PIX/ASA 7.x und höher: Beispiel für den Zugriff auf den Mail-Server (SMTP) in einem externen Netzwerk

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Zugehörige Produkte
Konfigurieren
Netzwerkdiagramm
Konfigurationen
ESMTP-TLS-Konfiguration
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Diese Beispielkonfiguration veranschaulicht, wie die PIX-Firewall für den Zugriff auf einen Mailserver im externen Netzwerk eingerichtet wird.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher: Mail Server Access on Inside Network Configuration Example, um die PIX/ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im Inside-Netzwerk einzurichten.

Weitere Informationen zum Einrichten der PIX/ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im DMZ-Netzwerk finden Sie unter PIX/ASA 7.x mit Mail-Server-Zugriff im Konfigurationsbeispiel für das DMZ-Netzwerk.

Weitere Informationen finden Sie unter ASA 8.3 und höher: SMTP-Server-Zugriff auf externe Netzwerkkonfiguration Beispiel für weitere Informationen zur identischen Konfiguration der Cisco Adaptive Security Appliance (ASA) mit Version 8.3 und höher.

Weitere Informationen zum Festlegen von Microsoft Exchange finden Sie in der Dokumentation zur Cisco Secure PIX Firewall. Wählen Sie Ihre Softwareversion aus, gehen Sie dann zum Konfigurationsleitfaden und lesen Sie das Kapitel zur Konfiguration für Microsoft Exchange.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX-Firewall 535
- PIX Firewall Software Version 7.1(1)
- Cisco Router der Serie 2500

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Zugehörige Produkte

Diese Konfiguration kann auch mit einer Adaptive Security Appliance (ASA) verwendet werden, die Version 7.x und höher ausführt.

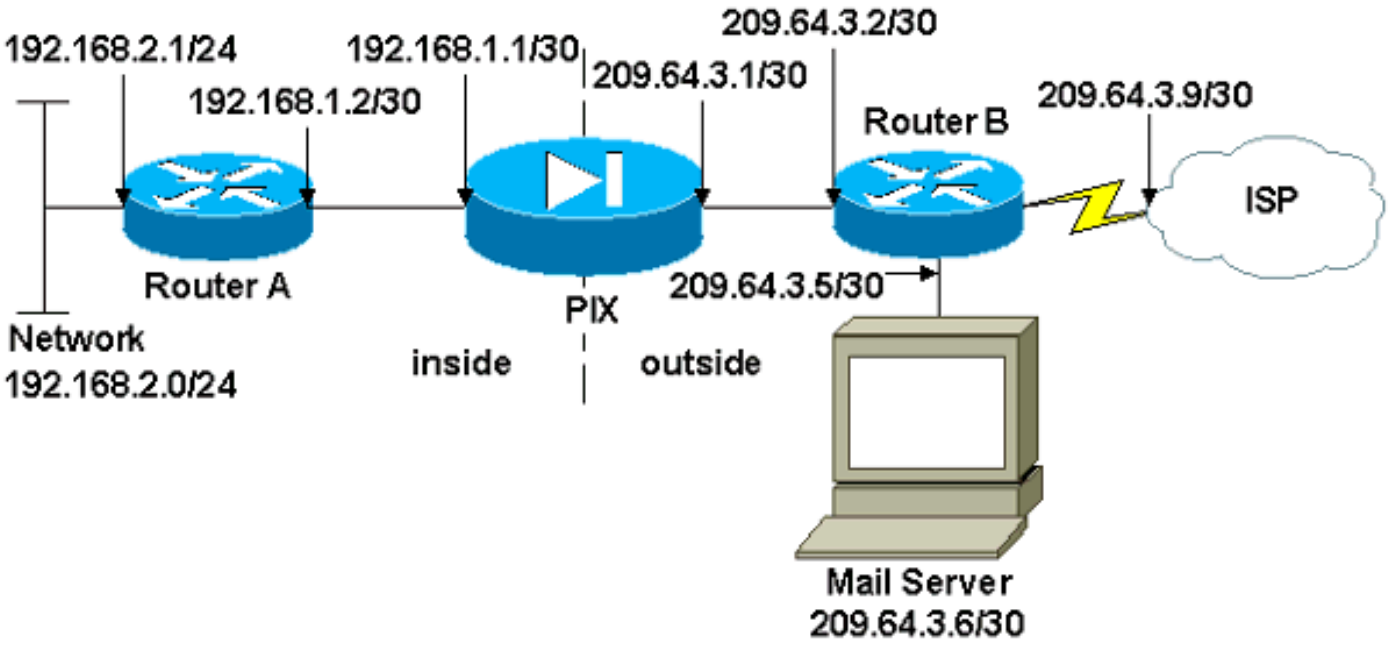
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie den Cisco CLI Analyzer, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen abzurufen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- PIX-Firewall
- Router A
- Router B

PIX-Firewall

```
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
```

ESMTP-TLS-Konfiguration

Hinweis: Wenn Sie die TLS-Verschlüsselung (Transport Layer Security) für die E-Mail-Kommunikation verwenden, werden die Pakete von der ESMTP-Überprüfungsfunktion (standardmäßig aktiviert) im PIX verworfen. Um E-Mails mit aktiviertem TLS zuzulassen, deaktivieren Sie die ESMTP-Überprüfungsfunktion, wie in dieser Ausgabe dargestellt.

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Der Cisco CLI Analyzer unterstützt bestimmte **show**-Befehle. Verwenden Sie CLI Analyzer, um eine Analyse der **Ausgabe von show**-Befehlen anzuzeigen.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Der Befehl **zum Debuggen der Protokollierungskonsole** leitet Meldungen an die PIX-Konsole weiter. Wenn die Verbindung zum Mailserver ein Problem darstellt, überprüfen Sie die Debug-Meldungen der Konsole, um die IP-Adressen der sendenden und empfangenden Stationen zu ermitteln, um das Problem zu ermitteln.

Zugehörige Informationen

- Konnektivität über Cisco PIX-Firewalls
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Cisco Firewalls der Serie ASA 5500-X
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems