# موجه ثنائي الواجهة مع تكوين جدار حماية Cisco IOS

## المحتويات



## المقدمة

تعمل عينة التكوين هذه من أجل مكتب صغير جدا متصل مباشرة بالإنترنت. من المفترض أن خدمة اسم المجال (DNS) وبروتوكول نقل البريد البسيط (SMTP) وخدمات الويب يتم توفيرها بواسطة نظام بعيد يشغله موفر خدمة الإنترنت (ISP). لا توجد خدمات على الشبكة الداخلية، مما يجعل هذا النوع من تكوينات جدار الحماية الأكثر بساطة، نظرا لوجود واجهتين فقط. لا يوجد تسجيل، نظرا لعدم توفر مضيف لتوفير خدمات التسجيل.

أحلت ثلاثة قارن مسحاج تخديد دون nat cisco ios جدار حماية تشكيل in order to شكلت ثلاثة قارن مسحاج تخديد دون NAT يستعمل ال cisco IOS® جدار حماية.

أحلت إثنان قارن مسحاج تخديد دون nat يستعمل cisco ios جدار حماية تشكيل in order to شكلت إثنان قارن مسحاج تخديد دون nat يستعمل ال cisco ios جدار حماية.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

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

- برنامج IOS الإصدار 12.2 من Cisco
- موجّه Cisco 3640

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة 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.

## معلومات أساسية

بما أن هذا التكوين يستخدم قوائم الوصول إلى الإدخال فقط، فإنه يقوم بكل من منع الانتحال وتصفية حركة المرور باستخدام نفس قائمة الوصول (101). يعمل هذا التكوين فقط لموجه ثنائي المنافذ. إيثرنت 1 هي الشبكة "الداخلية". التسلسل 0 هو الواجهة الخارجية. توضح قائمة الوصول (112) على التسلسل 0 هذا باستخدام عناوين IP العالمية لترجمة عنوان الشبكة (150.150.150.x) (NAT) كوجهات.

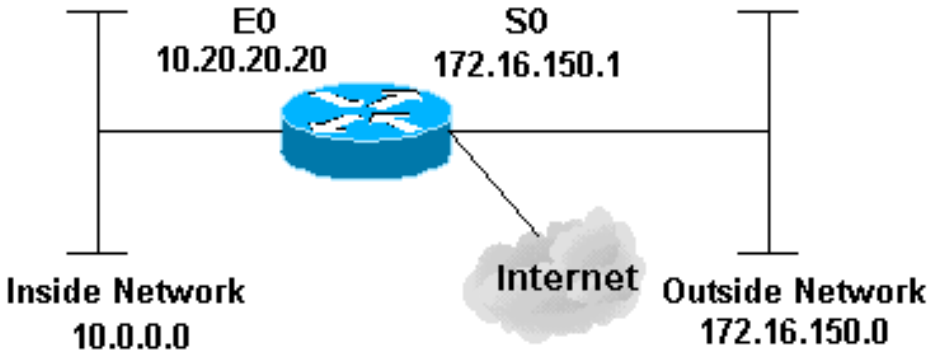
## التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

