ASA 8.3 e versioni successive: Esempio di configurazione dell'accesso al server di posta (SMTP) in una rete interna

Sommario

Introduzione

In questa configurazione di esempio viene mostrato come configurare l'appliance ASA Security per accedere a un server di posta (SMTP) situato nella rete interna.

Fare riferimento alla versione ASA 8.3 e successive: Accesso al server di posta (SMTP) sull'esempio di configurazione della DMZ per ulteriori informazioni su come configurare l'appliance di sicurezza ASA per l'accesso a un server di posta/SMTP situato sulla rete DMZ.

Fare riferimento alla versione ASA 8.3 e successive: Esempio di configurazione dell'accesso al server di posta (SMTP) sulla rete esterna per configurare l'appliance di sicurezza ASA per l'accesso a un server di posta/SMTP sulla rete esterna.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance (ASA) con versione 8.3 e successive.
- Cisco 1841 Router con software Cisco IOS® versione 12.4(20)T

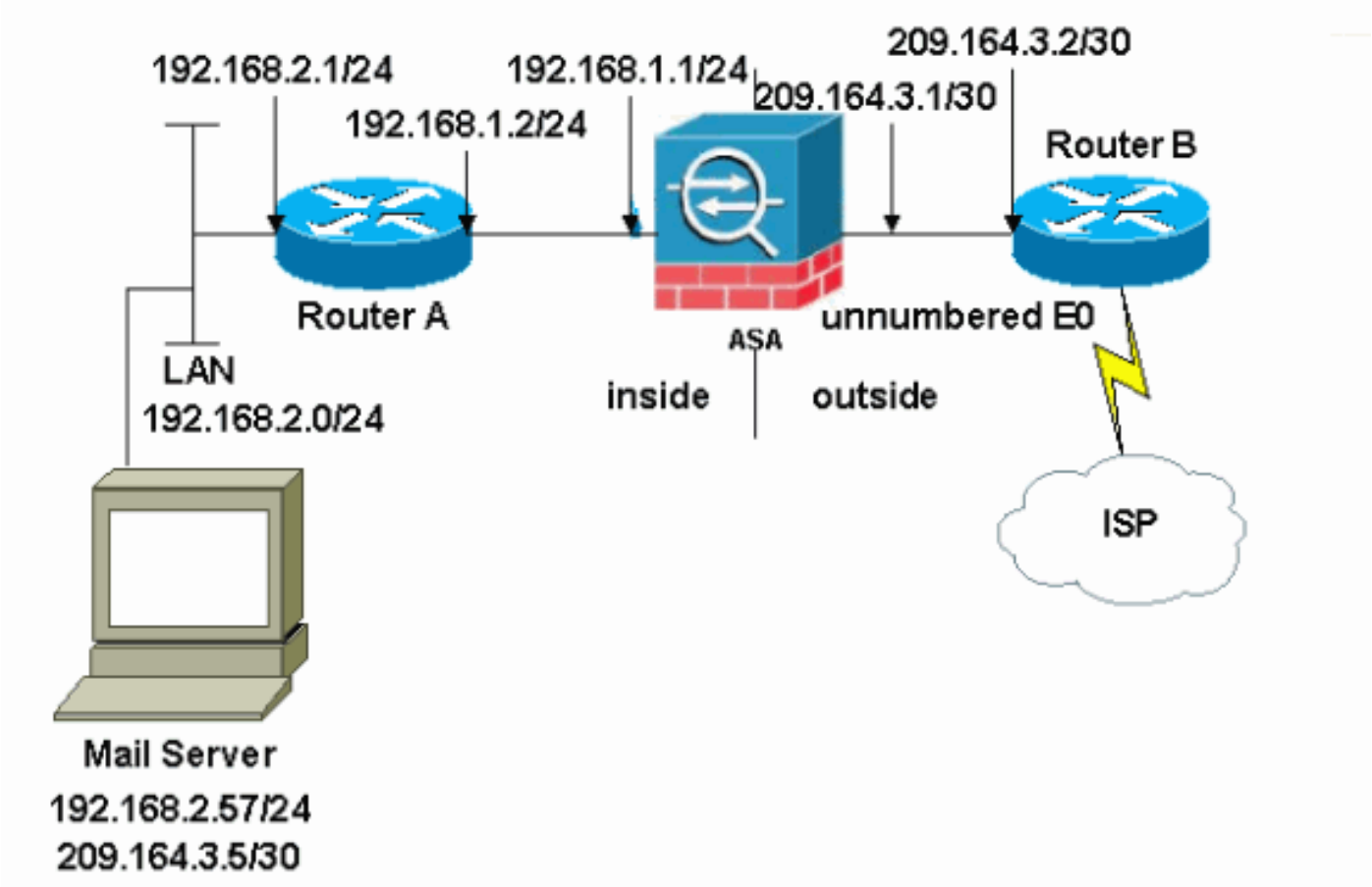
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

La configurazione della rete usata in questo esempio ha l'ASA con la rete interna (192.168.1.0/24) e la rete esterna (209.164.3.0/30). Il server di posta con indirizzo IP 209.64.3.5 si trova nella rete interna.

Configurazioni

Nel documento vengono usate queste configurazioni:

- ASA

- Router 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
```

Router 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
```

Nota: la configurazione del router A non è stata aggiunta. È sufficiente assegnare gli indirizzi IP sulle interfacce e impostare il gateway predefinito su 192.168.1.1, ossia l'interfaccia interna dell'ASA.

Configurazione TLS ESMTP

Nota: se si usa la crittografia Transport Layer Security (TLS) per la comunicazione della posta elettronica, la funzione di ispezione ESMTP (abilitata per impostazione predefinita) nell'appliance ASA scarta i pacchetti. Per consentire i messaggi di posta elettronica con TLS abilitato, disabilitare la funzione di ispezione ESMTP come mostrato nell'output. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtn08326.

```
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
```

Nota: in ASA versione 8.0.3 e successive, il comando **allow-tls** è disponibile per consentire la posta elettronica TLS con esmtp di ispezione abilitato, come mostrato:

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

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Il comando **logging buffered 7** indirizza i messaggi alla console ASA. Se la connettività al server di posta rappresenta un problema, esaminare i messaggi di debug della console per individuare gli indirizzi IP delle stazioni di invio e di ricezione e determinare il problema.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems