Mail مداخ لوصو :ثدحألا تارادصإلاو ASA 8.3 DMZ نيوكت لاثم ىلع (SMTP)

المحتويات

المقدمة

يوضح هذا التكوين النموذجي كيفية إعداد جهاز الأمان ASA للوصول إلى خادم بروتوكول نقل البريد البسيط (SMTP) الموجود على شبكة المنطقة المجردة من السلاح (DMZ).

ارجع إلى ASA 8.3 والإصدارات الأحدث: مثال الوصول إلى خادم البريد (SMTP) على تكوين الشبكة الداخلية للحصول على مزيد من المعلومات حول كيفية إعداد جهاز أمان ASA للوصول إلى خادم البريد/SMTP الموجود على الشبكة الداخلية.

ارجع إلى ASA 8.3 والإصدارات الأحدث: مثال الوصول إلى خادم البريد (SMTP) على تكوين الشبكة الخارجية للحصول على مزيد من المعلومات حول كيفية إعداد جهاز أمان ASA للوصول إلى خادم البريد/SMTP الموجود على الشبكة الخارجية.

ارجع إلى PIX/ASA 7.x وأعلى: وصول خادم Mail (SMTP) على مثال تكوين DMZ للحصول على تكوين مطابق على جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدارات 8.2 والإصدارات الأقدم.

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 مسحاج تخديد مع cisco ios® برمجية إطلاق T(20)12.4

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.

