Configurer l’ASA pour les réseaux internes doubles

Contenu

Introduction

Ce document décrit comment configurer un appareil de sécurité adaptable Cisco (ASA) qui exécute la version 9.x du logiciel afin que soient utilisés deux réseaux internes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

D’ailleurs, l’information contenue ici repose sur cette version.

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.

Informations générales

Lorsque vous ajoutez un deuxième réseau interne derrière le pare-feu d'un ASA, prenez en compte ces renseignements importants :

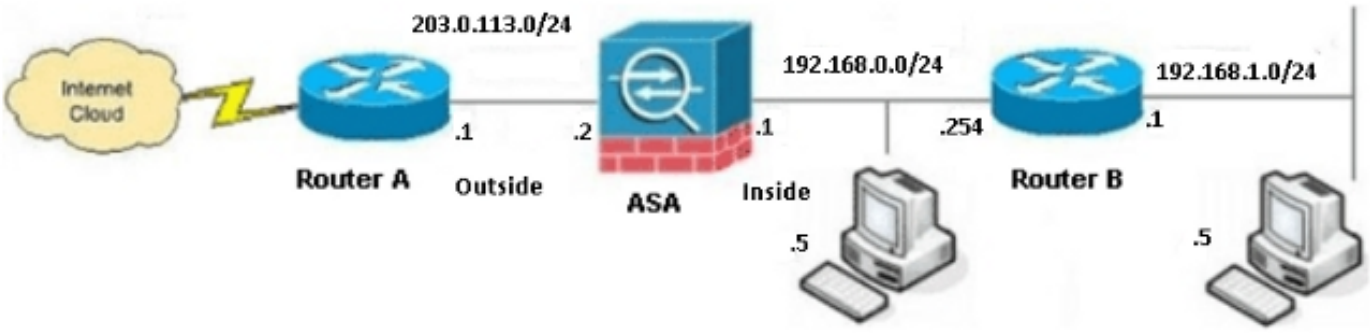
- L'ASA ne prend pas en charge les adresses secondaires.
- Un routeur doit être utilisé derrière l'ASA pour réaliser le routage entre le réseau actuel et le réseau nouvellement ajouté.
- La passerelle par défaut pour tous les hôtes doit pointer vers le routeur interne.
- Vous devez ajouter un routage par défaut sur le routeur interne qui est orienté vers l'ASA.
- Vous devez effacer le cache ARP (Address Resolution Protocol) du routeur interne.

Configuration

Utilisez les renseignements décrits dans la présente section pour configurer l'ASA.

Diagramme du réseau

Voici la topologie utilisée dans les exemples du présent document :



Note: Les schémas des adresses IP utilisés dans cette configuration ne peuvent pas être routés légalement sur Internet. Ce sont des adresses RFC 1918 qui sont utilisées dans un environnement de laboratoire.

Configuration de l'ASA 9.x

Si vous obtenez le résultat de la commande **write terminal** de votre périphérique Cisco, vous pouvez utiliser l'outil interpréteur de sortie (clients inscrits seulement) pour afficher les problèmes éventuels et les correctifs.

Voici la configuration pour l'ASA qui exécute la version logicielle 9.x :

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

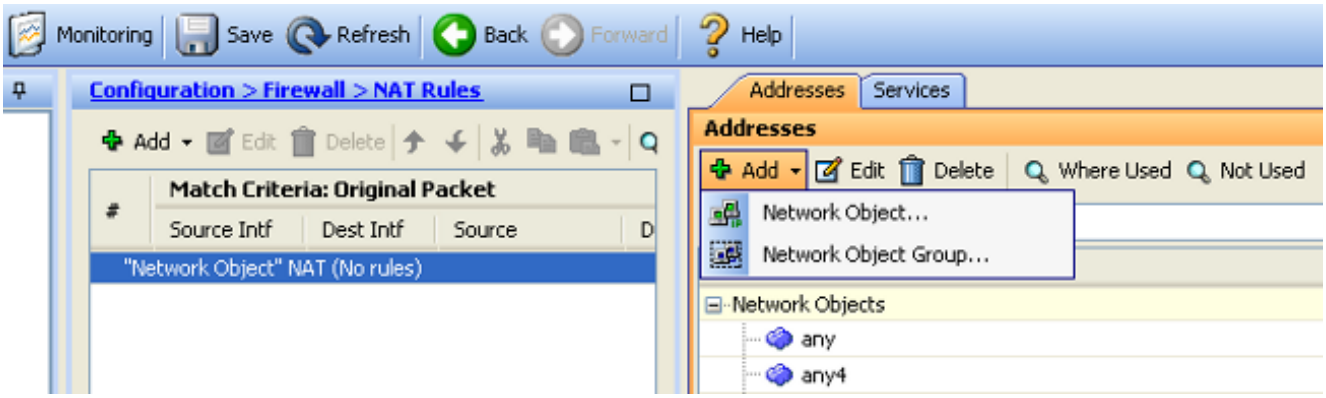
```
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
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
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Autoriser les hôtes internes à accéder aux réseaux externes avec PAT

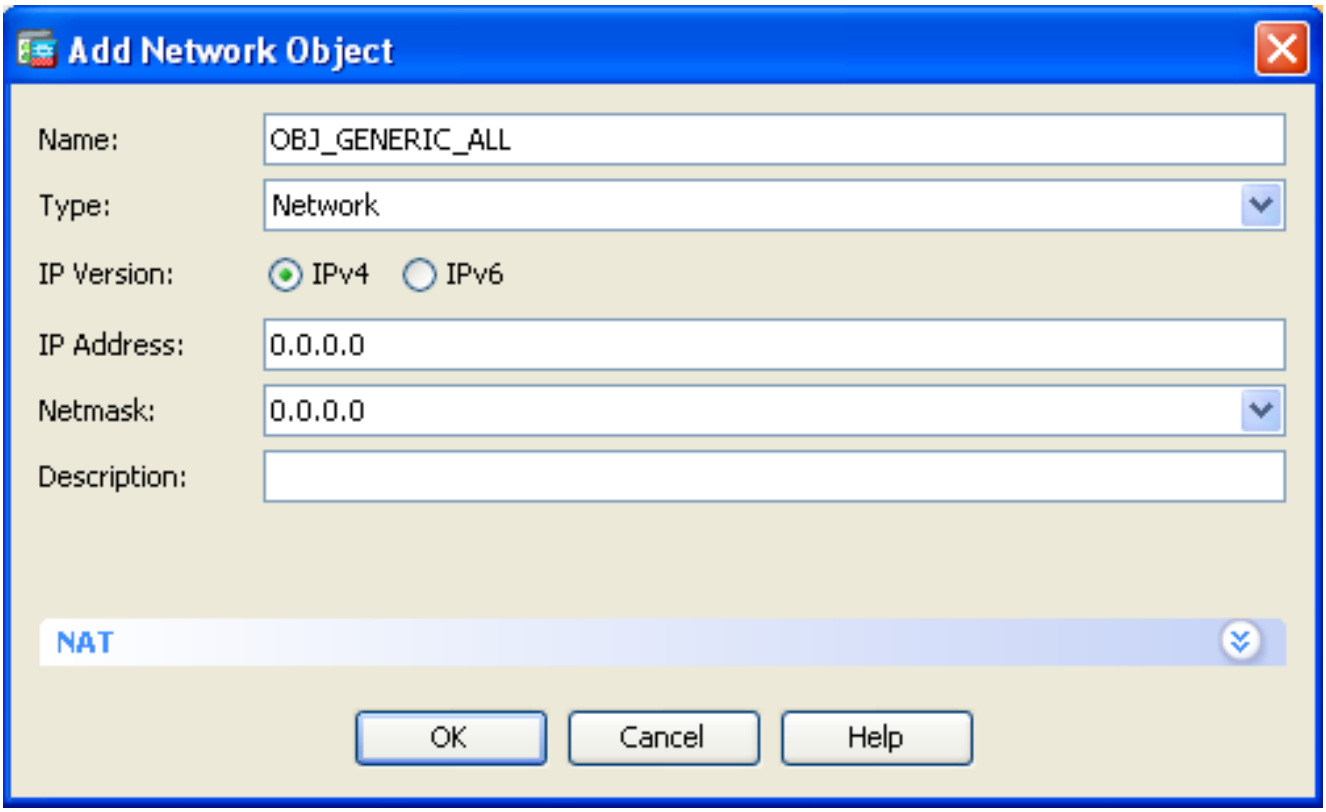
Si vous souhaitez que les hôtes internes partagent une seule adresse publique pour la traduction, utilisez la traduction d'adresses de port (PAT). Une des configurations PAT les plus simples implique la traduction de tous les hôtes internes, de sorte que ceux-ci semblent être l'adresse IP de l'interface externe. Il s'agit de la configuration PAT type, qui est utilisée lorsque le nombre d'adresses IP routables disponibles auprès du fournisseur de services Internet est limité à quelques-unes ou à une seule.

Suivez ces étapes pour permettre aux hôtes internes d'accéder aux réseaux externes avec la PAT :

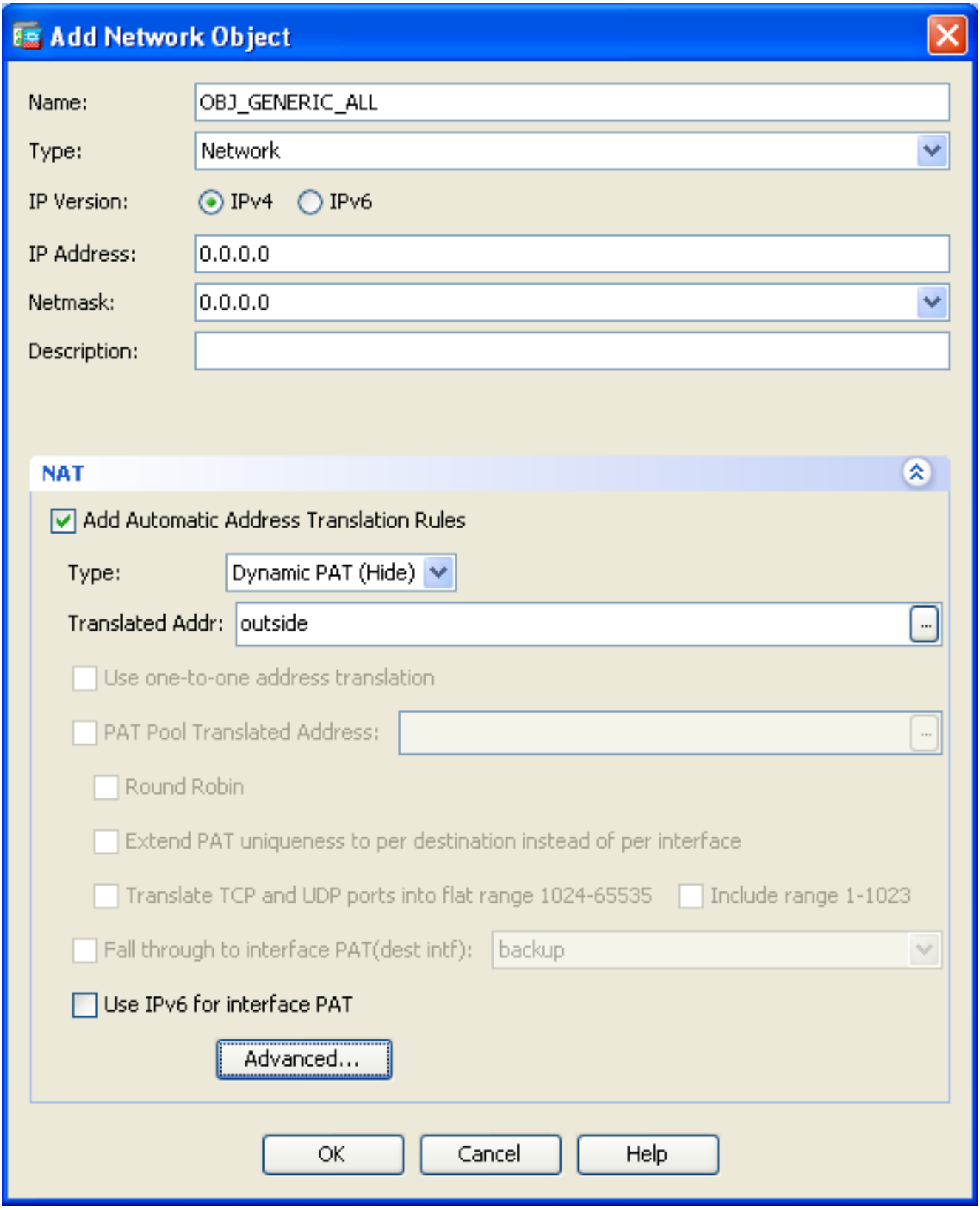
1. Allez à **Configuration > Firewall > NAT Rules**, puis cliquez sur **Add** et **Network Object** pour configurer une règle NAT dynamique :



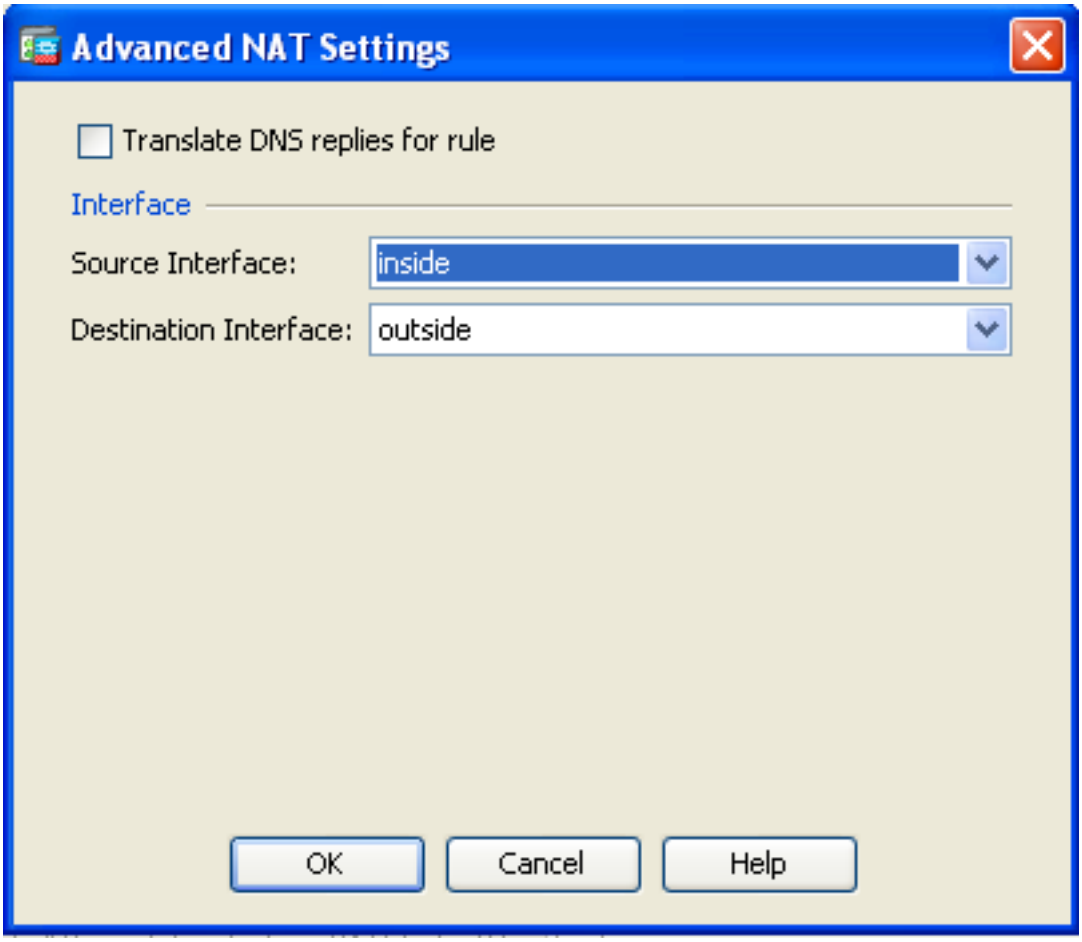
2. Configurez le réseau, l'hôte ou la plage exigeant la PAT dynamique. Dans cet exemple, tous les sous-réseaux internes ont été sélectionnés. Idéalement, ce processus serait répété pour les sous-réseaux donnés que vous souhaitez traduire de cette manière :



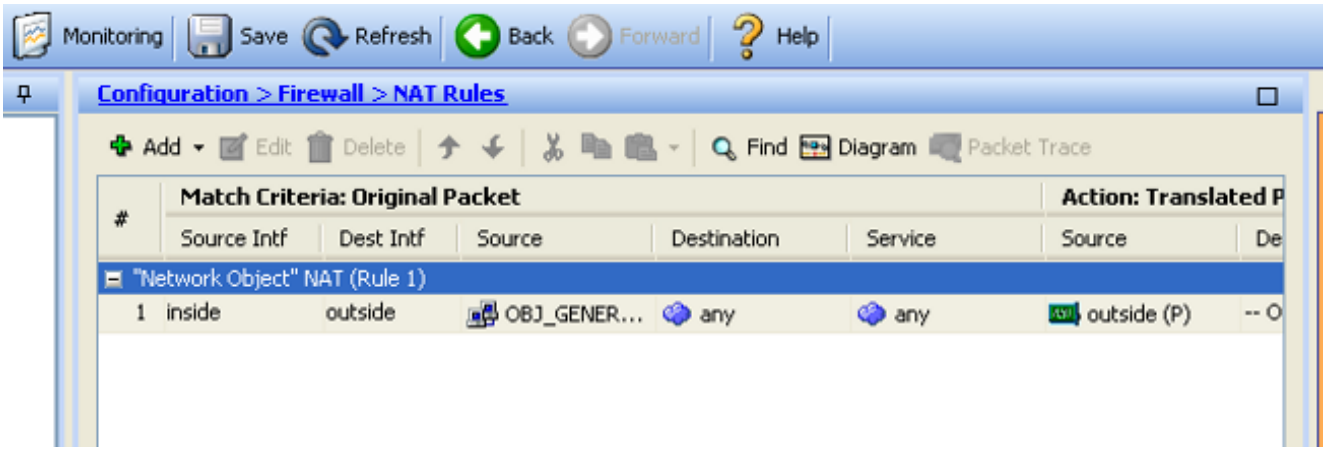
3. Cliquez sur **NAT**, cochez la case **Add Automatic Address Translation Rule**, entrez **Dynamic**, puis définissez l'option **Translated Addr** de manière à tenir compte de l'interface externe. Si vous cliquez sur les points de suspension, vous obtiendrez de l'aide pour sélectionner un objet préconfiguré, comme l'interface externe :



4. Cliquez sur **Avanced** pour sélectionner une interface de source et une interface de destination :



5. Cliquez sur **OK**, puis cliquez sur **Apply** pour appliquer les modifications. Par la suite, le gestionnaire des appareils de sécurité adaptatifs (ASDM) affiche la règle NAT :



Configuration du routeur B

Voici la configuration pour le routeur B :

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Vérification

Accédez à un site Web par HTTP au moyen d'un navigateur Web pour vérifier que votre configuration fonctionne correctement.

Dans cet exemple est utilisé un site hébergé à l'adresse IP *198.51.100.100*. Si la connexion est réussie, les sorties illustrées dans les sections suivantes peuvent être vues sur la CLI de l'ASA.

Connexion

Saisissez la commande **show connection address** pour vérifier la connexion :

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
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 correspondant à une connexion préexistante est autorisé à traverser le pare-feu sans qu'une ACL d'interface le bloque.

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.

> **Note**: Consultez le document Cisco sur les indicateurs de connexion TCP de l'ASA (montage et démontage de la connexion) pour en savoir plus sur les indicateurs de connexion.

Dépannage

Les renseignements de la présente section vous aideront à régler vos problèmes de configuration.

SYSLOG

Saisissez la commande **show log** pour visualiser les journaux du système (SYSLOG) :

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

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:192.168.1.5/58799 (203.0.113.2/58799)
```

Le pare-feu de l'ASA génère des SYSLOG pendant le fonctionnement normal. Les SYSLOG varient en verbosité selon la configuration de la journalisation. La sortie affiche deux SYSLOG qui sont vus au niveau six ou au niveau *informationnel*.

Dans cet exemple, deux SYSLOG sont générés. Le premier constitue un message de journalisation qui indique que le pare-feu a produit une traduction; particulièrement, 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 passe de l'interface interne à l'interface externe.

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 pour bloquer cette connexion, ou si un autre facteur a empêché l'établissement de la connexion (contraintes de ressources ou erreur de configuration), le pare-feu ne génère pas de journal pour indiquer que la connexion a été établie. Plutôt, il consigne un motif expliquant le refus de la connexion ou précise le facteur qui a empêché la connexion.

Packet Tracer

Saisissez cette commande pour activer la fonctionnalité de Packet Tracer :

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 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 Packet Tracer sur l'ASA vous permet de préciser un paquet *simulé* et de voir toutes les différentes étapes, vérifications et fonctions que le pare-feu accomplit quand il traite le trafic. Concernant cet outil, il est utile de trouver un exemple de trafic qui *devrait* à votre sens être autorisé à traverser le pare-feu et d'utiliser ces cinq valeurs pour simuler le trafic. Dans l'exemple précédent, Packet Tracer est utilisé pour simuler une tentative de connexion qui répond aux critères suivants :

- La simulation de paquet arrive sur l'interface interne.
- Le protocole utilisé est TCP.
- L'adresse IP du client simulé est 192.168.1.5.
- 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 avait aucune mention de l'interface externe dans la commande. C'est en raison de la conception de 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.

> **Astuce** : Pour en savoir plus sur la fonctionnalité de Packet Tracer, consultez la section Tracer des paquets avec Packet Tracer du *Guide de configuration de la gamme Cisco ASA 5500 à l'aide des interfaces CLI 8.4 et 8.6*.

Saisir

Entrez ces commandes pour appliquer une capture :

```
ASA# capture capin interface inside match tcp host 192.168.1.5 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 192.168.1.5.58799 > 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 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 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 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Le pare-feu de l'ASA peut capter le trafic qui entre ou sort de ses interfaces. La fonctionnalité de capture est fantastique, car elle peut définitivement démontrer si le trafic entre dans un pare-feu ou en sort. L'exemple précédent montre la configuration de deux captures nommées **capin** et **capout** sur les interfaces interne et externe, respectivement. Les commandes **capture** utilisent le mot-clé **match**, qui vous permet de préciser le trafic à capter.

Pour l'exemple de capture de *capin*, il est indiqué que vous souhaitez associer le trafic vu sur l'interface interne (entrée ou sortie) et qui correspond à *l'hôte TCP 192.168.1.5 à l'hôte TCP 198.51.100.100*. Autrement dit, vous souhaitez capter tout trafic TCP envoyé de *l'hôte 192.168.1.5* à l'hôte *198.51.100.100*, ou inversement. 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 pouvez tenter de rétablir la connexion et d'afficher les captures grâce à la commande **show capture*<capture_name>*** . Dans cet exemple, vous pouvez voir que le client est en mesure de se connecter au serveur, comme en témoigne la prise de contact TCP tridirectionnelle observée dans les captures.

Informations connexes

- Cisco Adaptive Security Device Manager
- Pare-feu de nouvelle génération Cisco ASA 5500-X
- Demandes de commentaires (RFC)
- Guide de configuration de la CLI Cisco ASA 9.0 – Configuration des routes statiques et par défaut

- Documentation et assistance techniques âÂÂ Cisco Systems