# Dépannage de configuration de traduction d'adresses réseau ASA

## Contenu



## Introduction

Ce document décrit comment dépanner la configuration de Traduction d'adresses de réseau (NAT) sur la plate-forme de l'appliance de sécurité adaptable Cisco (ASA). Ce document est valide pour la version 8.3 et ultérieures ASA.

> Remarque: Pour quelques exemples de base des configurations NAT, qui incluent un vidéo qui affiche une configuration NAT de base, voyez les informations relatives de section au bas de ce document.

## Dépannez la configuration NAT sur l'ASA

Quand vous dépannez des configurations NAT, il est important de comprendre comment la configuration NAT sur l'ASA est utilisée pour construire la table NAT de stratégie.

Ces erreurs de configuration expliquent la majorité des problèmes NAT produits par des administrateurs ASA :

- Les règles NAT de configuration sont en panne. Par exemple, une règle NAT manuelle est placée en haut de la table NAT, qui entraîne des règles plus spécifiques a placé un bas plus lointain la table NAT à ne jamais frapper.
- Les objets de réseau utilisés dans la configuration NAT sont trop larges, qui fait apparier par distraction le trafic ces règles NAT, et manquent des règles NAT plus spécifiques.

L'utilitaire de **traceur de paquet** peut être utilisé pour diagnostiquer la plupart des questions liées nat sur l'ASA. Voyez la section suivante pour plus d'informations sur la façon dont la configuration NAT est utilisée pour construire la table NAT de stratégie, et la façon dépanner et résoudre des problèmes NAT spécifiques.

Supplémentaire, la commande **nat de détail d'exposition** peut être utilisée afin de comprendre quelles règles NAT sont frappées par de nouvelles connexions.

# Comment la configuration ASA est utilisée pour construire le Tableau NAT de stratégie

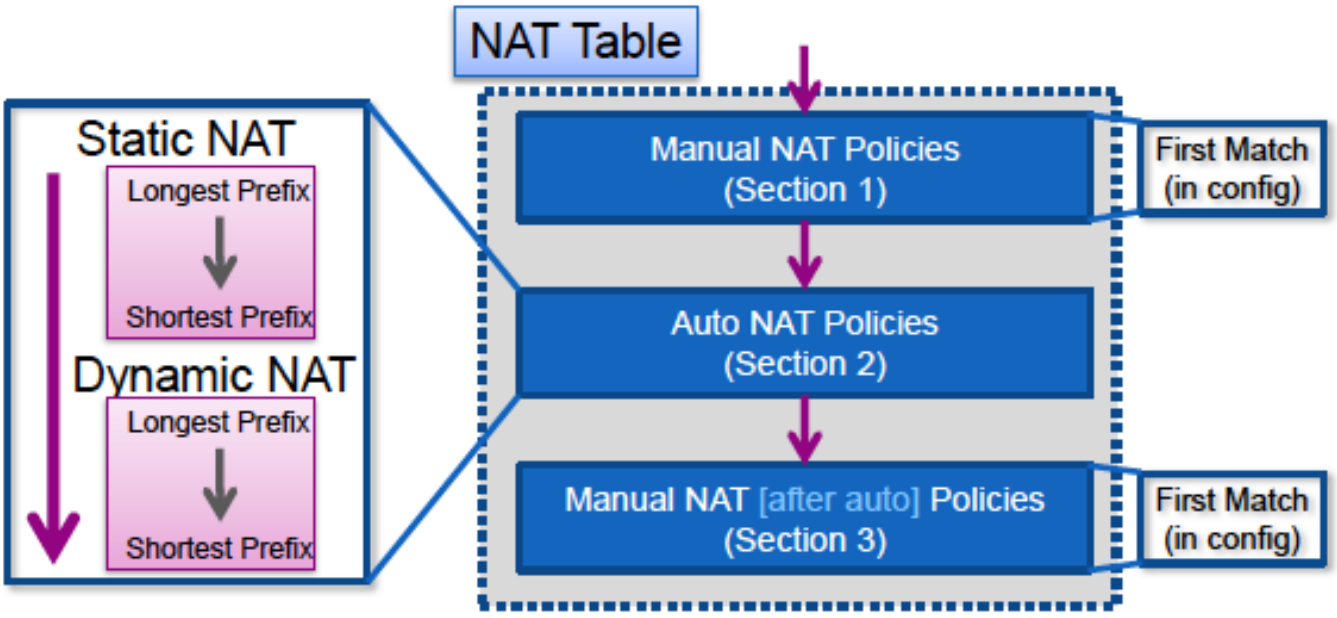
Tous les paquets traités par l'ASA sont évalués contre la table NAT. Débuts de cette évaluation au dessus (la section 1) et les travaux vers le bas jusqu'à une règle NAT est appariée. Une fois qu'une règle NAT est appariée, cette règle NAT est appliquée à la connexion et plus de stratégies NAT ne sont vérifiées contre le paquet.

La stratégie NAT sur l'ASA est établie de la configuration NAT.

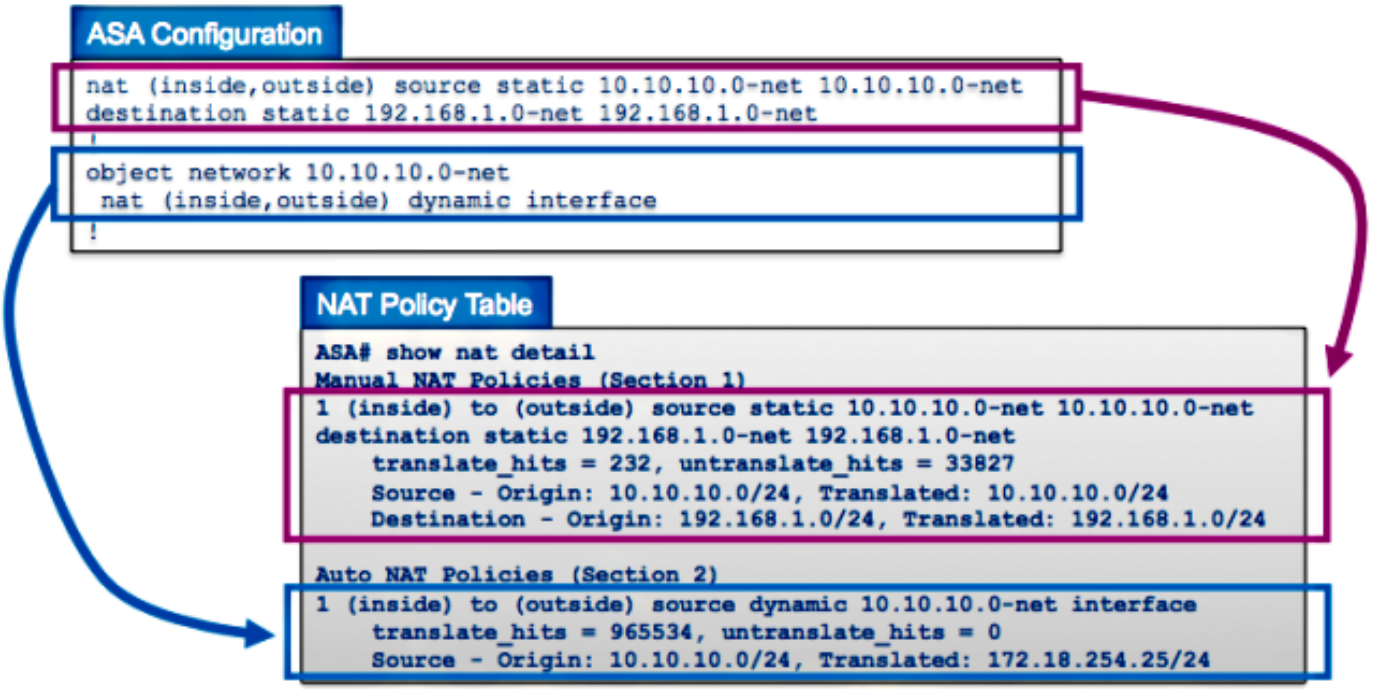
Les trois sections de la table NAT ASA sont :

| | |
|---|---|
| Section 1 | **Stratégies NAT manuelles**<br>Ceux-ci sont traités dans la commande dans laquelle ils apparaissent dans la configuration. |
| Section 2 | **Stratégies NAT automatiques**<br>Ceux-ci sont traités ont basé sur le type NAT (statique ou dynamique) et la longueur de préfixe (masque de sous-réseau) dans l'objet. |
| Section 3 | **stratégies NAT manuelles d'Après-automatique**<br>Ceux-ci sont traités dans la commande dans laquelle ils apparaissent dans la configuration. |

Ce diagramme affiche les différentes sections NAT et comment elles sont commandées :




Cet exemple affiche comment la configuration NAT de l'ASA avec deux règles (une déclaration NAT manuelle et une configuration NAT automatique) sont représentées dans la table NAT :




# Comment dépanner des problèmes NAT

## Utilisez l'utilitaire de Packet Tracer

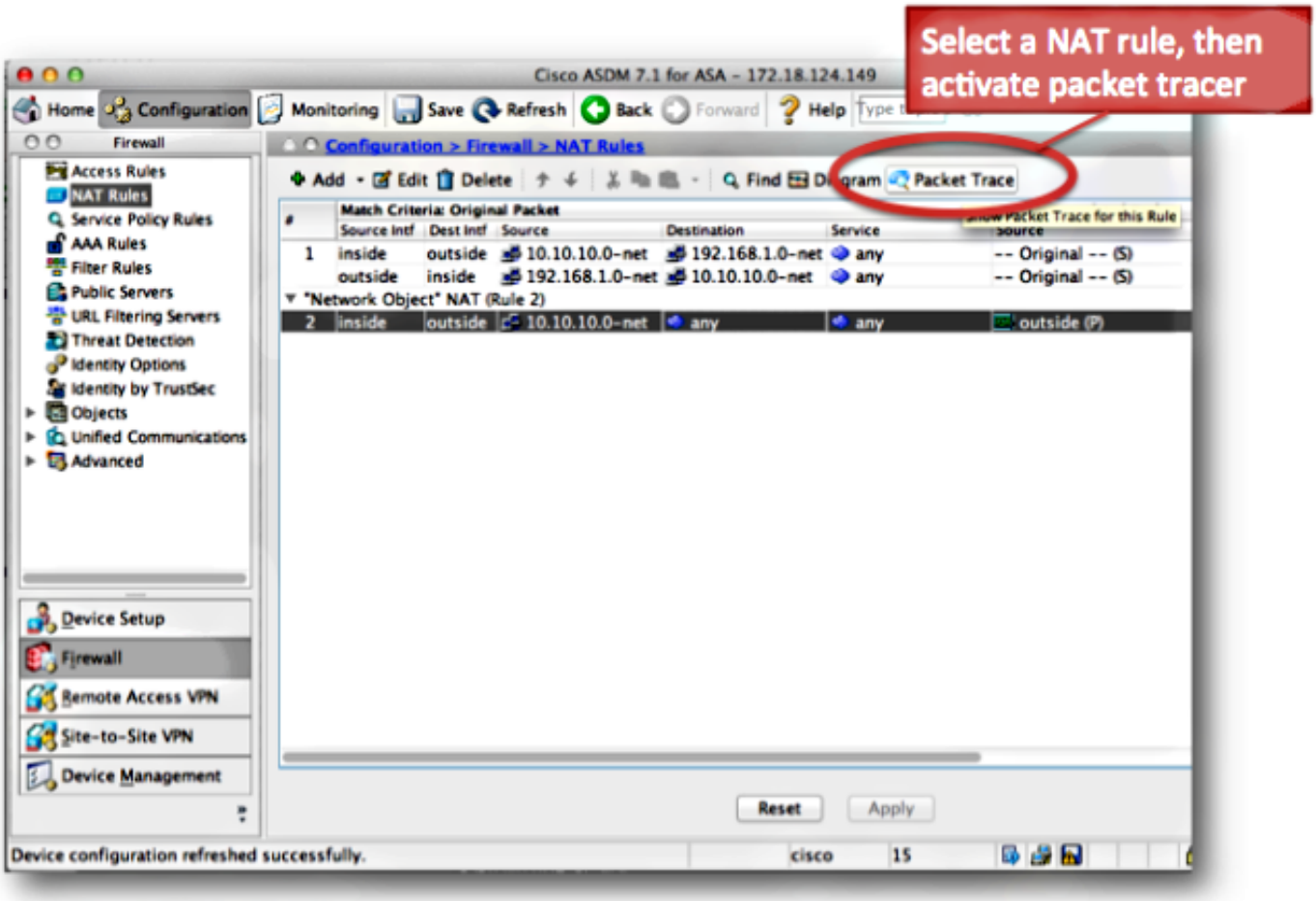
Afin de dépanner des problèmes avec des configurations NAT, employez l'utilitaire de **traceur de paquet** afin de vérifier qu'un paquet frappe la stratégie NAT. Le traceur de paquet te permet pour spécifier un paquet témoin qui écrit l'ASA, et l'ASA indique ce que la configuration s'applique au paquet et si elle est permise ou pas.

Dans l'exemple ci-dessous, un paquet TCP témoin qui écrit l'interface interne et est destiné à un

hôte sur l'Internet est donné. L'utilitaire de traceur de paquet prouve que le paquet apparie une règle NAT dynamique et est traduit à l'adresse IP extérieure de **172.16.123.4** :

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 10.10.10.0-net
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

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

ASA#
```

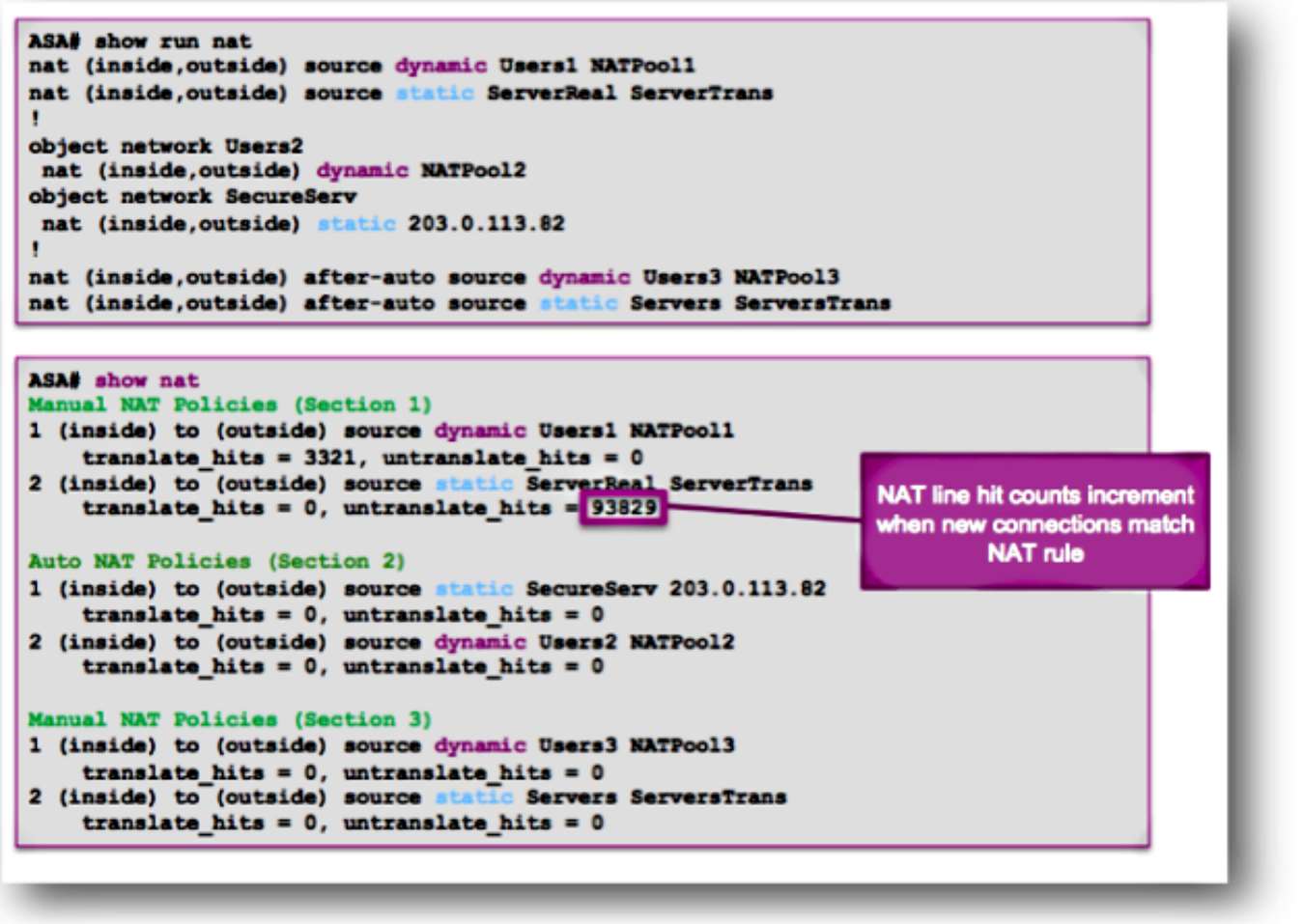
Choisissez la **règle NAT** et cliquez sur le **tracé de paquets** afin de lancer le traceur de paquet du Cisco Adaptive Security Device Manager (ASDM). Ceci utilise les adresses IP spécifiées dans la règle NAT comme entrées pour l'outil de traceur de paquet :




## Visualisez la sortie de la commande nat d'exposition

La sortie de la commande **nat de détail d'exposition** peut être utilisée afin de visualiser la table NAT de stratégie. Spécifiquement, les **translate_hits** et les compteurs d'**untranslate_hits** peuvent être utilisés afin de déterminer quelles entrées NAT sont utilisées sur l'ASA. Si vous voyez que votre nouvelle règle NAT n'a aucun **translate_hits** ou **untranslate_hits**, ce signifie qu'ou le trafic n'arrive pas à l'ASA, ou peut-être une règle différente qui a une haute priorité dans la table NAT apparie le trafic.

Voici la configuration NAT et la table NAT de stratégie d'une configuration différente ASA :




Dans l'exemple précédent, il y a six règles NAT configurées sur cette ASA. La sortie **nat d'exposition** affiche comment ces règles sont utilisées de construire la table NAT de stratégie, aussi bien que le nombre de **translate_hits** et d'**untranslate_hits** pour chaque règle. Ces compteurs de hit incrémentent seulement une fois par connexion. Après que la connexion soit établie par l'ASA, les paquets suivants qui apparient cette connexion en cours n'incrémentent pas les lignes NAT (tout comme les nombres de hits de liste d'accès de manière travaillez à l'ASA).

**Translate_hits** : Le nombre de nouvelles connexions qui apparient la règle NAT dans la direction en avant.

« La direction en avant » signifie que la connexion a été établie par l'ASA en direction des interfaces spécifiées dans la règle NAT. Si une règle NAT spécifiait que le serveur intérieur est traduit à l'interface extérieure, la commande des interfaces dans la règle NAT est « nat (à l'intérieur, dehors)… » ; si ce serveur initie une nouvelle connexion à un hôte sur l'extérieur, le compteur de **translate_hit** incrémente.

**Untranslate_hits** : Le nombre de nouvelles connexions qui apparient la règle NAT dans la direction inverse.

Si une règle NAT spécifie que le serveur intérieur est traduit à l'interface extérieure, la commande des interfaces dans la règle NAT est « nat (à l'intérieur, dehors)… » ; si un client sur l'extérieur de l'ASA initie une nouvelle connexion au serveur sur l'intérieur, le compteur d'**untranslate_hit** incrémente.

De nouveau, si vous voyez que votre nouvelle règle NAT n'a aucun **translate_hits** ou **untranslate_hits**, ce signifie qu'ou le trafic n'arrive pas à l'ASA, ou peut-être une règle différente qui

a une haute priorité dans la table NAT apparie le trafic.

### De la méthodologie de problème NAT dépannage

Employez le traceur de paquet afin de confirmer qu'un paquet témoin apparie la règle NAT appropriée de configuration sur l'ASA. Employez la commande **nat de détail d'exposition** afin de comprendre quelles règles NAT de stratégie sont frappées. Si une connexion apparie une configuration NAT différente que prévue, dépannez avec ces questions :

- Y a-t-il une règle NAT différente qui a la priorité au-dessus de la règle NAT que vous avez eu l'intention le trafic pour frapper ?
- Y a-t-il une règle NAT différente avec les définitions d'objet qui sont trop larges (le masque de sous-réseau est-il trop court, comme 255.0.0.0) qui fait apparier ce trafic la règle fausse ?
- Les stratégies NAT manuelles en panne, qui des causes sont-elles le paquet pour apparier la règle fausse ?
- Votre règle NAT inexactement configurée, qui des causes est-elle la règle de ne pas apparier votre trafic ?

Voyez la section suivante pour des exemples de problème et des solutions.

## Problèmes courants avec des configurations NAT

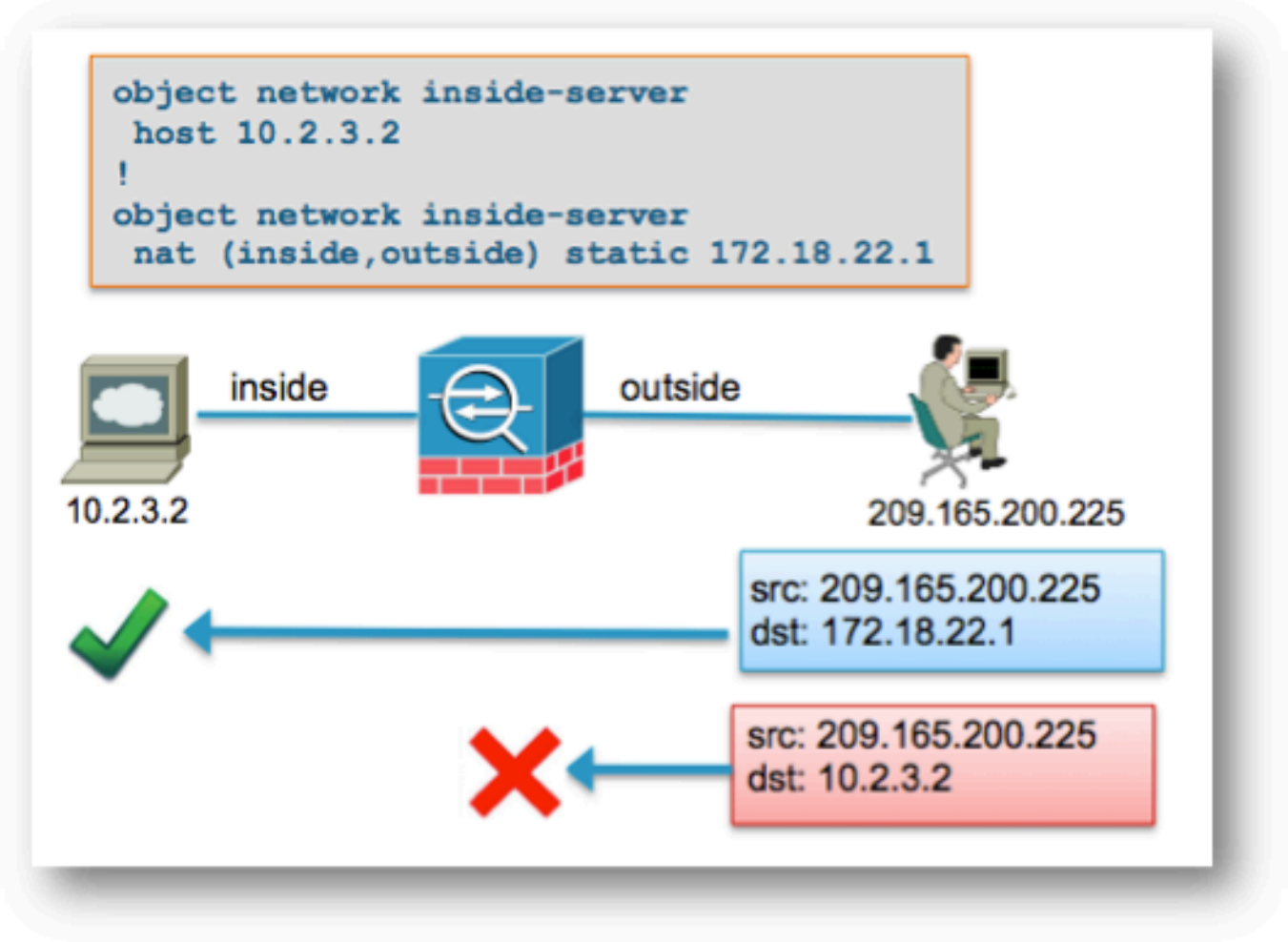
Voici quelques problèmes courants rencontrés quand vous configurez NAT sur l'ASA.

### Problème : Le trafic échoue en raison de l'erreur NAT de la panne de chemin inverse (RPF) : Règles NAT asymétriques appariées pour en avant et des flux inverses

Le contrôle NAT RPF s'assure qu'une connexion qui est traduite par l'ASA dans la direction en avant, telle que le TCP synchronisent (synchronisation), est traduit de la même règle NAT dans la direction inverse, telle que le TCP SYN/acknowledge (ACK).

Le plus généralement, ce problème est provoqué par par des connexions entrantes destinées à l'adresse (non traduite) locale dans une déclaration NAT. À un niveau de base, le RPF NAT vérifie que la connexion inverse du serveur au client apparie la même règle NAT ; s'il ne fait pas, le contrôle NAT RPF échoue.

Exemple :




Quand l'hôte d'extérieur chez **209.165.200.225** envoie un paquet destiné directement à l'adresse IP (non traduite) locale de **10.2.3.2**, l'ASA relâche le paquet et se connecte ce Syslog :

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:209.165.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

**Solution :**

D'abord, assurez-vous que l'hôte envoie des données à l'adresse NAT globale correcte. Si l'hôte envoie des paquets destinés à l'adresse exacte, vérifiez les règles NAT qui sont frappées par la connexion. Vérifiez que les règles NAT sont correctement définies, et que les objets référencés dans les règles NAT sont corrects. Vérifiez également que la commande des règles NAT est appropriée.

Employez l'utilitaire de traceur de paquet afin de spécifier les détails du paquet refusé. Le traceur de paquet devrait afficher le paquet lâché dû à la panne de contrôle RPF. Ensuite, regardez la sortie du traceur de paquet afin de voir quelles règles NAT sont frappées pendant la phase NAT et la phase NAT-RPF.

Si un paquet apparie une règle NAT pendant la phase NAT de RPF-contrôle, qui indique que l'inversion d'écoulement frapperait une traduction NAT, mais n'apparie pas une règle pendant la phase NAT, qui indique que l'écoulement en avant ne frapperait pas une règle NAT, le paquet est lâché.

Cette sortie apparie le scénario affiché dans le diagramme précédent, où l'hôte d'extérieur envoie inexactement le trafic à l'adresse IP locale du serveur et pas de l'adresse IP (traduite) globale :

```
ASA# packet-tracer input outside tcp 209.165.200.225 1234 10.2.3.2 80

.....

Phase: 8
Type: NAT
Subtype: rpf-check
Result: DROP
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Quand le paquet est destiné à l'adresse IP tracée correcte de 172.18.22.1, le paquet apparie la règle NAT correcte pendant la phase UN-NAT dans la direction en avant, et la même règle pendant la phase NAT de RPF-contrôle :

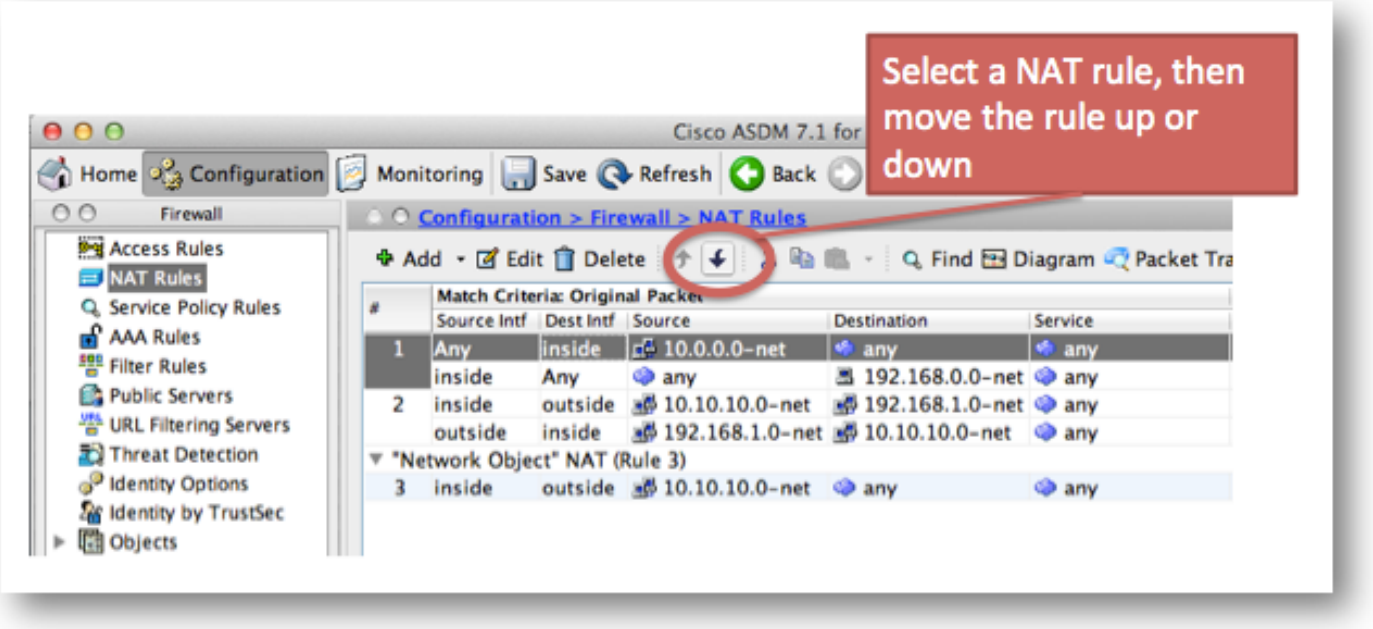
```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 1234 172.18.22.1 80
...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

## Problème : Les règles NAT manuelles sont en panne, qui entraîne les correspondances incorrectes de paquet

Les règles NAT manuelles sont traitées ont basé sur leur apparence dans la configuration. Si une règle NAT très large est répertoriée d'abord dans la configuration, elle pourrait ignorer des autres, plus de règle spécifique plus loin vers le bas dans la table NAT. Employez le traceur de paquet afin de vérifier que la règle NAT votre trafic frappe ; il pourrait être nécessaire de réorganiser les entrées NAT manuelles à une commande différente.

### Solution :

Commandez à nouveau les règles NAT avec l'ASDM.




**Solution :**

Des règles NAT peuvent être commandées à nouveau avec le CLI si vous retirez la règle et la réinsérez à un numéro de ligne spécifique. Afin d'insérer une nouvelle règle à une ligne spécifique, introduisez le numéro de ligne juste après que les interfaces soient spécifiées.

Exemple :

```
ASA(config)# nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

## Problème : Une règle NAT est trop large et apparie du trafic par distraction

Parfois on crée des règles NAT qui utilisent les objets qui sont trop larges. Si ces règles sont placées près du dessus de la table NAT (en haut de section 1, par exemple), elles pourraient apparier plus de trafic que destiné et entraîner des règles NAT plus loin en bas de la table de ne jamais être frappé.

**Solution :**

Employez le traceur de paquet afin de déterminer si votre trafic apparie une règle avec les définitions d'objet qui sont trop larges. Si c'est le cas, vous devriez réduire la portée de ces objets, ou déplacez les règles plus loin en bas de la table NAT, ou à la section d'après-automatique (section 3) de la table NAT.

## Problème : Une règle NAT détourne le trafic à une interface incorrecte

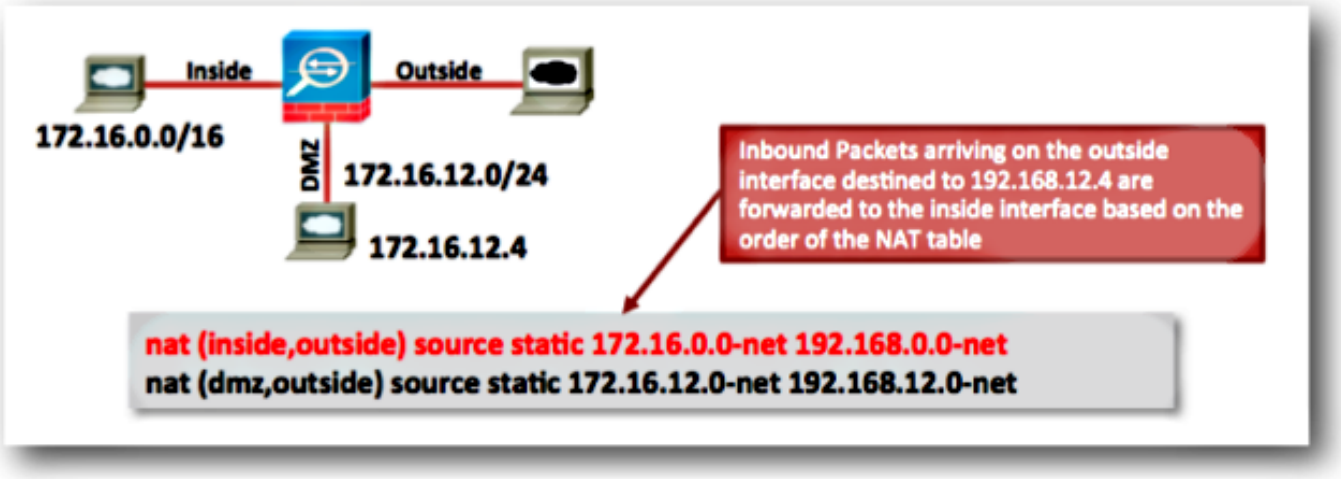
Les règles NAT peuvent avoir la priorité au-dessus de la table de routage quand elles déterminent quelle interface un paquet de sortie l'ASA. Si un paquet entrant apparie une adresse IP traduite dans une déclaration NAT, la règle NAT est utilisée afin de déterminer l'interface de sortie.

Le NAT détournent des contrôles de contrôle (qui est ce qui peut ignorer la table de routage) pour voir s'il y a n'importe quelle règle NAT qui spécifie la translation d'adresses d'adresse de destination pour un paquet entrant qui arrive sur une interface. S'il y a aucune règle qui spécifie

explicitement comment traduire l'adresse IP de la destination de ce paquet, alors la table de routage globale n'est consultée pour déterminer l'interface de sortie. S'il y a une règle qui spécifie explicitement comment traduire l'adresse IP de destination de paquets, alors la règle NAT « tire » le paquet à l'autre interface dans la traduction et la table globale de routage est efficacement sautée.

Ce problème le plus souvent est vu pour le trafic d'arrivée, qui arrive sur l'interface extérieure, et est habituellement dû aux règles NAT en panne qui détournent le trafic aux interfaces fortuites.

Exemple :



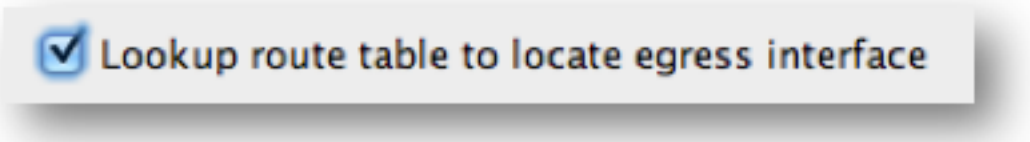

**Solutions :**

Ce problème peut être résolu avec l'un ou l'autre de ces actions :

- Commandez à nouveau la table NAT de sorte que l'entrée plus spécifique soit répertoriée d'abord.
- Utilisez les plages d'adresses IP globales non-recouvertes pour les déclarations NAT.

Notez que si la règle NAT est une règle d'identité, (qui signifie que les adresses IP ne sont pas changées par la règle) alors le mot clé de **recherche de route** peut être utilisé (ce mot clé s'applique pas applicable à l'exemple ci-dessus puisque la règle NAT n'est pas une règle d'identité). Le mot clé de **recherche de route** fait exécuter l'ASA un contrôle supplémentaire quand il apparie une règle NAT. Il vérifie que la table de routage de l'ASA en avant le paquet à la même interface de sortie à laquelle cette configuration NAT détourne le paquet. Si l'interface de sortie de table de routage n'apparie pas le NAT détournent l'interface, la règle NAT n'est pas appariée (la règle est ignorée) et le paquet continue en bas de la table NAT à traiter par une plus défunte règle NAT.

**L'option de recherche de route est seulement disponible si la règle NAT est une règle NAT de « identité », ainsi il signifie que les adresses IP ne sont pas changées par la règle.** L'option de **recherche de route** peut être activée par règle NAT si vous ajoutez la **recherche de route à l'**extrémité de la ligne NAT, ou si vous cochez la **table de routage de consultation pour localiser la** case d'**interface de sortie** dans la configuration de règle NAT dans l'ASDM :




### Problème : Une règle NAT entraîne l'ASA au Protocole ARP (Address Resolution Protocol) de proxy pour le trafic sur l'interface tracée

Les ARPs de proxy ASA pour la plage d'adresses IP globale dans une déclaration NAT sur l'interface globale. Cette fonctionnalité de proxy ARP peut être désactivée sur une base par-NAT de règle si vous ajoutez le mot clé de NO--proxy-**ARP à la** déclaration NAT.

Ce problème est également vu quand le sous-réseau d'adresse globale est par distraction créé pour être beaucoup plus grand qu'il a été destiné pour être.

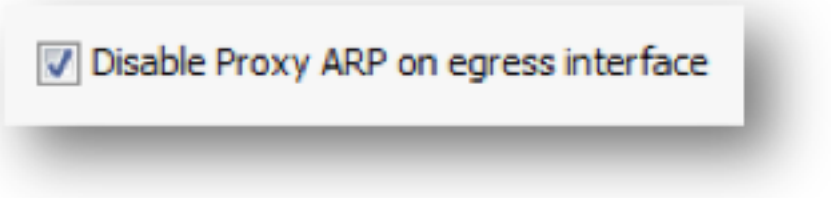
**Solution :**

Ajoutez le mot clé de NO--proxy-**ARP à la** ligne NAT si possible.

Exemple :

```
ASA(config)# object network inside-server
ASA(config-network-object)# nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA(config-network-object)# end
ASA#
ASA# show run nat
object network inside-server
nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA#
```

Ceci peut être également accompli avec l'ASDM. Dans la règle NAT, cochez le **proxy ARP de débronchement sur la** case d'**interface de sortie**.




## Informations connexes

- VIDÉO : Expédition de port ASA pour l'accès de serveur DMZ (versions 8.3 et 8.4)
- Configuration NAT de base ASA : Web server dans le DMZ dans la version 8.3 et ultérieures ASA
- Ouvrage 2 : Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, 9.1
- Support et documentation techniques - Cisco Systems