أستكشاف أخطاء جدار حماية ASA الذي يمنع وظائف DNScyrpt من الجهاز الظاهري Umbrella وإصلاحها

المحتويات

المقدمة

نظرة عامة

السبب

دارق

استثناءات فحص الحزمة - أوامر IOS

استثناءات فحص الحزمة - واجهة ASDM

المزيد من المعلومات

المقدمة

تصف هذه المقالة كيفية أستكشاف أخطاء وظيفة حظر جدار حماية ASA وإصلاحها.

نظرة عامة

يمكن أن يقوم جدار حماية Cisco ASA بحظر وظائف DNScrypt التي يوفرها الجهاز الظاهري Umbrella. يؤدي هذا إلى تحذير لوحة معلومات المظلة هذا:

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

يمكن أيضا رؤية رسائل الخطأ هذه في سجلات جدار حماية ASA:

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

تم تصميم تشفير DNSCrypt لحماية محتويات استعلامات DNS الخاصة بك، وعلى هذا النحو، يوقف أيضا جدران الحماية من إجراء فحص الحزمة.

السبب

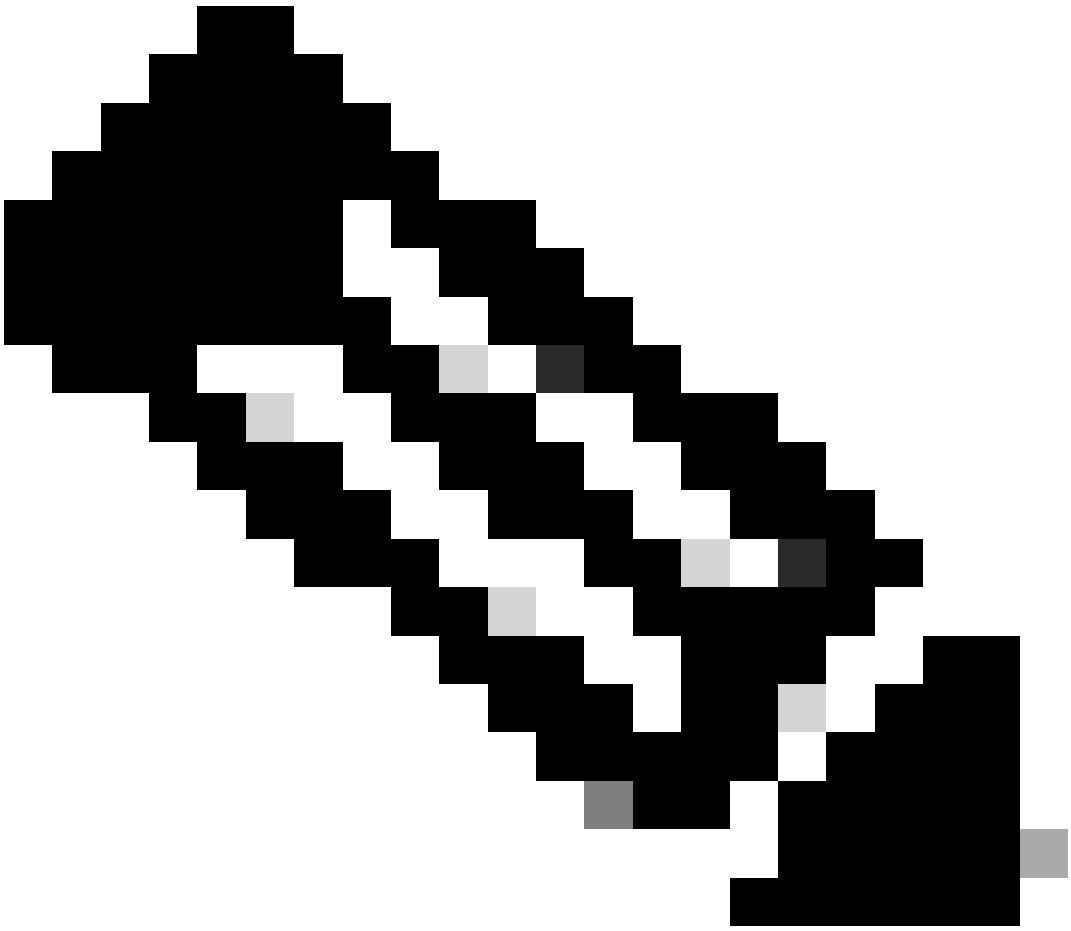
يجب ألا تتسبب هذه الأخطاء في تأثير يواجه أي مستخدم دقة DNS.

يرسل الجهاز الظاهري استعلامات الاختبار لتحديد توفر DNScrypt وهي استعلامات الاختبار

التي تم حظرها. ومع ذلك، تشير رسائل الخطأ هذه إلى أن الجهاز الظاهري لا يضيف أمانا إضافيا من خلال تشفير حركة مرور DNS الخاصة بشركتك.

قرار

نوصي بتعطيل فحص حزم DNS لحركة مرور البيانات بين الجهاز الظاهري ومحققي DNS ل Umbrella. على الرغم من أن هذا يعجز التسجيل وفحص البروتوكول على ASA، فإنه يحسن الأمان بالسماح بتشفير DNS.



ملاحظة: يتم توفير هذه الأوامر للتوجيه فقط ويوصى باستشارة خبير Cisco قبل إجراء أي تغييرات على بيئة الإنتاج.
أيضا كن على علم بهذا العيب على ASA قد يؤثر على DNS عبر TCP، والذي يمكن أن يتسبب أيضا في مشاكل مع DNSCrypt:
دعم فحص DNS CSCsm90809 ل DNS عبر TCP

إستثناءات فحص الحزمة - أوامر IOS

1. قم بإنشاء قائمة تحكم في الوصول (ACL) جديدة تسمى 'dns_inspection' مع قواعد لرفض حركة المرور إلى 208.67.220.220 و 208.67.222.222.
<#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. قم بإزالة سياسة فحص DNS الحالية على ASA. على سبيل المثال:

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

3. إنشاء خريطة فئة تطابق قائمة التحكم في الوصول (ACL) التي تم إنشاؤها في الخطوة #1:

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

4. قم بتكوين خريطة سياسة ضمن global_policy. يجب أن يتطابق هذه مع خريطة الفئة التي تم إنشاؤها في الخطوة #3. قم بتمكين فحص DNS.

