L'ASA libèrent 9.(x) la connexion de trois réseaux internes avec l'exemple de configuration d'Internet

Contenu

Introduction

Ce document fournit des informations sur la façon dont installer la version 9.1(5) de l'appliance de sécurité adaptable Cisco (ASA) pour l'usage 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.

Composants utilisés

Les informations dans ce document sont basées sur la version 9.1(5) de l'appliance de sécurité adaptable Cisco (ASA).

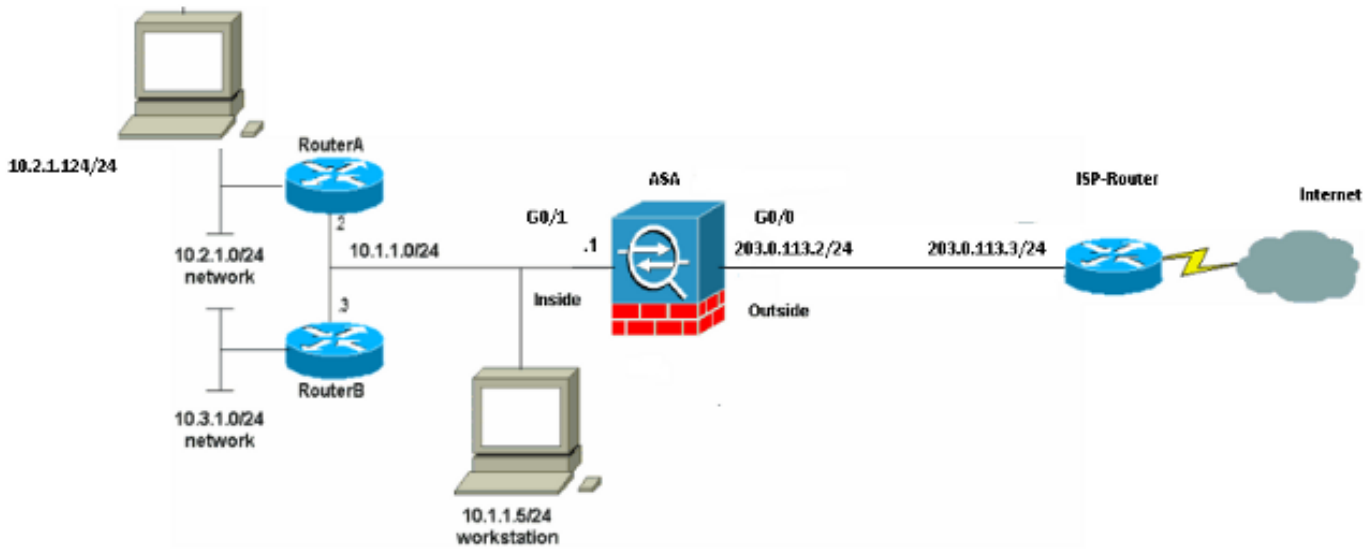
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

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

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés 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
- Révision 9.1 ASA et configuration plus récente

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#
```

Révision 9.1 ASA et configuration plus récente

```
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
```

Vérifiez

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

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Essayez d'accéder à un site Web par l'intermédiaire du HTTP avec un web browser. Cet exemple utilise un site qui est hébergé chez 198.51.100.100. Si la connexion est réussie, cette sortie peut être vue sur l'ASA CLI.

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 web server est permis de retour par le Pare-feu parce qu'il apparie une ***connexion*** dans la table de connexion de Pare-feu. Trafiquez qu'apparie une connexion qui préexiste est autorisée par le Pare-feu et n'est pas bloquée par un ACL d'interface.

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte de 198.51.100.100 hors fonction de l'interface extérieure. Ce rapport est établi avec le protocole TCP et a été de veille pendant six secondes. Les indicateurs de connexion indiquent l'état actuel de cette connexion. Plus d'informations sur des indicateurs de connexion peuvent être trouvées dans des 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 ASA génère des Syslog pendant le fonctionnement normal. Les Syslog s'étendent dans la verbosité basée sur la configuration de journalisation. La sortie affiche deux Syslog qui sont vus au niveau six, ou de niveau « informationnel ».

Dans cet exemple, il y a deux Syslog générés. Le premier est un message de log qui indique que le Pare-feu a établi une traduction, spécifiquement une traduction dynamique de TCP (PAT). Il indique l'adresse IP source et le port et l'adresse IP et le port traduits pendant que le trafic traverse de l'intérieur aux interfaces extérieures.

Le deuxième Syslog indique que le Pare-feu a établi une connexion dans sa table de connexion pour ce trafic spécifique entre le client et serveur. Si le Pare-feu était configuré afin de bloquer cette tentative de connexion, ou un autre facteur empêchait la création de cette connexion (des contraintes de ressource ou une mauvaise configuration possible), le Pare-feu ne génèrerait pas un log qui indique que la connexion a été établie. Au lieu de cela il se connecterait une raison pour que la connexion soit refusée ou une indication au sujet de quel facteur a empêché la connexion de l'création.

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
```

En tant qu'élément de cette configuration, PAT est configuré afin de traduire les adresses IP internes d'hôte aux adresses qui sont routable sur l'Internet. Afin de confirmer que ces traductions sont créées, vous pouvez vérifier la table de traductions NAT (xlate). **Le show xlate de**

commande, une fois combiné avec le mot clé **local** et l'adresse IP interne de l'hôte, affiche toutes les entrées actuelles dans la table de traduction pour cet hôte. La sortie précédente prouve qu'il y a une traduction actuellement établie pour cet hôte entre les interfaces internes et externes. L'IP d'hôte interne et le port sont traduits à l'adresse de 203.0.113.2 par notre configuration. Les indicateurs les ont répertorié, r i, indiquent que la traduction est **dynamique** et un **portmap**. Plus d'informations sur différentes configurations NAT peuvent être trouvées dans les informations sur NAT.

Dépannez

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

L'ASA fournit les plusieurs outils avec lesquels pour dépanner la Connectivité. Si la question persiste après que vous vérifiiez la configuration et vérifiiez la sortie répertoriée précédemment, ces techniques et outil pourraient aider à déterminer la cause de votre panne 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 de traceur de paquet sur l'ASA te permet pour spécifier un paquet simulé et pour voir tous les divers étapes, contrôles, et fonctions par lesquelles le Pare-feu passe quand il traite le trafic. Avec cet outil, il est utile d'identifier un exemple du trafic que vous croyez devriez être laissé traverser le Pare-feu, et l'utilise que 5-tupple afin de simuler le trafic. Dans l'exemple précédent, le traceur de paquet est utilisé afin de simuler une tentative de connexion qui répond à ces critères :

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

Notez qu'il n'y avait aucune mention de l'interface **dehors** dans la commande. C'est par conception de traceur de paquet. L'outil vous indique comment les processus de Pare-feu qui type de tentative de connexion, qui inclut comment elle la conduirait, et hors de quelle interface. Plus d'informations sur le traceur de paquet peuvent être trouvées en paquets de suivi avec Packet Tracer.

Capture

```
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 qui écrit ou laisse ses interfaces. Cette fonctionnalité de capture est fantastique parce qu'elle peut définitivement prouver si le trafic arrive à, ou des feuilles de, un Pare-feu. L'exemple précédent a affiché la configuration de deux captures nommées **capin** et **capout** sur les interfaces internes et externes respectivement. Les ordres de capture ont utilisé le mot clé de **correspondance**, qui te permet pour être spécifique au sujet de quel trafic vous voulez capturer.

Pour le **capin de** capture**,** on l'a indiqué que vous avez voulu apparier le trafic vu sur l'interface interne (d'entrée ou de sortie) cet **hôte 198.51.100.100 de 10.2.1.124 d'hôte de TCP de** correspondances. En d'autres termes, vous voulez capturer n'importe quel trafic TCP qui est envoyé de l'**hôte 10.2.1.124 pour héberger 198.51.100.100** ou **vice versa**. L'utilisation du mot clé de **correspondance** permet au Pare-feu pour capturer ce trafic bidirectionnel. L'ordre de capture défini pour l'interface extérieure ne met pas en référence l'adresse IP de client interne parce que les attitudes PAT de Pare-feu sur cette adresse IP de client. En conséquence, vous ne pouvez pas **être assortie** avec cette adresse IP de client. Au lieu de cela, cet exemple en emploie afin d'indiquer que toutes les adresses IP possibles apparieraient cette condition.

Après que vous configuriez les captures, vous tenteriez alors d'établir une connexion de nouveau, et poursuivez pour visualiser les captures avec la commande de ***<capture_name> de show capture***. Dans cet exemple, vous pouvez voir que le client pouvait se connecter au serveur comme évident par la prise de contact à trois voies de TCP vue dans les captures.