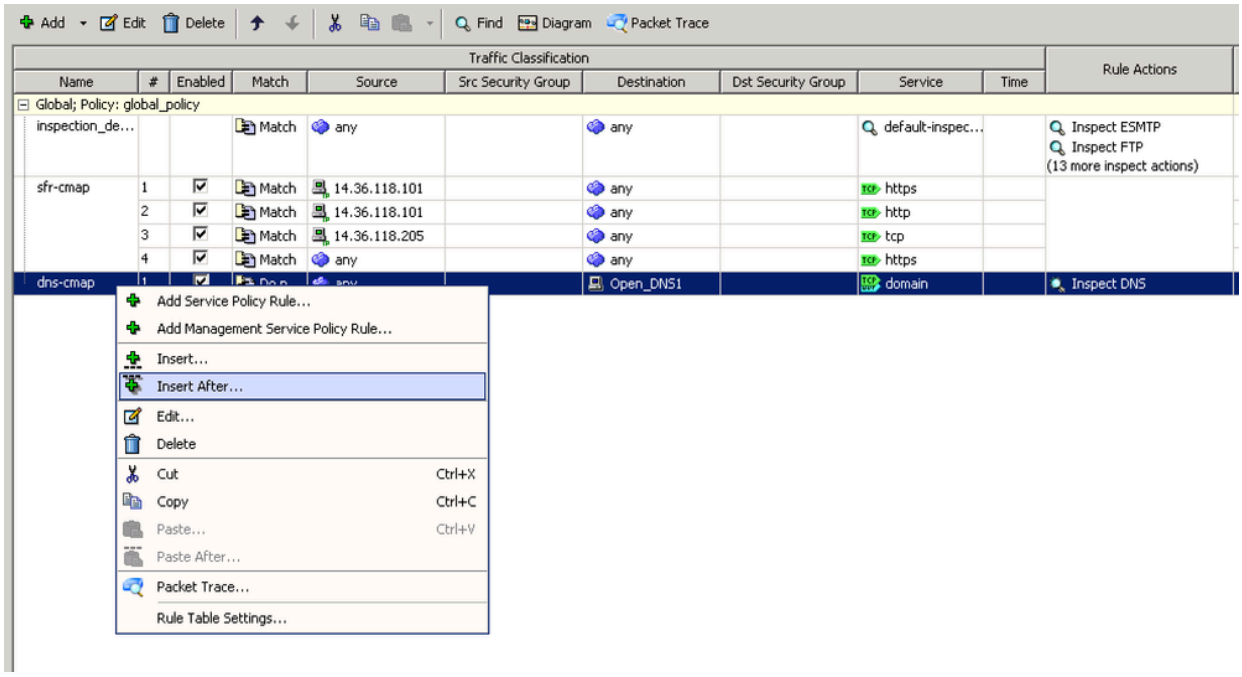
8. 両方のUmbrellaネットワークオブジェクトをDestinationフィールドに追加し、OKをクリックします。



