# ASA 8.3 e posterior: Exemplo de Configuração de Acesso ao Servidor de Correio (SMTP - Mail Server Access on Outside Network Configuration Example)

## Contents



## Introduction

Este exemplo de configuração fornece informações sobre como configurar o Adaptive Security Appliance (ASA) para acesso a um servidor de e-mail localizado na rede externa.

Consulte o ASA 8.3 e posterior: Exemplo de Acesso ao Servidor de Correio (SMTP) no DMZ Configuration Example para obter mais informações sobre como configurar o ASA Security Appliance para acesso a um servidor de email/SMTP localizado na rede DMZ.

Consulte o ASA 8.3 e posterior: Exemplo de Acesso ao Servidor de Email (SMTP) na Configuração de Rede Interna para configurar o ASA Security Appliance para acesso a um servidor de email/SMTP localizado na Rede Interna.

Consulte o PIX/ASA 7.x ou posterior: Exemplo de Acesso ao Servidor de Email (SMTP) em Rede Externa para a configuração idêntica no Cisco Adaptive Security Appliance (ASA) com versões 8.2 e anteriores.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Adaptive Security Appliance (ASA) que executa a versão 8.3 e posterior
- Roteador Cisco 1841 com Software Cisco IOS® versão 12.4(20)T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

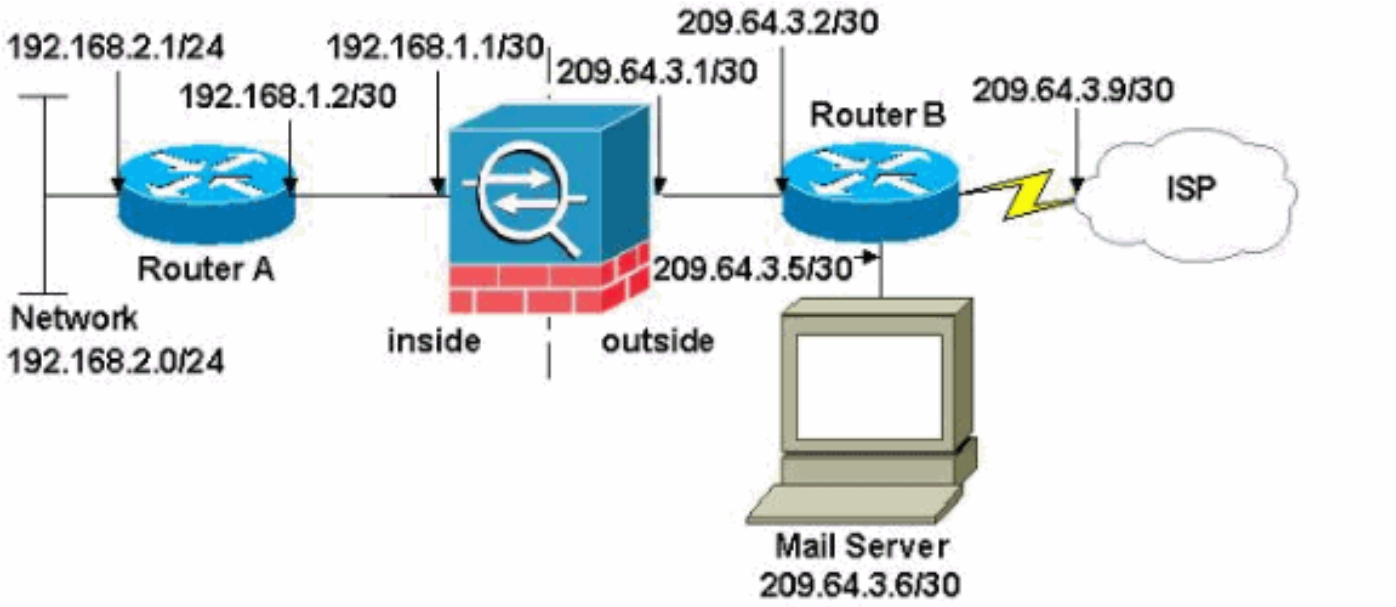
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Observação:** use o Cisco CLI Analyzer para obter mais informações sobre os comandos usados nesta seção.

### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




**Observação:** os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 que foram usados em um ambiente de laboratório.

A configuração de rede usada neste exemplo tem o ASA com rede interna (192.168.1.0/30) e a rede externa (209.64.3.0/30). O servidor de e-mail com endereço IP 209.64.3.6 está localizado na

rede externa. Configure a instrução NAT de modo que qualquer tráfego da rede 192.168.2.x que passa da interface interna (Ethernet0) para a interface externa (Ethernet 1) seja convertido em um endereço no intervalo de 209.64.3.129 a 209.64.3.253. O último endereço disponível (209.64.3.254) é reservado para a Port Address Translation (PAT) .

## Configurações

Este documento utiliza as seguintes configurações:

- 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
```

## Configuração de TLS ESMTP

**Observação:** se você usar a criptografia TLS (Transport Layer Security) para comunicação por e-mail, o recurso de inspeção ESMTP (ativado por padrão) no ASA descarta os pacotes. Para permitir os e-mails com TLS ativado, desative o recurso de inspeção ESMTP como mostrado nesta saída. Consulte o bug da Cisco ID CSCtn08326 para obter mais informações.

```
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
```

# Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

# Troubleshoot

O Cisco CLI Analyzer suporta determinados comandos **show**. Use o Analisador CLI para exibir uma análise da saída do comando **show**.

O comando logging buffered 7 direciona mensagens para o console ASA. Se a conectividade com o servidor de e-mail for um problema, examine as mensagens de depuração do console para localizar os endereços IP das estações de envio e de recebimento para determinar o problema.

# Informações Relacionadas

- Firewalls Cisco ASA 5500-X Series
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems