مجموعة حماية جدار الحماية بدون تكوين NAT باستخدام Cisco IOS

المحتويات

المقدمة

يقدم هذا المستند مثالا للتكوين النموذجي للشركات الصغيرة المتصلة بالإنترنت والتي تقوم بتشغيل خوادمها الخاصة. الاتصال بالإنترنت عبر خط تسلسلي. يتصل إيثرنت 0 بالشبكة الداخلية (شبكة محلية واحدة). يتصل إيثرنت 1 بشبكة DMZ، والتي تحتوي على عقدة واحدة تستخدم لتوفير الخدمات للعالم الخارجي. قام مزود خدمة الإنترنت (ISP) بتعيين المجموعة 24/192.168.27.0 للشركة. هذا بشكل متساو بين DMZ وشبكة LAN الداخلية مع قناع الشبكة الفرعية 255.255.255.128. وتتمثل السياسة الأساسية في ما يلي:

- السماح للمستخدمين الموجودين على الشبكة الداخلية بالاتصال بأية خدمة على الإنترنت العامة.
- السماح لأي شخص على الإنترنت بالاتصال بخدمات WWW و FTP وبروتوكول نقل البريد البسيط (SMTP) على خادم DMZ، وإجراء استعلامات نظام اسم المجال (DNS) عليه. وهذا يسمح للأشخاص الخارجيين بعرض صفحات الشركة على الويب، والتقاط الملفات التي قامت الشركة بنشرها للاستهلاك الخارجي، وإرسال البريد إلى الشركة.
- السماح للمستخدمين الداخليين بالاتصال بخدمة POP على خادم DMZ (لالتقاط بريدهم) وبرنامج Telnet (لإدارتها).
- لا تسمح لأي شيء على المنطقة المنزوعة السلاح ببدء أي إتصالات، إما بالشبكة الخاصة أو بالإنترنت.
- تدقيق جميع الاتصالات التي تعبر جدار الحماية إلى خادم SYSLOG على الشبكة الخاصة. تستخدم الأجهزة الموجودة على الشبكة الداخلية خادم DNS على DMZ. يتم إستخدام قوائم الوصول إلى الإدخال على جميع الواجهات لمنع الانتحال. يتم إستخدام قوائم الوصول إلى الإخراج للتحكم في حركة المرور التي يمكن إرسالها إلى أي واجهة محددة.

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.

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.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS الإصدار 12.2(15)T13 من Cisco مع مجموعة ميزات جدار الحماية
- الموجه VXR 7204 من Cisco

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.

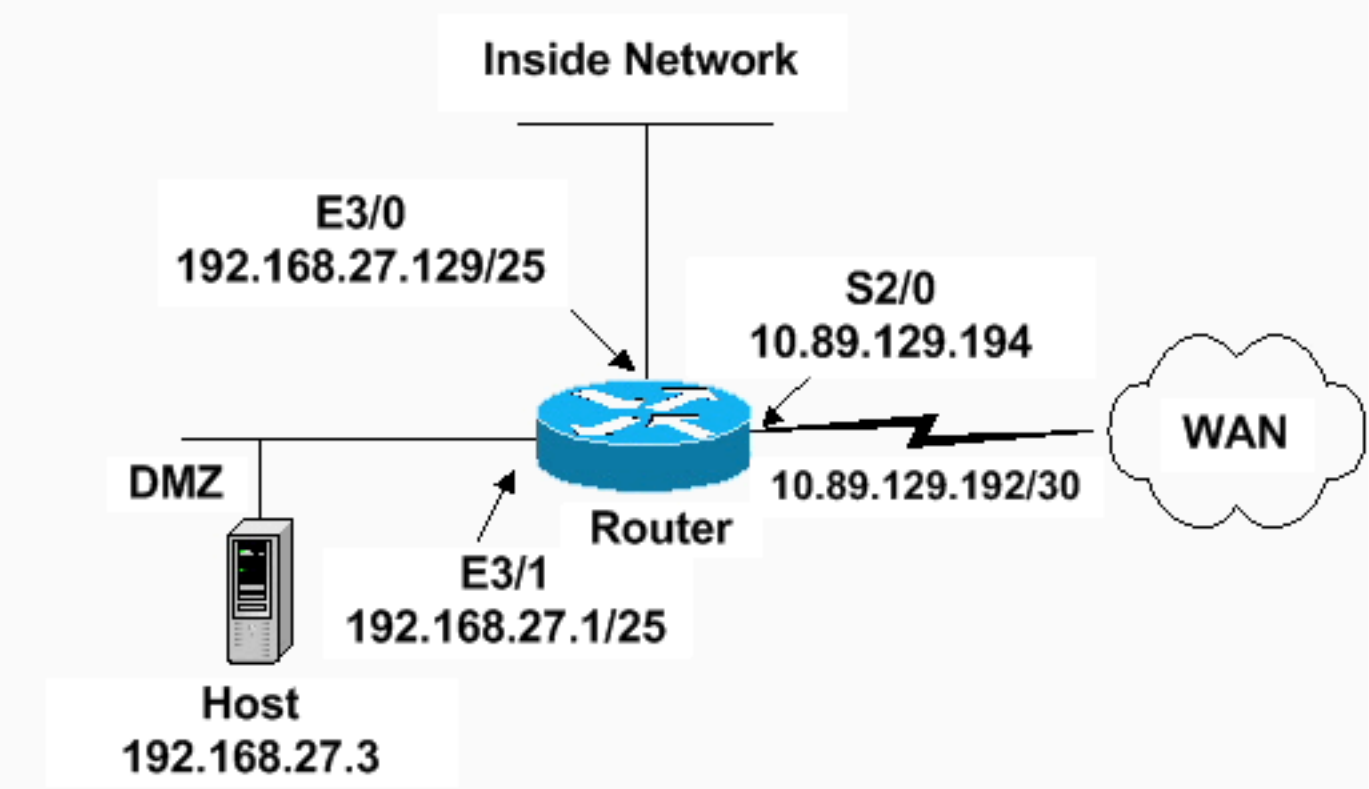
التكوين

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:



التكوينات

يستخدم هذا المستند هذا التكوين.

الموجه VXR 7204

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
logging queue-limit 100
<enable secret 5 <something
!
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect audit-trail
!
Sets the length of time a TCP session !--- is ---!
still managed after no activity. ! ip inspect tcp idle-
time 14400
!
Sets the length of time a UDP session !--- is still ---!
managed after no activity. ! ip inspect udp idle-time
1800
!
Sets the length of time a DNS name lookup session ---!
!--- is still managed after no activity. ! ip inspect
dns-timeout 7
!
Sets up inspection list "standard" !--- to be used ---!
for inspection of inbound Ethernet 0 !--- and inbound
```

```
 serial (applied to both interfaces). ! ip inspect name
                                                standard cuseeme
                                      ip inspect name standard ftp
                                     ip inspect name standard h323
                                     ip inspect name standard http
                                     ip inspect name standard rcmd
                                ip inspect name standard realaudio
                                     ip inspect name standard smtp
                                  ip inspect name standard sqlnet
                               ip inspect name standard streamworks
                                     ip inspect name standard tcp
                                    ip inspect name standard tftp
                                     ip inspect name standard udp
                                  ip inspect name standard vdolive
                                               ip audit notify log
                                      ip audit po max-events 100
                                                                !
                                           no voice hpi capture buffer
                                     no voice hpi capture destination
                                                                !
                                     mta receive maximum-recipients 0
                                                                !



                                                 interface ethernet 3/0
                                   ip address 192.168.27.129 255.255.255.128
                                                                !
 Apply the access list to allow all legitimate !--- ---!
 traffic from the inside network and prevent spoofing. !
                                               ip access-group 101 in
                                                                !
Apply inspection list "standard" for inspection !-- ---!
- of inbound Ethernet traffic. This inspection opens !--
   - temporary entries on access lists 111 and 121. ! ip
                                                 inspect standard in
                                                         duplex full

                                                 interface ethernet 3/1
                                    ip address 192.168.27.1 255.255.255.128


                                                                !
Apply the access list to permit DMZ traffic (except ---!
 spoofing) !--- on the DMZ interface inbound. The DMZ is
     not permitted to initiate !--- any outbound traffic
   except Internet Control Message Protocol (ICMP). ! ip
                                                 access-group 111 in
                                                                !
 Apply inspection list "standard" for inspection of ---!
      outbound !--- traffic from e1. This adds temporary
entries on access list 111 !--- to allow return traffic,
and protects servers in DMZ from !--- distributed denial
      of service (DDoS) attacks. ip inspect standard out
                                                         duplex full
                                                                !
                                                   interface serial 2/0
                                    ip address 10.89.129.194 255.255.255.252
 Apply the access list to allow legitimate traffic. ---!
                                               ! ip access-group 121 in
                                                 serial restart_delay 0
                                                                !
                                                       ip classless
                                                  no ip http-server

