موجه ثنائي الواجهة بدون NAT باستخدام تكوين جدار حماية Cisco IOS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوين
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يعمل نموذج التكوين هذا لمكتب صغير جدا يتصل مباشرة بالإنترنت، مع افتراض 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 وواجهتان فقط. لا يوجد أيضا تسجيل لعدم توفر مضيف لتقديم خدمات التسجيل.

ونظرا لأن هذا التكوين يستخدم قوائم الوصول إلى الإدخال فقط، فإنه يقوم بكل من منع الانتحال وتصفية حركة المرور باستخدام قائمة الوصول نفسها. يعمل هذا التكوين فقط لموجه ثنائي المنافذ. إيثرنت 0 هو الشبكة "الداخلية". التسلسل 0 هو إرتباط ترحيل إطارات إلى ISP.

أحلت إثنان قارن مسحاج تخديد مع nat cisco ios جدار حماية تشكيل in order to شكلت إثنان قارن مسحاج تخديد مع NAT يستعمل cisco IOS® جدار حماية.

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

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تنطبق المعلومات الواردة في هذا المستند على إصدارات البرامج والمكونات المادية التالية:

- برنامج IOS® الإصدار 12.2(15)T13 من Cisco، مدعوم من برنامج Cisco IOS الإصدار T.11.3.3
- موجّه Cisco 2611

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.

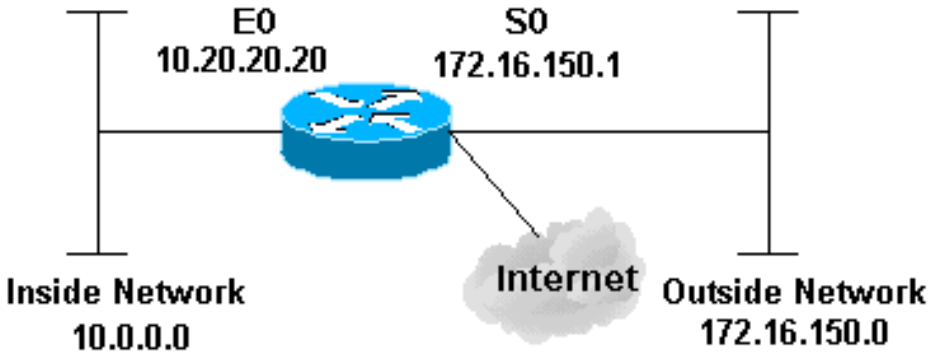
التكوين

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

يستعمل هذا وثيقة هذا تشكيل:

الموجه 2514
version 12.2 ! service password-encryption

```
no service udp-small-servers
no service tcp-small-servers
no cdp run
!
hostname cbac-cisco
!
no ip source-route
!
/enable secret 5 $1$FrMn$wBu0Xgv/Igy5Y.DarCmrm
!
username cisco privilege 15 password 7 0822455D0A16
no ip source-route
ip domain-name cisco.com
ip name-server 172.16.150.5
!
Set up inspection list "myfw". !--- Inspect for the ---!
protocols that actually get used. ! ip inspect name myfw
cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
interface Ethernet0/0
description Cisco Ethernet RTP
ip address 10.20.20.20 255.255.255.0
no ip directed-broadcast
!
Apply the access list in order to allow all ---!
legitimate traffic !--- from the inside network but
prevent spoofing. ! ip access-group 101 in ! no ip
proxy-arp ! !--- Apply inspection list "myfw" to
Ethernet 0 inbound. !--- When conversations are
initiated from the internal network !--- to the outside,
this inspection list causes temporary additions !--- to
the traffic allowed in by serial interface 0 acl 111
when !--- traffic returns in response to the initiation.
! ip inspect myfw in
no ip route-cache
!
no cdp enable
!
interface Serial0/0
description Cisco FR
ip address 172.16.150.1 255.255.255.0
encapsulation frame-relay IETF
no ip route-cache
no arp frame-relay
bandwidth 56
service-module 56 clock source line
service-module 56k network-type dds
frame-relay lmi-type ansi
!
Access list 111 allows some ICMP traffic and ---!
administrative Telnet, !--- and does anti-spoofing.
There is no inspection on Serial 0. !--- However, the
inspection on the Ethernet interface adds temporary
entries !--- to this list when hosts on the internal
network make connections !--- out through the Frame
Relay. ! ip access-group 111 in no ip directed-broadcast
```

```
no ip route-cache bandwidth 56 no cdp enable frame-relay
       interface-dlci 16 ! ip classless ip route 0.0.0.0
0.0.0.0 Serial0 ! !--- Access list 20 is used to control
       which network management stations !--- can access
through SNMP. ! access-list 20 permit 172.16.150.8 ! !--
- The access list allows all legitimate traffic from the
inside network !--- but prevents spoofing. ! access-list
   101 permit tcp 172.16.150.0 0.0.0.255 any access-list
   101 permit udp 172.16.150.0 0.0.0.255 any access-list
    101 permit icmp 172.16.150.0 0.0.0.255 any !--- This
  deny is the default. access-list 101 deny ip any any !
    !--- Access list 111 controls what can come from the
   outside world !--- and it is anti-spoofing. ! access-
list 111 deny ip 127.0.0.0 0.255.255.255 any access-list
111 deny ip 172.16.150.0 0.0.0.255 any ! !--- Perform an
  ICMP stuff first. There is some danger in these lists.
!--- They are control packets, and allowing *any* packet
opens !--- you up to some possible attacks. For example,
      teardrop-style !--- fragmentation attacks can come
    through this list. ! access-list 111 permit icmp any
      172.16.150.0 0.0.0.255 administratively-prohibited
  access-list 111 permit icmp any 172.16.150.0 0.0.0.255
       echo access-list 111 permit icmp any 172.16.150.0
    0.0.0.255 echo-reply access-list 111 permit icmp any
   172.16.150.0 0.0.0.255 packet-too-big access-list 111
    permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
  access-list 111 permit icmp any 172.16.150.0 0.0.0.255
 traceroute access-list 111 permit icmp any 172.16.150.0
   0.0.0.255 unreachable ! !--- Allow Telnet access from
   10.11.11.0 corporate network administration people. !
    access-list 111 permit tcp 10.11.11.0 0.0.0.255 host
 172.16.150.1 eq telnet ! !--- This deny is the default.
   ! access-list 111 deny ip any any ! !--- Apply access
list 20 for SNMP process. ! snmp-server community secret
          RO 20 ! line con 0 exec-timeout 5 0 password 7
14191D1815023F2036 login local line vty 0 4 exec-timeout
 5 0 password 7 14191D1815023F2036 login local length 35
                                                    end
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين 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 **فحص** **in** myfw **ip** للقارن إثرنيت0/0.

بالنسبة لهذه الأوامر، ارجع إلى وكيل مصادقة أستكشاف الأخطاء وإصلاحها، إلى جانب معلومات أستكشاف الأخطاء وإصلاحها الأخرى.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إصدار أوامر **debug**.

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).