

PIX/ASA 7.x 以降：外部ネットワークのメール (SMTP) サーバのアクセスの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[関連製品](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[ESMTP TLS の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この設定例では、外部ネットワークにあるメールサーバにアクセスするために PIX Firewall を設定する方法を説明します。

[PIX/ASA 7.x以降を参照してください。内部ネットワークでのメールサーバアクセスの設定例](#)』を参照してください。

PIX/ASAセキュリティアプライアンスをDMZネットワーク上のメール/SMTPサーバにアクセスするように設定するには、『[DMZネットワーク上のメールサーバアクセスを使用したPIX/ASA 7.xの設定例](#)』を参照してください。

バージョン 8.3 以降の Cisco Adaptive Security Appliance (ASA) での ASDM を使用した同等な設定の詳細について『[ASA 8.3.x 以降：外部ネットワークでのメール\(SMTP\)サーバアクセスの設定例](#)』を参照してください。

Microsoft Exchange の設定方法については、Cisco Secure PIX Firewall のドキュメントを参照してください。ソフトウェアのバージョンを選択した後、設定ガイドに移動し、Microsoft Exchange の設定方法に関する章を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX Firewall 535
- PIX Firewall ソフトウェア リリース 7.1(1)
- Cisco 2500 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

関連製品

この構成は、バージョン 7.x 以降が稼働する適応型セキュリティ アプライアンス (ASA) でも使用できます。

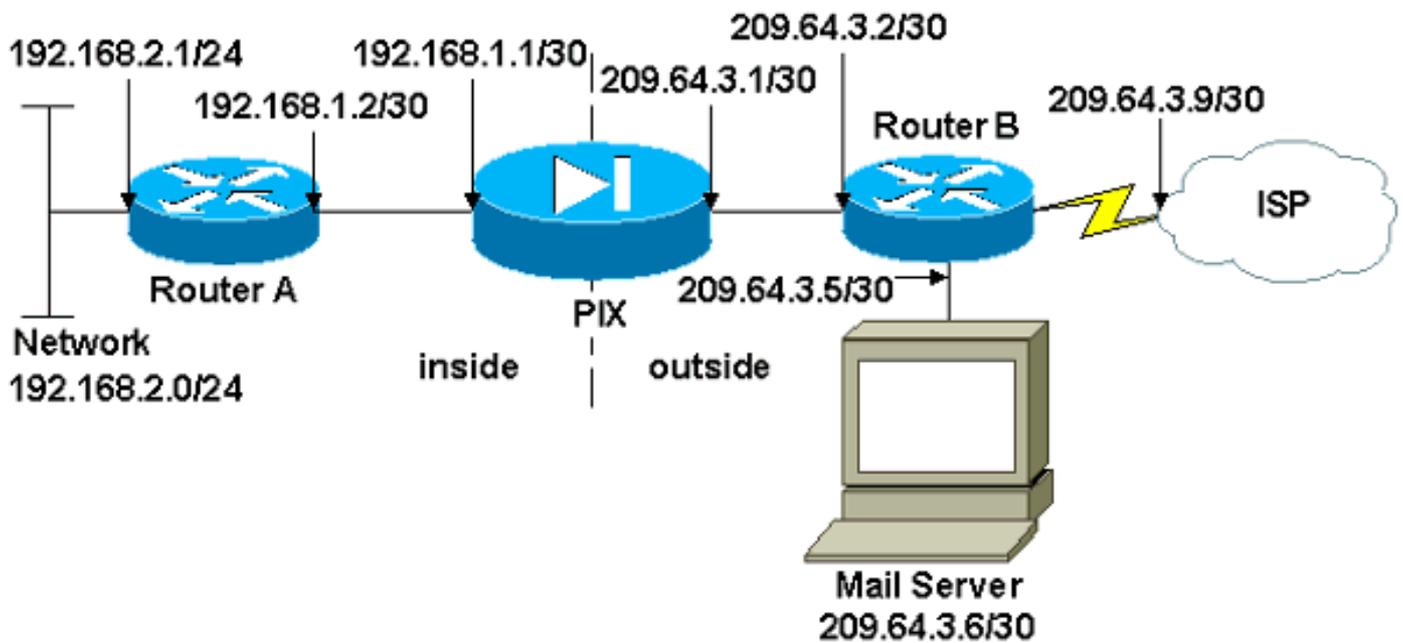
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用される[れるコマンド](#)の詳細については、Cisco CLI Analyzerを使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- [PIX ファイアウォール](#)
- [ルータ A](#)
- [ルータ B](#)

PIX ファイアウォール

```

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

```

ルータ 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
```

ルータ 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 の設定

注：Transport Layer Security(TLS)暗号化を電子メール通信に使用する場合、PIXのESMTPインスペクション機能（デフォルトで有効）はパケットをドロップします。TLS が有効な電子メールを許可するには、次の出力のように ESMTP インスペクション機能を無効にします。

```
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

[Cisco CLI Analyzer](#)では、特定のshowコマンドをサポートします。CLIアナライザを使用して、showコマンド出力の分析を表示します。

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

logging console debugging コマンドで、メッセージが PIX コンソールに転送されます。メールサーバへの接続に問題がある場合は、コンソール デバッグ メッセージを調べて、送信側と受信側のステーションの IP アドレスを見つけ、問題を特定します。

関連情報

- [Cisco PIX ファイアウォールを經由した接続の確立](#)
- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [Cisco ASA 5500-Xシリーズファイアウォール](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)