

ASA 8.3(x) : Exemple de configuration de la connexion de trois réseaux internes à Internet

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration ASA 8.3](#)

[ASA 8.3 et versions ultérieures](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit des informations sur la façon de configurer l'appliance de sécurité adaptative (ASA) Cisco avec la version 8.3(1) pour une utilisation avec trois réseaux internes. Des routes statiques sont utilisées sur les routeurs pour simplifier l'exemple.

Reportez-vous à la section [PIX/ASA : Exemple de configuration de la connexion de trois réseaux internes à Internet](#) pour la même configuration 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 de ce document sont basées sur l'appliance de sécurité adaptative (ASA) Cisco avec la version 8.3(1).

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a

cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

[Conventions](#)

Référez-vous à [Conventions des conseils techniques Cisco](#) pour plus d'informations sur les conventions du document.

[Configuration](#)

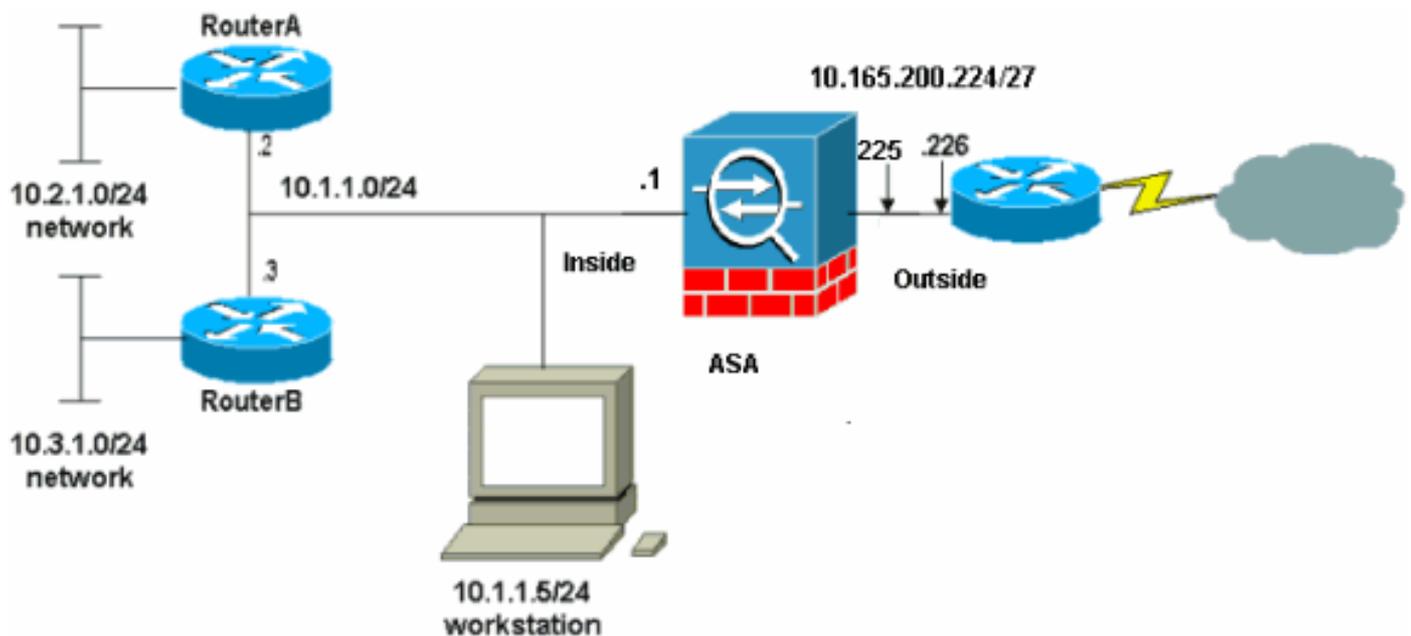
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

[Diagramme du réseau](#)

Ce document utilise cette configuration du réseau.

Remarque : la passerelle par défaut des hôtes du réseau 10.1.1.0 pointe vers le routeur A. Une route par défaut sur RouterB est ajoutée qui pointe vers RouterA. Le routeur A dispose d'une route par défaut qui pointe vers l'interface interne ASA.



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](#).

[Configuration ASA 8.3](#)

Ce document utilise les configurations suivantes.

Si vous disposez de la sortie d'une commande **write terminal** de votre périphérique Cisco, vous

[pouvez utiliser l'Outil Interpréteur de sortie \(clients inscrits uniquement\) pour afficher les problèmes potentiels ainsi que les correctifs.](#)

- [Configuration du routeur A](#)
- [Configuration du routeur B](#)
- [ASA 8.3 et versions ultérieures](#)

Configuration du routeur A

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
```

```
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

Configuration du routeur B

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
```

```
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA 8.3 et versions ultérieures

Remarque : les commandes non par défaut sont indiquées en **gras**.

Configuration en cours pour ASA 8.3(1)

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.165.200.225 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa831-k8.bin

ftp mode passive

!--- Output Suppressed !--- Creates an object called
OBJ_GENERIC_ALL. !--- Any host IP not already matching
another configured !--- object will get PAT to the
outside interface IP !--- on the ASA (or 10.165.200.226)
for internet bound traffic. object network
OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface

!--- Output Suppressed !--- Define a default route to
the ISP router. route outside 0.0.0.0 0.0.0.0
10.165.200.226 1

!--- Define a route to the INTERNAL router with network
10.2.1.0. route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network
10.3.1.0. route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

Remarque : Pour plus d'informations sur la configuration de NAT et PAT sur ASA 8.3, référez-vous à [Informations sur NAT](#).

Pour plus d'informations sur la configuration des listes d'accès sur PIX/ASA, référez-vous à [PIX/ASA 7.x : Redirection \(transfert\) de port avec les commandes nat, global, static et access-list](#).

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.

Remarque : Pour plus d'informations sur le dépannage de PIX/ASA, référez-vous à [Dépannage des connexions via PIX et ASA](#).

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**.

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug icmp trace** Indique si les requêtes ICMP des hôtes atteignent le PIX. Vous devez ajouter la commande **access-list** pour autoriser ICMP dans votre configuration afin d'exécuter ce débogage.
- **logging buffer debugging** Montre les connexions établies et refusées aux hôtes qui passent par le PIX. Les informations sont stockées dans la mémoire tampon du journal PIX et la sortie peut être vue à l'aide de la commande **show log**.

Référez-vous à [Configuration du Syslog PIX](#) pour plus d'informations sur la configuration de la journalisation.

Informations connexes

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