PIX/ASA 7.x及更高版本：外部網路上的郵件(SMTP)伺服器訪問配置示例

目錄

簡介

此示例配置演示如何設定PIX防火牆以訪問位於外部網路上的郵件伺服器。

請參閱PIX/ASA 7.x及更高版本：用於設定PIX/ASA安全裝置以訪問位於內部網路上的郵件/SMTP伺服器的配置示例。

請參閱在DMZ網路上具有郵件伺服器訪問許可權的PIX/ASA 7.x配置示例，以設定PIX/ASA安全裝置以訪問位於DMZ網路上的郵件/SMTP伺服器。

請參閱ASA 8.3及更高版本：有關在8.3版及更高版本的Cisco Adaptive Security Appliance(ASA)上相同配置的詳細資訊，請參閱Mail(SMTP)Server Access on Outside Network配置示例。

有關如何設定Microsoft Exchange的詳細資訊，請參閱Cisco安全PIX防火牆文檔。選擇軟體版本，然後轉到配置指南並閱讀有關如何為Microsoft Exchange配置的章節。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX防火牆535
- PIX防火牆軟體版本7.1(1)
- Cisco 2500路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

相關產品

此配置還可以與運行7.x及更高版本的自適應安全裝置(ASA)配合使用。

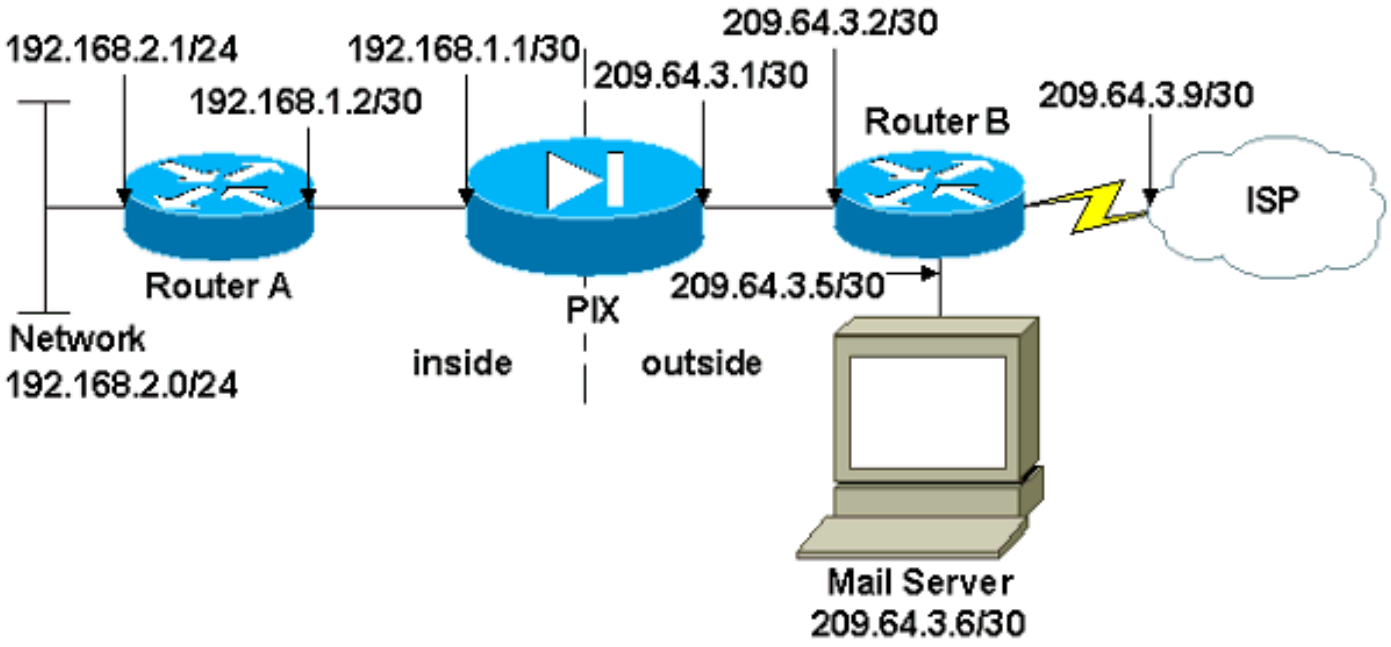
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Cisco CLI Analyzer獲取本節所用命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- PIX防火牆
- 路由器A
- 路由器B

PIX防火牆

```
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
```

路由器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
```

路由器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
```

ESMTP TLS配置

注意：如果對電子郵件通訊使用傳輸層安全(TLS)加密，則PIX中的ESMTP檢查功能（預設啟用）會丟棄資料包。要允許啟用TLS的電子郵件，請按照此輸出所示禁用ESMTP檢查功能。

```
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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

Cisco CLI Analyzer支援某些show指令。使用CLI Analyzer檢視show指令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

logging console debugging命令將消息定向到PIX控制檯。如果與郵件伺服器的連線存在問題，請檢查控制檯調試消息以找到傳送站和接收站的IP地址以確定問題。

相關資訊

- 通過Cisco PIX防火牆建立連線
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- Cisco ASA 5500-X系列防火牆
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems