

ASA 8.3 et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie (SMTP) sur la zone DMZ

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration ASA](#)

[Configuration TLS ESMTP](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

Introduction

Cet exemple de configuration montre comment configurer l'appliance de sécurité ASA pour l'accès à un serveur SMTP (Simple Mail Transfer Protocol) situé sur le réseau DMZ (Demilitarized Zone).

Référez-vous à [ASA 8.3 et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie \(SMTP\) sur le réseau interne](#) 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 interne.

Référez-vous à [ASA 8.3 et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie \(SMTP\) sur le réseau externe](#) 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 externe.

Référez-vous à [PIX/ASA 7.x et versions ultérieures : Exemple de configuration de l'accès au serveur de messagerie \(SMTP\) sur DMZ](#) pour une configuration identique sur Cisco Adaptive Security Appliance (ASA) 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 :

- 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.

Conventions

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

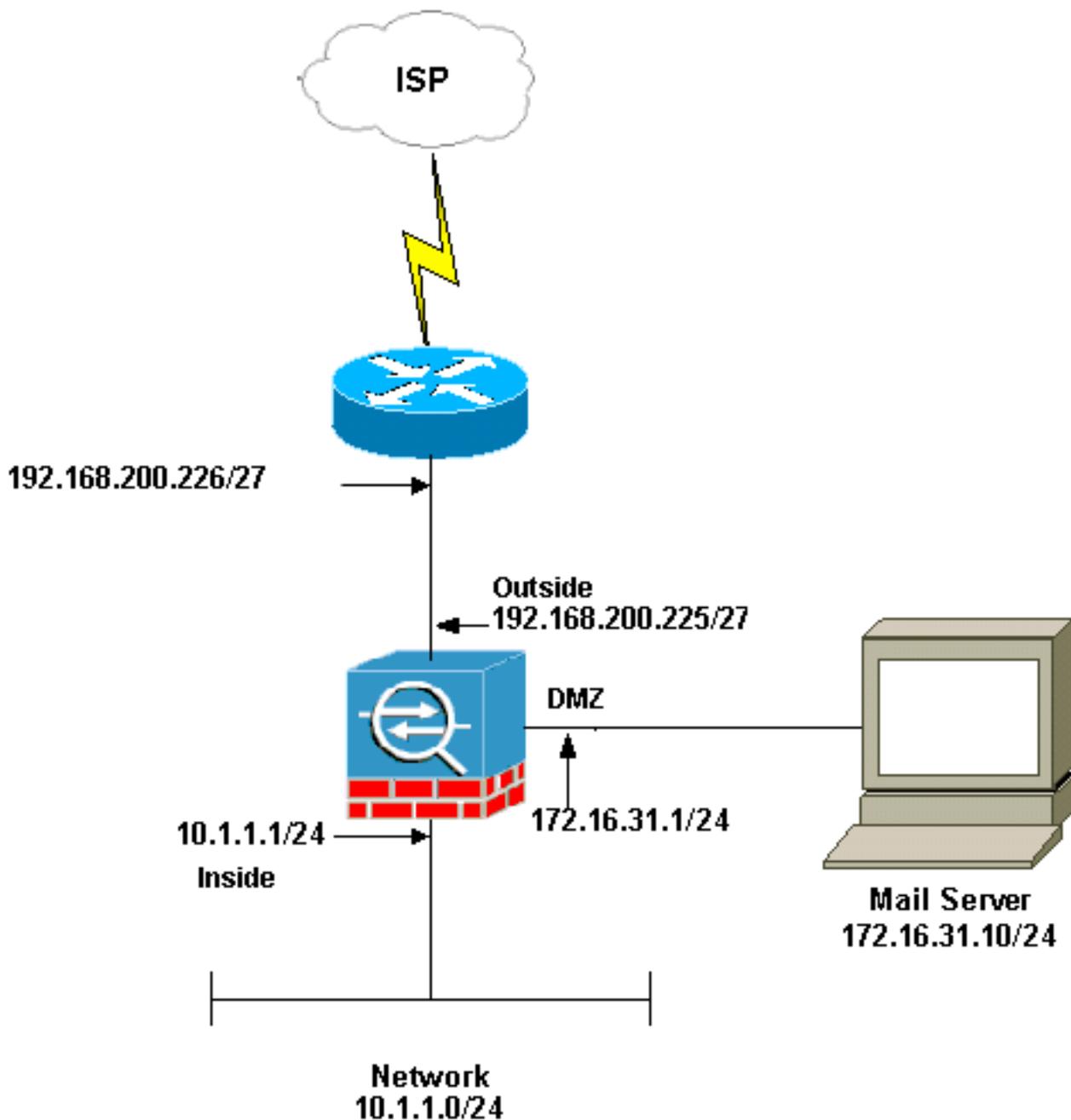
Configuration

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) 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 (10.1.1.0/24) et le réseau externe (192.168.200.0/27). Le serveur de messagerie dont l'adresse IP est 172.16.31.10 se trouve dans le réseau DMZ (Zone démilitarisée). Pour que le serveur de messagerie soit accessible par l'intérieur, les utilisateurs configurent la NAT d'identité. Configurez une liste d'accès, qui est **dmz_int** dans cet exemple, afin d'autoriser les connexions SMTP sortantes du serveur de messagerie aux hôtes du réseau interne et de les lier à l'interface DMZ.

De même, pour que les utilisateurs externes accèdent au serveur de messagerie, configurez une NAT statique et également une liste d'accès, qui est **outside_int** dans cet exemple, afin de permettre aux utilisateurs externes d'accéder au serveur de messagerie et de lier cette liste d'accès à l'interface externe.

[Configuration ASA](#)

Ce document utilise la configuration suivante :

Configuration 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
 security-level 0
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 no nameif
 no security-level
 no ip address
!
!--- Configure the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host 192.168.200.227 eq smtp
!--- Allows outgoing SMTP connections. !--- This access
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400

object network obj-192.168.200.228-192.168.200.253
 range 192.168.200.228-192.168.200.253
object network obj-192.168.200.254
 host 192.168.200.254
```

```

object-group network nat-pat-group
  network-object object obj-192.168.200.228-
192.168.200.253
  network-object object obj-192.168.200.254

object network obj-10.1.1.0
  subnet 10.1.1.0 255.255.255.0
  nat (inside,outside) dynamic nat-pat-group

!--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
  subnet 10.1.1.0 255.255.255.0
  nat (inside,dmz) static obj-10.1.1.0

!--- This network static uses address translation. !---
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
  host 172.16.31.10
  nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0 192.168.200.226 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
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.

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
!
!--- The inspect esmtp command (included in the map)

```

```
allows !--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]
```

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](#) (clients [enregistrés](#) uniquement) 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

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- [debug icmp trace](#) - Indique si les requêtes ICMP (Internet Control Message Protocol) des hôtes atteignent l'ASA. Vous devez ajouter la commande **access-list** afin d'autoriser ICMP dans votre configuration afin d'exécuter ce débogage. **Remarque :** Afin d'utiliser ce débogage, assurez-vous d'autoriser ICMP dans la liste d'accès `outside_int` comme le montre ce résultat :

```
access-list outside_int extended permit tcp any host 192.168.200.227 eq smtp
access-list outside_int extended permit icmp any any
```

- [logging buffered 7](#) - Utilisé en mode de configuration globale pour permettre au dispositif de sécurité adaptatif d'envoyer des messages syslog dans la mémoire tampon du journal. Le contenu de la mémoire tampon du journal ASA peut être vu à l'aide de la commande [show logging](#).

Référez-vous à [Configurer Syslog à l'aide d'ASDM](#) pour plus d'informations sur la configuration de la journalisation.

Informations connexes

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