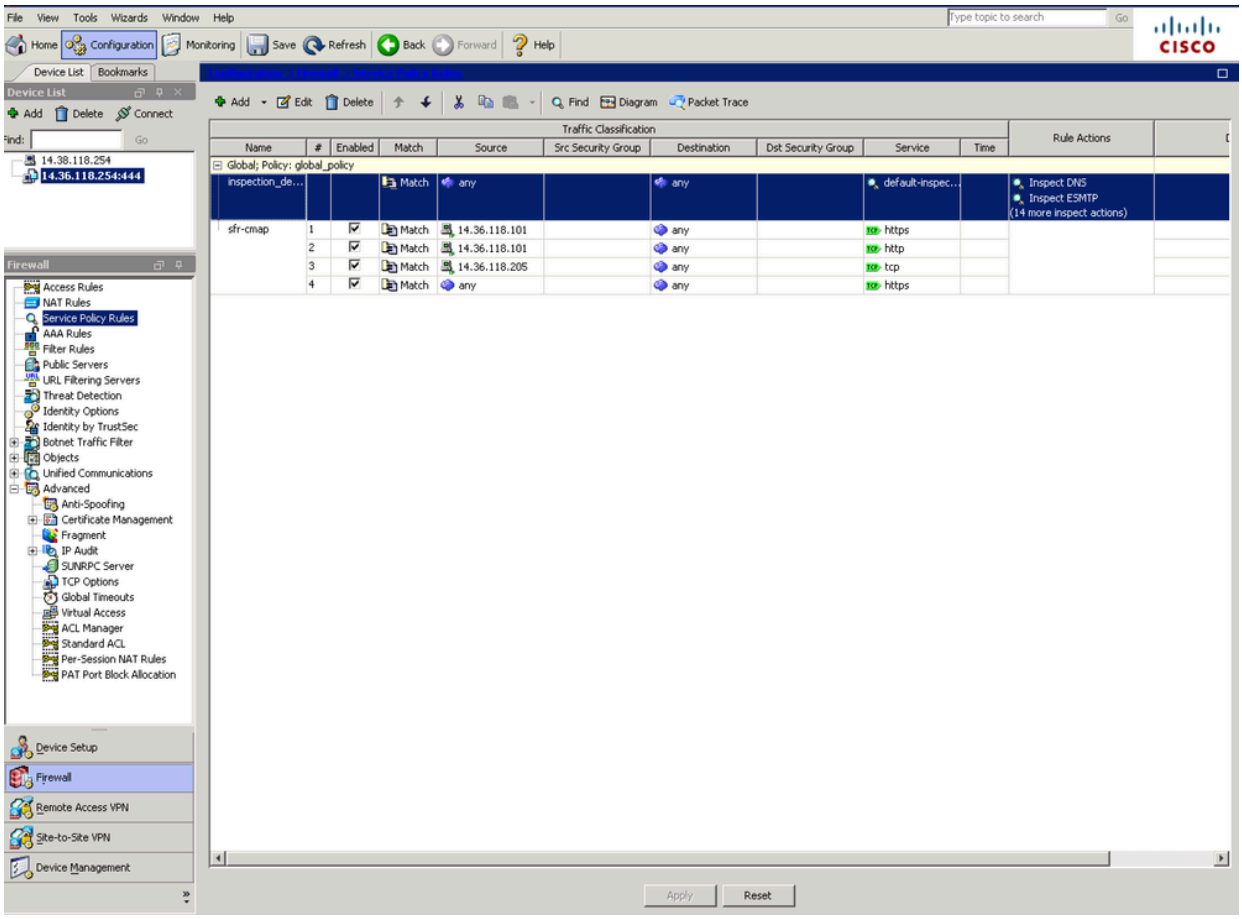
```
policy-map global_policy
 class dns_inspect_cmap
  inspect dns
```

5. وبمجرد تمكينها، يمكنك التحقق من أن حركة المرور تصل إلى الاستبعاد عن طريق التشغيل:

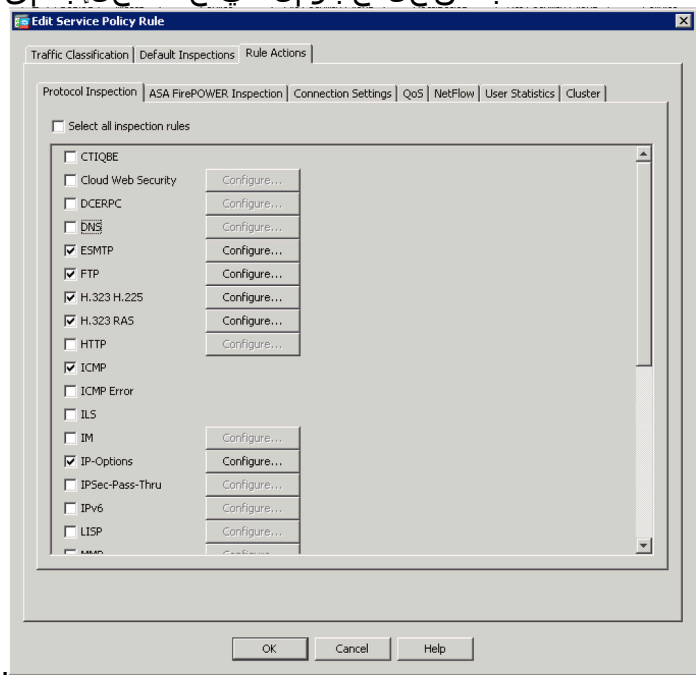
```
sh access-list dns_inspect
```

إستثناءات فحص الحزم - واجهة ASDM

1. قم بالوصول إلى أي فحص لحزم DNS إذا كان ذلك ممكنا.وتم ذلك في التكوين > جدار الحماية > قواعد سياسة الخدمة.

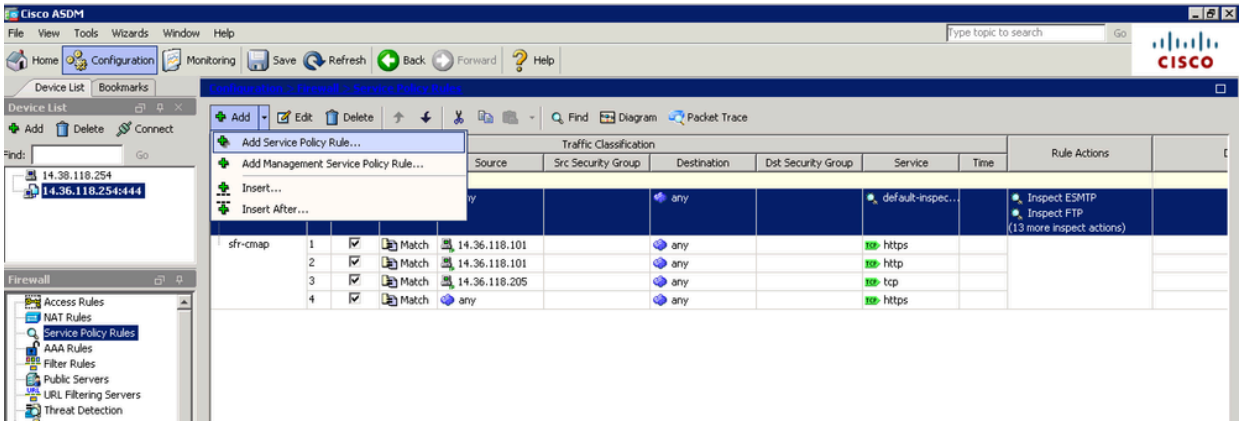


2. في المثال، يتم تمكين فحص DNS ضمن الفئة "نهج عام" و"فحص_default". ركز هو وطقطقة حررت. في الإطار الجديد، قم بإلغاء تحديد المربع الخاص ب "DNS"

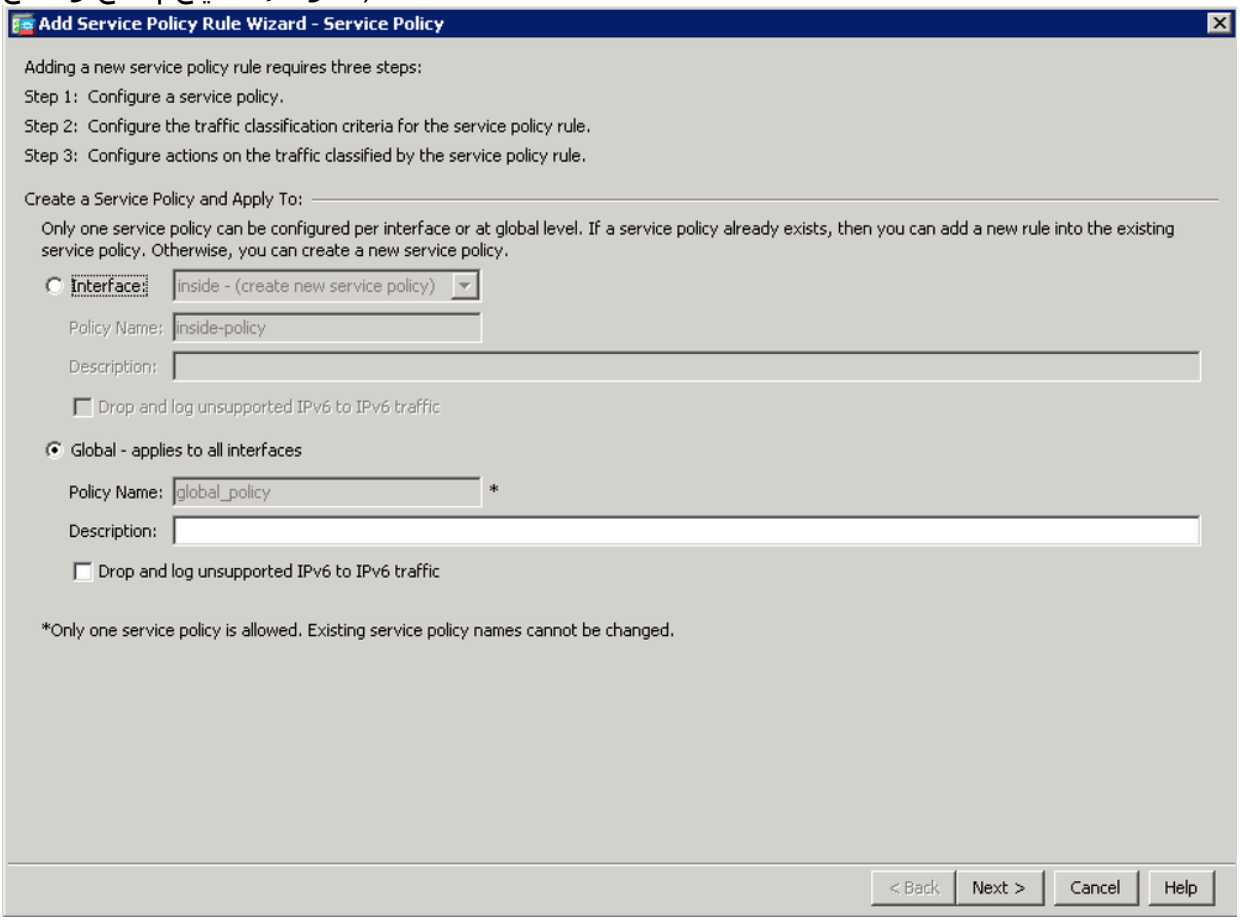


ضمن علامة التبويب "إجراء القاعدة".

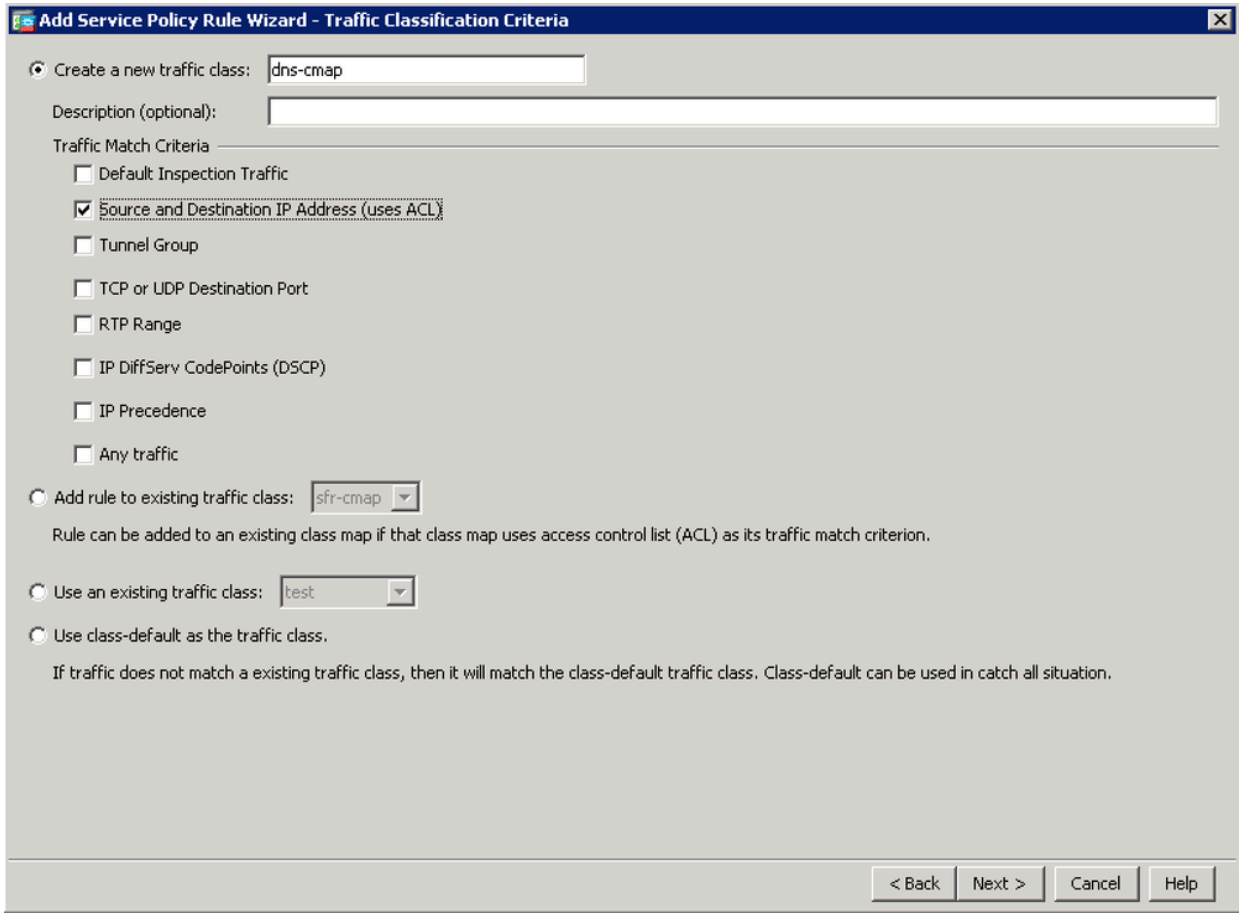
3. الآن يمكنك إعادة تكوين فحص DNS، هذه المرة مع إعفاءات حركة المرور الإضافية. انقر فوق إضافة > قاعدة نهج الخدمة Add Service Policy...



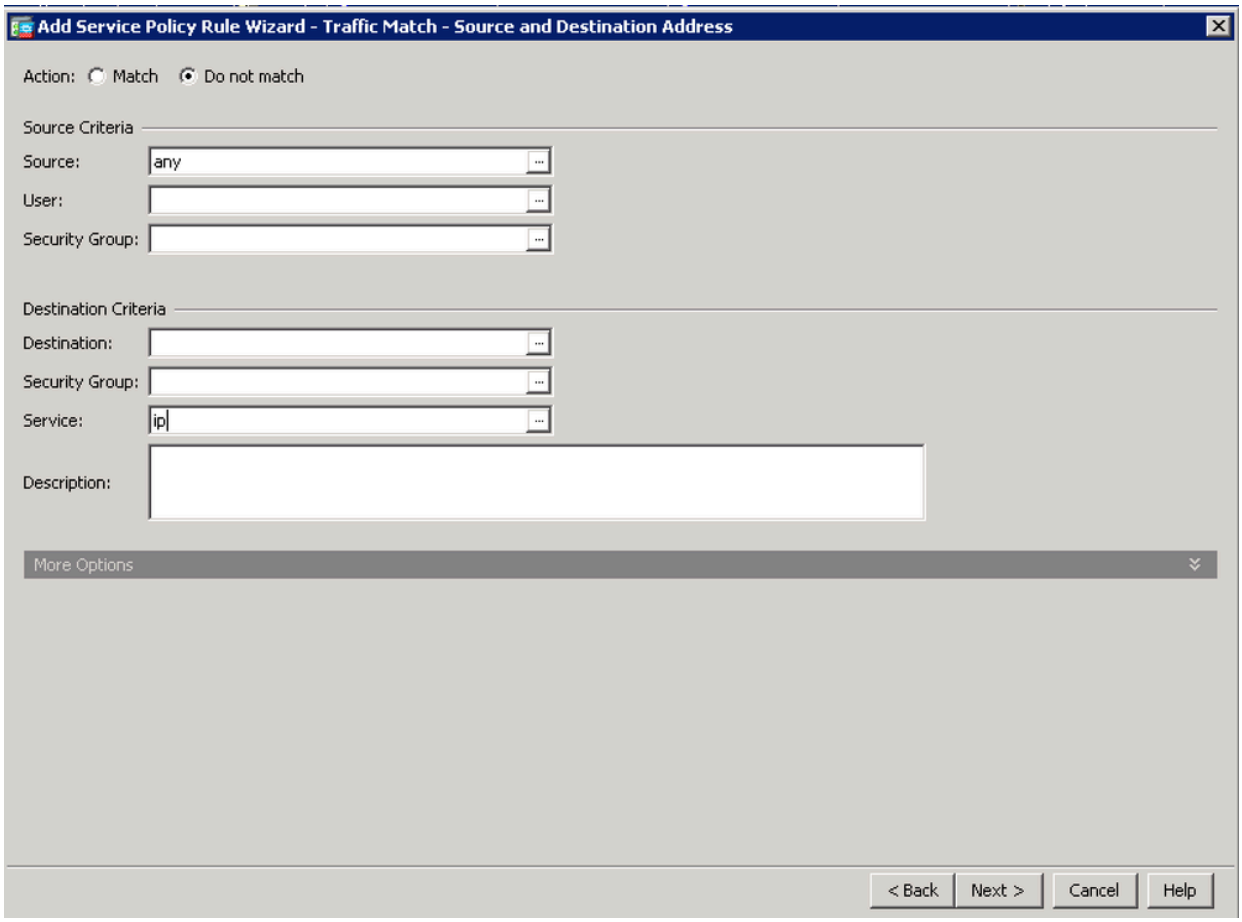
4. حدد "عام - يطبق على جميع الواجهات" وانقر على التالي (يمكنك أيضا تطبيق هذه على واجهة معينة إذا أردت).



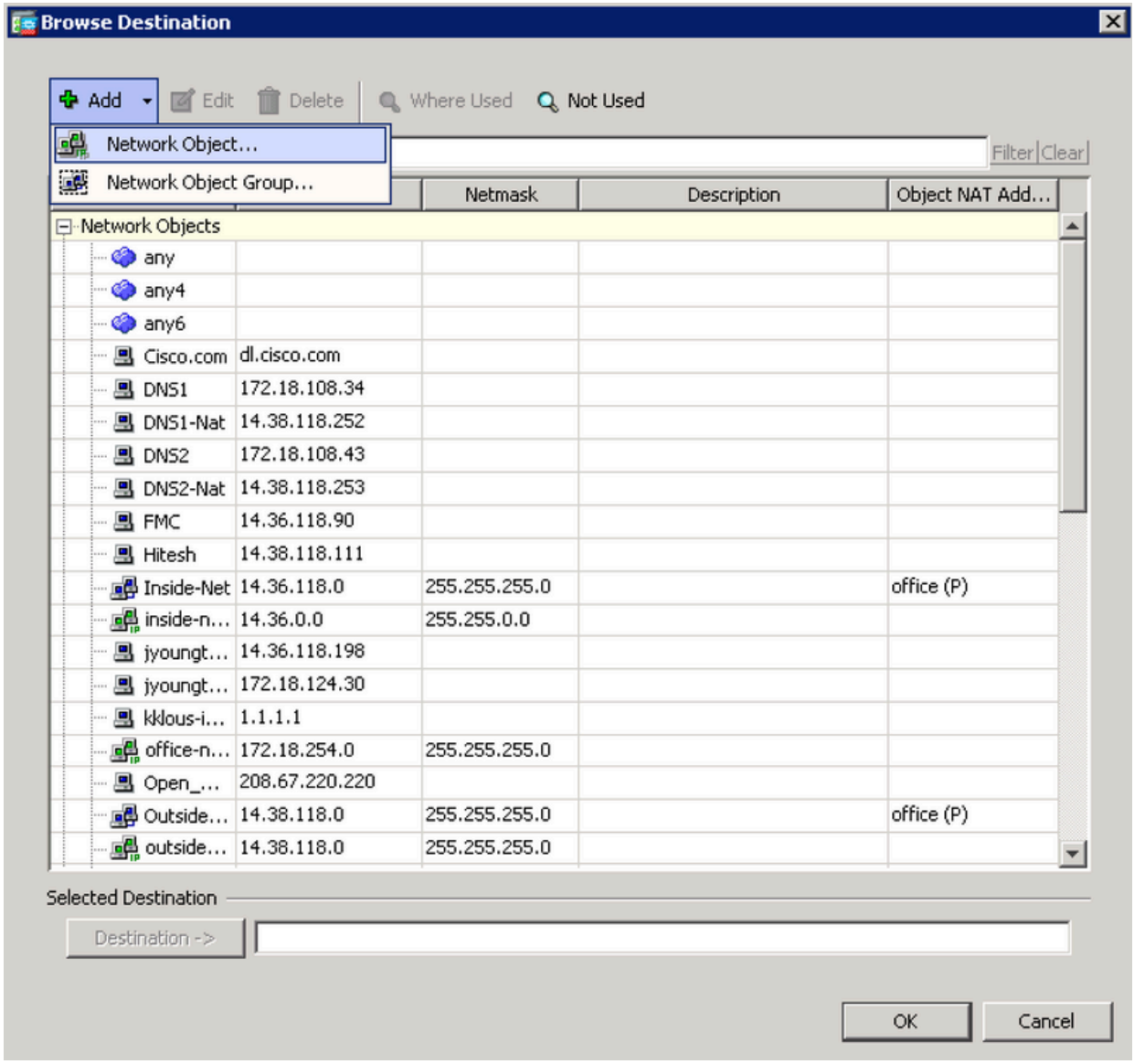
5. قم بإعطاء اسم لخريطة الفئة (على سبيل المثال 'dns-cmap') وحدد الخيار "عنوان IP المصدر والوجهة (يستخدم قائمة التحكم في الوصول)". انقر التالي.

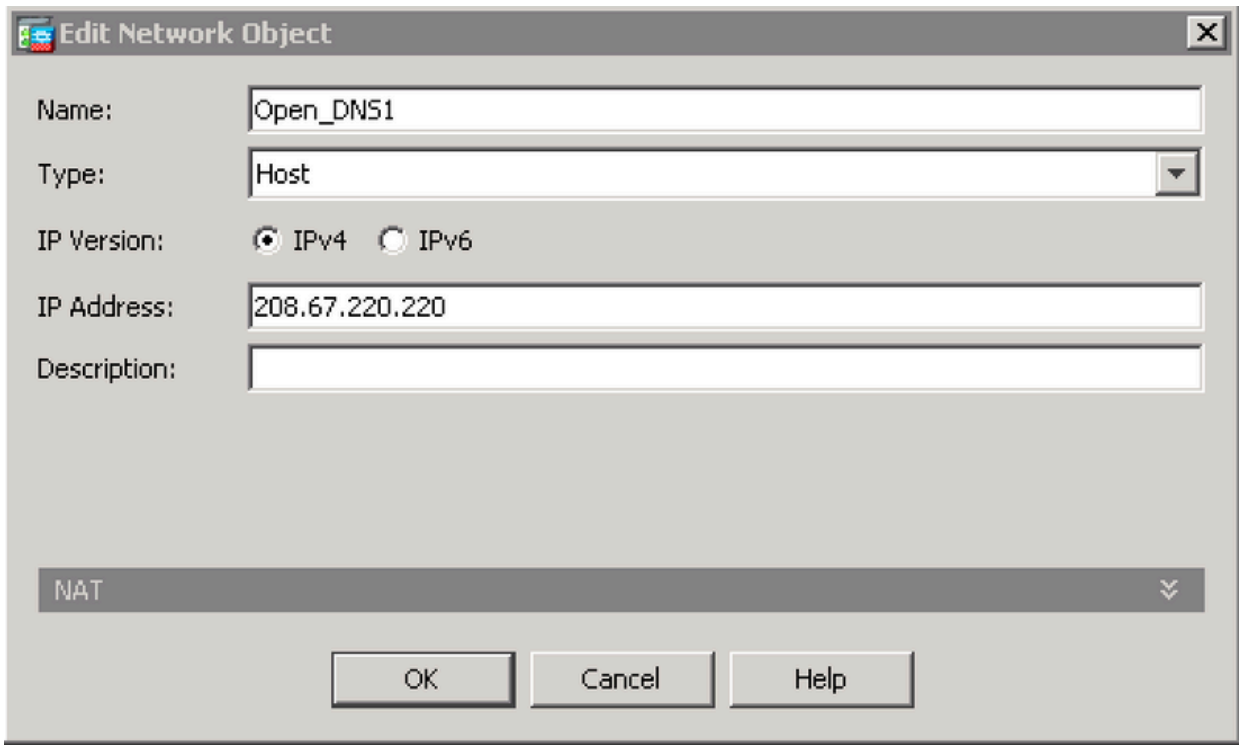


6. ابدأ بتكوين حركة المرور التي لا تريد فحصها باستخدام الإجراء "عدم المطابقة". للمصدر، يمكنك إستخدام الخيار "أي" لإعفاء حركة المرور الموجهة إلى خوادم DNS الخاصة ب Umbrella. بدلا من ذلك، يمكنك إنشاء تعريف كائن شبكة هنا لاستثناء عنوان IP الخاص بالجهاز الظاهري فقط.

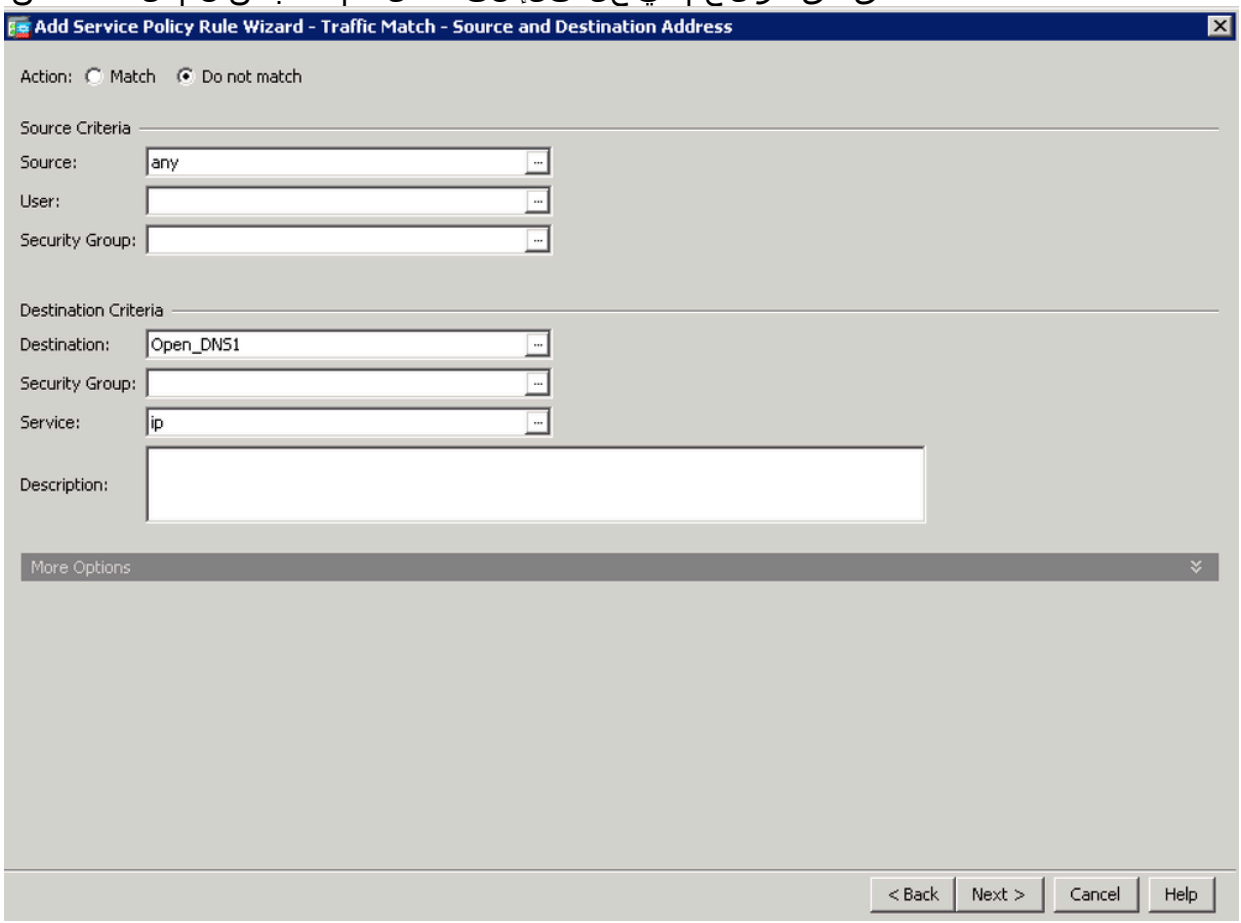


7. طقطقت ... على الغاية مجال. في الإطار التالي، انقر على إضافة > كائن الشبكة وقم بإنشاء كائن باستخدام عنوان IP الخاص ب '208.67.222.222'. كرر هذه الخطوة لإنشاء كائن بعنوان IP '208.67.220.220'.

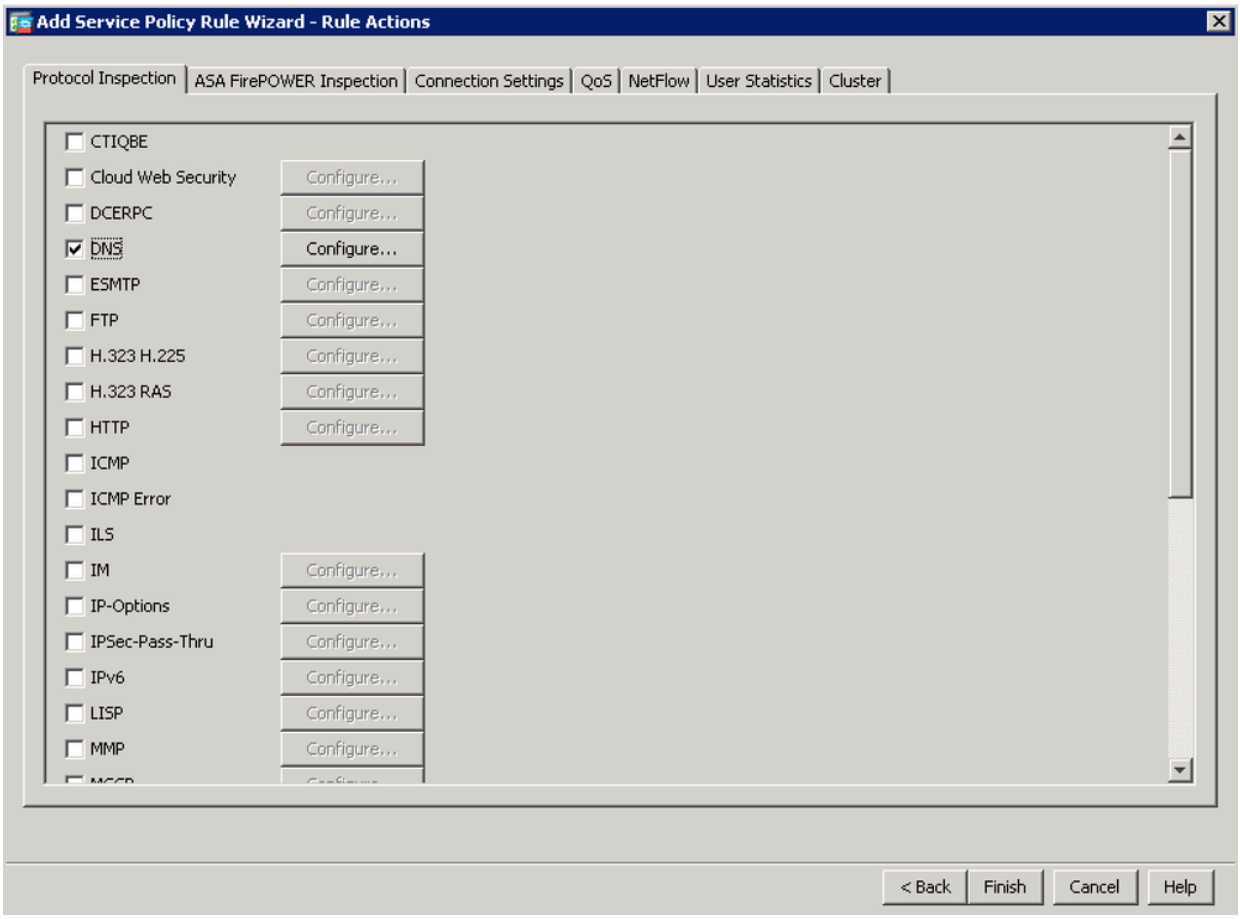

Browse Destination
Add
Edit
Delete
Where Used
Not Used
Network Object...
Network Object Group...
Filter
Clear
Netmask
Description
Object NAT Add...
Network Objects
any
any4
any6
Cisco.com dl.cisco.com
DNS1 172.18.108.34
DNS1-Nat 14.38.118.252
DNS2 172.18.108.43
DNS2-Nat 14.38.118.253
FMC 14.36.118.90
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: Open_DNS1
Type: Host
IP Version: IPv4 IPv6
IP Address: 208.67.220.220
Description:
NAT
OK
Cancel
Help

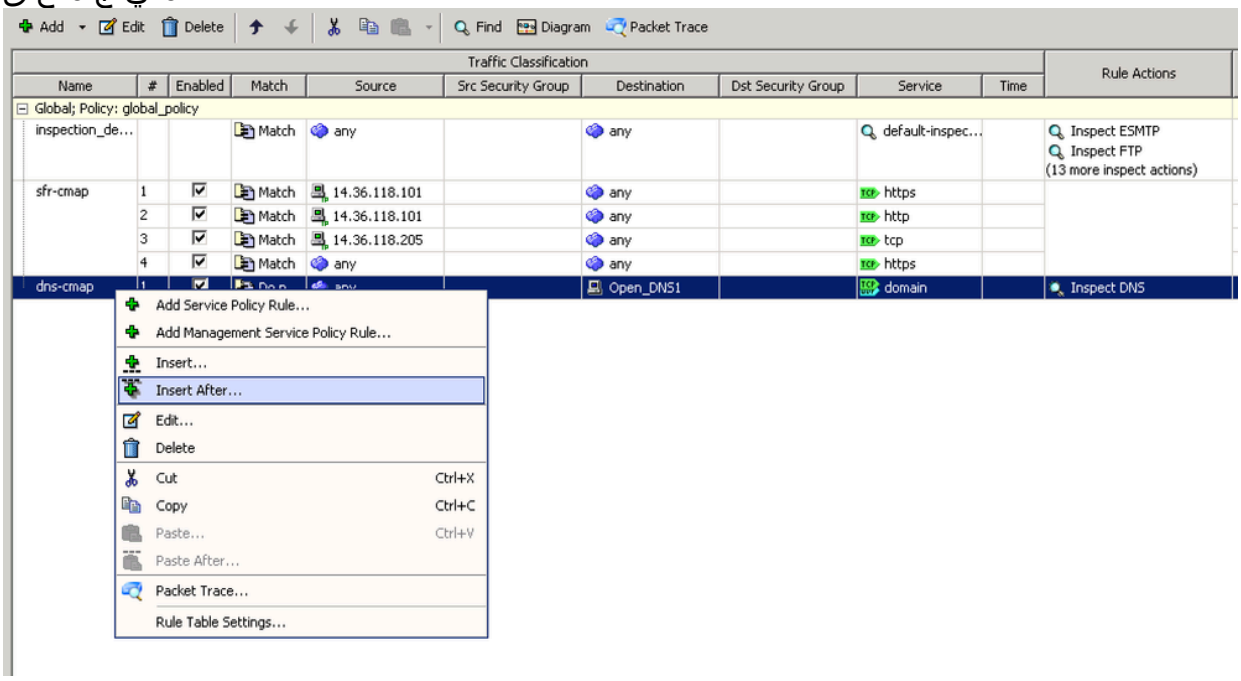
8. أضفت كل من شبكة مظلة كائن إلى الغاية مجال وطقطقة ok.



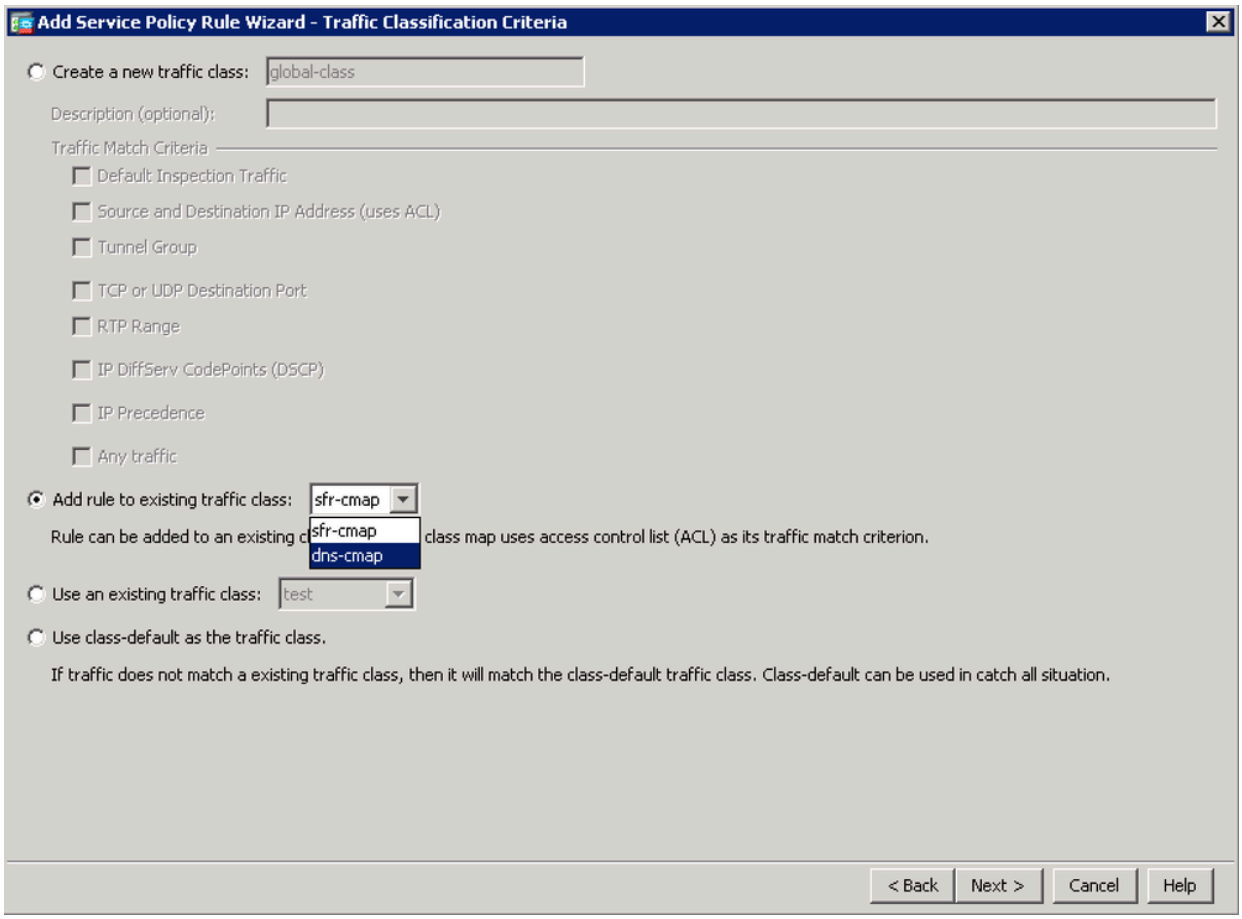
9. في الإطار التالي، حدد المربع "DNS" وانقر فوق إنهاء.



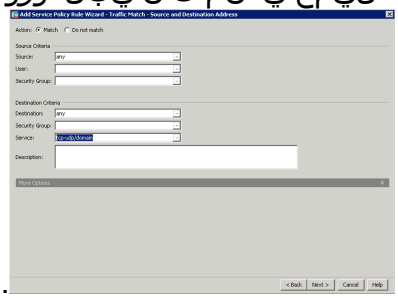
10. يعرض ASA الآن السياسة العالمية الجديدة لـ 'dns-cmap'. أنت تحتاج الآن أن يشكل الحركة مرور متبق أن يكون فحصت ب الـ ASA. ويتم القيام بذلك من خلال النقر بزر الماوس الأيمن فوق 'dns-cmap' وتحديد الخيار "إدراج بعد..." مما يخلق قاعدة جديدة.



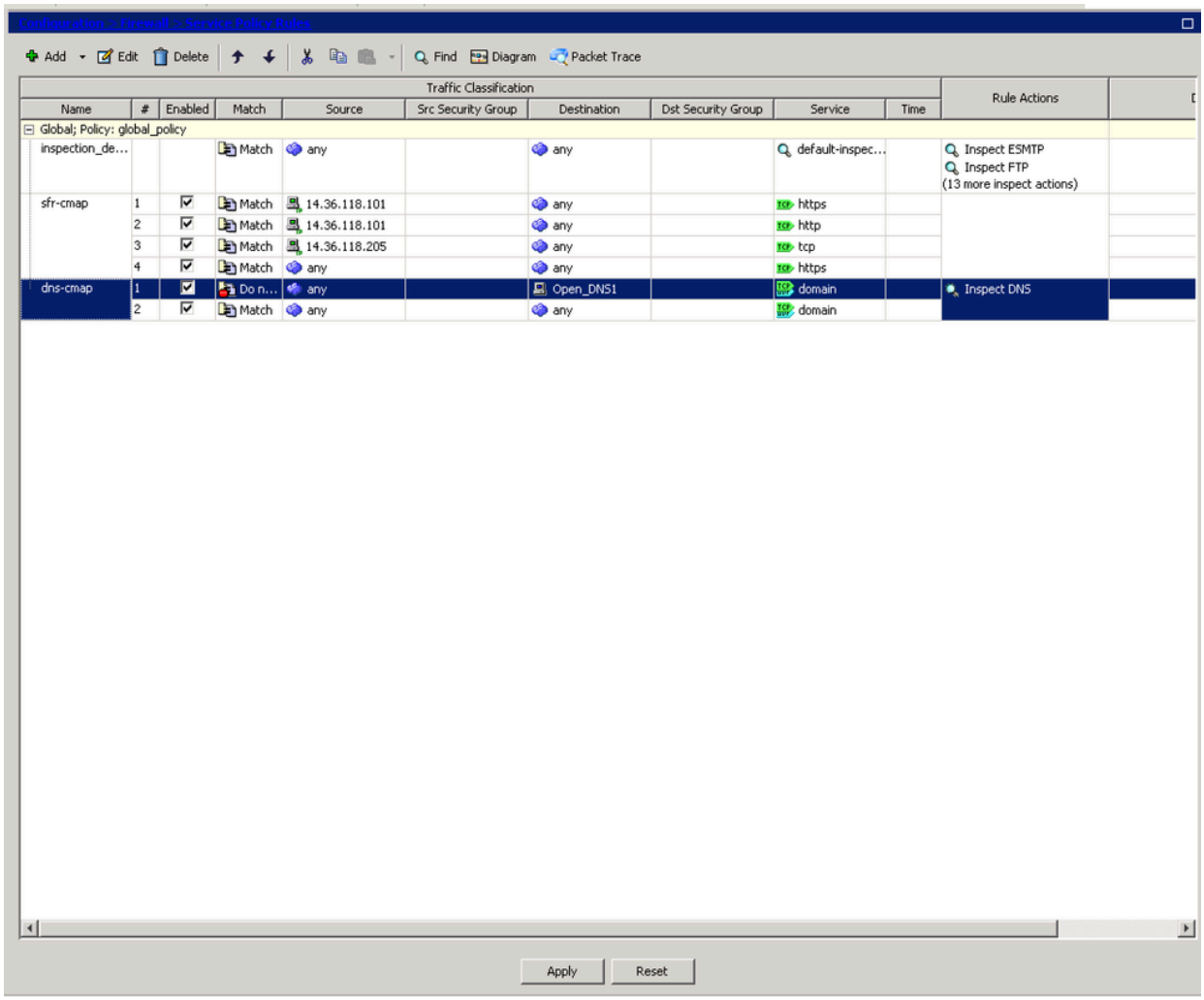
11. في أول نافذة انقر على التالي ثم على زر "إضافة قاعدة إلى فئة حركة المرور الموجودة:". حدد "DNS-cmap" من القائمة المنسدلة ثم انقر فوق التالي.



12. أترك الإجراء ك 'Match'. أختر مصدر حركة المرور التي تخضع لتفتيش DNS ووجهتها وخدمتها. على سبيل المثال، نحن نطابق حركة مرور البيانات من أي عميل يذهب إلى خادم TCP أو UDP DNS. انقر فوق Next (التالي).



13. أترك الخيار 'DNS' محددا وانقر على إنهاء.
14. انقر فوق تطبيق في أسفل النافذة.



المزيد من المعلومات

إذا كنت تفضل تعطيل DNScrypt بدلا من تكوين إعفاءات ASA، فيرجى الاتصال بدعم Umbrella.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).