ASA 8.3 y posterior: Acceso al servidor del correo (S TP) en el ejemplo de configuración de la red interna

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Configurar
Diagrama de la red
Configuraciones
Configuración ESMTP TLS
Verificación
Troubleshooting
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.

Refiera a ASA 8.3 y posterior: Envíe el acceso al servidor (S TP) en el ejemplo de la configuración de DMZ para más información sobre cómo configurar el dispositivo de seguridad ASA para el acceso a un servidor mail/SMTP situado en la red DMZ.

Refiera a ASA 8.3 y posterior: Envíe el acceso al servidor (S TP) en la configuración de red externa Exampleto configura el dispositivo de seguridad ASA para el acceso a un servidor mail/SMTP situado en la red externa.

Refiera al PIX/ASA 7.x y posterior: Envíe el acceso al servidor (S TP) en el ejemplo de configuración de la red interna para más información de la configuración idéntica en el dispositivo de seguridad adaptante de Cisco (ASA) con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

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.

- El dispositivo de seguridad adaptante de Cisco (ASA) ese funciona con la versión 8.3 y posterior.
- Cisco 1841 Router con la versión 12.4(20)T del Cisco IOS ® Software

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

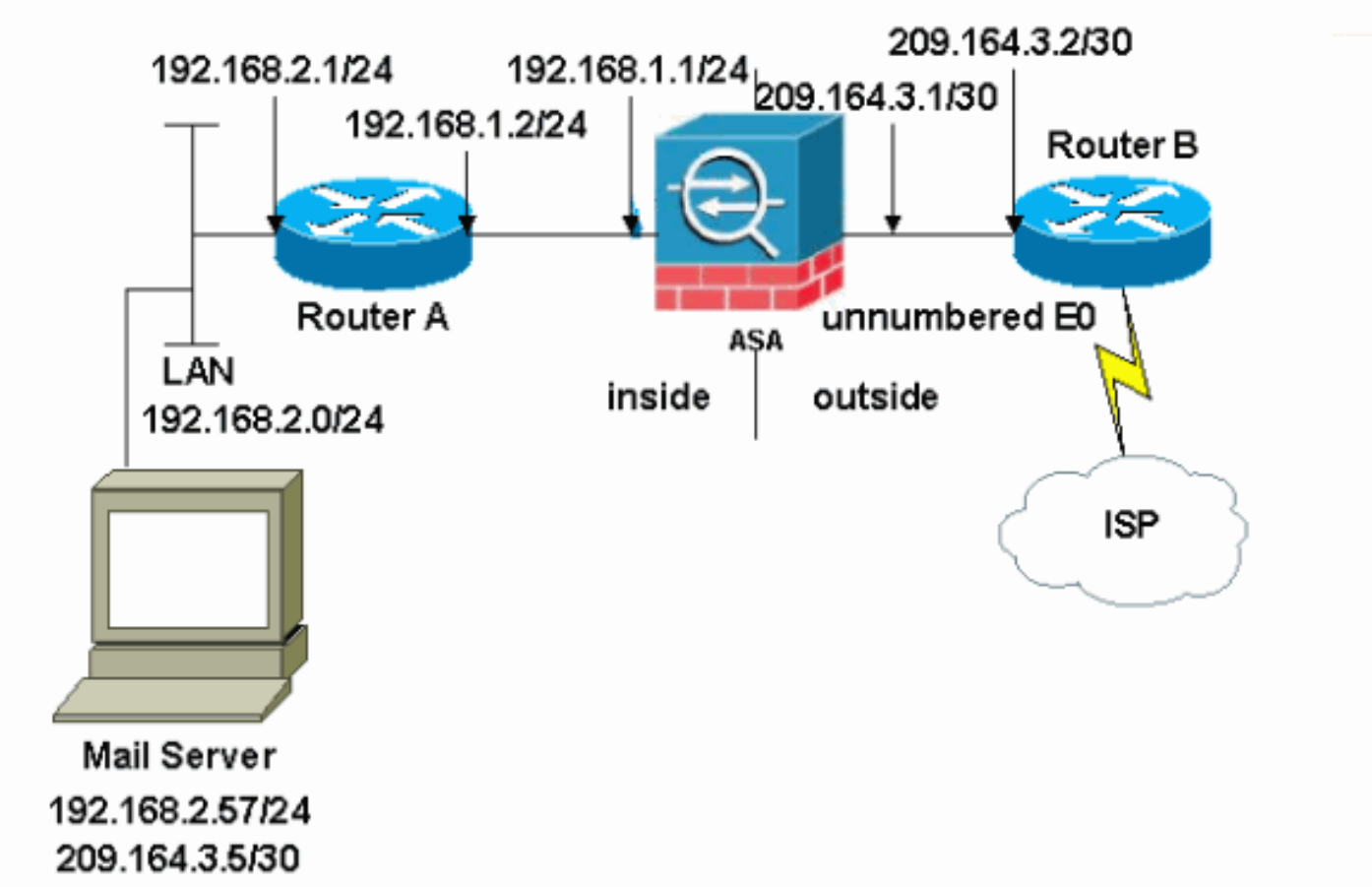
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados 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 la red usada 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 mail server con la dirección IP 209.64.3.5 está situado 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 this access list as required. !--- Note: There is one and only one access list allowed per !--- interface per direction, for example, inbound on the outside interface. !--- Because of limitation, any additional lines that need placement in !--- the access list need to be specified here. If the server !--- in question is not 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-192.168.2.57 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. route 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. route 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 inspect 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 global 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 209.164.3.2 255.255.255.252 !
interface Serial0 !--- Instructs the serial interface to
use !--- the address of the Ethernet interface when the
need arises. ip unnumbered ethernet 0 ! interface
Serial1 no ip address no ip directed-broadcast ! ip
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 serial 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 configuración del router A no se agrega. Usted tiene que dar solamente los IP Addresses en las interfaces y fijar el default gateway a 192.168.1.1, que es la interfaz interior del ASA.

Configuración ESMTP TLS

Nota: Si usted utiliza el cifrado de Transport Layer Security (TLS) para la comunicación del email entonces la característica del La inspección ESMTP (habilitada por abandono) en el ASA cae los paquetes. Para permitir los email con TLS habilitó, inhabilita la característica del La inspección ESMTP como esta salida muestra. Refiera al Id. de bug Cisco CSCtn08326 (clientes registrados solamente) para 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 la Versión de ASA 8.0.3 y posterior, el comando de permitir-**TLS** está disponible permitir el correo electrónico de TLS con examina el 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.

Troubleshooting

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

El registro mitigó 7 que el comando dirige los mensajes a la consola ASA. Si la Conectividad al mail server es un problema, examine los mensajes del debug de la consola para localizar los IP Addresses del envío y de las estaciones receptoras para determinar el problema.

Información Relacionada

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