Exemples et références de NAT

Les rubriques suivantes fournissent des exemples de configuration de la NAT, ainsi que des renseignements sur la configuration et le dépannage avancés.

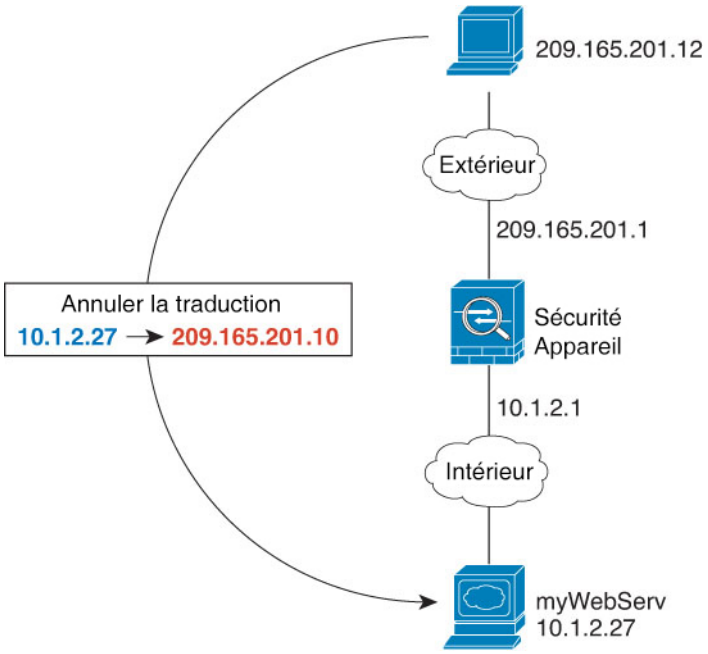
Exemples de NAT d'objets réseau

Voici quelques exemples de configuration pour la NAT d'objet réseau.

Fournir l'accès à un serveur Web interne (NAT statique)

Dans l'exemple suivant, une NAT statique est effectuée pour un serveur Web interne. L'adresse réelle se trouve sur un réseau privé, une adresse publique est donc requise. Une NAT statique est nécessaire pour que les hôtes puissent initier le trafic vers le serveur Web à une adresse fixe.

Illustration 1 : NAT statique pour un serveur Web interne



Procédure

Étape 1 Créez un objet réseau pour le serveur Web interne.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

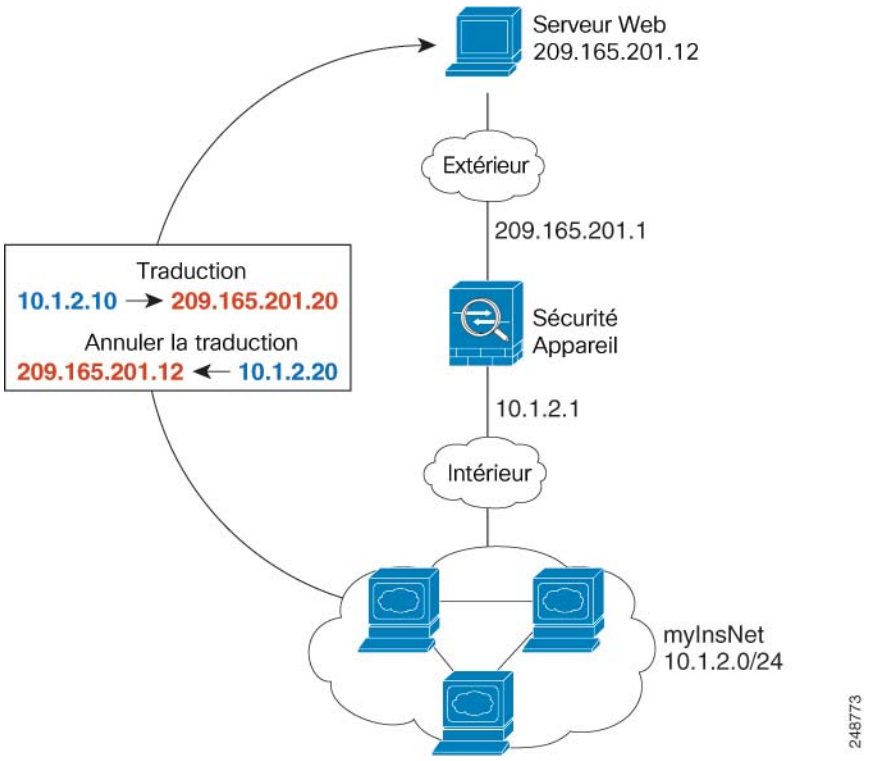
Étape 2 Configurez la NAT statique pour l'objet :

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

NAT pour les hôtes internes (NAT dynamique) et NAT pour un serveur Web externe (NAT statique)

Dans l'exemple suivant, la NAT dynamique est configurée pour les utilisateurs internes sur un réseau privé lorsqu'ils accèdent à l'extérieur. De plus, lorsque des utilisateurs internes se connectent à un serveur Web externe, l'adresse du serveur Web est traduite en une adresse qui semble se trouver sur le réseau interne.

Illustration 2 : NAT dynamique pour l'interne, NAT statique pour le serveur Web externe



Procédure

Étape 1 Créez un objet réseau pour l'ensemble de NAT dynamique vers lequel vous souhaitez traduire les adresses internes.

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

Étape 2 Créez un objet réseau pour le réseau interne.

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

Étape 3 Activez la NAT dynamique pour le réseau interne à l'aide de l'objet pool de NAT dynamique.

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

Étape 4 Créez un objet réseau pour le serveur Web externe.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

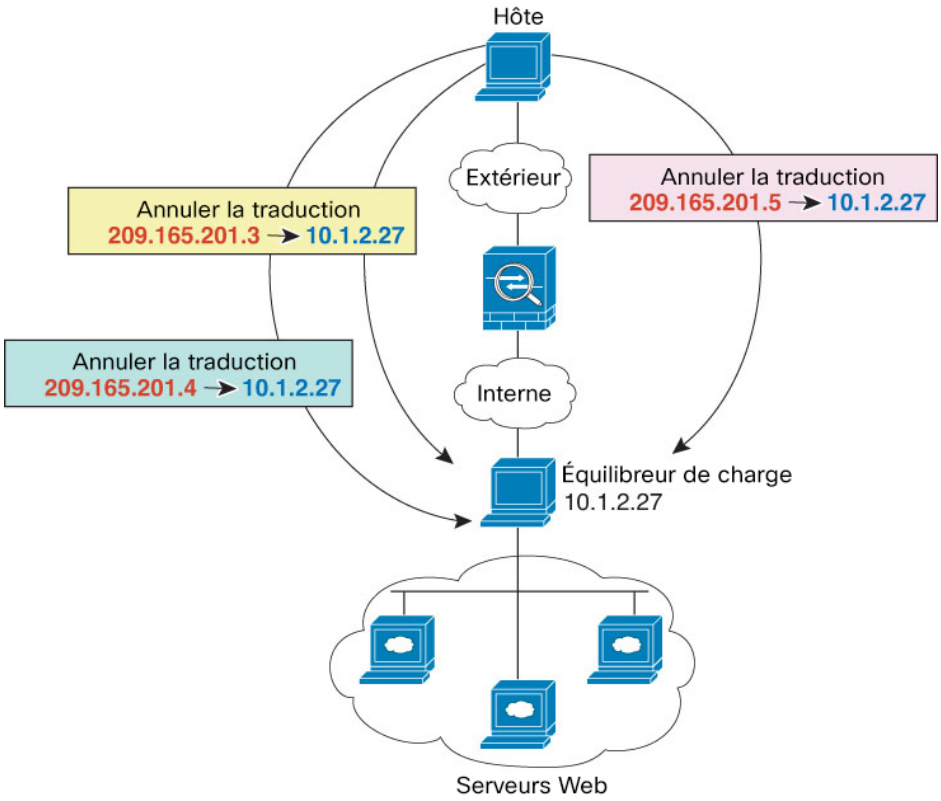
Étape 5 Configurez la NAT statique pour le serveur Web.

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs)

L'exemple suivant montre un équilibreur de charge interne qui se traduit en plusieurs adresses IP. Lorsqu'un hôte externe accède à l'une des adresses IP mappées, celle-ci n'est pas traduite en adresse unique de l'équilibreur de charge. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

Illustration 3 : NAT statique avec règle One-to-Many (un vers plusieurs) pour un équilibreur de charge interne



Procédure

Étape 1 Créez un objet réseau pour les adresses auxquelles vous souhaitez mapper l'équilibreur de charge.

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

Étape 2 Créez un objet réseau pour l'équilibreur de charge.

```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27
```

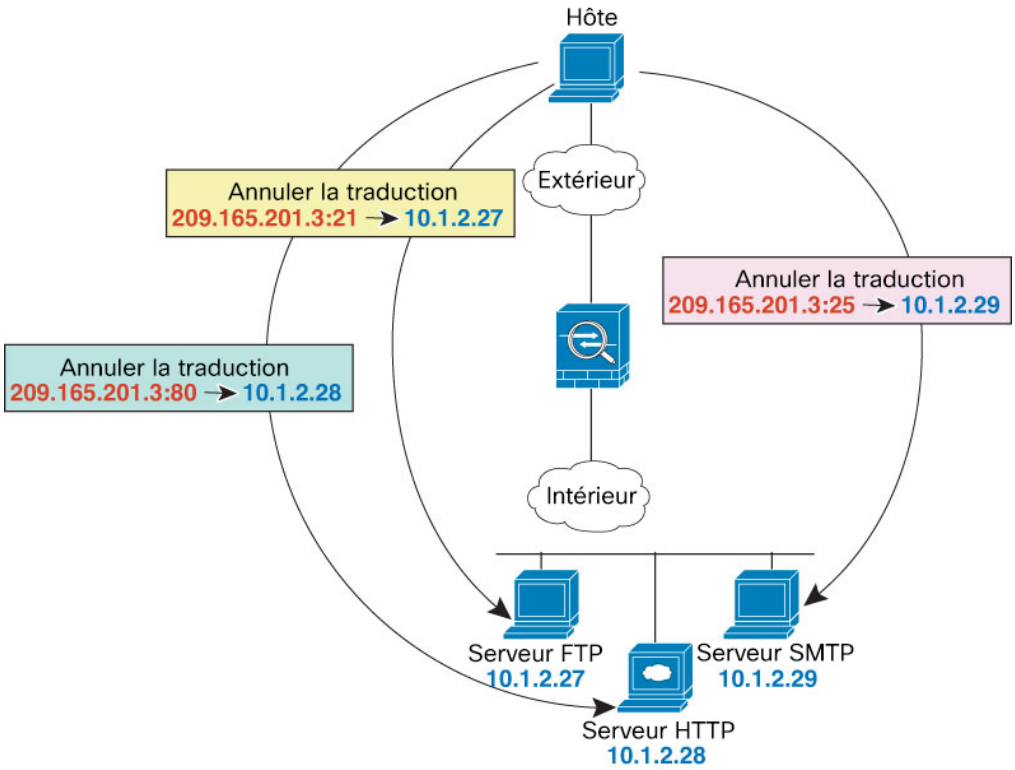
Étape 3 Configurez la NAT statique pour l'équilibreur de charge appliquant l'objet de plage.

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port)

L'exemple de NAT statique avec traduction de port statique suivant fournit une adresse unique permettant aux utilisateurs distants d'accéder à FTP, HTTP et SMTP. Ces serveurs sont en fait des périphériques différents sur le réseau réel, mais pour chaque serveur, vous pouvez spécifier des règles NAT statiques avec des règles de traduction de port qui utilisent la même adresse IP mappée, mais des ports différents.

Illustration 4 : NAT statique avec traduction de port



Procédure

Étape 1 Créez un objet réseau pour le serveur FTP et configurez la NAT statique avec la traduction de port, en mappant le port FTP sur lui-même.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
 ftp
```

Étape 2 Créez un objet réseau pour le serveur HTTP et configurez la NAT statique avec la traduction de port, en mappant le port HTTP sur lui-même.

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp http
 http
```

Étape 3 Créez un objet réseau pour le serveur SMTP et configurez la NAT statique avec la traduction de port, en mappant le port SMTP sur lui-même.

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp smtp
 smtp
```

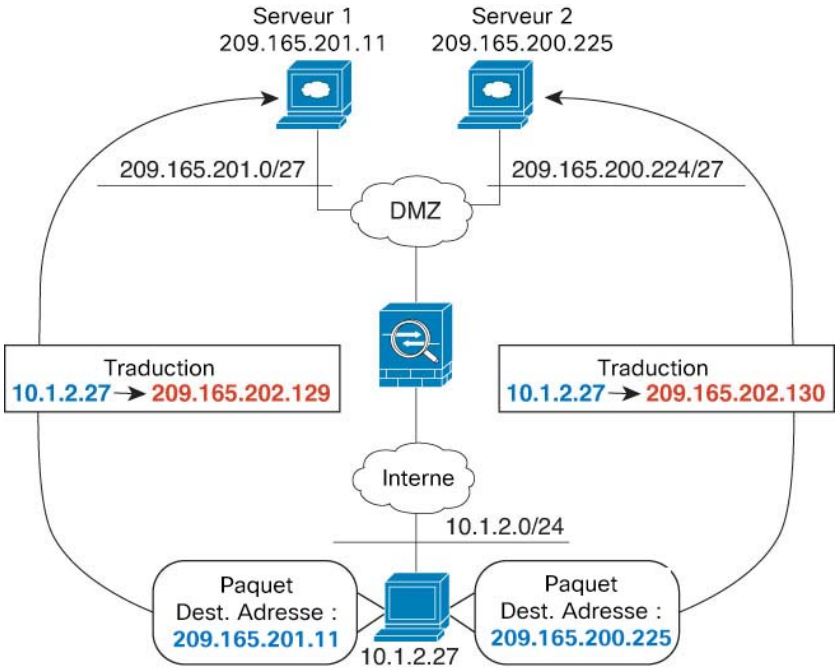
Exemples pour la NAT Twice

Cette section inclut les exemples de configuration suivants :

Traduction différente selon la destination (PAT manuelle dynamique)

La figure suivante montre un hôte sur le réseau 10.1.2.0/24 accédant à deux serveurs différents. Lorsque l'hôte accède au serveur par l'adresse 209.165.201.11, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au serveur à partir de l'adresse 209.165.200.225, l'adresse réelle est traduite en 209.165.202.130 :*port*.

Illustration 5 : NAT manuelle avec différentes adresses de destination



Procédure

Étape 1 Créez un objet réseau pour le réseau interne

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

Étape 2 Créez un objet réseau pour le réseau DMZ 1

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

Étape 3 Ajoutez un objet réseau pour l'adresse PAT :

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

Étape 4 Configurez la première règle de NAT manuelle

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite.

Étape 5 Ajoutez un objet réseau pour le réseau DMZ 2.

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

Étape 6 Ajoutez un objet réseau pour l'adresse PAT :

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

Étape 7 Configurez la deuxième règle NAT manuelle :

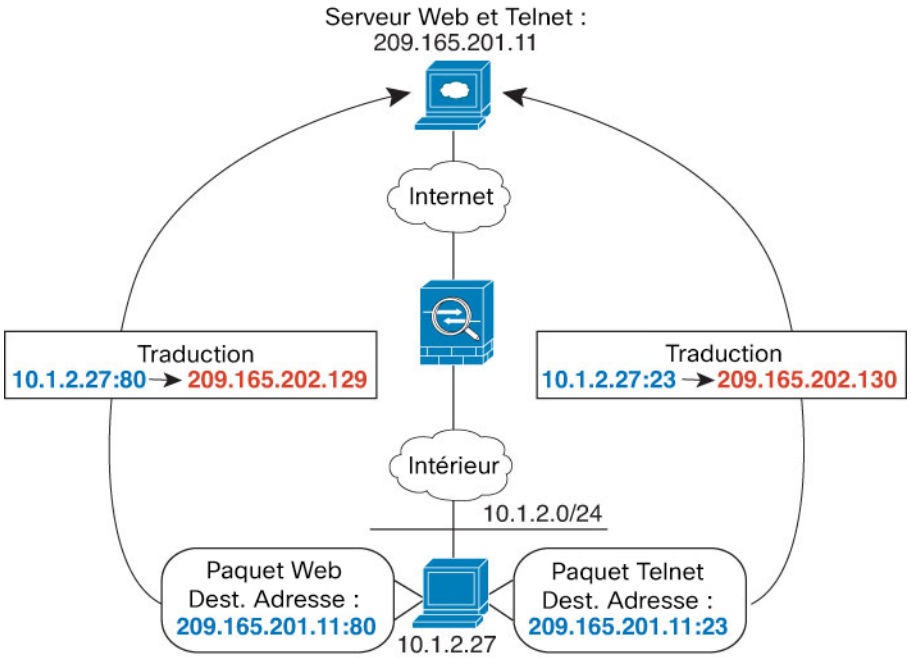
Exemple :

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

Traduction différente selon l'adresse et le port de destination (PAT dynamique)

La figure suivante montre l'utilisation des ports source et de destination. L'hôte du réseau 10.1.2.0/24 accède à un hôte unique pour les services Web et Telnet. Lorsque l'hôte accède au serveur pour les services Telnet, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au même serveur pour les services Web, l'adresse réelle est traduite par 209.165.202.130 :*port*.

Illustration 6 : NAT Twice avec différents ports de destination



Procédure

Étape 1 Ajoutez un objet réseau pour le réseau interne.

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

Étape 2 Ajoutez un objet réseau pour le serveur Telnet/Web.

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

Étape 3 Ajoutez un objet réseau pour l'adresse PAT lorsque vous utilisez Telnet.

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

Étape 4 Ajoutez un objet de service pour Telnet :

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

Étape 5 Configurez la première règle NAT Twice :

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour ceux-ci en spécifiant la même adresse pour les adresses de destination réelles et mappées, et le même port pour le service réel et mappé.

Étape 6 Ajoutez un objet réseau pour l'adresse PAT lorsque vous utilisez HTTP.

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

Étape 7 Ajoutez un objet de service pour HTTP :

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

Étape 8 Configurez la deuxième règle NAT manuelle :

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
```

```
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

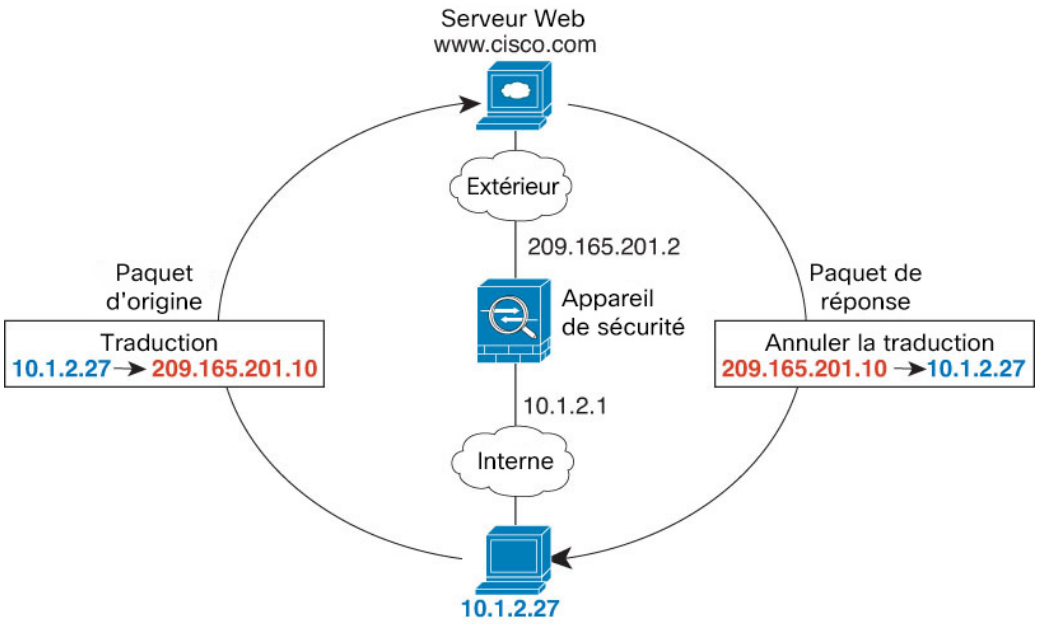
NAT en mode routage et transparent

Vous pouvez configurer la NAT en mode de pare-feu routé et transparent. Les sections suivantes décrivent l'utilisation typique de chaque mode de pare-feu.

NAT en mode routé

La figure suivante montre un exemple de NAT typique en mode routé, avec un réseau privé à l'intérieur.

Illustration 7 : Exemple de NAT : mode routé



1. Lorsque l'hôte interne en 10.1.2.27 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.2.27, est convertie en une adresse mappée, 209.165.201.10.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.10, et l'ASA reçoit le paquet, car l'ASA effectue un ARP mandataire pour réclamer le paquet.
3. L'ASA remplace ensuite la traduction de l'adresse mappée, 209.165.201.10, par l'adresse réelle, 10.1.2.27, avant de l'envoyer à l'hôte.

NAT en mode transparent ou dans un groupe de pont

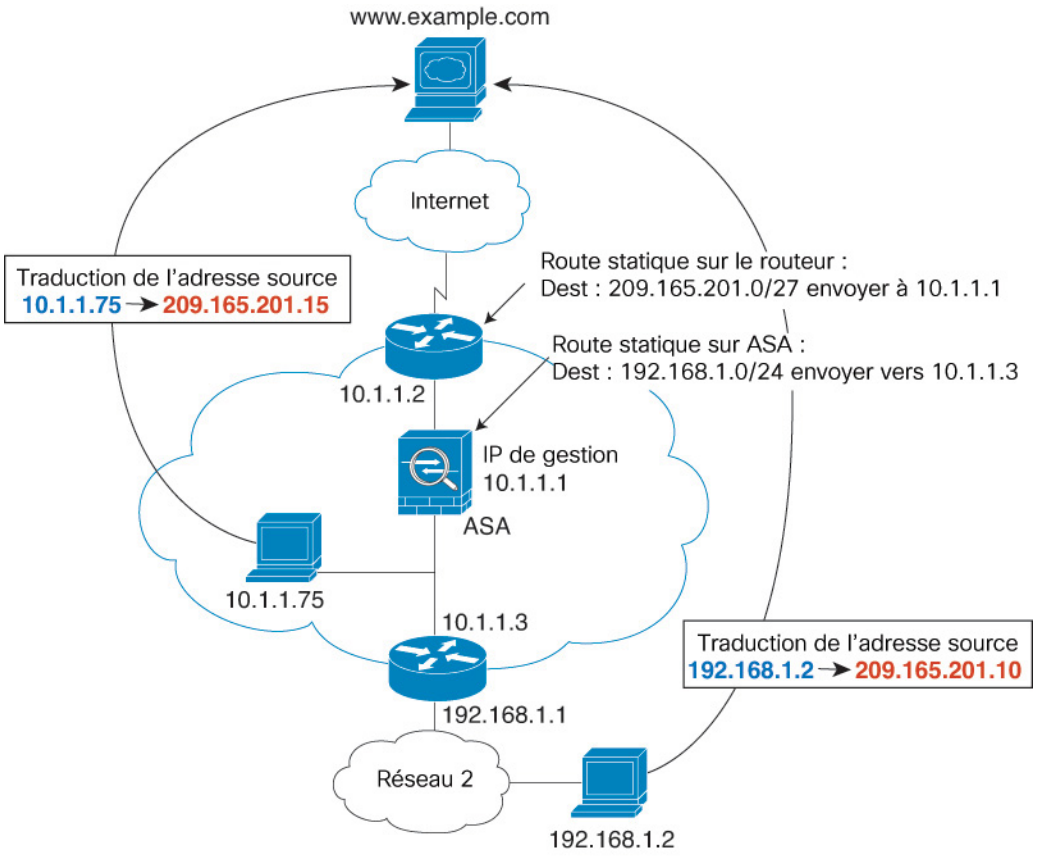
L'utilisation de la NAT en mode transparent élimine le besoin pour les routeurs en amont ou en aval d'effectuer la NAT pour leurs réseaux. Il peut remplir une fonction similaire dans un groupe de ponts en mode routé.

La NAT en mode transparent, ou en mode routé entre les membres d'un même groupe de ponts, comporte les exigences et les limites suivantes :

- Vous ne pouvez pas configurer l'interface PAT lorsque l'adresse mappée est une interface de membre d'un groupe de ponts, car aucune adresse IP n'est associée à l'interface.
- L'inspection ARP n'est pas prise en charge. De plus, si, pour une raison quelconque, un hôte de l'un des côtés de l'ASA envoie une requête ARP à un hôte de l'autre côté de l'ASA et que l'adresse réelle de l'hôte initiateur est mappée à une adresse différente sur le même sous-réseau, l'adresse réelle reste visible dans la requête ARP.
- La traduction entre des réseaux IPv4 et IPv6 n'est pas prise en charge. La traduction entre deux réseaux IPv6 ou entre deux réseaux IPv4 est prise en charge.

La figure suivante montre un scénario NAT typique en mode transparent, avec le même réseau sur les interfaces interne et externe. Le pare-feu transparent dans ce scénario effectue le service NAT, de sorte que le routeur en amont n'a pas à effectuer de NAT.

Illustration 8 : Exemple NAT : mode transparent



1. Lorsque l'hôte interne en 10.1.1.75 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.1.75, est remplacée par une adresse mappée, 209.165.201.15.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.15, et ASA reçoit le paquet, car le routeur en amont inclut ce réseau mappé dans une voie de routage statique dirigée vers l'adresse IP de gestion ASA.

3. ASA annule ensuite la traduction de l'adresse mappée, 209.165.201.15, vers l'adresse réelle, 10.1.1.1.75. Comme l'adresse réelle est directement connectée, l'ASA l'envoie directement à l'hôte.
4. Pour l'hôte 192.168.1.2, le même processus se produit, sauf pour le trafic de retour, l'ASA recherche la voie de routage dans sa table de routage et envoie le paquet au routeur en aval à l'adresse 10.1.1.3 en fonction de la route statique ASA pour 192.168.1.0 /24.

Routage des paquets NAT

L'ASA doit être la destination de tous les paquets envoyés à l'adresse mappée. L'ASA doit également déterminer l'interface de sortie de tous les paquets qu'il reçoit et qui sont destinés aux adresses mappées. Cette section décrit comment l'ASA gère l'acceptation et la livraison des paquets avec la NAT.

Adresses mappées et routage

Lorsque vous traduisez l'adresse réelle en adresse mappée, l'adresse mappée que vous choisissez détermine comment configurer le routage, le cas échéant, pour l'adresse mappée.

Consultez les lignes directrices supplémentaires concernant les adresses IP mappées dans Lignes directrices supplémentaires pour la NAT.

Les rubriques suivantes expliquent les types d'adresses mappées.

Adresses sur le même réseau que l'interface mappée

Si vous utilisez des adresses sur le même réseau que l'interface mappée, l'ASAutilise un serveur mandataire ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car ASA n'a pas à constituer la passerelle pour d'autres réseaux. Cette solution est idéale si le réseau externe contient un nombre adéquat d'adresses libres, une considération si vous utilisez une traduction 1:1 comme la NAT dynamique ou statique. La PAT dynamique étend considérablement le nombre de traductions que vous pouvez utiliser avec un petit nombre d'adresses. Ainsi, même si les adresses disponibles sur le réseau externe sont petites, cette méthode peut être utilisée. Pour PAT, vous pouvez même utiliser l'adresse IP de l'interface mappée.

Remarque Si vous configurez l'interface mappée sur n'importe quelle interface et que vous spécifiez une adresse mappée sur le même réseau que l'une des interfaces mappées, si une requête ARP pour cette adresse mappée arrive sur une interface *différente*, vous devez configurer manuellement une entrée ARP pour ce réseau sur l'interface d'entrée, en précisant son adresse MAC. En règle générale, si vous spécifiez une interface pour l'interface mappée, vous utilisez un réseau unique pour les adresses mappées, cette situation ne se produit donc pas. Configurez l'ARP à l'aide de la commande **arp**.

Adresses sur un réseau unique

Si vous avez besoin de plus d'adresses qu'il n'y en a sur le réseau d'interface de destination (mappé), vous pouvez identifier les adresses sur un autre sous-réseau. Le routeur en amont a besoin d'une route statique pour les adresses mappées qui pointe vers ASA.

Sinon, pour le mode routé, vous pouvez configurer une voie de routage statique sur ASA pour les adresses mappées en utilisant n'importe quelle adresse IP du réseau de destination comme passerelle, puis redistribuer

la voie de routage en utilisant votre protocole de routage. Par exemple, si vous utilisez la NAT pour le réseau interne (10.1.1.0/24) et que vous utilisez l'adresse IP mappée 209.165.201.5, vous pouvez configurer une voie de routage statique pour 209.165.201.5 255.255.255.255 (adresse de l'hôte) vers le périphérique 10.165.201.5. Passerelle 1.99 qui peut être redistribuée.

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

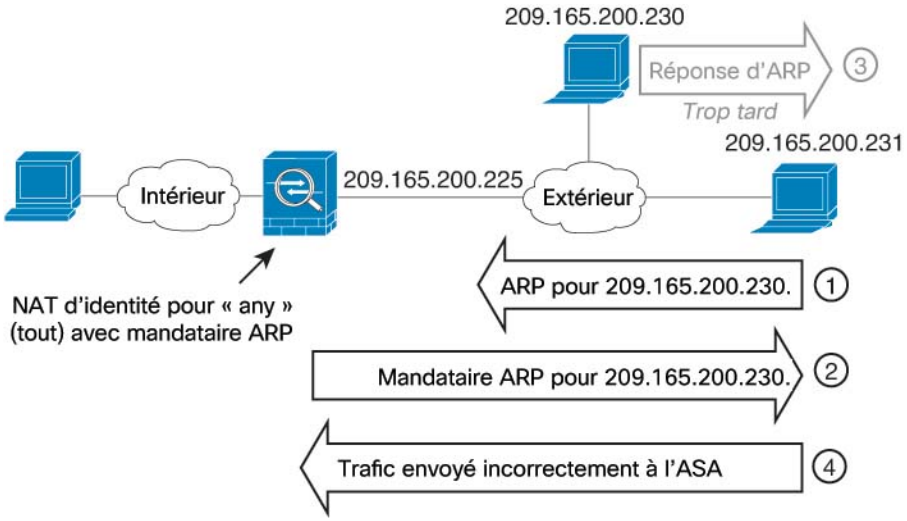
Pour le mode transparent, si l'hôte réel est connecté directement, configurez la voie de routage statique sur le routeur en amont pour pointer vers ASA : spécifiez l'adresse IP du groupe de ponts. Pour les hôtes distants en mode transparent, dans la voie de routage statique sur le routeur en amont, vous pouvez également spécifier l'adresse IP du routeur en aval.

Même adresse que l'adresse réelle (NAT d'identité)

Dans le comportement par défaut de la NAT d'identité, le mandataire ARP est activé, ce qui correspond aux autres règles NAT statiques. Vous pouvez désactiver le mandataire ARP si vous le souhaitez. Vous pouvez également désactiver le mandataire ARP pour la NAT statique normale si vous le souhaitez, auquel cas vous devez vous assurer d'avoir les routages appropriés sur le routeur en amont.

Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité. Par exemple, si vous configurez une règle NAT d'identité large pour « n'importe quelle » adresse IP, laisser le mandataire ARP activé peut entraîner des problèmes pour les hôtes du réseau directement connectés à l'interface mappée. Dans ce cas, quand un hôte sur le réseau mappé souhaite communiquer avec un autre hôte sur le même réseau, l'adresse de la demande ARP correspond à la règle NAT (qui correspond à « n'importe quelle » adresse). L'ASA fera ensuite passer l'ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à ASA. (Notez que ce problème se produit même si vous avez une règle NAT Twice ; bien que la règle NAT doive correspondre aux adresses source et de destination, la décision du protocole ARP est prise uniquement en fonction de l'adresse « source »). Si la réponse ARP ASA est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers ASA.

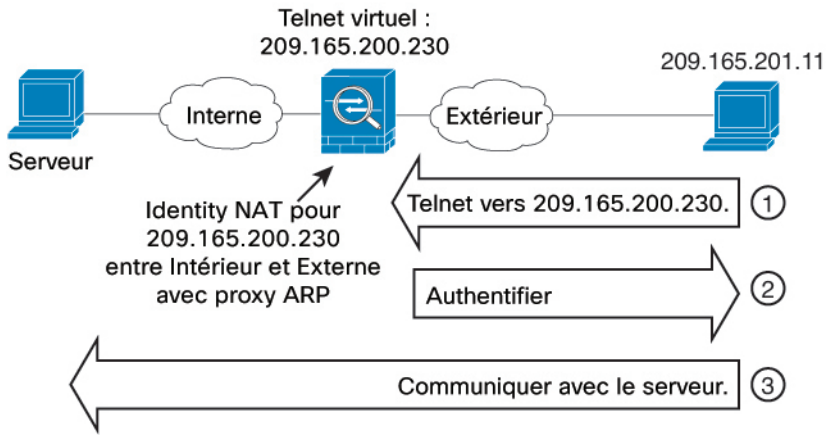
Illustration 9 : Problèmes de mandataire ARP avec la NAT d'identité



Dans de rares cas, vous avez besoin d'un ARP mandataire pour la NAT d'identité; par exemple pour le Telnet virtuel. Lors de l'utilisation de l'AAA pour l'accès au réseau, un hôte doit s'authentifier auprès de l'ASA à

l'aide d'un service tel que Telnet avant que tout autre trafic ne puisse être transmis. Vous pouvez configurer un serveur Telnet virtuel sur l'ASA pour fournir les informations de connexion nécessaires. Lorsque vous accédez à l'adresse Telnet virtuelle depuis l'extérieur, vous devez configurer une règle NAT d'identité pour l'adresse spécifiquement pour la fonctionnalité ARP du proxy. En raison des processus internes de Telnet virtuel, le mandataire ARP permet à l'ASA de conserver le trafic destiné à l'adresse Telnet virtuelle au lieu d'envoyer ce dernier vers l'interface source conformément à la règle NAT. (Voir la figure suivante.)

Illustration 10 : ARP mandataire et Telnet virtuel



Exigences de routage en mode transparent pour les réseaux distants

Lorsque vous utilisez la NAT en mode transparent, certains types de trafic nécessitent des routes statiques. Consultez le guide de configuration des opérations générales pour en savoir plus.

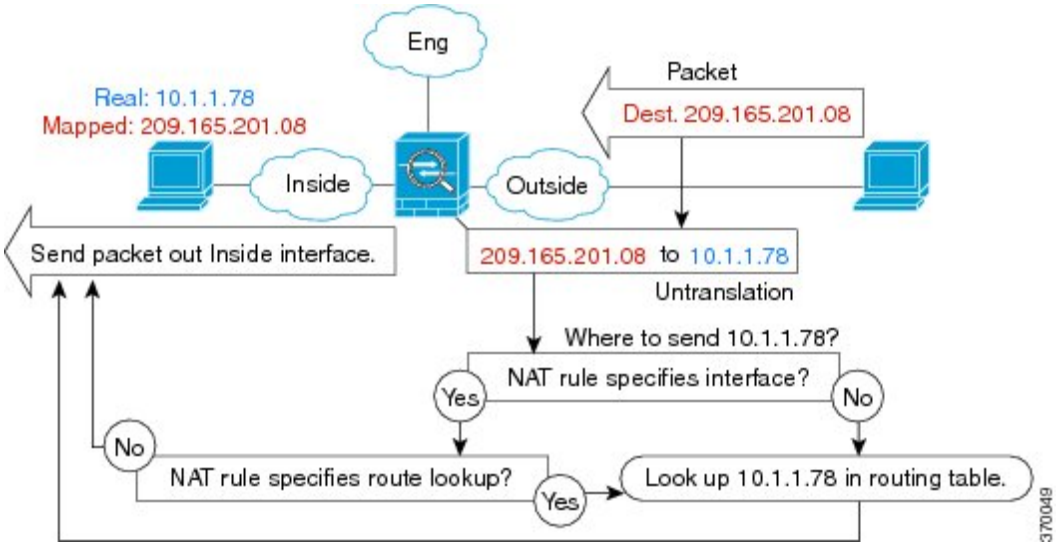
Détermination de l'interface de sortie

Lorsque vous utilisez la NAT et que l'ASA reçoit du trafic pour une adresse mappée, l'ASA détraduit l'adresse de destination en fonction de la règle NAT, puis il envoie le paquet vers l'adresse réelle. L'ASA détermine l'interface de sortie pour le paquet comme suit :

- Interfaces de groupe de ponts en mode transparent ou en mode routé : l'ASA détermine l'interface de sortie pour l'adresse réelle à l'aide de la règle NAT ; vous devez préciser les interfaces de membre du groupe de ponts source et de destination dans le cadre de la règle NAT.
- Interfaces standard en mode routé : l'ASA détermine l'interface de sortie de l'une des manières suivantes :
  - Vous configurez l'interface dans la règle NAT : l'ASA utilise la règle NAT pour déterminer l'interface de sortie. Cependant, vous avez la possibilité d'utiliser à la place une recherche de routage. Dans certains scénarios, un remplacement de recherche de routage est requis.
  - Vous ne configurez pas l'interface dans la règle NAT : l'ASA utilise une recherche de routage pour déterminer l'interface de sortie.

La figure suivante montre la méthode de sélection de l'interface de sortie en mode routé. Dans presque tous les cas, une recherche de routage est équivalente à l'interface de règle NAT, mais dans certaines configurations, les deux méthodes peuvent différer.

Illustration 11 : Sélection de l'interface de sortie en mode routé avec NAT



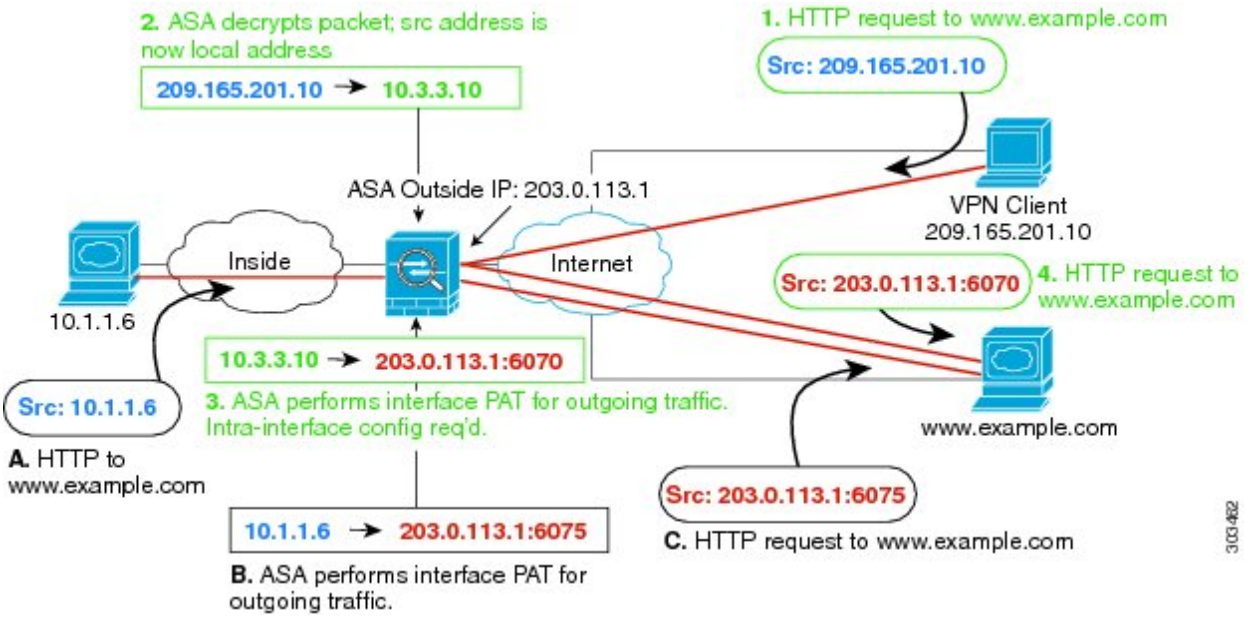
NAT pour VPN

Les rubriques suivantes expliquent l'utilisation de la NAT avec les différents types de VPN.

NAT et VPN d'accès à distance

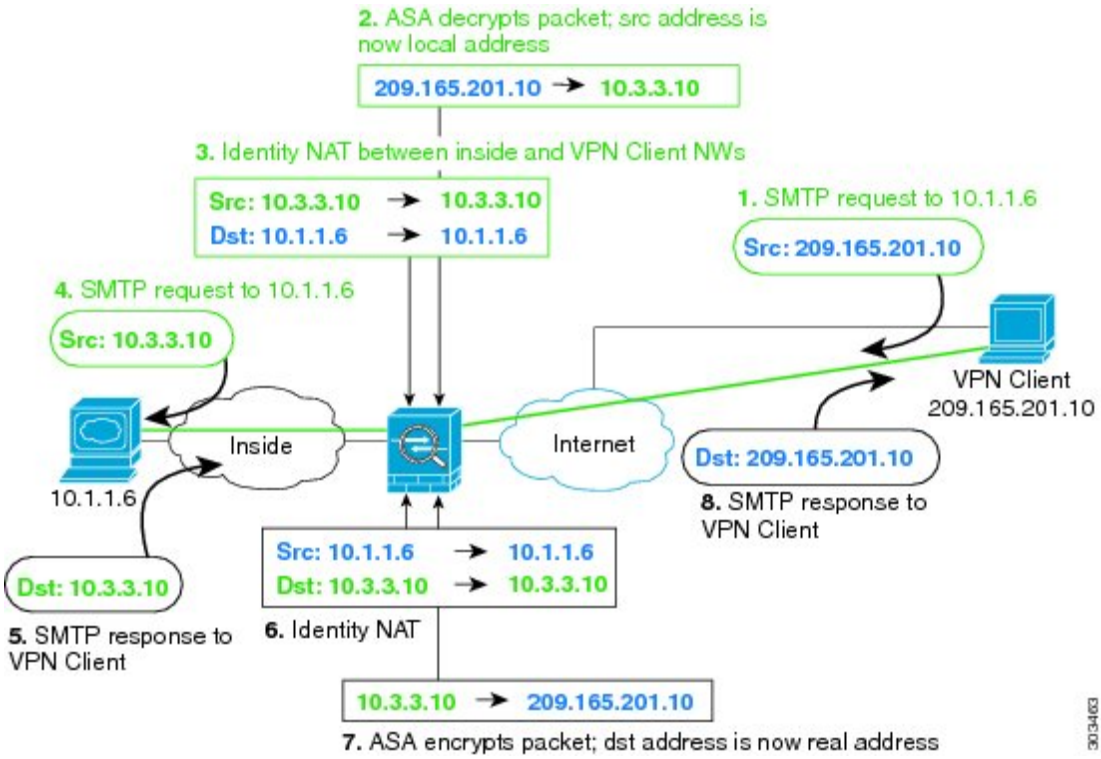
La figure suivante montre un serveur interne (10.1.1.6) et un client VPN (209.165.201.10) qui accèdent à Internet. Sauf si vous configurez la tunnellisation fractionnée pour le client VPN (où seul le trafic spécifié passe par le tunnel VPN), le trafic VPN lié à Internet doit également passer par l'ASA. Lorsque le trafic VPN entre dans l'ASA, l'ASA déchiffre le paquet; le paquet obtenu comprend l'adresse locale du client VPN (10.3.3.10) comme source. Pour les réseaux internes et de clients VPN, vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Pour permettre au trafic VPN de quitter la même interface par laquelle il est entré, vous devez également activer la communication intra-interface (également connue sous le nom de mise en réseau en épingle à cheveux).

Illustration 12 : PAT d'interface pour le trafic VPN lié à Internet (intra-interface)



La figure suivante montre un client VPN qui souhaite accéder à un serveur de messagerie interne. Comme l'ASA s'attend à ce que le trafic entre le réseau interne et tout réseau externe corresponde à la règle PAT de l'interface que vous avez configurée pour l'accès Internet, le trafic du client VPN (10.3.3.10) vers le serveur SMTP (10.1.1.6) sera abandonné en raison d'un échec de chemin inverse : le trafic de 10.3.3.10 à 10.1.1.6 ne correspond pas à une règle NAT, mais le trafic de retour de 10.1.1.6 à 10.3.3.10 *doit* correspondre à la règle PAT de l'interface pour le trafic sortant. Comme les flux avant et inverse ne correspondent pas, l'ASA abandonne le paquet lorsqu'il est reçu. Pour éviter cette défaillance, vous devez exempter le trafic interne vers client VPN de la règla PAT d'interface en utilisant une règle NAT d'identité entre ces réseaux. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 13 : NAT d'identité pour les clients VPN



Consultez l'exemple de configuration NAT suivant pour le réseau ci-dessus :

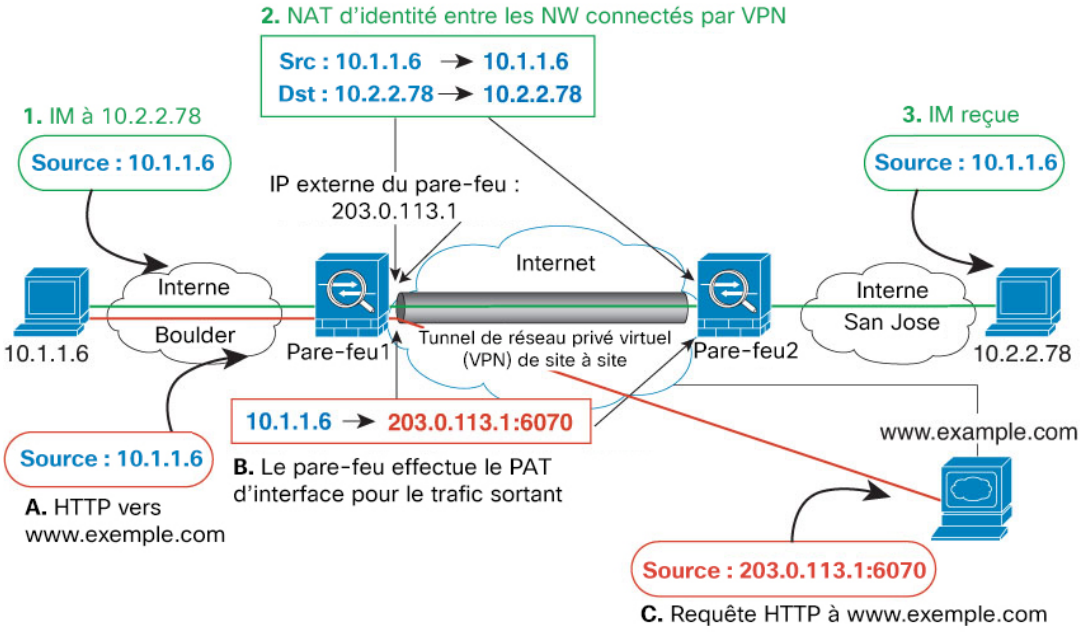
```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

NAT et VPN de site à site

La figure suivante montre un tunnel de site à site connectant les bureaux de Bouder et de San Jose. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de la section 10.1.1.6 à Boulder vers www.exemple.com), vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Cependant, pour le trafic que vous souhaitez acheminer par le tunnel VPN (par exemple, de la version 10.1.1.6 à Boulder au 10.2.2.78 à San Jose), vous ne souhaitez

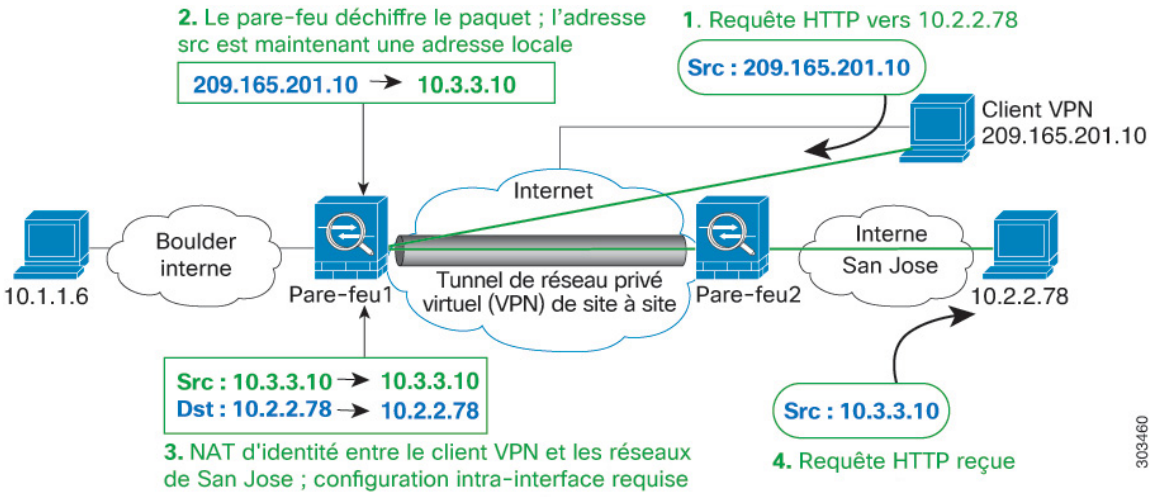
pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 14 : PAT d'interface et NAT d'identité pour le VPN de site à site



La figure suivante montre un client VPN connecté à Pare-feu1 (Boulder), avec une requête Telnet pour un serveur (10.2.2.78) accessible par un tunnel de site à site entre Pare-feu1 et Pare-feu2 (San Jose). Comme il s'agit d'une connexion en épingle à cheveux, vous devez activer la communication intra-interface, qui est également requise pour le trafic à destination d'Internet par tunnellisation non divisée en provenance du client VPN. Vous devez également configurer la NAT d'identité entre le client VPN et les réseaux de Boulder et San Jose, comme vous le feriez entre n'importe quel réseau connecté par VPN pour exempter ce trafic des règles de la NAT sortante.

Illustration 15 : Accès du client VPN au VPN de site à site



Consultez l'exemple de configuration NAT suivant pour Firewall1 (Boulder) pour le deuxième exemple :

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside
```

Consultez l'exemple de configuration NAT suivant pour Firewall2 (San Jose) :

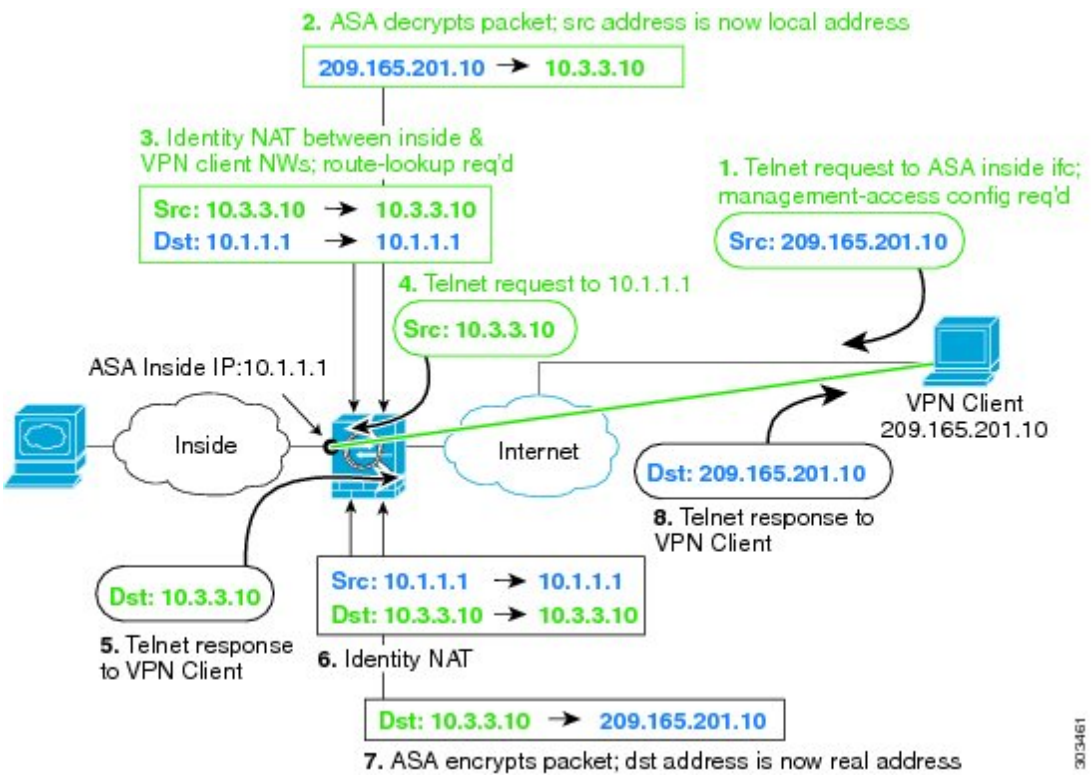
```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```

Accès à la gestion de la NAT et du VPN

Lorsque vous utilisez le VPN, vous pouvez autoriser l'accès de gestion à une interface autre que celle à partir de laquelle vous avez saisi l'ASA (voir la commande **management-access**). Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSH, Telnet ou SNMP ; ou vous pouvez envoyer un message Ping à l'interface interne.

La figure suivante montre un client VPN qui établit une session Telnet avec l'interface interne de l'ASA. Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité selon NAT et VPN d'accès à distance, à la page 15 ou NAT et VPN de site à site, à la page 17, vous devez configurer la NAT avec l'option de recherche de routage. Sans recherche de routage, l'ASA envoie le trafic hors de l'interface spécifiée dans la commande NAT, indépendamment de ce que dit la table de routage; dans l'exemple ci-dessous, l'interface de sortie est l'interface interne. Vous ne souhaitez pas que l'ASA envoie le trafic de gestion au réseau interne; il ne reviendra jamais à l'adresse IP de l'interface interne. L'option recherche de routage permet à l'ASA d'envoyer le trafic directement à l'adresse IP de l'interface interne plutôt qu'au réseau interne. Pour le trafic du client VPN vers un hôte du réseau interne, l'option de recherche de routage aboutira toujours à l'interface de sortie correcte (interne), de sorte que le flux de trafic normal n'est pas affecté. Consultez la section Détermination de l'interface de sortie, à la page 14 pour plus d'informations sur l'option de recherche de routage.

Illustration 16 : Accès à la gestion du VPN



Consultez l'exemple de configuration NAT suivant pour le réseau ci-dessus :

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
```

```
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

Dépannage de la NAT et du VPN

Consultez les outils de surveillance suivants pour résoudre les problèmes de NAT avec le VPN :

- Packet tracer : lorsqu'il est utilisé correctement, Packet Tracer indique les règles NAT auxquelles un paquet correspond.
- **show nat detail** : affiche le nombre d'accès et le trafic non traduit pour une règle NAT donnée.
- **show conn all** : permet d'afficher les connexions actives, y compris le trafic vers et à partir du boîtier.

Pour vous familiariser avec une configuration non fonctionnelle par rapport à une configuration fonctionnelle, vous pouvez effectuer les étapes suivantes :

1. Configurez le VPN sans NAT d'identité.
2. Entrez **show nat detail** et **show conn all**.
3. Ajoutez la configuration NAT d'identité.
4. Répétez **show nat detail** et **show conn all**.

Traduction de réseaux IPv6

Dans les cas où vous devez transférer du trafic entre des réseaux IPv6 uniquement et des réseaux IPv4 uniquement, vous devez utiliser la NAT pour convertir les types d'adresses. Même avec deux réseaux IPv6, vous souhaiterez peut-être masquer les adresses internes du réseau externe.

Vous pouvez utiliser les types de traduction suivants avec les réseaux IPv6 :

- NAT64, NAT46 : Traduit les paquets IPv6 en IPv4 et vice versa. Vous devez définir deux politiques, une pour la traduction d'IPv6 à IPv4 et une pour la traduction d'IPv4 à IPv6. Bien que vous puissiez accomplir cela à l'aide d'une seule règle NAT Twice, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT Twice lorsque vous spécifiez une destination, la création de deux règles network object NAT (NAT objet de réseau) est la meilleure solution.

Remarque NAT46 prend uniquement en charge les mappages statiques.

- NAT66 : traduit les paquets IPv6 en une adresse IPv6 différente. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.

Remarque NAT64 et NAT 46 ne sont possibles que sur les interfaces routées standard. NAT66 est possible sur les interfaces routées et les membres du groupe de ponts.

NAT64/46 : traduction d'adresses IPv6 en IPv4

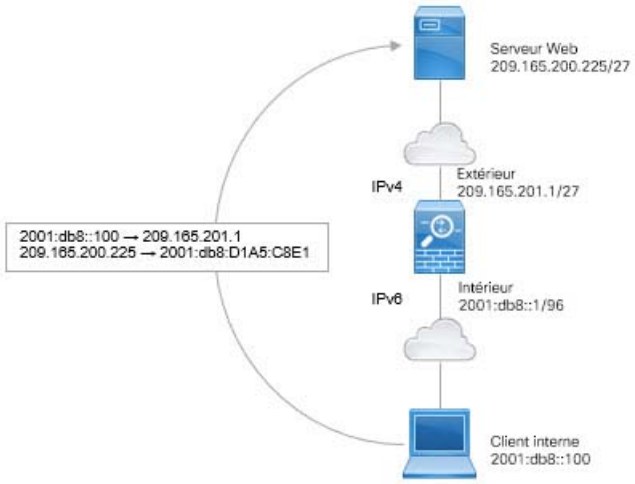
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses IPv6 pour lier les adresses IPv4 dans le réseau IPv6.

- L'ensemble d'adresses IPv4 pour la règle NAT64 est normalement de petite taille et peut généralement ne pas avoir assez d'adresses pour un mappage individuel avec les adresses client IPv6. La PAT dynamique pourrait plus facilement répondre au plus grand nombre possible d'adresses de clients IPv6 par rapport à la NAT dynamique ou statique.
- L'ensemble d'adresses IPv6 pour la règle NAT46 peut être égal ou supérieur au nombre d'adresses IPv4 à mapper. Cela permet de faire correspondre chaque adresse IPv4 à une adresse IPv6 différente. NAT46 prend uniquement en charge les mappages statiques, vous ne pouvez donc pas utiliser la PAT dynamique.

Vous devez définir deux politiques, une pour le réseau IPv6 source et une pour le réseau IPv4 de destination. Bien que vous puissiez accomplir cela à l'aide d'une seule règle NAT Twice, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT Twice lorsque vous spécifiez une destination, la création de deux règles network object NAT (NAT objet de réseau) est la meilleure solution.

Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe

Voici un exemple simple où vous avez un réseau interne IPv6 uniquement et que vous souhaitez convertir à IPv4 pour le trafic envoyé sur Internet. Cet exemple suppose que vous n'avez pas besoin de la traduction DNS, de sorte que vous pouvez effectuer les traductions NAT64 et NAT46 dans une seule règle NAT Twice.



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne.

Procédure

Étape 1 Créez un objet réseau pour le réseau IPv6 interne.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

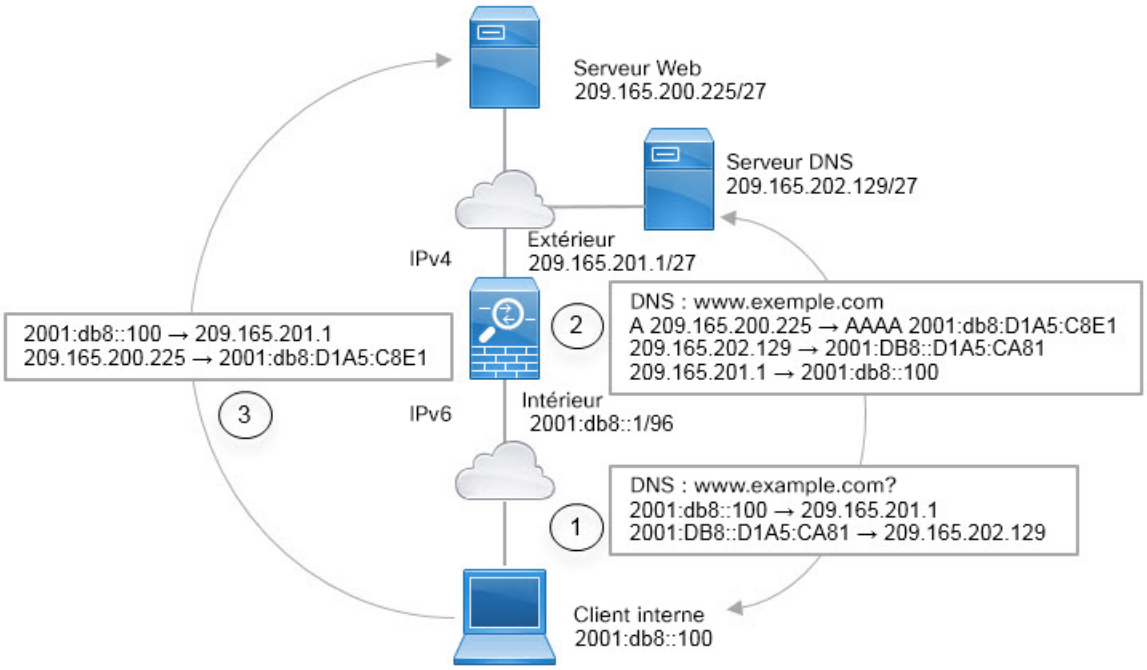
Étape 2 Créez la règle NAT Twice pour traduire le réseau IPv6 en IPv4 et inversement.

```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe. Inversement, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée.

Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS

Voici un exemple typique dans lequel vous avez un réseau interne IPv6 uniquement, mais il existe certains services IPv4 uniquement sur Internet externe dont les utilisateurs internes ont besoin.



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne. Vous activez la réécriture DNS sur la règle NAT46, afin que les réponses du serveur DNS externe puissent être converties d'enregistrements A (IPv4) en enregistrements AAAA (IPv6) et les adresses converties d'IPv4 à IPv6.

Voici une séquence typique d'une requête Web où un client à l'adresse 2001:DB8::100 sur le réseau IPv6 interne tente d'ouvrir www.example.com.

1. L'ordinateur du client envoie une requête DNS au serveur DNS à l'adresse 2001:DB8::D1A5:CA81. Les règles NAT effectuent les traductions suivantes pour la source et la destination dans la requête DNS :
   - 2001:DB8::100 sur un port unique sur 209.165.201.1 (règle PAT de l'interface NAT64.)
   - 2001:DB8::D1A5:CA81 à 209.165.202.129 (la règle NAT46. D1A5 : CA81 est l'équivalent IPv6 de 209.165.202.129.)
2. Le serveur DNS répond par un enregistrement A, indiquant que www.example.com est au 209.165.200.225. La règle NAT46, avec la réécriture DNS activée, convertit l'enregistrement A en enregistrement AAAA équivalent au protocole IPv6, et traduit 209.165.200.225 en 2001:db8:D1A5:C8E1 dans l'enregistrement AAAA. De plus, les adresses de source et de destination dans la réponse DNS ne sont pas traduites :
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100
3. Le client IPv6 a maintenant l'adresse IP du serveur Web et envoie une requête HTTP à www.example.com à l'adresse 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) La source et la destination de la requête HTTP sont traduites :
   - 2001:DB8::100 sur un port unique sur 209.156.101.54 (règle PAT de l'interface NAT64).
   - 2001:db8:D1A5:C8E1 à 209.165.200.225 (la règle NAT46.)

La procédure suivante explique comment configurer cet exemple.

Procédure

Étape 1 Créez un objet réseau pour le réseau IPv6 interne et ajoutez la règle NAT64.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe.

Étape 2 Créez un objet réseau pour le réseau traduit IPv6 pour le réseau IPv4 externe et ajoutez la règle NAT46.

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

Grâce à cette règle, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée. En outre, les réponses DNS des enregistrements A (IPv4) sont converties en enregistrements AAAA (IPv6) et les adresses IPv4 en IPv6.

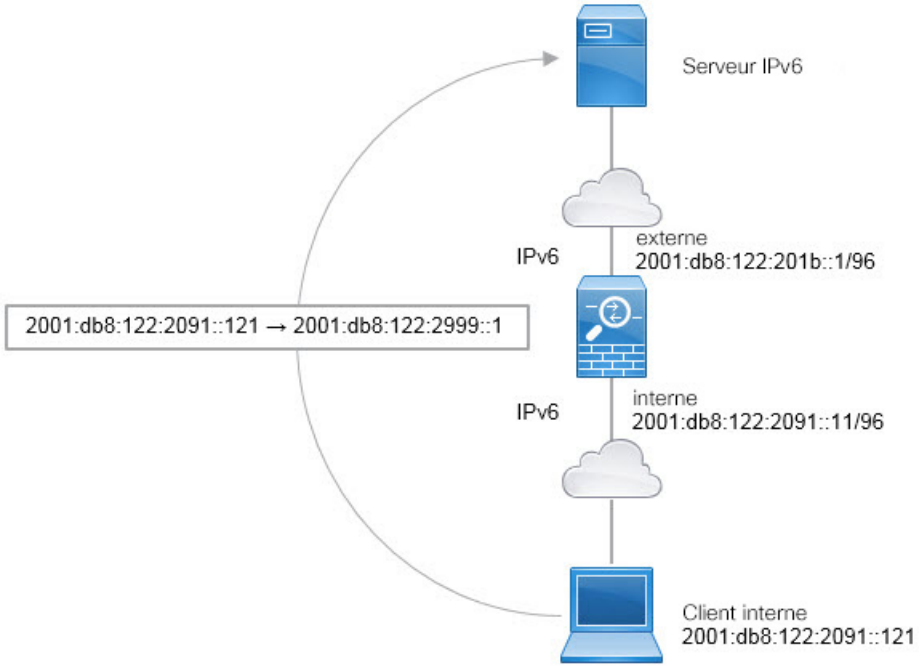
NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6

Lorsque vous passe z d'un réseau IPv6 à un autre réseau IPv6, vous pouvez traduire les adresses en adresses IPv6 différentes sur le réseau externe. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.

Comme vous n'effectuez pas de traduction entre différents types d'adresses, vous n'avez besoin que d'une seule règle pour les traductions NAT66. Vous pouvez facilement modéliser ces règles à l'aide de network object NAT (NAT objet de réseau). Toutefois, si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle en utilisant uniquement la NAT Twice.

Exemple NAT66, de traduction statique entre réseaux

Vous pouvez configurer une traduction statique entre des regroupements d'adresses IPv6 en utilisant network object NAT (NAT objet de réseau). L'exemple suivant explique comment convertir des adresses internes sur le réseau 2001:db8:122:2091::/96 en adresses externes sur le réseau 2001:db8:122:2999::/96.



Procédure

Créez l'objet réseau pour le réseau IPv6 interne et ajoutez la règle NAT statique.

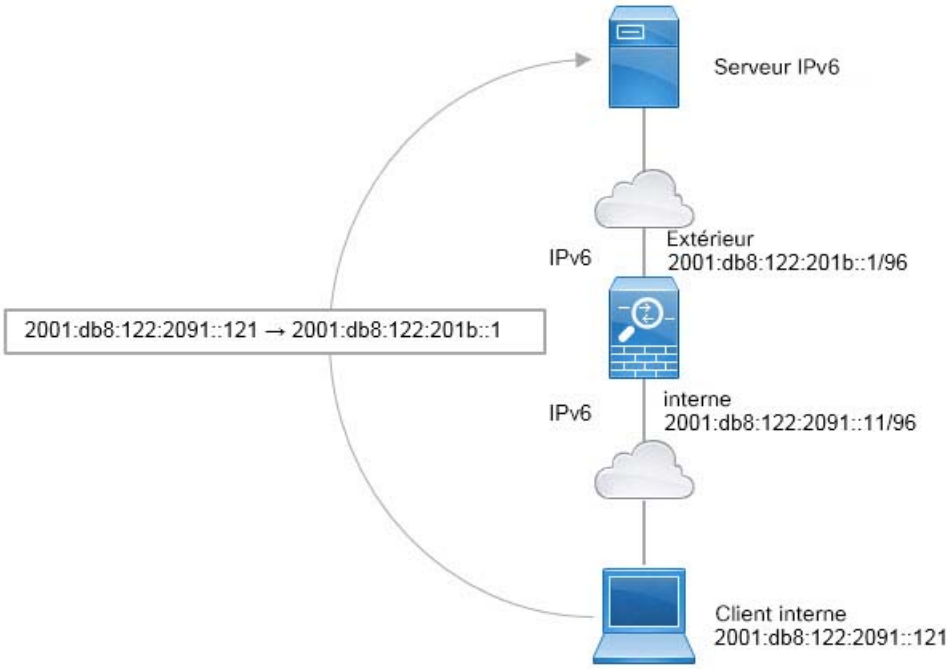
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

Avec cette règle, tout trafic provenant du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne vers l'interface externe reçoit une traduction NAT66 statique vers une adresse sur le réseau 2001:db8:122:2999::/96.

Exemple de NAT66, PAT d'interface IPv6 simple

Une approche simple pour la mise en œuvre de NAT66 consiste à affecter de manière dynamique des adresses internes à différents ports de l'adresse IPv6 de l'interface externe.

Lorsque vous configurez une règle PAT d'interface pour NAT66, toutes les adresses globales configurées sur cette interface sont utilisées pour le mappage PAT. Les adresses link-local ou site-local pour l'interface ne sont pas utilisées pour la PAT.



Procédure

Créez l'objet réseau pour le réseau IPv6 interne et ajoutez la règle PAT dynamique.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

Avec cette règle, tout trafic du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT66 vers l'une des adresses globales IPv6 configurées pour l'interface externe.

Réécriture des requêtes et réponses DNS à l'aide de la NAT

Vous devrez peut-être configurer ASA pour modifier les réponses DNS en remplaçant l'adresse dans la réponse par une adresse qui correspond à la configuration NAT. Vous pouvez configurer la modification DNS lorsque vous configurez chaque règle de traduction. La modification DNS est également connue sous le nom de contrôle DNS.

Cette fonctionnalité réécrit l'adresse dans les requêtes DNS et les réponses qui correspondent à une règle NAT (par exemple, l'enregistrement A pour IPv4, l'enregistrement AAAA pour IPv6 ou l'enregistrement PTR pour les requêtes DNS inversées). Pour les réponses DNS passant d'une interface mappée à toute autre interface, l'enregistrement est réécrit de la valeur mappée à la valeur réelle. Inversement, pour les réponses DNS traversant

une interface vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette fonctionnalité fonctionne avec NAT44, NAT 66, NAT46 et NAT64.

Voici les principales circonstances dans lesquelles vous devez configurer la réécriture DNS sur une règle NAT.

- La règle est NAT64 ou NAT46 et le serveur DNS se situe sur le réseau externe. Vous devez réécrire le DNS pour convertir les enregistrements DNS A (pour IPv4) et les enregistrements AAAA (pour IPv6).
- Le serveur DNS est à l'extérieur, les clients sont à l'intérieur et certains des noms de domaine complets que les clients utilisent mènent aux autres hôtes internes.
- Le serveur DNS est à l'intérieur et répond par des adresses IP privées, les clients sont à l'extérieur et les clients accèdent aux noms de domaine complets qui pointent vers des serveurs hébergés à l'intérieur.

Limites de réécriture DNS

Voici quelques limites concernant la réécriture DNS :

- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle NAT Twice, vous ne pouvez pas configurer la modification DNS si vous spécifiez l'adresse de destination ainsi que l'adresse source. Ces types de règles sont susceptibles d'être assorties d'une traduction différente pour une adresse unique lorsqu'on passe à A par rapport à B. Par conséquent, ne peut pas faire correspondre avec précision l'adresse IP à l'intérieur de la réponse DNS à la règle NAT double exacte; la réponse DNS ne contient pas d'information sur la combinaison d'adresses source/destination dans le paquet qui a déclenché la demande DNS.
- Vous devez activer l'inspection des applications DNS avec la réécriture DNS NAT activée pour que les règles NAT réécrivent les requêtes et les réponses DNS. Par défaut, l'inspection DNS avec la réécriture DNS NAT est appliquée de manière globale. Vous n'avez donc probablement pas besoin de modifier la configuration de l'inspection.
- En fait, la réécriture DNS s'effectue sur l'entrée xlate, et non sur la règle NAT. Ainsi, s'il n'y a pas de xlate pour une règle dynamique, la réécriture ne peut pas s'effectuer correctement. Le même problème ne se produit pas pour la NAT statique.
- La réécriture DNS ne réécrit pas les messages de mise à jour dynamique DNS (opcode 5).

Les rubriques suivantes présentent des exemples de réécriture DNS dans les règles NAT.

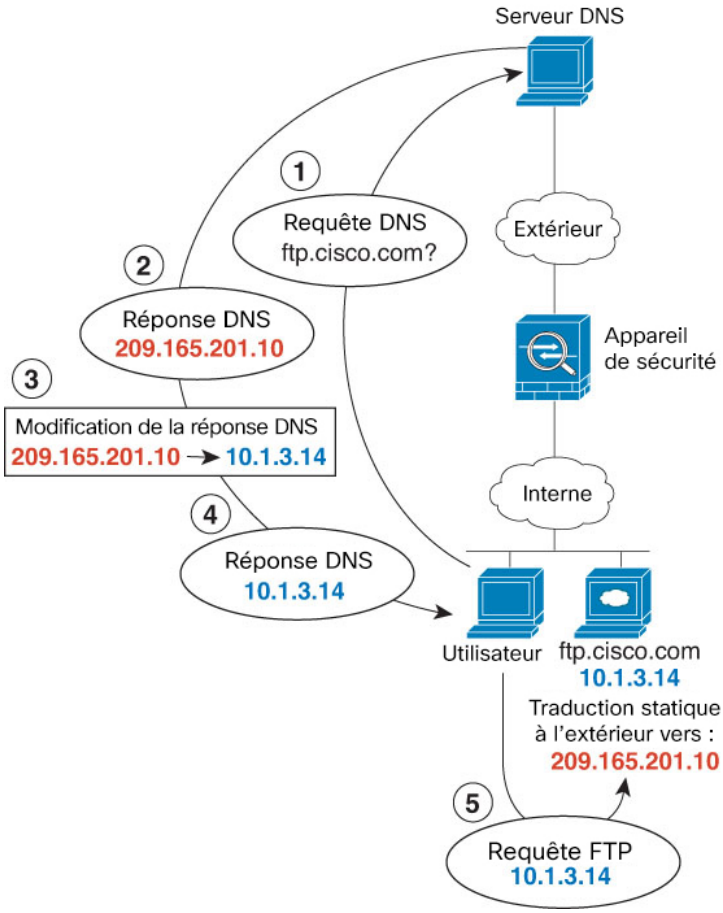
Modification de la réponse DNS, serveur DNS externe

La figure suivante montre un serveur DNS accessible à partir de l'interface externe. Un serveur, ftp.cisco.com, se trouve sur l'interface interne. Vous configurez NAT pour traduire statiquement l'adresse réelle ftp.cisco.com (10.1.3.14) en une adresse mappée (20.165.201.10) visible sur le réseau externe.

Dans ce cas, vous souhaitez activer la modification de la réponse DNS pour cette règle statique afin que les utilisateurs internes qui ont accès à ftp.cisco.com avec l'adresse réelle reçoivent l'adresse réelle du serveur DNS, et non l'adresse mappée.

Lorsqu'un hôte interne envoie une requête DNS pour l'adresse ftp.cisco.com, le serveur DNS répond par l'adresse mappée (209.165.201.10). Le système fait référence à la règle statique pour le serveur interne et traduit l'adresse dans la réponse DNS au format 10.3.1.14. Si vous n'activez pas la modification de la réponse

DNS, l'hôte interne tente d'envoyer le trafic vers l'adresse 209.165.201.10 au lieu d'accéder directement à ftp.cisco.com.



Procédure

Étape 1 Créez un objet réseau pour le serveur FTP.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.3.14
```

Étape 2 Configurez la règle NAT statique avec modification DNS.

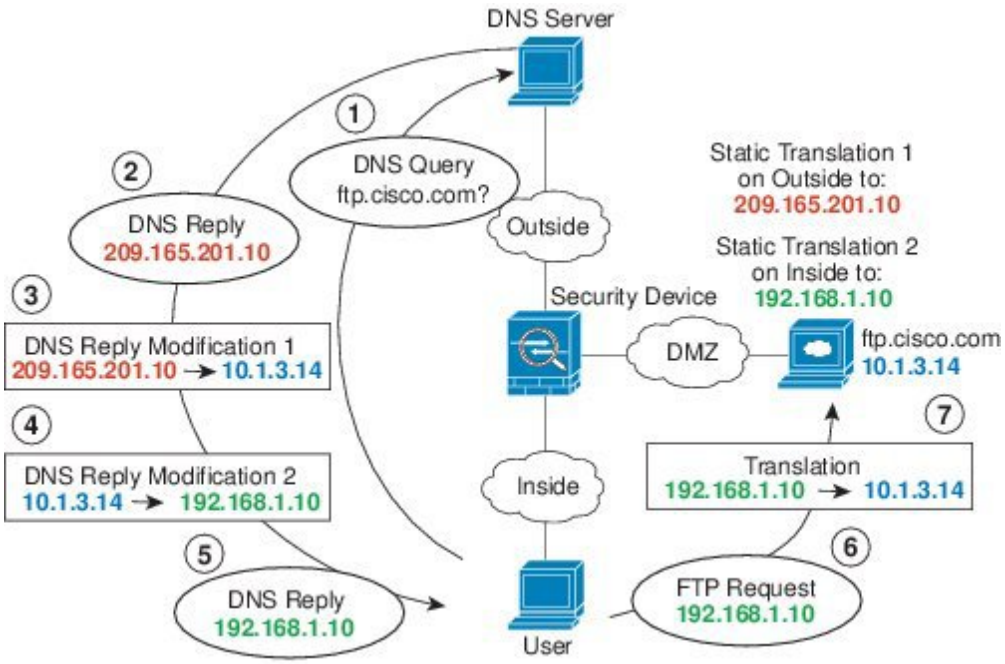
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés

La figure suivante montre un utilisateur du réseau interne demandant l'adresse IP pour ftp.cisco.com, qui se trouve sur le réseau DMZ, à partir d'un serveur DNS externe. Le serveur DNS répond avec l'adresse mappée (209.165.201.10) selon la règle statique entre l'extérieur et DMZ, même si l'utilisateur ne se trouve pas sur le réseau DMZ. L'ASA traduit l'adresse dans la réponse DNS en 10.1.3.14.

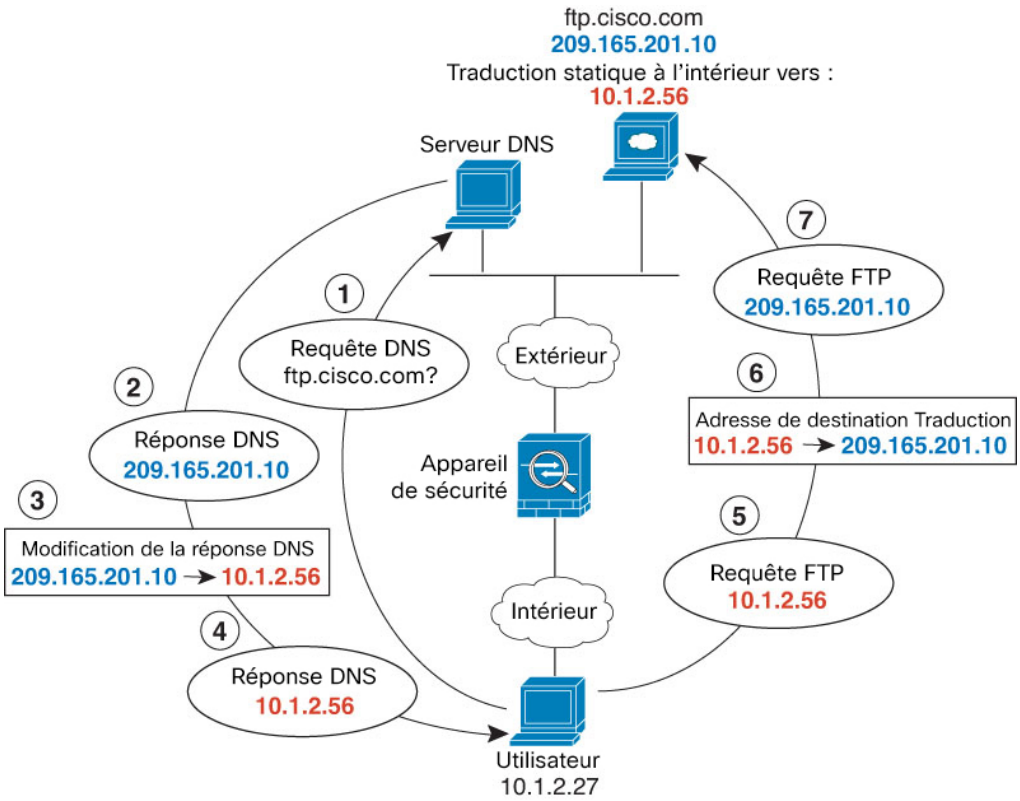
Si l'utilisateur doit accéder à ftp.cisco.com en utilisant l'adresse réelle, aucune autre configuration n'est requise. S'il y a également une règle statique entre l'intérieur et DMZ, vous devez également activer la modification de la réponse DNS sur cette règle. La réponse DNS sera ensuite modifiée deux fois. Dans ce cas, l'ASA traduit à nouveau l'adresse dans la réponse DNS en 192.168.1.10 selon la règle statique entre l'intérieur et DMZ.

Illustration 17 : Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés



Modification de la réponse DNS, serveur DNS sur le réseau hôte

La figure suivante montre un serveur FTP et un serveur DNS à l'extérieur. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.20.10. Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (10.1.2.56), vous devez configurer la modification de la réponse DNS pour la traduction statique.



Procédure

Étape 1 Créez un objet réseau pour le serveur FTP.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

Étape 2 Configurez la règle NAT statique avec modification DNS.

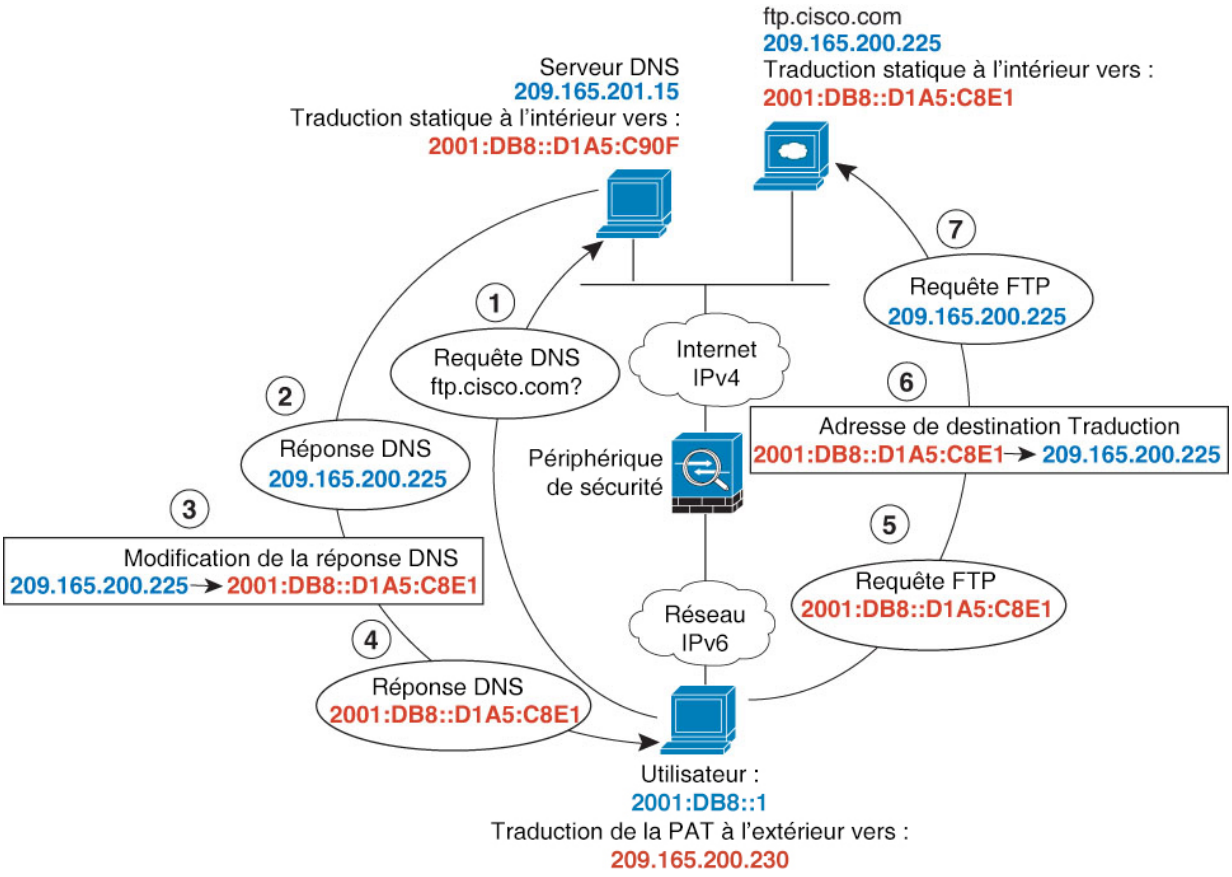
```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

Modification de la réponse DNS64

La figure suivante montre un serveur FTP et un serveur DNS sur le réseau IPv4 externe. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur IPv6 interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.200.225.

Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (2001:DB8::D1A5:C8E1, où D1A5:C8E1 est l'équivalent IPv6 de 209.165.200.225), vous devez configurer

la modification de la réponse DNS pour la traduction statique. Cet exemple comprend également une traduction NAT statique pour le serveur DNS et une règle PAT pour les hôtes IPv6 internes.



Procédure

Étape 1 Créez un objet réseau pour le serveur FTP et configurez la NAT statique avec modification DNS. Comme il s'agit d'une traduction un à un, incluez l'option **net-to-net** pour NAT46.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

Étape 2 Créez un objet réseau pour le serveur DNS et configurez la NAT statique. Incluez l'option **rnet-to-net** pour NAT46.

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

Étape 3 Configurez un pool PAT IPv4 pour traduire le réseau IPv6 interne.

Exemple :

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

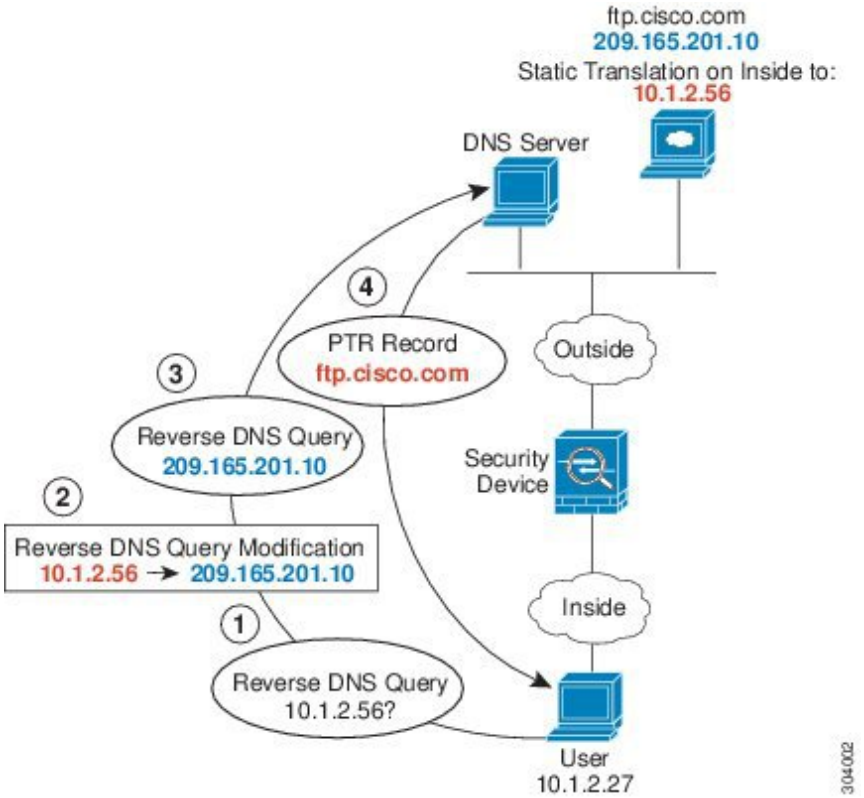
Étape 4 Créez un objet réseau pour le réseau IPv6 interne, et configurez la NAT dynamique avec un pool PAT.

```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

Modification PTR, serveur DNS sur le réseau hôte

La figure suivante montre un serveur FTP et un serveur DNS à l'extérieur. L'ASA dispose d'une traduction statique pour le serveur externe. Dans ce cas, lorsqu'un utilisateur interne effectue une recherche DNS inversée pour 10.1.2.56, l'ASA modifie la requête DNS inversée avec l'adresse réelle, et le serveur DNS répond avec le nom du serveur, ftp.cisco.com.

Illustration 18 : Modification PTR, serveur DNS sur le réseau hôte



À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.