Dépannage de la configuration de la traduction d'adresses réseau (NAT) ASA

Table des matières

Introduction

Ce document décrit comment dépanner la configuration de la traduction d'adresses de réseau (NAT) sur la plate-forme Cisco Adaptive Security Appliance (ASA).

Conditions préalables

Exigences

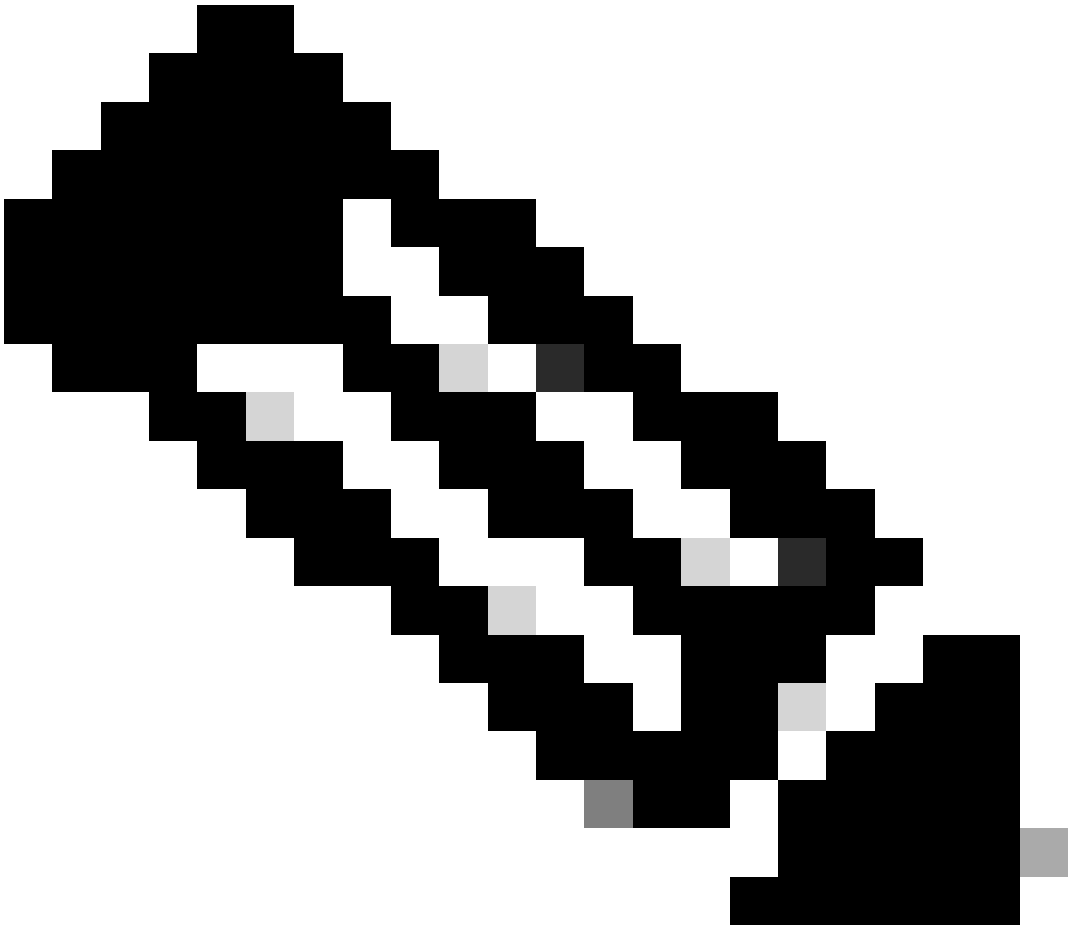
Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations de ce document sont basées sur ASA version 8.3 et ultérieures.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Dépannage de la configuration NAT sur l'ASA



> Remarque : pour obtenir des exemples de configuration NAT de base, notamment une vidéo présentant une configuration NAT de base, reportez-vous à la section Informations connexes au bas de ce document.

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

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

- Les règles de configuration NAT sont hors service. Par exemple, une règle NAT manuelle est placée en haut de la table NAT, ce qui empêche l'exécution de règles plus spécifiques placées plus bas dans la table NAT.
- Les objets réseau utilisés dans la configuration NAT sont trop larges, ce qui entraîne une correspondance accidentelle du trafic avec ces règles NAT et l'absence de règles NAT plus

spécifiques.

L'utilitaire packet tracer peut être utilisé pour diagnostiquer la plupart des problèmes liés à la NAT sur l'ASA. Reportez-vous à la section suivante pour plus d'informations sur la façon dont la configuration NAT est utilisée pour créer la table de stratégie NAT, et sur la façon de dépanner et de résoudre des problèmes NAT spécifiques.

En outre, la commande show nat detail peut être utilisée afin de comprendre quelles règles NAT sont touchées par les nouvelles connexions.

Utilisation de la configuration ASA pour créer la table de stratégie NAT

Tous les paquets traités par l'ASA sont évalués par rapport à la table NAT. Cette évaluation commence en haut (section 1) et se poursuit jusqu'à ce qu'une règle NAT soit mise en correspondance.

En général, une fois qu'une règle NAT est mise en correspondance, cette règle NAT est appliquée à la connexion et plus aucune stratégie NAT n'est vérifiée par rapport au paquet, mais il y a quelques avertissements expliqués ci-dessous.

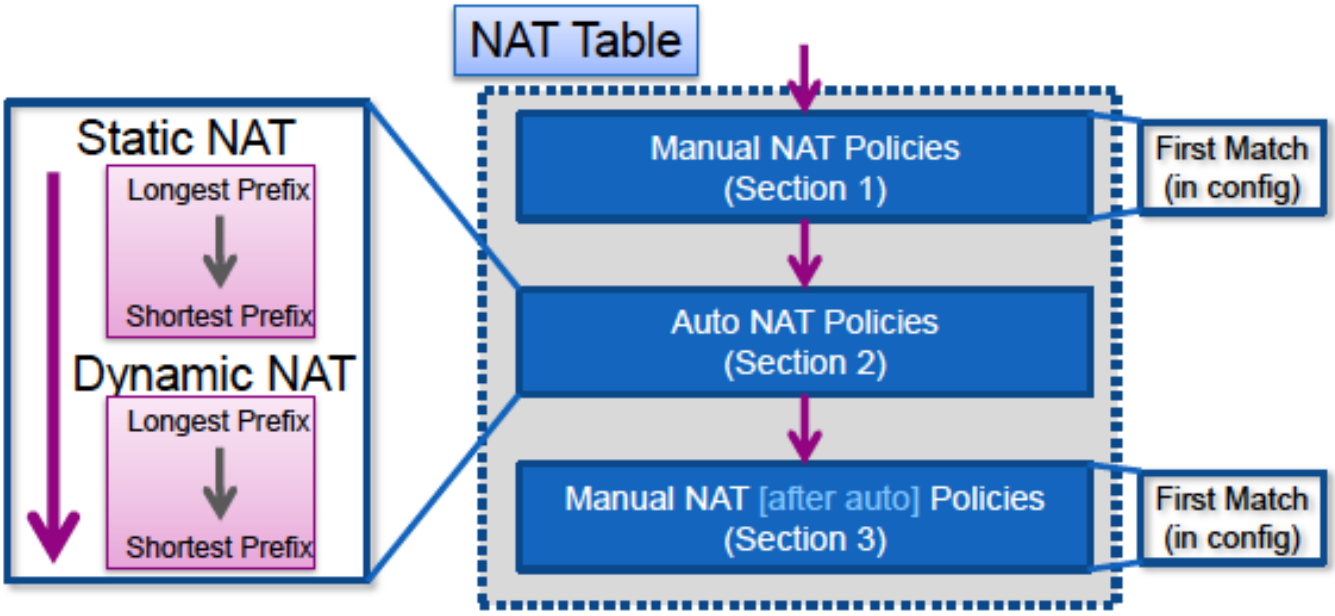
La table de stratégie NAT

La stratégie NAT sur l'ASA est construite à partir de la configuration NAT.

Les trois sections de la table NAT ASA sont les suivantes :

Section 1	Stratégies NAT manuelles Ils sont traités dans l'ordre dans lequel ils apparaissent dans la configuration.
Section 2	Stratégies NAT automatiques Elles sont traitées en fonction du type NAT (statique ou dynamique) et de la longueur du préfixe (masque de sous-réseau) dans l'objet.
Section 3	Politiques NAT manuelles après-auto Ils sont traités dans l'ordre dans lequel ils apparaissent dans la configuration.

Ce diagramme montre les différentes sections NAT et comment elles sont ordonnées :



Correspondance de règle NAT

Section 1

- Un flux est d'abord évalué par rapport à la section 1 de la table NAT qui commence par la première règle.
  - Si l'IP source et de destination du paquet correspondent aux paramètres de la règle NAT manuelle, la traduction est appliquée et le processus s'arrête et aucune autre règle NAT n'est évaluée dans une section.
  - Si aucune règle NAT n'est mise en correspondance, le flux est ensuite évalué par rapport à la section 2 de la table NAT.

Section 2

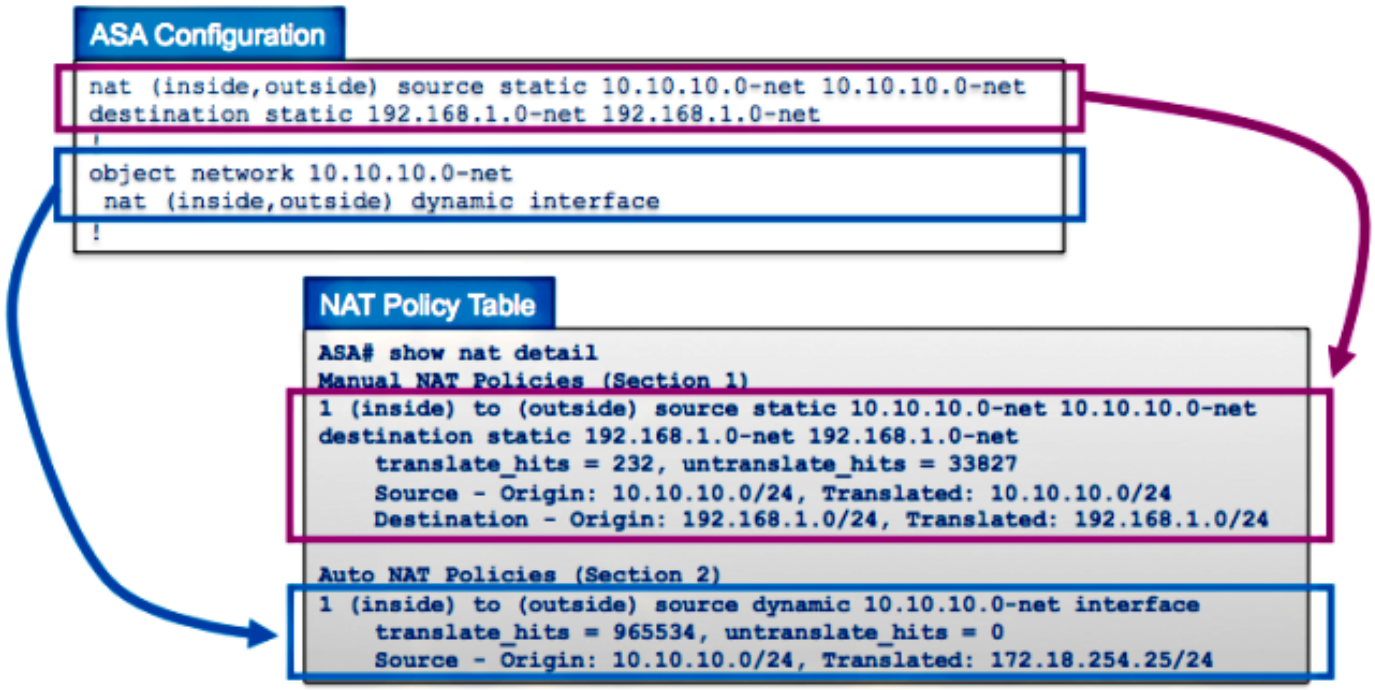
- Un flux est évalué par rapport aux règles NAT de la section 2 dans l'ordre spécifié précédemment, d'abord les règles NAT statiques, puis les règles NAT dynamiques.
  - Si une règle de traduction correspond à l'adresse IP source ou de destination du flux, la traduction peut être appliquée et les autres règles peuvent continuer à être évaluées pour voir si elles correspondent à l'autre adresse IP du flux. Par exemple, une règle NAT automatique peut traduire l'adresse IP source et une autre règle NAT automatique peut traduire la destination.
  - Si le flux correspond à une règle NAT automatique, lorsque la fin de la section 2 est atteinte, la recherche NAT s'arrête et les règles de la section 3 ne sont pas évaluées.
  - Si aucune règle NAT de la section 2 n'est mise en correspondance avec le flux, la recherche passe à la section 3

Section 3

- Le processus de la section 3 est essentiellement le même que celui de la section 1. Si l'IP source et de destination du paquet correspondent aux paramètres de la règle NAT manuelle, la traduction est appliquée et le processus s'arrête et aucune autre règle NAT n'est évaluée

dans une section.

Cet exemple montre comment la configuration NAT ASA avec deux règles (une instruction NAT manuelle et une configuration NAT automatique) sont représentées dans la table NAT :



Résolution des problèmes liés à la fonction NAT

Utilisation de l’utilitaire Packet Tracer

Afin de dépanner les problèmes avec les configurations NAT, utilisez l'utilitaire packet tracer afin de vérifier qu'un paquet atteint la politique NAT. Packet Tracer vous permet de spécifier un exemple de paquet qui entre dans l'ASA, et l'ASA indique quelle configuration s'applique au paquet et s'il est autorisé ou non.

Dans l’exemple suivant, un exemple de paquet TCP qui entre dans l’interface interne et est destiné à un hôte sur Internet est fourni. L'utilitaire Packet Tracer montre que le paquet correspond à une règle NAT dynamique et est traduit en l'adresse IP externe 172.16.123.4 :

<#root>

ASA#

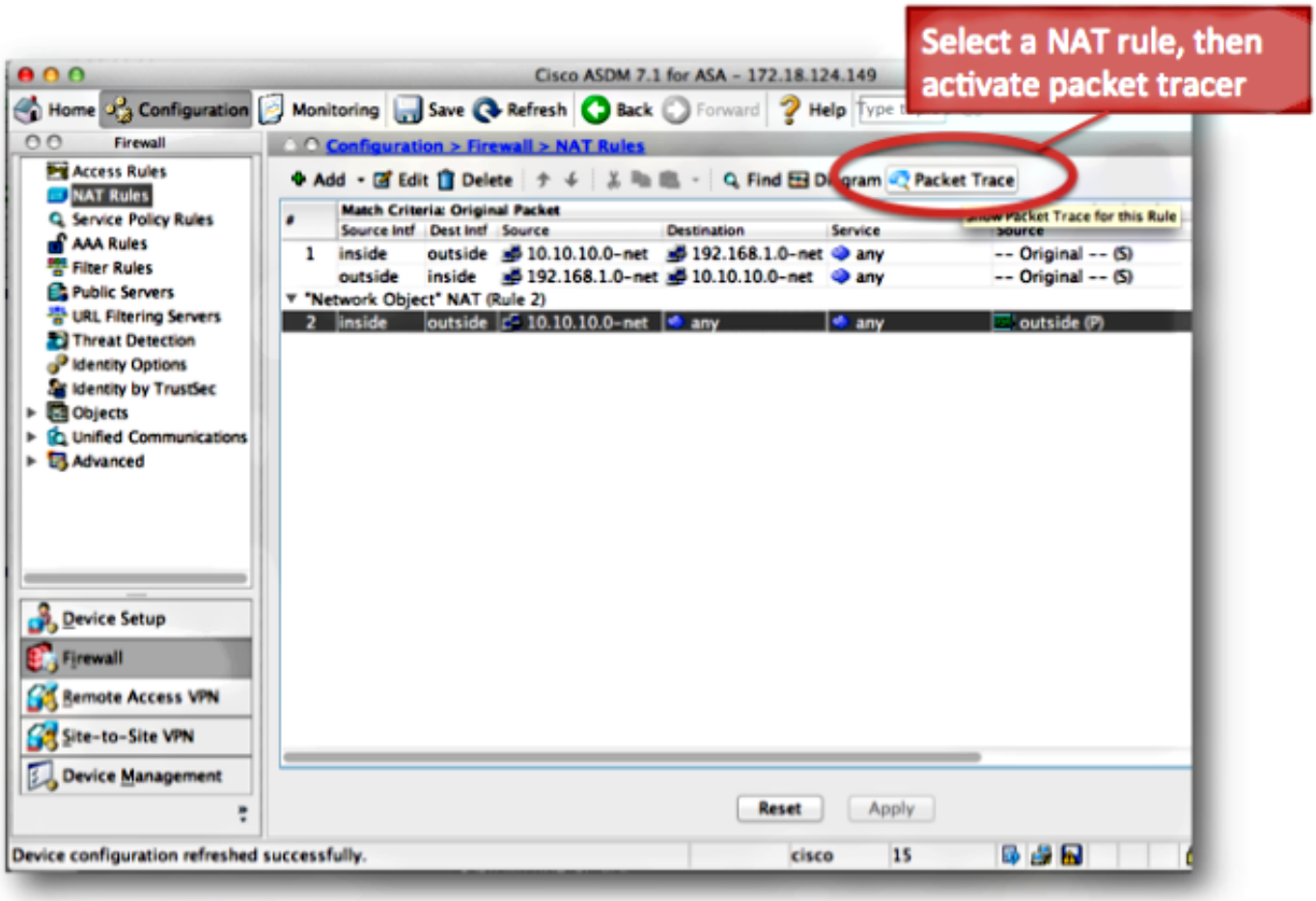
packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(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 Packet Trace afin d'activer le traceur de paquets à partir de Cisco Adaptive Security Device Manager (ASDM). Cette commande utilise les adresses IP spécifiées dans la règle NAT comme entrées pour l'outil Packet Tracer :

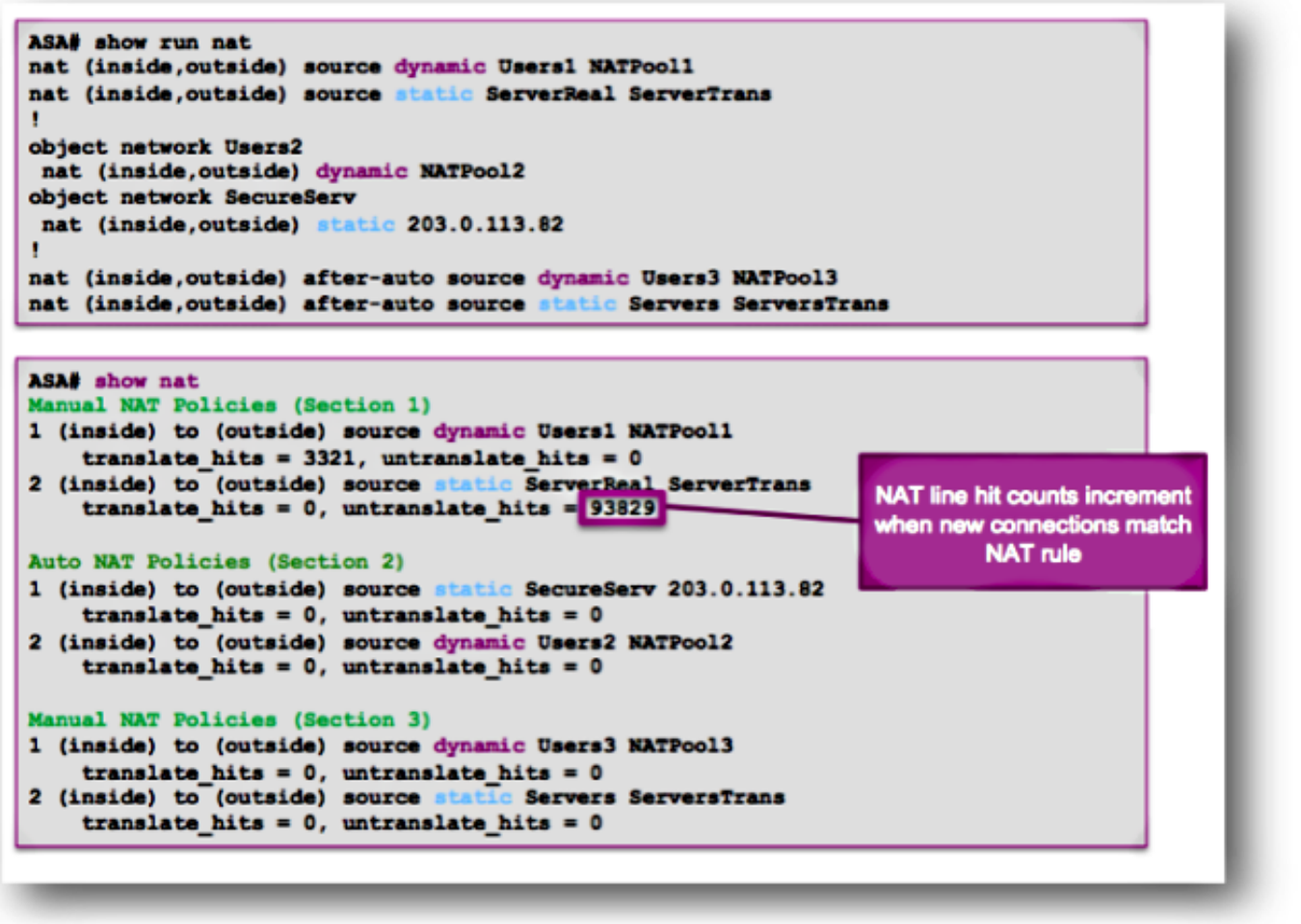


Affichage du résultat de la commande show nat

Le résultat de la commande show nat detail peut être utilisé afin d'afficher la table de stratégie NAT. Plus précisément, les compteurs translate_hits et 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 pas translate_hits ou untranslate_hits, cela signifie que soit le trafic n'arrive pas à l'ASA, soit peut-être une règle différente qui a une priorité plus élevée dans la table NAT correspond au trafic.

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



Dans l'exemple précédent, six règles NAT sont configurées sur cet ASA. Le résultat de show nat montre comment ces règles sont utilisées pour construire la table de stratégie NAT, ainsi que le nombre de translate_hits et de untranslate_hits pour chaque règle.

Ces compteurs d'accès n'incrémentent qu'une fois par connexion. Une fois la connexion établie par l'intermédiaire de l'ASA, les paquets suivants qui correspondent à cette connexion actuelle n'incrémentent pas les lignes NAT (de la même manière que le nombre de succès de la liste d'accès fonctionne sur l'ASA).

Translate_hits : nombre de nouvelles connexions qui correspondent à la règle NAT dans la direction avant.

« Direction avant » signifie que la connexion a été établie via l'ASA dans la direction des interfaces spécifiées dans la règle NAT.

Si une règle NAT a spécifié que le serveur interne est traduit vers l'interface externe, l'ordre des interfaces dans la règle NAT est "nat (inside, outside)..."; si ce serveur initie une nouvelle connexion à un hôte sur l'extérieur, le compteur translate_hit s'incrémente.

Untranslate_hits : Nombre de nouvelles connexions qui correspondent à la règle NAT dans le sens inverse.

Si une règle NAT spécifie que le serveur interne est traduit vers l'interface externe, l'ordre des interfaces dans la règle NAT est "nat (inside, outside)..."; si un client à l'extérieur de l'ASA initie une nouvelle connexion au serveur à l'intérieur, le compteur untranslate_hit s'incrémente.

Encore une fois, si vous voyez que votre nouvelle règle NAT n'a pas translate_hits ou untranslate_hits, cela signifie que soit le trafic n'arrive pas à l'ASA, soit peut-être une règle différente qui a une priorité plus élevée dans la table NAT correspond au trafic.

Méthodologie de dépannage des problèmes NAT

Utilisez packet tracer afin de confirmer qu'un exemple de paquet correspond à la règle de configuration NAT appropriée sur l'ASA. Utilisez la commande show nat detail afin de comprendre quelles règles de stratégie NAT sont atteintes. Si une connexion correspond à une configuration NAT différente de celle attendue, posez les questions suivantes :

- Existe-t-il une autre règle NAT qui prévaut sur la règle NAT que vous aviez l'intention d'atteindre ?
- Existe-t-il une autre règle NAT avec des définitions d'objet trop larges (le masque de sous-réseau est trop court, par exemple 255.0.0.0) qui fait que ce trafic correspond à la mauvaise règle ?
- Les stratégies NAT manuelles sont-elles désordonnées, ce qui entraîne la correspondance du paquet avec la mauvaise règle ?
- Votre règle NAT est-elle configurée de manière incorrecte, ce qui entraîne une non-correspondance de la règle avec votre trafic ?

Reportez-vous à la section suivante pour obtenir des exemples de problèmes et de solutions.

Problèmes courants avec les configurations NAT

Voici quelques problèmes courants rencontrés lors de la configuration de la fonction NAT sur l'ASA.

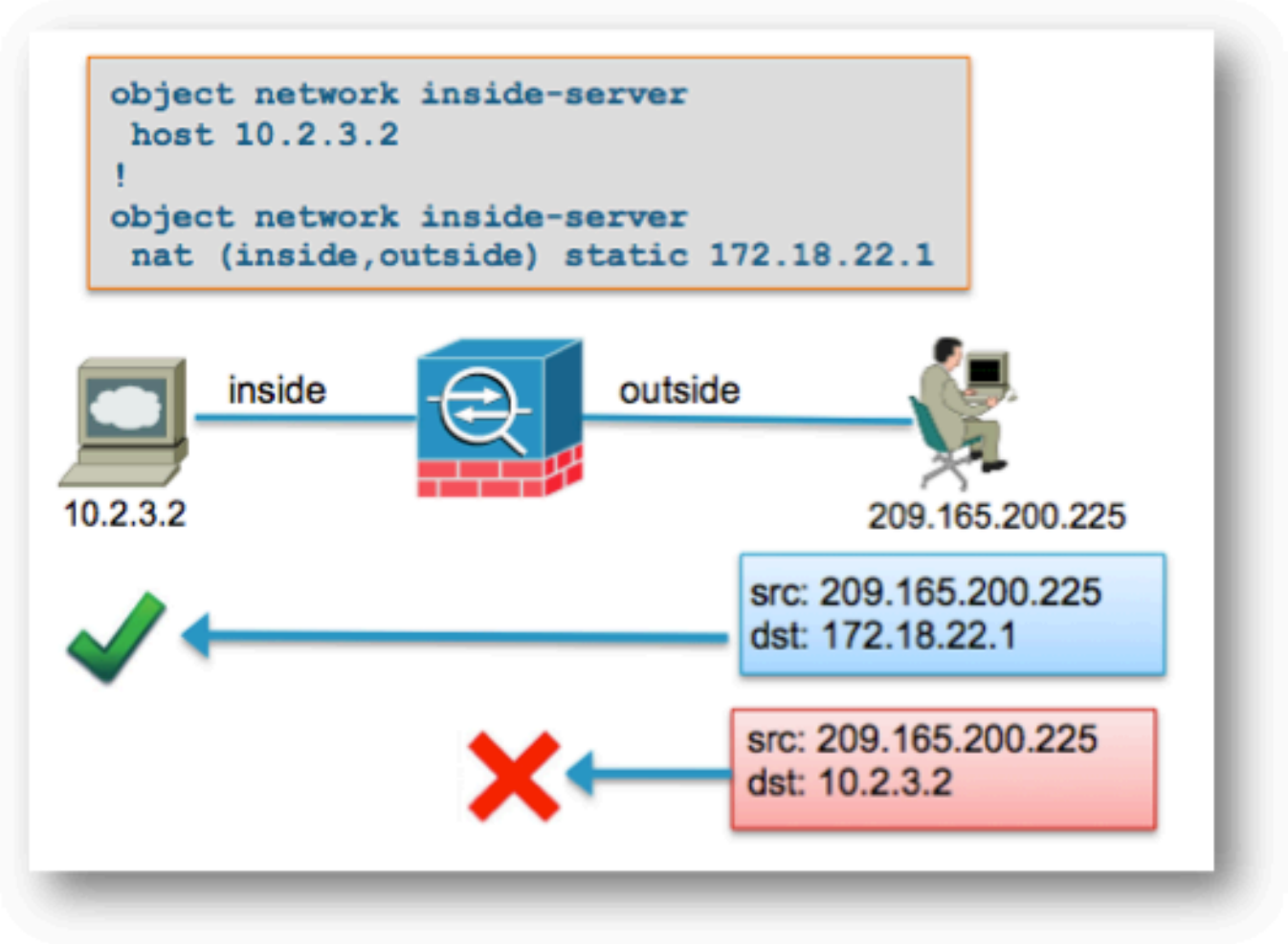
Problème : le trafic échoue en raison de la défaillance du chemin inverse NAT (RPF) Erreur : les règles NAT asymétriques correspondent pour les flux aller et retour

Le contrôle NAT RPF garantit qu'une connexion qui est traduite par l'ASA dans le sens direct,

comme la synchronisation TCP (SYN), est traduite par la même règle NAT dans le sens inverse, comme la synchronisation TCP/accusé de réception (ACK).

Le plus souvent, ce problème est causé par des connexions entrantes destinées à l'adresse locale (non traduite) dans une instruction NAT. Au niveau de base, le NAT RPF vérifie que la connexion inverse du serveur au client correspond à la même règle NAT ; dans le cas contraire, le contrôle NAT RPF échoue.

Exemple : 209.165.200.225



Quand l'hôte externe à 192.168.200.225 envoie un paquet destiné directement à l'adresse IP locale (non traduite) de 10.2.3.2, l'ASA abandonne le paquet et consigne ce syslog :

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Solution :

Assurez-vous tout d’abord que l’hôte envoie les données à l’adresse NAT globale correcte. Si

l'hôte envoie des paquets destinés à l'adresse correcte, vérifiez les règles NAT qui sont atteintes 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 l'ordre des règles NAT est approprié.

Utilisez l'utilitaire Packet Tracer afin de spécifier les détails du paquet refusé. Packet Tracer doit afficher le paquet abandonné en raison de l'échec de la vérification RPF.

Ensuite, examinez la sortie de Packet Tracer afin de voir quelles règles NAT sont atteintes dans la phase NAT et la phase NAT-RPF.

Si un paquet correspond à une règle NAT dans la phase NAT RPF-check, qui indique que le flux inverse atteindrait une traduction NAT, mais ne correspond pas à une règle dans la phase NAT, qui indique que le flux direct n'atteindrait PAS une règle NAT, le paquet est abandonné.

Ce résultat correspond au scénario illustré dans le schéma précédent, où l'hôte externe envoie incorrectement le trafic à l'adresse IP locale du serveur et non à l'adresse IP globale (traduite) :

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 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)#
```

Lorsque le paquet est destiné à l'adresse IP mappée correcte de 172.18.22.1, le paquet correspond à la règle NAT correcte dans la phase UN-NAT dans le sens direct, et à la même règle dans la phase NAT RPF-check :

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 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

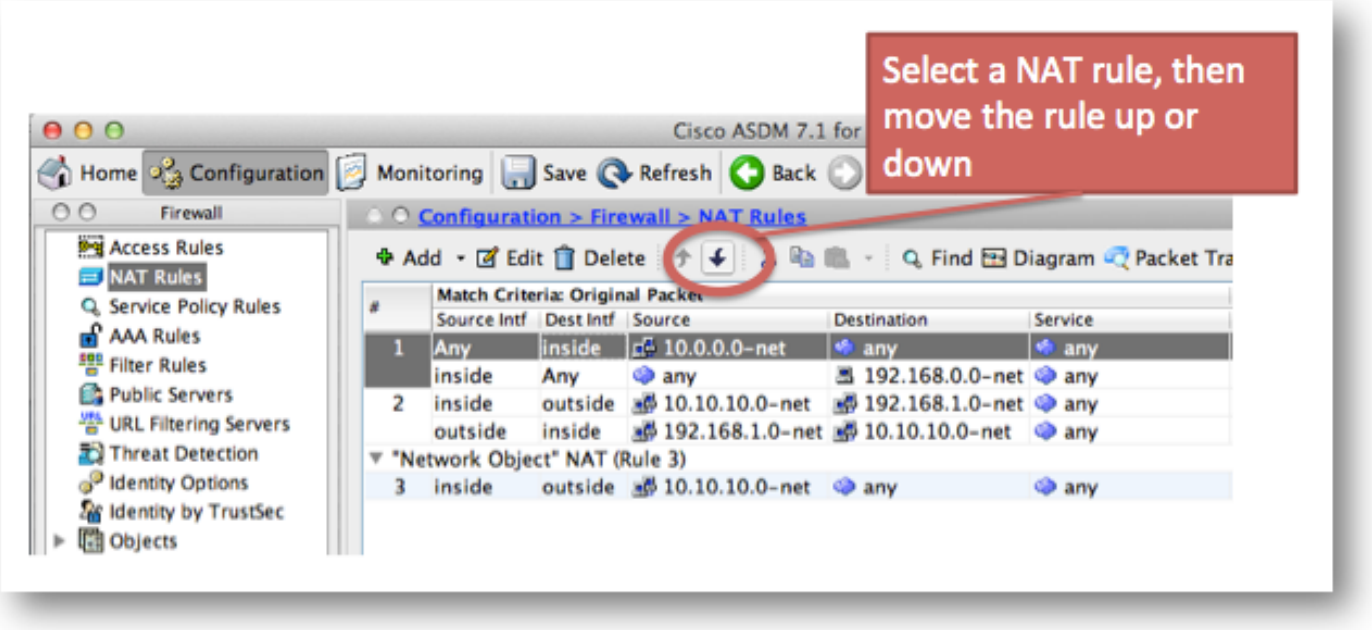
```
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

Problème : les règles NAT manuelles sont désordonnées, ce qui entraîne des correspondances de paquets incorrectes

Les règles NAT manuelles sont traitées en fonction de leur apparence dans la configuration. Si une règle NAT très large est répertoriée en premier dans la configuration, elle peut remplacer une autre règle plus spécifique plus loin dans la table NAT. Utilisez Packet Tracer afin de vérifier quelle règle NAT votre trafic atteint ; il peut être nécessaire de réorganiser les entrées NAT manuelles dans un ordre différent.

Solution :

Réorganisez les règles NAT avec ASDM.



Solution :

Les règles NAT peuvent être réorganisées avec l'interface de ligne de commande si vous supprimez la règle et la réinsérez à un numéro de ligne spécifique. Afin d'insérer une nouvelle règle sur une ligne spécifique, entrez le numéro de ligne juste après la spécification des interfaces.

Exemple :

<#root>

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 fait correspondre certains trafics par inadvertance. Parfois, des règles NAT sont créées qui utilisent des objets trop larges. Si ces règles sont placées près du haut de la table NAT (en haut de la section 1, par exemple), elles peuvent correspondre à plus de trafic que prévu et faire en sorte que les règles NAT plus loin dans la table ne soient jamais atteintes.

Solution

Utilisez Packet Tracer afin de déterminer si votre trafic correspond à une règle avec des définitions d'objet trop larges. Si c'est le cas, vous devez réduire la portée de ces objets, ou déplacer les règles plus loin dans la table NAT, ou vers la section after-auto (Section 3) de la table NAT.

Problème

Une règle NAT détourne le trafic vers une interface incorrecte. Les règles NAT peuvent avoir priorité sur la table de routage lorsqu'elles déterminent quelle interface un paquet sort de l'ASA. Si un paquet entrant correspond à une adresse IP traduite dans une instruction NAT, la règle NAT est utilisée afin de déterminer l'interface de sortie.

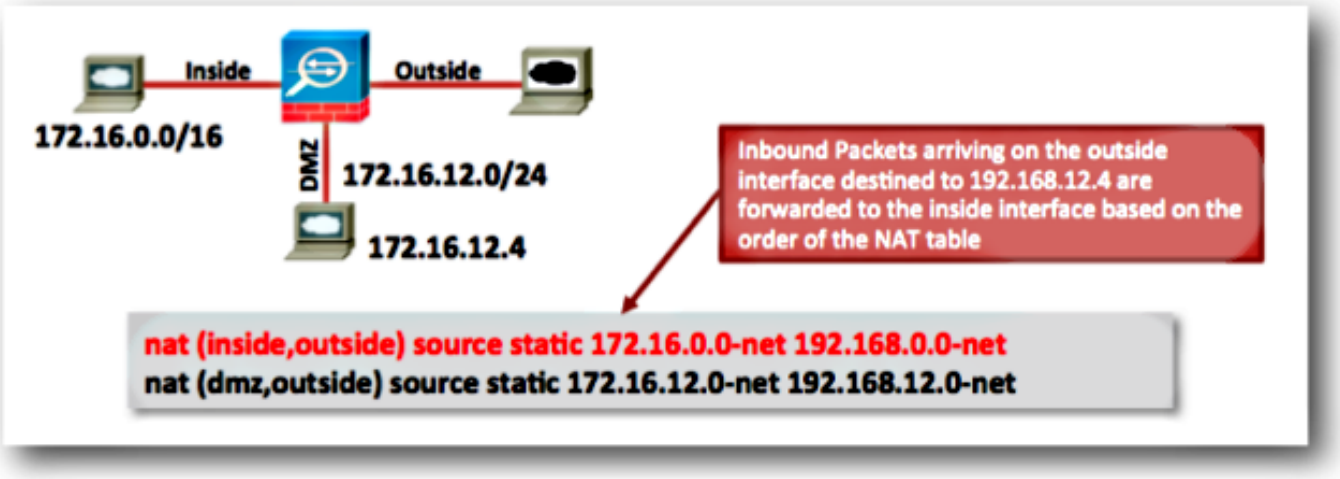
La vérification de renvoi NAT (qui peut remplacer la table de routage) vérifie s'il existe une règle NAT qui spécifie la traduction d'adresse de destination pour un paquet entrant qui arrive sur une interface.

Si aucune règle ne spécifie explicitement comment traduire cette adresse IP de destination de paquet, la table de routage globale est consultée pour déterminer l'interface de sortie.

S'il existe une règle qui spécifie explicitement comment traduire l'adresse IP de destination du paquet, alors la règle NAT extrait le paquet vers l'autre interface dans la traduction et la table de routage globale est effectivement contournée.

Ce problème est le plus souvent rencontré pour le trafic entrant, qui arrive sur l'interface externe, et est généralement dû à des règles NAT désordonnées qui détournent le trafic vers des interfaces non voulues.

Exemple :



Solutions :

Ce problème peut être résolu avec l'une des actions suivantes :

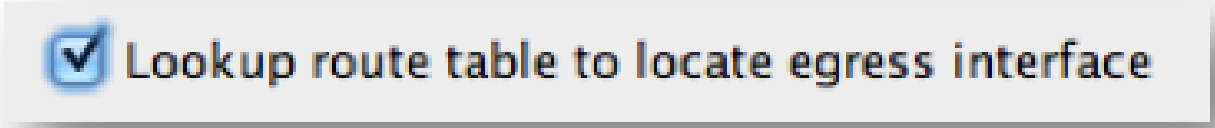
- Réorganisez la table NAT de sorte que l'entrée plus spécifique apparaisse en premier.
- Utilisez des plages d'adresses IP globales sans chevauchement pour les instructions NAT.

Notez que si la règle NAT est une règle d'identité, (ce qui signifie que les adresses IP ne sont pas modifiées par la règle) alors le mot clé route-lookup peut être utilisé (ce mot clé n'est pas applicable à l'exemple précédent puisque la règle NAT n'est pas une règle d'identité).

Le mot clé route-lookup entraîne l'ASA à effectuer une vérification supplémentaire lorsqu'il correspond à une règle NAT. Il vérifie que la table de routage de l'ASA transfère le paquet à la même interface de sortie vers laquelle cette configuration NAT le détourne.

Si l'interface de sortie de la table de routage ne correspond pas à l'interface de renvoi NAT, la règle NAT n'est pas mise en correspondance (la règle est ignorée) et le paquet continue vers le bas de la table NAT pour être traité par une règle NAT ultérieure.

L'option route-lookup n'est disponible que si la règle NAT est une règle NAT d'identité, ce qui signifie que les adresses IP ne sont pas modifiées par la règle. L'option route-lookup peut être activée par règle NAT si vous ajoutez route-lookup à la fin de la ligne NAT, ou si vous cochez la case Lookup route table to locate exit interface dans la configuration de la règle NAT dans ASDM :



Problème : une règle NAT amène l'ASA à utiliser le protocole ARP (Address Resolution Protocol) proxy pour le trafic sur l'interface mappée

Proxy ASA ARP pour la plage d'adresses IP globales dans une instruction NAT sur l'interface globale. Cette fonctionnalité ARP de proxy peut être désactivée sur une base de règle NAT si vous ajoutez le mot clé no-proxy-arp à l'instruction NAT.

Ce problème se produit également lorsque le sous-réseau d'adresses globales est créé par inadvertance pour être beaucoup plus grand que prévu.

Solution

Ajoutez si possible le mot clé no-proxy-arp à la ligne NAT.

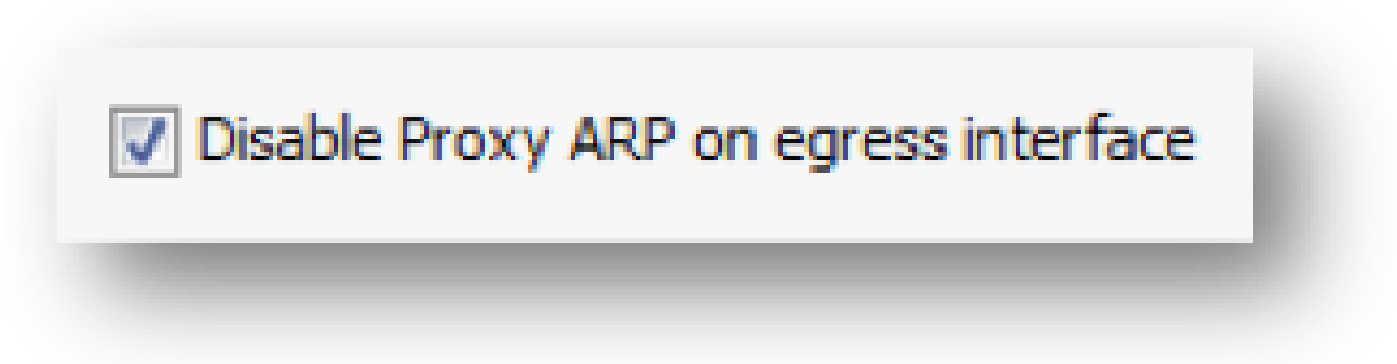
Exemple :

<#root>

```
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#
```

Cela peut également être réalisé avec l'ASDM. Dans la règle NAT, cochez la case Disable Proxy ARP on exit interface.



.

Informations connexes

- VIDÉO : Transfert de port ASA pour l'accès au serveur DMZ (versions 8.3 et 8.4)
- Configuration NAT ASA de base : serveur Web dans la DMZ dans ASA version 8.3 et ultérieure
- Livre 2 : Guide de configuration de l'interface de ligne de commande du pare-feu Cisco ASA 9.1
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.