**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.

## الموجه 3640

```
version 12.2
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
no service password-encryption
!
hostname pig
!
boot system flash flash:c3640-jk9o3s-mz.122-21a.bin
logging buffered 4096 debugging
enable secret 5 $1$chHU$wiC58FP/IDloZuorCkzEz1
enable password ww
!
clock timezone CET 1
clock summer-time CET recurring
ip subnet-zero
!
!
no ip domain-lookup
!
 This is the Cisco IOS Firewall !--- configuration ---!
and what to inspect. ip inspect name ethernetin cuseeme
timeout 3600
ip inspect name ethernetin ftp timeout 3600
ip inspect name ethernetin h323 timeout 3600
ip inspect name ethernetin http timeout 3600
ip inspect name ethernetin rcmd timeout 3600
ip inspect name ethernetin realaudio timeout 3600
ip inspect name ethernetin smtp timeout 3600
ip inspect name ethernetin sqlnet timeout 3600
ip inspect name ethernetin streamworks timeout 3600
ip inspect name ethernetin tcp timeout 3600
ip inspect name ethernetin tftp timeout 30
ip inspect name ethernetin udp timeout 15
ip inspect name ethernetin vdolive timeout 3600
ip audit notify log
ip audit po max-events 100
!
call rsvp-sync
!
!
!
!
!
!
!
 This is the inside of the network. interface ---!
Ethernet0/0 ip address 10.20.20.20 255.255.255.0
ip access-group 101 in
ip nat inside
ip inspect ethernetin in
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Serial1/0
no ip address
```

```
                                                shutdown
                                                !
                                        interface Serial1/1
                                             no ip address
                                                shutdown
                                                !
                                        interface Serial1/2
                                             no ip address
                                                shutdown
                                                !
    This is the outside of the interface. interface ---!
         Serial1/3 ip address 172.16.150.1 255.255.255.0
                                      ip access-group 112 in
                                             ip nat outside
                                                !
                                    .Define the NAT pool ---!
  ip nat pool mypool 172.16.150.3 172.16.150.255 netmask
                                                255.255.255.0
                    ip nat inside source list 1 pool mypool
                                                ip classless
                      ip route 0.0.0.0 0.0.0.0 172.16.150.2
                                                ip http server
                                                !
                  access-list 1 permit 10.0.0.0 0.255.255.255
Access list applied on the inside for anti-spoofing ---!
                reasons. access-list 101 permit tcp 10.0.0.0
                                            0.255.255.255 any
    access-list 101 permit udp 10.0.0.0 0.255.255.255 any
  access-list 101 permit icmp 10.0.0.0 0.255.255.255 any
                     access-list 101 deny   ip any any log
     Access list applied on the outside for security ---!
     reasons. access-list 112 permit icmp any 172.16.150.0
                                          0.0.0.255 unreachable
  access-list 112 permit icmp any 150.150.150.0 0.0.0.255
                                                echo-reply
    access-list 112 permit icmp any 172.16.150.0 0.0.0.255
                                             packet-too-big
    access-list 112 permit icmp any 172.16.150.0 0.0.0.255
                                           time-exceeded
    access-list 112 permit icmp any 172.16.150.0 0.0.0.255
                                              traceroute
    access-list 112 permit icmp any 172.16.150.0 0.0.0.255
                                  administratively-prohibited
    access-list 112 permit icmp any 172.16.150.0 0.0.0.255
                                                      echo
                    access-list 112 deny  ip any any log
                                                !
                                                !
                                        dial-peer cor custom
                                                !
                                                !
                                                !
                                                !
                                                !
                                               line con 0
                                          exec-timeout 0 0
                                                line 97 102
                                                 line aux 0
                                               line vty 0 4
                                          exec-timeout 0 0
                                               password ww
                                                     login
                                                !
                                               end
```

# 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** .

- **يعرض show version**—معلومات حول إصدار البرنامج الذي تم تحميله حاليا بالإضافة إلى معلومات الأجهزة والأجهزة.
- **debug ip nat**— يعرض معلومات حول حزم IP التي تتم ترجمتها بواسطة ميزة IP nat.
- **عرض ترجمات ip nat**—يعرض NATs نشطة.
- **show log**—يعرض معلومات التسجيل.
- **show ip access-list**— يعرض محتويات جميع قوائم الوصول إلى IP الحالية.
- **show ip inspection session**—يعرض الجلسات الموجودة التي يتم تتبعها وفحصها حاليا بواسطة جدار حماية Cisco IOS.
- **debug ip inspection tcp**—يعرض الرسائل حول أحداث جدار حماية Cisco IOS.

وهذه عينة من مخرجات الأمر من الأمر **show version**.

```
pig#show version
Cisco Internetwork Operating System Software
(IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2
.Copyright (c) 1986-2004 by cisco Systems, Inc
Compiled Fri 09-Jan-04 16:23 by kellmill
Image text-base: 0x60008930, data-base: 0x615DE000

(ROM: System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1

pig uptime is 59 minutes
System returned to ROM by reload at 16:05:44 CET Wed Jan 14 2004
"System image file is "flash:c3640-jk9o3s-mz.122-21a.bin


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
.third-party authority to import, export, distribute or use encryption
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
.to comply with U.S. and local laws, return this product immediately

:A summary of U.S. laws governing Cisco cryptographic products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
.export@cisco.com

.cisco 3640 (R4700) processor (revision 0x00) with 126976K/4096K bytes of memory
Processor board ID 10577176
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
.MICA-6DM Firmware: CP ver 2730 - 5/23/2001, SP ver 2730 - 5/23/2001
.Bridging software
.X.25 software, Version 3.0.0
.(SuperLAT software (copyright 1990 by Meridian Technology Corp
.TN3270 Emulation software
(Ethernet/IEEE 802.3 interface(s 2
```

```
(Low-speed serial(sync/async) network interface(s 4
(terminal line(s 6
(Virtual Private Network (VPN) Module(s 1
.DRAM configuration is 64 bits wide with parity disabled
.125K bytes of non-volatile configuration memory
(32768K bytes of processor board System flash (Read/Write
```

أول، دققت nat يعمل بشكل صحيح يستعمل **debug ip nat** و**أبديت ip nat ترجمة** كما هو موضح في هذا إنتاج.

```
pig#debug ip nat
IP NAT debugging is on
#pig
 [Mar  1 01:40:47.692 CET: NAT: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [80*
[Mar  1 01:40:47.720 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [80*
[Mar  1 01:40:47.720 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [81*
[Mar  1 01:40:47.748 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [81*
[Mar  1 01:40:47.748 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [82*
[Mar  1 01:40:47.784 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [82*
[Mar  1 01:40:47.784 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [83*
[Mar  1 01:40:47.836 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [83*
[Mar  1 01:40:47.836 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [84*
[Mar  1 01:40:47.884 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [84*

pig#show ip nat translations
  Pro Inside global      Inside local       Outside local      Outside global
                  ---                ---           10.0.0.1      172.16.150.4 ---
```

دون إضافة بيان **فحص ip**، تأكد من أن قوائم الوصول تعمل بشكل صحيح. **الـ deny ip any** مع الـ **log**يقول الكلمة المفتاح أنت ما الحزم يكون منعت.

في هذه الحالة، هذه هي حركة المرور العائدة من جلسة Telnet إلى 172.16.150.2 من 10.0.0.1 (مترجمة إلى 172.16.150.4).

وهذا نموذج إخراج من الأمر **show log**.

```
pig#show log
,Syslog logging: enabled (0 messages dropped, 0 messages rate-limited
(flushes, 0 overruns 0
Console logging: level debugging, 92 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 60 messages logged
(Logging Exception size (4096 bytes
Trap logging: level informational, 49 message lines logged

:(Log Buffer (4096 bytes

Mar  1 01:24:08.518 CET: %SYS-5-CONFIG_I: Configured from console by console*
Mar  1 01:26:47.783 CET: %SYS-5-CONFIG_I: Configured from console by console*
(Mar  1 01:27:09.876 CET: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23*
packet 1 ,(11004)172.16.150.4 <-
(Mar  1 01:33:03.371 CET: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23*
packets 3 ,(11004)172.16.150.4 <-
```

أستخدم الأمر **show ip access-lists** لمعرفة عدد الحزم التي تطابق قائمة الوصول.

```
pig#show ip access-lists
Standard IP access list 1
(permit 10.0.0.0, wildcard bits 0.255.255.255 (28 matches
Extended IP access list 101
(permit tcp 10.0.0.0 0.255.255.255 any (32 matches
```

```
                                        permit udp 10.0.0.0 0.255.255.255 any
                                (permit icmp 10.0.0.0 0.255.255.255 any (22 matches
                                                    deny ip any any log
                                                Extended IP access list 112
                                    permit icmp any 172.16.150.0 0.0.0.255 unreachable
                            (permit icmp any 172.16.150.0 0.0.0.255 echo-reply (10 matches
                                    permit icmp any 172.16.150.0 0.0.0.255 packet-too-big
                                     permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
                                        permit icmp any 172.16.150.0 0.0.0.255 traceroute
                        permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited
                                            permit icmp any 172.16.150.0 0.0.0.255 echo
                                                (deny ip any any log (12 matches
                                                                                    #pig
```

بمجرد إضافة بيان **فحص ip**، يمكنك أن ترى أن هذا السطر تمت إضافته ديناميكيا في قائمة الوصول للسماح بجلسة عمل برنامج Telnet هذه:

```
(permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq 11004 (16 matches

                                                    pig#show ip access-lists
                                                  Standard IP access list 1
                                (permit 10.0.0.0, wildcard bits 0.255.255.255 (44 matches
                                                Extended IP access list 101
                                        (permit tcp 10.0.0.0 0.255.255.255 any (50 matches
                                            permit udp 10.0.0.0 0.255.255.255 any
                                (permit icmp 10.0.0.0 0.255.255.255 any (22 matches
                                                    deny ip any any log
                                                Extended IP access list 112
            (permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq 11004 (16 matches
                                    permit icmp any 172.16.150.0 0.0.0.255 unreachable
                            (permit icmp any 172.16.150.0 0.0.0.255 echo-reply (10 matches
                                    permit icmp any 172.16.150.0 0.0.0.255 packet-too-big
                                     permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
                                        permit icmp any 172.16.150.0 0.0.0.255 traceroute
                        permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited
                                            permit icmp any 172.16.150.0 0.0.0.255 echo
                                                (deny ip any any log (12 matches
                                                                                    #pig
```

يمكنك أيضا التحقق باستخدام الأمر **show ip inspection session** الذي يظهر الجلسات الحالية التي تم إنشاؤها من خلال جدار الحماية.

```
                                                    pig#show ip inspect session
                                                        Established Sessions
                Session 624C31A4 (10.0.0.1:11006)=>(172.16.150.2:23) tcp SIS_OPEN
```

أخيرا، على مستوى أكثر تقدما، يمكنك أيضا تمكين الأمر **debug ip inspection tcp**.

```
                                                    pig#debug ip inspect tcp
                                                INSPECT TCP Inspection debugging is on
                                                                                    #pig
                                    Mar  1 01:49:51.756 CET: CBAC sis 624C31A4 pak 624D0FA8 TCP S*
                                (seq 2890060460(0) (172.16.150.4:11006) => (172.16.150.2:23
                                    Mar  1 01:49:51.776 CET: CBAC sis 624C31A4 pak 624D0CC4 TCP S*
                        (ack 2890060461 seq 1393191461(0) (10.0.0.1:11006) <= (172.16.150.2:23
                                     Mar  1 01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284 TCP*
                    (ack 1393191462 seq 2890060461(0) (172.16.150.4:11006) => (172.16.150.2:23
                                Mar  1 01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284 TCP P ack*
                        (seq 2890060461(12) (172.16.150.4:11006) => (172.16.150.2:23 1393191462
                                    Mar  1 01:49:51.780 CET: CBAC* sis 624C31A4 pak 62576284 TCP ack*
                            (seq 2890060473(0) (172.16.150.4:11006) => (172.16.150.2:23 1393191462
```

# استكشاف الأخطاء وإصلاحها

بعد تكوين موجه جدار حماية IOS، إذا لم تعمل الاتصالات، فتأكد من تمكين الفحص باستخدام الأمر **ip inspection (name defined) in or out** على الواجهة. في هذا تشكيل، طبقت **ip** فحص **إثرنيت** in ل القارن **إثرنيت0/0**.

للحصول على أستكشاف الأخطاء العامة وإصلاحها على هذا التكوين، ارجع إلى أستكشاف أخطاء تكوينات جدار حماية Cisco IOS وإصلاحها ووكيل مصادقة أستكشاف الأخطاء وإصلاحها.

## المشكلة

لا يمكنك تنفيذ تنزيلات HTTP نظرا لفشلها أو انقضاء مهلتها. فكيف يجري حل ذلك؟

## الحل

يمكن حل المشكلة عن طريق إزالة **فحص ip** لحركة مرور HTTP حتى لا يتم فحص حركة مرور HTTP ويحدث التنزيل كما هو متوقع.

# معلومات ذات صلة

- صفحة دعم جدار حماية IOS
- 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).