A syslog server is located at this address. logging ---!
```

```
192.168.27.131 !--- This command enables the logging of
   session !--- information (addresses and bytes). !---
   Access list 20 is used to control which !--- network
 management stations can access via SNMP. ! access-list
                                  20 permit 192.168.27.5
                                                       !
 Use an access list to allow all legitimate traffic ---!
  from !--- the inside network and prevent spoofing. The
  inside !--- network can only connect to the Telnet and
  POP3 !--- service of 192.168.27.3 on DMZ, and can ping
 (ICMP) to the DMZ. !--- Additional entries can be added
to permit SMTP, WWW, and !--- so forth, if necessary. In
   addition, the inside network can !--- connect to any
   service on the Internet. ! access-list 101 permit tcp
     192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3
access-list 101 permit tcp 192.168.27.128 0.0.0.127 host
                                  192.168.27.3 eq telnet
   access-list 101 permit icmp 192.168.27.128 0.0.0.127
                                  192.168.27.0 0.0.0.127
       access-list 101 deny ip 192.168.27.128 0.0.0.127
                                  192.168.27.0 0.0.0.127
 access-list 101 permit ip 192.168.27.128 0.0.0.127 any
                        access-list 101 deny ip any any
                                                       !
                                                       !
  The access list permits ping (ICMP) from the DMZ ---!
    and denies all !--- traffic initiated from the DMZ.
Inspection opens !--- temporary entries to this list. !
 access-list 111 permit icmp 192.168.27.0 0.0.0.127 any
                        access-list 111 deny ip any any
                                                       !
                                                       !
                                                       !
  Access list 121 allows anyone on the Internet to ---!
connect to !--- WWW, FTP, DNS, and SMTP services on the
DMZ host. It also !--- allows some ICMP traffic. access-
    list 121 permit udp any host 192.168.27.3 eq domain
    access-list 121 permit tcp any host 192.168.27.3 eq
                                                  domain
 access-list 121 permit tcp any host 192.168.27.3 eq www
 access-list 121 permit tcp any host 192.168.27.3 eq ftp
access-list 121 permit tcp any host 192.168.27.3 eq smtp
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                            administratively-prohibited
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                                                  echo
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                                             echo-reply
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                                           packet-too-big
  access-list 121 permit icmp any 192.169.27.0 0.0.0.255
                                           time-exceeded
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                                             traceroute
  access-list 121 permit icmp any 192.168.27.0 0.0.0.255
                                            unreachable
                        access-list 121 deny ip any any

                                                       !
   Apply access list 20 for SNMP process. ! snmp- ---!
 server community secret RO 20 snmp-server enable traps
 tty ! call rsvp-sync ! mgcp profile default ! dial-peer
    cor custom ! gatekeeper shutdown ! 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

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** .

- **show access-list**—يتحقق من التكوين الصحيح لقوائم الوصول التي تم تكوينها في running-configuration.

```
Router#show access-list
Standard IP access list 20
    permit 192.168.27.5 10
Extended IP access list 101
    permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3 10
    permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq telnet 20
    permit icmp 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 30
    deny ip 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 40
    permit ip 192.168.27.128 0.0.0.127 any 50
    deny ip any any 60
Extended IP access list 111
    permit icmp 192.168.27.0 0.0.0.127 any 10
    (deny ip any any (9 matches 20
Extended IP access list 121
    permit udp any host 192.168.27.3 eq domain 10
    permit tcp any host 192.168.27.3 eq domain 20
    permit tcp any host 192.168.27.3 eq www 30
    permit tcp any host 192.168.27.3 eq ftp 40
    permit tcp any host 192.168.27.3 eq smtp 50
    permit icmp any 192.168.27.0 0.0.0.255 administratively-prohibited 60
    permit icmp any 192.168.27.0 0.0.0.255 echo 70
    permit icmp any 192.168.27.0 0.0.0.255 echo-reply 80
    permit icmp any 192.168.27.0 0.0.0.255 packet-too-big 90
    permit icmp any 192.169.27.0 0.0.0.255 time-exceeded 100
    permit icmp any 192.168.27.0 0.0.0.255 traceroute 110
    permit icmp any 192.168.27.0 0.0.0.255 unreachable 120
    (deny ip any any (4866 matches 130
#Router
```

- **show ip audit all**—للتحقق من تكوين أوامر التسجيل.

```
Router#show ip audit all
Event notification through syslog is enabled
Event notification through Net Director is disabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 250
PostOffice:HostID:0 OrgID:0 Msg dropped:0
Curr Event Buf Size:0 Configured:100:
Post Office is not enabled - No connections are active

#Router
```

- **show ip inspection all**—يتحقق من تكوين قواعد فحص جدار حماية Cisco IOS لكل واجهة.

```
Router#show ip inspect all
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
[max-incomplete sessions thresholds are [400:500
.max-incomplete tcp connections per host is 50. Block-time 0 minute
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 14400 sec -- udp idle-time is 1800 sec
```

```
                                                dns-timeout is 7 sec
                                            Inspection Rule Configuration
                                                Inspection name standard
                                    cuseeme alert is on audit-trail is on timeout 14400
                                        ftp alert is on audit-trail is on timeout 14400
                                       h323 alert is on audit-trail is on timeout 14400
                                       http alert is on audit-trail is on timeout 14400
                                       rcmd alert is on audit-trail is on timeout 14400
                                  realaudio alert is on audit-trail is on timeout 14400
                                       smtp alert is on audit-trail is on timeout 14400
                                     sqlnet alert is on audit-trail is on timeout 14400
                                streamworks alert is on audit-trail is on timeout 1800
                                      tcp alert is on audit-trail is on timeout 14400
                                      tftp alert is on audit-trail is on timeout 1800
                                       udp alert is on audit-trail is on timeout 1800
                                  vdolive alert is on audit-trail is on timeout 14400
                                                    Interface Configuration
                                                Interface Ethernet3/0
                                        Inbound inspection rule is standard
                                  cuseeme alert is on audit-trail is on timeout 14400
                                      ftp alert is on audit-trail is on timeout 14400
                                     h323 alert is on audit-trail is on timeout 14400
                                     http alert is on audit-trail is on timeout 14400
                                     rcmd alert is on audit-trail is on timeout 14400
                               realaudio alert is on audit-trail is on timeout 14400
                                     smtp alert is on audit-trail is on timeout 14400
                                   sqlnet alert is on audit-trail is on timeout 14400
                              streamworks alert is on audit-trail is on timeout 1800
                                     tcp alert is on audit-trail is on timeout 14400
                                     tftp alert is on audit-trail is on timeout 1800
                                      udp alert is on audit-trail is on timeout 1800
                                  vdolive alert is on audit-trail is on timeout 14400
                                        Outgoing inspection rule is not set
                                                Inbound access list is 101
                                            Outgoing access list is not set
                                                Interface Ethernet3/1
                                         Inbound inspection rule is not set
                                       Outgoing inspection rule is standard
                                  cuseeme alert is on audit-trail is on timeout 14400
                                      ftp alert is on audit-trail is on timeout 14400
                                     h323 alert is on audit-trail is on timeout 14400
                                     http alert is on audit-trail is on timeout 14400
                                     rcmd alert is on audit-trail is on timeout 14400
                               realaudio alert is on audit-trail is on timeout 14400
                                     smtp alert is on audit-trail is on timeout 14400
                                   sqlnet alert is on audit-trail is on timeout 14400
                              streamworks alert is on audit-trail is on timeout 1800
                                     tcp alert is on audit-trail is on timeout 14400
                                     tftp alert is on audit-trail is on timeout 1800
                                      udp alert is on audit-trail is on timeout 1800
                                  vdolive alert is on audit-trail is on timeout 14400
                                                Inbound access list is 111
                                            Outgoing access list is not set
                                                                        #Router
```

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 التكوين، يتم تطبيق **معيار فحص ip** على واجهة إيثرنت 0/3 ويطبق **خرج معيار فحص ip** على واجهة إيثرنت 1/3.

راجع أستكشاف أخطاء تكوينات جدار حماية Cisco IOS وإصلاحها للحصول على مزيد من المعلومات حول أستكشاف الأخطاء وإصلاحها.

معلومات ذات صلة

- صفحة دعم جدار حماية Cisco 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).