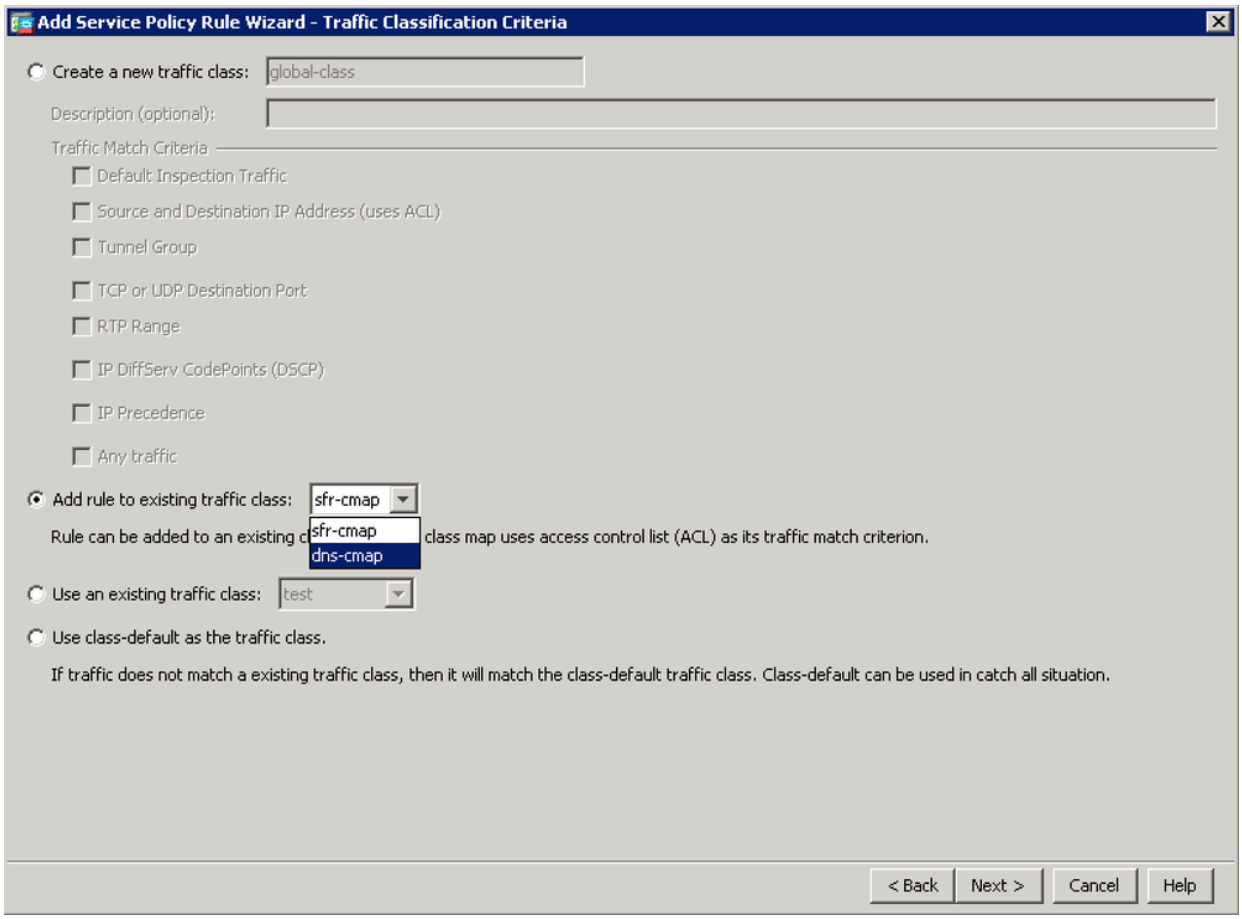
9. 次のウィンドウで「DNS」のボックスをオンにし、Finishをクリックします。



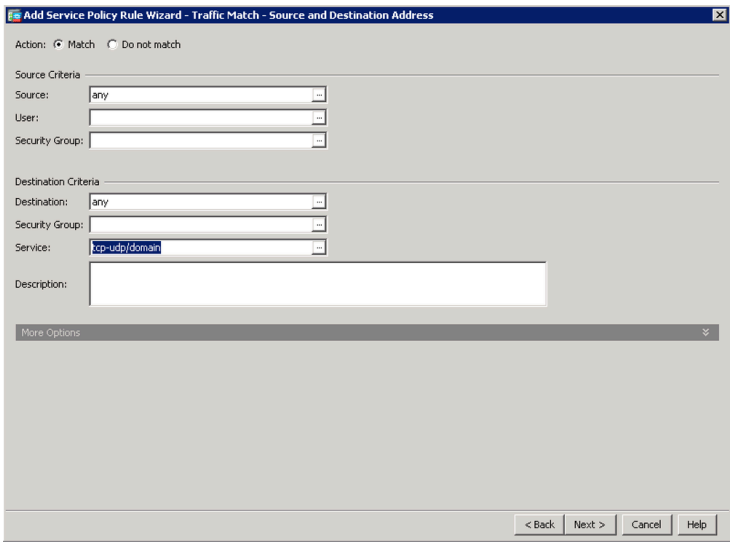
10. ASAに「dns-cmap」の新しいグローバルポリシーが表示されます。 次に、ASAによって検査される残りのトラフィックを設定する必要があります。これを行うには、「dns-cmap」を右クリックし、「Insert After...」オプションを選択して新しいルールを作成します。



