ASA 8.3 及更高版本：内部网络上的邮件 (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内部网络的邮件 (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 DMZ 网络的邮件/SMTP 服务器的更多信息，请参阅 DMZ 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：有关设置 ASA 安全设备以访问位于外部网络的邮件/SMTP 服务器的信息，请参阅外部网络中的邮件 (SMTP) 服务器访问配置示例。

有关详细信息，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。

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。

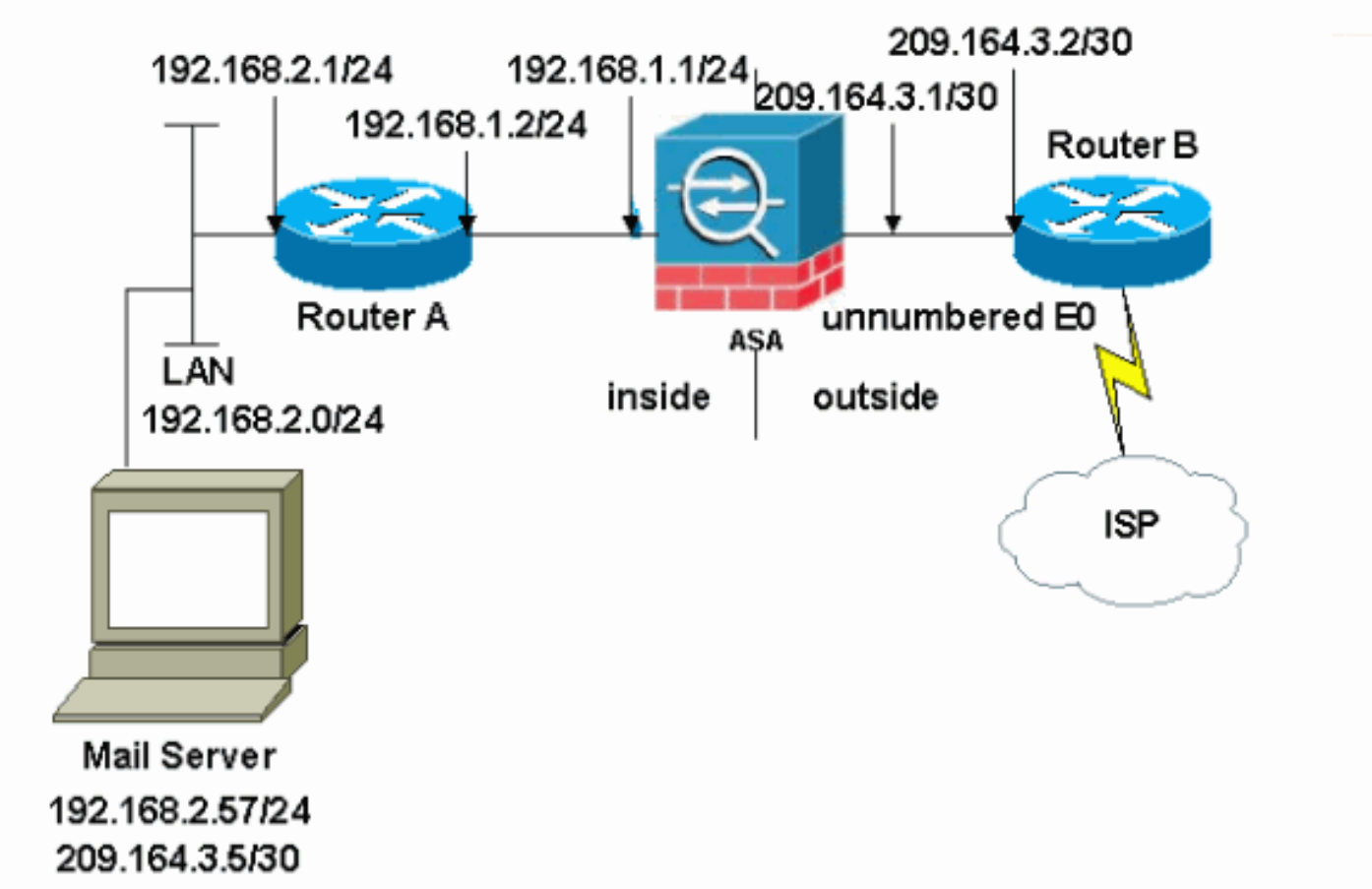
配置

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 (192.168.1.0/24) 和外部网络 (209.164.3.0/30) 的 ASA。IP 地址为 209.64.3.5 的邮件服务器位于内部网络中。

配置

本文档使用以下配置：

- ASA
- 路由器 B

ASA

```
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 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
255.255.255.0 ! !--- Define the IP address for the
outside interface. interface Ethernet4 nameif outside
security-level 0 ip address 209.164.3.1 255.255.255.252
! interface Ethernet5 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Create an access list that permits
Simple !--- Mail Transfer Protocol (SMTP) traffic from
anywhere !--- to the host at 209.164.3.5 (our server).
The name of this list is !--- smtp. Add additional lines
to this access list as required. !--- Note: There is one
and only one access list allowed per !--- interface per
direction, for example, inbound on the outside
interface. !--- Because of limitation, any additional
lines that need placement in !--- the access list need
to be specified here. If the server !--- in question is
not SMTP, replace the occurrences of SMTP with !--- www,
DNS, POP3, or whatever else is required. access-list
smtp extended permit tcp any host 209.164.3.5 eq smtp
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover no asdm history enable arp timeout 14400 !---
Specify that any traffic that originates inside from the
!--- 192.168.2.x network NATs (PAT) to 209.164.3.129 if
!--- such traffic passes through the outside interface.
object network obj-192.168.2.0 subnet 192.168.2.0
255.255.255.0 nat (inside,outside) dynamic 209.164.3.129
!--- Define a static translation between 192.168.2.57 on
the inside and !--- 209.164.3.5 on the outside. These
are the addresses to be used by !--- the server located
inside the ASA. object network obj-192.168.2.57 host
192.168.2.57 nat (inside,outside) static 209.164.3.5 !--
- Apply the access list named smtp inbound on the
outside interface. access-group smtp in interface
outside !--- Instruct the ASA to hand any traffic
destined for 192.168.x.x !--- to the router at
192.168.1.2. route inside 192.168.0.0 255.255.0.0
192.168.1.2 1 !--- Set the default route to 209.164.3.2.
!--- The ASA assumes that this address is a router
address. route outside 0.0.0.0 0.0.0.0 209.164.3.2 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 as "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 netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
!--- SMTP/ESMTP is inspected as "inspect esmtp" is
included in the map. service-policy global_policy global
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

路由器 B

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname 2522-R5
 !
 enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
 !
 ip subnet-zero
 !
 !
 !
 !
 !
 interface Ethernet0

!--- Sets the IP address of the Ethernet interface to
209.164.3.2. ip address 209.164.3.2 255.255.255.252 !
interface Serial0 !--- Instructs the serial interface to
use !--- the address of the Ethernet interface when the
need arises. ip unnumbered ethernet 0 ! interface
Serial1 no ip address no ip directed-broadcast ! ip
classless !--- Instructs the router to send all traffic
!--- destined for 209.164.3.x to 209.164.3.1. ip route
209.164.3.0 255.255.255.0 209.164.3.1 !--- Instructs the
router to send !--- all other remote traffic out serial
0. ip route 0.0.0.0 0.0.0.0 serial 0 ! ! line con 0
transport input none line aux 0 autoselect during-login
line vty 0 4 exec-timeout 5 0 password ww login ! end
```

注意： 未添加路由器 A 的配置。您只需提供接口上的 IP 地址并将默认网关设置为 192.168.1.1，这是 ASA 的内部接口。

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
```

注意： 在 ASA 8.0.3 版及更高版本中，使用 **allow-tls** 命令可以在启用了 inspect esmtp 的情况下允许 TLS 电子邮件，如下所示：

```
policy-map type inspect esmtp tls-esmtp
parameters
```

```
allow-tls
inspect esmtp tls-esmtp
```

验证

当前没有可用于此配置的验证过程。

故障排除

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。

logging buffered 7 命令将消息导向 ASA 控制台.如果与邮件服务器的连接有问题，请检查控制台调试消息，查找发送站和接收站的 IP 地址以便确定问题所在。

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**