

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration TLS ESMTP](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Cet exemple de configuration fournit des informations sur la configuration de l'appliance de sécurité adaptatif (ASA) pour l'accès à un serveur de messagerie situé sur le réseau externe.

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 : Exemple de configuration de l'accès au serveur de messagerie \(SMTP\) sur le réseau interne](#) afin de configurer l'appliance de sécurité ASA pour l'accès à un serveur de messagerie/SMTP situé sur le réseau interne.

Consultez [PIX/ASA 7.x et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie \(SMTP\) sur le réseau externe](#) pour la configuration identique sur l'appliance de sécurité adaptative (ASA) Cisco avec les versions 8.2 et antérieures.

## 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 :

- Appareil de sécurité adaptatif Cisco (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.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

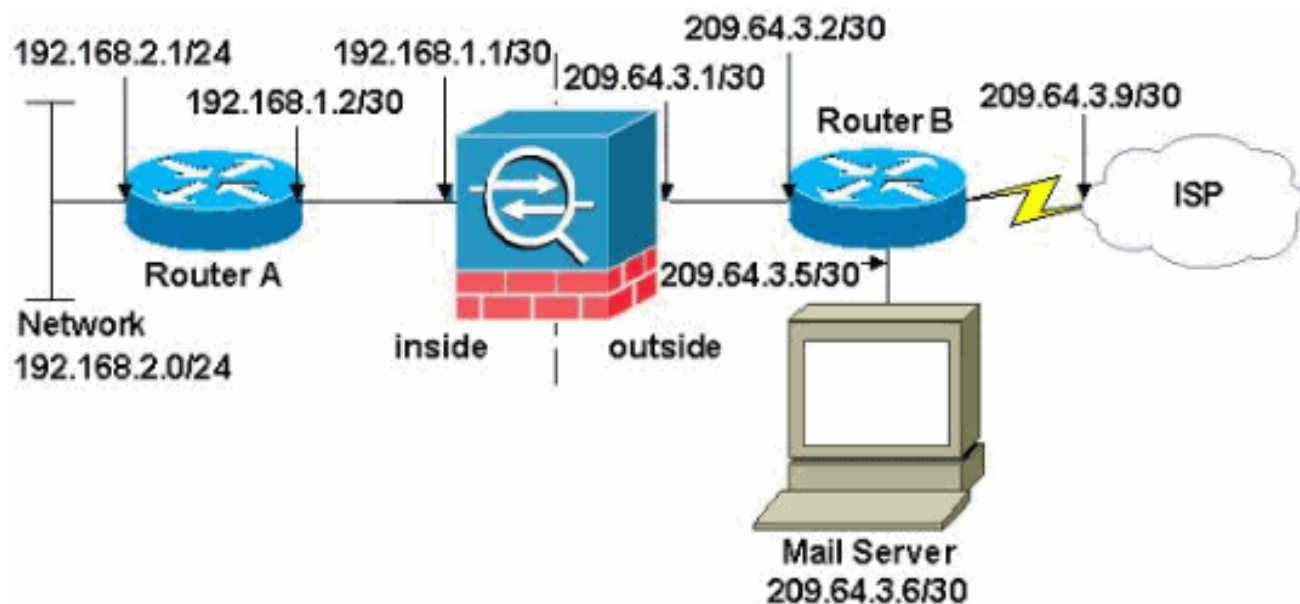
## Configuration

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

**Remarque** : utilisez [Cisco CLI Analyzer](#) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## 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 (192.168.1.0/30) et le réseau externe (209.64.3.0/30). Le serveur de messagerie dont l'adresse IP est 209.64.3.6 se trouve sur le réseau externe. Configurez l'instruction NAT de sorte que tout trafic provenant du réseau 192.168.2.x qui passe de l'interface interne (Ethernet0) à l'interface externe

(Ethernet 1) se traduit par une adresse comprise entre 209.64.3.129 et 209.64.3.253. La dernière adresse disponible (209.64.3.254) est réservée à la traduction d'adresses de port (PAT) .

## Configurations

Ce document utilise les configurations suivantes :

- [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
```

## 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
```

## Vérification

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

## Dépannage

L'[analyseur CLI de Cisco](#) prend en charge certaines commandes **show**. Utilisez l'analyseur CLI pour afficher une analyse de la sortie de la commande **show**.

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

- [Pare-feu de la gamme Cisco ASA 5500-X](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)