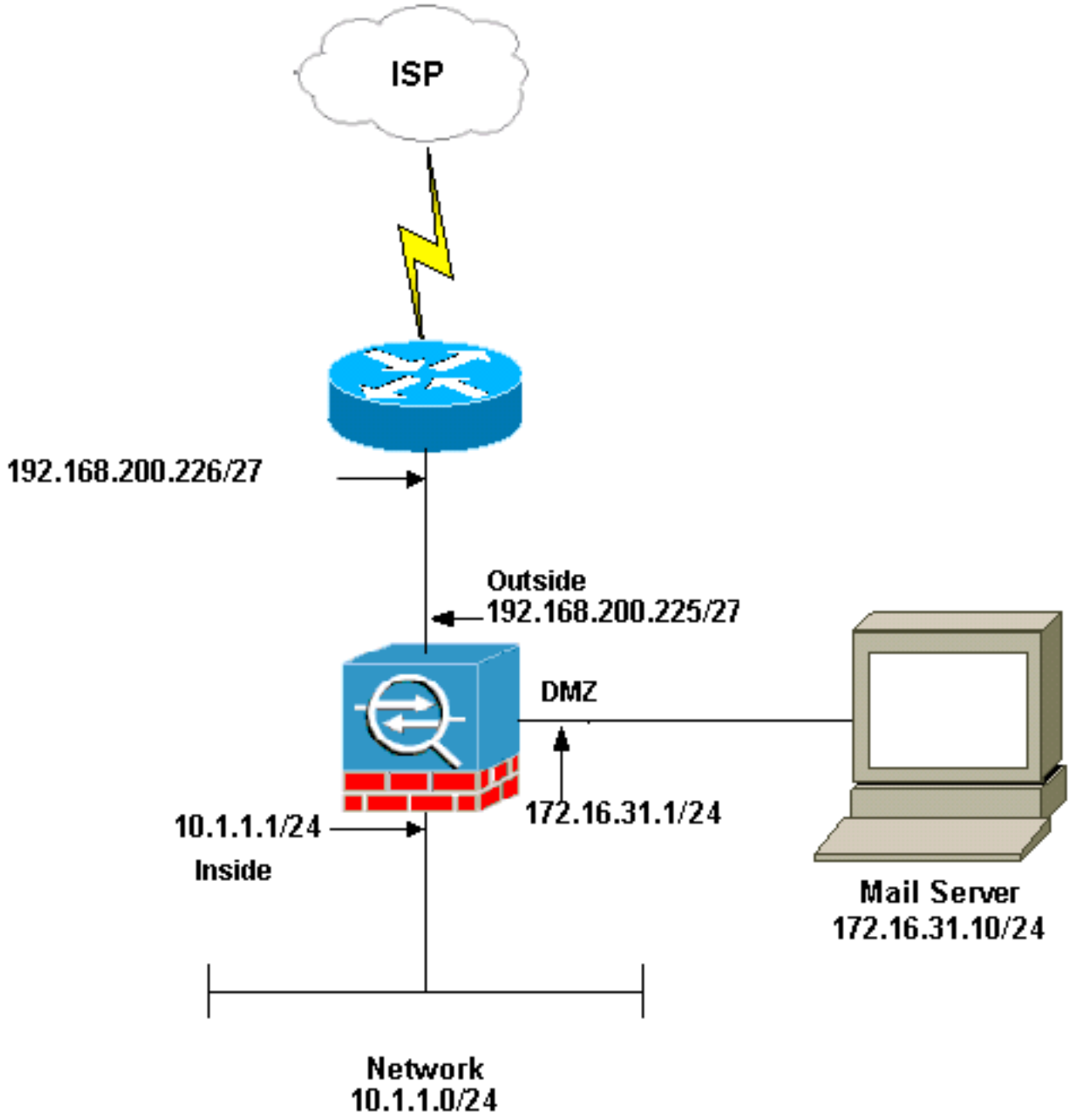
التكوين

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:



ملاحظة: ال ip ليس يخاطب 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 (24/10.1.1.0) والشبكة الخارجية (27/192.168.200.0). يوجد خادم البريد بعنوان IP 172.16.31.10 في شبكة المنطقة المجردة من السلاح (DMZ). لكي يتم الوصول إلى MailServer من الداخل، يقوم المستخدمون بتكوين NAT للهوية. قم بتكوين قائمة وصول، وهي **dmz_int** في هذا المثال، للسماح باتصالات SMTP الصادرة من خادم البريد إلى الأجهزة المضيفة في الشبكة الداخلية وربطها بواجهة DMZ.

بالمثل للمستخدمين الخارجيين أن ينفذ ال MailServer يشكل NAT ساكن إستاتيكي وأيضا قائمة وصول، أي **خارج_int** في هذا مثال، in order to سمحت للمستخدمين الخارجيين أن ينفذ ال MailServer وربط هذا قائمة الوصول إلى القارن خارجي.

تكوين ASA

يستعمل هذا وثيقة هذا تشكيل:

تكوين 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
security-level 0
no ip address
!
interface Ethernet1
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet2
no nameif
no security-level
no ip address
!
Configure the inside interface. interface Ethernet3 ---!
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host  192.168.200.227 eq smtp
Allows outgoing SMTP connections. !--- This access ---!
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

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


object network obj-192.168.200.228-192.168.200.253
range 192.168.200.228-192.168.200.253
object network obj-192.168.200.254
host 192.168.200.254

object-group network nat-pat-group
network-object object obj-192.168.200.228-
```

```
192.168.200.253
network-object object obj-192.168.200.254

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic nat-pat-group

This network static does not use address ---!
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
nat (inside,dmz) static obj-10.1.1.0

This network static uses address translation. !--- ---!
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
host 172.16.31.10
nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0  192.168.200.226 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
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
The inspect esmtp command (included in the map) ---!
.allows !--- SMTP/ESMTP to inspect the application


policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
The inspect esmtp command (included in the map) ---!
.allows !--- SMTP/ESMTP to inspect the application

service-policy global_policy global
```

```
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
end :
[OK]
```

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 (العملاء المسجلون فقط) 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
```

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.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- debug icmp trace — يعرض ما إذا كانت طلبات بروتوكول رسائل التحكم في الإنترنت (ICMP) من الأجهزة المضيفة تصل إلى ASA. تحتاج إلى إضافة الأمر **access-list** للسماح ب ICMP في التكوين الخاص بك لتشغيل تصحيح الأخطاء هذا.**ملاحظة:** لاستخدام تصحيح الأخطاء هذا، تأكد من السماح ب ICMP في int_ كما يوضح هذا الإخراج:

```
access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
access-list outside_int extended permit icmp any any
```

- التسجيل المخزن مؤقتا 7 — يستخدم في وضع التكوين العام لتمكين جهاز الأمان القابل للتكيف لإرسال رسائل syslog إلى المخزن المؤقت للسجل. يمكن رؤية محتويات المخزن المؤقت لسجل ASA باستخدام الأمر show logging .

راجع تكوين syslog باستخدام ASDM للحصول على مزيد من المعلومات حول كيفية إعداد التسجيل.

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).