

ASA 8.3 et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie (SMTP) sur un réseau interne

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration TLS ESMTP](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Cet exemple de configuration décrit comment configurer un dispositif de sécurité ASA pour l'accès à un serveur de messagerie (SMTP) situé dans le réseau interne.

Référez-vous à [ASA 8.3 et versions ultérieures : Exemple d'accès au serveur de messagerie \(SMTP\) sur la DMZ Configuration](#) pour plus d'informations sur la configuration de l'appliance de sécurité ASA pour l'accès à un serveur de messagerie/SMTP situé sur le réseau DMZ.

Référez-vous à [ASA 8.3 et versions ultérieures : Accès au serveur de messagerie \(SMTP\) sur le réseau externe Exemple de configuration](#) pour configurer l'appliance de sécurité ASA pour l'accès à un serveur de messagerie/SMTP situé sur le réseau externe.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Adaptive Security Appliance (ASA) qui exécute les versions 8.3 et ultérieures.
- Routeur Cisco 1841 avec logiciel Cisco IOS[®] version 12.4(20)T

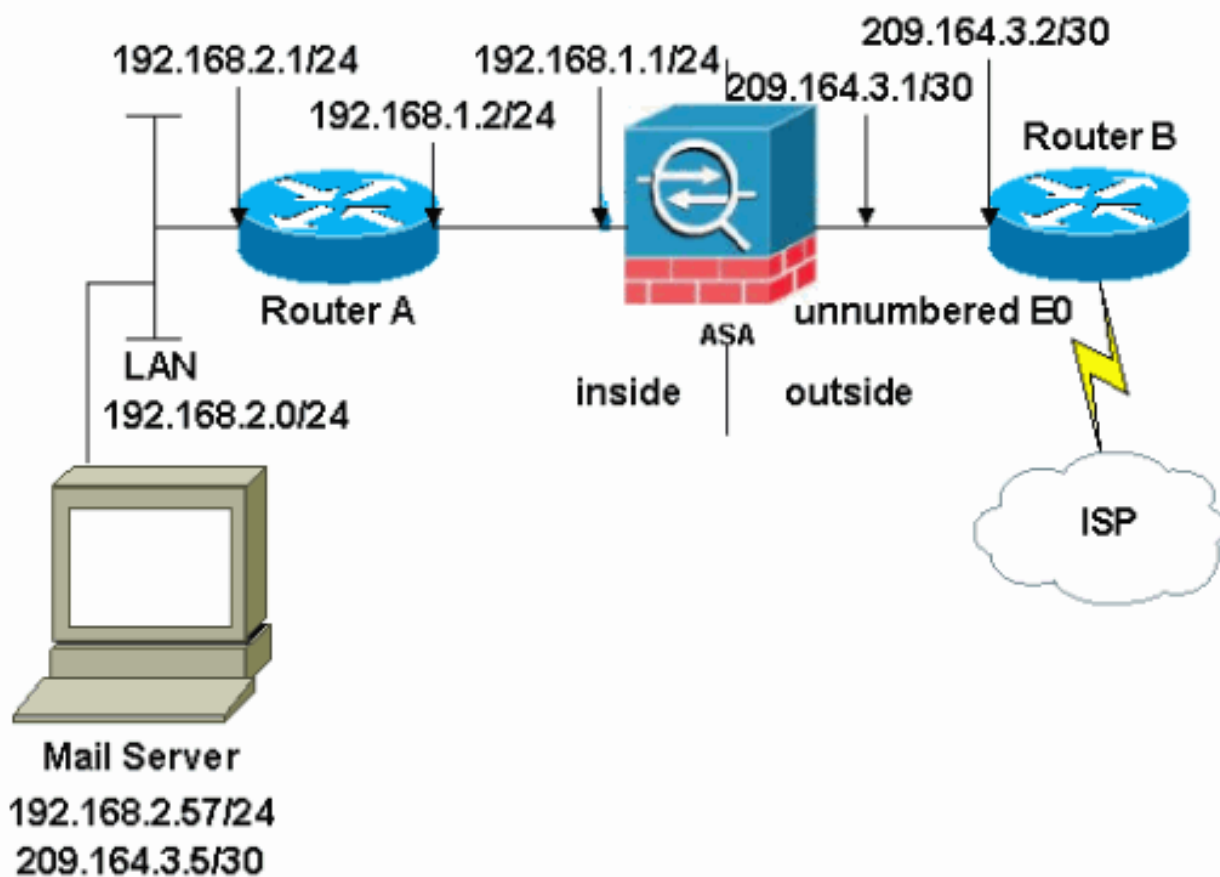
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisées dans un environnement de laboratoire.](#)

La configuration de réseau utilisée dans cet exemple a l'ASA avec le réseau interne (192.168.1.0/24) et le réseau externe (209.164.3.0/30). Le serveur de messagerie dont l'adresse IP est 209.64.3.5 se trouve sur le réseau interne.

Configurations

Ce document utilise les configurations suivantes :

- [ASA](#)

- [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
```

```
!
```

```
!--- 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 the 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 lists that need placement in !--- the access list need to be specified here. If the server !--- in question is 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-192.16
  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. r
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.
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 gl
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

Router 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 209.164.3.2 255.255.255.2
interface Serial0 !--- Instructs the serial interface to use !--- the address of the Ethernet interface
the need arises. ip unnumbered ethernet 0 ! interface Serial1 no ip address no ip directed-broadcast !
classless !--- Instructs the router to send all traffic !--- destined for 209.164.3.x to 209.164.3.1. i
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
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

```

Remarque : La configuration du routeur A n'est pas ajoutée. Vous devez seulement donner les adresses IP sur les interfaces et définir la passerelle par défaut sur 192.168.1.1, qui est l'interface interne de l'ASA .

Configuration TLS ESMTP

Remarque : si vous utilisez le chiffrement TLS (Transport Layer Security) pour la communication par courrier électronique, la fonction d'inspection ESMTP (activée par défaut) de l'ASA supprime les paquets. Afin d'autoriser les e-mails avec TLS activé, désactivez la fonction d'inspection ESMTP comme le montre ce résultat. Référez-vous à l'ID de bogue Cisco [CSCtn08326](#) pour plus d'informations.

```

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

```

Remarque : dans ASA version 8.0.3 et ultérieures, la commande **allow-tls** est disponible pour autoriser les e-mails TLS avec inspect esmtp activé comme indiqué :

```

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

```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

La commande `logging buffered 7` dirige les messages vers la console ASA. Si la connectivité au serveur de messagerie pose problème, examinez les messages de débogage de la console pour localiser les adresses IP des stations d'envoi et de réception afin de déterminer le problème.

Informations connexes

- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)