# Exemple de configuration de l'instruction NAT et PAT sur le pare-feu Cisco Secure ASA

## Contenu


Introduction
Conditions préalables
Conditions requises
Components Used
Configurer - Plusieurs instructions NAT avec NAT manuel et automatique
Diagramme du réseau
ASA versions 8.3 et ultérieures
Configurer - Plusieurs pools globaux
Diagramme du réseau
ASA versions 8.3 et ultérieures
Configurer - Combiner les instructions NAT et PAT
Diagramme du réseau
ASA versions 8.3 et ultérieures
Configurer - Plusieurs instructions NAT avec instructions manuelles
Diagramme du réseau
ASA versions 8.3 et ultérieures
Configurer - Utiliser la NAT de stratégie
Diagramme du réseau
ASA versions 8.3 et ultérieures
Vérification
Connexion
Syslog
Traductions NAT (Xlate)
Dépannage


## Introduction

Ce document fournit des exemples de configurations de base NAT (Network Address Translation) et PAT (Port Address Translation) sur le pare-feu Cisco Secure Adaptive Security Appliance (ASA). Ce document fournit également les schémas de réseau simplifiés. Pour plus d'informations, reportez-vous à la documentation ASA de votre version logicielle ASA.

Ce document propose une analyse personnalisée de votre périphérique Cisco.

Référez-vous à Configuration NAT sur ASA sur les appliances de sécurité ASA 5500/5500-X pour plus d'informations.

# Conditions préalables

## Conditions requises

Cisco recommande que vous connaissiez le pare-feu Cisco Secure ASA.

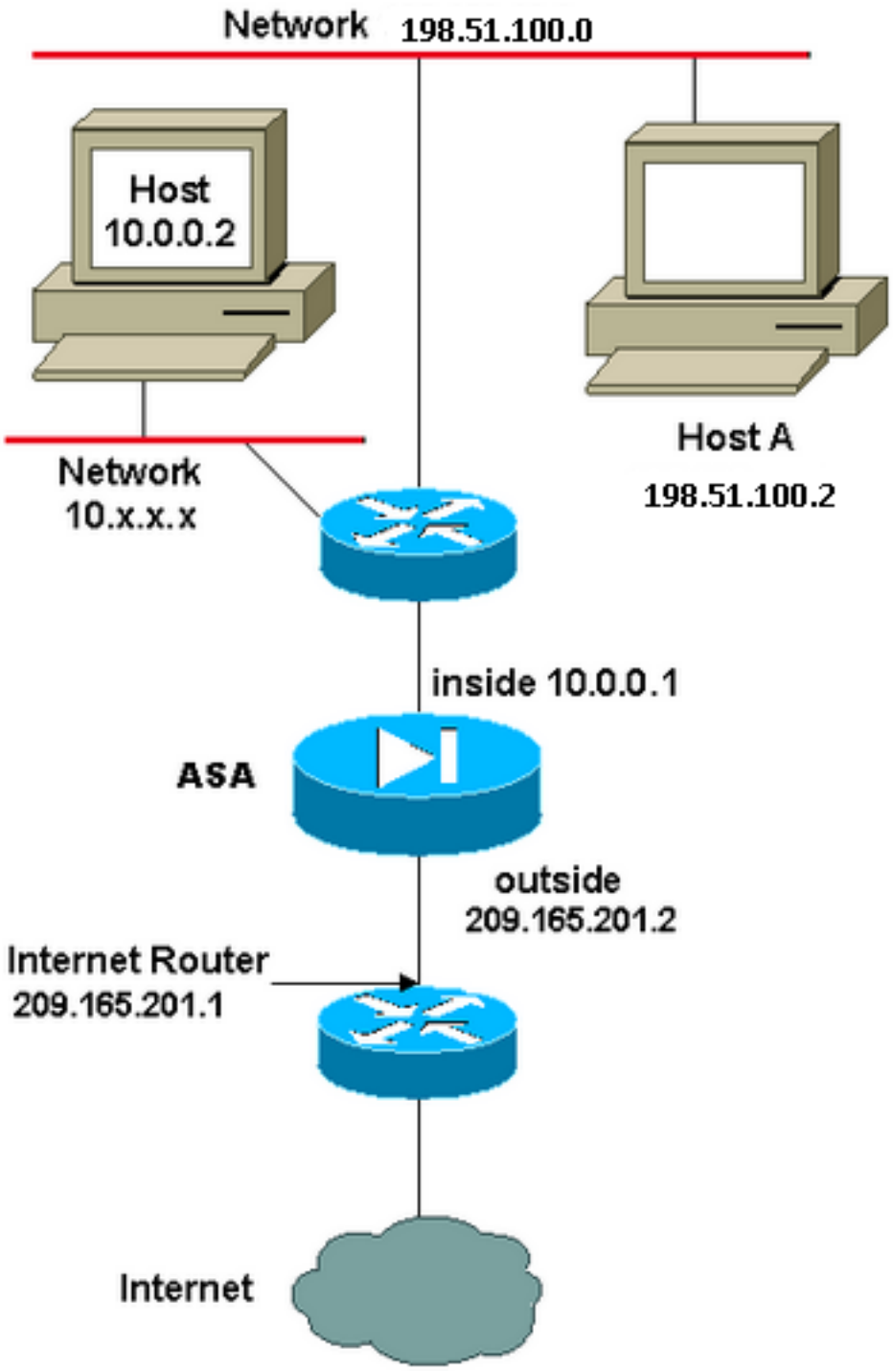
## Components Used

Les informations de ce document sont basées sur le logiciel pare-feu Cisco Secure ASA version 8.4.2 et ultérieure.

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.

# Configurer - Plusieurs instructions NAT avec NAT manuel et automatique

## 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'affecter 209.165.201.1 à l'interface interne du routeur Internet et 209.165.201.2 à l'interface externe de l'ASA.

L'administrateur réseau a déjà fait attribuer une adresse de classe C au réseau, 198.51.100.0/24, et quelques postes de travail utilisent ces adresses afin d'accéder à Internet. Ces stations de travail ne nécessitent aucune traduction d'adresses car elles possèdent 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 prendre en charge cette conception de réseau, l'administrateur réseau doit utiliser deux instructions 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 du 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.

> **Note**: 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.

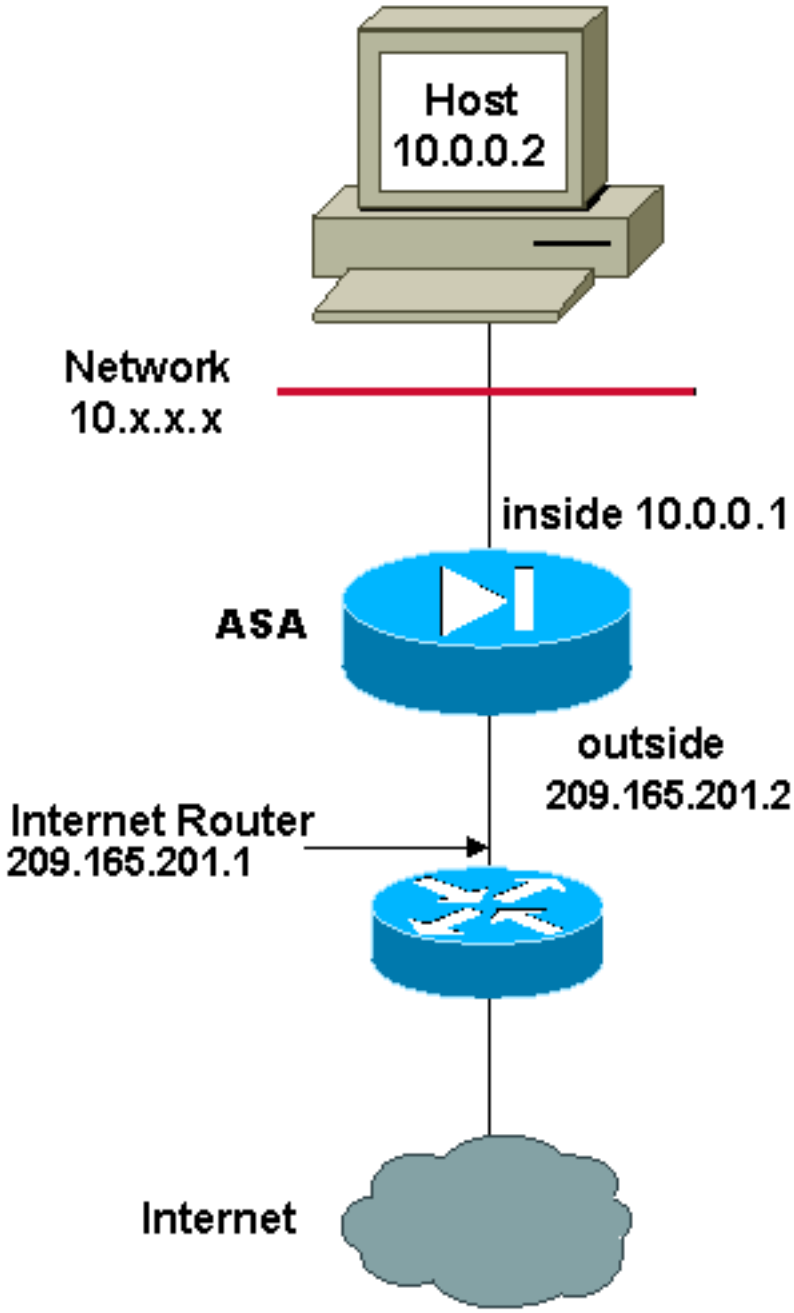
### ASA versions 8.3 et ultérieures

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
```

## Configurer - 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
```

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

## ASA versions 8.3 et ultérieures

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:**

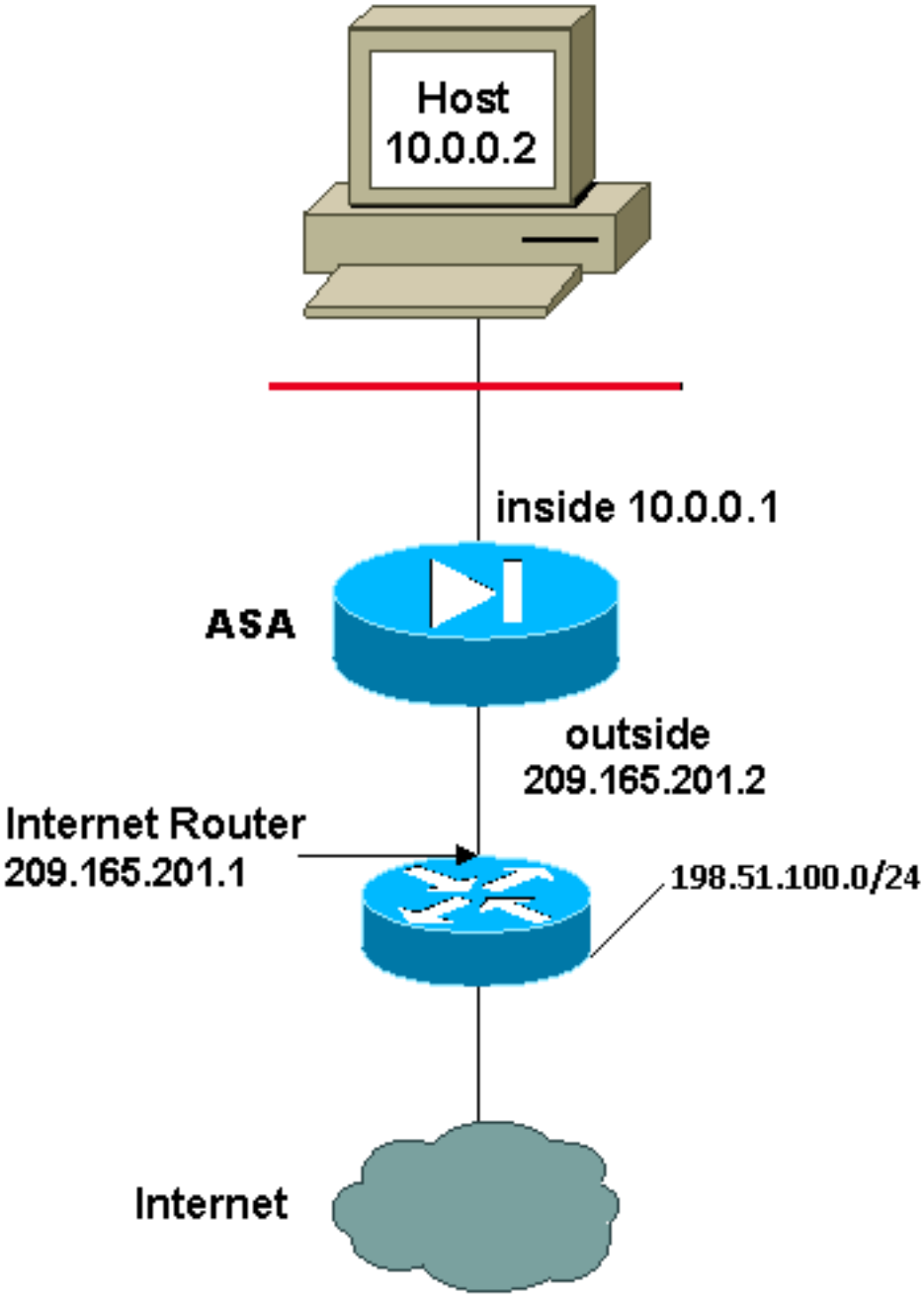
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

**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
```

# Configurer - Combiner les instructions NAT et PAT

## 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 externe 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 qu'à tout moment, plus de 28 personnes peuvent essayer de quitter 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 indiquent à l'ASA de traduire l'adresse source en 209.165.201.3 à 209.165.201.29 pour les 27 premiers utilisateurs internes à passer par l'ASA. Une fois ces adresses épuisées, l'ASA traduit toutes les adresses source suivantes en 209.165.201.30 jusqu'à ce qu'une des adresses du pool NAT devienne libre.

> **Note**: Un système d'adressage générique est utilisé dans la déclaration NAT. Cette instruction indique à l'ASA de traduire n'importe quelle adresse source interne lorsqu'elle est

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

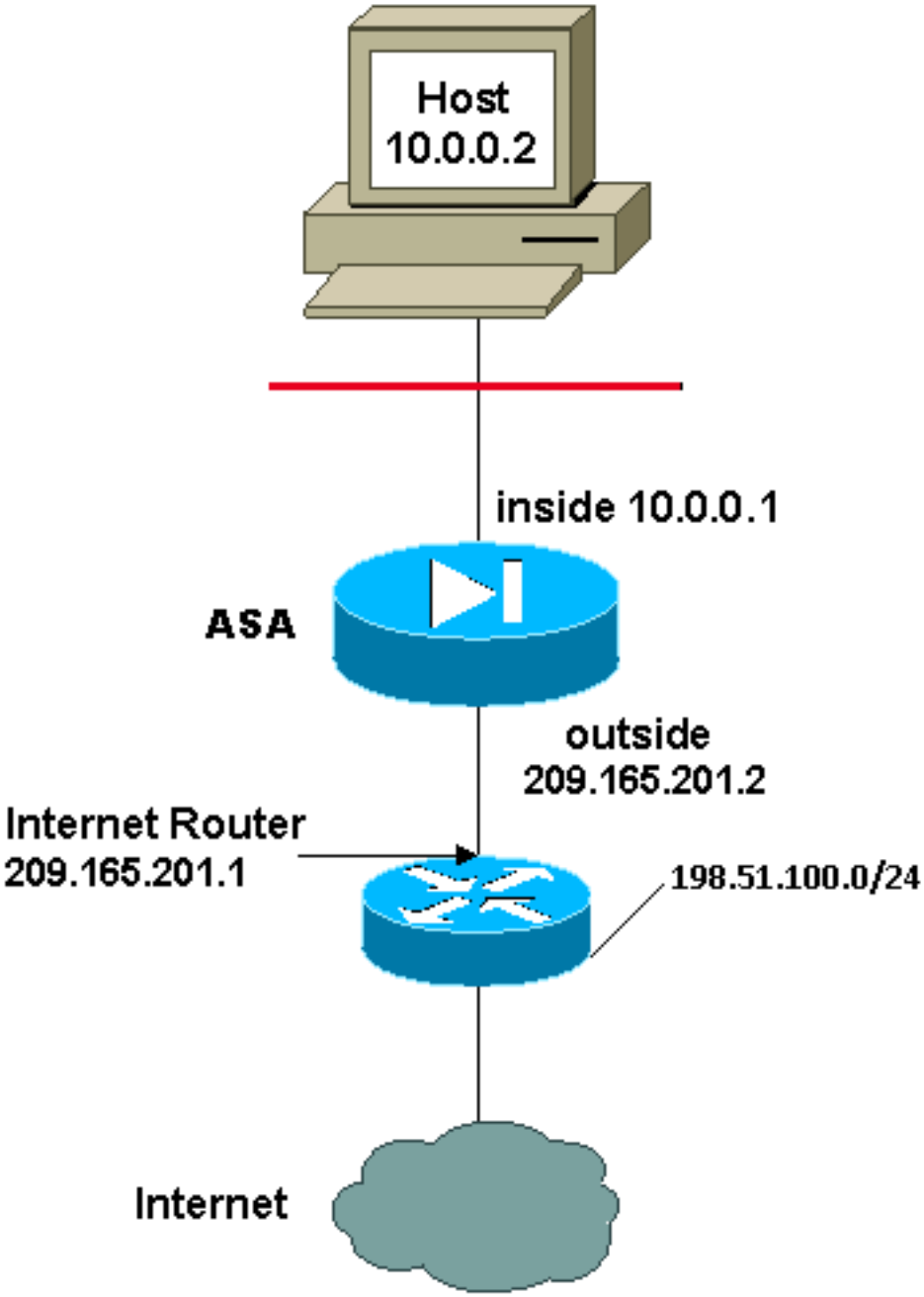
### ASA versions 8.3 et ultérieures

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
```

## Configurer - Plusieurs instructions NAT avec instructions 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'affecter 209.165.201.1 à l'interface interne sur le routeur Internet et 209.165.201.2 à l'interface externe 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. Cela traduit l'adresse source de n'importe quel trafic issu du réseau 10.0.0.0/8 et destiné à n'importe quel emplacement autre que 198.51.100.0/24 en une adresse de la plage comprise entre 209.165.201.3 et 209.165.201.30.

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

## ASA versions 8.3 et ultérieures

Voici la configuration .

**Using the Manual Nat statements:**

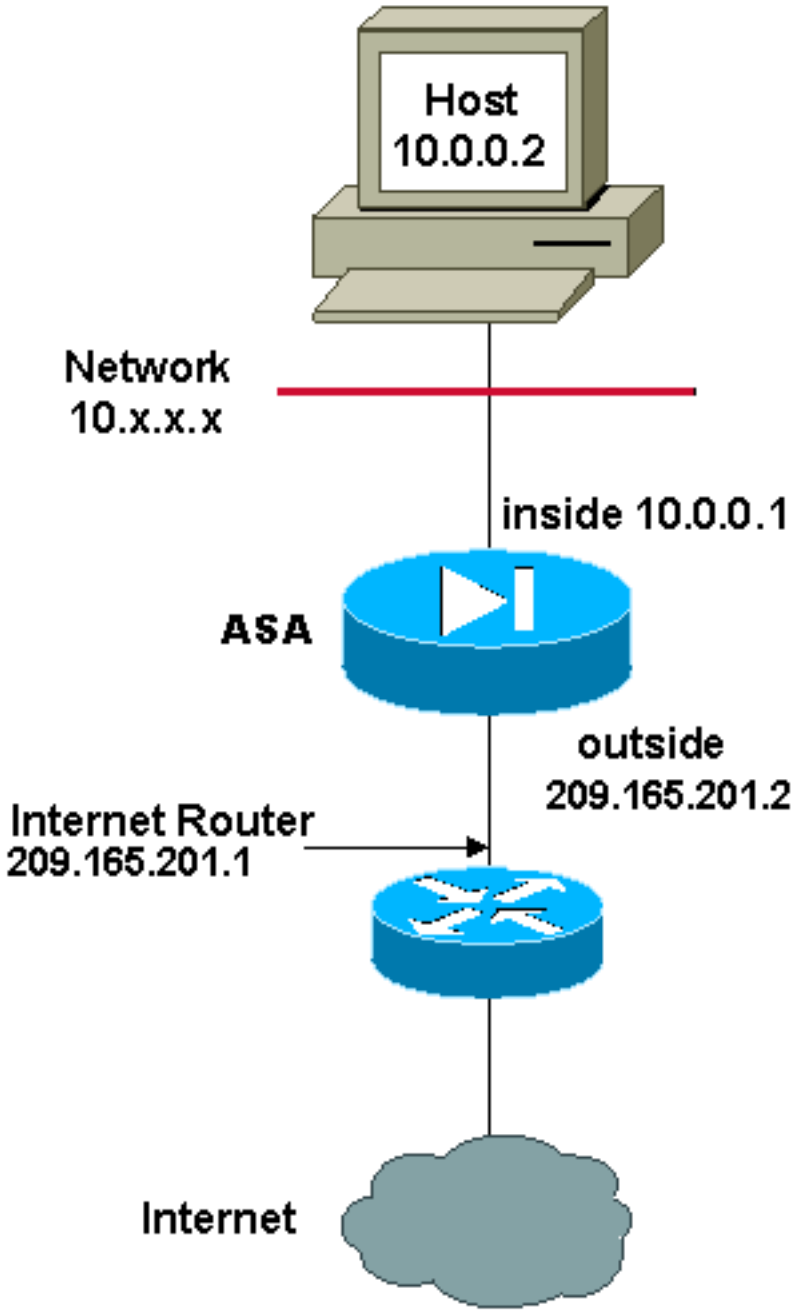
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

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
```

# Configurer - Utiliser la NAT de stratégie

## 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.

> **Note**: Tous les types de NAT prennent en charge le NAT de stratégie excepté l'exemption NAT (liste d'accès NAT 0). L'exemption NAT utilise une liste de contrôle d'accès (ACL) afin d'identifier les adresses locales, mais diffère de la NAT de stratégie car les ports ne sont pas pris en compte.

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 comme adresse source pour le Web et 209.165.201.4 est utilisé pour Telnet, et doit convertir toutes les adresses internes qui se trouvent 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
```

### ASA versions 8.3 et ultérieures

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
```

> **Note**: Pour plus d'informations sur la configuration de NAT et PAT sur ASA version 8.4, référez-vous à Informations sur NAT.
>
> Pour plus d'informations sur la configuration des listes d'accès sur ASA version 8.4, référez-vous à Informations sur les listes d'accès.

## Vérification

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, le résultat de la section suivante est visible sur l'interface de ligne de commande ASA.

## 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 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 à travers le pare-feu sans être 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 | 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 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 (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
```

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 xlate (traduction). 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 10.165.200.226 selon la configuration.

Les indicateurs répertoriés, **r i** , indiquent que la traduction est **dynamique** et **portmap**. Vous trouverez plus d'informations sur les différentes configurations NAT dans Informations sur NAT.

# Dépannage

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