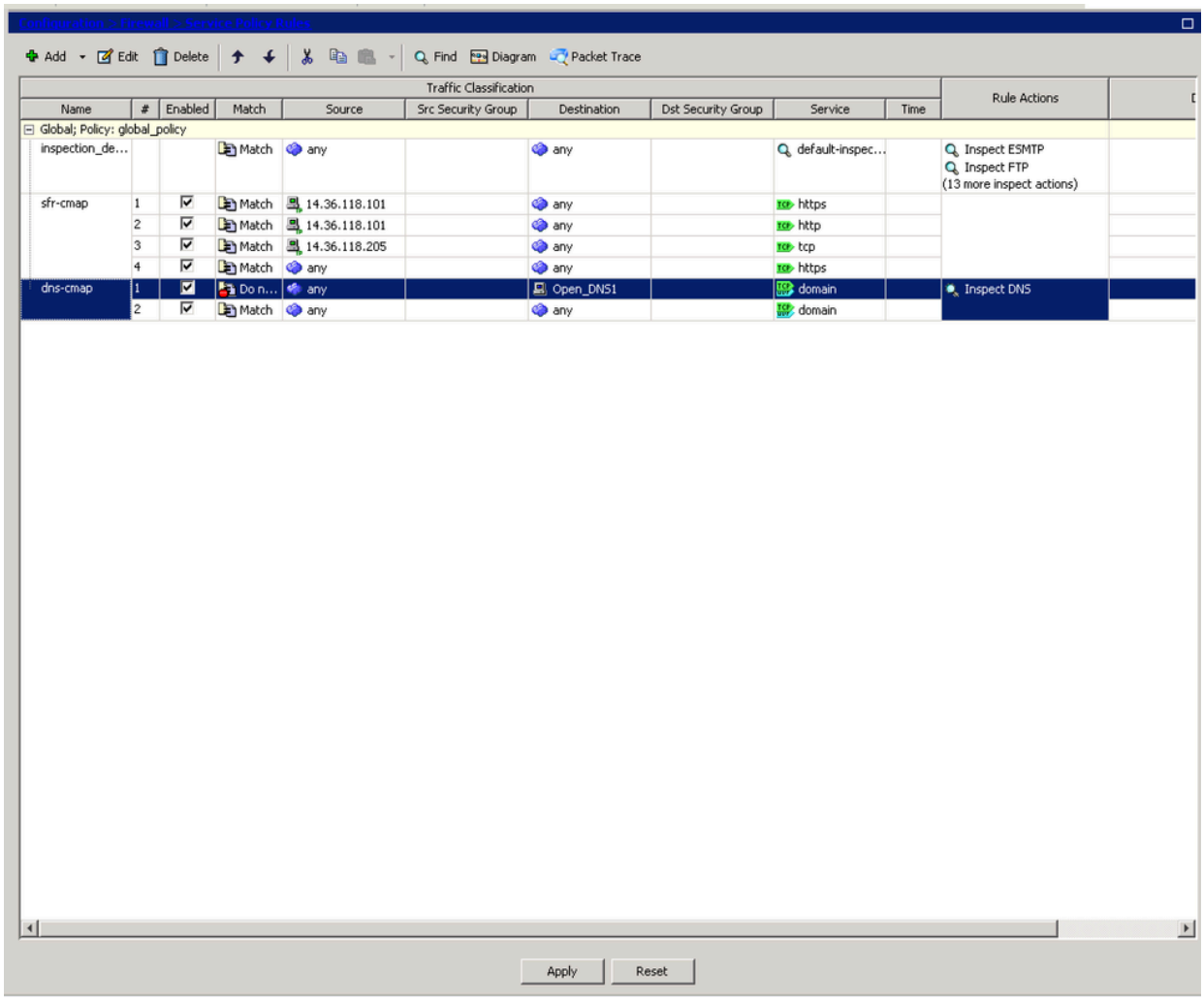
11. 最初のウィンドウでNextをクリックし、次にAdd rule to existing traffic class：オプションボタンをチェックします。ドロップダウンから「dns-cmap」を選択し、Nextをクリックします。



12. アクションは「Match」のままにします。 DNSインスペクションの対象となるトラフィックの送信元、宛先、およびサービスを選択します。 ここでは、たとえば、任意のクライアントから任意のTCPまたはUDP DNSサーバに送信されるトラフィックを照合します。[Next] をクリックします。



13. 「DNS」オプションにチェックマークを付けたまま、Finishをクリックします。
14. ウィンドウの下部にあるApplyをクリックします。



詳細情報

ASAの例外を設定するのではなく、DNScryptを無効にしたい場合は、Umbrellaサポートにお問い合わせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。