

Solucionar problemas do firewall ASA que bloqueia a funcionalidade DNSCrypt do Umbrella Virtual Appliance

Contents

[Introdução](#)

[Overview](#)

[Causa](#)

[Resolução](#)

[Exceções de inspeção de pacote - Comandos IOS](#)

[Exceções de Inspeção de Pacotes - Interface ASDM](#)

[Mais informações](#)

Introdução

Este artigo descreve como solucionar problemas do firewall ASA que bloqueia a funcionalidade DNSCrypt.

Overview

O Cisco ASA Firewall pode bloquear a funcionalidade DNSCrypt oferecida pelo Umbrella Virtual Appliance. Isso resulta neste aviso do Painel de controle do Umbrella:

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>

Essas mensagens de erro também podem ser vistas nos logs de firewall do ASA:

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

A criptografia DNSCrypt foi projetada para proteger o conteúdo de suas consultas DNS e, como tal, também impede que os firewalls executem a inspeção de pacotes.

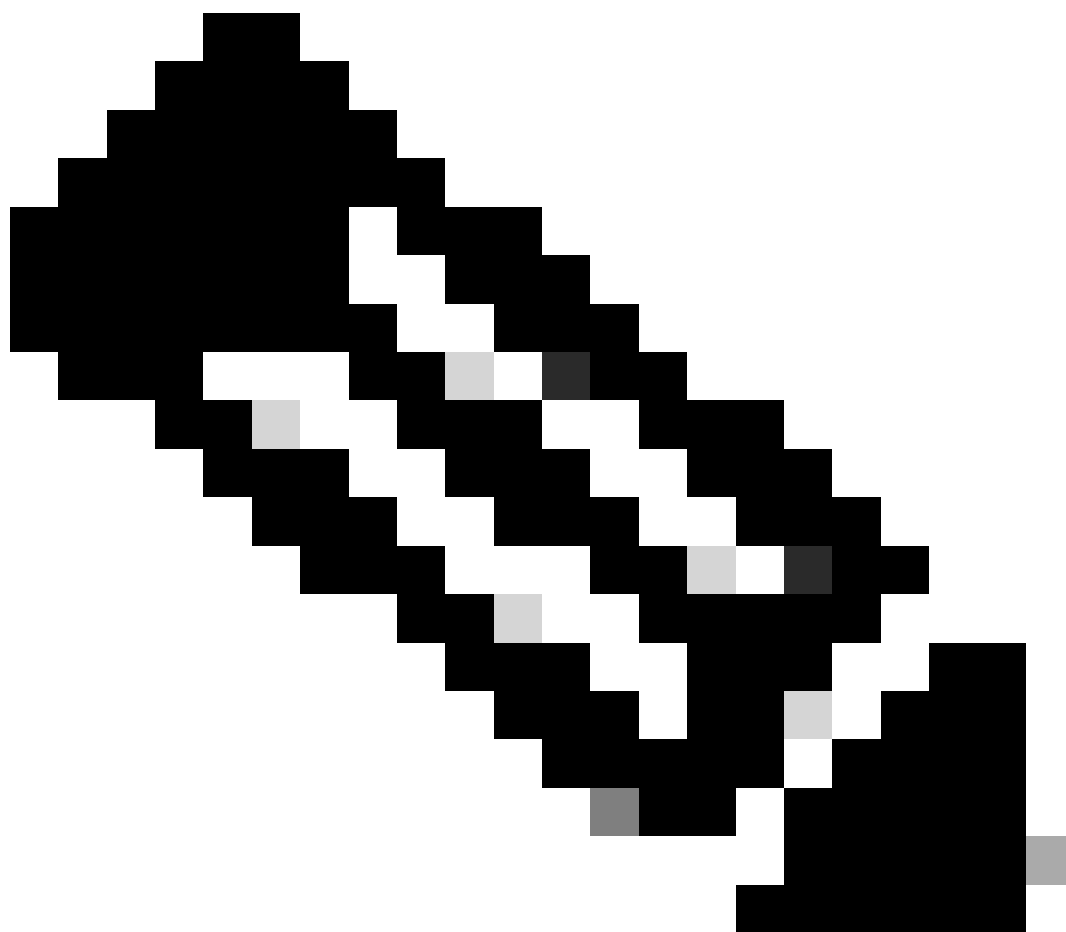
Causa

Esses erros não devem causar nenhum impacto para o usuário com a resolução DNS.

O Virtual Appliance envia consultas de teste para determinar a disponibilidade do DNScrypt e são essas consultas de teste que são bloqueadas. No entanto, essas mensagens de erro indicam que o Virtual Appliance não está adicionando segurança adicional ao criptografar o tráfego DNS da sua empresa.

Resolução

Recomendamos desativar a inspeção de pacotes DNS para o tráfego entre os resolvedores de DNS do Virtual Appliance e do Umbrella. Embora isso desative a inspeção de registro e protocolo no ASA, aumenta a segurança permitindo a criptografia DNS.



Note: Esses comandos são fornecidos apenas para orientação e recomenda-se que um especialista da Cisco seja consultado antes de fazer qualquer alteração em um ambiente de produção.

Esteja ciente também deste defeito no ASA pode afetar o DNS sobre o TCP, o que também pode causar problemas com o DNScrypt:

[CSCsm90809](#) Suporte de inspeção de DNS para DNS sobre TCP

Exceções de Inspeção de Pacotes - Comandos IOS

1. Crie uma nova ACL chamada 'dns_inspect' com regras para negar o tráfego para 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 encryption

```
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. Remova a política de inspeção de DNS atual no ASA. Por exemplo:

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

3. Crie um mapa de classe correspondente à ACL criada na Etapa #1:

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

4. Configure um mapa de políticas em global_policy. Ele deve corresponder ao mapa de classe criado na Etapa #3. Habilite a inspeção de DNS.

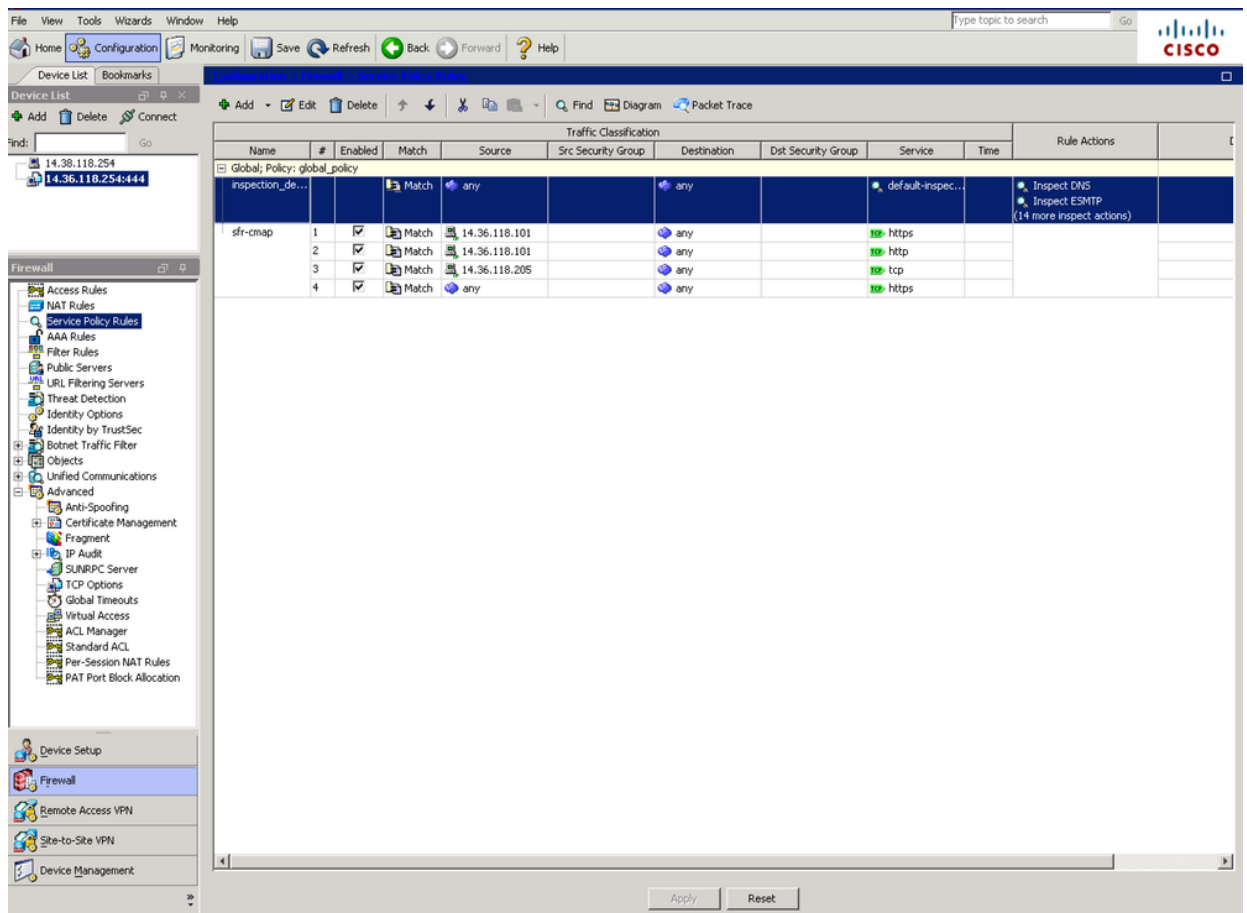
```
policy-map global_policy
class dns_inspect_cmap
inspect dns
```

5. Depois de habilitado, você pode verificar se o tráfego está atingindo as exclusões executando:

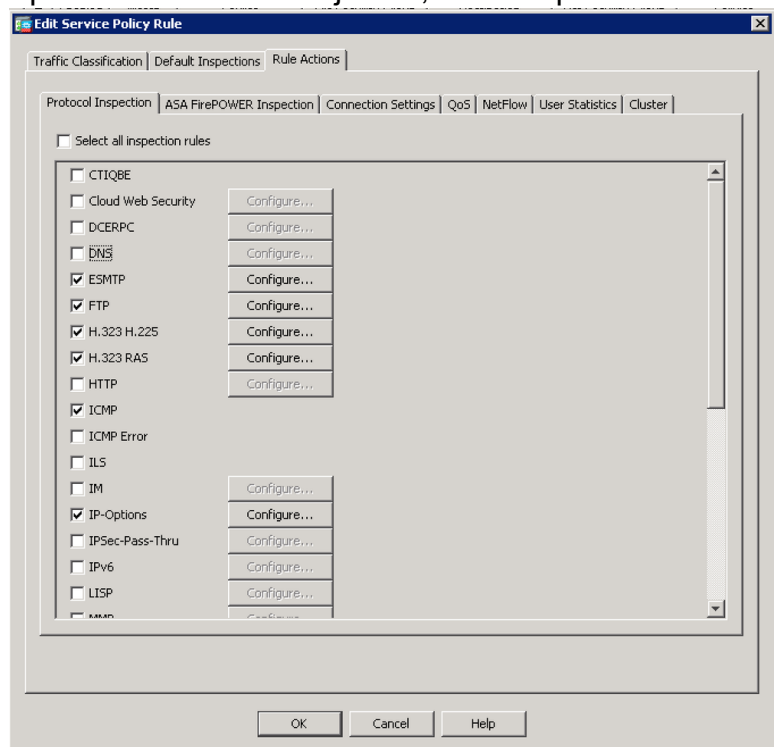
```
sh access-list dns_inspect
```

Exceções de Inspeção de Pacotes - Interface ASDM

1. Primeiro desabilite qualquer inspeção de pacote DNS, se aplicável. Isso é feito em Configuration > Firewall > Service Policy Rules.

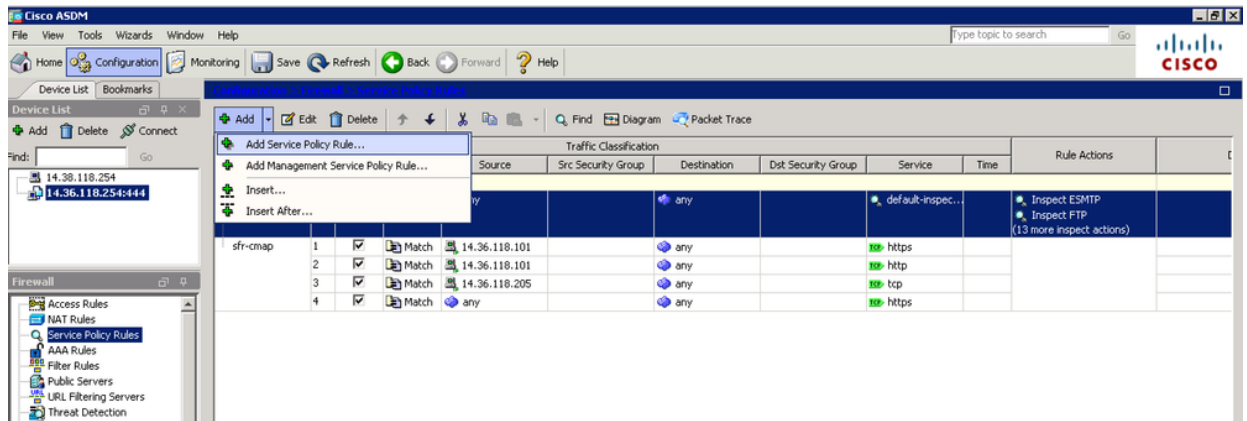


- No exemplo, a inspeção de DNS está habilitada na política global e na classe 'inspection_default'. Realce-o e clique em Edit. Na nova janela, desmarque a caixa

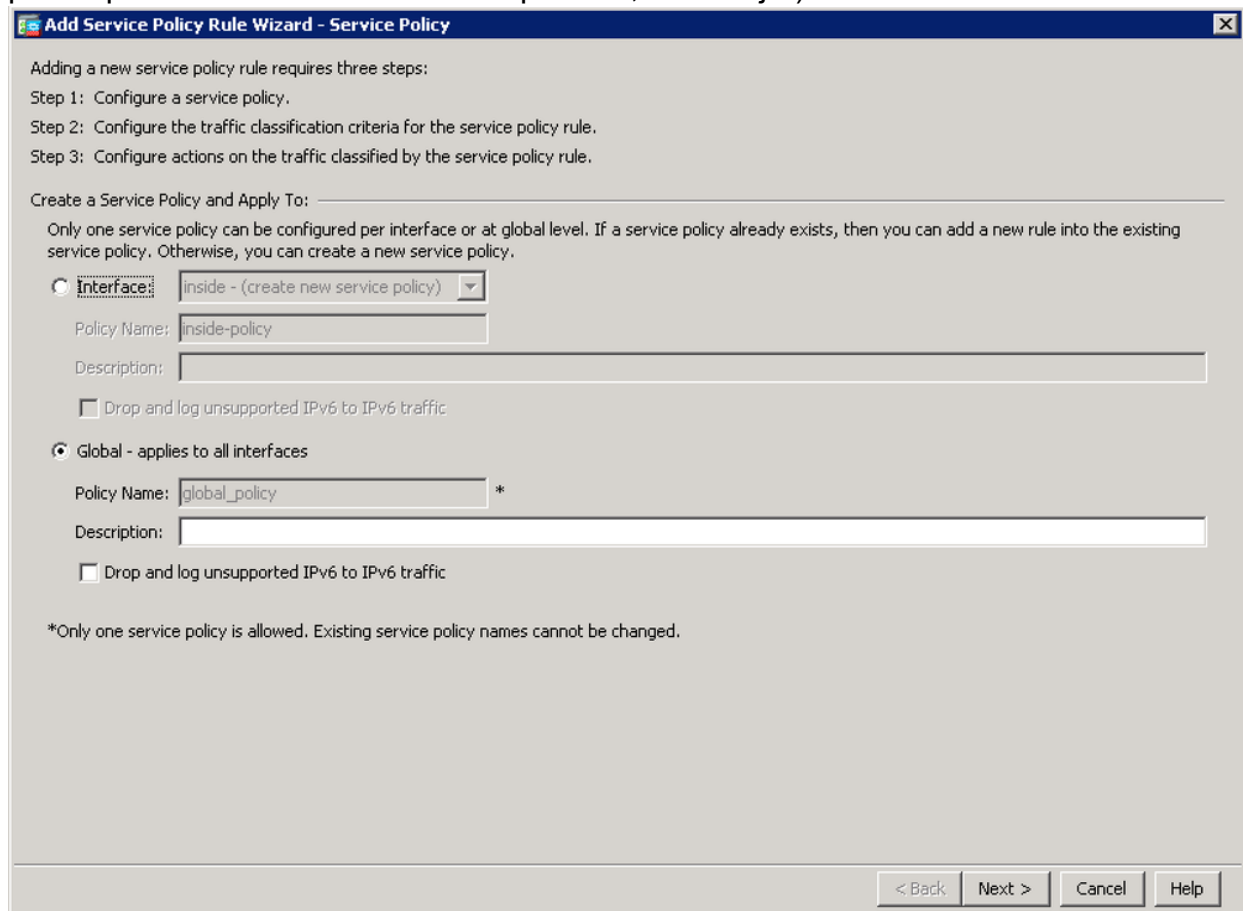


para 'DNS' na guia "Rule Action".

- Agora você pode reconfigurar a inspeção de DNS, desta vez com isenções de tráfego adicionais. Clique em Add > Add Service Policy Rule...



4. Selecione "Global - Aplica-se a todas as interfaces" e clique em Next (você também pode aplicar isso a uma interface específica, se desejar).



5. Dê um nome ao mapa de classe (por exemplo 'dns-cmap') e marque a opção "Endereço IP de origem e destino (usa ACL)". Clique em Avançar.

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:

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:

☐ 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. Comece configurando o tráfego que você não deseja que seja inspecionado usando a ação "Não corresponder".
- Para Source, você pode usar a opção 'any' para isentar todo o tráfego destinado aos servidores DNS da Umbrella. Como alternativa, você pode criar uma definição de objeto de rede aqui para isentar apenas o endereço IP do dispositivo virtual específico.

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

Action: ☐ Match ☒ Do not match

Source Criteria

Source: ...

User: ...

Security Group: ...

Destination Criteria

Destination: ...

Security Group: ...

Service: ...

Description:

More Options 

< Back Next > Cancel Help

7. Clique em ... no campo Destino. Na próxima janela, clique em Add > Network Object e crie um objeto com o endereço IP '208.67.222.222'. Repita esta etapa para criar um objeto com o endereço 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:

Type:

Host

IP Version:
☒ IPv4
☐ IPv6

IP Address:

Description:

NAT

OK
Cancel
Help

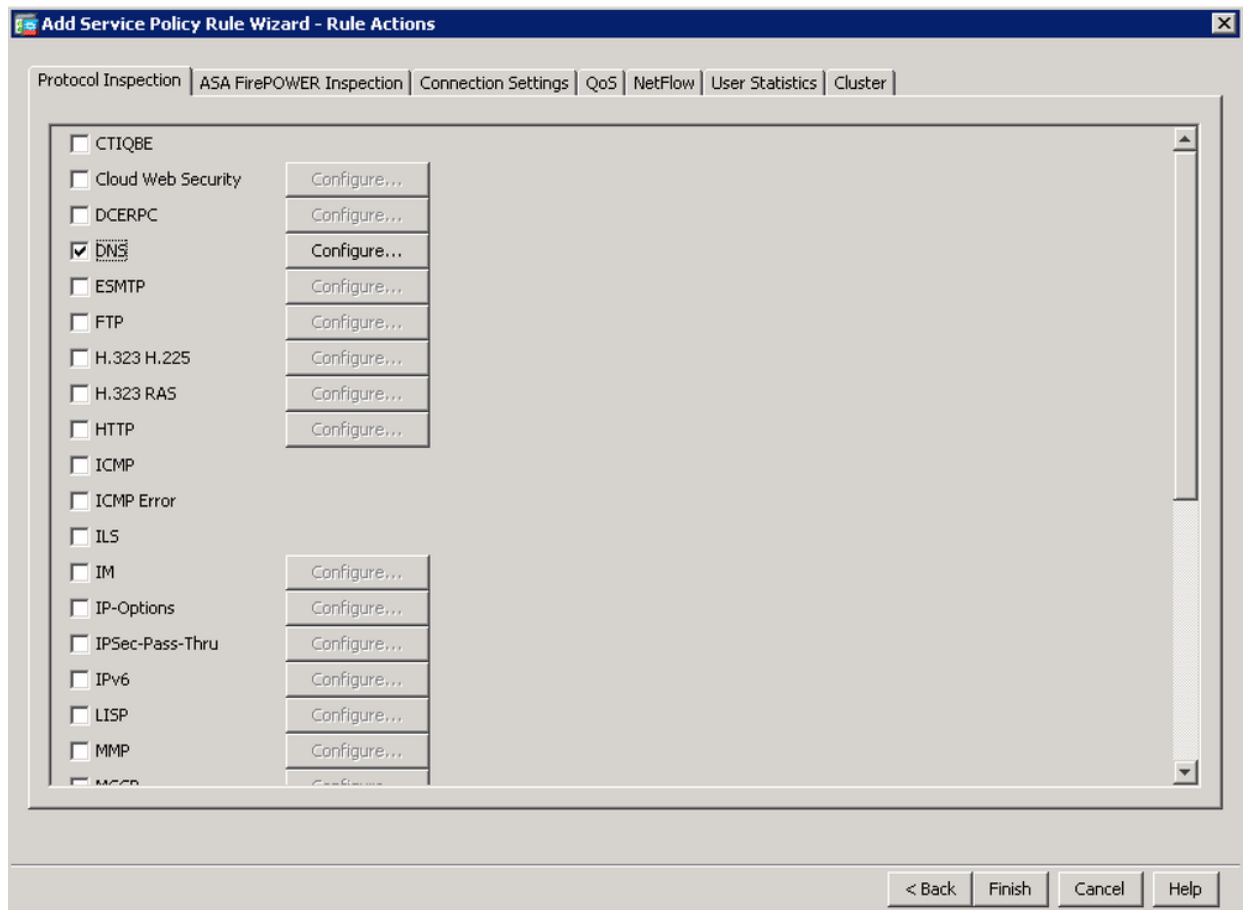
8. Adicione ambos os objetos de rede Umbrella ao campo Destino e clique em OK.

The screenshot shows a Windows-style dialog box titled "Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address". It has a close button (X) in the top right corner. The dialog is divided into several sections:

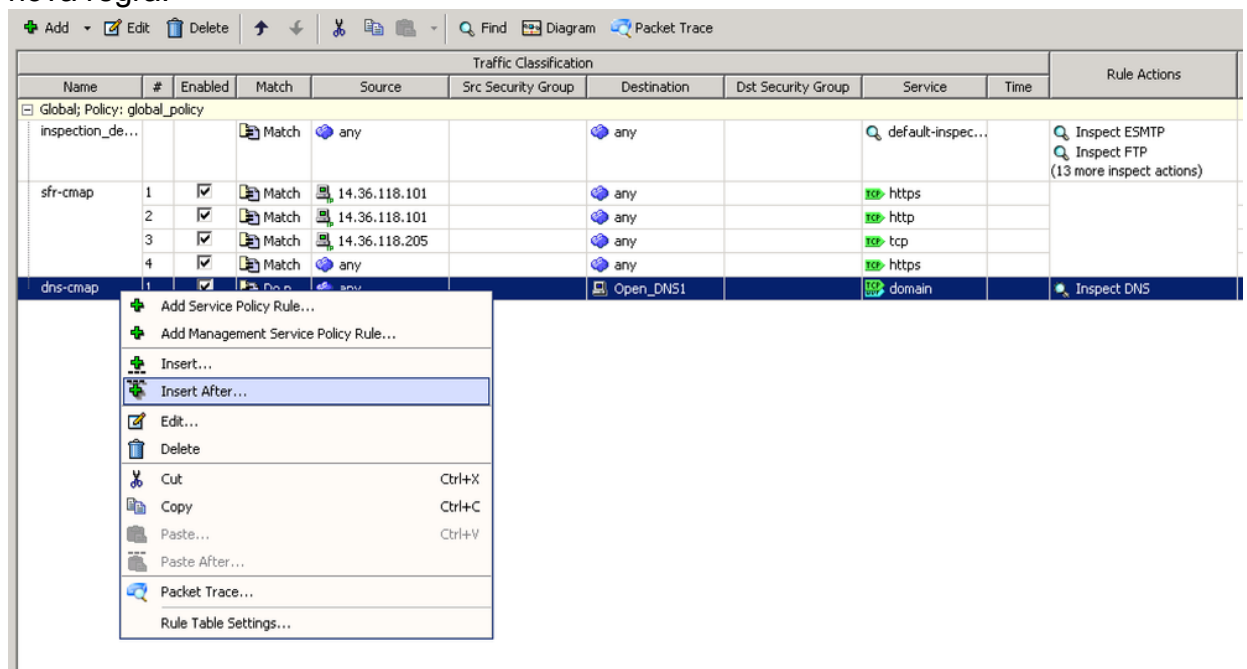
- Action:** Two radio buttons are present: "Match" (unselected) and "Do not match" (selected).
- Source Criteria:** A section header followed by three input fields:
 - Source:** A text box containing "any" with a dropdown arrow on the right.
 - User:** An empty text box with a dropdown arrow on the right.
