

Troubleshoot ASA Firewall Blocking DNScrypt Functionality from the Umbrella Virtual Appliance

Contents

[Introduction](#)

[Overview](#)

[Cause](#)

[Resolution](#)

[Packet Inspection Exceptions –IOS Commands](#)

[Packet Inspection Exceptions –ASDM Interface](#)

[Further Information](#)

Introduction

This article describes how to troubleshoot the ASA Firewall blocking DNScrypt functionality.

Overview

The Cisco ASA Firewall can block the DNScrypt functionality offered by the Umbrella Virtual Appliance. This results in this Umbrella Dashboard warning:

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>

These error messages can also be seen in the ASA firewall logs:

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

DNSCrypt encryption is designed to protect the contents of your DNS queries and as such also stops firewalls from performing packet inspection.

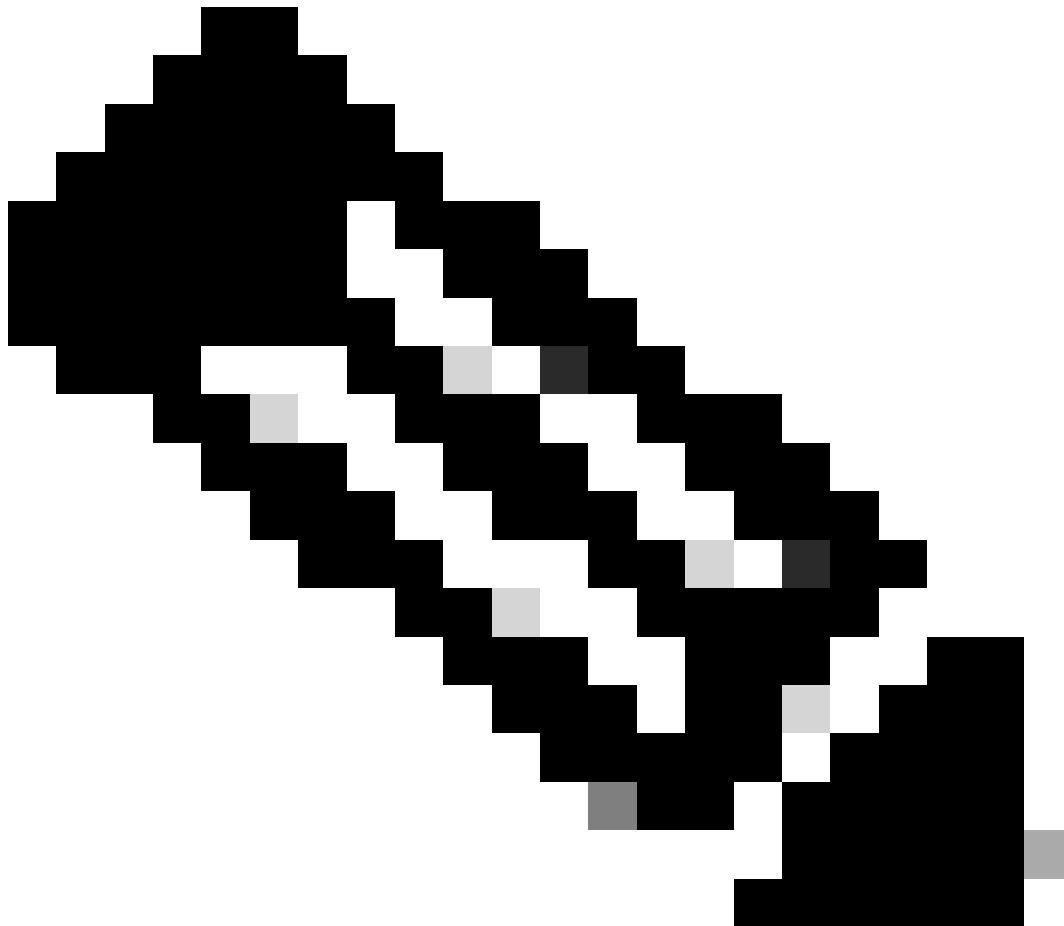
Cause

These errors must not cause any user facing impact with DNS resolution.

The Virtual Appliance sends test queries to determine the availability of DNScrypt and it is those test queries that are blocked. However, these error messages do indicate that the Virtual Appliance is not adding additional security by encrypting your company's DNS traffic.

Resolution

We recommend disabling DNS packet inspection for traffic between the Virtual Appliance and Umbrella's DNS resolvers. Although this disables the logging and protocol inspection on the ASA, it enhances security by allowing DNS encryption.



Note: These commands are provided for guidance only and it is recommended that a Cisco expert be consulted prior to making any changes to a production environment. Also be aware this defect on ASA *might affect DNS over TCP, which can also cause problems with DNSCrypt:*
[CSCsm90809](#) *DNS inspection support for DNS over TCP*

Packet Inspection Exceptions – IOS Commands

1. Create a new ACL called 'dns_inspect' with rules to deny traffic to 208.67.222.222 and 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. Remove the current DNS inspection policy on the ASA. For example:

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

3. Create a class-map matching the ACL created in Step #1:

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

4. Configure a policy-map under the global_policy. This must match the class-map created in Step #3. Enable DNS inspection.

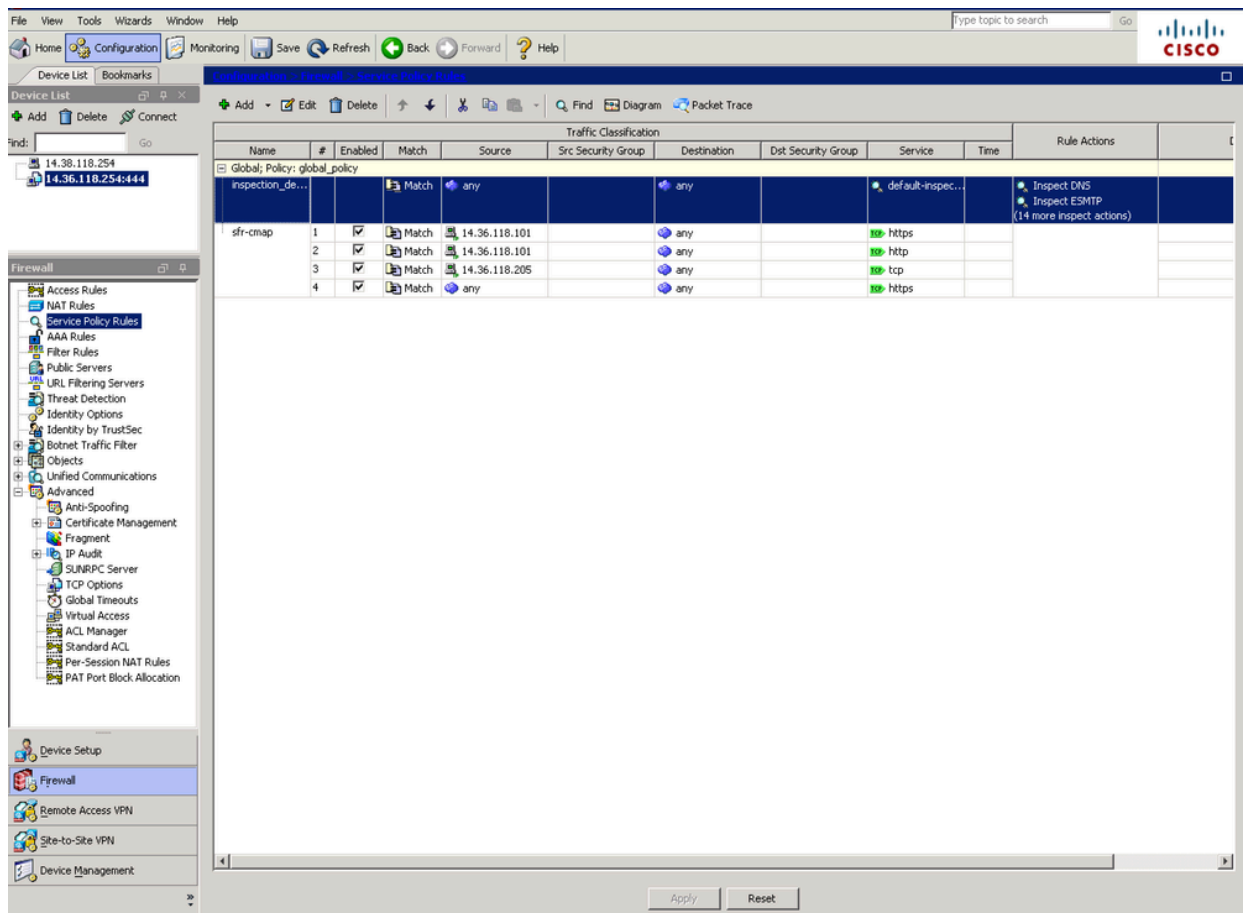
```
policy-map global_policy
class dns_inspect_cmap
inspect dns
```

5. Once enabled you can verify that traffic is hitting the exclusions by running:

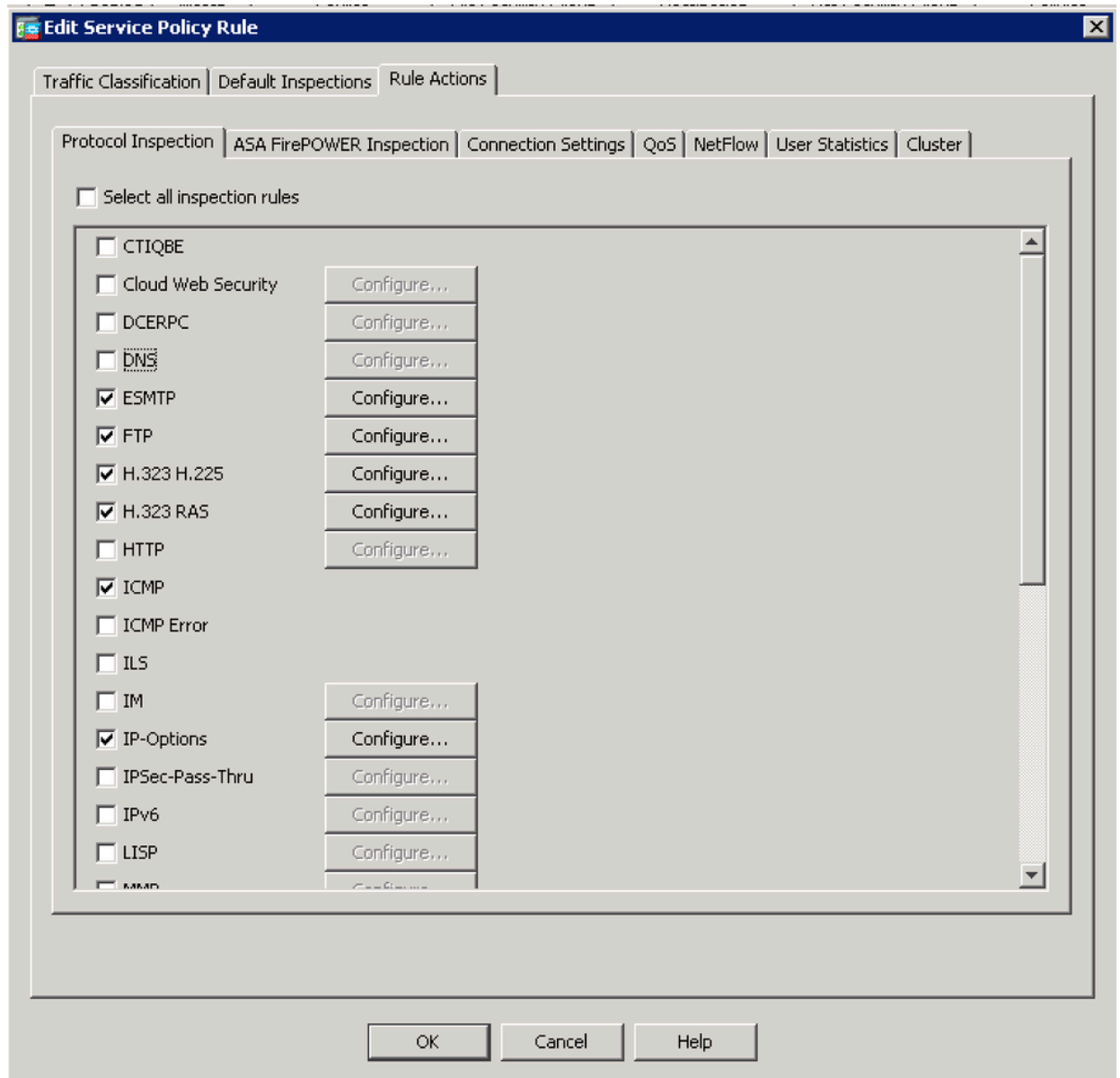
```
sh access-list dns_inspect
```

Packet Inspection Exceptions – ASDM Interface

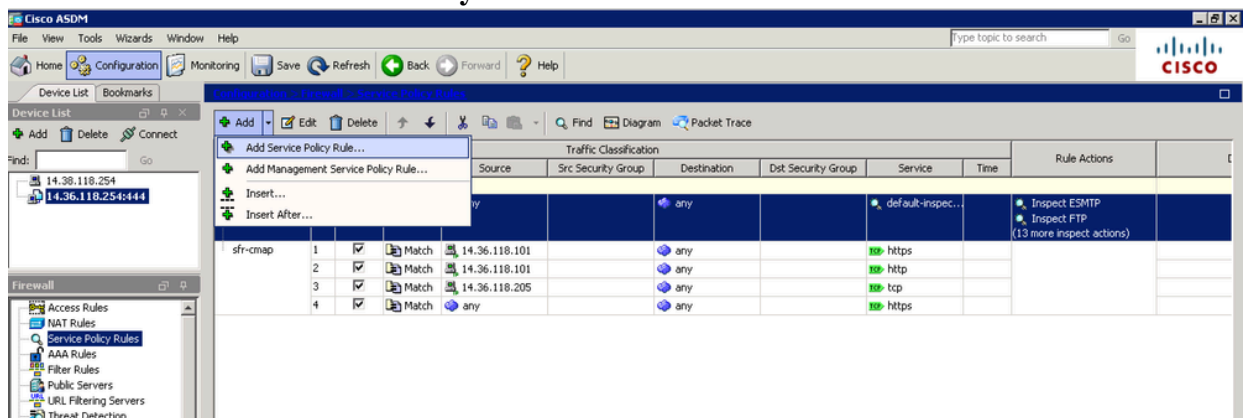
1. First disable any DNS packet inspection if applicable. This is done in **Configuration > Firewall > Service Policy Rules**.



2. In the example the DNS inspection is enabled under the Global Policy and 'inspection_default' class. Highlight it and click on **Edit**. On the new window uncheck the box for 'DNS' under the "Rule Action" tab.



3. Now you can re-configure the DNS inspection, this time with additional traffic exemptions. Click on **Add > Add Service Policy Rule...**



4. Select "Global - Applies to all interfaces" and click on **Next** (you can also apply this to a specific Interface if you wish).

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:
 Step 1: Configure a service policy.
 Step 2: Configure the traffic classification criteria for the service policy rule.
 Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To: _____

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

☐ **Interface:** inside - (create new service policy)
 Policy Name:
 Description:
☐ Drop and log unsupported IPv6 to IPv6 traffic

☒ **Global - applies to all interfaces**
 Policy Name: *
 Description:
☐ Drop and log unsupported IPv6 to IPv6 traffic

*Only one service policy is allowed. Existing service policy names cannot be changed.

< Back Next > Cancel Help

5. Give a name to the class-map (for example 'dns-cmap') and check the option "Source and Destination IP Address (uses ACL)". Click **Next**.

Add Service Policy Rule Wizard - Traffic Classification Criteria

☒ **Create a new traffic class:**
 Description (optional):

Traffic Match Criteria

☐ Default Inspection Traffic
☒ **Source and Destination IP Address (uses ACL)**
☐ Tunnel Group
☐ TCP or UDP Destination Port
☐ RTP Range
☐ IP DiffServ CodePoints (DSCP)
☐ IP Precedence
☐ Any traffic

☐ **Add rule to existing traffic class:** sfr-cmap
 Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match criterion.

☐ **Use an existing traffic class:** test

☐ **Use class-default as the traffic class.**
 If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back Next > Cancel Help

6. Start by configuring the traffic that you do not want to be inspected by using the "Do not match" action.

For Source, you can use the option 'any' to exempt all traffic destined to Umbrella's DNS servers. Alternatively, you can create a Network Object definition here to only exempt the specific Virtual Appliance IP address.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ☐ Match ☒ Do not match

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service: ip

Description:

More Options

< Back Next > Cancel Help

7. Click ... on the Destination field. On next window, click on **Add > Network Object** and create an object with the IP Address of '208.67.222.222'. Repeat this step to create an object with IP Address of '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:

Type:

IP Version:
☒ IPv4
☐ IPv6

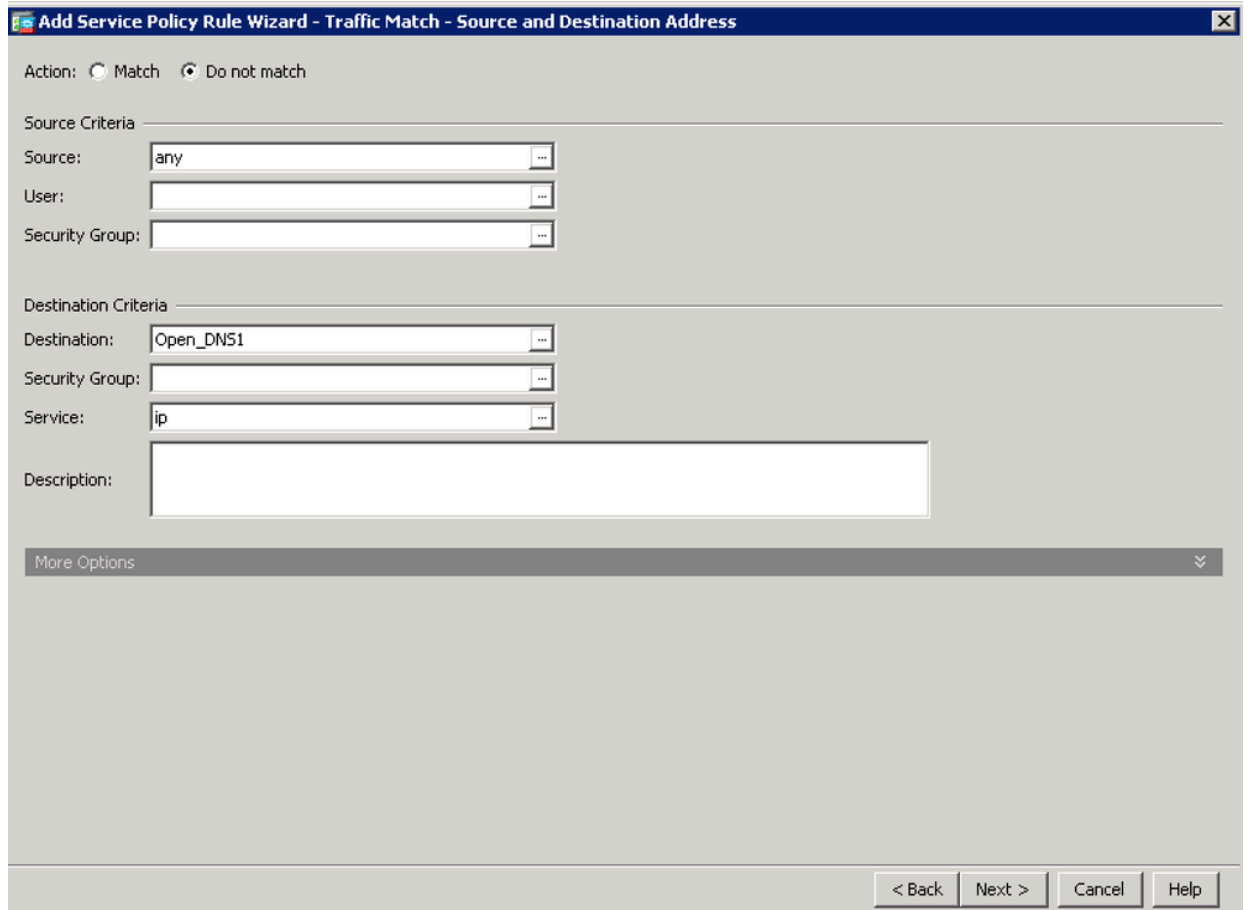
IP Address:

Description:

NAT

OK
Cancel
Help

8. Add both Umbrella network objects to the Destination field and click **OK**.



The screenshot shows the 'Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address' window. It has a title bar with a close button. The window contains two sections: 'Source Criteria' and 'Destination Criteria'. In the 'Source Criteria' section, the 'Source' field is set to 'any', and 'User' and 'Security Group' fields are empty. In the 'Destination Criteria' section, the 'Destination' field is set to 'Open_DNS1', and 'Security Group' and 'Service' fields are empty. A 'Description' text area is also present. At the bottom right, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. A 'More Options' link is visible at the bottom left of the main content area.

Action: ☐ Match ☒ Do not match

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: Open_DNS1

Security Group:

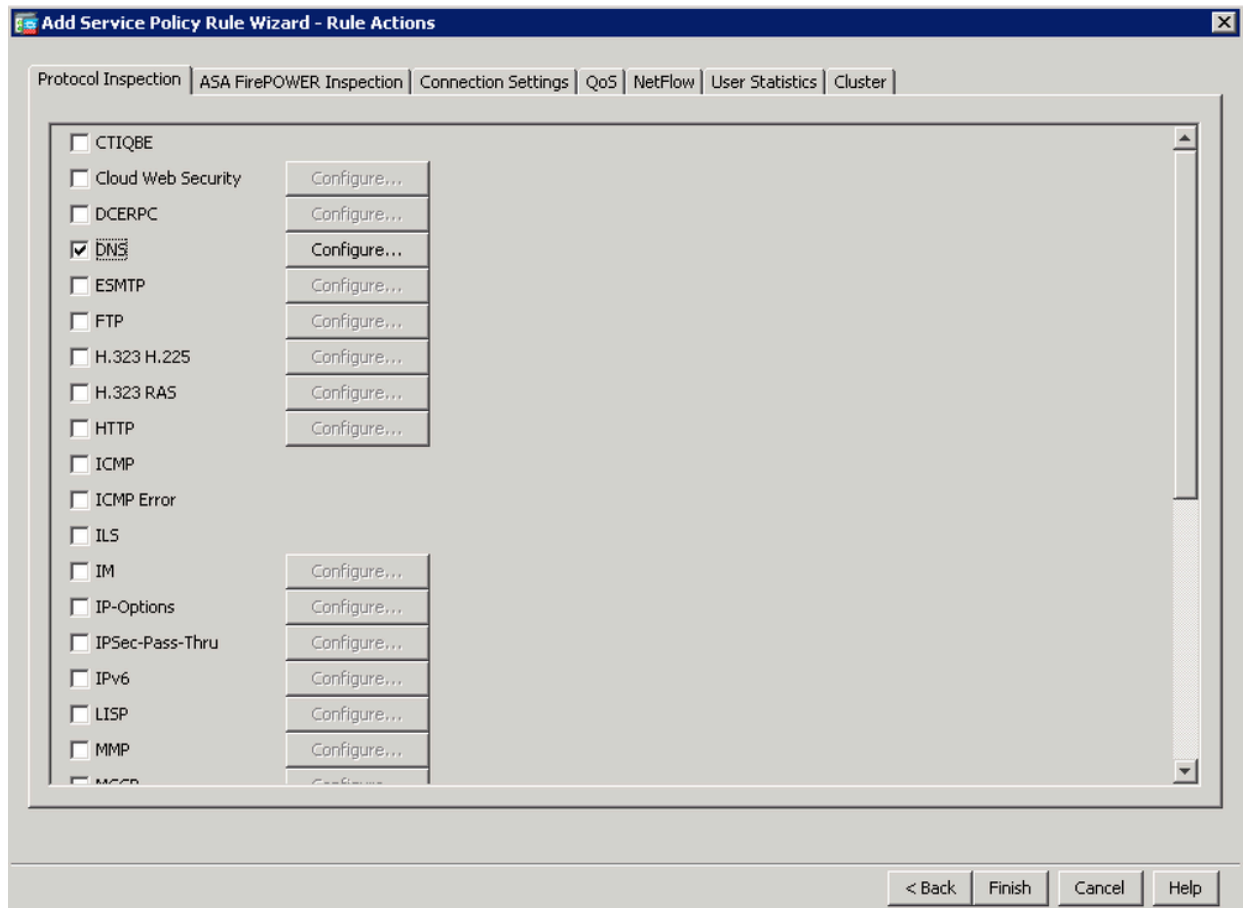
Service: ip

Description:

More Options

< Back Next > Cancel Help

9. On the next window check the box for 'DNS' and click on **Finish**.



The screenshot shows the 'Add Service Policy Rule Wizard - Rule Actions' window. It has a title bar with a close button. The window features a tabbed interface with tabs for 'Protocol Inspection', 'ASA FirePOWER Inspection', 'Connection Settings', 'QoS', 'NetFlow', 'User Statistics', and 'Cluster'. The 'Protocol Inspection' tab is selected. It contains a list of protocols with checkboxes and 'Configure...' buttons. The 'DNS' checkbox is checked. At the bottom right, there are buttons for '< Back', 'Finish', 'Cancel', and 'Help'.

Protocol Inspection ASA FirePOWER Inspection Connection Settings QoS NetFlow User Statistics Cluster

☐ CTIQBE

☐ Cloud Web Security Configure...

☐ DCERPC Configure...

☒ DNS Configure...

☐ ESMTP Configure...

☐ FTP Configure...

☐ H.323 H.225 Configure...

☐ H.323 RAS Configure...

☐ HTTP Configure...

☐ ICMP

☐ ICMP Error

☐ ILS

☐ IM Configure...

☐ IP-Options Configure...

☐ IPSec-Pass-Thru Configure...

☐ IPv6 Configure...

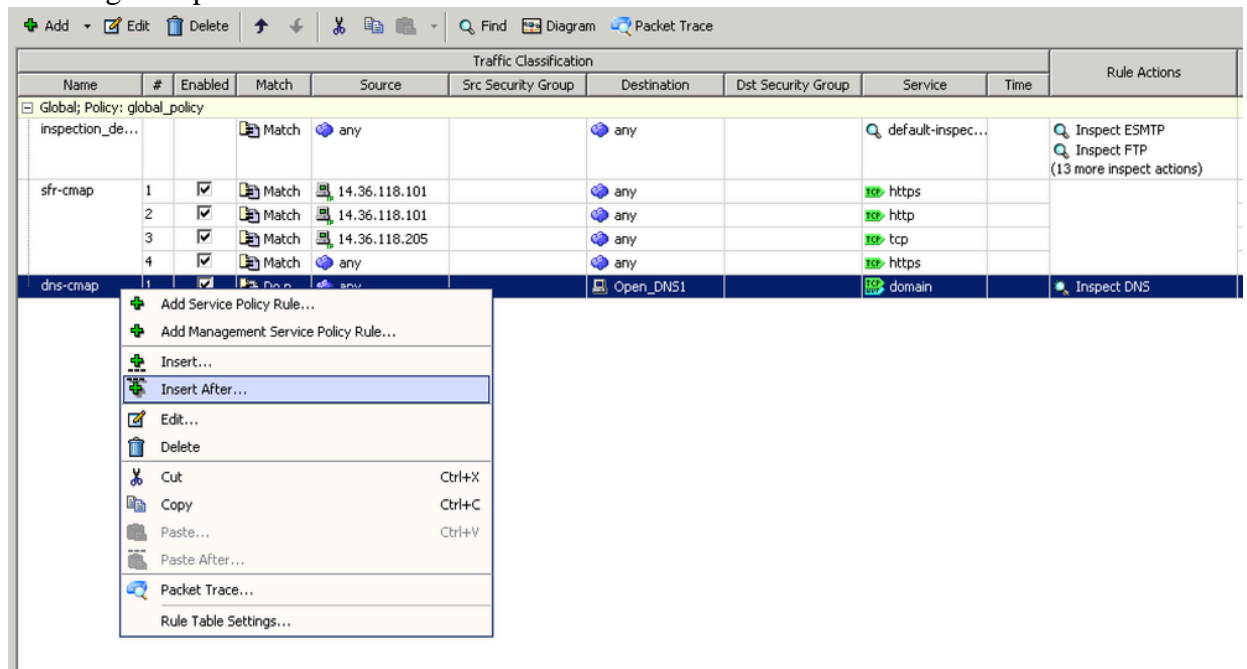
☐ LISP Configure...

☐ MMP Configure...

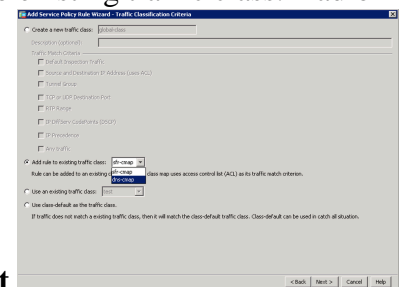
☐ MSSP Configure...

< Back Finish Cancel Help

10. The ASA now shows the new Global-Policy for 'dns-cmap'. Now you need to configure the remaining traffic that is inspected by the ASA. This is done by right clicking on 'dns-cmap' and selecting the option "Insert After..." which creates a new rule.

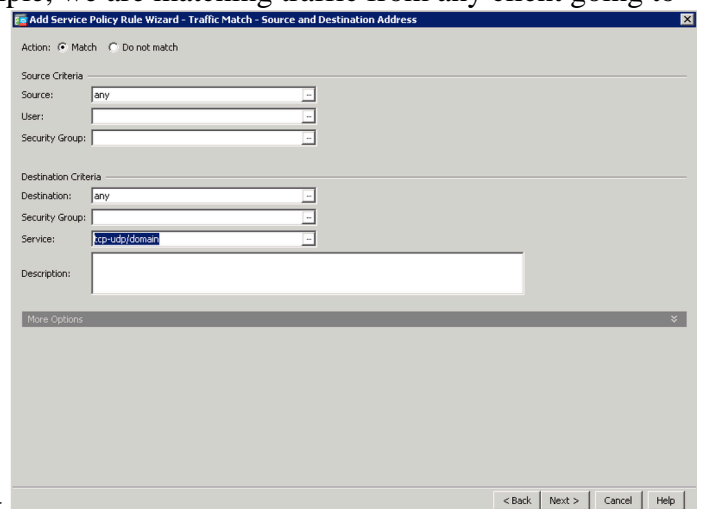


11. On first window click on **Next** and on then check the "Add rule to existing traffic class:" radio



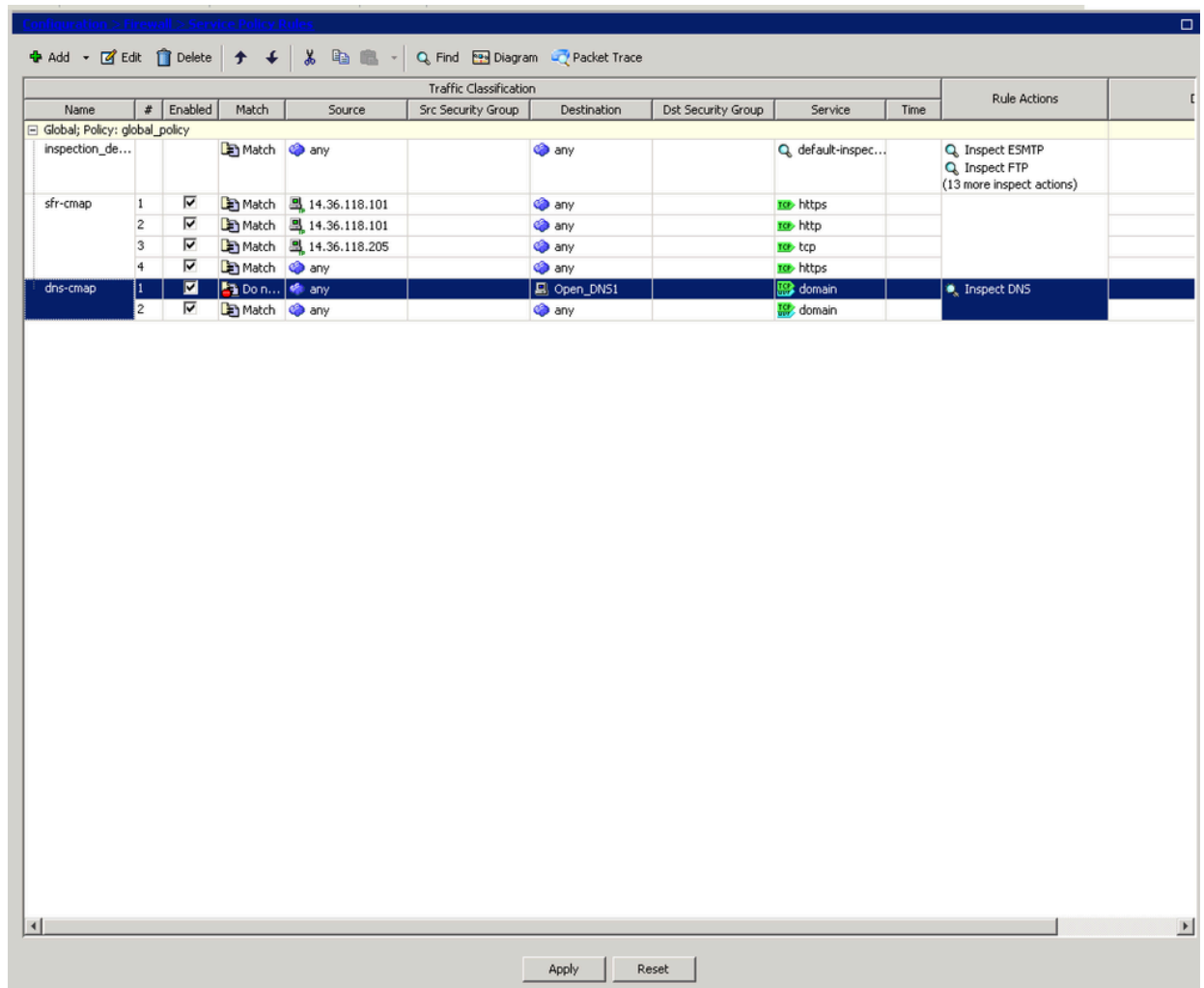
button. Select 'dns-cmap' from the drop-down and then click **Next**.

12. Leave the Action as 'Match'. Choose the Source, Destination and Service of traffic that is subject to DNS inspection. Here, for example, we are matching traffic from any client going to



any TCP or UDP DNS Server. Click **Next**.

13. Leave the 'DNS' option checked and click on **Finish**.
14. Click on **Apply** at the bottom of the window.



Further Information

If you would prefer to disable DNScrypt rather than configuring ASA exemptions, please contact Umbrella support.