ASA 8.3 والإصدارات الأحدث: وصول خادم البريد (SMTP) على مثال تكوين الشبكة الداخلي

المحتويات

المقدمة

يوضح هذا التكوين النموذجي كيفية إعداد جهاز الأمان ASA للوصول إلى خادم بريد (SMTP) موجود على الشبكة الداخلية.

ارجع إلى ASA 8.3 والإصدارات الأحدث: وصول خادم Mail (SMTP) على مثال تكوين DMZ للحصول على مزيد من المعلومات حول كيفية إعداد جهاز أمان ASA للوصول إلى خادم Mail/SMTP الموجود على شبكة DMZ.

ارجع إلى ASA 8.3 والإصدارات الأحدث: مثال تكوين الشبكة الخارجية الخاص بوصول خادم البريد (SMTP) لإعداد جهاز أمان ASA للوصول إلى خادم البريد/SMTP الموجود على الشبكة الخارجية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- أجهزة الأمان المعدلة (ASA) من Cisco التي تشغل الإصدار 8.3 والإصدارات الأحدث.
- cisco 1841 مسجاح تخدي مع cisco ios® برمجية إطلاق 12.4(20)T

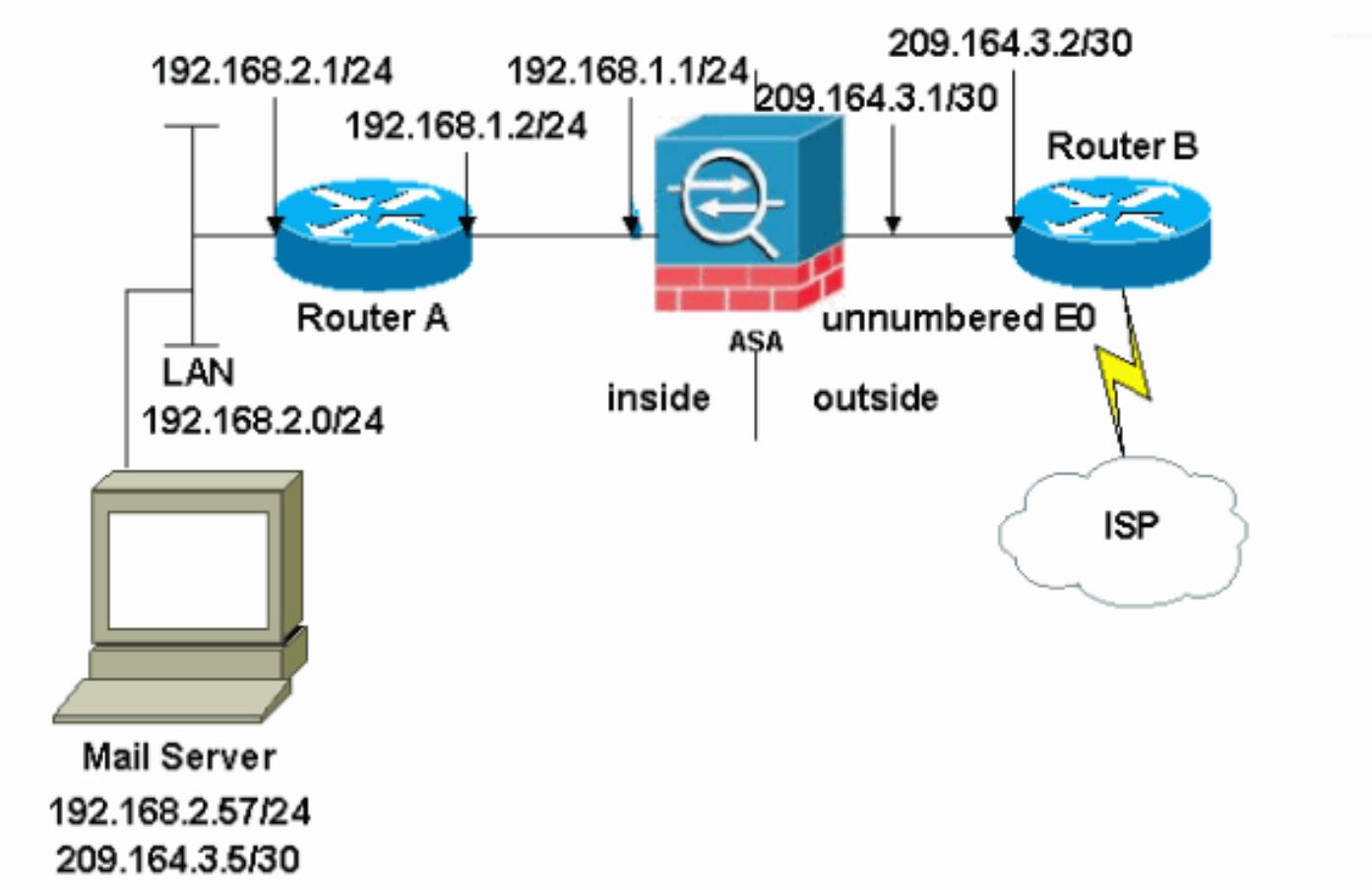
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس خاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

يحتوي إعداد الشبكة المستخدم في هذا المثال على ASA مع الشبكة الداخلية (192.168.1.0/24) والشبكة الخارجية (209.164.3.0/30). يوجد خادم البريد بعنوان IP 209.64.3.5 في الشبكة الداخلية.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- ASA
- الموجه B

ASA

```
ASA#show run
: Saved
:
```

```
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU 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 192.168.1.1 255.255.255.0
!

!--- Define the IP address for the outside interface. interface Ethernet4 nameif outside
 security-level 0
 ip address 209.164.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- Create an access list that permits Simple !--- Mail Transfer Protocol (SMTP) traffic from anywhere
to the host at 209.164.3.5 (our server). The name of this list is !--- smtp. Add additional lines to th
access list as required. !--- Note: There is one and only one access list allowed per !--- interface pe
direction, for example, inbound on the outside interface. !--- Because of limitation, any additional li
that need placement in !--- the access list need to be specified here. If the server !--- in question i
SMTP, replace the occurrences of SMTP with !--- www, DNS, POP3, or whatever else is required.


access-list smtp extended permit tcp any host 209.164.3.5 eq smtp

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- Specify that any traffic that originates inside from the !--- 192.168.2.x network NATs (PAT) to
209.164.3.129 if !--- such traffic passes through the outside interface. object network obj-192.168.2.0
  subnet 192.168.2.0 255.255.255.0
```

```
  nat (inside,outside) dynamic 209.164.3.129

!--- Define a static translation between 192.168.2.57 on the inside and !--- 209.164.3.5 on the outside
These are the addresses to be used by !--- the server located inside the ASA. object network obj-192.16
  host 192.168.2.57
  nat (inside,outside) static 209.164.3.5

!--- Apply the access list named smtp inbound on the outside interface. access-group smtp in interface
outside

!--- Instruct the ASA to hand any traffic destined for 192.168.x.x !--- to the router at 192.168.1.2. r
inside 192.168.0.0 255.255.0.0 192.168.1.2 1

!--- Set the default route to 209.164.3.2. !--- The ASA assumes that this address is a router address.
outside 0.0.0.0 0.0.0.0 209.164.3.2 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 as "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 inspec
netbios inspect rsh inspect rtsp inspect skinny inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!

!--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map. service-policy global_policy gl
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

الموجه B

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname 2522-R5
 !
 enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
 !
 ip subnet-zero
 !
 !
 !
 !
 !
 interface Ethernet0
```

```
!--- Sets the IP address of the Ethernet interface to 209.164.3.2. ip address 209.164.3.2 255.255.255.2
interface Serial0 !--- Instructs the serial interface to use !--- the address of the Ethernet interface
the need arises. ip unnumbered ethernet 0 ! interface Serial1 no ip address no ip directed-broadcast !
classless !--- Instructs the router to send all traffic !--- destined for 209.164.3.x to 209.164.3.1. ip
route 209.164.3.0 255.255.255.0 209.164.3.1

!--- Instructs the router to send !--- all other remote traffic out serial 0. ip route 0.0.0.0 0.0.0.0
0
 !
 !
 line con 0
  transport input none
 line aux 0
  autoselect during-login
 line vty 0 4
  exec-timeout 5 0
  password ww
  login
 !
 end
```

ملاحظة: ال تتم إضافة الموجه A. أنت فقط تحتاج أن يعطي العنوان على القارن وعينت التقصير مدخل إلى 192.168.1.1، أي يكون القارن داخلي من ال ASA .

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 ASA تقوم بإسقاط الحزم. للسماح برسائل البريد الإلكتروني مع تمكين TLS، قم بتعطيل ميزة فحص ESMTP كما يظهر هذا الإخراج. راجع معرف تصحيح الأخطاء من Cisco CSCtn08326 للحصول على مزيد من المعلومات.

```
ciscoasa(config)#
policy-map global_policy

ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

ملاحظة: في الإصدار 8.0.3 من ASA والإصدارات الأحدث، يتوفر الأمر **allow-tls** للسماح ببريد TLS الإلكتروني مع تمكين فحص esmtp كما هو موضح:

```
policy-map type inspect esmtp tls-esmtp
parameters
allow-tls
inspect esmtp tls-esmtp
```

التحقق من الصحة

ال يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوجه الأمر logging buffered 7 الرسائل إلى وحدة تحكم ASA. إذا كان الاتصال بخادم البريد يمثل مشكلة، فتحقق من رسائل تصحيح أخطاء وحدة التحكم لتحديد موقع عناوين IP الخاصة بمحطات الإرسال والاستقبال لتحديد المشكلة.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- 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).