ASA 8.3 及更高版本：DMZ 上的邮件 (SMTP) 服务器访问配置示例

目录

简介

此配置示例展示了如何设置 ASA 安全设备以访问位于隔离区 (DMZ) 网络的简单邮件传输协议 (SMTP) 服务器。

请参阅 ASA 8.3及以上版本：有关如何设置 ASA 安全设备以访问位于内部网络的邮件/SMTP 服务器的更多信息，请参阅内部网络中的邮件 (SMTP) 服务器访问配置示例。

请参阅 ASA 8.3及以上版本：有关如何设置 ASA 安全设备以访问位于外部网络的邮件/SMTP 服务器的更多信息，请参阅外部网络中的邮件 (SMTP) 服务器访问配置示例。

请参阅 PIX/ASA 7.x 及更高版本：有关在 8.2 及更低版本的思科自适应安全设备 (ASA) 上进行相同配置的信息，请参阅 DMX 中的邮件 (SMTP) 服务器访问配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 8.3 及更高版本的思科自适应安全设备 (ASA)。
- 装有 Cisco IOS® 软件版本 12.4(20)T 的 Cisco 1841 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

此示例中使用的网络设置具有带内部网络 (10.1.1.0/24) 和外部网络 (192.168.200.0/27) 的 ASA。IP 地址为 172.16.31.10 的邮件服务器位于隔离区 (DMZ) 网络中。对于由内部访问的邮件服务器，用户会配置标识 NAT。配置访问列表，在本例中，此列表为 **dmz_int**，以允许从邮件服务器到主机的出站 SMTP 连接位于内部网络中并将此列表绑定到 DMZ 接口。

同样地，要让外部用户访问邮件服务器，请配置一个静态 NAT 和一个访问列表，在本例中，此列表为 **outside_int**，以允许外部用户访问邮件服务器并将此列表绑定到外部接口。

ASA 配置

本文档使用以下配置：

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： 如果对邮件通信使用传输层安全 (TLS) 加密，则 ASA 中的 ESMTP 检查功能（默认情况下启用）会丢弃数据包。要允许在启用了 TLS 功能的情况下使用电子邮件，请禁用 ESMTP 检查功能，如此输出所示。有关详细信息，请参阅 Cisco Bug ID CSCtn08326（仅限注册用户）。

```
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
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **debug icmp trace** - 显示主机的互联网控制消息协议 (ICMP) 请求是否到达 ASA。需要添加 **access-list** 命令，在您的配置中允许 ICMP，以便运行此 debug 命令。**注意：** 要使用此调试，请确保在 access-list outside_int 中允许 ICMP，如此输出所示：`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** - 用于在全局配置模式中，使自适应安全设备将系统日志消息发送到日志缓冲区。ASA 日志缓冲区的内容可使用 **show logging 命令**查看。

有关如何设置日志记录的更多信息，请参阅使用 ASDM 配置系统日志。

相关信息

- **Cisco ASA 5500 系列自适应安全设备**
- **请求注解 (RFC)**
- **技术支持和文档 - Cisco Systems**