

對Umbrella虛擬裝置的ASA防火牆阻止DNSScrypt功能進行故障排除

目錄

[簡介](#)

[概觀](#)

[原因](#)

[解析](#)

[資料包檢測例外 — IOS命令](#)

[資料包檢測異常 — ASDM介面](#)

[更多資訊](#)

簡介

本文描述如何對ASA防火牆阻止DNSScrypt功能進行故障排除。

概觀

Cisco ASA防火牆可以阻止Umbrella虛擬裝置提供的DNSScrypt功能。這將導致此傘狀控制面板警告：

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防火牆日誌中也可以看到以下錯誤消息：

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

DNSScrypt加密旨在保護DNS查詢的內容，因此也會阻止防火牆執行資料包檢測。

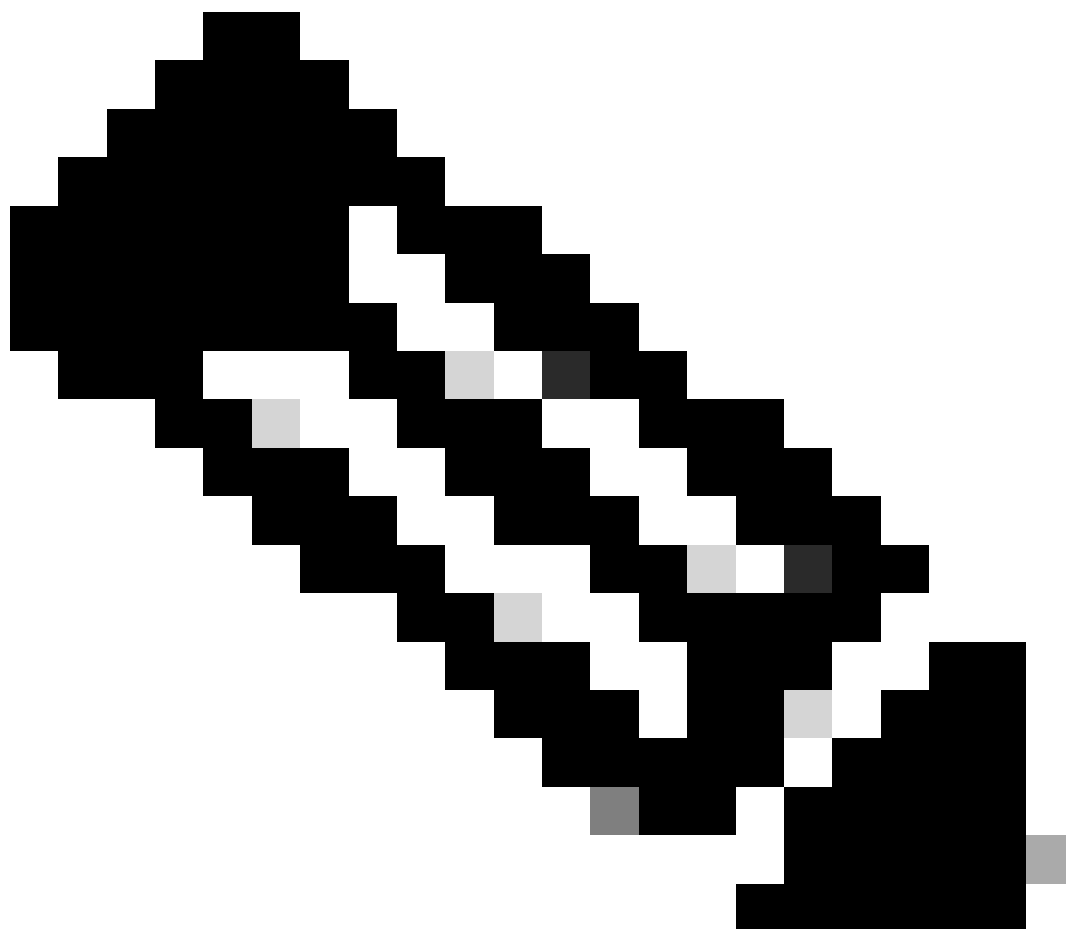
原因

這些錯誤不能導致任何使用者面對DNS解析的影響。

Virtual Appliance傳送測試查詢以確定DNSScrypt的可用性，這些測試查詢會被阻止。但是，這些錯誤消息確實表示虛擬裝置不會通過加密您公司的DNS流量來增加額外的安全性。

解析

我們建議對虛擬裝置和Umbrella的DNS解析器之間的流量禁用DNS資料包檢測。雖然這會禁用ASA上的日誌記錄和協定檢查，但它通過允許DNS加密來增強安全性。



附註：這些命令僅供參考，建議在對生產環境進行任何更改之前諮詢思科專家。
還要注意ASA上的此缺陷 可能會影響TCP上的DNS，這也會導致DNSEncrypt出現問題：
[CSCsm90809 DNS檢測支援](#)，用於通過TCP的DNS

資料包檢測例外 — IOS命令

1. 建立一個名為「dns_inspect」的新ACL，其中包含的規則用於拒絕流量到達208.67.222.222和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. 刪除ASA上的當前DNS檢查策略。舉例來說：

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

3. 建立與步驟1中建立的ACL匹配的類映#1:

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

4. 在global_policy下配置策略對映。此對映必須與步驟10中建立的類對映匹#3。啟用DNS檢測。

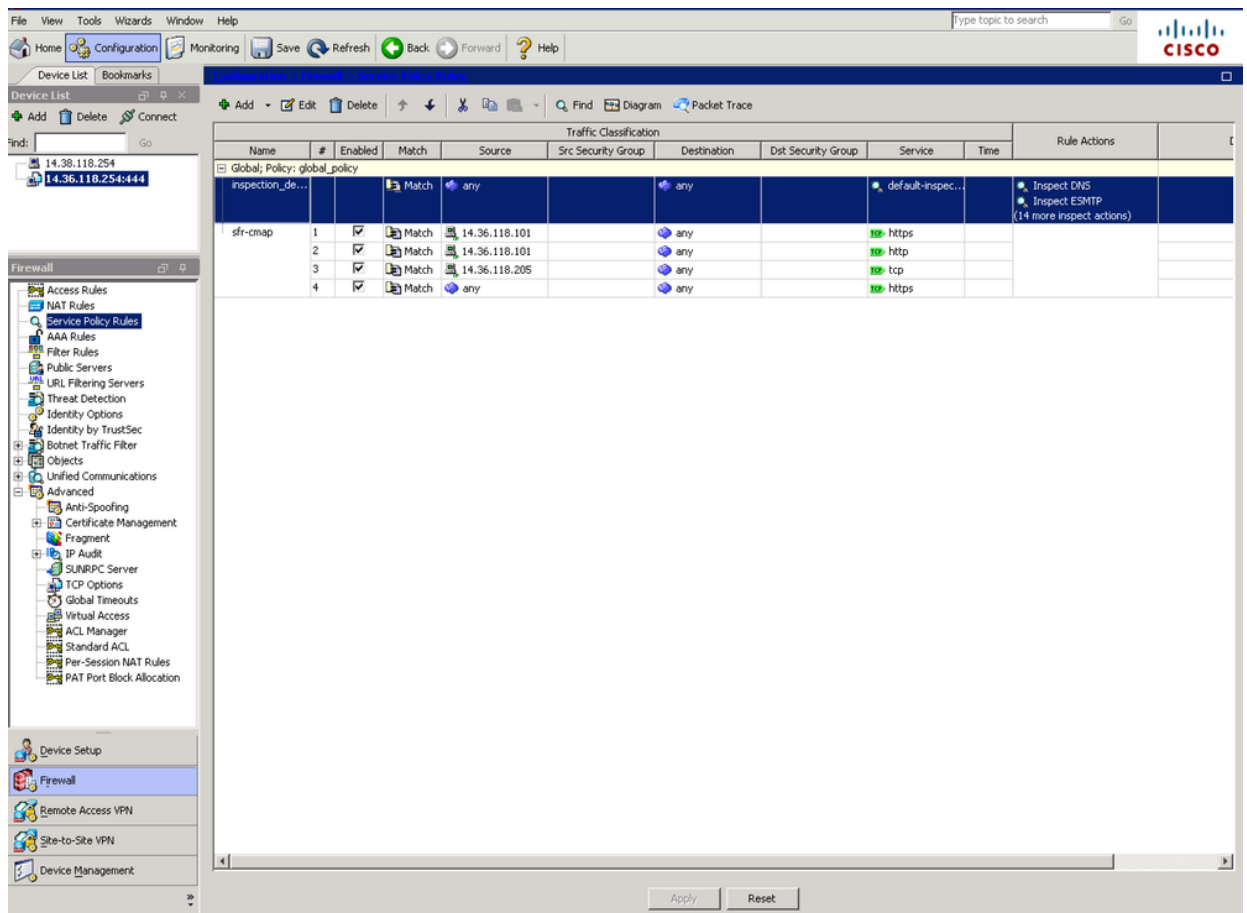
```
policy-map global_policy
class dns_inspect_cmap
inspect dns
```

5. 啟用後，您可以通過運行以下命令來驗證流量是否正在訪問排除項：

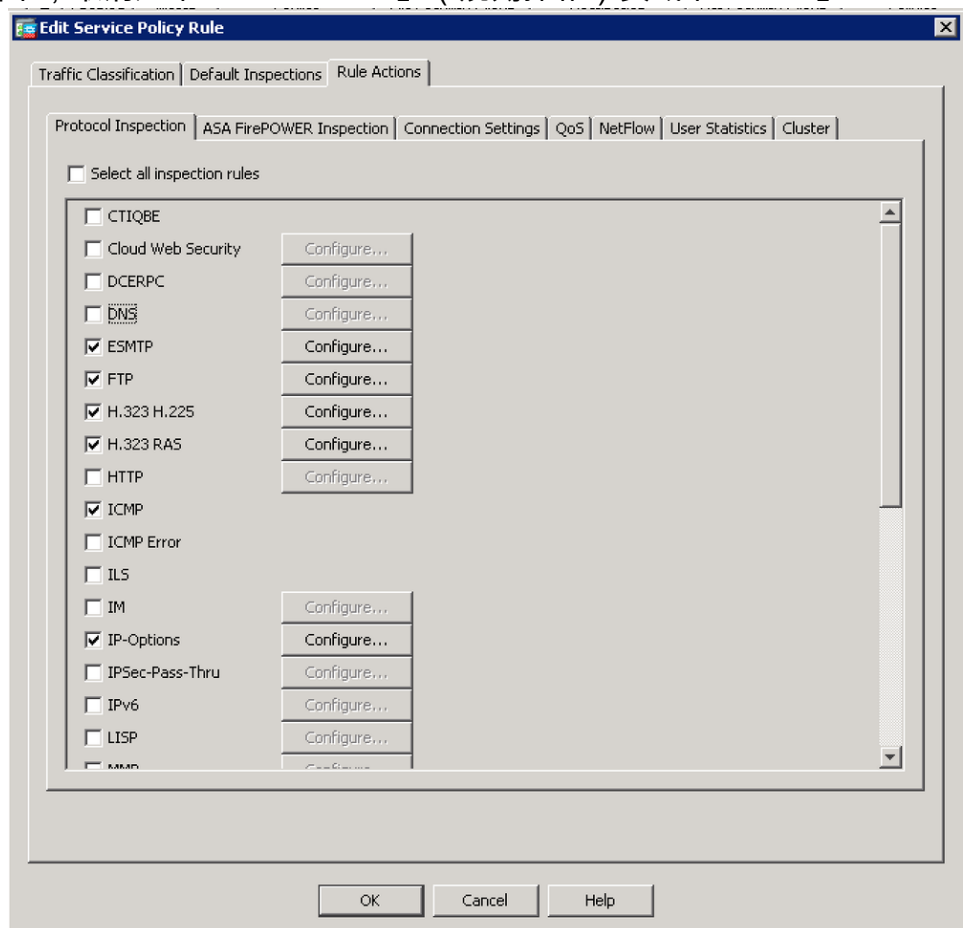
```
sh access-list dns_inspect
```

資料包檢測例外 — ASDM介面

1. 首先禁用任何DNS資料包檢測（如果適用）。此操作在配置 > 防火牆 > 服務策略規則中完成。

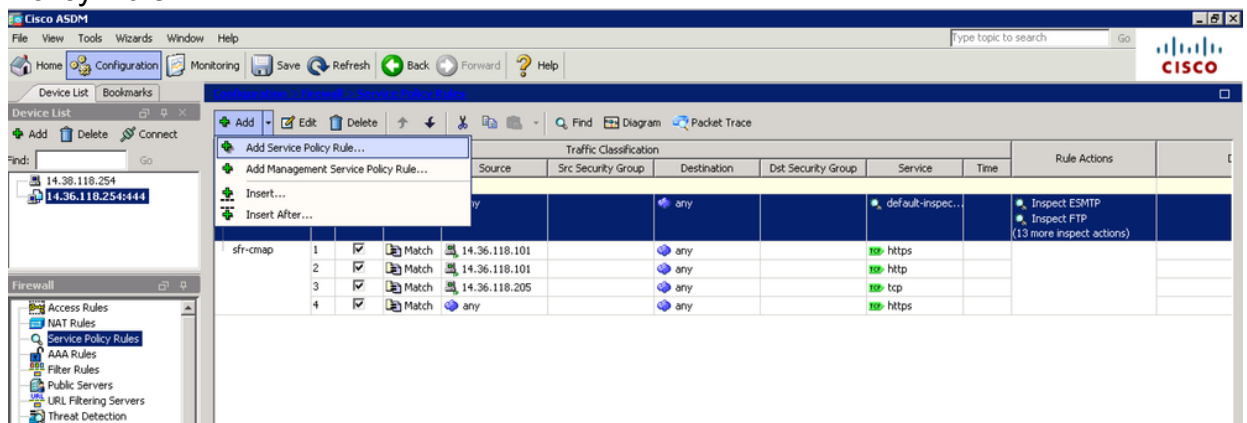


2. 在本示例中，DNS檢查在Global Policy和「inspection_default」類下啟用。選中它並按一下Edit。在新視窗中，取消選中「Rule Action」（規則操作）頁籤下「DNS」

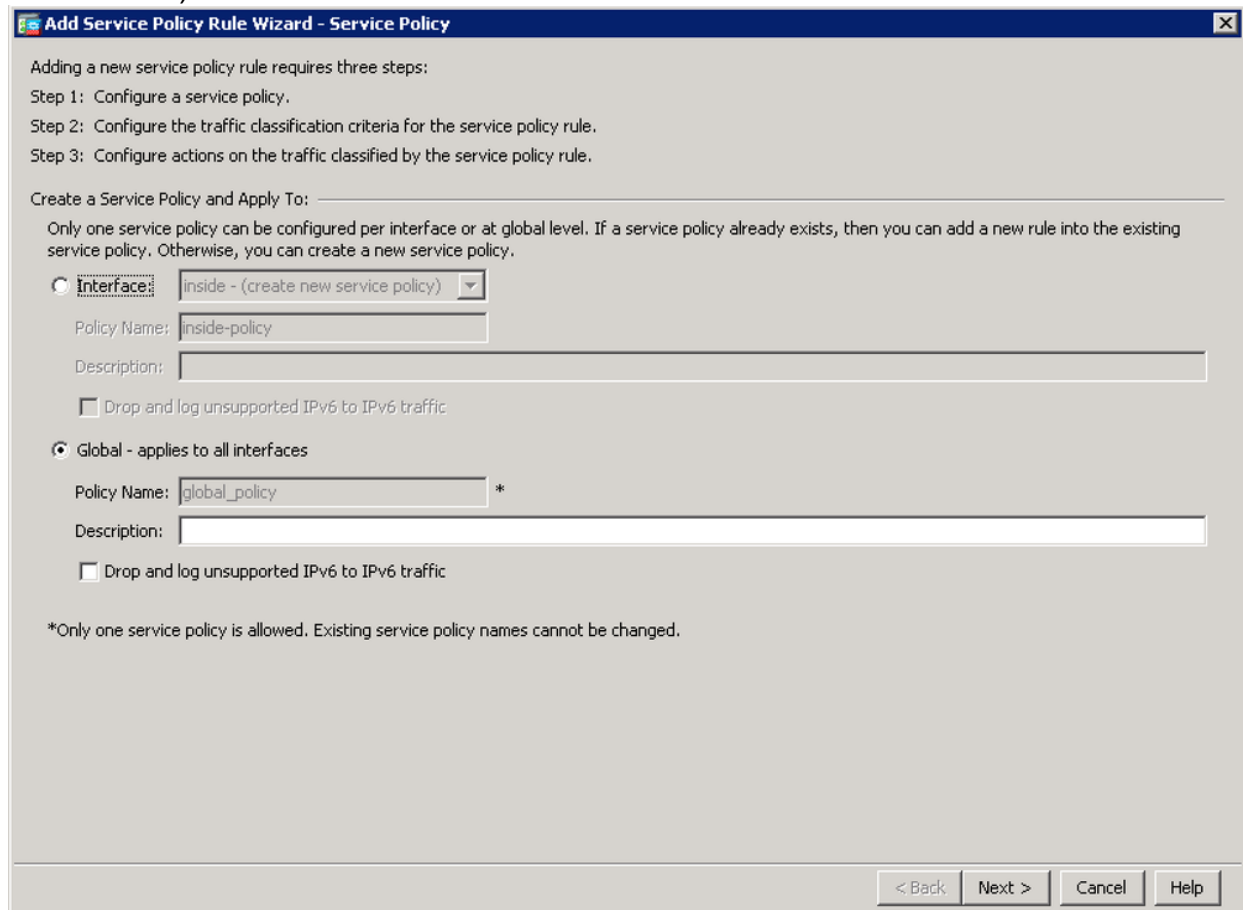


(DNS)的覈取方塊。

3. 現在，您可以重新配置DNS檢測，這次使用額外的流量免除。按一下Add > Add Service Policy Rule...



4. 選擇「全域性 — 應用於所有介面」，然後按一下下一步（如果需要，您也可以將其應用於特定介面）。



5. 為類對映指定一個名稱（例如「dns-cmap」），並選中「源和目標IP地址（使用ACL）」選項。單擊「下一步」。

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. 首先使用「不匹配」操作配置您不希望檢查的流量。
對於Source，您可以使用「any」選項免除發往Umbrella DNS伺服器的所有流量。或者，您可以在這裡建立網路對象定義，以僅免除特定的虛擬裝置IP地址。

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. 按一下Destination欄位上的.....。在下一個視窗中，按一下Add > Network Object，然後建立一個IP地址為「208.67.222.222」的對象。重複此步驟，建立IP地址為「208.67.220.220」的對象。

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:

Type:

IP Version:
☒ IPv4
☐ IPv6

IP Address:

Description:

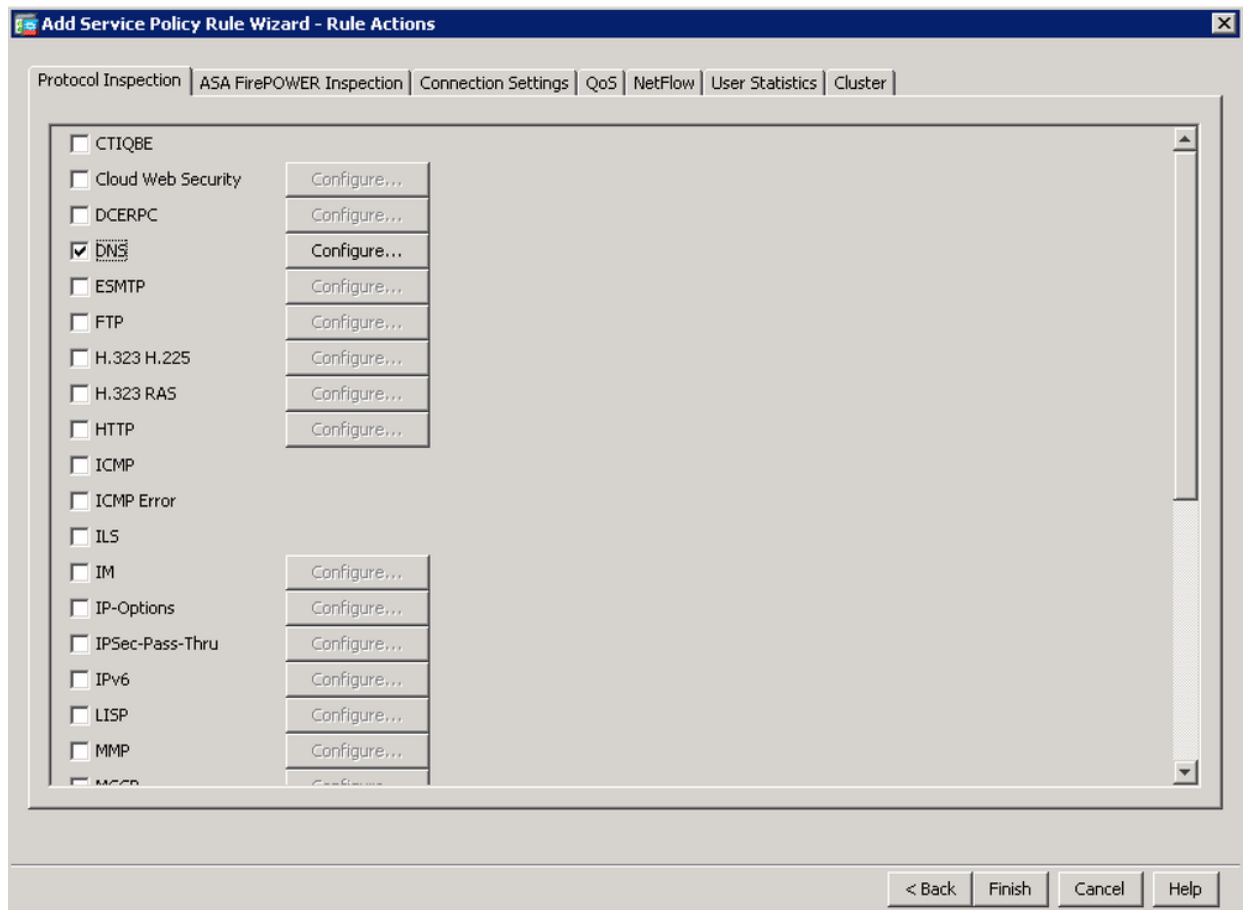
NAT

OK
Cancel
Help

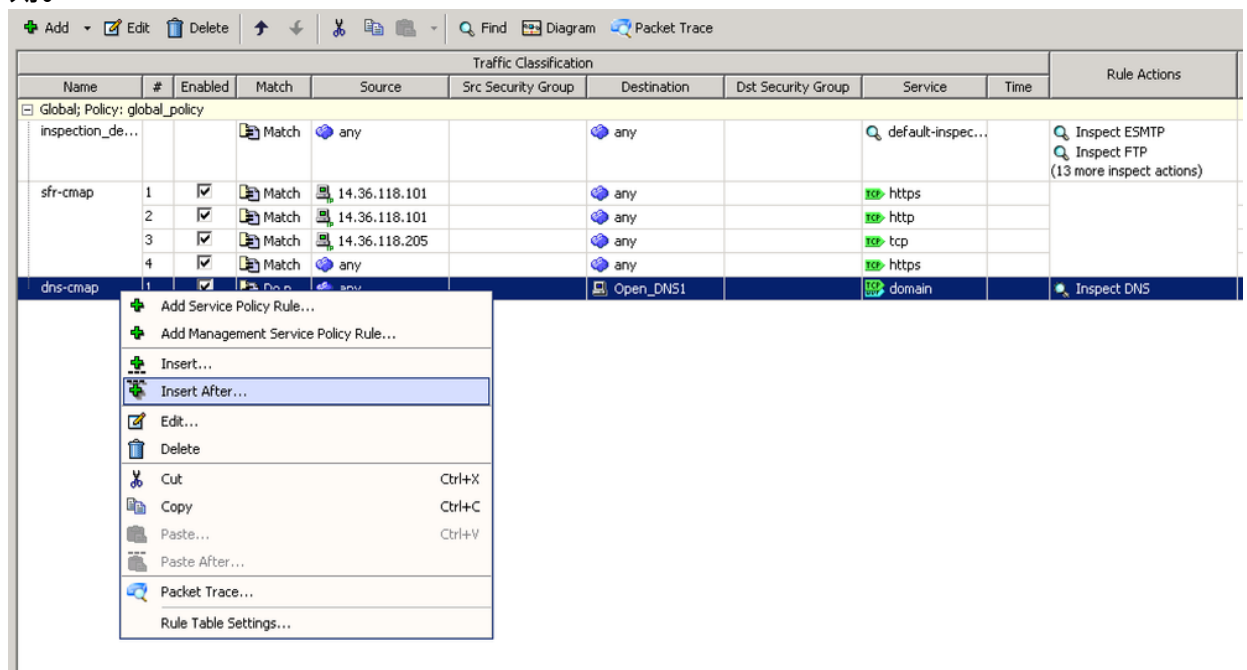
8. 將兩個Umbrella網路對象新增到Destination欄位，然後按一下OK。

The screenshot shows a Windows-style dialog box titled "Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address". At the top, there are two radio buttons for "Action": "Match" (unselected) and "Do not match" (selected). Below this, the "Source Criteria" section has three fields: "Source:" with the value "any", "User:" (empty), and "Security Group:" (empty). The "Destination Criteria" section has three fields: "Destination:" with the value "Open_DNS1", "Security Group:" (empty), and "Service:" with the value "ip". There is also a "Description:" text area which is currently empty. At the bottom of the main content area is a "More Options" section with a downward arrow. The bottom of the dialog box contains four buttons: "< Back", "Next >", "Cancel", and "Help".

9. 在下一個視窗中，選中「DNS」覈取方塊，然後按一下Finish。



10. ASA現在顯示「dns-cmap」的新全域性策略。現在，您需要配置ASA檢查的剩餘流量。這可以通過按一下右鍵「dns-cmap」並選擇選項「插入後於.....」來完成 建立新規則。



11. 在第一個視窗中，按一下Next，然後按一下，選中「Add rule to existing traffic class: (將規則新增到現有流量類:)」單選按鈕。從下拉選單中選擇「dns-cmap」，然後按一下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:

Rule can be added to an existing 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

12. 將操作保留為「Match」。選擇接受DNS檢查的流量的源、目的地和服務。例如，此處我們將匹配來自任何客戶端的流向任何TCP或UDP DNS伺服器的流量。按「Next」（下

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:

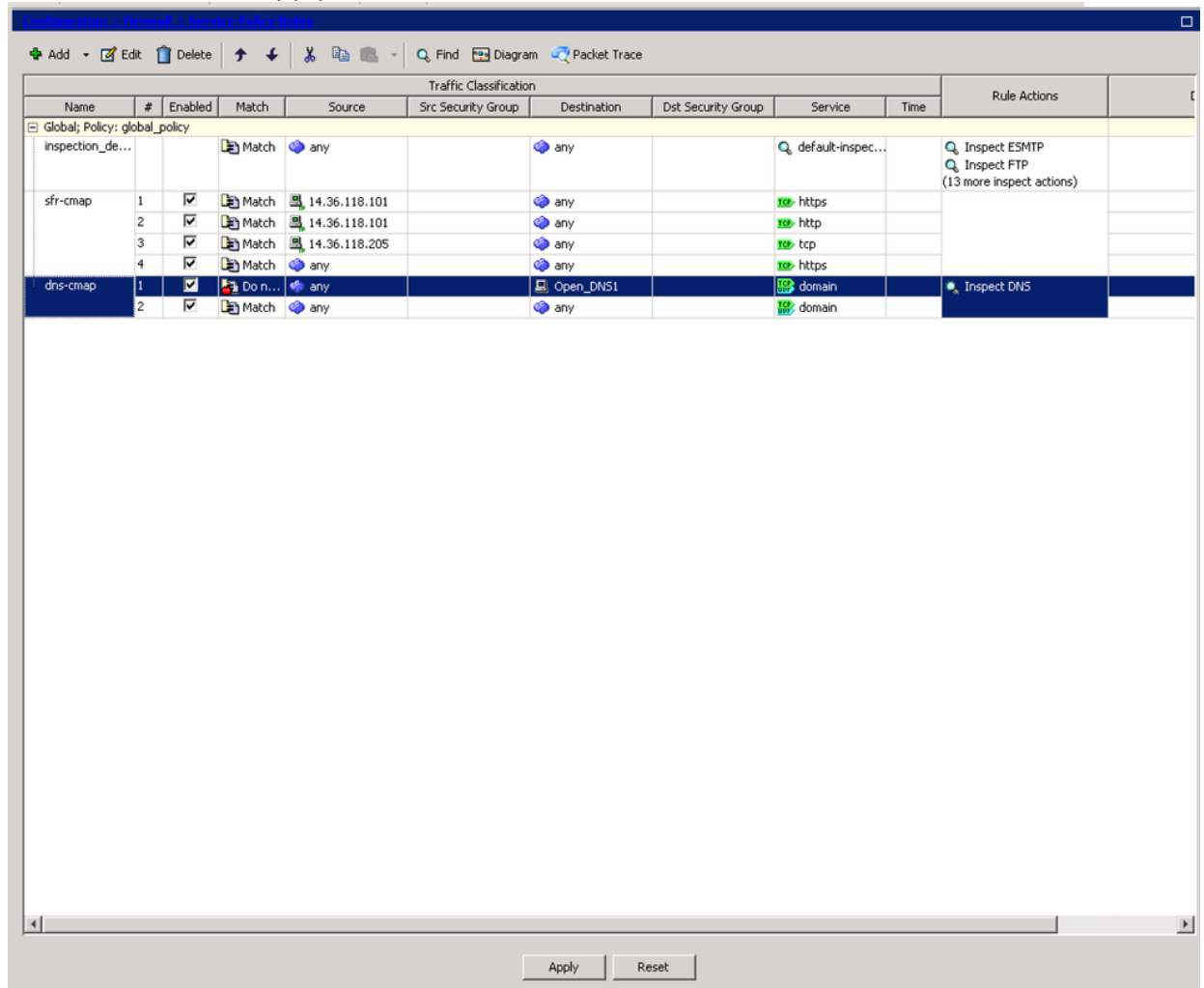
More Options

< Back Next > Cancel Help

一步)。

13. 保持選中「DNS」選項，然後按一下Finish。

14. 按一下視窗底部的Apply。



更多資訊

如果您希望禁用DNSCrypt而不是配置ASA例外，請與Umbrella支援聯絡。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。