 - Security Group:** An empty text box with a dropdown arrow on the right.
- Destination Criteria:** A section header followed by three input fields:
 - Destination:** A text box containing "Open_DNS1" with a dropdown arrow on the right.
 - Security Group:** An empty text box with a dropdown arrow on the right.
 - Service:** A text box containing "ip" with a dropdown arrow on the right.
- Description:** A large, empty text area.
- More Options:** A section header with a dropdown arrow pointing downwards.

At the bottom right of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

9. Na próxima janela, marque a caixa para 'DNS' e clique em Finish.



10. O ASA agora mostra a nova Política Global para 'dns-cmap'. Agora você precisa configurar o tráfego restante que é inspecionado pelo ASA. Isso é feito clicando com o botão direito em 'dns-cmap' e selecionando a opção "Inserir após..." que cria uma nova regra.



11. Na primeira janela, clique em Next e, em seguida, marque o botão de opção "Add rule to existing traffic class.". Selecione 'dns-cmap' na lista suspensa e clique em Avançar.

12. Deixe a Ação como 'Correspondência'. Escolha a Origem, o Destino e o Serviço do tráfego que está sujeito à inspeção DNS. Aqui, por exemplo, estamos correspondendo o tráfego de qualquer cliente que vai para qualquer Servidor DNS TCP ou UDP. Clique

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: any

Security Group:

Service: tcp-udp/domain

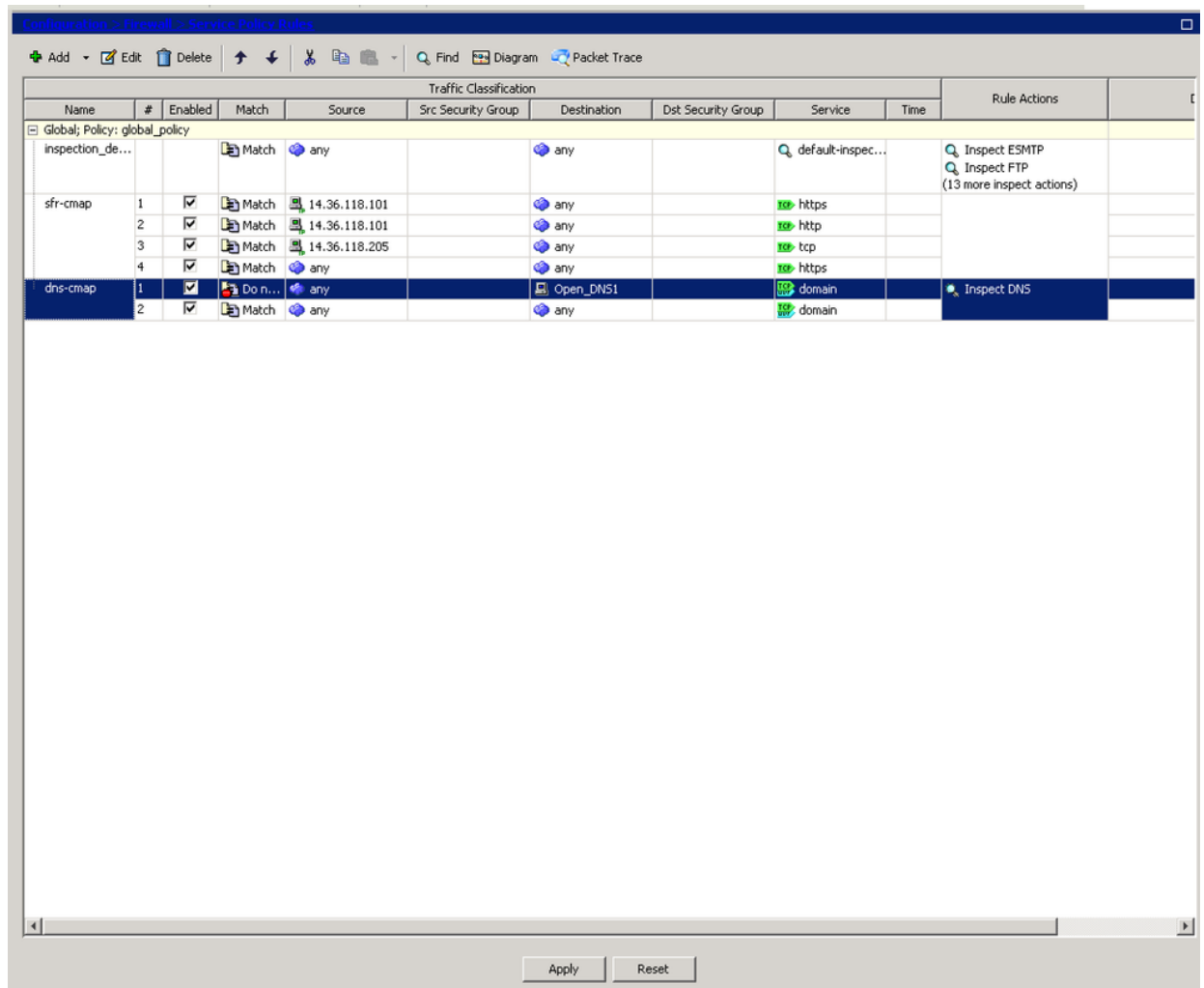
Description:

More Options

< Back Next > Cancel Help

em Next.

13. Deixe a opção 'DNS' marcada e clique em Finish.
14. Clique em Apply na parte inferior da janela.



Mais informações

Se preferir desabilitar o DNScrypt em vez de configurar as isenções do ASA, entre em contato com o suporte do Umbrella.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.