PIX/ASA 7.x والإصدارات الأحدث: Mail (SMTP) Server Access على مثال تكوين الشبكة الخارجية

المحتويات

المقدمة

يوضح هذا التكوين العينة كيفية إعداد جدار حماية PIX للوصول إلى خادم بريد موجود على الشبكة الخارجية.

ارجع إلى PIX/ASA 7.x والإصدارات الأحدث: مثال تكوين الشبكة على وصول خادم البريد من أجل إعداد جهاز أمان PIX/ASA للوصول إلى خادم بريد/SMTP موجود على الشبكة الداخلية.

ارجع إلى PIX/ASA 7.x مع الوصول إلى Mail Server على مثال تكوين الشبكة DMZ لإعداد جهاز أمان PIX/ASA للوصول إلى خادم بريد/SMTP موجود على شبكة DMZ.

ارجع إلى ASA 8.3 والإصدارات الأحدث: مثال وصول خادم البريد (SMTP) إلى تكوين الشبكة الخارجية للحصول على مزيد من المعلومات حول التكوين المتطابق على جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدار 8.3 والإصدارات الأحدث.

ارجع إلى وثائق جدار حماية PIX الآمن من Cisco للحصول على مزيد من المعلومات حول كيفية تعيين Microsoft Exchange. أختر الإصدار البرنامج الخاص بك، ثم انتقل إلى دليل التكوين واقرأ الفصل الخاص بكيفية التكوين ل Microsoft Exchange.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- جدار حماية PIX 535
- برنامج جدار حماية PIX الإصدار 7.1(1)
- الموجهات 2500 من Cisco

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه 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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان القابل للتكيف (ASA) الذي يشغل الإصدار 7.x والإصدارات الأحدث.

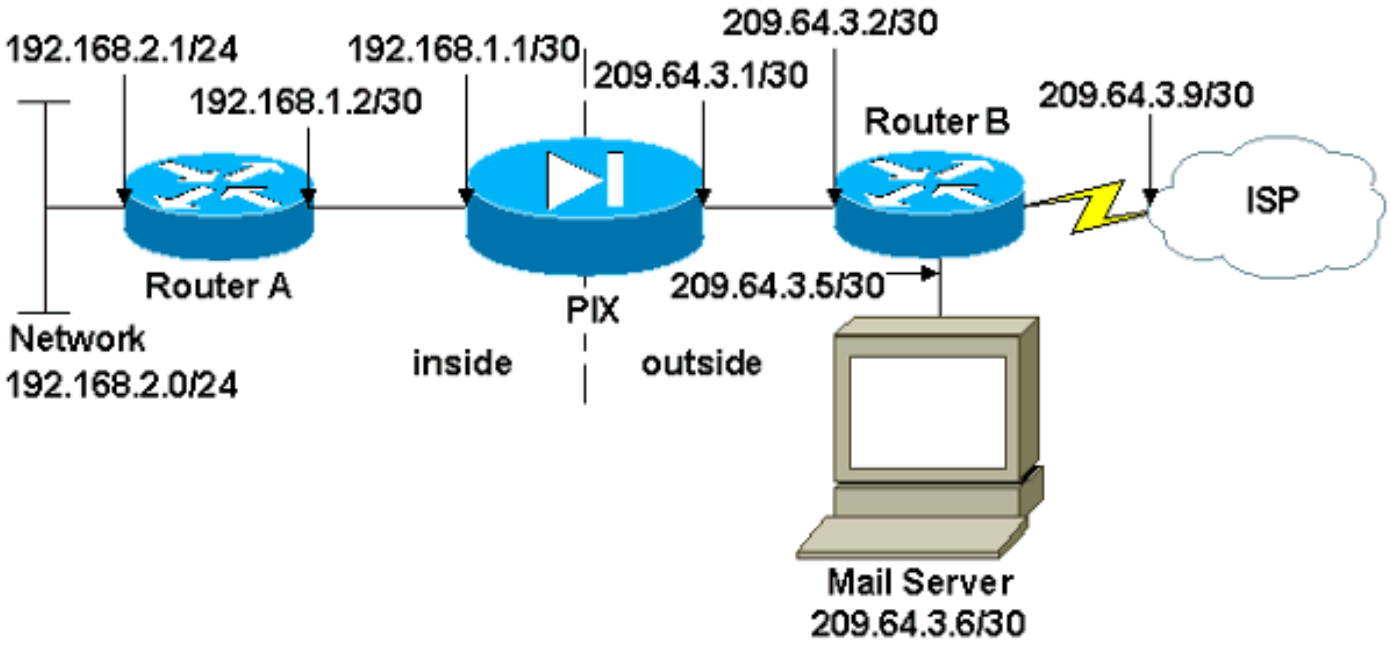
التكوين

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

ملاحظة: أستخدم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- جدار حماية PIX
- الموجه A
- الموجه B

جدار حماية PIX

```
PIX Version 7.1(1)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!

!--- Define the IP address for the inside interface.
interface Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!

!--- Define the IP address for the outside interface.
interface Ethernet4 nameif outside
 security-level 0
 ip address 209.64.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
```

```
!--- This command defines the global for the Network
Address Translation !--- (NAT) statement. In this case,
the two commands state that any traffic !--- from the
192.168.2.x network that passes from the inside
interface (Ethernet0) !--- to the outside interface
(Ethernet 1) translates into an address !--- in the
range of 209.64.3.129 through 209.64.3.253 and contains
a subnet !--- mask of 255.255.255.128. global (outside)
1 209.64.3.129-209.64.3.253 netmask 255.255.255.128

!--- This command reserves the last available address
(209.64.3.254) for !--- for Port Address Translation
(PAT). In the previous statement, !--- each address
inside that requests a connection uses one !--- of the
addresses specified. If all of these addresses are in
use, !--- this statement provides a failsafe to allow
additional inside stations !--- to establish
connections. global (outside) 1 209.64.3.254

!--- This command indicates that all addresses in the
192.168.2.x range !--- that pass from the inside
(Ethernet0) to a corresponding global !--- designation
are done with NAT. !--- As outbound traffic is permitted
by default on the PIX, no !--- static commands are
needed. nat (inside) 1 192.168.2.0 255.255.255.0

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The PIX forwards packets with
these addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1

!--- Sets the default route for the PIX Firewall at
209.64.3.2. route outside 0.0.0.0 0.0.0.0 209.64.3.2 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
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
!
!

!--- SMTP/ESMTP is inspected since "inspect esmtp" is
included in the map. policy-map global_policy class
inspection_default inspect dns maximum-length 512
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
Cryptochecksum:8a63de5ae2643c541a397c2de7901041
: end
```

الجزء A

```
Current configuration:
  !
  version 12.0
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the PIX-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the PIX. ip route 0.0.0.0 0.0.0.0
192.168.1.1
  !
  !
  line con 0
   transport input none
   line aux 0
   autoselect during-login
   line vty 0 4
   exec-timeout 5 0
   password ww
   login
  !
  end
```

الجزء B

```
Current configuration:
  !
  version 12.0
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
```

```
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the PIX-facing Ethernet
interface. ip address 209.64.3.2 255.255.255.252 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the server-facing Ethernet interface. ip
address 209.64.3.5 255.255.255.252 no ip directed-
broadcast ! interface Serial0 !--- Assigns an IP address
to the Internet-facing interface. ip address 209.64.3.9
255.255.255.252 no ip directed-broadcast no ip mroute-
cache ! interface Serial1 no ip address no ip directed-
broadcast ! ip classless !--- All non-local packets are
to be sent out serial 0. In this case, !--- the IP
address on the other end of the serial interface is not
known, !--- or you can specify it here. ip route 0.0.0.0
0.0.0.0 serial 0
  !

!--- This statement is required to direct traffic
destined to the !--- 209.64.3.128 network (the PIX
global pool) to the PIX to be translated !--- back to
the inside addresses. ip route 209.64.3.128
255.255.255.128 209.64.3.1
  !
  !
  line con 0
   transport input none
  line aux 0
   autoselect during-login
  line vty 0 4
   exec-timeout 5 0
   password ww
   login
  !
  end
```

تكوين ESMTP TLS

ملاحظة: إذا كنت تستخدم تشفير أمان طبقة النقل (TLS) لاتصالات البريد الإلكتروني، فإن ميزة فحص ESMTP (التي يتم تمكينها بشكل افتراضي) في PIX تقوم بإسقاط الحزم. للسماح بر سائل البريد الإلكتروني مع تمكين TLS، قم بتعطيل ميزة فحص ESMTP كما يظهر هذا الإخراج.

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit
```

التحقق من الصحة

ال يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) أوامر **show** معينة. أستخدم CLI Analyzer (محلل واجهة سطر الأوامر) لعرض تحليل مخرج الأمر **show**.

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

يوجه أمر **تصحيح أخطاء وحدة تحكم التسجيل** الرسائل إلى وحدة تحكم PIX. إذا كان الاتصال بخادم البريد يمثل مشكلة، فتحقق من رسائل تصحيح أخطاء وحدة التحكم لتحديد موقع عناوين IP الخاصة بمحاولات الإرسال والاستقبال لتحديد المشكلة.

معلومات ذات صلة

- إنشاء إمكانية اتصال من خلال جدران الحماية التي تدعم تقنية PIX من Cisco
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- جدران الحماية من الجيل التالي Cisco ASA 5500-X Series
- 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).