

Exemple de configuration de la connexion de trois réseaux internes à ASA version 9.x avec Internet

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration ASA 9.1](#)

[Configurations](#)

[Vérification](#)

[Connexion](#)

[Syslog](#)

[Traductions NAT](#)

[Dépannage](#)

[Packet Tracer](#)

[Saisir](#)

Introduction

Ce document fournit des informations sur la configuration de l'appareil de sécurité adaptative Cisco (ASA) version 9.1(5) pour une utilisation avec trois réseaux internes. Des routes statiques sont utilisées sur les routeurs pour simplifier l'exemple.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur la version 9.1(5) de Cisco Adaptive Security Appliance (ASA).

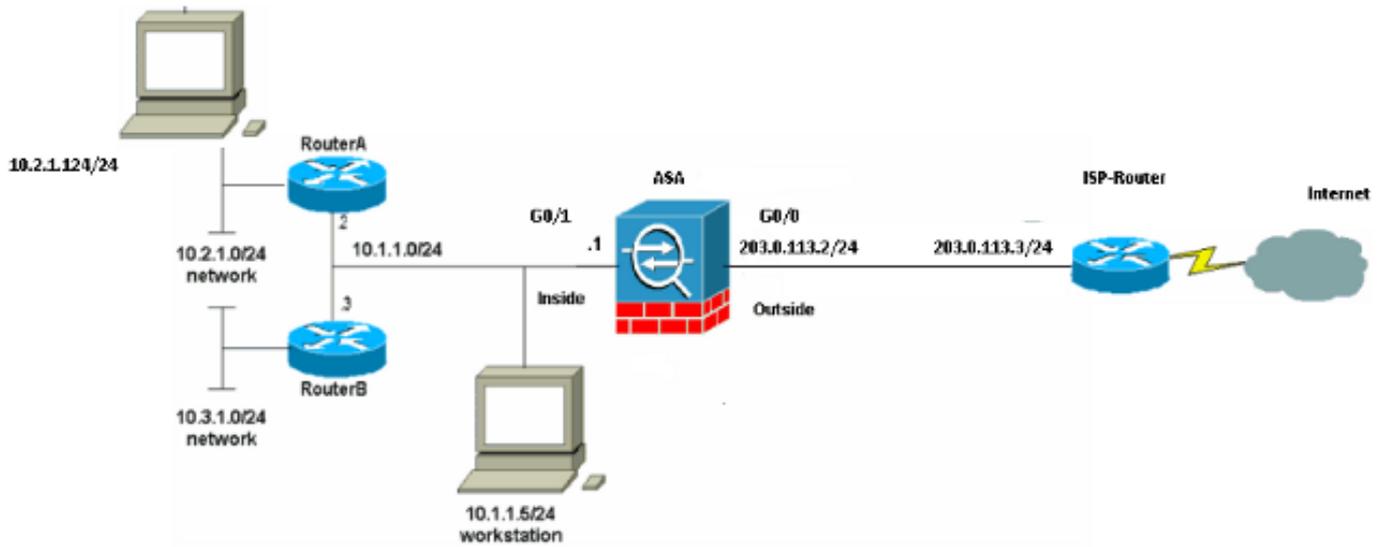
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

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

Note: Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\)](#) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



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

Configuration ASA 9.1

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.

Configurations

- [Configuration du routeur A](#)
- [Configuration du routeur B](#)
- [Configuration ASA version 9.1 et ultérieure](#)

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#

Configuration ASA version 9.1 et ultérieure

ASA#**show run**

```
: Saved  
:  
ASA Version 9.1(5)  
!  
hostname ASA  
enable password 8Ry2YjIyt7RRXU24 encrypted  
passwd 2KFQnbNIdI.2KYOU encrypted  
names  
!  
interface GigabitEthernet0/0  
nameif outside  
security-level 0
```

```
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- 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 0.0.0.0 203.0.113.3 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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Essayez d'accéder à un site Web via HTTP à l'aide d'un navigateur Web. Cet exemple utilise un site hébergé à l'adresse 198.51.100.100. Si la connexion réussit, cette sortie peut être vue sur l'interface de ligne de commande ASA.

Connexion

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
flags UIO
```

L'ASA est un pare-feu dynamique et le trafic de retour du serveur Web est autorisé à revenir par le pare-feu car il correspond à une *connexion* dans la table de connexion du pare-feu. Le trafic qui correspond à une connexion qui existe déjà est autorisé par le pare-feu et n'est pas bloqué par une liste de contrôle d'accès d'interface.

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte 198.51.100.100 à partir de l'interface externe. Cette connexion se fait avec le protocole TCP et est inactive depuis six secondes. Les indicateurs de connexion précisent l'état actuel de la connexion. Vous trouverez plus d'informations sur les indicateurs de connexion dans [les indicateurs de connexion TCP ASA](#).

Syslog

```
ASA(config)# show log | include 10.2.1.124
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

Le pare-feu de l'ASA génère des SYSLOG pendant le fonctionnement normal. Les SYSLOG varient en verbosité selon la configuration de la journalisation. Le résultat montre deux Syslogs qui sont vus au niveau 6, ou 'informationnel'.

Dans cet exemple, deux SYSLOG sont générés. Le premier est un message de journal qui indique que le pare-feu a construit une traduction, en particulier une traduction TCP dynamique (PAT). Il indique l'adresse IP source et le port, ainsi que l'adresse IP et le port traduits lorsque le trafic traverse de l'intérieur vers l'extérieur.

Le deuxième SYSLOG indique que le pare-feu a établi une connexion dans sa table de connexions précisément pour ce trafic, entre le client et le serveur. Si le pare-feu a été configuré afin de bloquer cette tentative de connexion, ou si un autre facteur a empêché la création de cette connexion (contraintes de ressources ou une éventuelle erreur de configuration), le pare-feu ne génère pas de journal indiquant que la connexion a été créée. Au lieu de cela, il consigne une raison pour laquelle la connexion est refusée ou une indication sur le facteur qui empêche la création de la connexion.

Traductions NAT

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

Dans le cadre de cette configuration, la PAT est configurée afin de traduire les adresses IP d'hôte internes en adresses routables sur Internet. Afin de confirmer que ces traductions sont créées, vous pouvez vérifier la table des traductions NAT (xlate). La commande **show xlate**, lorsqu'elle est

associée au mot clé **local** et à l'adresse IP de l'hôte interne, affiche toutes les entrées présentes dans la table de traduction de cet hôte. La sortie précédente montre qu'une traduction est actuellement créée pour cet hôte entre les interfaces interne et externe. L'adresse IP et le port de l'hôte interne sont traduits en l'adresse 203.0.113.2 selon notre configuration. Les indicateurs listés, **r i**, indiquent que la traduction est **dynamique** et une **portmap**. Vous trouverez plus d'informations sur les différentes configurations NAT dans [Informations sur NAT](#).

Dépannage

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

L'ASA fournit plusieurs outils pour dépanner la connectivité. Si le problème persiste après que vous ayez vérifié la configuration et vérifié le résultat indiqué précédemment, ces outils et techniques peuvent vous aider à déterminer la cause de votre échec de connectivité.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 1234 198.51.100.100 80
```

```
--Omitted--
```

```
Result:
```

```
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La fonctionnalité Packet Tracer de l'ASA vous permet de spécifier un paquet simulé et de voir toutes les étapes, vérifications et fonctions que le pare-feu traverse lorsqu'il traite le trafic. Avec cet outil, il est utile d'identifier un exemple de trafic que vous croyez être autorisé à traverser le pare-feu, et d'utiliser ce 5-tupple afin de simuler le trafic. Dans l'exemple précédent, Packet Tracer est utilisé pour simuler une tentative de connexion qui répond aux critères suivants :

- Le paquet simulé arrive à l'intérieur.
- Le protocole utilisé est **TCP**.
- L'adresse IP du client simulé est 10.2.1.124.
- Le client envoie le trafic provenant du port **1234**.
- Le trafic est destiné à un serveur ayant l'adresse IP 198.51.100.100.
- Le trafic est destiné au port 80.

Notez qu'il n'y a pas eu de mention de l'interface **externe** dans la commande. C'est par conception Packet Tracer. L'outil vous indique comment le pare-feu traite ce type de tentative de connexion et indiquera comment il l'acheminera et à partir de quelle interface. Vous trouverez plus d'informations sur packet tracer dans [Tracing Packets with Packet Tracer](#).

Saisir

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
```

```
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA# show capture capin
```

```
3 packets captured
```

```
1: 11:31:23.432655      10.2.1.124.18711 > 198.51.100.100.80: S 780523448:  
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>  
2: 11:31:23.712518      198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:  
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>  
3: 11:31:23.712884      10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068  
win 32768
```

```
ASA# show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869      203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:  
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>  
2: 11:31:23.712472      198.51.100.100.80 > 203.0.113.2.18711: S 95714629:  
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>  
3: 11:31:23.712914      203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630  
win 32768/pre>
```

Le pare-feu ASA peut capturer le trafic entrant ou sortant de ses interfaces. Cette fonctionnalité de capture est fantastique car elle peut prouver de manière définitive si le trafic arrive à un pare-feu ou s'il en sort. L'exemple précédent montre la configuration de deux captures nommées **capin** et **capout** respectivement sur les interfaces interne et externe. Les commandes de capture ont utilisé le mot clé **match**, qui vous permet d'être précis sur le trafic que vous voulez capturer.

Pour la **chaîne** de capture, il a été indiqué que vous vouliez faire correspondre le trafic vu sur l'interface interne (entrée ou sortie) qui correspond à l'**hôte tcp 10.2.1.124** **hôte 198.51.100.100**. En d'autres termes, vous voulez capturer tout trafic TCP qui est envoyé de l'**hôte 10.2.1.124** à l'**hôte 198.51.100.100** ou **vice versa**. L'utilisation du mot-clé **match** permet au pare-feu de capter ce trafic dans les deux sens. La commande capture définie pour l'interface externe ne fait pas référence à l'adresse IP du client interne, car le pare-feu effectue la PAT sur cette adresse IP du client. Par conséquent, vous ne pouvez pas associer cette adresse IP au client. Plutôt, cet exemple utilise **any** pour indiquer que toutes les adresses IP possibles correspondent à cette condition.

Après avoir configuré les captures, vous essayez de rétablir une connexion et de les afficher à l'aide de la commande **show capture <capture_name>**. Dans cet exemple, vous pouvez voir que le client a été en mesure de se connecter au serveur comme le montre la connexion TCP en trois étapes vue dans les captures.