# PIX/ASA 7.x/FWSM 3.x: ترجمة عناوين IP عالمية متعددة إلى عنوان IP محلي واحد باستخدام NAT الخاص بالسياسة الثابتة

## المحتويات



## المقدمة

يزود هذا وثيقة عينة تشكيل ل يخطط واحد محلي عنوان إلى إثنان أو أكثر شامل عنوان من خلال baser شبكة عنوان ترجمة (NAT) على ال PIX/Adaptive أمن جهاز (7.x (ASA برمجية.

## المتطلبات الأساسية

### المتطلبات

تأكد من تلبية هذه المتطلبات قبل تجربة هذا التكوين:

- تأكد من أن لديك معرفة عملية ب PIX/ASA 7.x CLI وخبرة سابقة في تكوين قوائم الوصول و NAT الثابتة.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- يستخدم هذا المثال المحدد ASA 5520. ومع ذلك، تعمل تكوينات NAT الخاصة بالسياسة على أي جهاز PIX أو ASA يشغل الإصدار 7.x.

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.

## الاصطلاحات

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

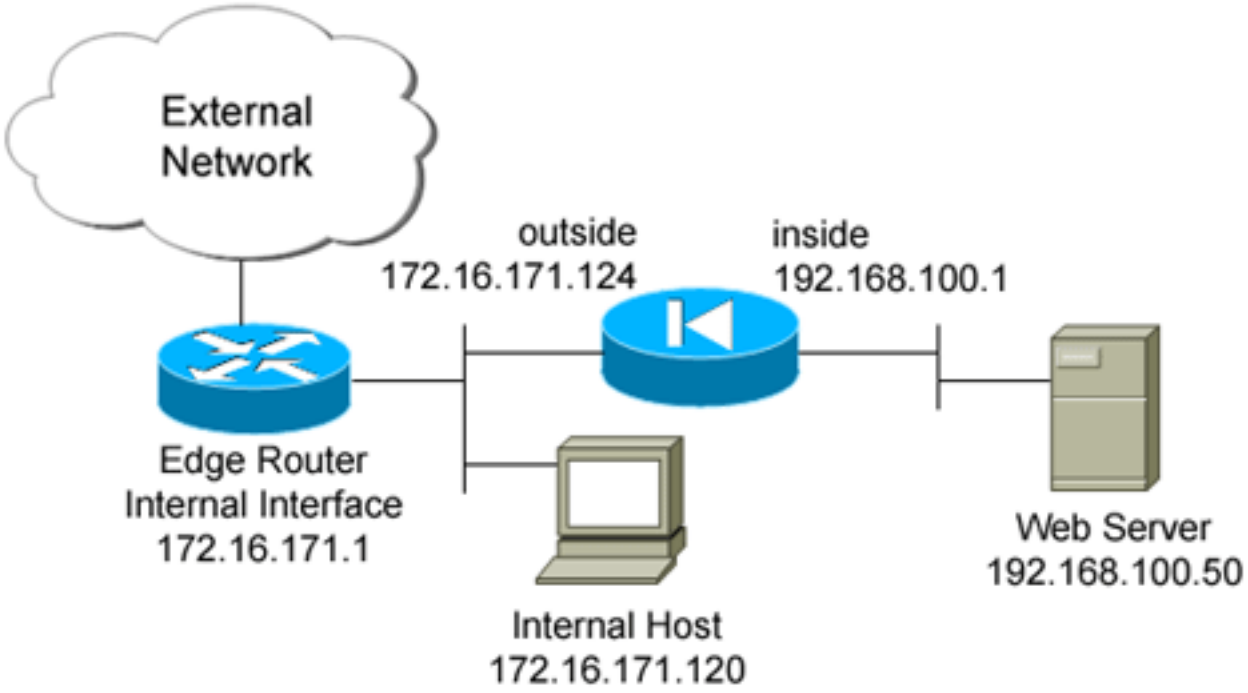
# التكوين

يحتوي مثال التكوين هذا على خادم ويب داخلي على 192.168.100.50، موجود خلف ASA. متطلب أن يكون الخادم بحاجة إلى أن يكون قابل للوصول إليه لواجهة الشبكة الخارجية عن طريق عنوانه الداخلي IP 192.168.100.50 وعنوانه الخارجي 172.16.171.125. هناك أيضا متطلب لسياسة الأمان أن عنوان IP الخاص 192.168.100.50 يمكن الوصول إليه فقط بواسطة شبكة 24/172.16.171.0. وبالإضافة إلى ذلك، فإن بروتوكول رسائل التحكم في الإنترنت (ICMP) وحركة مرور المنفذ 80 هي البروتوكولات الوحيدة المسموح بها الواردة إلى خادم الويب الداخلي. نظرا لوجود عنوانين عموميين ل IP تم تعيينهما إلى عنوان IP محلي واحد، يلزمك إستخدام NAT الخاص بالسياسة. وإلا، فإن PIX/ASA يرفض حادثتي البدء من واحد إلى واحد مع خطأ عنوان متداخل.

**ملاحظة:** أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي




## التكوين

يستخدم هذا المستند هذا التكوين.

```
ciscoasa(config)#show run
Saved :
:
(ASA Version 7.2(2
!
```

```
                                        hostname ciscoasa
                 enable password 8Ry2YjIyt7RRXU24 encrypted
                                                   names
                                                       !
                                 interface GigabitEthernet0/0
                                                nameif outside
                                              security-level 0
                    ip address 172.16.171.124 255.255.255.0
                                                       !
                                 interface GigabitEthernet0/1
                                                nameif inside
                                             security-level 100
                     ip address 192.168.100.1 255.255.255.0
                                                       !
                                 interface GigabitEthernet0/2
                                                 shutdown
                                               no nameif
                                          no security-level
                                              no ip address
                                                       !
                                 interface GigabitEthernet0/3
                                                 shutdown
                                               no nameif
                                          no security-level
                                              no ip address
                                                       !
                                      interface Management0/0
                                           nameif management
                                         security-level 100
                       ip address 192.168.1.1 255.255.255.0
                                          management-only
                                                       !
                             passwd 2KFQnbNIdI.2KYOU encrypted
                                           ftp mode passive


policy_nat_web1 and policy_nat_web2 are two access- ---!
     lists that match the source !--- address we want to
translate on. Two access-lists are required, though they
                !--- can be exactly the same. access-list
  policy_nat_web1 extended permit ip host 192.168.100.50
                                                      any
     access-list policy_nat_web2 extended permit ip host
                                        192.168.100.50 any

        The inbound_outside access-list defines the ---!
     security policy, as previously described. !--- This
access-list is applied inbound to the outside interface.
         access-list inbound_outside extended permit tcp
                                    172.16.171.0 255.255.255.0
                                host 192.168.100.50 eq www
        access-list inbound_outside extended permit icmp
                                    172.16.171.0 255.255.255.0
                             host 192.168.100.50 echo-reply
        access-list inbound_outside extended permit icmp
                                    172.16.171.0 255.255.255.0
                                 host 192.168.100.50 echo
access-list inbound_outside extended permit tcp any host
                                        172.16.171.125 eq www
    access-list inbound_outside extended permit icmp any
                                host 172.16.171.125 echo-reply
    access-list inbound_outside extended permit icmp any
                                    host 172.16.171.125 echo
                                           pager lines 24
```

```
logging asdm informational
mtu management 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

This first static allows users to reach the ---!
translated global IP address of the !--- web server.
Since this static appears first in the configuration,
for connections !--- initiated outbound from the
internal web server, the ASA translates the source !---
address to 172.16.171.125. static (inside,outside)
172.16.171.125  access-list policy_nat_web1

The second static allows networks to access the web ---!
server by its private !--- IP address of 192.168.100.50.
static (inside,outside) 192.168.100.50  access-list
policy_nat_web2

Apply the inbound_outside access-list to the ---!
outside interface. access-group inbound_outside in
interface outside

route outside 0.0.0.0 0.0.0.0 172.16.171.1 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
http server enable
http 192.168.1.0 255.255.255.0 management
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 preset_dns_map
parameters
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
!
service-policy global_policy global
prompt hostname context
```

## التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

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

1. على موجه IOS® 172.16.171.1 للتدفق، تحقق من إمكانية الوصول إلى كلا عنواني IP العامين لخادم الويب عبر الأمر **ping**.

```
router#ping 172.16.171.125

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.171.125, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router#ping 192.168.100.50

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 192.168.100.50, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

2. على ال ASA، دققت أن أنت ترى الترجمات أن يكون بنيت في الترجمة (xlate) طاولة.

```
ciscoasa(config)#show xlate global 192.168.100.50
                                    in use, 28 most used 2
Global 192.168.100.50 Local 192.168.100.50
ciscoasa(config)#show xlate global 172.16.171.125
                                    in use, 28 most used 2
Global 172.16.171.125 Local 192.168.100.50
```

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إذا لم ينجح إختبار الاتصال أو الاتصال، فحاول إستخدام syslog لتحديد ما إذا كانت هناك أي مشاكل في تكوين الترجمة. على شبكة تستخدم بشكل خفيف (مثل بيئة معملية)، يكون حجم مخزن التسجيل المؤقت كافيا عادة لاستكشاف المشكلة وإصلاحها. وإلا، يلزمك إرسال syslogs إلى خادم syslog خارجي. قم بتمكين التسجيل إلى المخزن المؤقت على المستوى 6 لمعرفة ما إذا كان التكوين صحيحا في إدخالات syslog هذه.

```
ciscoasa(config)#logging buffered 6
ciscoasa(config)#logging on

From 172.16.171.120, initiate a TCP connection to port 80 to both the external !--- ---!
(172.16.171.125) and internal addresses (192.168.100.50). ciscoasa(config)#show log
Syslog logging: enabled
        Facility: 20
Timestamp logging: disabled
```

```
                                    Standby logging: disabled
                                Deny Conn when Queue Full: disabled
                                    Console logging: disabled
                                    Monitor logging: disabled
                            Buffer logging: level debugging, 4223 messages logged
                                       Trap logging: disabled
                                    History logging: disabled
                                          Device ID: disabled
                                       Mail logging: disabled
                            ASDM logging: level informational, 4032 messages logged
                        .ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command%
                                ASA-7-609001: Built local-host outside:172.16.171.120%
                                ASA-7-609001: Built local-host inside:192.168.100.50%
ASA-6-302013: Built inbound TCP connection 67 for outside:172.16.171.120/33687%
                    (to inside:192.168.100.50/80 (172.16.171.125/80 (172.16.171.120/33687)
ASA-6-302013: Built inbound TCP connection 72 for outside:172.16.171.120/33689%
                    (to inside:192.168.100.50/80 (192.168.100.50/80 (172.16.171.120/33689)
```

إن يرى أنت ترجمة خطأ في السجل، فحصت مزدوج تشكيل nat ك. إن لا يراقب أنت أي syslogs، استعملت **الالتقاط** وظيفة على ال ASA أن يحاول أن على قبض الحركة مرور على القارن. لإعداد التقاط، يجب عليك أولا تحديد قائمة وصول للمطابقة على نوع معين من حركة المرور أو تدفق TCP. بعد ذلك، يجب عليك تطبيق هذا الالتقاط على واجهة واحدة أو أكثر لبدء التقاط الحزم.

```
Create a capture access-list to match on port 80 traffic to !--- the external IP address of ---!
.172.16.171.125. !--- Note: These commands are over two lines due to spatial reasons

ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.120
                                        host 172.16.171.125 eq 80
ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.125
                                         eq 80 host 172.16.171.120
                                                #(ciscoasa(config

.Apply the capture to the outside interface ---!

ciscoasa(config)#capture capout access-list acl_capout interface outside

After you initiate the traffic, you see output similar to this when you view !--- the ---!
capture. Note that packet 1 is the SYN packet from the client, while packet !--- 2 is the SYN-
ACK reply packet from the internal server. If you apply a capture !--- on the inside interface,
.in packet 2 you should see the server reply with !--- 192.168.100.50 as its source address

ciscoasa(config)#show capture capout
                                                packets captured 4
S :172.16.171.125.80 < 172.16.171.120.21505 13:17:59.157859 :1
                        <win 4128 <mss 1460 (0)2696120951:2696120951
S :172.16.171.120.21505 < 172.16.171.125.80 13:17:59.159446 :2
 <ack 2696120952 win 4128 <mss 536 (0)1512093091:1512093091
. :172.16.171.125.80 < 172.16.171.120.21505 13:17:59.159629 :3
                                        ack 1512093092 win 4128
. :172.16.171.125.80 < 172.16.171.120.21505 13:17:59.159873 :4
                                        ack 1512093092 win 4128
```

## معلومات ذات صلة

- مرجع أمر ASA 7.2
- برنامج جدار حماية Cisco PIX

- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات 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).