PIX/ASA: تنفيذ إرساء DNS باستخدام الأمر الثابت وواجهات NAT إثنين مثال تكوين

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
معلومات أساسية
السيناريو: واجهات NAT (من الداخل والخارج)
طوبولوجيا
المشكلة: يتعذر على العميل الوصول إلى خادم WWW
الحل: الكلمة الأساسية "DNS"
الحل البديل: تسريحة الشعر
تكوين فحص DNS
تكوين Split-DNS
التحقق من الصحة
التقاط حركة مرور DNS
استكشاف الأخطاء وإصلاحها
لم يتم إجراء إعادة كتابة DNS
فشل إنشاء الترجمة
إسقاط رد UDP DNS
معلومات ذات صلة

المقدمة

يزود هذا وثيقة عينة تشكيل أن ينجز domain name نظام (DNS) توثيق على ال ASA 5500 sery أمن أداة أو PIX 500 sery أمن أداة يستعمل ساكن إستاتيكي شبكة عنوان ترجمة (NAT) عبارة. يسمح توثيق DNS لجهاز الأمان بإعادة كتابة سجلات DNS A.

تؤدي إعادة كتابة DNS وظيفتين:

- يترجم عنوان عام (الموجه أو العنوان المعين) في رد DNS إلى عنوان خاص (العنوان الحقيقي) عندما يكون عميل DNS على واجهة خاصة.
- يترجم عنوان خاص إلى عنوان عام عندما يكون عميل DNS على الواجهة العامة.

ملاحظة: يحتوي التكوين الوارد في هذا المستند على واجهات NAT؛ في الداخل والخارج. على سبيل المثال، إرساء DNS مع ستاتيكس وثلاث واجهات NAT (في الداخل والخارج و DMZ)، ارجع إلى PIX/ASA: تنفيذ إرساء DNS باستخدام الأمر الثابت وثلاث أمثلة تكوين واجهات NAT.

راجع عبارات PIX/ASA 7.x NAT و PAT واستخدام أوامر nat و global و static و route و access-list وإعادة توجيه المنفذ (إعادة توجيه) على PIX للحصول على مزيد من المعلومات حول كيفية إستخدام NAT على جهاز الأمان.

المتطلبات الأساسية

المتطلبات

يجب تمكين فحص DNS من أجل تنفيذ إرساء DNS على جهاز الأمان. يكون فحص DNS قيد التشغيل بشكل افتراضي. إذا كان قد تم إيقاف تشغيله، فراجع قسم تكوين فحص DNS لاحقا في هذا المستند لإعادة تمكينه. عند تمكين فحص DNS، يقوم جهاز الأمان بتنفيذ المهام التالية:

- يترجم سجل DNS بناء على التشكيل مكتمل باستخدام الأوامر **الثابتة** و**nat** (إعادة كتابة DNS). تنطبق الترجمة فقط على السجل A في الرد على DNS. لذلك، لا تتأثر عمليات البحث العكسية، التي تطلب سجل PTR، بإعادة كتابة DNS.**ملاحظة:** لا تتوافق إعادة كتابة DNS مع ترجمة عنوان المنفذ الثابت (PAT) لأن قواعد PAT المتعددة تنطبق على كل سجل A، وقاعدة PAT التي سيتم إستخدامها غامضة.
- فرض الحد الأقصى لطول رسالة DNS (الافتراضي هو 512 بايت والحد الأقصى للطول هو 65535 بايت). يتم إجراء إعادة التجميع حسب الضرورة للتحقق من أن طول الحزمة أقل من الحد الأقصى للطول الذي تم تكوينه. يتم إسقاط الحزمة إذا تجاوزت الحد الأقصى للطول.**ملاحظة:** إذا قمت بإصدار الأمر **فحص DNS** دون خيار الحد الأقصى للطول، لا يتم التحقق من حجم حزمة DNS.
- فرض طول اسم المجال 255 بايت وطول التسمية 63 بايت.
- للتحقق من سلامة اسم المجال المشار إليه بواسطة المؤشر في حالة مواجهة مؤشرات الضغط في رسالة DNS.
- يتحقق لمعرفة ما إذا كانت حلقة مؤشر الضغط موجودة أم لا.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان ASA 5500 Series Security Appliance، الإصدار 7.2(1).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX 500 Series Security Appliance، الإصدار 6.2 أو إصدار أحدث.

ملاحظة: ينطبق تكوين مدير أجهزة الأمان المعدلة (ASDM) من Cisco على الإصدار x.7 فقط.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

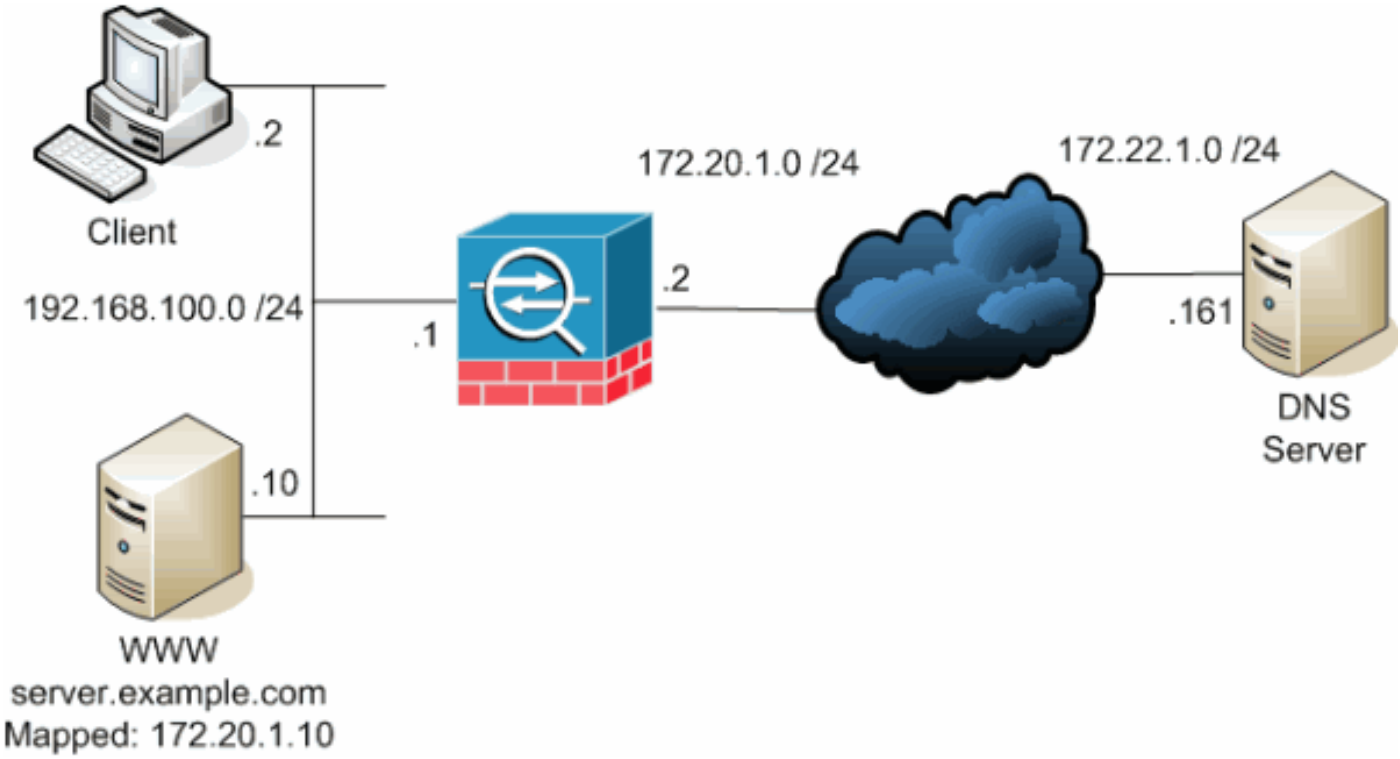
في تبادل DNS نموذجي يرسل العميل عنوان URL أو اسم المضيف إلى خادم DNS لتحديد عنوان IP لذلك المضيف. يتلقى خادم DNS الطلب، ويبحث عن تعيين اسم إلى عنوان IP لذلك المضيف، ثم يوفر السجل A مع عنوان IP

للعميل. في حين أن هذا الإجراء يعمل بشكل جيد في العديد من الحالات، إلا أنه من الممكن أن تحدث مشاكل. يمكن أن تحدث هذه المشاكل عندما يكون العميل والمضيف الذي يحاول العميل الوصول إليه على الشبكة الخاصة نفسها خلف NAT، ولكن خادم DNS الذي يستخدمه العميل يكون على شبكة عامة أخرى.

السيناريو: واجهات NAT (من الداخل والخارج)

طوبولوجيا

في هذا السيناريو، يقع العميل وخادم WWW الذي يحاول العميل الوصول إليه على الواجهة الداخلية ل ASA. تم تكوين ميزة PAT الديناميكية للسماح للعميل بالوصول إلى الإنترنت. شكلت NAT ساكن إستاتيكي مع قائمة منفذ أن يسمح الخادم منفذ إلى الإنترنت، as well as يسمح إنترنت مضيف أن ينفذ ال WWW نادل.



هذا رسم بياني مثال من هذا حالة. في هذه الحالة، يريد العميل في 192.168.100.2 إستخدام عنوان URL **server.example.com** للوصول إلى خادم WWW على 192.168.100.10. يتم توفير خدمات DNS للعميل بواسطة خادم DNS الخارجي في 172.22.1.161. نظرا لوجود خادم DNS على شبكة عامة أخرى، فإنه لا يعرف عنوان IP الخاص لخادم WWW. بدلا من ذلك، فإنه يعرف العنوان المعين لخادم WWW وهو 172.20.1.10. وبالتالي، يحتوي خادم DNS على تعيين IP لعنوان إلى اسم **server.example.com** إلى **172.20.1.10**.

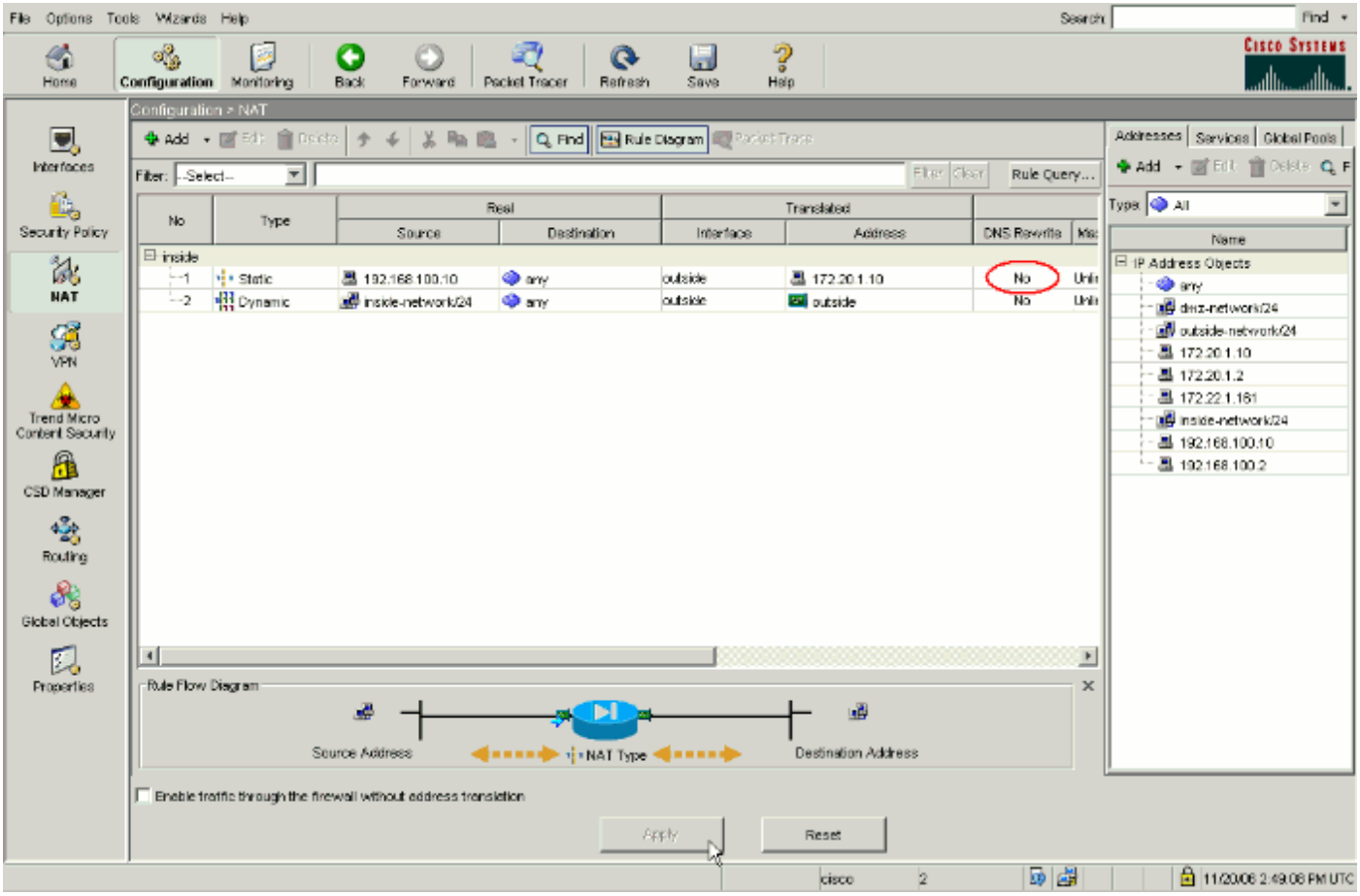
المشكلة: يتعذر على العميل الوصول إلى خادم WWW

بدون تعليمات DNS أو حل آخر ممكن في هذه الحالة، إذا أرسل العميل طلب DNS لعنوان IP الخاص ب server.example.com، فلن يتمكن من الوصول إلى خادم WWW. وذلك لأن العميل يستلم سجلا A يحتوي على العنوان العام المعين: 172.20.1.10 من خادم WWW. عندما يحاول العميل الوصول إلى عنوان IP هذا، يسقط جهاز الأمان الحزم لأنه لا يسمح بإعادة توجيه الحزمة على الواجهة نفسها. فيما يلي ما يبدو عليه جزء NAT من التكوين عندما لا يتم تمكين DNS doctoring:

```
ciscoasa(config)#show running-config
Saved :
:
(ASA Version 7.2(1
```

```
!
hostname ciscoasa

Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- ---!
      Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
                                    .in interface outside !--- Output suppressed
```

هذا ما يبدو عليه التكوين في ASDM عندما لا يتم تمكين إرساء DNS:



فيما يلي التقاط حزمة للأحداث عندما لا يتم تمكين DNS doctoring:

1. يرسل العميل استعلام DNS.

```
No.     Time       Source           Destination      Protocol Info
    DNS        Standard query       172.22.1.161    192.168.100.2  0.000000       1
A server.example.com

                                        (Frame 1 (78 bytes on wire, 78 bytes captured
                Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
                                                        (00:0a:b8:9c:c6:1f)
                 Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
                                                        (172.22.1.161)
                   (User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53
                                                    (Domain Name System (query
                                                          [Response In: 2]
                                                    Transaction ID: 0x0004
                                                (Flags: 0x0100 (Standard query
                                                          Questions: 1
                                                        Answer RRs: 0
                                                      Authority RRs: 0
                                                     Additional RRs: 0
                                                                Queries
                                              server.example.com: type A, class IN
                                                        Name: server.example.com
```

```
                                                    (Type: A (Host address
                                                        (Class: IN (0x0001
```

2. يتم تنفيذ ضرب على استعلام DNS بواسطة ASA ويتم إعادة توجيه الاستعلام. لاحظ أن عنوان المصدر للحزمة تغير إلى الواجهة الخارجية من ال ASA.

```
No.     Time      Source           Destination         Protocol Info
      1 0.000000      172.22.1.161       172.20.1.2      DNS      Standard query
A server.example.com

(Frame 1 (78 bytes on wire, 78 bytes captured
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(f1:22:00:30:94:01)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
(User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53
(Domain Name System (query
[Response In: 2]
Transaction ID: 0x0004
(Flags: 0x0100 (Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
(Type: A (Host address
(Class: IN (0x0001
```

3. يرد خادم DNS بالعنوان المعين لخادم WWW.

```
No.     Time      Source           Destination         Protocol Info
      2 0.005005      172.20.1.2       172.22.1.161    DNS      Standard query response
A 172.20.1.10

(Frame 2 (94 bytes on wire, 94 bytes captured
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
(User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044
(Domain Name System (response
[Request In: 1]
[Time: 0.005005000 seconds]
Transaction ID: 0x0004
(Flags: 0x8580 (Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
(Type: A (Host address
(Class: IN (0x0001
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
(Type: A (Host address
(Class: IN (0x0001
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. يقوم ASA بإلغاء ترجمة عنوان الوجهة لاستجابة DNS وإعادة توجيه الحزمة إلى العميل. لاحظ أنه بدون تمكين تعليمات DNS، يظل **العنوان** في الإجابة هو العنوان المعين لخادم WWW.

```
No.     Time      Source          Destination         Protocol Info
DNS     Standard query response      192.168.100.2   172.22.1.161  0.005264       2
A 172.20.1.10

                                                (Frame 2 (94 bytes on wire, 94 bytes captured
                                  Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
                                                                    (c0:c8:e4:00:00:04)
                                    Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
                                                                          (192.168.100.2)
                                     (User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879
                                                                  (Domain Name System (response
                                                                            [Request In: 1]
                                                                  [Time: 0.005264000 seconds]
                                                                      Transaction ID: 0x0004
                                                  (Flags: 0x8580 (Standard query response, No error
                                                                        Questions: 1
                                                                      Answer RRs: 1
                                                                    Authority RRs: 0
                                                                   Additional RRs: 0
                                                                           Queries
                                                        server.example.com: type A, class IN
                                                               Name: server.example.com
                                                                 (Type: A (Host address
                                                                     (Class: IN (0x0001
                                                                                  Answers
                                                server.example.com: type A, class IN, addr 172.20.1.10
                                                                  Name: server.example.com
                                                                    (Type: A (Host address
                                                                        (Class: IN (0x0001
                                                                     Time to live: 1 hour
                                                                           Data length: 4
                                                                       Addr: 172.20.1.10
```

5. عند هذه النقطة، يحاول العميل الوصول إلى خادم WWW على 172.20.1.10. يقوم ASA بإنشاء إدخال اتصال لهذا الاتصال. ومع ذلك، نظرا لأنه لا يسمح لحركة المرور بالتدفق من الداخل إلى الخارج إلى الداخل، فينتهي وقت الاتصال. تظهر سجلات ASA هذا:

```
ASA-6-302013: Built outbound TCP connection 54175 for%
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to%
inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

الحل: الكلمة الأساسية "DNS"

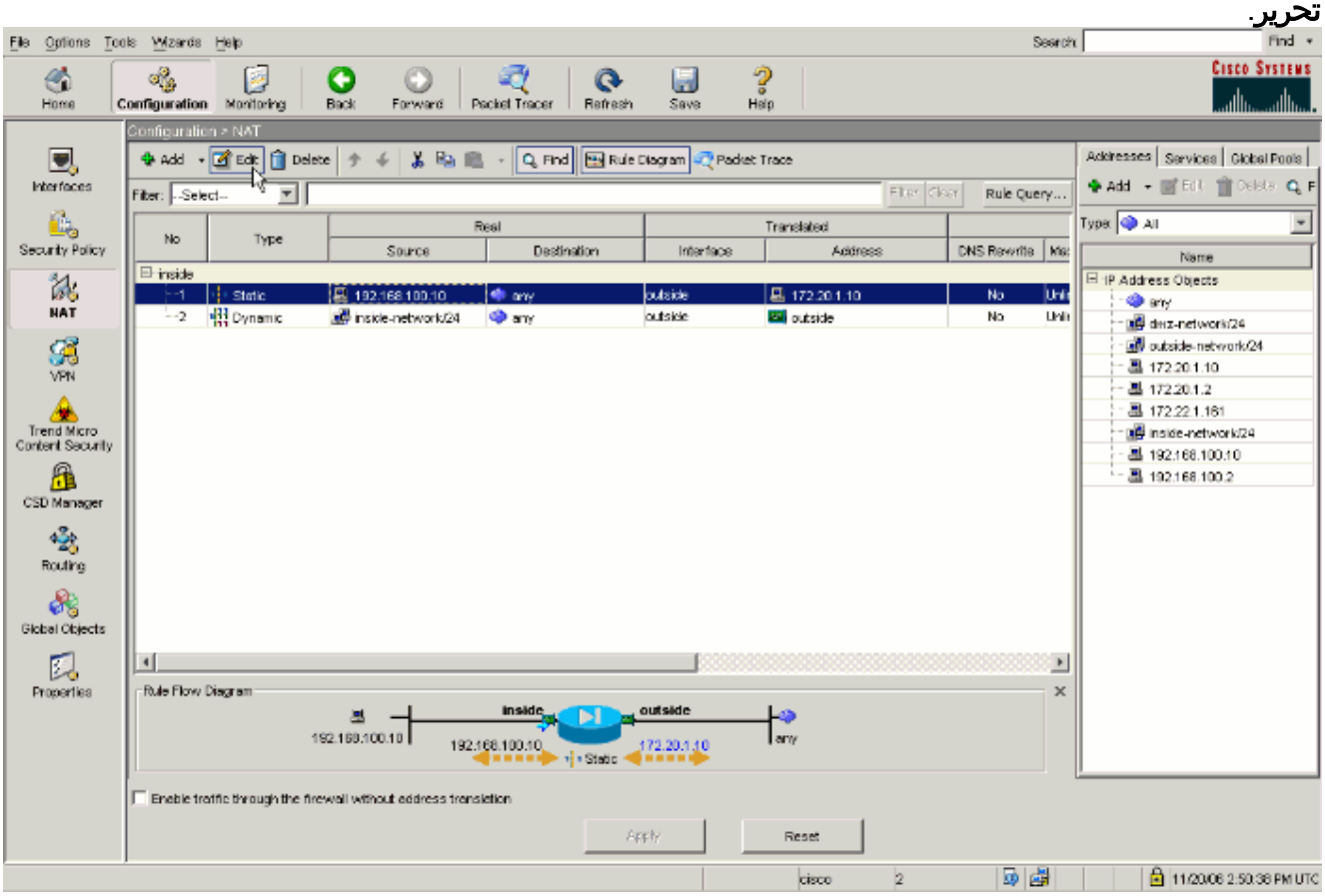
توثيق DNS باستخدام الكلمة الأساسية "DNS"

يمنح توثيق DNS باستخدام الكلمة الأساسية **DNS** جهاز الأمان القدرة على اعتراض محتويات ردود خادم DNS على العميل وإعادة كتابتها. عند تكوين جهاز الأمان بشكل صحيح، يمكن لجهاز الأمان تغيير السجل A للسماح للعميل في سيناريو مثل السيناريو الذي تمت مناقشته في المشكلة: يتعذر على العميل الوصول إلى قسم خادم WWW للاتصال. في هذه الحالة، ومع تمكين إرساء DNS، يقوم جهاز الأمان بإعادة كتابة السجل A لتوجيه العميل إلى **192.168.100.10**، بدلا من **172.20.1.10**. يتم تمكين إرساء DNS عند إضافة الكلمة الأساسية **DNS** إلى عبارة NAT ثابتة. فيما يلي ما يبدو عليه جزء NAT من التكوين عند تمكين إرساء DNS:

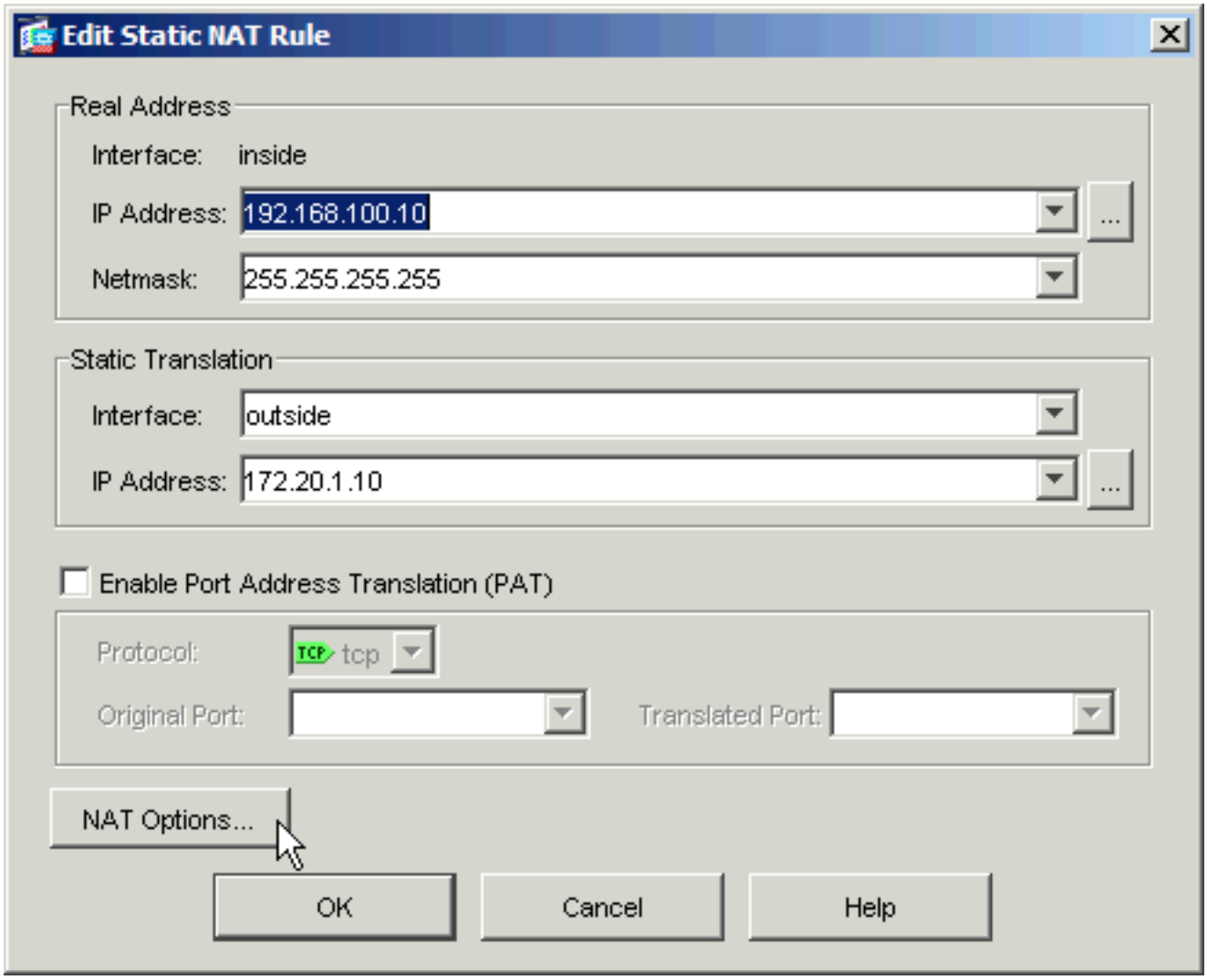
```
ciscoasa(config)#show run
Saved :
:
(ASA Version 7.2(1
!
hostname ciscoasa

Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- ---!
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
The "dns" keyword is added to instruct the security appliance to modify !--- DNS records ---!
.related to this entry. access-group OUTSIDE in interface outside !--- Output suppressed
```

أكمل الخطوات التالية لتكوين تعليمات DNS في ASDM:

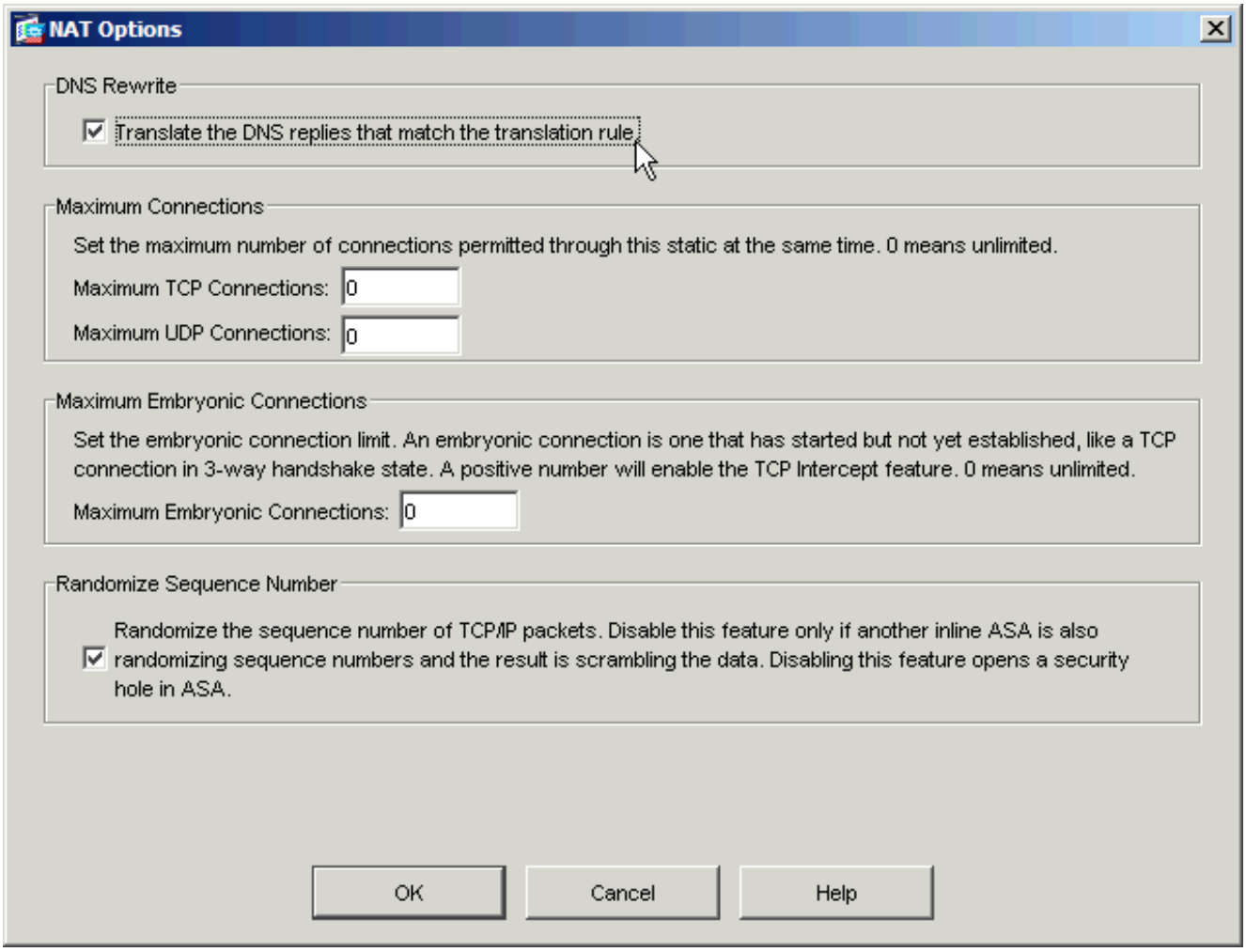
1. انتقل إلى **التكوين > NAT** واختر قاعدة NAT الثابتة التي سيتم تعديلها. انقر فوق **تحرير**.



2. طقطقة **nat خيار...**



3. حدد خانة الاختيار **ترجمة ردود DNS التي تطابق قاعدة الترجمة**.



4. طقطقة **ok** أن يترك ال nat خيار نافذة. طقطقة **ok** أن يترك ال edit ساكن إستاتيكي nat قاعدة نافذة. انقر فوق **تطبيق** لإرسال التكوين الخاص بك إلى جهاز الأمان.

فيما يلي التقاط حزمة للأحداث عند تمكين DNS doctoring:

1. يرسل العميل استعلام DNS.

```
No.     Time       Source           Destination      Protocol Info
DNS     Standard query      172.22.1.161    192.168.100.2  0.000000      1
A server.example.com

(Frame 1 (78 bytes on wire, 78 bytes captured
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
(User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53
(Domain Name System (query
[Response In: 2]
Transaction ID: 0x000c
(Flags: 0x0100 (Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
(Type: A (Host address
(Class: IN (0x0001
```

2. يتم تنفيذ ضرب على استعلام DNS بواسطة ASA ويتم إعادة توجيه الاستعلام. لاحظ أن عنوان المصدر للحزمة

تغير إلى الواجهة الخارجية من ال ASA.

```
No.     Time      Source           Destination         Protocol Info
      DNS      Standard query        172.22.1.161       172.20.1.2  0.000000       1
A server.example.com

                                        (Frame 1 (78 bytes on wire, 78 bytes captured
                Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
                                                                (f1:22:00:30:94:01)
                    Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
                                                                (172.22.1.161)
                (User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53
                                                        (Domain Name System (query
                                                              [Response In: 2]
                                                            Transaction ID: 0x000c
                                                    (Flags: 0x0100 (Standard query
                                                               Questions: 1
                                                             Answer RRs: 0
                                                           Authority RRs: 0
                                                         Additional RRs: 0
                                                                   Queries
                                            server.example.com: type A, class IN
                                                    Name: server.example.com
                                                      (Type: A (Host address
                                                          (Class: IN (0x0001
```

3. يرد خادم DNS بالعنوان المعين لخادم WWW.

```
No.     Time      Source           Destination       Protocol Info
DNS      Standard query response      172.20.1.2     172.22.1.161  0.000992       2
          A 172.20.1.10

                                        (Frame 2 (94 bytes on wire, 94 bytes captured
                Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
                                                                (00:0a:b8:9c:c6:1e)
                    Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
                                                                (172.20.1.2)
                (User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035
                                                        (Domain Name System (response
                                                              [Request In: 1]
                                                    [Time: 0.000992000 seconds]
                                                            Transaction ID: 0x000c
                                    (Flags: 0x8580 (Standard query response, No error
                                                               Questions: 1
                                                             Answer RRs: 1
                                                           Authority RRs: 0
                                                         Additional RRs: 0
                                                                   Queries
                                            server.example.com: type A, class IN
                                                    Name: server.example.com
                                                      (Type: A (Host address
                                                          (Class: IN (0x0001
                                                                  Answers
                                server.example.com: type A, class IN, addr 172.20.1.10
                                                    Name: server.example.com
                                                      (Type: A (Host address
                                                          (Class: IN (0x0001
                                                      Time to live: 1 hour
                                                            Data length: 4
                                                         Addr: 172.20.1.10
```

4. يقوم ASA بإلغاء ترجمة عنوان الوجهة لاستجابة DNS وإعادة توجيه الحزمة إلى العميل. لاحظ أنه مع تمكين تعليمات DNS، تتم إعادة كتابة ADDR في الإجابة ليكون العنوان الحقيقي لخادم WWW.

```
No.     Time      Source           Destination       Protocol Info
DNS      Standard query response      192.168.100.2    172.22.1.161  0.001251       2
```

```
A 192.168.100.10

                                (Frame 2 (94 bytes on wire, 94 bytes captured
     Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
                                                        (c0:c8:e4:00:00:04)
       Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
                                                            (192.168.100.2)
        (User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985
                                                (Domain Name System (response
                                                          [Request In: 1]
                                                [Time: 0.001251000 seconds]
                                                    Transaction ID: 0x000c
                                (Flags: 0x8580 (Standard query response, No error
                                                        Questions: 1
                                                      Answer RRs: 1
                                                    Authority RRs: 0
                                                    Additional RRs: 0
                                                              Queries
                                        server.example.com: type A, class IN
                                                Name: server.example.com
                                                  (Type: A (Host address
                                                      (Class: IN (0x0001
                                                             Answers
                    server.example.com: type A, class IN, addr 192.168.100.10
                                                Name: server.example.com
                                                  (Type: A (Host address
                                                      (Class: IN (0x0001
                                                    Time to live: 1 hour
                                                         Data length: 4
                                                    Addr: 192.168.100.10
                                    .has been rewritten to be 192.168.100.10 172.20.1.10 ---!
```

5. عند هذه النقطة، يحاول العميل الوصول إلى خادم WWW على 192.168.100.10. نجح الاتصال. لم يتم التقاط حركة مرور على ASA لأن العميل والخادم على الشبكة الفرعية نفسها.

التكوين النهائي باستخدام الكلمة الأساسية "DNS"

هذا هو التكوين النهائي ل ASA لإجراء توثيق DNS باستخدام الكلمة الأساسية **DNS** وواجهات NAT.

التكوين النهائي ASA 7.2(1)

```
ciscoasa(config)#show running-config
Saved :
:
(ASA Version 7.2(1
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
```

```
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
 !
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
 !
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
 Simple access-list that permits HTTP access to the ---!
   mapped !--- address of the WWW server. pager lines 24
   logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10
netmask 255.255.255.255 dns
 PAT and static NAT configuration. The DNS keyword ---!
   instructs !--- the security appliance to rewrite DNS
 records related to this entry. access-group OUTSIDE in
interface outside
   The Access Control List (ACL) that permits HTTP ---!
 access !--- to the WWW server is applied to the outside
   interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
  timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
   sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
 username cisco password ffIRPGpDSOJh9YLq encrypted http
    server enable no snmp-server location no snmp-server
    contact snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
  console timeout 0 ! class-map inspection_default match
  default-inspection-traffic ! ! policy-map type inspect
dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
 DNS inspection map. policy-map global_policy class ---!
inspection_default inspect ftp inspect h323 h225 inspect
 h323 ras inspect rsh inspect rtsp inspect esmtp inspect
     sqlnet inspect skinny inspect sunrpc inspect xdmcp
    inspect sip inspect netbios inspect tftp inspect dns
MY_DNS_INSPECT_MAP
DNS inspection is enabled using the configured map. ---!
                inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
   ! service-policy global_policy global prompt hostname
 context Cryptochecksum:a4a38088109887c3ceb481efab3dcf32
                                                    : end
```

الحل البديل: تسريحة الشعر

تسريحة باستخدام NAT ثابت

تحذير: يتضمن **الربط** مع NAT ساكن إستاتيكي إرسال كل حركة مرور البيانات بين العميل وخادم WWW من خلال جهاز الأمان. تأكد من الكمية المتوقعة لحركة مرور البيانات ومن إمكانيات جهاز الأمان لديك قبل تنفيذ هذا الحل.

تسريحة الشعر هي العملية التي من خلالها يتم إعادة حركة المرور إلى نفس الواجهة التي وصلت عليها. تم إدخال هذه الميزة في برنامج جهاز الأمان الإصدار 7.0. بالنسبة للإصدارات الأقدم من 7.2(1)، يلزم تشفير ذراع واحد على الأقل لحركة مرور البيانات فائقة الأداء (الواردة أو الصادرة). ومن الفقرة 7-2 (1) وما بعدها، لم يعد هذا الشرط قائما. قد تكون حركة المرور الواردة وحركة المرور الصادرة غير مشفرة عند إستخدام 7.2(1).

يمكن إستخدام تسريحة الشعر، مع جملة NAT الثابتة، لتحقيق نفس التأثير مثل تأثيث DNS. لا تغير هذه الطريقة محتويات سجل DNS A الذي يتم إرجاعه من خادم DNS إلى العميل. وبدلا من ذلك، عند إستخدام إعادة الفرز، كما هو الحال في السيناريو الذي تمت مناقشته في هذا المستند، يمكن للعميل إستخدام عنوان **172.20.1.10** الذي يتم إرجاعه بواسطة خادم DNS للاتصال.

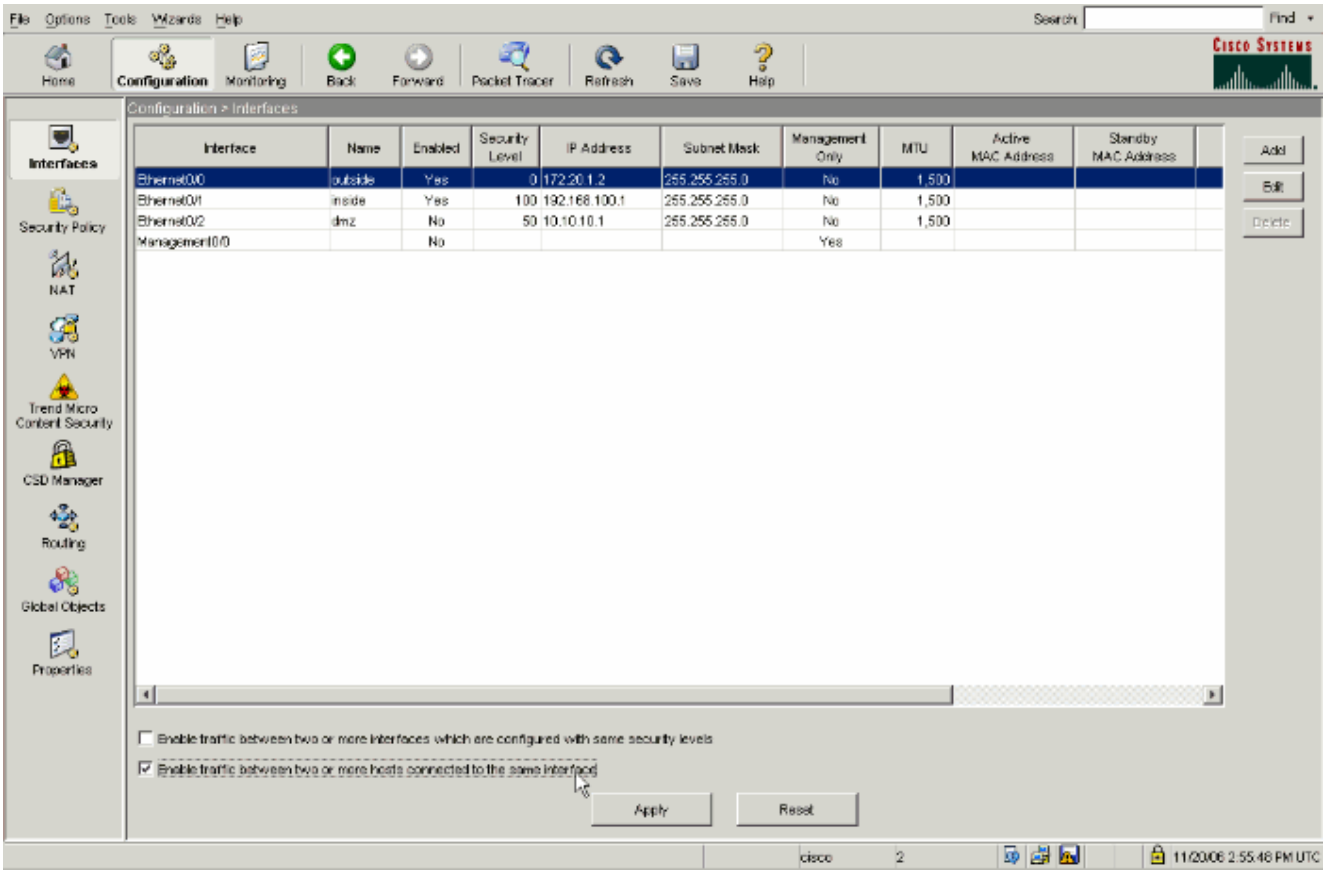
فيما يلي ما يبدو عليه الجزء ذو الصلة من التكوين عند إستخدام تسريحة الشعر و NAT الثابت لتحقيق تأثير إرساء DNS. يتم شرح الأوامر باللون الغامق بتفاصيل أكبر في نهاية هذا الإخراج:

```
ciscoasa(config)#show run
Saved :
:
(ASA Version 7.2(1
!
hostname ciscoasa
Output suppressed. same-security-traffic permit intra-interface ---!
Enable hairpinning. global (outside) 1 interface !--- Global statement for client access to ---!
the Internet. global (inside) 1 interface
Global statment for hairpinned client access through !--- the security appliance. nat ---!
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should be
natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255
Static NAT statment mapping requests for the public IP address of !--- the WWW server that ---!
.appear on the inside interface to the WWW server's !--- real address of 192.168.100.10
```

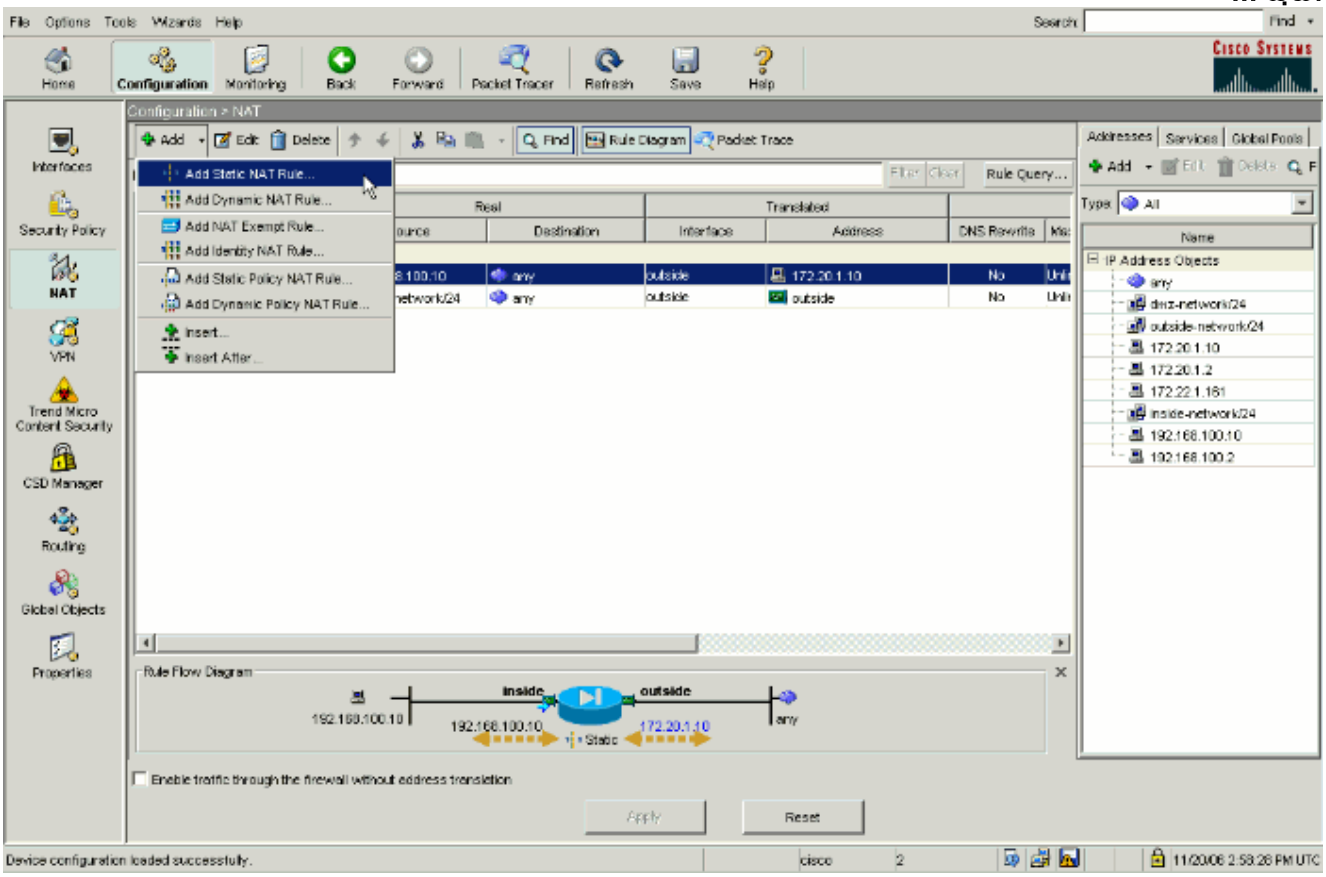
- **نفسه-security-traffic**— يمكن هذا الأمر حركة مرور بنفس مستوى الأمان من نقل جهاز الأمان. تتيح كلمات **السماح** الأساسية **داخل الواجهة** لحركة مرور الأمان نفسها دخول نفس الواجهة ومغادرتها، وبالتالي يتم تمكين تسريحة الشعر.**ملاحظة:** ارجع إلى حركة مرور بيانات الأمان نفسها للحصول على مزيد من المعلومات حول تسريحة الأمر **نفسه-security-traffic**.
- **global (inside) 1 interface**— يجب أن تخضع جميع حركة مرور البيانات التي تعبر جهاز الأمان ل NAT. يستعمل هذا أمر القارن داخلي من الجهاز أمن in order to مكنت حركة مرور أن يدخل القارن داخلي أن يخضع ضرب بما أن هو معبأ إلى الخلف خارج القارن داخلي.
- **ساكن إستاتيكي (داخل، داخل) 172.20.1.10 192.168.100.10 netmask 255.255.255.255**- يقوم إدخال NAT الثابت هذا بإنشاء تخطيط ثان لعنوان IP العام لخادم WW. مهما، بخلاف أول ساكن إستاتيكي nat مدخل، هذه المرة العنوان 172.20.1.10 يخطط إلى القارن داخلي من الجهاز أمن. وهذا يسمح لجهاز الأمان بالاستجابة للطلبات التي يراها لهذا العنوان على الواجهة الداخلية. وبعد ذلك، فإنه يعيد توجيه تلك الطلبات إلى العنوان الحقيقي لخادم WWW من خلال نفسه.

أتمت هذا steps in order to شكلت تصغير مع ساكن إستاتيكي nat في ASDM:

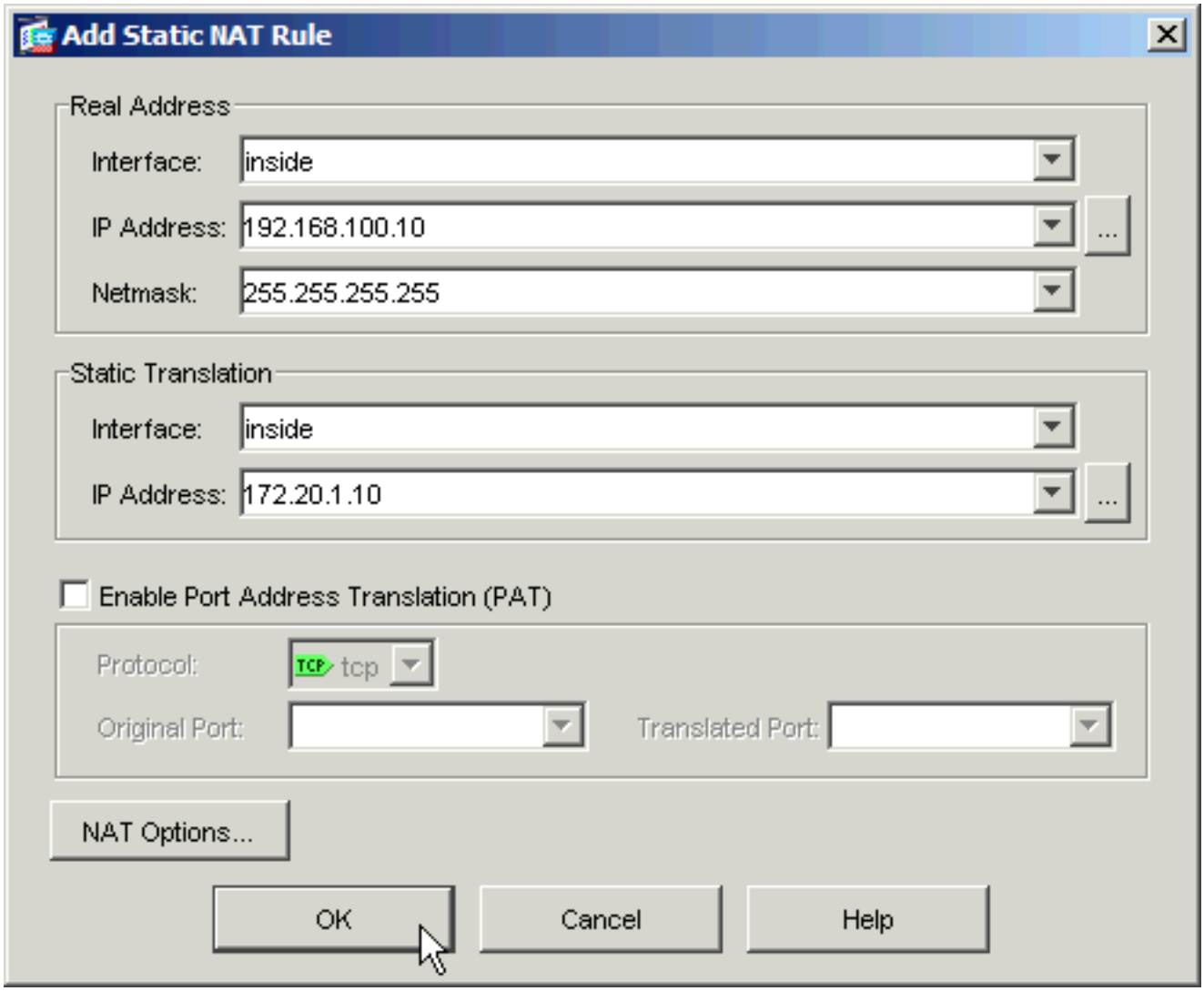
1. انتقل إلى **التكوين > الواجهات**.
2. في أسفل النافذة، حدد خانة الاختيار **تمكين حركة مرور البيانات بين جهازين مضيفين أو أكثر متصلين بنفس الواجهة**.



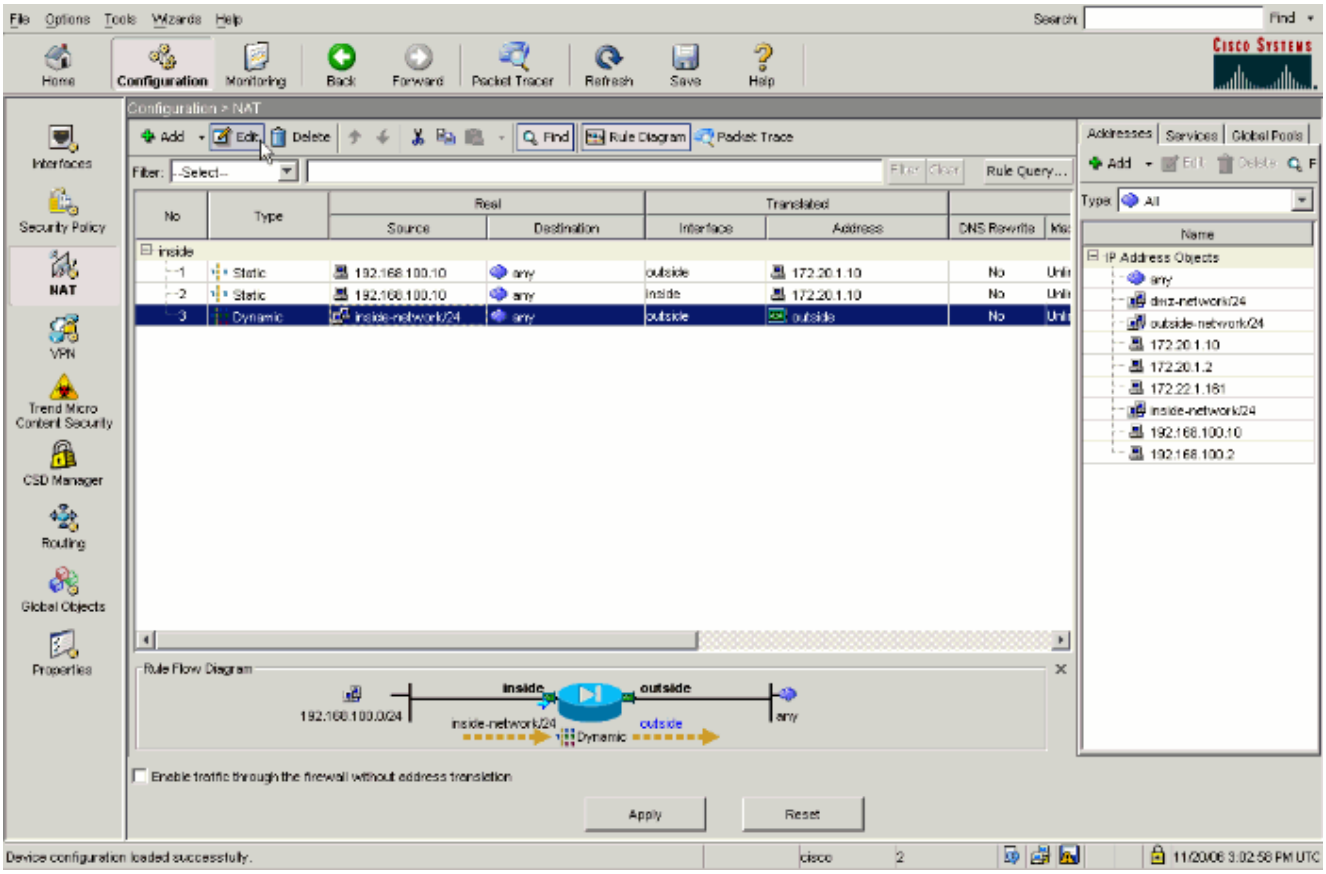
3. طقطقة **يطبق**.
4. انتقل إلى **التكوين** > **NAT** واختر **إضافة** > **إضافة قاعدة NAT الثابتة**....



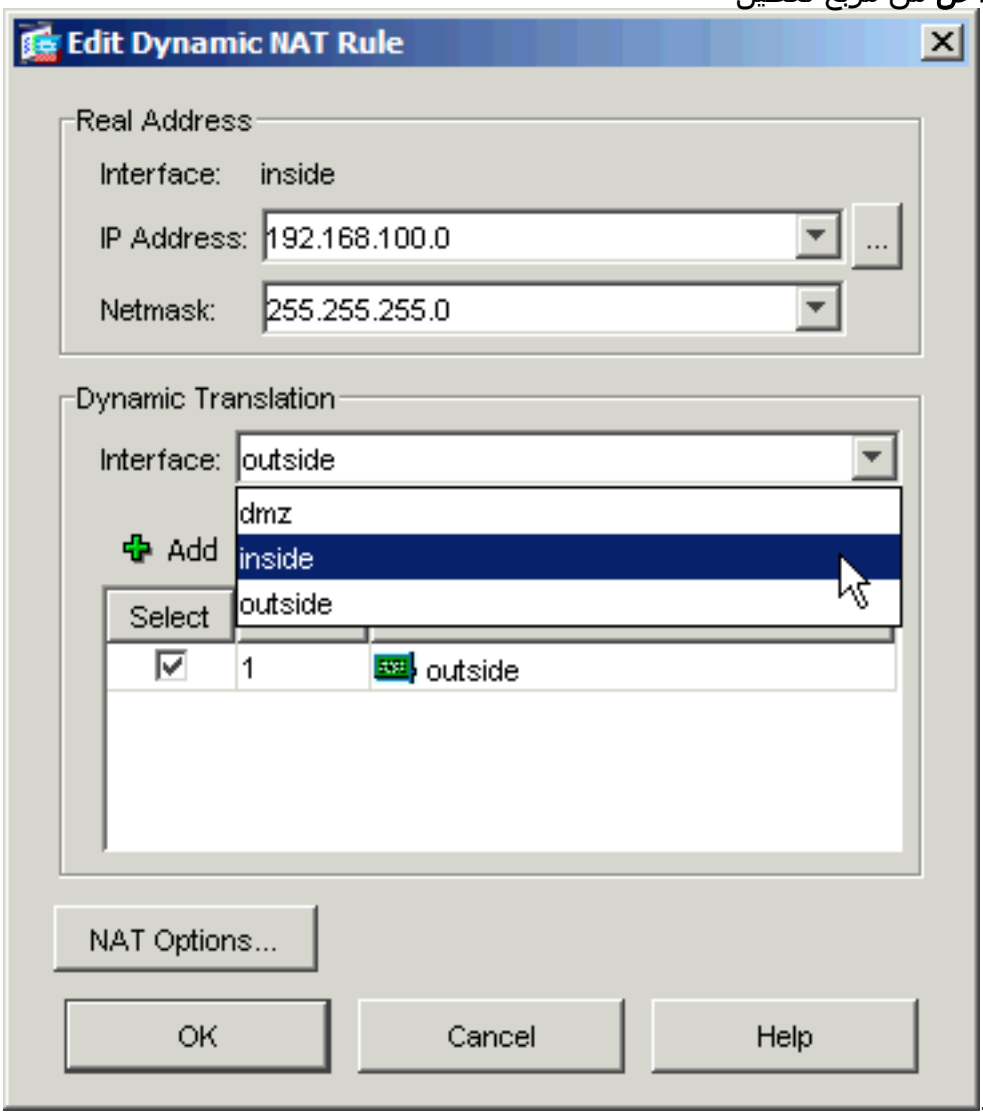
5. قم بتعبئة التكوين للترجمة الثابتة الجديدة.ملء منطقة **العنوان الحقيقي** بمعلومات خادم WWW.قم بملء منطقة **الترجمة الثابتة** بالعنوان والواجهة التي تريد تعيين خادم WWW إليها.في هذه الحالة، أخترت القارن داخلي أن يسمح مضيف على القارن داخلي أن ينفذ ال WWW نادل عن طريق ال يخطط عنوان 172.20.1.10.



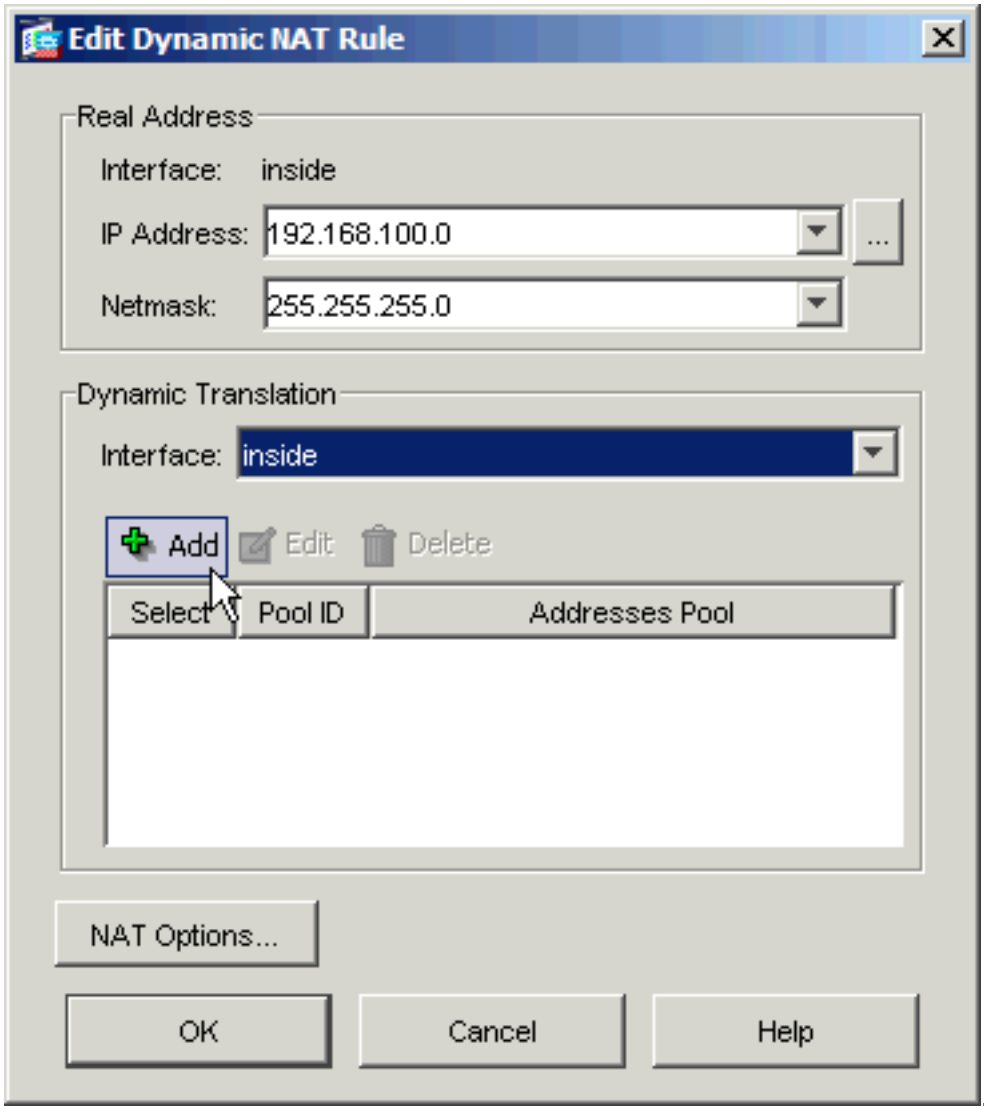
6. طقطقة **ok** أن يترك ال إضافة ساكن إستاتيكي nat قاعدة نافذة.
7. أخترت الحالي حركي ضرب ترجمة وطقطقة
يحرر.



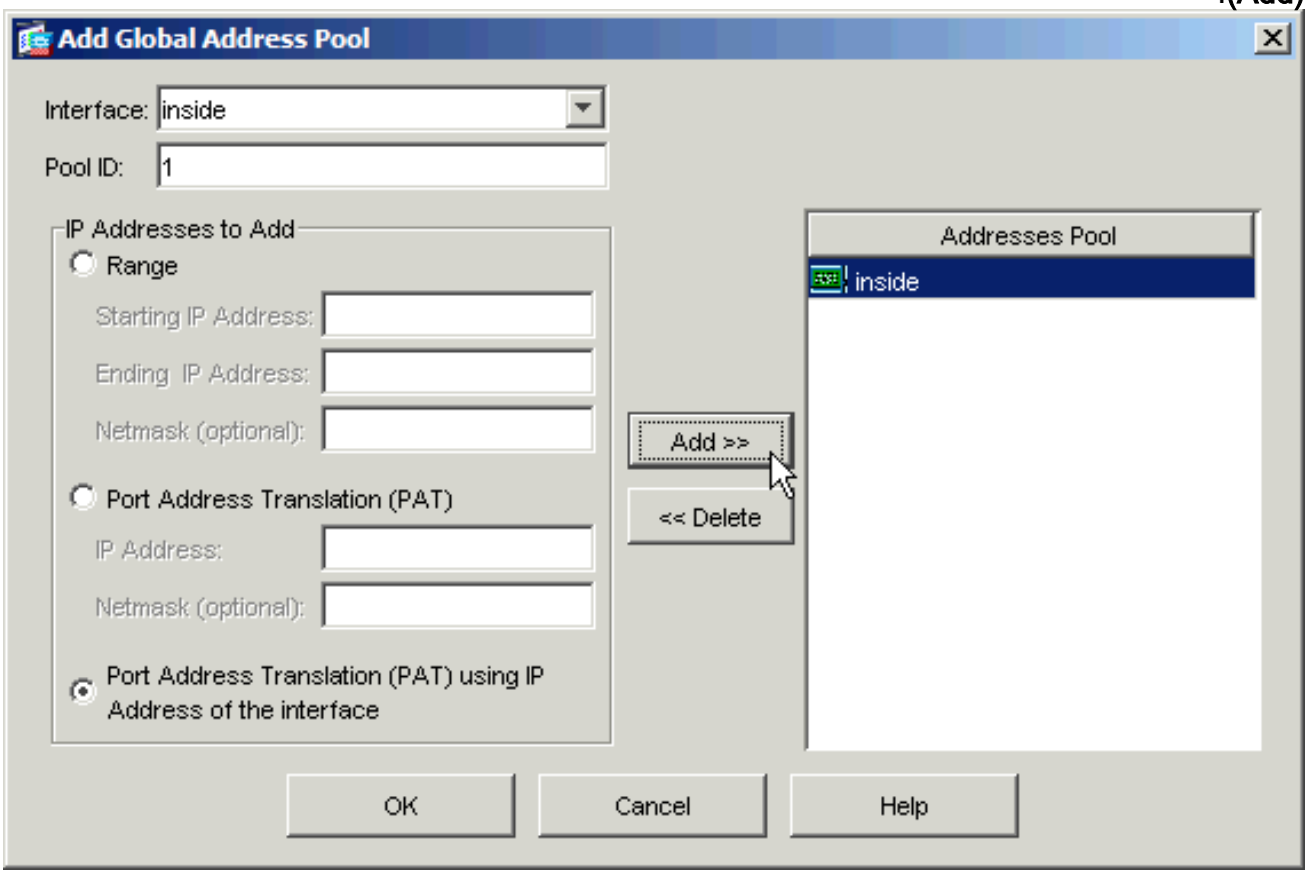
8. أختر **الداخل** من مربع تعطيل



الواجهة.



9. انقر فوق **إضافة (Add)**.
10. أخترت الإذاعة زر يعين **أيسر عنوان ترجمة (ضرب) يستعمل عنوان من القارن**. انقر فوق **إضافة (Add)**.



11. انقر فوق **موافق** لمغادرة الإطار إضافة تجمع عناوين عمومي. طقطقة **ok** أن يترك ال edit حركي nat قاعدة نافذة. انقر فوق **تطبيق** لإرسال التكوين الخاص بك إلى جهاز الأمان.

فيما يلي تسلسل الأحداث التي تحدث عند تكوين تسريحة الشعر. بافتراض أن العميل قد استفسر بالفعل عن خادم DNS وتلقى ردا **بقيمة 172.20.1.10** على عنوان خادم WWW:

1. يحاول العميل الاتصال بخادم WWW على 172.20.1.10.
```
ASA-7-609001: Built local-host inside:192.168.100.2%
```
2. يرى جهاز الأمان الطلب ويتعرف على أن خادم WWW هو 192.168.100.10.
```
ASA-7-609001: Built local-host inside:192.168.100.10%
```
3. يقوم جهاز الأمان بإنشاء ترجمة PAT ديناميكية للعميل. مصدر حركة مرور العميل هو الآن الواجهة الداخلية لجهاز الأمان: 192.168.100.1.
```
ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to%
inside:192.168.100.1/1026
```

4. يقوم جهاز الأمان بإنشاء اتصال TCP بين العميل وخادم WWW من خلال نفسه. لاحظ العناوين المعينة لكل مضيف بين أقواس.
```
ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012%
(to inside:192.168.100.10/80 (172.20.1.10/80 (192.168.100.1/1026)
```

5. يتحقق الأمر **show xlate** على جهاز الأمان من أن حركة مرور العميل تتم ترجمتها من خلال جهاز الأمان.
```
ciscoasa(config)#show xlate
in use, 9 most used 3
Global 172.20.1.10 Local 192.168.100.10
Global 172.20.1.10 Local 192.168.100.10
(PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013
```

6. يتحقق الأمر **show conn** على جهاز الأمان من نجاح الاتصال بين جهاز الأمان وخادم WWW نيابة عن العميل. لاحظ العنوان الحقيقي للعميل بين أقواس.
```
ciscoasa#show conn
TCP out 192.168.100.1(192.168.100.2):11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

التكوين النهائي مع تسريحة وبطاقة NAT الثابتة

هذا هو التشكيل النهائي من ال ASA أن يستعمل تصغير و ساكن إستاتيكي nat أن يحقق DNS توثيق تأثير مع إثنان nat قارن.

التكوين النهائي 1)ASA 7.2)

```
ciscoasa(config-if)#show running-config
Saved :
:
(ASA Version 7.2(1
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
```

```
                                                nameif inside
                                             security-level 100
                                  ip address 192.168.100.1 255.255.255.0
                                                             !
                                             interface Ethernet0/2
                                                       shutdown
                                                      no nameif
                                                 no security-level
                                                     no ip address
                                                             !
                                            interface Management0/0
                                                       shutdown
                                                      no nameif
                                                 no security-level
                                                     no ip address
                                                  management-only
                                                             !
                                  passwd 2KFQnbNIdI.2KYOU encrypted
                                                 ftp mode passive
                              same-security-traffic permit intra-interface
                          access-list OUTSIDE extended permit tcp any host
                                                 172.20.1.10 eq www
 Simple access-list that permits HTTP access to the ---! mapped !--- address of the WWW server. pager lines 24
   logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface !--- Global statement for client access to the
       Internet. global (inside) 1 interface !--- Global
  statment for hairpinned client access through !--- the
       security appliance. nat (inside) 1 192.168.100.0
     255.255.255.0 !--- The NAT statement defines which
  traffic should be natted. !--- The whole inside subnet
       in this case. static (inside,outside) 172.20.1.10
  192.168.100.10 netmask 255.255.255.255 !--- Static NAT
    statement mapping the WWW server's real address to a
    public !--- address on the outside interface. static
      (inside,inside) 172.20.1.10 192.168.100.10 netmask
       255.255.255.255 !--- Static NAT statement mapping
      requests for the public IP address of the !--- WWW
   server that appear on the inside interface to the WWW
   server's real address !--- of 192.168.100.10. access-
    group OUTSIDE in interface outside !--- The ACL that
permits HTTP access to the WWW server is applied !--- to
    the outside interface. route outside 0.0.0.0 0.0.0.0
 172.20.1.1 1 timeout xlate 3:00:00 timeout conn 1:00:00
    half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
   sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
  mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
                0:05:00 absolute username cisco password
  ffIRPGpDSOJh9YLq encrypted http server enable no snmp-
      server location no snmp-server contact snmp-server
        enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
         0 ! class-map inspection_default match default-
      inspection-traffic ! ! policy-map type inspect dns
MY_DNS_INSPECT_MAP parameters message-length maximum 512
       policy-map global_policy class inspection_default
  inspect ftp inspect h323 h225 inspect h323 ras inspect
   rsh inspect rtsp inspect esmtp inspect sqlnet inspect
 skinny inspect sunrpc inspect xdmcp inspect sip inspect
     netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
                inspect icmp policy-map type inspect dns
```

```
migrated_dns_map_1 parameters message-length maximum 512
   ! service-policy global_policy global prompt hostname
 context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
                                                    : end
```

ملاحظة: ارجع إلى هذا الفيديو، حول العملاء المسجلين فقط من Cisco ASA (العملاء المسجلون فقط)، للحصول على مزيد من المعلومات حول السيناريوهات المختلفة حيث يمكن إستخدام شد الشعر.

تكوين فحص DNS

لتمكين فحص DNS (إذا كان قد تم تعطيله مسبقا)، قم بإجراء هذه الخطوات. في هذا المثال، تتم إضافة فحص DNS إلى سياسة الفحص العام الافتراضية، والتي يتم تطبيقها بشكل عام بواسطة أمر **service-policy** كما لو كان ASA قد بدأ بتكوين افتراضي. ارجع إلى إستخدام إطار عمل السياسة النمطية للحصول على مزيد من المعلومات حول سياسات الخدمة والتفتيش.

1. قم بإنشاء خريطة سياسة فحص ل DNS.
```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
```

2. من وضع تكوين خريطة السياسة، أدخل وضع تكوين المعلمة لتحديد معلمات لمحرك الفحص.
```
ciscoasa(config-pmap)#parameters
```

3. في وضع تكوين معلمة خريطة السياسة، حدد طول الرسالة الرئيسية لرسائل DNS التي ستكون 512.
```
ciscoasa(config-pmap-p)#message-length maximum 512
```

4. الخروج من وضع تكوين معلمة خريطة السياسة ووضع تكوين خريطة السياسة.
```
ciscoasa(config-pmap-p)#exit
  ciscoasa(config-pmap)#exit
```

5. تأكد أن خريطة سياسة التفتيش تم إنشاؤها حسب الرغبة.
```
ciscoasa(config)#show run policy-map type inspect dns
                                                    !
          policy-map type inspect dns MY_DNS_INSPECT_MAP
                                              parameters
                                 message-length maximum 512
                                                    !
```

6. أدخل وضع تكوين خريطة السياسة ل **global_policy**.
```
ciscoasa(config)#policy-map global_policy
                                  #(ciscoasa(config-pmap
```

7. في وضع تكوين خريطة السياسة، حدد خريطة الفئة الافتراضية للطبقة 4/3، **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
                                #(ciscoasa(config-pmap-c
```

8. في وضع تكوين فئة خريطة السياسة، حدد أنه يجب فحص DNS باستخدام خريطة سياسة التفتيش التي تم إنشاؤها في الخطوات 1-3.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. خروج من وضع تكوين فئة خريطة السياسة ووضع تكوين خريطة السياسة.
```
ciscoasa(config-pmap-c)#exit
  ciscoasa(config-pmap)#exit
```

10. تحقق من تكوين خريطة سياسة **global_policy** كما هو مطلوب.
```
ciscoasa(config)#show run policy-map
                                                    !
        The configured DNS inspection policy map. policy-map type inspect dns ---!
MY_DNS_INSPECT_MAP parameters message-length maximum 512 policy-map global_policy class
```

```
inspection_default inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp
      inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip
                              inspect netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
                                        ! .DNS application inspection enabled ---!
```

11. تحقق من تطبيق global_policy بشكل عام بواسطة سياسة الخدمة.

```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

تكوين Split-DNS

قم بإصدار الأمر **split-dns** في وضع تكوين نهج المجموعة لإدخال قائمة بالمجالات التي سيتم حلها من خلال نفق التقسيم. أستخدم الصيغة ***no*** من هذا الأمر لحذف قائمة.

عند عدم وجود قوائم مجال تقسيم نفقي، يرث المستخدمون أي قوائم موجودة في نهج المجموعة الافتراضي. قم بإصدار الأمر **split-dns none** لمنع توريث قوائم مجال تقسيم الاتصال النفقي.

أستخدم مساحة واحدة لفصل كل إدخال في قائمة المجالات. لا يوجد حد لعدد الإدخالات، لكن السلسلة بأكملها لا يمكن أن يزيد عن 255 حرفا. يمكنك إستخدام الحروف الهجائية والرقمية فقط، والواصلات (-)، والنقاط (.). يحذف الأمر **no split-dns**، عند إستخدامه بدون وسيطات، كل القيم الحالية، والتي تتضمن قيمة خالية تم إنشاؤها عند إصدار الأمر **split-dns none**.

يوضح هذا المثال كيفية تكوين المجالات Domain1 و Domain2 و Domain3 و Domain4 من أجل الحل من خلال تقسيم الاتصال النفقي لنهج المجموعة المسمى FirstGroup:

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

التقاط حركة مرور DNS

تتمثل إحدى طرق التحقق من أن جهاز الأمان يقوم بإعادة كتابة سجلات DNS بشكل صحيح في التقاط الحزم المعنية، كما هو موضح في المثال السابق. أتمت هذا steps in order to على قبض حركة مرور على ال ASA:

1. قم بإنشاء قائمة وصول لكل مثيل التقاط تريد إنشائه.يجب أن تحدد قائمة التحكم في الوصول حركة المرور التي تريد التقاطها. في هذا المثال، تم إنشاء قوائم التحكم في الوصول (ACL).قائمة التحكم في الوصول لحركة المرور على الواجهة الخارجية:

```
access-list DNSOUTCAP extended permit ip host 172.22.1.161 host 172.20.1.2
All traffic between the DNS server and the ASA. access-list DNSOUTCAP extended permit ---!
.ip host 172.20.1.2 host 172.22.1.161 !--- All traffic between the ASA and the DNS server
```

قائمة التحكم في الوصول (ACL) لحركة المرور على الواجهة الداخلية:

```
access-list DNSINCAP extended permit ip host 192.168.100.2 host 172.22.1.161
    All traffic between the client and the DNS server. access-list DNSINCAP extended ---!
permit ip host 172.22.1.161 host 192.168.100.2 !--- All traffic between the DNS server and
                                                                        .the client
```

2. إنشاء مثيل (مثيلات) الالتقاط:

```
ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside
This capture collects traffic on the outside interface that matches !--- the ACL ---!
DNSOUTCAP. ciscoasa#capture DNSINSIDE access-list DNSINCAP interface inside
This capture collects traffic on the inside interface that matches !--- the ACL ---!
.DNSINCAP
```

3. عرض الالتقاط.فيما يلي ما يبدو عليه المثال بعد تمرير بعض حركة مرور DNS:

```
ciscoasa#show capture DNSOUTSIDE
                                                packets captured 2
 udp 36  :172.22.1.161.53 < 172.20.1.2.1025 14:07:21.347195 :1
 udp 93  :172.20.1.2.1025 < 172.22.1.161.53 14:07:21.352093 :2
                                                packets shown 2
ciscoasa#show capture DNSINSIDE
                                                packets captured 2
udp 36  :172.22.1.161.53 < 192.168.100.2.57225 14:07:21.346951 :1
udp 93  :192.168.100.2.57225 < 172.22.1.161.53 14:07:21.352124 :2
                                                packets shown 2
```

4. (إختياري) انسخ الالتقاط (الالتقاط) إلى خادم TFTP بتنسيق PCAP للتحليل في تطبيق آخر.يمكن للتطبيقات التي يمكنها تحليل تنسيق PCAP إظهار تفاصيل إضافية مثل الاسم وعنوان IP في سجلات DNS A.

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

لم يتم إجراء إعادة كتابة DNS

تأكد من تكوين فحص DNS لديك على جهاز الأمان. راجع قسم تكوين فحص DNS.

فشل إنشاء الترجمة

إذا تعذر إنشاء اتصال بين العميل وخادم WWW، فقد يكون السبب هو تكوين NAT غير صحيح. تحقق من سجلات جهاز الأمان بحثا عن الرسائل التي تشير إلى فشل بروتوكول في إنشاء ترجمة من خلال جهاز الأمان. إذا ظهرت هذه الرسائل، فتحقق من تكوين NAT لحركة المرور المطلوبة ومن عدم وجود عناوين غير صحيحة.

```
ASA-3-305006: portmap translation creation failed for tcp src%
inside:192.168.100.2/11000 dst dmz:10.10.10.10/23
```

قم بمسح الإدخالات المتأخرة، ثم قم بإزالة عبارات NAT وإعادة تطبيقها لحل هذا الخطأ.

إسقاط رد UDP DNS

من الممكن أن تتلقى رسالة الخطأ هذه بسبب إسقاط حزمة DNS:

```
PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port%
(to dest_interface:dest_address/dest_port; (label length | domain-name length
.bytes exceeds remaining packet length of 44 bytes 52
```

قم بزيادة طول حزمة DNS بين 512-65535 لحل هذه المشكلة.

مثال:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
<ciscoasa(config-pmap-p)#message-length maximum <512-65535
```

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- إعلامات حقل منتج الأمان
- طلب التعليقات (RFCs)
- تثبيت الشعر على Cisco ASA
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances

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).