ASA 8.3 y posterior: Ejemplo de Configuración de Acceso de Servidor de Correo (SMTP) en Red Interna

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Configuraciones
Configuración de ESMTP TLS
Verificación
Troubleshoot
Información Relacionada

Introducción

Esta configuración de muestra demuestra cómo configurar el Dispositivo de Seguridad ASA para el acceso a un servidor de correo (S TP) ubicado en la red interna.

Consulte ASA 8.3 y posteriores: Acceso al servidor de correo (SMTP) en el ejemplo de configuración de DMZ para obtener más información sobre cómo configurar el dispositivo de seguridad ASA para acceder a un servidor de correo/SMTP ubicado en la red DMZ.

Consulte ASA 8.3 y posteriores: Ejemplo de Configuración de Correo (SMTP) Server Access on Outside Network para configurar el dispositivo de seguridad ASA para acceder a un servidor de correo/SMTP ubicado en la red externa.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adaptive Security Appliance (ASA) que ejecuta la versión 8.3 y posteriores.
- Router Cisco 1841 con software Cisco IOS® versión 12.4(20)T

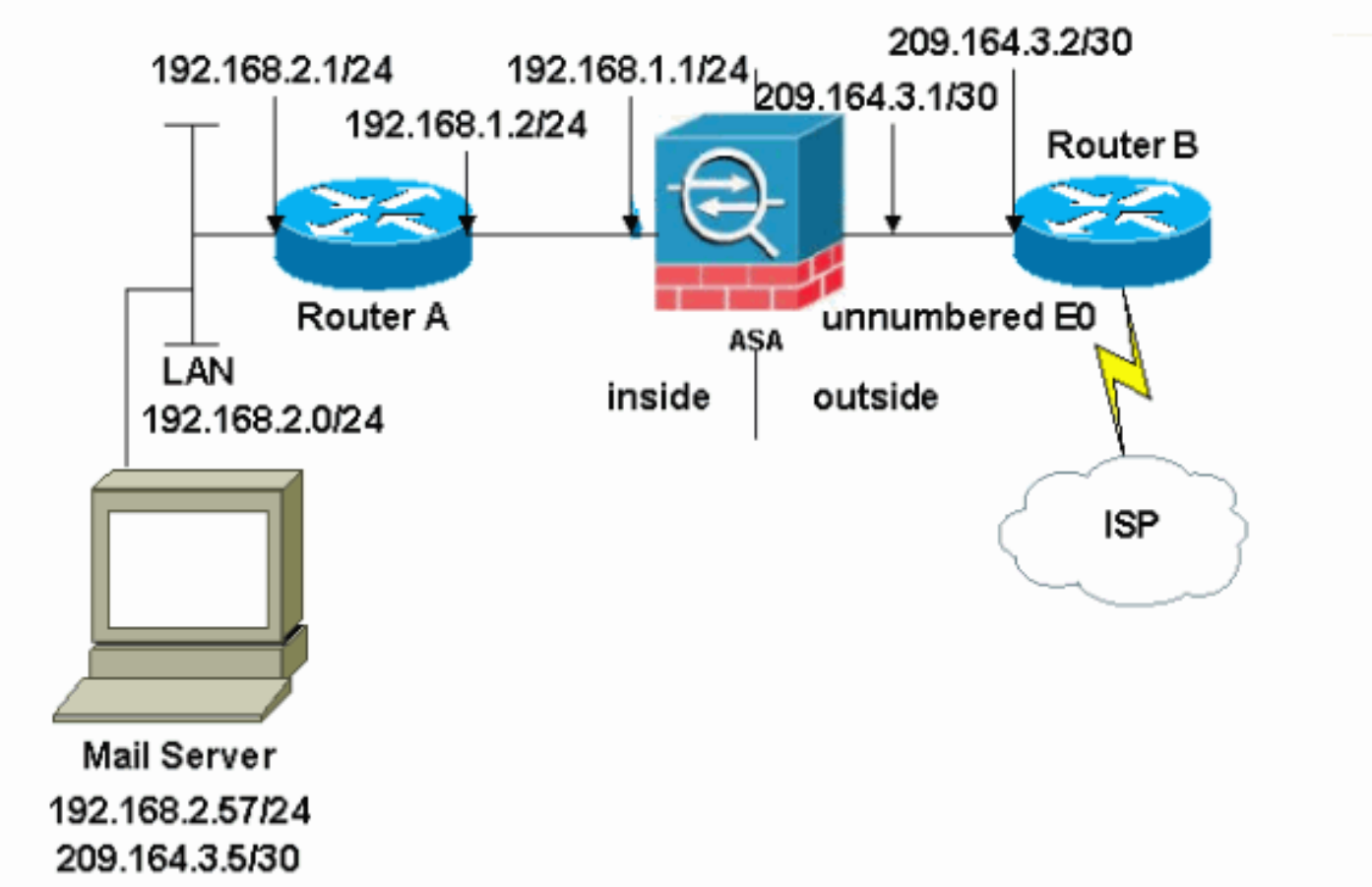
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

La configuración de red utilizada en este ejemplo tiene el ASA con la red interna (192.168.1.0/24) y la red externa (209.164.3.0/30). El servidor de correo con la dirección IP 209.64.3.5 se encuentra en la red interna.

Configuraciones

En este documento, se utilizan estas configuraciones:

- 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. i
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: No se agrega la configuración del router A. Sólo tiene que dar las direcciones IP en las interfaces y establecer el gateway predeterminado en 192.168.1.1, que es la interfaz interna del ASA .

Configuración de ESMTP TLS

Nota: Si utiliza el cifrado de seguridad de la capa de transporte (TLS) para la comunicación por correo electrónico, la función de inspección de ESMTP (activada de forma predeterminada) en el ASA descarta los paquetes. Para permitir los correos electrónicos con TLS habilitado, inhabilite la función de inspección ESMTP como muestra este resultado. Consulte Cisco bug ID CSCtn08326 para obtener más información.

```
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: En ASA versión 8.0.3 y posteriores, el comando **allow-tls** está disponible para permitir el correo electrónico TLS con el comando inspect esmtp habilitado como se muestra:

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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

El comando **logging buffered 7** dirige mensajes a la consola ASA. Si la conectividad con el servidor de correo es un problema, examine los mensajes de depuración de la consola para localizar las direcciones IP de las estaciones de envío y recepción para determinar el problema.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems