تكوين إعادة كتابة DNS على NAT ثلاثي الاتجاهات على ASA من الإصدار 9.x

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل أن ينجز domain name نظام (DNS) توثيق على ال ASA 5500-X sery أمن أداة (ASA) أن يستعمل كائن/تلقائي 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.

المتطلبات الأساسية

المتطلبات

تذكر Cisco أنه يجب تمكين فحص DNS لتنفيذ تعليمات DNS على جهاز الأمان. يكون فحص DNS قيد التشغيل بشكل افتراضي.

عند تمكين فحص DNS، يقوم جهاز الأمان بتنفيذ المهام التالية:

- يترجم سجل DNS بناء على التشكيل مكتمل باستخدام أوامر كائن/تلقائي nat (إعادة كتابة DNS). تنطبق الترجمة فقط على السجل A في الرد على DNS. لذلك لا تتأثر عمليات البحث العكسية، التي تطلب سجل المؤشر (PTR)، بإعادة كتابة DNS. في الإصدار 9.0(1) ASA) والإصدارات الأحدث، تتم ترجمة سجل DNS PTR لعمليات البحث العكسية في DNS عند إستخدام IPv4 NAT و IPv6 NAT و NAT64 مع تمكين الفحص باستخدام DNS لقاعدة NAT.**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 بإدخال الأمر **فحص DNS** دون خيار الحد الأقصى للطول، فلن 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

أسست المعلومة في هذا وثيقة على ال ASA 5500-X sery أمن جهاز، صيغة x.9.

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 ASA 5500 Series Security Appliance، الإصدار 8.4 أو إصدار أحدث.

ملاحظة: ينطبق تكوين ASDM على الإصدار x.7 فقط.

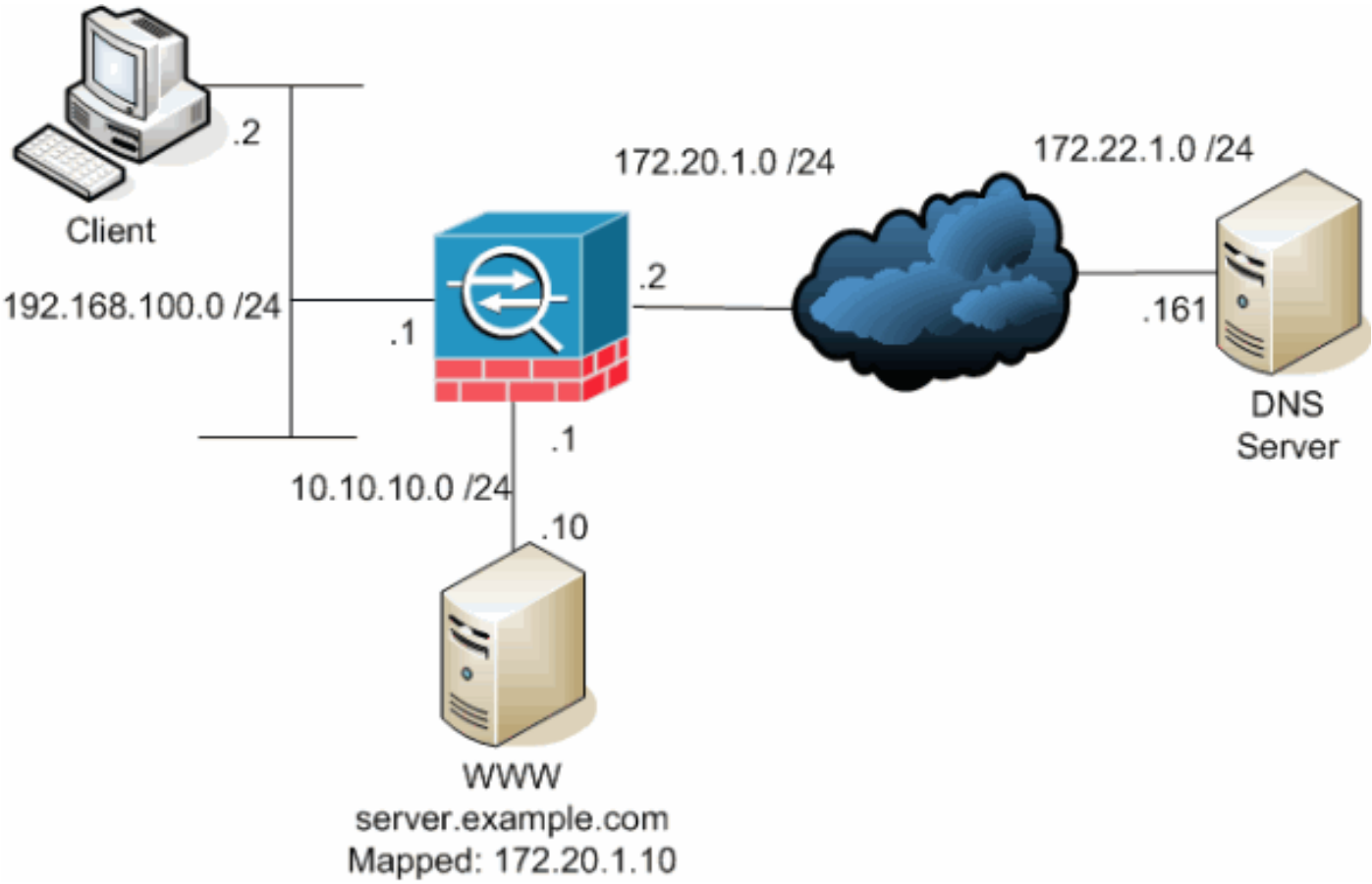
معلومات أساسية

في تبادل DNS نموذجي، يرسل العميل عنوان URL أو اسم المضيف إلى خادم DNS لتحديد عنوان IP الخاص بذلك 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: ثلاث واجهات NAT - داخل المنطقة المنزوعة السلاح وخارجها

طوبولوجيا



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 10.10.10.10. 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**.

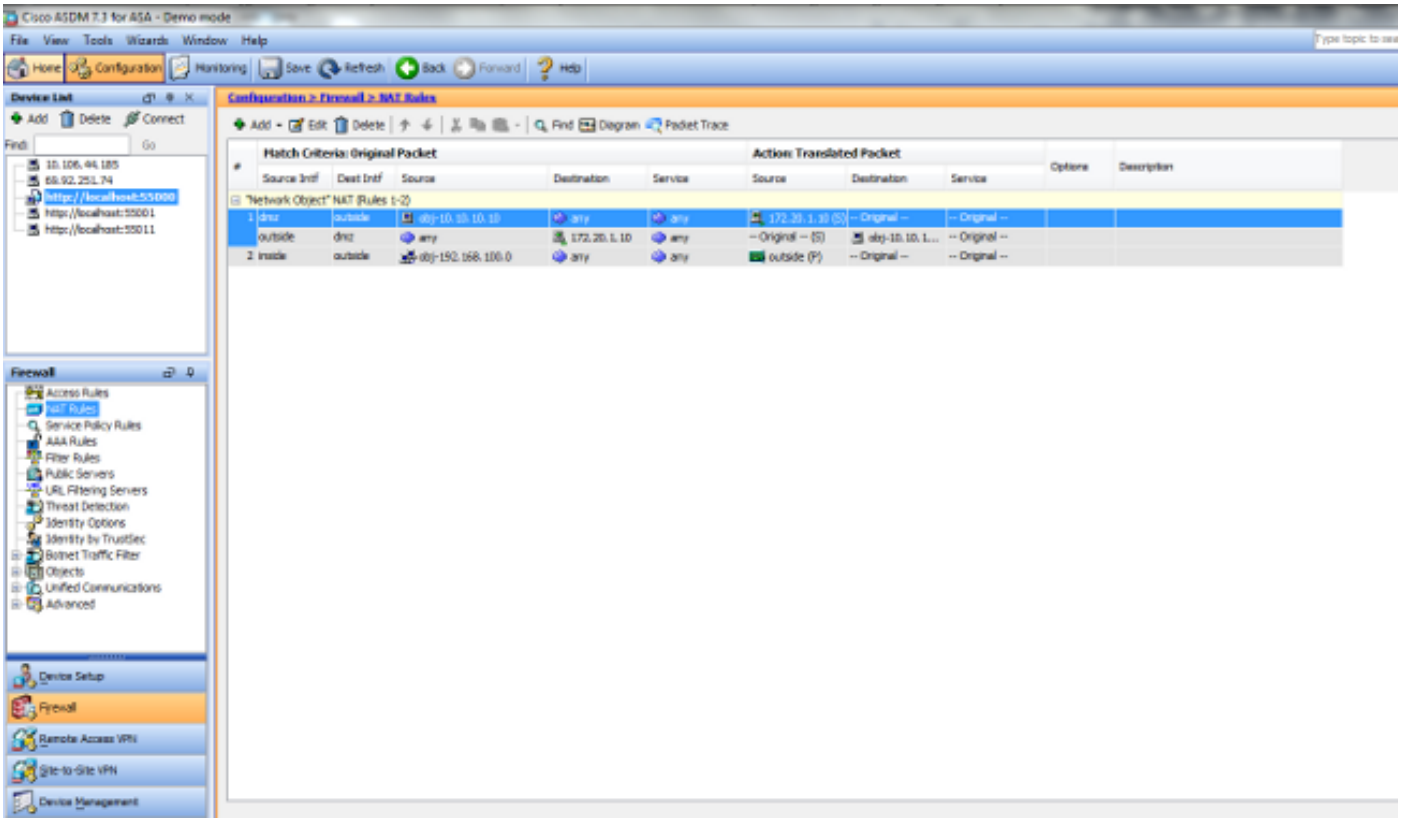
المشكلة: يتعذر على العميل الوصول إلى خادم WWW

بدون تعليمات DNS أو حل آخر ممكن في هذه الحالة، إذا قام العميل بإرسال 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 للخادم WWW وهو 172.20.1.10. 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:

```
ASA Version 9.x
!
hostname ciscoasa
```

```
.Output suppressed ---!

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
.Output suppressed ---!

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

Static translation to allow hosts on the outside access ---!
.to the WWW server ---!
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
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: 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
DNS Standard query response 172.20.1.2 172.22.1.161 0.005005 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: 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 DMZ، فقد انتهت مهلة 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 هذا الذي تمت مناقشته في القسم "مشكلة: يتعذر على العميل الوصول إلى خادم WWW" للاتصال. في هذه الحالة مع تمكين إرساء DNS، يقوم جهاز الأمان بإعادة كتابة السجل A لتوجيه العميل إلى 10.10.10.10 بدلا من 172.20.1.10. يتم تمكين إرساء DNS عند إضافة الكلمة الأساسية **DNS** إلى عبارة NAT ثابتة (الإصدار 8.2 وما

قبله) أو عبارة كائن/تلقائي NAT (الإصدار 8.3 والإصدارات الأحدث).

الإصدار 8.2 والإصدارات السابقة

هذا هو التكوين النهائي ل ASA لإجراء توثيق DNS باستخدام الكلمة الأساسية **DNS** وثلاث واجهات NAT للإصدارات 8.2 والإصدارات الأقدم.

```
ciscoasa#show running-config
Saved :
:
ASA Version 8.2.x
!
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
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
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

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 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,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside
```

```
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:d6637819c6ea981daf20d8c7aa8ca256
end :
```

الإصدار 8.3 والإصدارات الأحدث

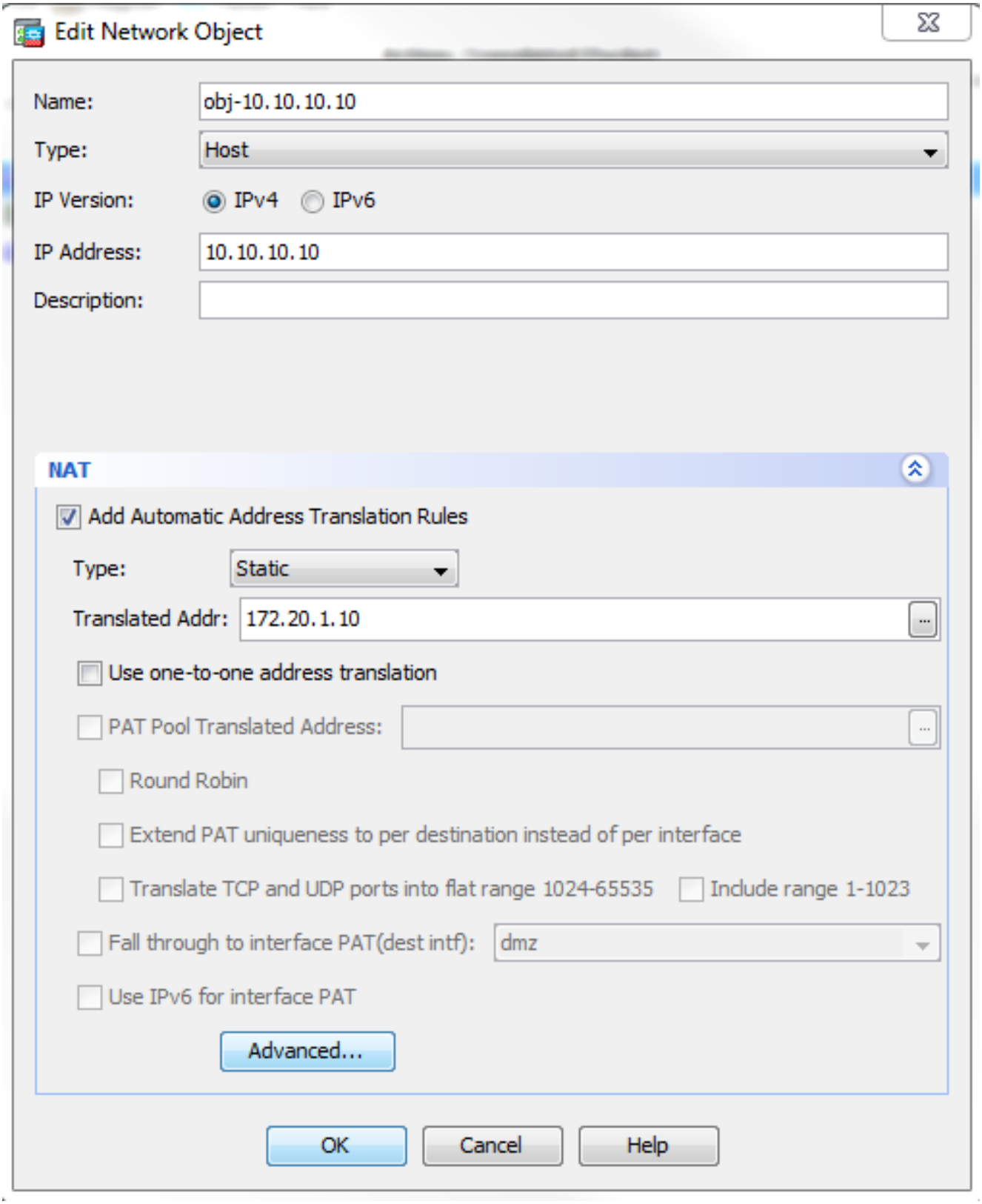
```
ASA Version 9.x
!
hostname ciscoasa

.Output suppressed ---!

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

.Output suppressed ---!

object network obj-192.168.100.0
```

```
 network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

 object network obj-10.10.10.10
 host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

Static translation to allow hosts on the outside access ---!
.to the WWW server ---!

access-group OUTSIDE in interface outside

.Output suppressed ---!
```

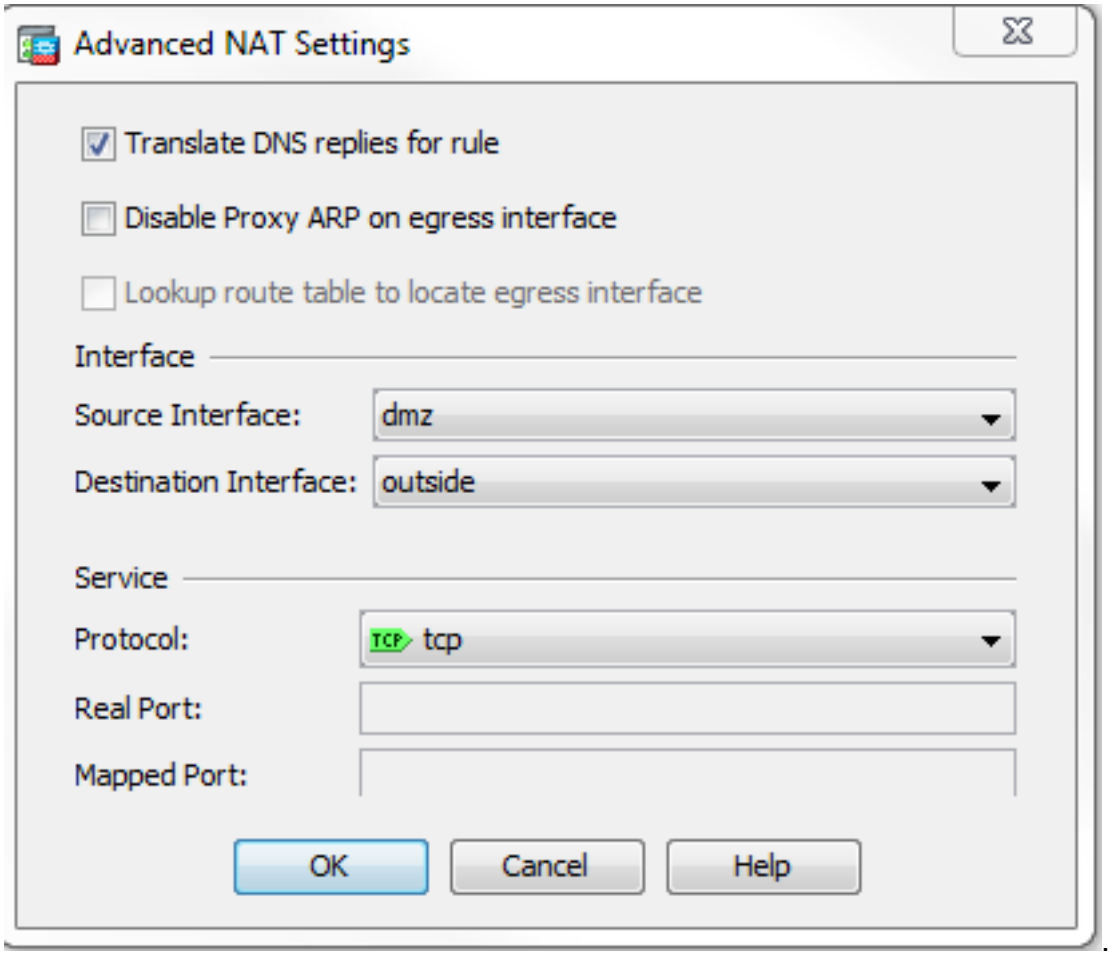
تكوين ASDM

أكمل الخطوات التالية لتكوين تعليمات DNS في ASDM:

1. أخترت **تشكيل > nat قاعدة** واخترت الكائن/تلقائي قاعدة أن يكون عدلت. انقر فوق **تحرير**.
2. طقطقة **متقدم...**



3. حدد خانة الاختيار **ترجمة ردود**



DNS.

4. طقطقة **ok** in order to تركت ال nat خيار نافذة.
5. طقطقة **ok** in order to يحرر كائن/nat قاعدة نافذة.
6. انقر فوق **تطبيق** لإرسال التكوين الخاص بك إلى جهاز الأمان.

التحقق من الصحة

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 2.507191 6
                                                              A 10.10.10.10

                                    (Frame 6 (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: 50752 (50752
                                                 (Domain Name System (response
                                                              [Request In: 5]
                                                  [Time: 0.002182000 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 10.10.10.10
                                                      Name: server.example.com
                                                        (Type: A (Host address
                                                            (Class: IN (0x0001
                                                      Time to live: 1 hour
                                                            Data length: 4
                                                          Addr: 10.10.10.10
```

5. عند هذه النقطة، يحاول العميل الوصول إلى خادم WWW على 10.10.10.10. نجح الاتصال.

التكوين النهائي باستخدام الكلمة الأساسية "DNS"

هذا هو التكوين النهائي من ASA لإجراء توثيق DNS باستخدام الكلمة الأساسية **DNS** وثلاث واجهات NAT.

```
ciscoasa# sh running-config
                                                                  Saved :
                                                                        :
                                                  Serial Number: JMX1425L48B :
                  Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz :
                                                                        :
                                                        ASA Version 9.1(5)4
                                                                        !
                                                          hostname ciscoasa
                                      enable password 9jNfZuG3TC5tCVH0 encrypted
                                              passwd 2KFQnbNIdI.2KYOU encrypted
                                                                   names
                                                               dns-guard
                                                                        !
                                                     interface Ethernet0/0
                                                                shutdown
                                                           nameif outside
                                                        security-level 0
                                          ip address 172.20.1.2 255.255.255.0
                                                                        !
                                                     interface Ethernet0/1
                                                                shutdown
                                                           nameif inside
                                                        security-level 100
```

```
ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
shutdown
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
object network obj-192.168.100.0
subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
nat (inside,outside) dynamic interface
object network obj-10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
```

```
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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 ip-options
  inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

حل بديل: غاية NAT

يمكن أن يوفر NAT للوجهة بديلا لإرساء DNS. يتطلب إستخدام NAT الوجهة في هذه الحالة إنشاء ترجمة كائن ثابت/nat تلقائي بين العنوان العام لخادم WWW في الداخل والعنوان الحقيقي على DMZ. لا يقوم NAT للوجهة بتغيير محتويات سجل DNS A الذي يتم إرجاعه من خادم DNS إلى العميل. بدلا من ذلك، عند إستخدام NAT الوجهة في سيناريو مثل ما تمت مناقشته في هذا المستند، يمكن للعميل إستخدام عنوان IP العام **172.20.1.10** الذي يتم إرجاعه بواسطة خادم DNS للاتصال بخادم WWW. يسمح الكائن الثابت/الترجمة التلقائية لجهاز الأمان بترجمة عنوان الوجهة من **172.20.1.10** إلى **10.10.10.10**. هنا الجزء ذو الصلة من التشكيل عندما غاية nat استعملت:

```
ASA Version 9.x
!
hostname ciscoasa
```

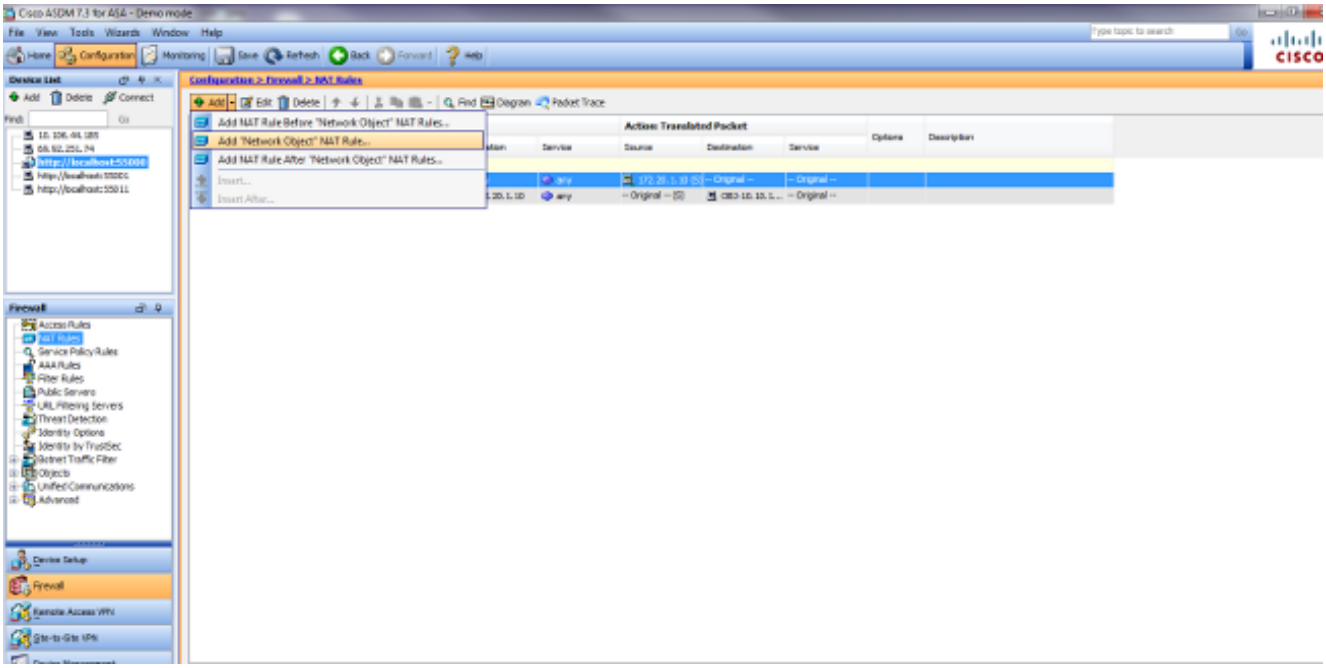
```
.Output suppressed ---!

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

.Output suppressed ---!

object network obj-192.168.100.0
 network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

The nat and global commands allow ---!
.clients access to the Internet ---!

object network obj-10.10.10.10
 host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

Static translation to allow hosts on the outside access ---!
.to the WWW server ---!

object network obj-10.10.10.10-1
 host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

تحقيق NAT للوجهة باستخدام بيان NAT يدوي/مرتين

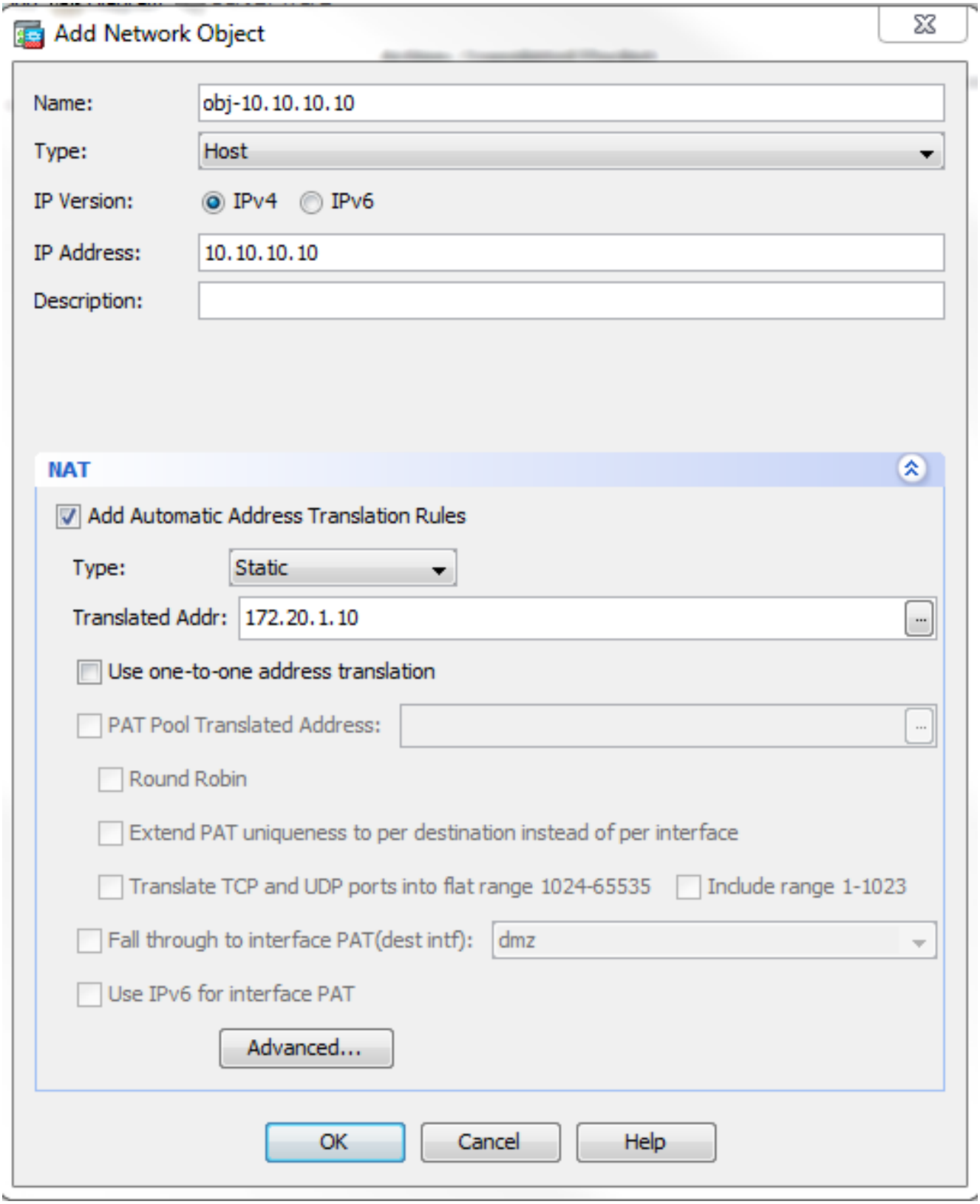
```
ASA Version 9.x
!
hostname ciscoasa

.Output suppressed ---!

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

.Output suppressed ---!

object network obj-192.168.100.0
 network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
 host 10.10.10.10

object network obj-172.20.1.10
 host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
        destination static obj-172.20.1.10 obj-10.10.10.10

Static translation to allow hosts on the inside access ---!
.to the WWW server via its outside address ---!

access-group OUTSIDE in interface outside

.Output suppressed ---!
```

أتمت هذا steps in order to شكلت غاية NAT في ال ASDM:

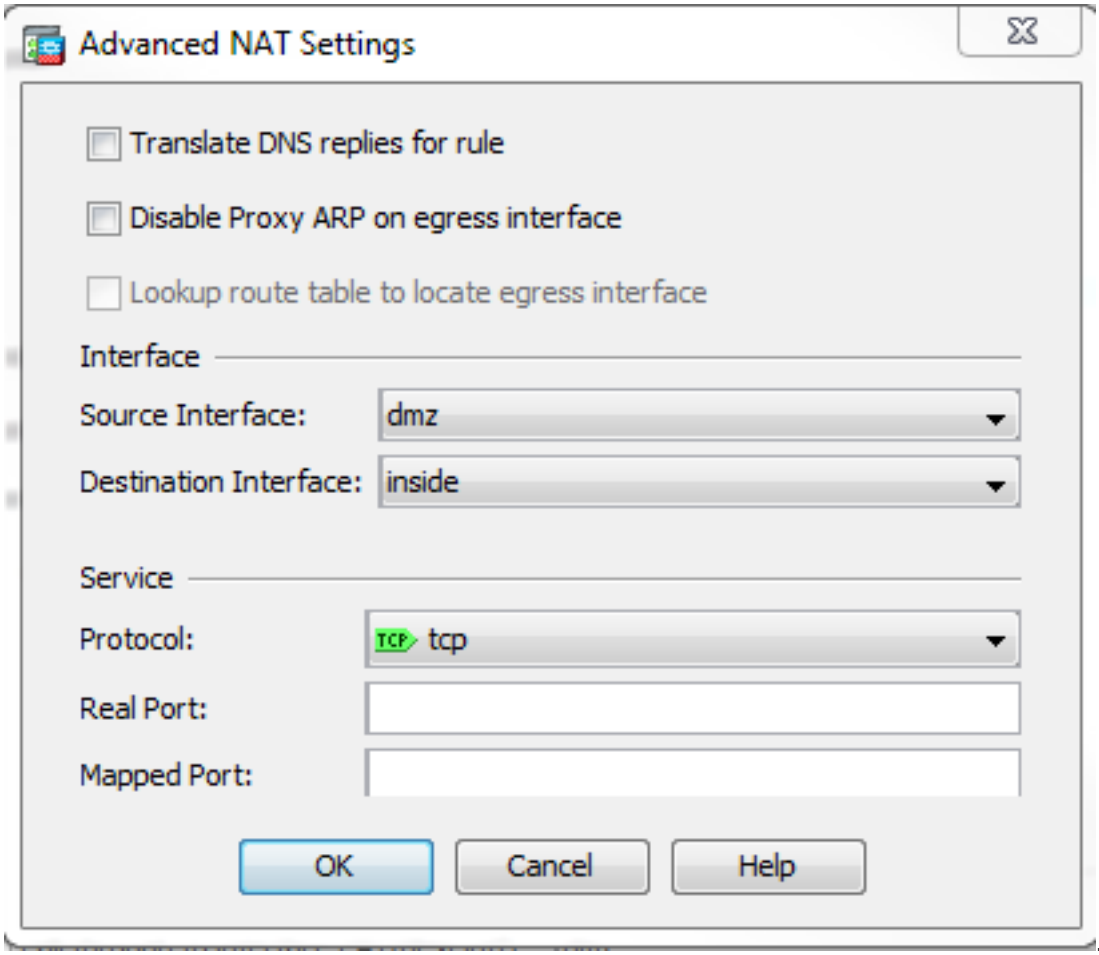
1. أخترت **تشكيل>nat قاعدة** واخترت **إضافة > إضافة "شبكة كائن" nat قاعدة...**



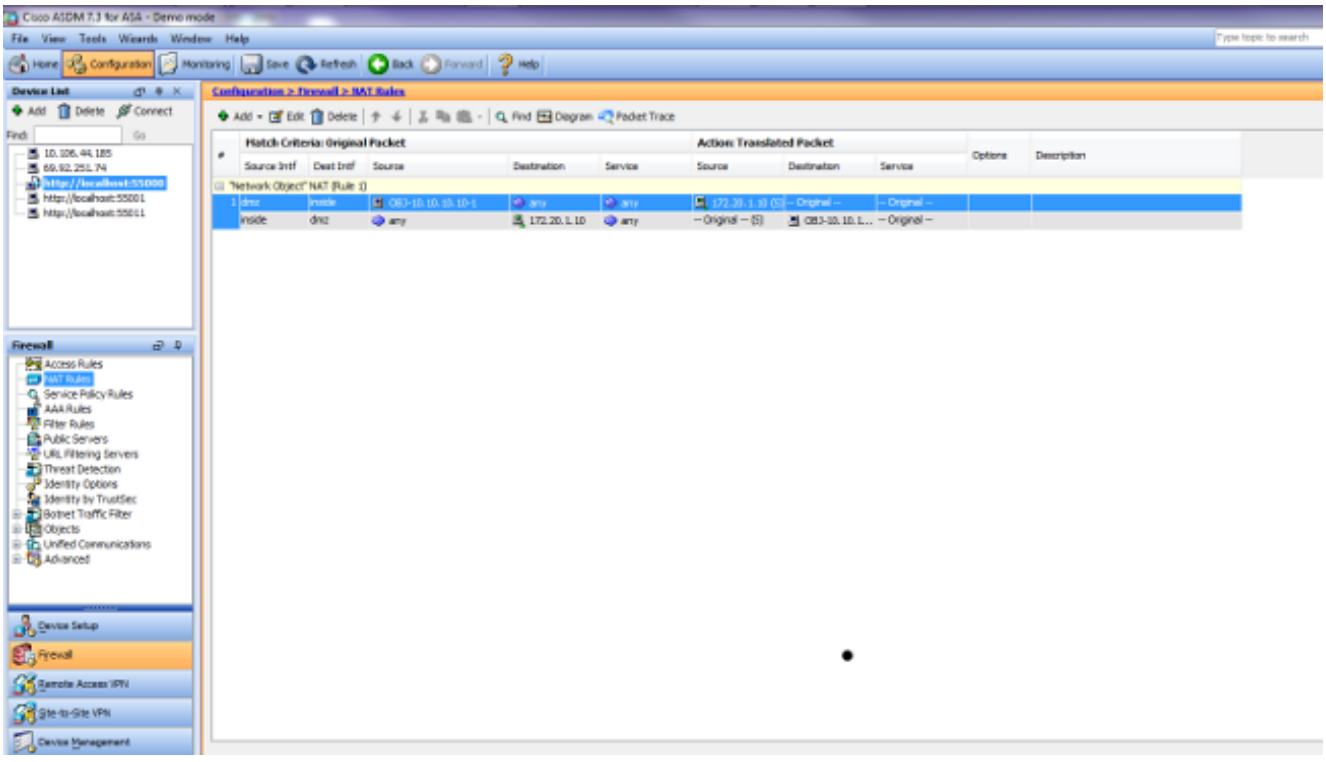
2. قم بتعبئة التكوين للترجمة الثابتة الجديدة. دخلت في الإسم مجال، **obj-10.10.10.10**.دخلت في العنوان مجال، العنوان من ال WWW نادل عنوان.من القائمة المنسدلة نوع، أختر **ساكن إستاتيكي**.دخلت في ال يترجم مجال، العنوان وقارن أن أنت تريد أن يعين ال WWW نادل إلى.طقطقة **متقدم**.



في القائمة المنسدلة "واجهة المصدر"، أختر **dmz**.في القائمة المنسدلة لواجهة الوجهة، أختر **داخلي**.في هذه الحالة، أخترت القارن داخلي أن يسمح مضيف على القارن داخلي أن ينفذ ال WWW نادل عن طريق ال يخطط عنوان



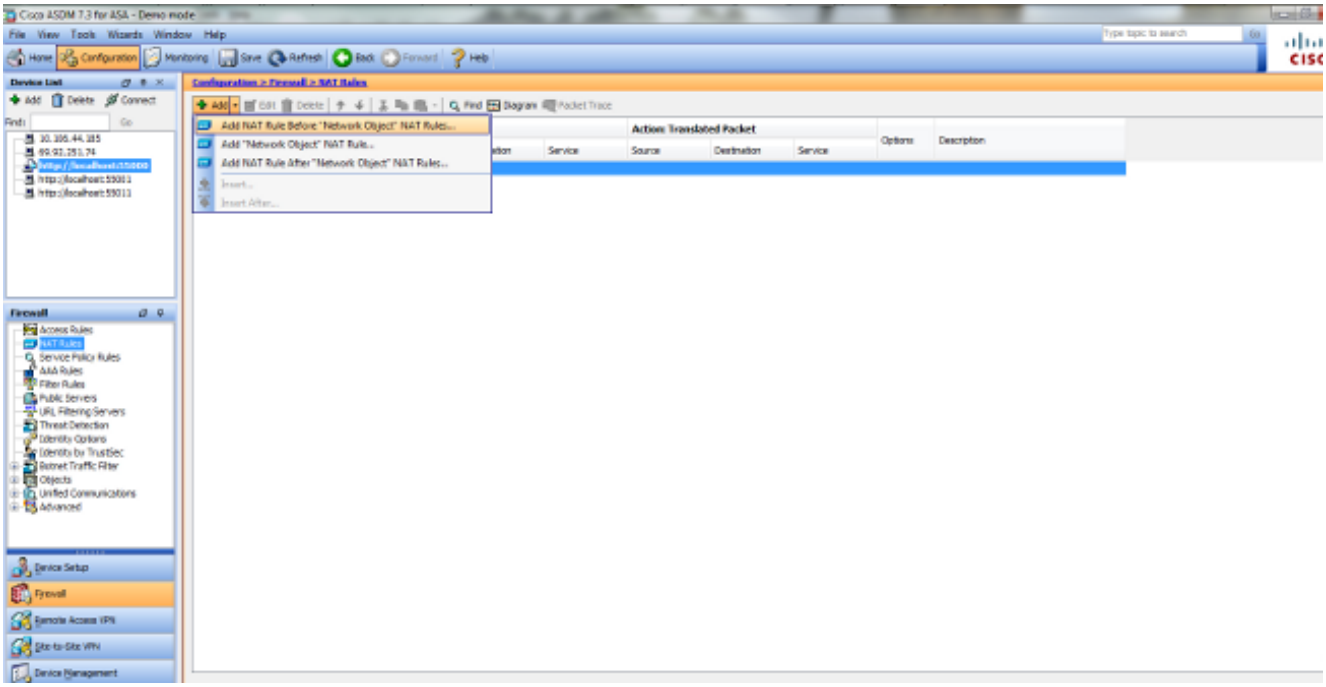
.172.20.1.10



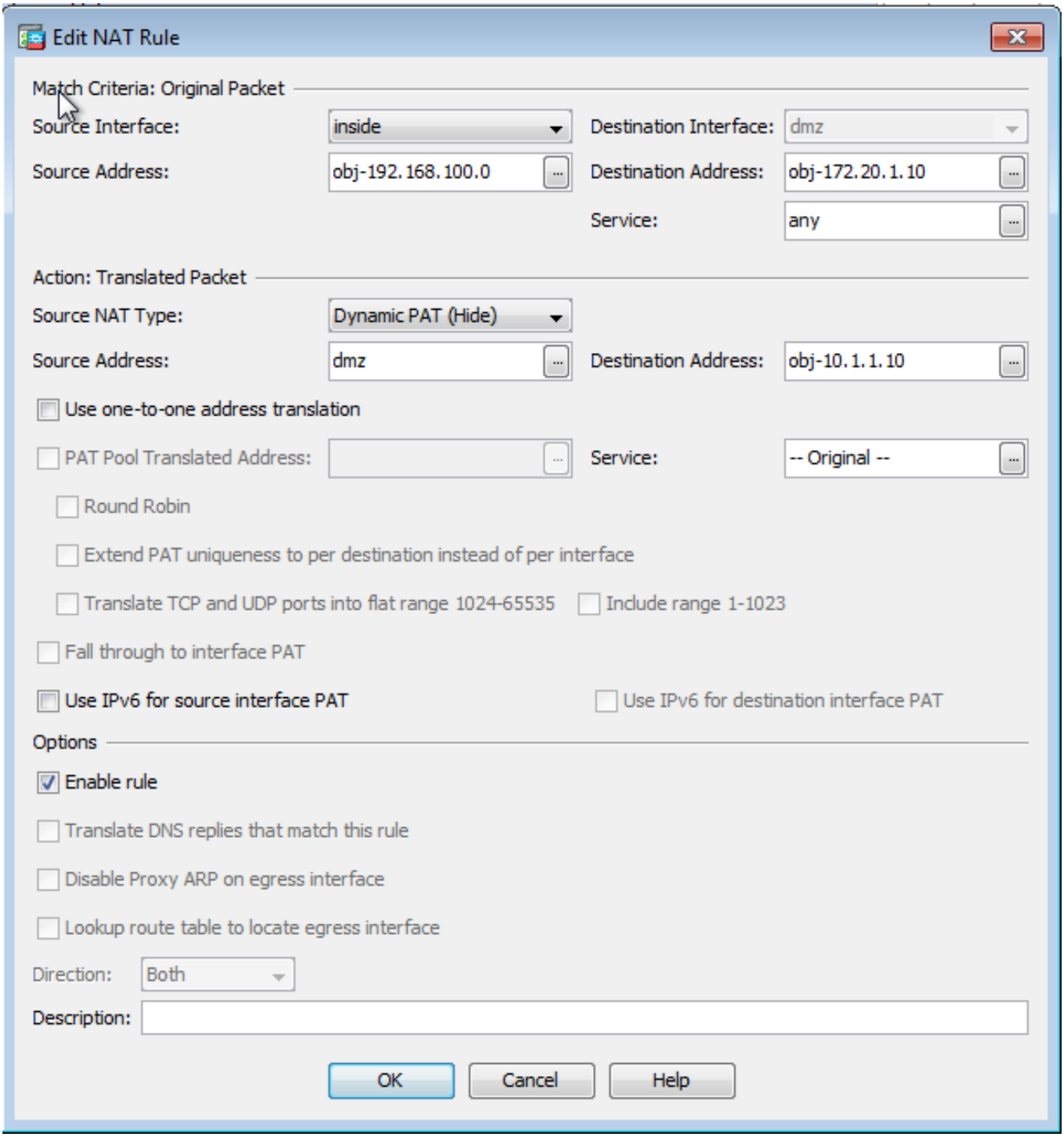
طقطقة ok in order to تركت الإضافة كائن/تلقائي nat قاعدة نافذة.انقر فوق **تطبيق** لإرسال التكوين إلى جهاز الأمان.

أسلوب بديل مع NAT يدويا/مرتين و ASDM

1. أخترت **تشكيل>nat قاعدة** واخترت **إضافة>إضافة nat قاعدة قبل "شبكة كائن" nat قاعدة....**



2. املأ التكوين للترجمة اليدوية/مرتين nat. في القائمة المنسدلة "واجهة المصدر"، أختر **الداخل**.في القائمة المنسدلة لواجهة الوجهة، أختر **dmz**.في حقل عنوان المصدر، أدخل كائن الشبكة الداخلي (obj-192.168.100.0).دخلت في الغاية عنوان مجال، ال tكائن IP الخاص بخادم 172.20.1.10) DMZ).في القائمة المنسدلة نوع NAT للمصدر، أختر **ضرب ديناميكي (إخفاء)**.دخلت في المصدر عنوان [إجراء: يترجم ربط قسم] مجال، **dmz**.في الوجهة العنوان [الإجراء: قسم الحزمة المترجم] الحقل، أدخل كائن IP الحقيقي للخادم DMZ (obj-10.10.10.10).



3. طقطقة ok in order to تركت الإضافة يدوي/مرتين nat قاعدة نافذة.
4. انقر فوق **تطبيق** لإرسال التكوين إلى جهاز الأمان.

هنا التسلسل الحادث أن يقع عندما غاية nat شكلت. 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 10.10.10.10.
```
ASA-7-609001: Built local-host dmz:10.10.10.10%
```
3. يقوم جهاز الأمان بإنشاء اتصال TCP بين العميل وخادم WWW. لاحظ العناوين المعينة لكل مضيف بين أقواس.
```
ASA-6-302013: Built outbound TCP connection 67956 for dmz:10.10.10.10/80%
(to inside:192.168.100.2/11001 (192.168.100.2/11001 (172.20.1.10/80)
```
4. يتحقق الأمر **show xlate** على جهاز الأمان من أن حركة مرور العميل تتم ترجمتها من خلال جهاز الأمان. في هذه الحالة، أول ترجمة ثابتة قيد الاستخدام.
```
ciscoasa#show xlate
```

```
in use, 9 most used 3
Global 192.168.100.0 Local 192.168.100.0
Global 172.20.1.10 Local 10.10.10.10
Global 172.20.1.10 Local 10.10.10.10
```

5. يتحقق الأمر **show conn** على جهاز الأمان من نجاح الاتصال بين العميل وخادم WWW من خلال جهاز الأمان. لاحظ العنوان الحقيقي لخادم WWW بين أقواس.

```
ciscoasa#show conn
TCP out 172.20.1.10(10.10.10.10):80 in 192.168.100.2:11001
idle 0:01:38 bytes 1486 flags UIO
```

التشكيل النهائي مع غاية NAT

هذا هو التكوين النهائي من ال ASA لإجراء توثيق DNS مع غاية NAT و 3 واجهات NAT.

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
shutdown
nameif outside
security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
shutdown
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
shutdown
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
object network obj-192.168.100.0
subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
host 10.10.10.10
object network obj-10.10.10.10-1
host 10.10.10.10
```

```
object network obj-172.20.1.10
host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
nat (inside,outside) dynamic interface
object network obj-10.10.10.10
nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
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 ip-options
       inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
                                  parameters
                       message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
                                  parameters
                       message-length maximum 512
                                               !
                 service-policy global_policy global
                                 prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
                                             end :
```

التكوين

أتمت هذا steps in order to مكنت فحص DNS (إن هو يكون أعجزت سابقا). 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.

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 محرك التفتيش.
```
ciscoasa(config-pmap)#parameters
```
3. في وضع تكوين معلمة خريطة السياسة، حدد الحد الأقصى لطول الرسالة لرسائل DNS التي يجب أن تكون 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، أستخدم خريطة سياسة التفتيش التي تم إنشاؤها في الخطوات 1-3 لتحديد أنه يجب فحص DNS.
```
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
```

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.

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 inside:192.168.100.10/80
```

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

معلومات ذات صلة

- دليل التكوين ASA 5500-X من Cisco
- مراجع أوامر سلسلة ASA 5500-X من Cisco
- إعلامات حقل منتج الأمان
- طلب التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

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).