Utilisation NAT et de PAT de déclaration sur l'exemple Cisco Secure de configuration de Pare-feu ASA

Contenu

Introduction

Ce document fournit des exemples de Traduction d'adresses de réseau (NAT) de base et des configurations de translation d'adresses d'adresse du port (PAT) sur le Pare-feu Cisco Secure de l'appliance de sécurité adaptable (ASA). Ce document fournit également les schémas de réseau simplifiés. Consultez la documentation ASA pour votre version de logiciel ASA pour plus d'informations détaillées.

Ce document propose une analyse personnalisée de votre périphérique Cisco.

Référez-vous à la configuration NAT sur l'ASA sur le pour en savoir plus d'appareils de Sécurité de gamme 5500/5500-X ASA.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du Pare-feu Cisco Secure ASA.

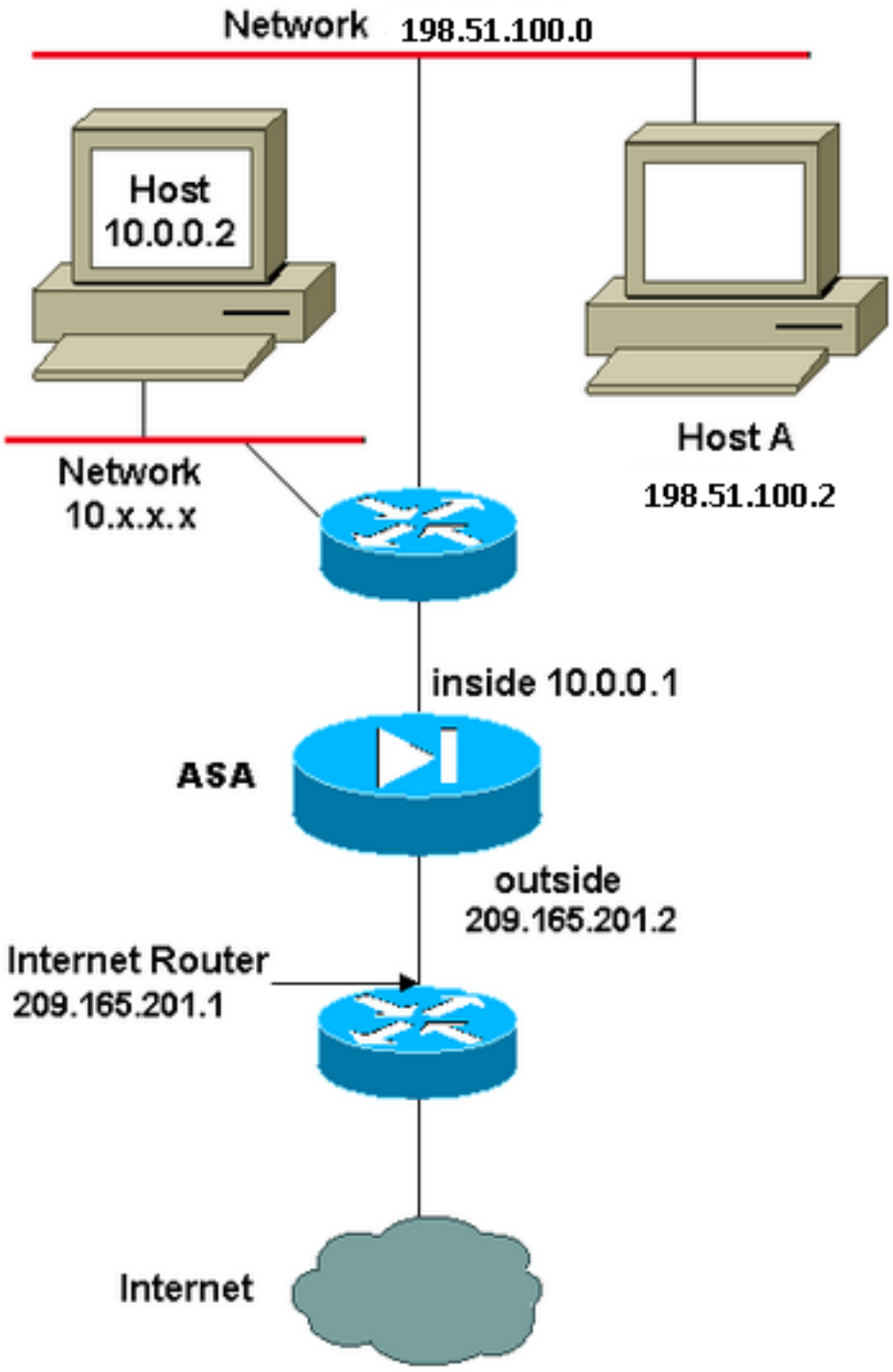
Composants utilisés

Les informations dans ce document sont basées sur la version 8.4.2 et ultérieures Cisco Secure de logiciel pare-feu 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 - Plusieurs déclarations NAT avec manuel et automatique NAT

Diagramme du réseau



Dans cet exemple, le fournisseur d'accès à Internet fournit à l'administrateur réseau un bloc d'adresses IP 209.165.201.0/27 de 209.165.201.1 à 209.165.201.30. Le gestionnaire de réseau décide d'assigner 209.165.201.1 à l'interface interne sur le routeur internet, et 209.165.201.2 à l'interface extérieure de l'ASA.

L'administrateur réseau a déjà une adresse de classe C assignée au réseau, 198.51.100.0/24, et a quelques postes de travail qui emploient ces adresses afin d'accéder à l'Internet. Ces postes de travail n'exigent aucune traduction d'adresses parce qu'ils ont déjà des adresses valides. Cependant, les nouvelles stations de travail ont des adresses attribuées dans le réseau 10.0.0.0/8, et elles doivent être traduites (parce que 10.x.x.x est l'un des espaces d'adresses non routables par RFC 1918 .

Afin de faciliter cette conception de réseaux, l'administrateur réseau doit utiliser deux déclarations NAT et un pool global dans la configuration ASA :

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Cette configuration ne traduit pas l'adresse source d'aucun trafic sortant du réseau 198.51.100.0/24. Cela traduit une adresse source dans le réseau 10.0.0.0/8 en une adresse de la plage 209.165.201.3 à 209.165.201.30.

> Remarque: Quand vous avez une interface avec un routage spécifique NAT, et s'il n'y a aucun regroupement global à une autre interface, vous devez employer 0 nat afin d'installer l'exception NAT.

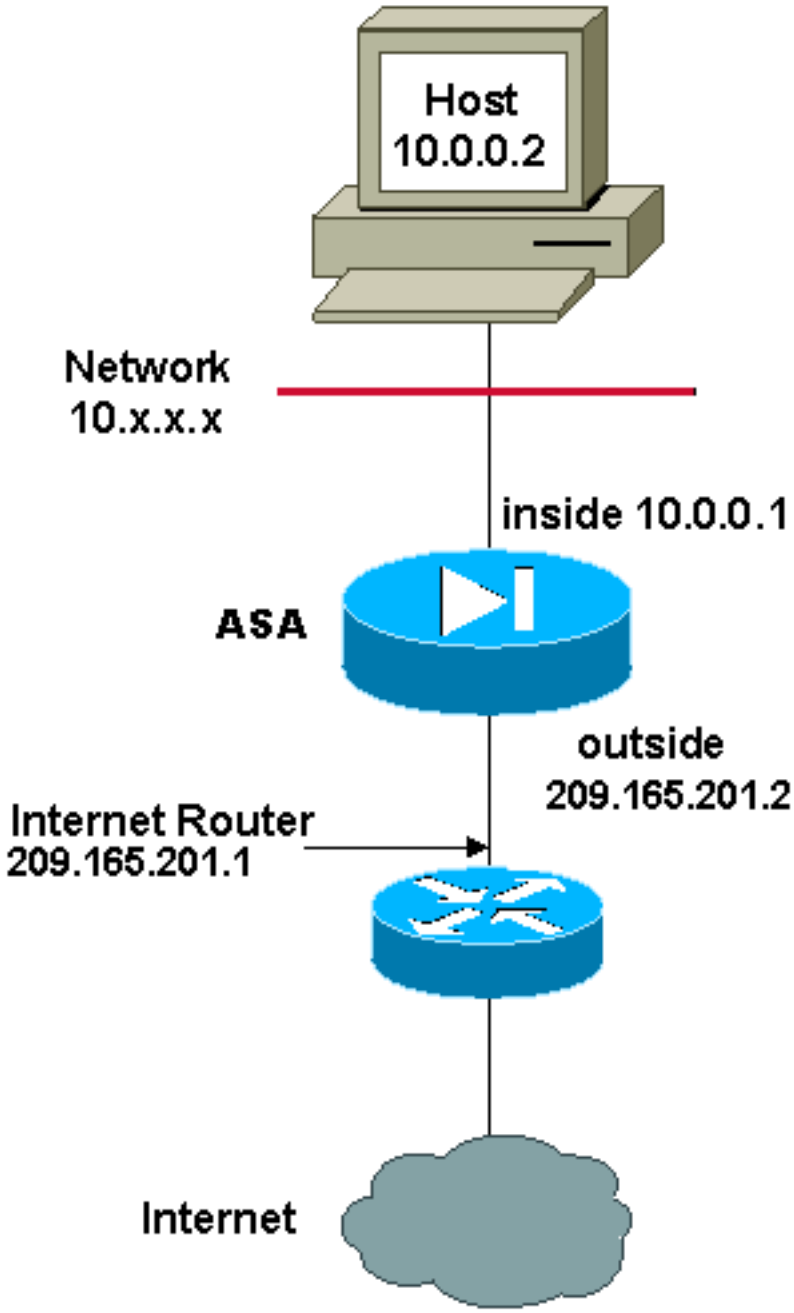
Version 8.3 et ultérieures ASA

Voici la configuration.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configurez - Plusieurs pools globaux

Diagramme du réseau



Dans cet exemple, le responsable du réseau a deux plages d'adresses IP qui s'enregistrent sur Internet. Le responsable du réseau doit convertir toutes les adresses internes, qui sont dans la plage 10.0.0.0/8 en adresses enregistrées. Les plages d'adresses IP que le responsable du réseau doit utiliser vont de 209.165.201.1 à 209.165.201.30 et de 209.165.200.225 à 209.165.200.254. Le responsable du réseau peut faire ceci de la façon suivante :

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> Remarque: Un système d'adressage générique est utilisé dans la déclaration NAT. Cette déclaration indique l'ASA traduire n'importe quelle adresse source interne quand elle sort à l'Internet. L'adresse de cette commande peut être plus spécifique si vous le désirez.

Version 8.3 et ultérieures ASA

Voici la configuration.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

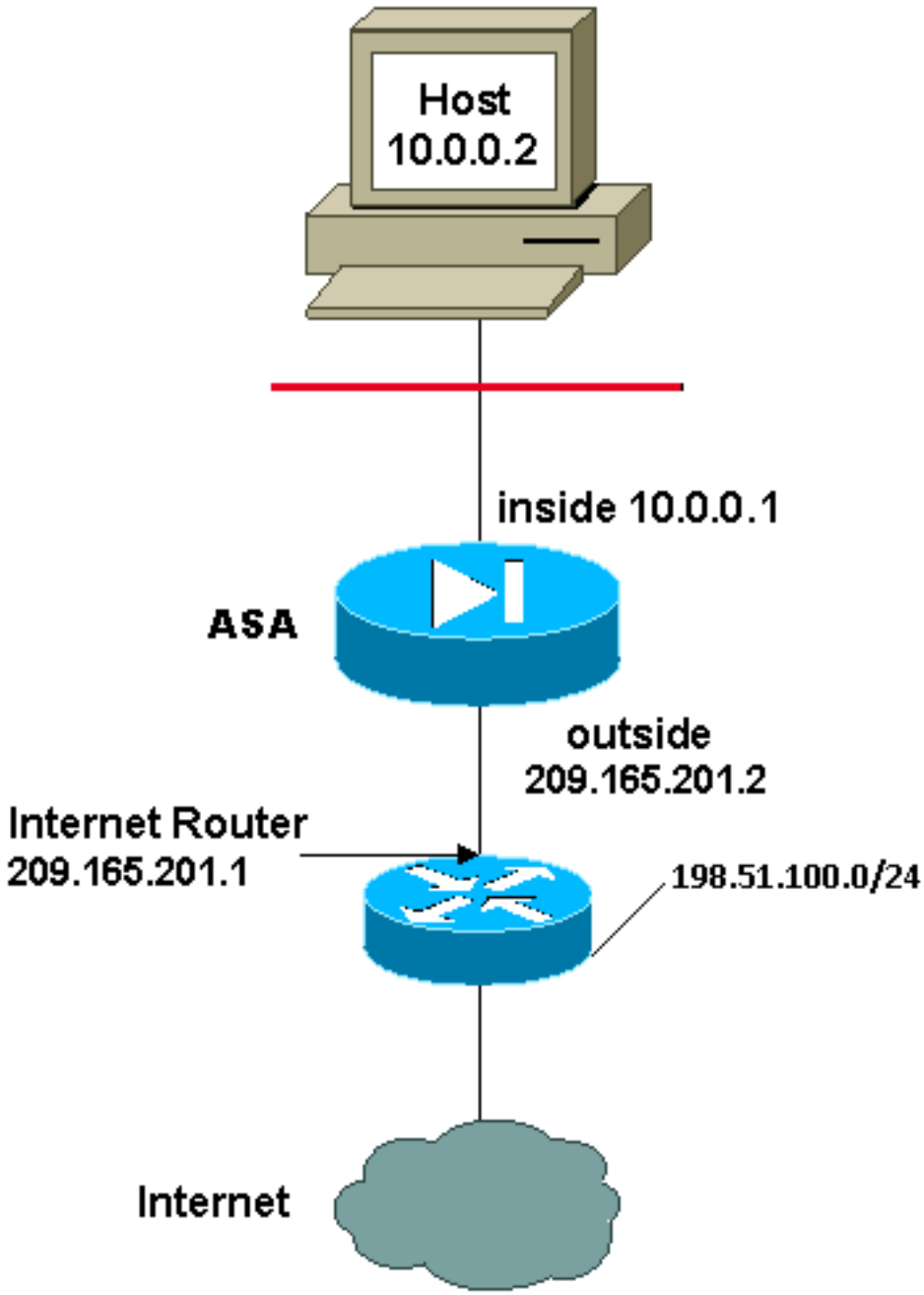
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurez - Mélangez NAT et TAPOTEZ les déclarations

Diagramme du réseau



Dans cet exemple, l'ISP fournit au responsable du réseau une plage d'adresses de 209.165.201.1 à 209.165.201.30 à l'usage de la société. Le gestionnaire de réseau a décidé d'utiliser 209.165.201.1 pour l'interface interne sur le routeur internet et 209.165.201.2 pour l'interface extérieure sur l'ASA. Vous pouvez utiliser la plage 209.165.201.3 à 209.165.201.30 pour le pool NAT. Cependant, le gestionnaire de réseau sait que, en même temps, il peut y avoir plus de 28 personnes qui essayent de sortir de l'ASA. Par conséquent, le responsable du réseau décide de prendre 209.165.201.30 et en faire une adresse PAT de sorte que plusieurs utilisateurs puissent partager une adresse simultanément.

Ces commandes demandent à l'ASA de traduire l'adresse source à 209.165.201.3 par 209.165.201.29 pour que les 27 premiers utilisateurs internes passent à travers l'ASA. Après que ces adresses soient épuisées, puis l'ASA traduit toutes les adresses sources ultérieures à 209.165.201.30 jusqu'à ce qu'une des adresses dans le groupe NAT devienne libre.

> Remarque: Un système d'adressage générique est utilisé dans la déclaration NAT. Cette déclaration indique l'ASA traduire n'importe quelle adresse source interne quand elle sort à

l'Internet. L'adresse de cette commande peut être plus spécifique si vous le désirez.

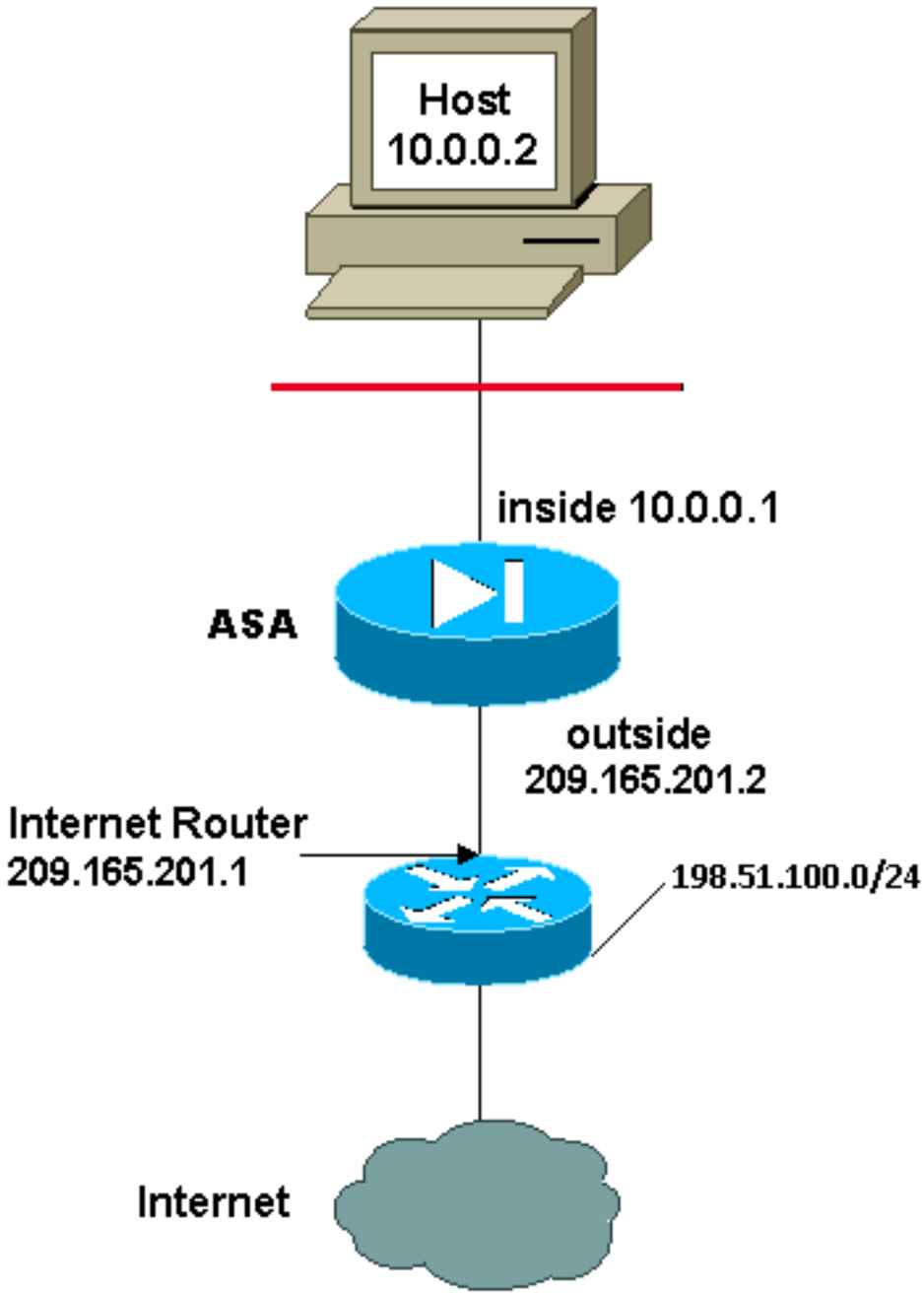
Version 8.3 et ultérieures ASA

Voici la configuration.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurez - Plusieurs déclarations NAT avec des déclarations manuelles

Diagramme du réseau



Dans cet exemple, l'ISP fournit au responsable du réseau une plage d'adresses allant de 209.165.201.1 à 209.165.201.30. Le gestionnaire de réseau décide d'assigner 209.165.201.1 à l'interface interne sur le routeur internet et 209.165.201.2 à l'interface extérieure de l'ASA.

Cependant, dans ce scénario, un autre segment de LAN privé est placé après le routeur Internet. Le responsable du réseau préférerait ne pas gaspiller d'adresses du pool global lorsque des hôtes de ces deux réseaux parlent entre eux. Le responsable du réseau doit toujours traduire l'adresse source pour tous les utilisateurs internes (10.0.0.0/8) lorsqu'ils accèdent à Internet.

Cette configuration ne traduit pas ces adresses avec une adresse source de 10.0.0.0/8 et une adresse de destination de 198.51.100.0/24. Il traduit l'adresse source de n'importe quel trafic initié du réseau 10.0.0.0/8 et destiné pour n'importe où autre que 198.51.100.0/24 dans une adresse de la plage 209.165.201.3 par 209.165.201.30.

Si vous disposez de la sortie d'une commande **write terminal** de votre périphérique Cisco, vous pouvez utiliser l'outil Interpréteur de sortie (clients enregistrés uniquement).

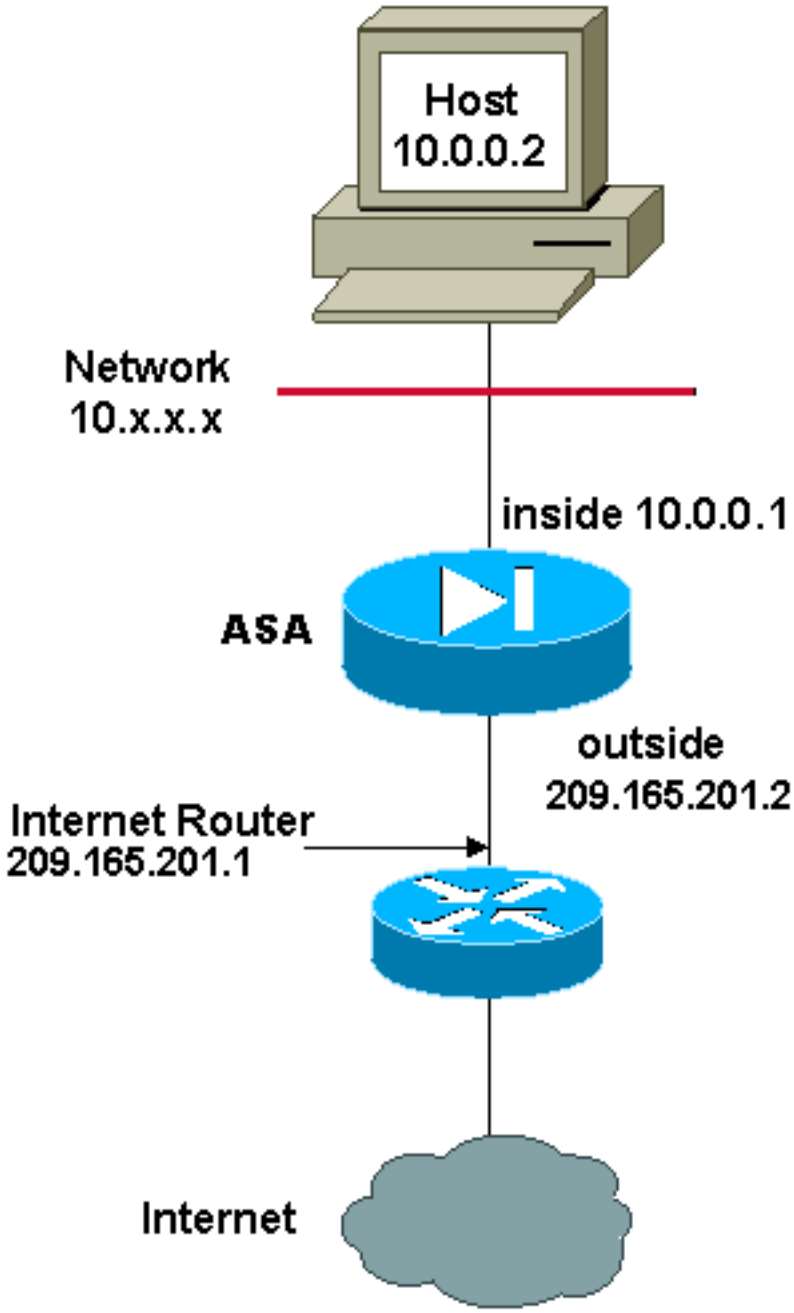
Version 8.3 et ultérieures ASA

Voici la configuration.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configurez - Utilisez la stratégie NAT

Diagramme du réseau



Lorsque vous utilisez une liste d'accès avec la commande **nat** pour n'importe quel ID NAT autre que 0, vous activez le NAT de stratégie.

Le NAT de stratégie vous permet d'identifier le trafic local pour la traduction d'adresses lorsque vous spécifiez les adresses (ou ports) source et de destination dans une liste d'accès. Le NAT normal utilise uniquement des adresses/ports source. Le routage spécifique NAT utilise les adresses/ports d'origine et de destination.

> Remarque: Tous les types de NAT prennent en charge le NAT de stratégie excepté l'exemption NAT (**liste d'accès NAT 0**). Le nat exemption emploie une liste de contrôle d'accès (ACL) afin d'identifier les adresses locales, mais diffère de la stratégie NAT parce que les ports ne sont pas considérés.

Avec le NAT de stratégie, vous pouvez créer plusieurs NAT ou déclarations statiques qui identifient la même adresse locale tant que la combinaison source/port et destination/port est unique pour chaque déclaration. Vous pouvez alors associer plusieurs adresses globales à chaque paire source/port et destination/port.

Dans cet exemple, le responsable du réseau fournit un accès à l'adresse IP de destination 172.30.1.11 pour le port 80 (Web) et le port 23 (Telnet), mais doit utiliser deux adresses IP différentes comme adresse source. 209.165.201.3 est utilisé pendant qu'une adresse source pour le Web et 209.165.201.4 est utilisée pour le telnet, et doit convertir toutes les adresses internes, qui sont dans la plage 10.0.0.0/8. Le responsable du réseau peut faire ceci de la façon suivante :

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

Version 8.3 et ultérieures ASA

Voici la configuration.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> Remarque: Pour plus d'informations sur la configuration de NAT et du TAPOTEMENT sur la version 8.4 ASA, référez-vous aux informations sur NAT.
>
> Pour plus d'informations sur la configuration des Listes d'accès sur la version 8.4 ASA, référez-vous aux informations sur des Listes d'accès.

Vérifiez

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, la sortie dans la section suivante peut être vue sur l'ASA CLI.

Connexion

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
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 sans être bloqué 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 | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 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:10.0.0.2/57431 (209.165.201.3/57431)
```

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 (Xlate)

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 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:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 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 xlate (traduction). **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 10.165.200.226 par 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

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.