

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de ESMTP TLS](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Esta configuración de ejemplo proporciona información sobre cómo configurar el dispositivo de seguridad adaptable (ASA) para el acceso a un servidor de correo ubicado en la red externa.

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 Mail \(SMTP\) Server Access on Inside Network](#) para configurar ASA Security Appliance para acceder a un servidor de correo/SMTP ubicado en la red interna.

Consulte [PIX/ASA 7.x y versiones posteriores : Ejemplo de Configuración de Mail Server Access on Outside Network \(SMTP\)](#) para la configuración idéntica en Cisco Adaptive Security Appliance (ASA) con las versiones 8.2 y anteriores.

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.

Convenciones

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

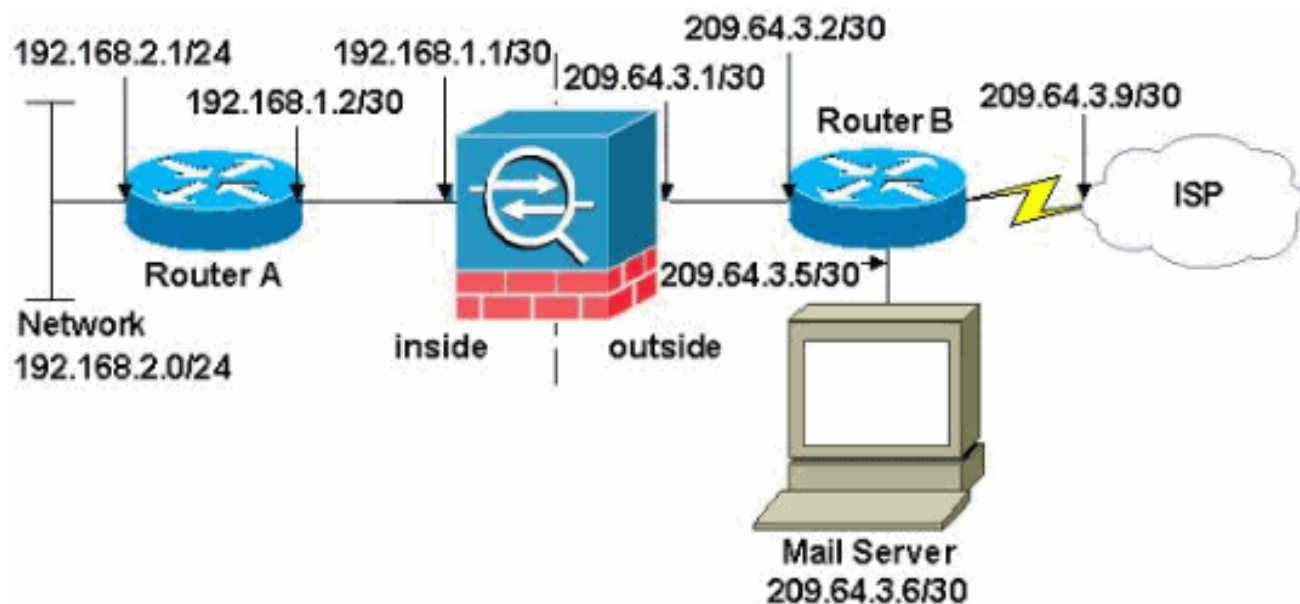
Configurar

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

Nota: Use el [Analizador de Cisco CLI](#) para obtener más información sobre los comandos usados en esta sección.

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 (192.168.1.0/30) y la red externa (209.64.3.0/30). El servidor de correo con la dirección IP 209.64.3.6 se encuentra en la red externa. Configure la instrucción NAT para que cualquier tráfico de la red 192.168.2.x que pasa de la interfaz interna (Ethernet0) a la interfaz exterior (Ethernet 1) se traduzca a una

dirección en el rango de 209.64.3.129 a 209.64.3.253. La última dirección disponible (209.64.3.254) está reservada para la traducción de direcciones de puerto (PAT) .

Configuraciones

En este documento, se utilizan estas configuraciones:

- [ASA](#)
- [Router A](#)
- [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
!
!--- Configure the inside interface. ? interface
Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!
!--- Configure the outside interface. interface
Ethernet4 nameif outside
 security-level 0
 ip address 209.64.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
boot system disk0:/asa831-k8.bin
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command states that any traffic !--- from the
192.168.2.x network that passes from the inside
interface (Ethernet0) !--- to the outside interface
(Ethernet 1) translates into an address !--- in the
range of 209.64.3.129 through 209.64.3.253 and contains
a subnet !--- mask of 255.255.255.128.  object network
obj-209.64.3.129_209.64.3.253
  range 209.64.3.129-209.64.3.253

!--- This command reserves the last available address
(209.64.3.254) for !--- for Port Address Translation
(PAT). In the previous statement, !--- each address
inside that requests a connection uses one !--- of the
addresses specified. If all of these addresses are in
use, !--- this statement provides a failsafe to allow
additional inside stations !--- to establish
connections. object network obj-209.64.3.254
  host 209.64.3.254

!--- This command indicates that all addresses in the
192.168.2.x range !--- that pass from the inside
(Ethernet0) to a corresponding global !--- designation
are done with NAT. !--- As outbound traffic is permitted
by default on the ASA, no !--- static commands are
needed. object-group network nat-pat-group
  network-object object obj-209.64.3.129_209.64.3.253
  network-object object obj-209.64.3.254

object network obj-192.168.2.0
  subnet 192.168.2.0 255.255.255.0
  nat (inside,outside) dynamic nat-pat-group

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The ASA forwards packets with
these addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1

!--- Sets the default route for the ASA Firewall at
209.64.3.2. route outside 0.0.0.0 0.0.0.0 209.64.3.2 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 since "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
rsh inspect rtsp inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:8a63de5ae2643c541a397c2de7901041
: end

```

Router A

Current configuration:

```

!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2522-R4
!
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
!
ip subnet-zero
!
!
!
!
!
interface Ethernet0
!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1
!
!
line con 0
  transport input none
line aux 0
  autoselect during-login
line vty 0 4
  exec-timeout 5 0
  password ww

```

```
login
!  
end
```

Router B

Current configuration:

```
!  
version 12.4  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname 2522-R4  
!  
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.  
!  
ip subnet-zero  
!  
!  
!  
interface Ethernet0  
  
!--- Assigns an IP address to the ASA-facing Ethernet  
interface. ip address 209.64.3.2 255.255.255.252 no ip  
directed-broadcast ! interface Ethernet1 !--- Assigns an  
IP address to the server-facing Ethernet interface. ip  
address 209.64.3.5 255.255.255.252 no ip directed-  
broadcast ! interface Serial0 !--- Assigns an IP address  
to the Internet-facing interface. ip address 209.64.3.9  
255.255.255.252 no ip directed-broadcast no ip mroute-  
cache ! interface Serial1 no ip address no ip directed-  
broadcast ! ip classless !--- All non-local packets are  
to be sent out serial 0. In this case, !--- the IP  
address on the other end of the serial interface is not  
known, !--- or you can specify it here. ip route 0.0.0.0  
0.0.0.0 serial 0  
!  
  
!--- This statement is required to direct traffic  
destined to the !--- 209.64.3.128 network (the ASA  
global pool) to the ASA to be translated !--- back to  
the inside addresses. ip route 209.64.3.128  
255.255.255.128 209.64.3.1  
!  
!  
line con 0  
  transport input none  
line aux 0  
  autoselect during-login  
line vty 0 4  
  exec-timeout 5 0  
  password ww  
  login  
!  
end
```

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
```

Verificación

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

Troubleshoot

[Cisco CLI Analyzer](#) admite ciertos **comandos show**. Utilice el Analizador CLI para ver un análisis del resultado del comando **show**.

El comando [logging buffered 7](#) dirige los 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

- [Firewalls Cisco ASA serie 5500-X](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)