ASA 8.3 及更高版本：在外部网络的邮件(SMTP)服务器访问配置示例

目录

简介

此配置示例提供了有关如何设置自适应安全设备 (ASA) 以访问位于外部网络的邮件服务器的信息。

请参阅 ASA 8.3 及更高版本：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 及更高版本：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，请参阅外部网络中的邮件 (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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

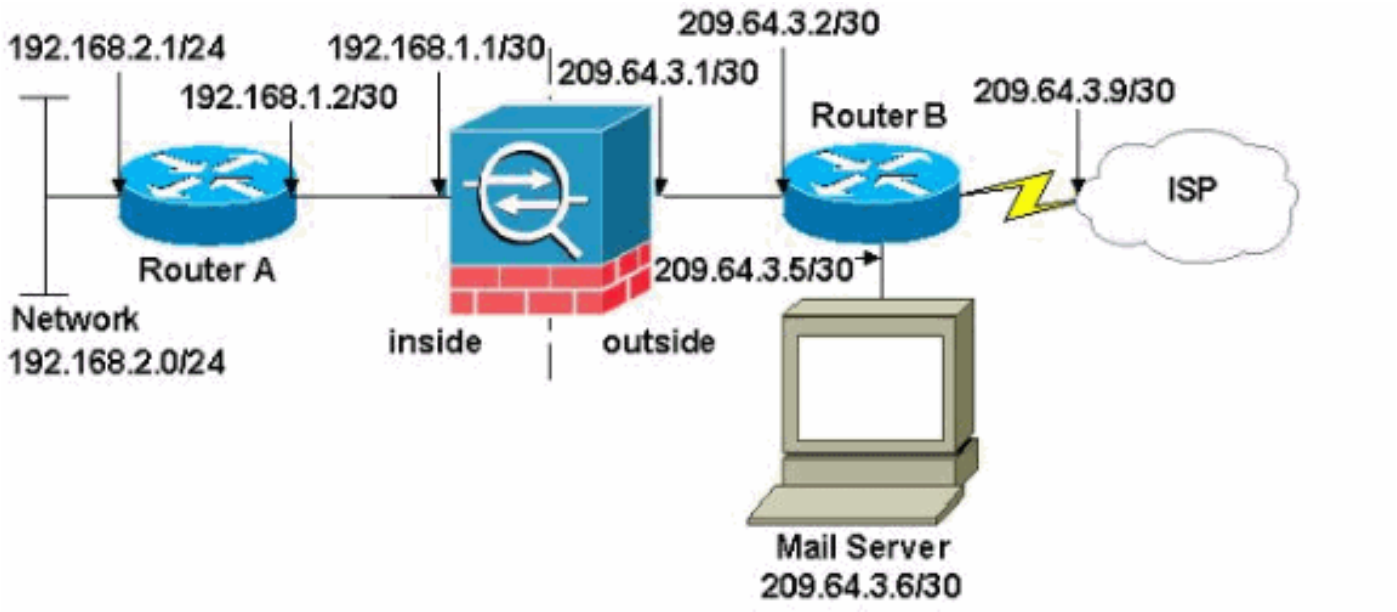
配置

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Cisco CLI Analyzer获取有关本节中使用的命令的详细信息。

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 (192.168.1.0/30) 和外部网络 (209.64.3.0/30) 的 ASA。IP 地址为 209.64.3.6 的邮件服务器位于外部网络中。配置NAT语句，使从192.168.2.x网络从内部接口（以太网接口0）传输到外部接口（以太网接口1）的任何流量转换为209.64.3.129到209.64.3.253范围内的地址。最后一个可用地址(209.64.3.253)09.64.3.254)保留用于端口地址转换(PAT)。

配置

本文档使用以下配置：

- ASA
- Router A
- Router 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
!

!--- Configure the inside interface. ? interface
Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!

!--- Configure 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
boot system disk0:/asa831-k8.bin
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command states 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.   object network
obj-209.64.3.129_209.64.3.253
   range 209.64.3.129-209.64.3.253
```

```
!--- 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. object network obj-209.64.3.254
   host 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 ASA, no !--- static commands are
needed. object-group network nat-pat-group
   network-object object obj-209.64.3.129_209.64.3.253
   network-object object obj-209.64.3.254

 object network obj-192.168.2.0
   subnet 192.168.2.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The ASA 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 ASA 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 12.4
  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 ASA-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 ASA. 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 12.4
  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 ASA-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 ASA
global pool) to the ASA 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 配置

注意：如果对电子邮件通信使用传输层安全(TLS)加密，则ASA中的ESMTP检测功能（默认启用）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。

```
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

Cisco CLI分析器支持某些**show**命令。使用CLI Analyzer查看对show命令输**出的**分析。

logging buffered 7 命令会将消息定向到 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-X系列防火墙
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems