PIX/ASA 7.x y posteriores: Ejemplo de Configuración de Acceso de Servidor de Correo (SMTP) en Red Externa

Contenido

Introducción

Esta configuración de ejemplo muestra cómo configurar el Firewall PIX para el acceso a un servidor de correo ubicado en la red externa.

Consulte PIX/ASA 7.x y superiores : Ejemplo de Configuración de Mail Server Access on Inside Network para configurar el PIX/ASA Security Appliance para acceder a un servidor de correo/SMTP ubicado en la red interna.

Consulte Ejemplo de Configuración de Red PIX/ASA 7.x con Acceso al Servidor de Correo en DMZ para configurar el Dispositivo de Seguridad PIX/ASA para el acceso a un servidor de correo/SMTP ubicado en la red DMZ.

Consulte ASA 8.3 y posteriores: Ejemplo de Configuración de Mail Server Access on Outside Network (SMTP) para obtener más información sobre la configuración idéntica en Cisco Adaptive Security Appliance (ASA) con la versión 8.3 y posteriores.

Refiérase a la documentación de Cisco Secure PIX Firewall para obtener más información sobre cómo configurar Microsoft Exchange. Elija su versión de software, luego vaya a la guía de configuración y lea el capítulo sobre cómo configurar para Microsoft Exchange.

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.

- Firewall PIX 535
- Software PIX Firewall versión 7.1(1)
- Cisco 2500 Routers

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.

Productos Relacionados

Esta configuración también se puede utilizar con un Adaptive Security Appliance (ASA) que ejecute la versión 7.x y posteriores.

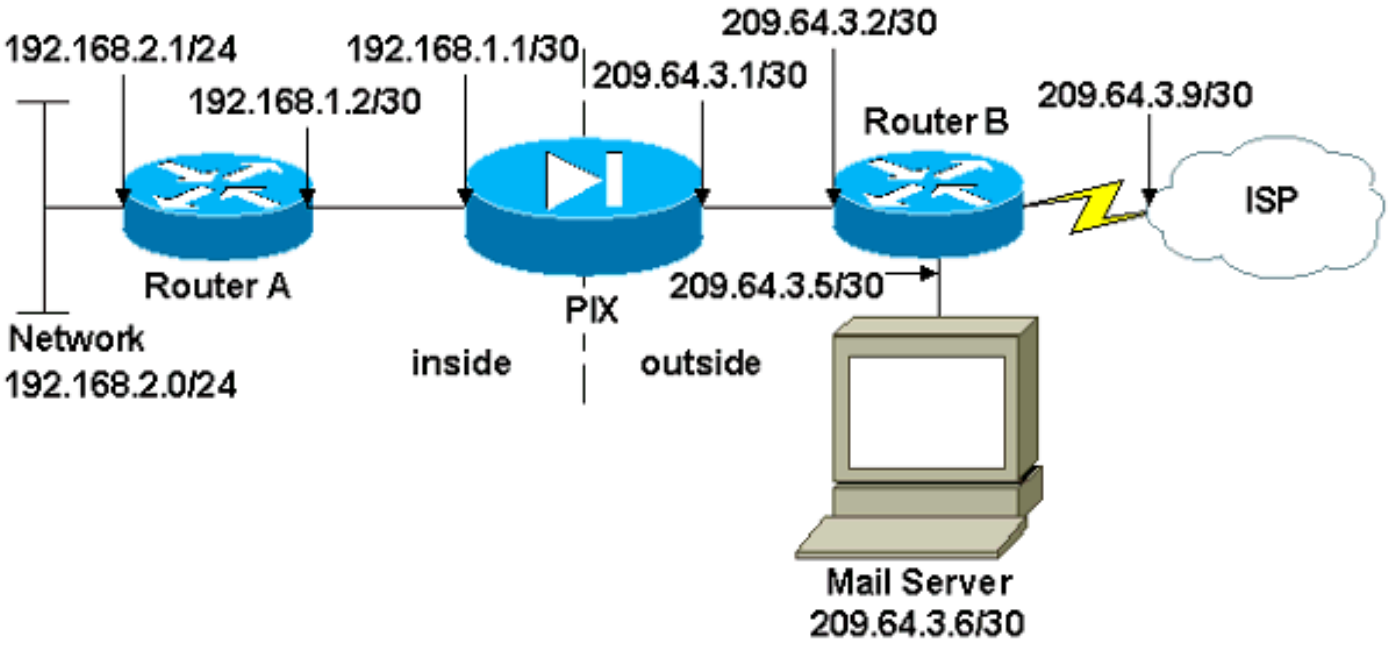
Configurar

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:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Firewall PIX
- Router A
- Router B

Firewall PIX

```
PIX Version 7.1(1)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 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 192.168.1.1 255.255.255.252
```

```
!

!--- Define the IP address for 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
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command defines the global for the Network
Address Translation !--- (NAT) statement. In this case,
the two commands state 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. global (outside)
1 209.64.3.129-209.64.3.253 netmask 255.255.255.128

!--- 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. global (outside) 1 209.64.3.254

!--- 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 PIX, no !--- static commands are
needed. nat (inside) 1 192.168.2.0 255.255.255.0

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The PIX 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 PIX 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 12.0
  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 PIX-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 PIX. 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 12.0
  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 PIX-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 PIX
global pool) to the PIX 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 de correo electrónico, la función de inspección de ESMTP (habilitada de forma predeterminada) en el PIX descarta los paquetes. Para permitir los correos electrónicos con TLS habilitado, inhabilite la función de inspección ESMTP como muestra este resultado.

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(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**.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

El comando **logging console debugging** dirige los mensajes a la consola PIX. 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

- Ajuste de conectividad mediante PIX firewalls de Cisco
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Firewalls Cisco ASA serie 5500-X
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems