ASA 8.3及更高版本：DMZ上郵件(SMTP)伺服器訪問的配置示例

目錄

簡介

此示例配置演示如何設定ASA安全裝置以訪問位於非軍事區(DMZ)網路上的簡單郵件傳輸協定(SMTP)伺服器。

請參閱ASA 8.3及更高版本：有關如何設定ASA安全裝置以訪問位於內部網路上的郵件/SMTP伺服器的詳細資訊，請參閱內部網路上的郵件(SMTP)伺服器訪問配置示例。

請參閱ASA 8.3及更高版本：有關如何設定ASA安全裝置以訪問位於外部網路上的郵件/SMTP伺服器的詳細資訊，請參閱Mail(SMTP)Server Access on Outside Network配置示例。

請參閱PIX/ASA 7.x及更高版本：DMZ上的郵件(SMTP)伺服器訪問配置示例在8.2及更低版本的思科自適應安全裝置(ASA)上獲取相同的配置。

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：

- 運行8.3及更高版本的思科自適應安全裝置(ASA)。
- 採用Cisco IOS®軟體版本12.4(20)T的Cisco 1841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。

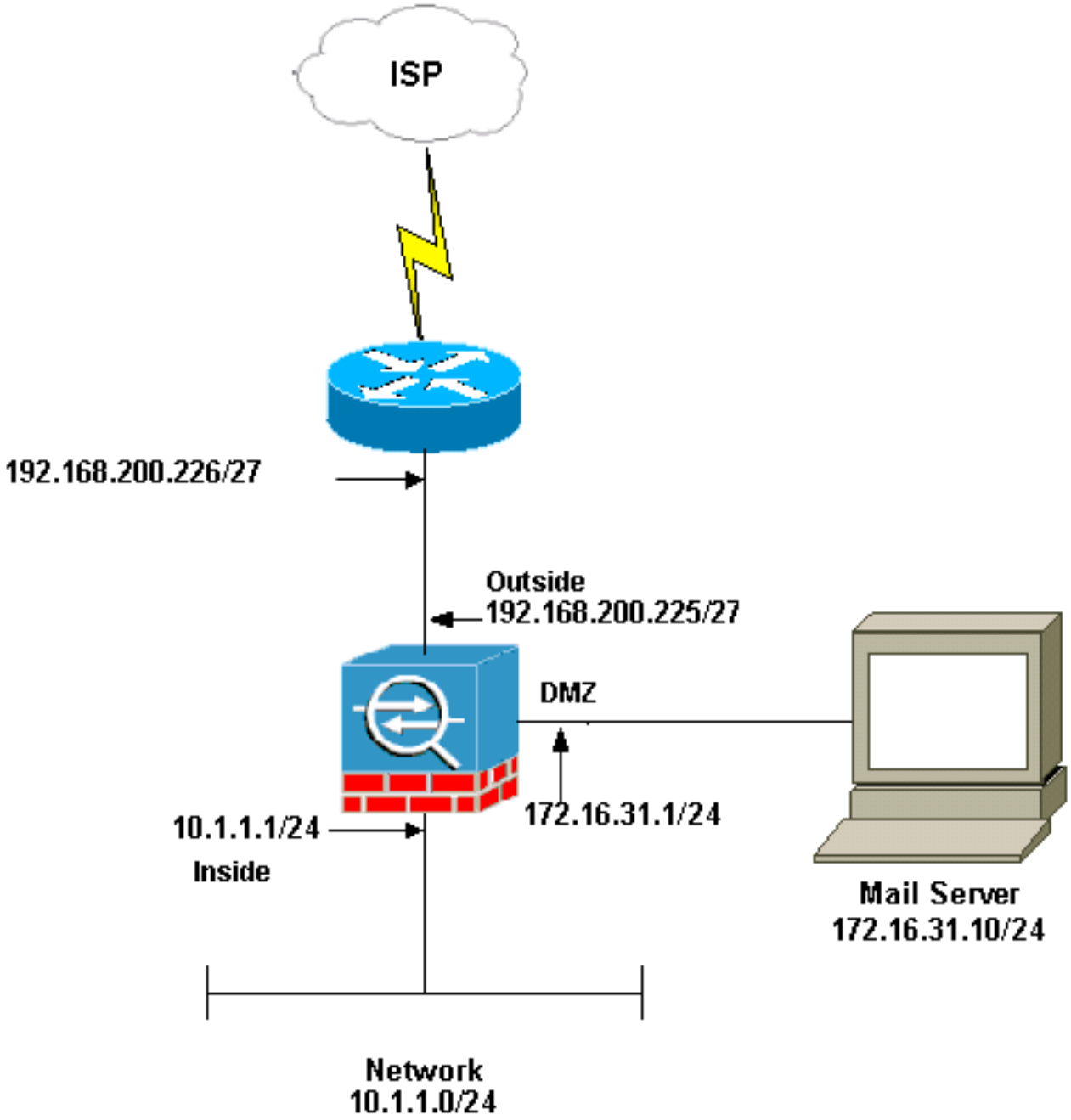
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是RFC 1918 ，已在實驗室環境中使用。

本示例中使用的網路設定包含具有內部網路(10.1.1.0/24)和外部網路(192.168.200.0/27)的ASA。IP地址為172.16.31.10的郵件伺服器位於非軍事區(DMZ)網路中。對於要由內部訪問的郵件伺服器，使用者配置身份NAT。配置訪問清單(在本示例中為**dmz_int**)，以允許從郵件伺服器到內部網路中主機的傳出SMTP連線，並將其繫結到DMZ介面。

類似地，外部使用者訪問Mailserver時配置靜態NAT和訪問清單(在本示例中為**outside_int**)，以允許外部使用者訪問Mailserver並將此訪問清單繫結到外部介面。

ASA配置

本檔案會使用以下設定：

ASA配置

```
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
 security-level 0
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 no nameif
 no security-level
 no ip address
!
!--- Configure the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host  192.168.200.227 eq smtp
!--- Allows outgoing SMTP connections. !--- This access
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400


  object network obj-192.168.200.228-192.168.200.253
   range 192.168.200.228-192.168.200.253
 object network obj-192.168.200.254
   host 192.168.200.254

 object-group network nat-pat-group
   network-object object obj-192.168.200.228-
192.168.200.253
```

```
   network-object object obj-192.168.200.254

 object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,dmz) static obj-10.1.1.0

!--- This network static uses address translation. !---
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
   host 172.16.31.10
   nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0  192.168.200.226 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
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.


policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- The  inspect esmtp  command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
```

```
: end
[OK]
```

ESMTP TLS配置

注意：如果您對電子郵件通訊使用傳輸層安全(TLS)加密，則ASA中的ESMTP檢查功能（預設情況下啟用）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。如需詳細資訊，請參閱Cisco錯誤ID CSCtn08326(僅限註冊客戶)。

```
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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- debug icmp trace — 顯示來自主機的網際網路控制消息協定(ICMP)請求是否到達ASA。您需要新增**access-list**命令才能在組態中允許ICMP，才能執行此偵錯。**注意**：若要使用此偵錯，請確保在`access-list outside_intICMP`以下輸出所示：
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- logging buffered 7 — 在全域性配置模式下用於使自適應安全裝置將系統日誌消息傳送到日誌緩衝區。可以使用show logging命令檢視ASA日誌緩衝區的內容。

有關如何設定日誌記錄的詳細資訊，請參閱使用ASDM配置系統日誌。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems