# NAT (Network Address Translation; Translation d'adresses de réseau)

Les rubriques suivantes expliquent la traduction d'adresses réseau (NAT) et comment la configurer sur défense contre les menaces .



## Pourquoi utiliser la NAT?

Chaque ordinateur et périphérique d'un réseau IP reçoit une adresse IP unique qui permet d'identifier l'hôte. En raison d'une pénurie d'adresses IPv4 publiques, la plupart de ces adresses IP sont privées et ne peuvent être routées nulle part en dehors du réseau privé de l'entreprise. RFC 1918 définit les adresses IP privées que vous pouvez utiliser en interne et qui ne doivent pas être annoncées :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

L'une des principales fonctions de la NAT est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses légales et routables qui peuvent être utilisées sur l'Internet public. De cette façon, la NAT conserve les adresses publiques, car elle peut être configurée pour annoncer au moins une adresse publique pour l'ensemble du réseau vers le monde extérieur.

Les autres fonctions de la NAT comprennent :

- Sécurité : le fait de garder les adresses IP internes masquées détourne les attaques directes.

- Solutions de routage IP : les adresses IP qui se chevauchent ne sont pas un problème lorsque vous utilisez la NAT.
- Souplesse : vous pouvez modifier les schémas d'adressages IP internes sans affecter les adresses publiques disponibles en externe. par exemple, pour un serveur accessible à Internet, vous pouvez conserver une adresse IP fixe pour l'utilisation d'Internet, mais à l'interne, vous pouvez modifier l'adresse du serveur.
- Traduction entre IPv4 et IPv6 (mode routage uniquement) Si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.

**Remarque** La NAT n'est pas requise. Si vous ne configurez pas la NAT pour un ensemble donné de trafic, ce trafic ne sera pas traduit, mais toutes les politiques de sécurité seront appliquées normalement.

# Principes de base de la NAT

Les rubriques suivantes expliquent certains des principes de base de la NAT.

## Terminologie NAT

Le présent document utilise les termes suivants :

- Real address/host/network/interface : L'adresse réelle est l'adresse définie sur l'hôte avant qu'elle ne soit traduite. Dans un scénario NAT typique, vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau interne serait le « vrai » réseau. Notez que vous pouvez traduire n'importe quel réseau connecté au périphérique, pas seulement un réseau interne. Par conséquent, si vous configurez la NAT pour traduire les adresses externes, « réel » peut faire référence au réseau externe lorsqu'il accède au réseau interne.
- Mapped address/host/network/interface (adresse/hôte/réseau/interface mappée) : l'adresse mappée est l'adresse dans laquelle l'adresse réelle est traduite. Dans un scénario NAT typique, où vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau externe serait le réseau « mappé ».

**Remarque** Pendant la traduction d'adresses, les adresses IP configurées pour les interfaces de périphérique ne sont pas traduites.

- Lancement bidirectionnel : la NAT statique permet aux connexions d'être lancées de façon *bidirectionnelle*, c'est-à-dire à la fois vers l'hôte et à partir de l'hôte.
- NAT de source et de destination : pour tout paquet donné, les adresses IP de source et de destination sont comparées aux règles de la NAT, et l'une d'elles ou les deux peuvent être traduites ou non traduites, selon le cas. Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ».

# Type de NAT

Vous pouvez implémenter la NAT en utilisant les méthodes suivantes :

- NAT dynamique : un groupe d'adresses IP réelles est mappé à un groupe (généralement plus petit) d'adresses IP mappées, selon le principe du premier arrivé, premier servi. Seul l'hôte réel peut initier le trafic. Consultez Traduction d'adresses réseau dynamique, à la page 26.
- Traduction dynamique des adresses de port (PAT) : un groupe d'adresses IP réelles est mappé à une adresse IP unique en utilisant un port source unique de cette adresse IP. Consultez PAT dynamique, à la page 32.
- NAT statique : un mappage cohérent entre une adresse IP réelle et une adresse IP mappée. Autorise le lancement de trafic bidirectionnel. Consultez NAT statique, à la page 43.
- NAT d'identité : une adresse réelle est traduite statiquement en elle-même, contournant essentiellement la NAT. Vous pourriez souhaiter configurer la NAT de cette façon lorsque vous souhaitez traduire un grand groupe d'adresses, mais que vous souhaitez ensuite exempter un plus petit sous-ensemble d'adresses. Consultez NAT d'identité, à la page 52.

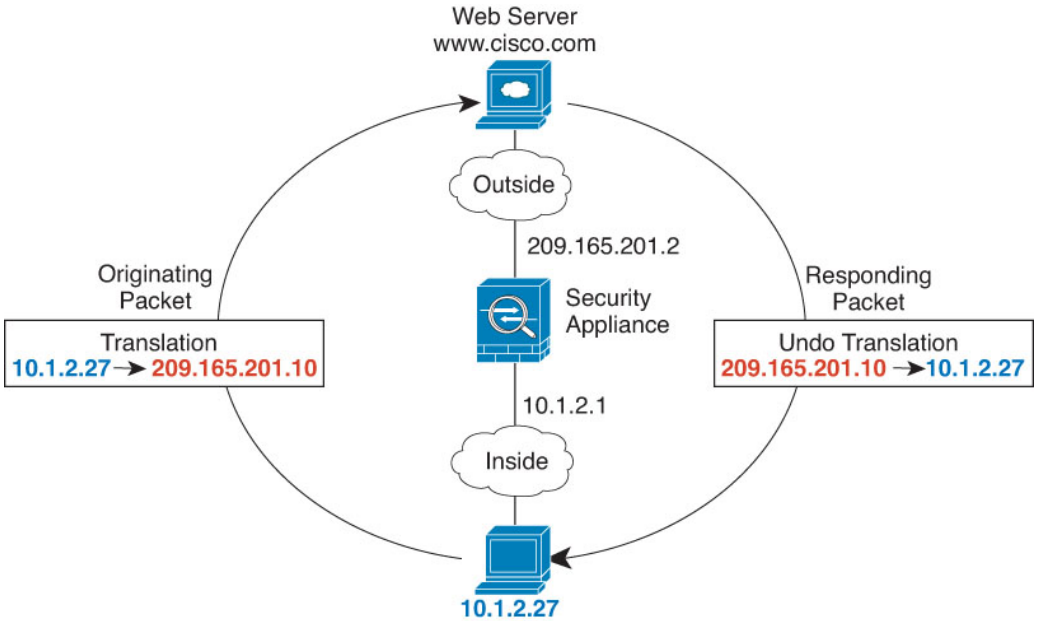
# NAT en mode routage et transparent

Vous pouvez configurer la NAT en mode de pare-feu routé et transparent. Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif. 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 1 : 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'appareil de défense contre les menaces reçoit le paquet, car l'appareil de défense contre les menaces effectue un ARP mandataire pour réclamer le paquet.
3. L'appareil de défense contre les menaces 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

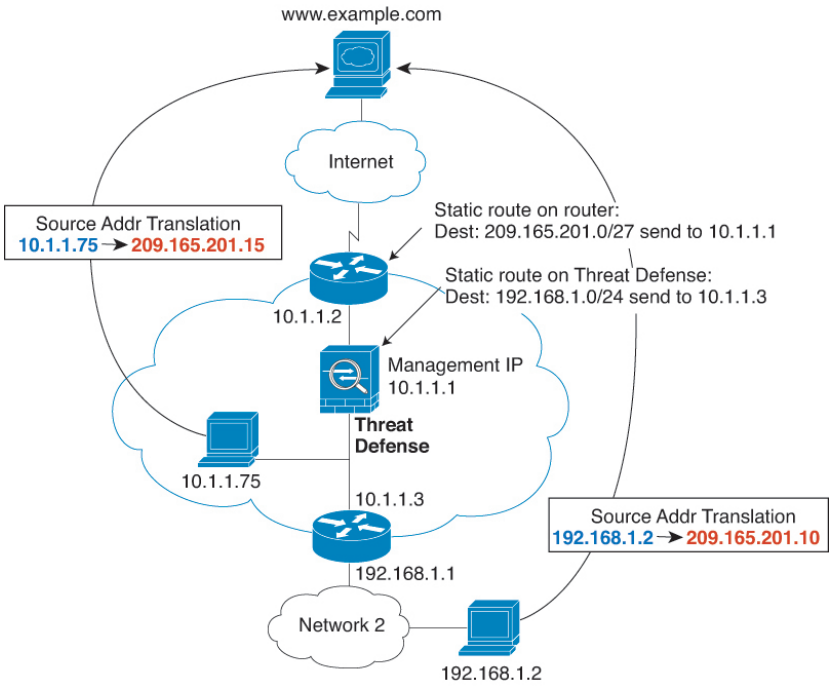
L'utilisation de la NAT en mode transparent élimine le besoin pour les routeurs en amont ou en aval d'effectuer la NAT pour leurs réseaux. Il peut remplir une fonction similaire dans un groupe de ponts en mode routé.

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 du défense contre les menaces envoie une requête ARP à un hôte de l'autre côté du défense contre les menaces 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 2 : 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 défense contre les menaces 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 défense contre les menaces.
3. défense contre les menaces 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, le défense contre les menaces 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, le défense contre les menaces 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 défense contre les menaces pour 192.168.1.0 /24.

# Auto NAT et Manual NAT (NAT manuelle)

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *auto NAT* et *manual NAT (NAT manuelle)*.

Nous vous recommandons d'utiliser l'auto NAT, sauf si vous avez besoin des fonctionnalités supplémentaires offertes par manual NAT (NAT manuelle). Il est plus facile de configurer auto NAT et ce pourrait être plus fiable pour des applications telles que la voix sur IP (VoIP). (Pour la VoIP, vous pourriez constater un échec dans la traduction des adresses indirectes qui n'appartiennent à aucun des objets utilisés dans la règle.)

## Auto NAT

Toutes les règles NAT configurées comme paramètre d'un objet réseau sont considérées comme des règles *auto NAT*. Il s'agit d'un moyen rapide et simple de configurer la NAT pour un objet réseau. Vous ne pouvez pas créer ces règles pour un objet de groupe, cependant.

Bien que ces règles soient configurées dans le cadre de l'objet lui-même, vous ne pouvez pas afficher la configuration NAT dans la définition de l'objet par le biais du gestionnaire d'objets.

Lorsqu'un paquet entre dans une interface, les adresses IP de source et de destination sont vérifiées par rapport aux règles auto NAT. Les adresses de source et de destination du paquet peuvent être traduites par des règles distinctes si des correspondances distinctes sont effectuées. Ces règles ne sont pas liées les unes aux autres; Différentes combinaisons de règles peuvent être utilisées en fonction du trafic.

Comme les règles ne sont jamais jumelées, vous ne pouvez pas préciser que sourceA/destinationA doit avoir une traduction différente de celle de sourceA/destinationB. Utilisez manual NAT (NAT manuelle) pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

## Manual NAT (NAT manuelle)

Manual NAT (NAT manuelle) vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle. Préciser les adresses de source et de destination vous permet de préciser que sourceA/destinationA peut avoir une traduction différente de celle de sourceA/destinationB.

**Remarque** Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ». Par exemple, si vous configurez la NAT statique avec traduction d'adresse de port et spécifiez l'adresse source comme une adresse de serveur Telnet, et que vous souhaitez que tout le trafic allant vers ce serveur Telnet ait le port traduit de 2323 à 23, vous devez spécifier les ports *source* à traduire (réel : 23, mappé : 2323). Vous spécifiez les ports source, car vous avez spécifié l'adresse du serveur Telnet comme adresse source.

L'adresse de destination est facultative. Si vous spécifiez l'adresse de destination, vous pouvez soit la mapper avec elle-même (NAT d'identité), soit la mapper avec une adresse différente. Le mappage de destination est toujours un mappage statique.

## Comparaison de Auto NAT et Manual NAT (NAT manuelle)

Les principales différences entre ces deux types de NAT sont les suivantes :

- Votre définition de l'adresse réelle.
  - NAT automatique : la règle NAT devient un paramètre pour un objet réseau. L'adresse IP de l'objet réseau sert d'adresse (réelle) d'origine.
  - Manual NAT (NAT manuelle) : vous identifiez un objet réseau ou un groupe d'objets réseau pour les adresses réelles et mappées. Dans ce cas, la NAT n'est pas un paramètre de l'objet réseau; l'objet ou le groupe de réseau est un paramètre de la configuration NAT. La possibilité d'utiliser un *groupe* d'objets réseau pour l'adresse réelle signifie que manual NAT (NAT manuelle) est plus évolutif.
- Mise en œuvre de la NAT de source et de destination.

- Auto NAT : chaque règle peut s'appliquer à la source ou à la destination d'un paquet. Deux règles peuvent donc être utilisées, une pour l'adresse IP source et une pour l'adresse IP de destination. Ces deux règles ne peuvent pas être liées ensemble pour appliquer une traduction précise pour une combinaison source/destination.
- Manual NAT (NAT manuelle) : une règle unique traduit à la fois la source et la destination. Un paquet correspond à une seule règle et les autres règles ne sont pas vérifiées. Même si vous ne configurez pas l'adresse de destination facultative, un paquet correspondant correspond toujours à une seule règle manual NAT (NAT manuelle). La source et la destination sont liées, vous pouvez donc appliquer différentes traductions selon la combinaison source/destination. Par exemple, sourceA/destinationA peut avoir une traduction différente de sourceA/destinationB.

- Ordre des règles NAT
  - Auto NAT : classés automatiquement dans la table NAT.
  - Manual NAT (NAT manuelle) : classés manuellement dans la table NAT (avant ou après les règles auto NAT ).

# Ordre des règles NAT

Les règlesAuto NAT et manual NAT (NAT manuelle) sont stockées dans un seul tableau qui est divisé en trois sections. Les règles de la section 1 sont appliquées en premier, puis les règles de la section 2 et finalement de la section 3 jusqu'à ce qu'une correspondance soit trouvée. Par exemple, si une correspondance est trouvée dans la section 1, les sections 2 et 3 ne sont pas évaluées. Le tableau suivant montre l'ordre des règles dans chaque section.

**Remarque** Il existe également une section 0, qui contient toutes les règles NAT créées par le système pour son propre usage. Ces règles ont priorité sur toutes les autres. Le système crée automatiquement ces règles et efface les xlates si nécessaire. Vous ne pouvez pas ajouter, modifier ni modifier les règles de la section 0.

*Tableau 1 : Tableau des règles NAT.*

| Section de tableau | Type de règle | Ordre des règles dans la section |
|---|---|---|
| Section 1 | Manual NAT (NAT manuelle) | Appliqués lors de la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Étant donné que la première correspondance est appliquée, vous devez vous assurer que les règles spécifiques précèdent les règles plus générales, sans quoi les règles spécifiques pourraient ne pas être appliquées comme vous le souhaitez. Par défaut, les règles manual NAT (NAT manuelle) sont ajoutées à la section 1.<br>Par « les règles spécifiques d'abord », nous entendons :<br>• Les règles statiques doivent précéder les règles dynamiques.<br>• Les règles qui incluent la traduction de destination doivent être placées avant les règles ne comprenant que la traduction de la source.<br>Si vous ne pouvez pas éliminer les règles en chevauchement, lorsque plusieurs règles peuvent s'appliquer en fonction de l'adresse source ou de destination, soyez particulièrement prudent en suivant ces recommandations. |
| Section 2 | Auto NAT | Si aucune correspondance n'est trouvée dans la section 1, les règles de la section 2 sont appliquées dans l'ordre suivant :<br>**1.** Règles statiques.<br>**2.** Règles dynamiques.<br>**Pour chaque type de règle, les consignes d'ordre suivantes sont utilisées :**<br>**1.** Quantité d'adresses IP réelles : de la plus petite à la plus grande. Par exemple, un objet avec une adresse sera évalué avant un objet avec 10 adresses.<br>**2.** Pour les quantités identiques, l'adresse IP du numéro est utilisée, du plus bas au plus élevé. Par exemple, 10.1.1.0 est évaluée avant 11.1.1.0.<br>**3.** Si la même adresse IP est utilisée, le nom de l'objet réseau est utilisé, par ordre alphabétique. Par exemple, abracadabra est évalué avant catwoman. |
| Section 3 | Manual NAT (NAT manuelle) | Si aucune correspondance n'est trouvée, les règles de la section 3 sont appliquées selon la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Cette section devrait contenir vos règles les plus générales. Vous devez également vous assurer que toutes les règles spécifiques de cette section précèdent les règles générales qui s'appliqueraient autrement. |

Pour les règles de la section 2, par exemple, les adresses IP suivantes sont définies dans les objets réseau :

- 192.168.1.0/24 (statique)
- 192.168.1.0/24 ( dynamique)
- 10.1.1.0/24 (statique)
- 192.168.1.1/32 (statique)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 172.16.1.0/24 ( dynamique) (objet abc)

L'ordre résultant serait le suivant :

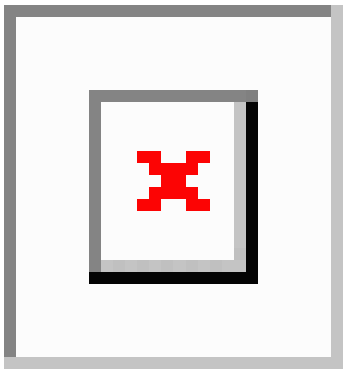
- 192.168.1.1/32 (statique)
- 10.1.1.0/24 (statique)
- 192.168.1.0/24 (statique)
- 172.16.1.0/24 ( dynamique) (objet abc)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 ( dynamique)

# Interfaces NAT

À l'exception des interfaces membres des groupes de ponts, vous pouvez configurer une règle NAT à appliquer à n'importe quelle interface (c'est-à-dire à toutes les interfaces) ou vous pouvez identifier des interfaces réelles et mappées spécifiques. Vous pouvez également spécifier n'importe quelle interface pour l'adresse réelle et une interface particulière pour l'adresse mappée, ou inversement.

Par exemple, vous pourriez souhaiter spécifier n'importe quelle interface pour l'adresse réelle et spécifier l'interface externe pour l'adresse mappée si vous utilisez les mêmes adresses privées sur plusieurs interfaces et que vous souhaitez les traduire toutes vers le même ensemble global lors de l'accès à .

***Illustration 3 : Spécification d'une interface***



Cependant, le concept d'interface « quelconque » (any) ne s'applique pas aux interfaces des membres des groupes de ponts. Lorsque vous spécifiez une interface « any », toutes les interfaces des membres des groupes de ponts sont exclues. Ainsi, pour appliquer la NAT aux membres du groupe de ponts, vous devez préciser

l'interface membre. Il peut en résulter de nombreuses règles similaires où une seule interface est différente. Vous ne pouvez pas configurer la NAT pour l'interface virtuelle de pont (BVI) elle-même, vous pouvez configurer la NAT pour les interfaces membres uniquement.

**Remarque** Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif. Lorsque vous spécifiez des interfaces, vous le faites indirectement en sélectionnant l'objet d'interface qui contient l'interface.

# Configurer le routage pour la NAT

Le périphérique défense contre les menaces  doit être la destination de tous les paquets envoyés à l'adresse traduite (mappée).

Lors de l'envoi de paquets, le périphérique utilise l'interface de destination si vous en spécifiez une, ou une recherche dans la table de routage si vous n'en spécifiez pas, pour déterminer l'interface de sortie. Pour la NAT d'identité, vous avez la possibilité d'utiliser une recherche de route même si vous spécifiez une interface de destination.

Le type de configuration de routage nécessaire dépend du type d'adresse mappée, comme expliqué dans les rubriques suivantes.

## Adresses sur le même réseau que l'interface mappée

Si vous utilisez des adresses sur le même réseau que l'interface mappée, l'appareil de défense contre les menaces utilise 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 appareil de défense contre les menaces  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 la table ARP dans les paramètres **avancés** de l'interface d'entrée.

## 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 appareil de défense contre les menaces .

Sinon, pour le mode routé, vous pouvez configurer une voie de routage statique sur appareil de défense contre les menaces  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.

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 appareil de défense contre les menaces : 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). Le appareil de défense contre les menaces fera ensuite passer l'ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à appareil de défense contre les menaces . (Notez que ce problème se produit même si vous avez une règle manual NAT (NAT manuelle) ; 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 appareil de défense contre les menaces est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers appareil de défense contre les menaces .

# Exigences et conditions préalables pour les politiques NAT

### Domaines pris en charge

N'importe quel

### Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

# Directives pour la NAT

Les rubriques suivantes fournissent des instructions détaillées pour la mise en œuvre de la NAT.

# Lignes directrices sur le mode pare-feu pour la NAT

La NAT est prise en charge en mode de pare-feu routé et transparent.

Cependant, la configuration de la NAT sur les interfaces membres de groupes de ponts (les interfaces qui font partie d'une interface virtuelle de groupe de ponts, ou BVI) a les restrictions suivantes :

- Lors de la configuration de la NAT pour les membres d'un groupe de ponts, vous spécifiez l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface de groupe de ponts (BVI) elle-même.
- Lorsque vous effectuez une NAT entre des interfaces de membres de groupes de ponts, vous devez préciser les adresses réelles et mappées. Vous ne pouvez pas définir « any » comme interface.
- 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.
- Vous ne pouvez pas traduire entre les réseaux IPv4 et IPv6 (NAT64/46) lorsque les interfaces de source et de destination sont membres du même groupe de ponts. La NAT statique/PAT 44/66, la NAT dynamique44/66 et le PAT44 dynamique sont les seules méthodes autorisées; Le PAT66 dynamique n'est pas pris en charge. Cependant, vous pouvez effectuer une NAT64/46 entre les membres de différents groupes de ponts ou entre un membre d'un groupe de ponts (source) et l'interface de routage standard (destination).

**Remarque** Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif.

# Directives pour la NAT pour IPv6

La NAT prend en charge IPv6 avec les directives et restrictions suivantes.

- Pour les interfaces en mode routé standard, vous pouvez également traduire entre IPv4 et IPv6.
- Vous ne pouvez pas traduire entre IPv4 et IPv6 pour des interfaces qui sont membres du même groupe de pont. Vous pouvez uniquement traduire entre deux réseaux IPv6 ou deux réseaux IPv4. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Pour la NAT statique, vous pouvez spécifier un sous-réseau IPv6 jusqu'à /64. Les sous-réseaux plus importants ne sont pas pris en charge.
- Lors de l'utilisation de FTP avec NAT46, lorsqu'un client FTP pour IPv4 se connecte à un serveur FTP pour IPv6, le client doit utiliser le mode passif étendu (EPSV), ou le mode Port étendu (EPRT); Les commandes PASV et PORT ne sont pas prises en charge avec IPv6.

# Bonnes pratiques pour la NAT IPv6

Vous pouvez utiliser la NAT pour traduire entre des réseaux IPv6, mais aussi entre des réseaux IPv4 et IPv6 (mode routage uniquement). Nous recommandons les bonnes pratiques suivantes :

- NAT66 (IPv6-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique.n 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. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (manual NAT (NAT manuelle) uniquement).
- NAT46 (IPv4-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Étant donné que l'espace d'adresse IPv6 est beaucoup plus important que l'espace d'adresse IPv4, vous pouvez facilement réaliser une traduction statique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (manual NAT (NAT manuelle) uniquement). Lors de la traduction vers un sous-réseau IPv6 (/96 ou inférieur), l'adresse mappée résultante est par défaut une adresse IPv4 intégrée, où les 32 bits de l'adresse IPv4 sont intégrés après le préfixe IPv6. Par exemple, si le préfixe IPv6 est un préfixe /96, l'adresse IPv4 est ajoutée dans les 32 derniers bits de l'adresse. Par exemple, si vous mappez 192.168.1.0/24 à 201b::0/96, 192.168.1.4 sera mappé à 201b::0.192.168.1.4 (affichée avec une notation mixte). Si le préfixe est inférieur, comme /64, l'adresse IPv4 est ajoutée après le préfixe et un suffixe 0s est ajouté après l'adresse IPv4. Vous pouvez également traduire les adresses réseau à réseau, où la première adresse IPv4 est mappée à la première adresse IPv6, la deuxième à la seconde, et ainsi de suite.
- NAT64 (IPv6-vers-IPv4) : il se peut que vous n'ayez pas assez d'adresses IPv4 pour le nombre d'adresses IPv6. Nous vous recommandons d'utiliser un ensemble PAT dynamique pour fournir un grand nombre de traductions IPv4.

# Prise en charge de la NAT pour les protocoles inspectés

Certains protocoles de couche d'application qui ouvrent des connexions secondaires ou qui intègrent des adresses IP dans les paquets sont inspectés pour fournir les services suivants :

- Pinhole création (création d'orifices) : certains protocoles d'application ouvrent des connexions TCP ou UDP secondaires sur des ports standard ou négociés. L'inspection ouvre des pinholes pour ces ports secondaires, vous n'avez donc pas besoin de créer des règles de contrôle d'accès pour les autoriser.
- Réécriture NAT : Les protocoles tels que le FTP intègrent les adresses IP et les ports pour les connexions secondaires dans les paquets de données dans le cadre du protocole. Si une traduction NAT est impliquée pour l'un ou l'autre des points terminaux, les moteurs d'inspection réécrivent les données du paquet pour refléter la traduction NAT des adresses et des ports intégrés. Les connexions secondaires ne fonctionneraient pas sans la réécriture de la NAT.
- Application de protocole : certaines inspections appliquent un certain degré de conformité aux RFC pour le protocole inspecté.

Le tableau suivant répertorie les protocoles inspectés qui appliquent la réécriture NAT et leurs limites NAT. Gardez ces limitations à l'esprit lors de l'écriture de règles NAT qui incluent ces protocoles. Les protocoles inspectés qui ne sont pas répertoriés ici n'appliquent pas la réécriture NAT. Ces inspections comprennent GTP, HTTP, IMAP, POP, SMTP, SSH et SSL.

**Remarque** La réécriture de la NAT est prise en charge sur les ports répertoriés uniquement. Pour certains de ces protocoles, vous pouvez étendre l'inspection à d'autres ports à l'aide des politiques d'analyse de réseau, mais la réécriture de la NAT n'est pas étendue à ces ports. Cela comprend l'inspection DCERPC, DNS, FTP et Sun RPC. Si vous utilisez ces protocoles sur des ports non standard, n'utilisez pas la NAT sur les connexions.

***Tableau 2 : Inspection des applications NAT prises en charge***

| Application | Protocole inspecté, port | Limites de la NAT | Pinholes créés |
|---|---|---|---|
| DCERPC | TCP/135 | No NAT64. | Oui |
| DNS sur UDP | UDP/53 | Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS. | Non |
| ESMTP | TCP/25 | No NAT64. | Non |
| FTP | TCP/21 | (Mise en grappe) Pas de PAT statique. | Oui |
| H.323 H.225 (signalisation d'appel)<br>H.323 RAS | TCP/1720<br>UDP/1718<br>Pour ARS, UDP/1718-1719 | (Mise en grappe) Pas de PAT statique.<br>Pas de PAT étendue.<br>No NAT64. | Oui |
| ICMP<br>Erreur ICMP | ICMP<br>(Le trafic ICMP dirigé vers une interface de périphérique n'est jamais inspecté.) | Aucune restriction. | Non |
| Options d'adresse IP | RSVP | No NAT64. | Non |
| Serveur de noms NetBIOS sur IP | UDP/133, 138 (ports sources) | Pas de PAT étendue.<br>No NAT64. | Non |
| RSH | TCP/514 | Pas de PAT<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique. | Oui |
| RTSP | TCP/554<br>(Aucun traitement pour la masquage HTTP.) | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique. | Oui |
| SIP | TCP/5060<br>UDP/5060 | Pas de PAT étendue.<br>Pas de NAT64 ou NAT46.<br>(Mise en grappe) Pas de PAT statique. | Oui |

| Application | Protocole inspecté, port | Limites de la NAT | Pinholes créés |
|---|---|---|---|
| Skinny (SCCP) | TCP/2000 | Pas de PAT étendue.<br>Pas de NAT64, NAT46 ou NAT66.<br>(Mise en grappe) Pas de PAT statique. | Oui |
| SQL*Net<br>(versions 1, 2) | TCP/1521 | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique. | Oui |
| Sun RPC | TCP/111<br>UDP/111 | Pas de PAT étendue.<br>No NAT64. | Oui |
| TFTP | UDP/69 | No NAT64.<br>(Mise en grappe) Pas de PAT statique.<br>Les adresses IP de charge utile ne sont pas traduites. | Oui |
| XDMCP | UDP/177 | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique. | Oui |

# Directives de destination de nom de domaine complet (FQDN)

Vous pouvez spécifier la destination traduite (mappée) dans une règle manual NAT (NAT manuelle) en utilisant un objet réseau de nom de domaine complet (FQDN) au lieu d'une adresse IP. Par exemple, vous pouvez créer une règle basée sur le trafic destiné au serveur Web www.exemple.com.

Lorsque vous utilisez un nom de domaine complet, le système obtient la résolution DNS et écrit la règle NAT en fonction de l'adresse renvoyée. Si vous utilisez plusieurs groupes de serveurs DNS, les domaines de filtre sont respectés et l'adresse est demandée au groupe approprié en fonction des filtres. Si plusieurs adresses sont obtenues à partir du serveur DNS, l'adresse utilisée est basée sur les éléments suivants :

- S'il existe une adresse sur le même sous-réseau que l'interface spécifiée, cette adresse est utilisée. S'il n'y en a pas sur le même sous-réseau, la première adresse renvoyée est utilisée.
- Le type d'adresse IP pour la source traduite et la destination traduite doivent correspondre. Par exemple, si l'adresse source traduite est au format IPv6, l'objet FQDN doit spécifier IPv6 comme type d'adresse. Si la source traduite est de type IPv4, l'objet FQDN peut spécifier IPv4 ou à la fois IPv4 et IPv6. Dans ce cas, une adresse IPv4 est sélectionnée.

Vous ne pouvez pas inclure un objet FQDN dans un groupe de réseaux utilisé pour la destination NAT manuelle. Dans la NAT, un objet FQDN doit être utilisé seul, car un seul hôte de destination est logique pour ce type de règle NAT.

Si le nom de domaine complet ne peut pas être résolu en adresse IP, la règle n'est pas fonctionnelle tant qu'une résolution DNS n'est pas obtenue.

# Directives supplémentaires pour la NAT

- Pour les interfaces membres d'un groupe de ponts, vous écrivez les règles NAT pour les interfaces membres. Vous ne pouvez pas écrire de règles NAT pour l'interface virtuelle de pont (BVI) elle-même.
- Vous ne pouvez pas écrire de règles NAT pour les interfaces de tunnel virtuel (VTI), qui sont utilisées dans le VPN de site à site. L'écriture de règles pour l'interface source du VTI n'appliquera pas la NAT au tunnel VPN. Pour écrire des règles NAT qui s'appliqueront au trafic VPN acheminé par tunnellisation sur un VTI, vous devez utiliser « any » comme interface; vous ne pouvez pas spécifier explicitement les noms d'interface.
- (Auto NAT seulement.) Vous ne pouvez définir qu'une seule règle NAT pour un objet donné; si vous souhaitez configurer plusieurs règles NAT pour un objet, vous devez créer plusieurs objets avec des noms différents qui spécifient la même adresse IP.
- Si un VPN est défini sur une interface, le trafic ESP entrant sur l'interface n'est pas soumis aux règles de la NAT. Le système autorise le trafic ESP uniquement pour les tunnels VPN établis, abandonnant le trafic non associé à un tunnel existant. Cette restriction s'applique aux ports ESP et UDP 500 et 4500.
- Si vous définissez un VPN de site à site sur un périphérique qui se trouve derrière un périphérique qui applique la PAT dynamique, de sorte que les ports UDP 500 et 4500 ne soient pas ceux réellement utilisés, vous devez établir la connexion à partir du périphérique qui se trouve derrière le PAT. Le répondeur ne peut pas lancer l'association de sécurité (SA), car il ne connaît pas les bons numéros de port.
- Si vous modifiez la configuration NAT et que vous ne souhaitez pas attendre que les traductions existantes expirent avant d'utiliser la nouvelle configuration NAT, vous pouvez effacer le tableau de traduction à l'aide de la commande **clear xlate** dans la CLI du périphérique . Cependant, l'effacement du tableau de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions.

  Si vous créez une nouvelle règle NAT qui doit s'appliquer à une connexion existante (comme un tunnel VPN), vous devez utiliser **clear conn** pour mettre fin à la connexion. Ensuite, la tentative de rétablissement de la connexion devrait atteindre la règle NAT et la connexion devrait être NATée correctement.

**Remarque** Si vous supprimez une règle NAT ou PAT dynamique, puis ajoutez une nouvelle règle avec des adresses mappées qui chevauchent les adresses de la règle supprimée, la nouvelle règle ne sera pas utilisée tant que toutes les connexions associées à la règle supprimée n'auront pas expiré ou n'auront pas été effacées à l'aide de utilisez les commandes **clear xlate** ou **clear conn**. Cette mesure de protection garantit que la même adresse ne est pas attribuée à plusieurs hôtes.

- Vous ne pouvez pas utiliser un groupe d'objets avec des adresses IPv4 et IPv6 ; le groupe d'objets ne doit comprendre qu'un seul type d'adresse.
- Un objet réseau utilisé dans la NAT ne peut pas inclure plus de 131 838 adresses IP, explicitement ou implicitement dans une plage d'adresses ou un sous-réseau. Fractionnez l'espace d'adresse en plages plus petites et écrivez des règles distinctes pour les objets plus petits.
- (Manual NAT (NAT manuelle) seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « tout » (IPv4 ou IPv6) dépend de la règle. Avant que appareil de défense contre les menaces  effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, appareil de défense contre les menaces  peut déterminer la valeur de **any** dans une règle NAT. Par exemple, si vous configurez une règle « any » pour un serveur

IPv6, et que ce serveur a été mappé à partir d'une adresse IPv4, « **any** » signifie « tout trafic IPv6 ». Si vous configurez une règle de « any » à « any » et que vous mappez la source à l'adresse IPv4 de l'interface, « **any** » signifie « tout trafic IPv4 », car l'adresse d'interface mappée signifie que la destination est également IPv4.

- Vous pouvez utiliser le même objet ou groupe mappé dans plusieurs règles NAT.
- L'ensemble d'adresses IP mappées ne peut pas inclure :
  - L'adresse IP de l'interface mappée. Si vous spécifiez l'interface « any » pour la règle, toutes les adresses IP d'interface sont non autorisées. Pour l'interface PAT (mode routage uniquement), spécifiez le nom de l'interface au lieu de son adresse.
  - L'adresse IP de l'interface de basculement
  - (Mode transparent.) L'adresse IP de gestion.
  - (NAT dynamique.) L'adresse IP de l'interface de secours lorsque le VPN est activé.
- Évitez d'utiliser des adresses qui se chevauchent dans les politiques NAT statiques et dynamiques. Par exemple, avec des adresses qui se chevauchent, une connexion PPTP peut ne pas s'établir si la connexion secondaire pour PPTP atteint le xlate statique au lieu de dynamique.
- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous spécifiez une interface de destination dans une règle, cette interface est utilisée comme interface de sortie plutôt que de rechercher la voie de routage dans la table de routage. Cependant, pour la NAT d'identité, vous avez la possibilité d'utiliser à la place une recherche de route.
- Si vous utilisez PAT sur le trafic RPC de Sun, qui est utilisé pour la connexion aux serveurs NFS, sachez que le serveur NFS peut rejeter des connexions si le port PAT est supérieur à 1024. La configuration par défaut des serveurs NFS est de rejeter les connexions des ports d'une valeur supérieure à 1024. L'erreur est généralement « Autorisation refusée ». Le mappage des ports supérieurs à 1024 se produit si vous ne sélectionnez pas l'option d'inclusion des ports réservés (1 à 1023) dans la plage de ports d'un ensemble PAT. Vous pouvez éviter ce problème en modifiant la configuration du serveur NFS pour autoriser tous les numéros de port.
- La NAT s'applique uniquement au trafic de transit. Le trafic généré par le système n'est pas soumis à la NAT.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.
- Vous ne pouvez pas utiliser la NAT sur la charge utile interne des registres PIM (Protocol Independent Multicast).
- (Manual NAT (NAT manuelle)) lors de la rédaction de règles NAT pour une configuration d'interface ISP double (interfaces principale et de secours utilisant les contrats de niveau de service dans la configuration de routage), ne spécifiez pas de critères de destination dans la règle. Assurez-vous que la règle de l'interface principale précède la règle de l'interface de secours. Cela permet au périphérique de choisir la bonne interface de destination NAT en fonction de l'état de routage actuel lorsque le fournisseur

de services Internet principal n'est pas disponible. Si vous spécifiez des objets de destination, la règle NAT sélectionnera toujours l'interface principale pour les règles autrement en double.

- Si vous obtenez la raison d'abandon ASP nat-no-xlate-to-pat- Pool pour le trafic qui ne devrait pas correspondre aux règles NAT définies pour l'interface, configurez les règles NAT d'identité pour le trafic affecté afin que le trafic puisse être non traduit.
- Si vous configurez la NAT pour les points terminaux d'un tunnel GRE, vous devez désactiver le maintien de l'activité sur les points terminaux, sinon le tunnel ne pourra pas être établi. Les points terminaux envoient des paquets keepalives aux adresses d'origine.

# Gérer les politiques NAT

La traduction d'adresses réseau (NAT) convertit l'adresse IP d'un paquet entrant en une adresse différente dans le paquet sortant. L'une des principales fonctions de la NAT est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses routables qui peuvent être utilisées sur l'Internet public. La NAT effectue le suivi des traductions, également appelée xlates, pour s'assurer que le trafic de retour est dirigé vers la bonne adresse hôte non traduite.

### Avant de commencer

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Les administrateurs des domaines ascendants peuvent cibler les politiques NAT sur les périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées. Si une politique NAT cible des périphériques dans différents domaines descendants, les administrateurs des domaines descendants peuvent uniquement afficher les informations sur les périphériques cibles appartenant à leur domaine.

### Procédure

**Étape 1** Choisissez **Devices (appareils)** > **NAT** .

**Étape 2** Gérez vos politiques NAT :

- Create (créer) : cliquez sur **New Policy** (Nouvelle politique) et sélectionnez **Threat Defense NAT** (NAT de défense contre les menaces). Consultez Création de politiques NAT, à la page 19.
- Copy (copier) : cliquez sur **Copier** (  ) à côté de la politique que vous souhaitez copier. Vous êtes invité à donner à la copie un nouveau nom unique. La copie comprend toutes les règles et configurations de politique, mais pas les affectations de périphériques.
- Report (rapport) : Cliquez sur **Rapport** (  ) de la politique. Vous êtes invité à enregistrer le rapport PDF, qui comprend les attributs de politique, les affectations de périphériques, les règles et les informations sur l'utilisation des objets.

- Edit (Modifier) : cliquez sur **Edit** ( ) à côté de la politique que vous souhaitez modifier. Consultez Configurer la NAT pour Threat Defense, à la page 20.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté de la politique que vous souhaitez supprimer, puis cliquez sur **OK**. Lorsqu'on vous demande s'il faut continuer, vous êtes également informé si un autre utilisateur a des modifications non enregistrées dans la politique.

**Mise en garde** Après avoir déployé une politique NAT sur un périphérique géré, vous ne pouvez pas supprimer la politique du périphérique. Au lieu de cela, vous devez déployer une politique NAT sans règle pour supprimer les règles NAT déjà présentes sur le périphérique géré. Vous ne pouvez pas non plus supprimer une politique qui est la dernière politique déployée sur les machines cibles, même si elle est obsolète. Avant de pouvoir supprimer complètement la politique, vous devez déployer une politique différente sur ces cibles.

# Création de politiques NAT

Lorsque vous créez une nouvelle politique NAT, vous devez au minimum lui donner un nom unique. Bien que vous ne soyez pas tenu de définir les cibles de politique au moment de la création de la politique, vous devez effectuer cette étape avant de pouvoir déployer la politique. Si vous appliquez une politique NAT sans règle à un périphérique, le système supprime toutes les règles NAT de ce périphérique.

**Procédure**

**Étape 1** Choisissez **Devices (appareils)** > **NAT** .

**Étape 2** Cliquez sur **New Policy (nouvelle politique** ) et dans la liste déroulante, choisissez **Threat Defense NAT** pour les périphériques défense contre les menaces .

**Firepower NAT** est destiné aux périphériques plus anciens qui ne sont pas abordés dans ce document.

**Étape 3** Saisissez un **nom** unique.

Dans un déploiement multidomaine, les noms de politique doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'une politique que vous ne pouvez pas voir dans votre domaine actuel.

**Étape 4** Vous pouvez également saisir une **Description**.

**Étape 5** Choisissez les périphériques sur lesquels vous souhaitez déployer la politique :

- Choisissez un périphérique dans la liste des **périphériques disponibles** et cliquez sur **Add to Policy** (Ajouter à la politique).
- Cliquez sur un appareil et faites-le glisser de la liste des **périphériques disponibles** vers la liste des **périphériques sélectionnés**.
- Supprimez un périphérique de la liste des **périphériques sélectionnés** en cliquant sur **Supprimer** ( ) à côté du périphérique.

**Étape 6** Cliquez sur **Save** (enregistrer).

# Configuration des cibles de politique NAT

Vous pouvez identifier les périphériques gérés que vous souhaitez cibler avec votre politique lors de la création ou de la modification d'une politique. Vous pouvez rechercher une liste de périphériques et de paires à haute disponibilité disponibles et les ajouter à une liste de périphériques sélectionnés.

**Procédure**

**Étape 1** Choisissez **Devices (appareils)** > **NAT** .

**Étape 2** Cliquez sur **Edit** ( ) à côté de la politique NAT que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

**Étape 3** Cliquez sur **Policy Assignments** (Attributions de politiques)

**Étape 4** Effectuez l'une des actions suivantes :

- Pour affecter un périphérique, une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste des **périphériques disponibles** et cliquez sur **Add to Policy** (Ajouter à la politique).. Vous pouvez également effectuer un glisser-déposer.
- Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques sélectionnés**.

**Étape 5** Cliquez sur **OK**.

# Configurer la NAT pour Threat Defense

La traduction d'adresses réseau peut être très complexe. Nous vous recommandons de garder vos règles aussi simples que possible pour éviter les problèmes de traduction et les situations de dépannage difficiles. Une planification rigoureuse avant de mettre en œuvre la NAT est essentielle. La procédure suivante fournit l'approche de base.

La politique NAT est une politique partagée. Vous affectez la politique aux périphériques qui devraient avoir des règles NAT similaires.

L'application ou non d'une règle donnée de la politique à un périphérique affecté est déterminée par les objets d'interface (zones de sécurité ou groupes d'interfaces) utilisés dans la règle. Si les objets d'interface comprennent une ou plusieurs interfaces pour le périphérique, la règle est déployée sur le périphérique. Ainsi, vous pouvez configurer des règles qui s'appliquent aux sous-ensembles de périphériques dans une politique partagée unique en concevant soigneusement vos objets d'interface. Les règles qui s'appliquent à « tout » objet d'interface sont déployées sur tous les périphériques.

Si vous remplacez le type d'une interface par un type non valide pour une utilisation avec une politique NAT qui cible un périphérique avec cette interface, la politique marque l'interface comme supprimée. Cliquez sur **Save** (Enregistrer) dans la politique NAT pour supprimer automatiquement l'interface de la politique.

Vous pouvez configurer plusieurs politiques NAT si des groupes de vos périphériques nécessitent des règles très différentes.

### Procédure

**Étape 1** Sélectionnez **Périphériques** > **NAT**.

- Cliquez sur **Nouvelle politique** > **NAT Threat Defense** pour créer une nouvelle politique. Attribuez un nom à la politique, affectez-y éventuellement des périphériques, puis cliquez sur **Save** (Enregistrer).

  Vous pourrez modifier les affectations de périphériques ultérieurement en modifiant la politique et en cliquant sur **Affectations de politique**.

- Cliquez sur **Edit** (✎) pour modifier une politique de NAT Threat Defense existante. Notez que la page affiche également les politiques NAT Firepower, qui ne sont pas utilisées par les périphériques défense contre les menaces .

  Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

**Étape 2** Décidez du type de règles dont vous avez besoin.

Vous pouvez créer des règles NAT dynamique, PAT dynamique, NAT statique et NAT d'identité. Pour un aperçu, consultez Type de NAT, à la page 3.

**Étape 3** Décidez quelles règles doivent être mises en œuvre en tant que NAT manuelle ou automatique.

Pour une comparaison de ces deux options d'implémentation, consultez Auto NAT et Manual NAT (NAT manuelle), à la page 5.

**Étape 4** Décidez quelles règles doivent être personnalisées par périphérique.

Comme vous pouvez affecter une politique NAT à plusieurs périphériques, vous pouvez configurer une seule règle sur de nombreux périphériques. Cependant, vous pouvez avoir des règles qui doivent être interprétées différemment par chaque périphérique ou certaines règles qui doivent s'appliquer à un sous-ensemble de périphériques uniquement.

Utilisez des objets d'interface pour contrôler les périphériques sur lesquels une règle est configurée. Ensuite, utilisez les remplacements d'objets sur les objets réseau pour personnaliser les adresses utilisées par périphérique.

Pour de plus amples renseignements, voir Personnalisation des règles NAT pour plusieurs périphériques, à la page 22.

**Étape 5** Créez les règles, comme expliqué dans les sections suivantes.

- Traduction d'adresses réseau dynamique, à la page 26
- PAT dynamique, à la page 32
- NAT statique, à la page 43
- NAT d'identité, à la page 52

**Étape 6** Gérer la politique et les règles NAT

Vous pouvez effectuer ce qui suit pour gérer la politique et ses règles.

- Pour modifier le nom ou la description de la politique, cliquez dans ces champs, saisissez vos modifications et cliquez en dehors des champs.

- Pour afficher uniquement les règles qui s'appliquent à un périphérique spécifique, cliquez sur **Filter by Device** (filtrer par périphérique) et sélectionnez le périphérique souhaité. Une règle s'applique à un périphérique s'il utilise un objet d'interface qui comprend une interface sur le périphérique.
- Pour afficher les avertissements et les erreurs dans la politique, cliquez sur **Afficher les avertissements**, puis choisissez un **périphérique**. Les avertissements et les erreurs indiquent les configurations qui pourraient nuire au flux de trafic ou empêcher le déploiement de la politique.
- Pour modifier les périphériques auxquels la politique est affectée, cliquez sur le lien **Policy Affectations** (affectations de politiques) et modifiez la liste des périphériques sélectionnés comme vous le souhaitez.
- Pour modifier l'activation ou la désactivation d'une règle, effectuez un clic droit sur la règle et sélectionnez l'option souhaitée dans la commande **State** (état). Vous pouvez désactiver temporairement une règle sans la supprimer à l'aide de ces contrôles.
- Pour ajouter une règle, cliquez sur le bouton **Add Rule** (ajouter une règle).
- Pour modifier une règle, cliquez sur **Edit** ( ) à côté de la règle.
- Pour supprimer une règle, cliquez sur **Supprimer** ( ) à côté de la règle.
- Pour modifier le nombre de règles affichées sur la page, utilisez la liste déroulante **Nombre de lignes par page**.
- Pour sélectionner plusieurs règles à activer, désactiver ou supprimer, cochez la case des règles ou la case dans l'en-tête, puis effectuez l'action.

**Étape 7** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

# Personnalisation des règles NAT pour plusieurs périphériques

Puisque la politique NAT est partagée, vous pouvez affecter une politique donnée à plus d'un périphérique. Cependant, vous pouvez configurer au plus une règle NAT automatique pour un objet donné. Ainsi, si vous souhaitez configurer différentes traductions pour un objet en fonction du périphérique effectuant la traduction, vous devez configurer avec soin les objets d'interface (zones de sécurité ou groupes d'interfaces) et définir les remplacements d'objets réseau pour l'adresse traduite.

Les objets d'interface déterminent sur quels périphériques une règle est configurée. Les remplacements d'objets de réseau déterminent quelles adresses IP sont utilisées par un périphérique donné pour cet objet.

Examinez les scénarios suivants :

- Les réseaux FTD-A et FTD-B ont des réseaux internes 192.168.1.0/24 reliés à l'interface nommée « interne ».
- Sur FTD-A, vous souhaitez traduire toutes les adresses 192.168.1.0/24 vers un pool NAT sur la plage 10.100.10.10 à 10.100.10.200 lorsque vous accédez à l'interface « externe ».
- Sur FTD-B, vous souhaitez traduire toutes les adresses 192.168.1.0/24 vers un pool NAT sur la plage 10.200.10.10 à 10.200.10.200 lorsque vous accédez à l'interface « externe ».

Pour accomplir ce qui précède, vous devez procéder comme suit. Bien que cet exemple de règle concerne la NAT automatique dynamique, vous pouvez généraliser la technique pour n'importe quel type de règle NAT.

### Procédure

**Étape 1** Créer les zones de sécurité pour les interfaces intérieures et extérieures.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Objets d'interface** dans la table des matières et cliquez sur **Ajouter** > **une zone de sécurité.** (Vous pouvez utiliser des groupes d'interface au lieu de zones.)
c) Configurer les propriétés de la zone intérieure.
   - **Nom** : saisissez un nom, par exemple **inside-zone**.
   - **Type** : Sélectionnez **Routed** (routage) pour les périphériques en mode routage, **Switched** (commuté) pour le mode transparent.
   - **Interfaces sélectionnées** : ajoutez les interfacesFTD-A/inside et FTD-B/inside à la liste des sélections.
d) Cliquez sur **Save** (enregistrer).
e) Cliquez sur **Add** > **Security Zone** (ajouter une zone de sécurité) et définissez les propriétés de la zone externe.
   - **Nom** : saisissez un nom, par exemple **outside-zone**.
   - **Type** : Sélectionnez **Routed** (routage) pour les périphériques en mode routage, **Switched** (commuté) pour le mode transparent.
   - **Interfaces sélectionnées** : ajoutez les interfacesFTD-A/outside et FTD-B/outside à la liste des sélections.
f) Cliquez sur **Save** (enregistrer).

**Étape 2** Créez l'objet réseau pour le réseau interne d'origine dans la page Object Management (gestion d'objets).

a) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
b) Configurez les propriétés du réseau interne.
   - **Nom** : saisissez un nom, par exemple, **inside-network**.
   - **Réseau** : saisissez l'adresse du réseau, par exemple, **192.168.1.0/24**.
c) Cliquez sur **Save** (enregistrer).

**Étape 3** Créez l'objet réseau pour le regroupement NAT traduit et définissez les remplacements.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).
b) Configurez les propriétés du regroupement NAT pour FTD-A.
   - **Nom** : saisissez un nom, par exemple, **NAT- pool**.
   - **Réseau** : Saisissez la plage d'adresses à inclure dans le groupement pour FTD-A, par exemple, **10.100.10.10-10.100.10.200**.
c) Sélectionnez **Allow Overrides** (Permettre les remplacements).

d) Cliquez sur l'en-tête **Overrides** (Remplacements) pour ouvrir la liste des remplacements d'objets.
e) Cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue Add Object Override (ajouter un remplacement d'objet).
f) Sélectionnez FTD-B et **ajoutez-le** à la liste des périphériques sélectionnés.
g) Cliquez sur **Override** (Remplacer) et remplacez **Network** (réseau) par **10.200.10.10-10.200.10.200**
h) Cliquez sur **Add** (Ajouter) pour ajouter le remplacement au périphérique.

   En définissant un remplacement pour FTD-B, chaque fois que le système configure cet objet sur FTD-B, il utilise la valeur de remplacement au lieu de la valeur définie dans l'objet d'origine.

i) Cliquez sur **Save** (enregistrer).

**Étape 4** Configurez la règle NAT.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :

   - **NAT Rule** = Auto NAT Rule.
   - **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

   - **Objets de l'interface source** = inside-zone.
   - **Objets d'interface de destination** = outside-zone.

   **Remarque** Les objets d'interface contrôlent les périphériques sur lesquels la règle est configurée. Étant donné que, dans cet exemple, les zones contiennent des interfaces pour FTD-A et FTD-B uniquement, même si la politique NAT était affectée à des périphériques supplémentaires, la règle serait déployée sur ces deux périphériques uniquement.

e) Pour **Translation** (traduction), configurez les options suivantes :

   - **Source d'origine** = objet de réseau interne.
   - **Adresse** > **de la source traduite**= objet NAT-pool.

f) Cliquez sur **Save** (enregistrer).

   Vous avez maintenant une seule règle qui sera interprétée différemment pour FTD-A et FTD-B, fournissant des traductions uniques pour les réseaux internes protégés par chaque pare-feu.

# Recherche et filtrage dans le tableau de règles NAT

Vous pouvez effectuer des recherches et filtrer le tableau des règles NAT pour vous aider à trouver les règles que vous devez modifier ou visualiser. Lorsque vous filtrez le tableau, seules les règles de correspondance sont affichées. Notez que bien que les numéros de règles changent pour être successivement 1, 2, etc., le filtrage ne modifie pas le numéro de règle réel ni l'emplacement de la règle dans le tableau par rapport aux règles masquées. Le filtrage modifie simplement ce que vous pouvez voir pour vous aider à localiser les règles qui vous intéressent.

Lors de la modification de la politique NAT, vous pouvez utiliser les champs au-dessus du tableau pour effectuer les types de recherche/filtrage suivants :

- **Filter by Device**(filtrer par périphérique) : Cliquez sur **Filter by Device** (filtrer par périphérique), sélectionnez les périphériques dont vous souhaitez afficher les règles, puis cliquez sur **OK**. L'application d'une règle à un périphérique est déterminée par les contraintes d'interface de la règle. Si vous spécifiez une zone de sécurité ou un groupe d'interfaces pour l'interface source ou de destination, la règle s'applique à un périphérique si au moins une interface du périphérique se trouve dans la zone ou le groupe. Si une règle NAT s'applique à une interface de source et à une interface de destination, elle s'applique à tous les périphériques.

  Si vous effectuez également une recherche de texte ou à attributs multiples, les résultats sont limités aux périphériques sélectionnés.

  Pour supprimer ce filtre, cliquez sur **Filter by Device** (filtrer par périphérique) et désélectionnez les périphériques, ou sélectionnez **All** (Tous) et cliquez sur **OK**.

- **Recherche en texte simple** : Dans la zone **Filter** (Filtrer), saisissez une chaîne et appuyez sur Entrée. La chaîne est comparée à toutes les valeurs des règles. Par exemple, si vous saisissez « network-object-1 », qui est le nom d'un objet réseau, vous obtiendrez des règles qui utilisent l'objet dans les attributs de source, de destination et d'ensemble (pool) PAT.

  Pour les objets de réseau et de port, la chaîne est également comparée au contenu des objets utilisés dans la règle. Par exemple, si un objet d'ensemble PAT comprend la plage 10.100.10.3 à 10.100.10.100, la recherche sur 10.100.10.3 ou 10.100.10.100 (ou un 10.100.10 partiel) inclura les règles qui utilisent cet objet d'ensemble PAT Cependant, la correspondance doit être exacte : la recherche sur 10.100.10.5 ne correspondra pas à cet objet de l'ensemble PAT, même si l'adresse IP se trouve dans la plage d'adresses IP de l'objet.

  Pour supprimer le filtre, cliquez sur le **x** à droite de la zone du filtre.

- **Recherche à attributs multiples** : si une recherche textuelle simple vous renvoie trop de résultats, vous pouvez configurer plusieurs valeurs pour la recherche. Cliquez dans la zone **Filter** (Filtrer) pour ouvrir la liste des attributs, puis sélectionnez ou saisissez les chaînes pour les attributs que vous souhaitez rechercher, et cliquez sur le bouton **Filter** (Filtrer). Ces attributs sont les mêmes que ceux que vous configureriez dans une règle NAT. Les attributs sont soumis à une opération AND, donc les résultats filtrés incluent uniquement les règles qui correspondent à tous les attributs que vous avez configurés.

  - Pour les attributs binaires, tels que l'état de la règle (activé/désactivé), la configuration d'un ensemble PAT (activé/désactivé), le sens de la règle (uni/bi) ou le type de règle (statique/ dynamique), cochez ou décochez les cases appropriées. Cochez les deux cases si vous ne vous souciez pas de la valeur de l'attribut. Si vous décochez les deux cases, aucune règle ne correspondra au filtre.

  - Pour les attributs de chaîne de caractères, saisissez une chaîne complète ou partielle pertinente pour cet attribut. Il s'agira de noms d'objets, pour des zones de sécurité/des groupes d'interfaces, des objets de réseau ou des objets de port. Il peut également s'agir du contenu de l'objet réseau ou de port, qui est mis en correspondance de la même manière que pour les recherches de texte simples.

  Pour supprimer le filtre, cliquez sur le **x** à droite de la zone du filtre, ou cliquez dans la zone du filtre pour ouvrir la liste déroulante, et cliquez sur le bouton Effacer.

# Activation, désactivation ou suppression de plusieurs règles

Vous pouvez activer ou désactiver les règles NAT manuelles, ou supprimer n'importe quelle règle NAT, une par une. Vous pouvez également sélectionner plusieurs règles et appliquer des modifications à toutes ces règles en même temps. Étant donné que l'activation/désactivation s'applique uniquement à la NAT manuelle, si vous sélectionnez une combinaison de types de règles, vous pouvez uniquement les supprimer.

Notez que lorsque vous activez ou désactivez des règles, peu importe que vous sélectionniez des règles qui étaient déjà activées ou désactivées. Par exemple, l'activation d'une règle déjà activée ne modifie pas son état.

**Procédure**

**Étape 1** Sélectionnez **Devices (Périphériques)** > **NAT** et modifiez la **politique NAT de défense contre les menaces**.

**Étape 2** (Facultatif) Filtrez les règles NAT pour localiser celles que vous souhaitez modifier.

Le filtrage est particulièrement utile si vous avez une politique NAT de taille importante. Par exemple, vous pouvez rechercher les règles désactivées pour trouver celles qui doivent être activées.

**Étape 3** Sélectionnez les règles que vous souhaitez modifier.

- Cochez la case dans la colonne de gauche de la règle pour sélectionner (ou désélectionner) des règles individuelles.
- Cochez la case dans l'en-tête du tableau pour sélectionner toutes les règles sur la page actuellement affichée.

Votre sélection est conservée lorsque vous passez d'une page à l'autre. Cependant, en pratique, il est plus logique d'effectuer vos actions sur les règles sélectionnées sur une page avant de passer à la page suivante.

**Étape 4** Effectuez l'action souhaitée. Lorsque vous sélectionnez plusieurs règles, vous êtes invité à confirmer l'action.

Notez que ces actions sont également disponibles dans le menu contextuel.

- Pour activer toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Enable (Activer)**.
- Pour désactiver toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Disable (Désactiver)**.
- Pour supprimer toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Delete (Supprimer)**.

# Traduction d'adresses réseau dynamique

Les rubriques suivantes expliquent la NAT dynamique et comment la configurer.

## À propos de la NAT dynamique

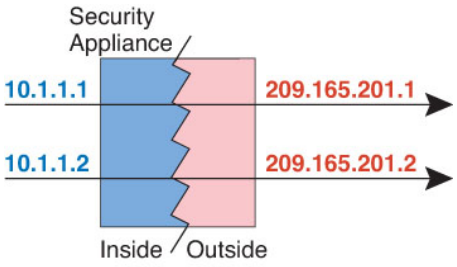
La NAT dynamique traduit un groupe d'adresses réelles en un ensemble d'adresses mappées qui sont routables sur le réseau de destination. Le ensemble mappé comprend généralement moins d'adresses que le groupe réel. Lorsqu'un hôte que vous souhaitez traduire accède au réseau de destination, la NAT attribue à l'hôte une

adresse IP de l'ensemble mappé. La traduction est créée uniquement lorsque l'hôte réel lance la connexion. La traduction n'est en place que pour la durée de la connexion et un utilisateur donné ne conserve pas la même adresse IP après l'expiration de la traduction. Par conséquent, les utilisateurs du réseau de destination ne peuvent pas établir de connexion fiable avec un hôte qui utilise la NAT dynamique, même si la connexion est autorisée par une règle d'accès.

**Remarque** Pour la durée de la traduction, un hôte distant peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès. Une connexion réussie à partir d'un hôte distant peut réinitialiser le minuteur d'inactivité de la connexion.

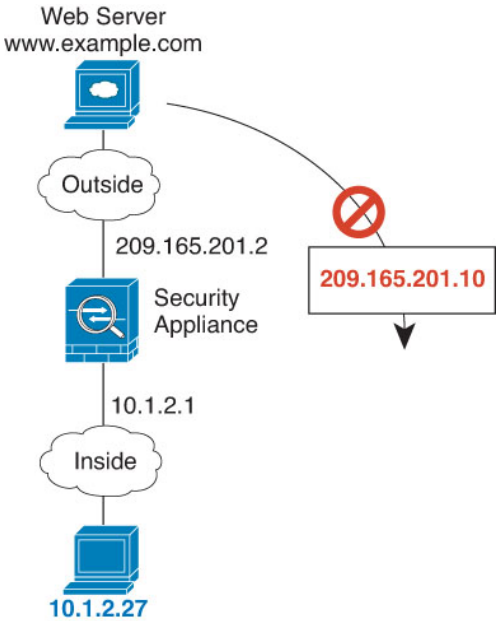
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

***Illustration 4 : Traduction d'adresses réseau dynamique***




La figure suivante montre un hôte distant tentant d'établir une connexion à une adresse mappée. Cette adresse ne figure pas dans la table de traduction actuellement; par conséquent, le paquet est abandonné.

***Illustration 5 : L'hôte distant tente d'établir une connexion à une adresse mappée***



## Avantages et désavantages de la NAT dynamique

La NAT dynamique présente les désavantages suivants :

- Si l'ensemble mappé comporte moins d'adresses que le groupe réel, vous risquez de manquer d'adresses si le trafic est supérieur aux attentes.

  Utilisez PAT ou une méthode de secours PAT si cet événement se produit souvent, car PAT fournit plus de 64 000 traductions utilisant les ports d'une seule adresse.

- Vous devez utiliser un grand nombre d'adresses routables dans l'ensemble mappé, et les adresses routables peuvent ne pas être disponibles en grande quantité.

L'avantage de la NAT dynamique est que certains protocoles ne peuvent pas utiliser la PAT. La PAT ne fonctionne pas avec les éléments suivants :

- Les protocoles IP qui n'ont pas de port à sucrharger, comme GRE version 0.
- Certaines applications multimédias qui ont un flux de données sur un port et le chemin de contrôle sur un autre port, et qui ne sont pas conformes aux normes ouvertes.

## Configurer la NAT automatique dynamique

Utilisez les règles de NAT automatique dynamique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).

- **Type** : sélectionnez **Dynamic** (Dynamique).

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'objet réseau ou le groupe qui contient les adresses mappées.

**Étape 6** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 109.
- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

**Étape 7** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 8** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

## Configurer la NAT manuelle dynamique

Utilisez des règles de NAT manuelles dynamiques lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT dynamique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle .

Pour la NAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

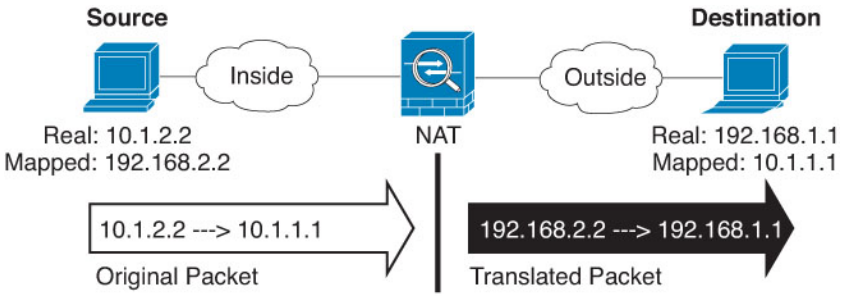
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.




- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

**Étape 6** Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'objet réseau ou le groupe qui contient les adresses mappées.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

**Étape 7** (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port**(port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

**Étape 8** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- (Pour la traduction de source uniquement.) **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction

NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 109.

- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

**Étape 9** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 10** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

# PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

## À propos de la PAT dynamique

La PAT dynamique traduit plusieurs adresses réelles en une seule adresse IP mappée en convertissant l'adresse réelle et le port source en adresse mappée et en un port unique.

Chaque connexion nécessite une session de traduction distincte, car le port source diffère pour chaque connexion. Par exemple, 10.1.1.1:1025 nécessite une traduction distincte de 10.1.1.1:1026.

La figure suivante montre un scénario PAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir. L'adresse mappée est la même pour chaque traduction, mais le port est attribué dynamiquement.

***Illustration 6 : PAT dynamique***


Pour la durée de la traduction, un hôte distant sur le réseau de destination peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse du port (réelle et mappée) est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès.

Après l'expiration de la connexion, la traduction de port expire également.

**Remarque** Nous vous recommandons d'utiliser différents ensembles de PAT pour chaque interface. Si vous utilisez le même ensemble pour plusieurs interfaces, en particulier si vous l'utilisez pour l'interface « n'importe quelle », l'ensemble peut être rapidement épuisé, et aucun port n'est disponible pour les nouvelles traductions.

## Avantages et inconvénients de la PAT dynamique

La PAT dynamique vous permet d'utiliser une seule adresse mappée, préservant ainsi les adresses routables. Vous pouvez même utiliser l'adresse IP de l'interface appareil de défense contre les menaces comme adresse PAT.

Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.

La PAT dynamique ne fonctionne pas avec certaines applications multimédias dont le flux de données est différent de celui du chemin de contrôle. Pour obtenir plus de renseignements, consultez Prise en charge de la NAT pour les protocoles inspectés, à la page 13.

La PAT dynamique peut également créer un grand nombre de connexions semblant provenir d'une seule adresse IP, et les serveurs peuvent interpréter le trafic comme une attaque DoS. Vous pouvez configurer un ensemble d'adresses PAT et utiliser une affectation des adresses PAT à tour de rôle pour atténuer cette situation.

## Directives pour les objets du regroupement PAT

Lors de la création d'objets réseau pour un ensemble de PAT, suivez ces directives.

### Pour un ensemble de PAT

- Les ports sont mappés à un port disponible dans la plage 1 024 à 65 535. Vous pouvez éventuellement inclure les ports réservés, ceux en dessous de 1024, pour rendre l'ensemble de la plage de ports disponible pour les traductions.

  Lors du fonctionnement dans une grappe, des blocs de 512 ports par adresse sont alloués aux membres de la grappe, et les mappages sont effectués dans ces blocs de ports. Si vous activez également l'allocation de blocs, les ports sont distribués en fonction de la taille de l'allocation de blocs, dont la taille par défaut est également de 512.

- Si vous activez l'allocation de blocs pour un ensemble PAT, les blocs de ports sont alloués dans la plage 1 024 à 65535 uniquement. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte.
- Si vous utilisez le même objet de pool PAT dans deux règles distinctes, veillez à spécifier les mêmes options pour chaque règle. Par exemple, si une règle spécifie une PAT étendue, l'autre règle doit également spécifier une PAT étendue.
- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utilisent la même adresse IP PAT. Si aucun port n'est disponible, cela peut empêcher la connexion. Utilisez l'option tourniquet (round robin) pour éviter ce problème.
- Pour des performances optimales, limitez à 10 000 le nombre d'adresses IP dans un ensemble de PAT.

#### Pour PAT étendu pour un ensemble PAT

- De nombreuses inspections d'applications ne prennent pas en charge la PAT étendue.
- Si vous activez la PAT étendue pour une règle PAT dynamique, vous ne pouvez pas utiliser une adresse dans l'ensemble PAT comme adresse PAT dans une NAT statique distincte avec règle de traduction de port. Par exemple, si l'ensemble PAT comprend la version 10.1.1, vous ne pouvez pas créer de règle NAT statique avec traduction de port en utilisant 10.1.1.1 comme adresse PAT.
- Si vous utilisez un ensemble de PAT et que vous définissez une interface de secours, vous ne pouvez pas définir une PAT étendue.
- Pour les déploiements VoIP qui utilisent ICE ou TURN, n'utilisez pas la PAT étendue. ICE et TURN reposent sur la liaison PAT pour être la même pour toutes les destinations.
- Vous ne pouvez pas utiliser la PAT étendue sur les unités d'une grappe.
- La PAT étendue augmente l'utilisation de la mémoire sur le périphérique.

#### Pour un tourniquet (round robin) pour un ensemble de PAT

- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utiliseront la même adresse IP PAT si des ports sont disponibles. Cependant, cette « permanence » ne survit pas à un basculement. Si le périphérique bascule, les connexions ultérieures à partir d'un hôte pourraient ne pas utiliser l'adresse IP initiale.
- La « permanence » d'adresse IP est également affectée si vous combinez des règles de pool PAT/round robin avec des règles PAT d'interface sur la même interface. Pour une interface donnée, choisissez un ensemble de PAT ou une PAT d'interface; ne créez pas de règles PAT concurrentes.
- La méthode « round robin », en particulier lorsqu'elle est combinée à une PAT étendue, peut consommer une grande quantité de mémoire. Étant donné que les ensembles NAT sont créés pour chaque protocole/adresse IP/plage de ports mappés, la répétition alternée entraîne la création d'un grand nombre d'ensembles NAT simultanés, qui utilisent de la mémoire. Une PAT étendue se traduit par un nombre encore plus important de pools NAT simultanés.

## Configurer la PAT automatique dynamique

Utilisez les règles PAT automatiques dynamiques pour traduire les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire vers une adresse unique (l'adresse de l'interface de destination ou une autre adresse) ou utiliser un groupement d'adresses PAT pour fournir le plus grand nombre de traductions possibles.

#### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :

- **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau.
- **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.
- **Groupement de PAT** : créez un objet réseau qui comprend une plage ou créez un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Dynamic** (Dynamique).

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'une des sources suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin. Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide.

**Étape 6** Si vous faites appel à la réserve PAT, sélectionnez la page **PAT Pool** et procédez comme suit :

a) Sélectionnez **Enable PAT pool** (activer la réserve PAT).
b) Sélectionnez le groupe d'objets réseau qui contient les adresses de la réserve dans le champ **PAT** > **Address** (adresse PAT).

   Vous pouvez également sélectionner l'IP de **l'interface de destination**, ce qui est une autre façon d'implémenter l'interface PAT.

c) (Facultatif) Sélectionnez les options suivantes selon vos besoins :

   - **Use Round Robin Allocation** (utiliser l'affectation tourniquet) : Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
   - **Extended PAT Table** (le tableau PAT étendu) : Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.
   - **Flat Port Range** (plage plate de ports), **Include Reserved Ports** (inclure les ports de la réserve) : Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.
   - **Block Allocation** (attribution en bloc) : Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

**Étape 7** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Fallthrough to Interface PAT (Destination Interface)** (Transition vers l'interface PAT (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.

Vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite ou regroupement de PAT.

- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

**Étape 8** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 9** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

## Configurer la PAT manuelle dynamique

Utilisez des règles PAT manuelles dynamiques lorsque la PAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La PAT dynamique traduit les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire vers une adresse unique (l'adresse de l'interface de destination ou une autre adresse) ou utiliser un groupement d'adresses PAT pour fournir le plus grand nombre de traductions possibles.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.
  - **Groupement de PAT** : créez un objet réseau qui comprend une plage ou créez un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle .

Pour la NAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.

- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

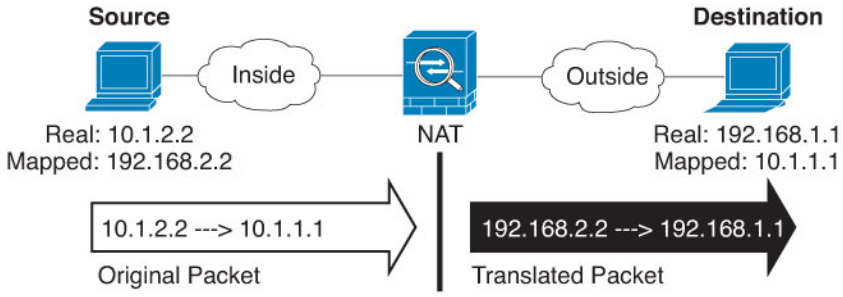
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.




- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

**Étape 6** Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'une des sources suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin. Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

**Étape 7** (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port**(port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

**Étape 8** Si vous faites appel à la réserve PAT, sélectionnez la page **PAT Pool** et procédez comme suit :

a) Sélectionnez **Enable PAT pool** (activer la réserve PAT).

b) Sélectionnez le groupe d'objets réseau qui contient les adresses de la réserve dans le champ **PAT** > **Address** (adresse PAT).

Vous pouvez également sélectionner l'IP de **l'interface de destination**, ce qui est une autre façon d'implémenter l'interface PAT.

c) (Facultatif) Sélectionnez les options suivantes selon vos besoins :

- **Use Round Robin Allocation** (utiliser l'affectation tourniquet) : Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
- **Extended PAT Table** (le tableau PAT étendu) : Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.

- **Flat Port Range** (plage plate de ports), **Include Reserved Ports** (inclure les ports de la réserve) : Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces  exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.
- **Block Allocation** (attribution en bloc) : Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

**Étape 9** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

**Étape 10** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 11** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

## Configurer PAT avec l'attribution de bloc de ports

Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs sont libérés lorsque le dernier xlate qui utilise un port dans le bloc est supprimé.

La réduction de la journalisation est la principale raison de l'attribution de blocs de ports. L'attribution du bloc de ports est journalisée, les connexions sont journalisées, mais les xlates créés dans le bloc de ports ne sont pas journalisés. En revanche, cela rend l'analyse du journal plus difficile.

Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le

port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte. Vous pouvez créer une règle NAT distincte qui n'utilise pas l'allocation de bloc pour les applications qui utilisent des numéros de port faibles; pour les NAT doubles, assurez-vous que la règle est placée avant la règle d'attribution Block (blocage).

### Avant de commencer

Notes sur l'utilisation des règles NAT :

- Vous pouvez inclure l'option **Use Round Robin Allocation** (Utiliser l'allocation Round Robin), mais vous ne pouvez pas inclure les options pour étendre l'unicité PAT, en utilisant une plage uniforme, y compris les ports réservés, ou en passant par l'interface PAT. D'autres informations sur le port et l'adresse de source ou de destination sont également autorisées.
- Comme pour toutes les modifications de NAT, si vous remplacez une règle existante, vous devez effacer les xlates liés à la règle remplacée pour que la nouvelle règle prenne effet. Vous pouvez les effacer explicitement ou simplement attendre qu'ils expirent. Lorsque vous utilisez une grappe, vous devez effacer les xlates globalement dans la grappe.

**Remarque** Si vous basculez entre une PAT standard et une règle PAT d'attribution de blocs, pour la NAT d'objet, vous devez d'abord supprimer la règle, puis effacer les xlates. Vous pouvez ensuite créer la nouvelle règle NAT d'objet. Sinon, vous verrez des abandons p-port-block-state-mismatch dans la sortie **show asp drop**.

- Pour un groupement (pool) PAT donné, vous devez préciser (ou ne pas préciser) l'allocation de bloc pour toutes les règles qui utilisent le groupement. Vous ne pouvez pas allouer de blocs dans une règle et pas dans une autre. Les groupements de PAT qui se chevauchent ne peuvent pas non plus combiner des paramètres d'allocation de bloc. Vous ne pouvez pas non plus superposer la NAT statique avec des règles de traduction de port avec le groupement.

### Procédure

**Étape 1** (Facultatif) Configurez les paramètres globaux d'allocation de bloc de port PAT.

Quelques paramètres globaux contrôlent l'attribution des blocs de ports. Si vous souhaitez modifier les valeurs par défaut de ces options, vous devez configurer un objet FlexConfig et l'ajouter à votre politique FlexConfig.

a) Sélectionnez **Objects (objets)** > **Object Management (Gestion des objets)** > **FlexConfig** > **FlexConfig Object (Objet FlexConfig)** et créez un nouvel objet.

b) Configurez la taille d'allocation de bloc, qui correspond au nombre de ports dans chaque bloc.

**xlate block-allocation size** *value*

La plage est de 32 à 4096. La valeur par défaut est 512. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

Si vous n'utilisez pas la valeur par défaut, assurez-vous que la taille que vous choisissez est divisée de manière égale en 64 512 (le nombre de ports dans la plage 1024-65535). Sinon, certains ports ne pourront pas être utilisés. Par exemple, si vous spécifiez 100, il y aura 12 ports inutilisés.

c) Configurez le nombre maximal de blocs qui peuvent être alloués par hôte.

*nombre* xlate block-allocation maximum-per-host

La limite s'applique par protocole. Une limite de 4 signifie donc tout au plus 4 blocs UDP, 4 blocs TCP et 4 blocs ICMP par hôte. La plage est de 1 à 8, la valeur par défaut est 4. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

d) (Facultatif) Activez la génération syslog provisoire.

**xlate block-allocation pba-interim-logging** *seconds*

Par défaut, le système génère des messages syslog lors de la création et de la suppression d'un bloc de port. Si vous activez la journalisation provisoire, le système génère le message suivant à l'intervalle que vous spécifiez. Les messages font état de tous les blocages de ports actifs à ce moment-là, y compris le protocole (ICMP, TCP, UDP), l'interface source et de destination, l'adresse IP et le blocage de ports. Vous pouvez spécifier un intervalle de 21 600 à 604 800 secondes (de 6 heures à 7 jours).

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

**Exemple :**

Dans l'exemple suivant, la taille de l'allocation de bloc est à 64 et le maximum par hôte à 8 et active la journalisation provisoire toutes les 6 heures.

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) Sélectionner les options suivantes dans l'objet FlexConfig :

- **Deployment** = **Everytime**
- **Type** = **Append**

f) Cliquez sur **Save** (Enregistrer) pour créer l'objet FlexConfig.

g) Sélectionnez **Devices** > **FlexConfig**(périphériques FlexConfig) et créez ou modifiez la politique FlexConfig affectée aux périphériques dont ces paramètres doivent être ajustés.

h) Sélectionnez votre objet dans la liste des objets disponibles et cliquez sur **>** pour le déplacer vers la liste des objets sélectionnés.

i) Cliquez sur **Save** (enregistrer).

Vous pouvez cliquer sur Preview Config **Aperçu de la configuration**, sélectionner l'un des périphériques cibles et vérifier que les commandes xlate s'affichent correctement.

**Étape 2** Ajoutez des règles NAT qui utilisent l'allocation de bloc de ports de groupement (pool) PAT.

a) Sélectionnez **Devices (Périphériques)** > **NAT** et ajoutez ou modifiez la politique NAT de défense contre les menaces.

b) Ajoutez ou modifiez une règle NAT et configurez au moins les options suivantes.

- **Type** = **Dynamic**
- In **Translation (Traduction)** > **Original Source (Source d'origine)**, sélectionnez l'objet qui définit l'adresse source.
- Dans l'onglet **PAT Pool**, configurez les options suivantes :
  - Sélectionnez **Enable PAT pool** (activer le groupement PAT).

- Dans **PAT** > **Address**(adresse PAT), sélectionnez un objet ou un groupe réseau qui définit le groupement PAT.
- Sélectionnez l'option de **l'attribution en bloc**.

c) Enregistrez vos modifications à la règle et à la politique NAT.

# NAT statique

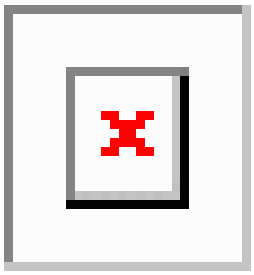
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

## À propos de la NAT statique

La NAT statique crée une traduction fixe d'une adresse réelle en adresse mappée. Comme l'adresse mappée est la même pour chaque connexion consécutive, la NAT statique permet l'établissement d'une connexion bidirectionnelle, à la fois vers et à partir de l'hôte (si une règle d'accès existe qui le permet). Avec la NAT et la PAT dynamiques, en revanche, chaque hôte utilise une adresse ou un port différent pour chaque traduction ultérieure, de sorte que le lancement bidirectionnel n'est pas pris en charge.

La figure suivante montre un scénario de NAT statique typique. La traduction est toujours active, de sorte que les hôtes réels et distants peuvent initier des connexions.

***Illustration 7 : NAT statique***



**Remarque** Vous pouvez désactiver la bidirectionnalité si vous le souhaitez.

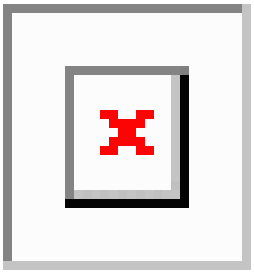
### NAT statique avec traduction de port

La NAT statique avec traduction de port vous permet de spécifier un protocole et un port réels et mappés.

Lorsque vous spécifiez le port avec une NAT statique, vous pouvez choisir de mapper le port et/ou l'adresse IP à la même valeur ou à une valeur différente.

La figure suivante présente un scénario typique de NAT statique avec traduction de port, représentant à la fois un port mappé sur lui-même et un port mappé à une valeur différente. l'adresse IP est mappée sur une valeur différente dans les deux cas. La traduction est toujours active, donc les hôtes traduits et distants peuvent initier des connexions.

*Illustration 8 : NAT statique typique avec scénario de traduction de port*



Les règles statiques de NAT avec traduction de port limitent l'accès à l'adresse IP de destination pour le port spécifié uniquement. Si vous essayez d'accéder à l'adresse IP de destination sur un port différent non couvert par une règle NAT, la connexion est bloquée. De plus, pour manual NAT (NAT manuelle), le trafic qui ne correspond pas à l'adresse IP source de la règle NAT sera abandonné s'il correspond à l'adresse IP de destination, quel que soit le port de destination. Par conséquent, vous devez ajouter des règles supplémentaires pour tout autre trafic autorisé vers l'adresse IP de destination. Par exemple, vous pouvez configurer une règle NAT statique pour l'adresse IP, sans spécification de port, et la placer après la règle de traduction de port.

**Remarque** Pour les applications qui nécessitent une inspection d'application pour les canaux secondaires (par exemple, FTP et VoIP), la NAT traduit automatiquement les ports secondaires.

Voici quelques autres utilisations de la NAT statique avec traduction de port.

**NAT statique avec traduction de port d'identité**

Vous pouvez simplifier l'accès externe aux ressources internes. Par exemple, si vous avez trois serveurs distincts qui fournissent des services sur des ports différents (comme FTP, HTTP et SMTP), vous pouvez donner aux utilisateurs externes une seule adresse IP pour accéder à ces services. Vous pouvez ensuite configurer la NAT statique avec traduction de port d'identité pour mapper l'adresse IP externe unique avec les adresses IP correctes des serveurs réels en fonction du port auquel ils tentent d'accéder. Vous n'avez pas besoin de modifier le port, car les serveurs utilisent des ports standard (21, 80 et 25, respectivement).

**NAT statique avec traduction de port pour les ports non standard**

Vous pouvez également utiliser la NAT statique avec traduction de port pour traduire un port bien connu en un port non standard ou inversement. Par exemple, si les serveurs Web internes utilisent le port 8080, vous pouvez autoriser les utilisateurs externes à se connecter au port 80, puis annuler la traduction sur le port d'origine 8080. De même, pour fournir une sécurité supplémentaire, vous pouvez demander aux utilisateurs Web de se connecter au port non standard 6785, puis annuler la traduction sur le port 80.

**NAT d'interface statique avec traduction de port**

Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec l'adresse/le port 23 de l'interface externe.

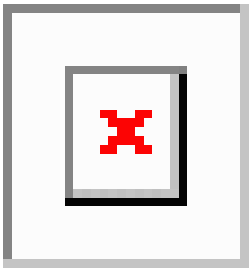
## NAT statique un vers plusieurs

En règle générale, vous configurez la NAT statique avec un mappage un à un. Cependant, dans certains cas, vous souhaiterez peut-être configurer une seule adresse réelle avec plusieurs adresses mappées (une vers

plusieurs). Lorsque vous configurez la NAT statique un-à-plusieurs, lorsque l'hôte réel lance le trafic, il utilise toujours la première adresse mappée. Cependant, pour le trafic initié vers l'hôte, vous pouvez initier le trafic vers n'importe laquelle des adresses mappées, et elles ne seront pas traduites vers l'adresse unique réelle.

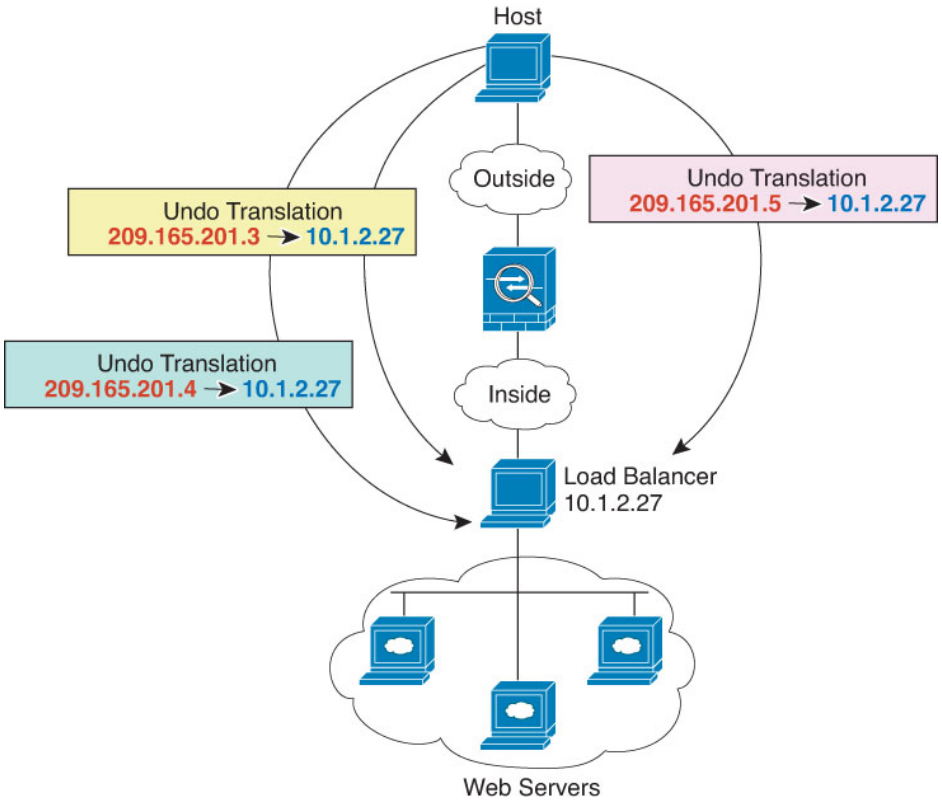
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction IP de l'hôte réel/premier IP mappée est techniquement la seule traduction bidirectionnelle.

***Illustration 9 : NAT statique un vers plusieurs***



Par exemple, vous avez un équilibreur de charge en 10.1.2.27. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

***Illustration 10 : Exemple de NAT statique un vers plusieurs***



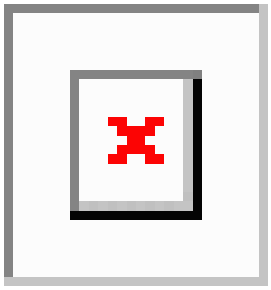
## Autres scénarios de mappage (non recommandés)

La NAT a la flexibilité d'autoriser tout type de scénario de mappage statique : un à un, un à plusieurs, mais aussi les mappages de quelques-uns à plusieurs, de plusieurs à plusieurs et de plusieurs à un. Nous vous recommandons d'utiliser uniquement des mappages un à un ou un à plusieurs. Ces autres options de mappage peuvent avoir des conséquences imprévues.

D'un point de vue fonctionnel, les valeurs « peu à plusieurs » et « un à plusieurs » sont identiques. mais comme la configuration est plus complexe et que les mappages ne sont peut-être pas évidents au premier abord, nous vous recommandons de créer une configuration un-vers-plusieurs pour chaque adresse réelle qui l'exige. Par exemple, pour un scénario de plusieurs vers plusieurs, les quelques adresses réelles sont mappées aux nombreuses adresses mappées dans l'ordre (A à 1, B à 2, C à 3). Lorsque toutes les adresses réelles sont mappées, l'adresse mappée suivante est mappée à la première adresse réelle, et ainsi de suite jusqu'à ce que toutes les adresses mappées soient mappées (A à 4, B à 5, C à 6). Il en résulte plusieurs adresses mappées pour chaque adresse réelle. Tout comme dans une configuration un-à-plusieurs, seuls les premiers mappages sont bidirectionnels; les mappages suivants permettent d'amorcer le trafic *vers* l'hôte réel, mais tout le trafic en *provenance de* l'hôte réel utilise uniquement la première adresse mappée pour la source.

La figure suivante montre un scénario typique de NAT statique quelques-uns-plusieurs.

***Illustration 11 : NAT statique quelques-uns vers plusieurs***

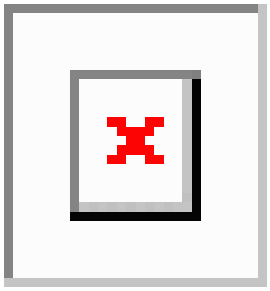


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un lancement bidirectionnel. Les adresses réelles supérieures restantes peuvent initier le trafic, mais le trafic ne peut pas être amorcé vers elles (le trafic de retour d'une connexion est redirigé vers la bonne adresse réelle en raison du quintuple unique (IP source, IP de destination, port source, port de destination, ) pour la connexion).

**Remarque** La NAT plusieurs vers quelques ou plusieurs vers un n'est pas une PAT. Si deux hôtes réels utilisent le même numéro de port source et vont au même serveur externe et au même port de destination TCP, et que les deux hôtes sont traduits vers la même adresse IP, les deux connexions seront réinitialisées en raison d'un conflit d'adresse (le 5-uple n'est pas unique).

La figure suivante montre un scénario de NAT statique « plusieurs à quelques-uns » typique.

*Illustration 12 : NAT statique plusieurs à quelques-uns*



Au lieu d'utiliser une règle statique de cette façon, nous vous suggérons de créer une règle un-à-un pour le trafic qui nécessite un lancement bidirectionnel, puis de créer une règle dynamique pour le reste de vos adresses.

## Configurer la NAT statique automatique

Utilisez les règles de NAT automatique statique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : Vous avez les options suivantes pour spécifier l'adresse traduite :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
  - **Address** (adresse) : crée un objet réseau ou un groupe contenant des hôtes, des plages ou des sous-réseaux. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Statique**.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'une des sources suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez **Address** (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
- (Facultatif) **Port d'origine**, **Port traduit** : si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans **Port d'origine** et saisissez les numéros de port d'origine et traduit. Par exemple, vous pouvez traduire TCP/80 en 8080 au besoin.

**Étape 6** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 109. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Mappage de réseau à réseau** : Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que

l'interface mappée, le système utilise un proxy 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 l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées 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.

**Étape 7** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 8** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

## Configurer la NAT manuelle statique

Utilisez des règles de NAT manuelle statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT statique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : Vous avez les options suivantes pour spécifier l'adresse traduite :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
  - **Adresse** : crée un objet réseau ou un groupe contenant des hôtes, une plage ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle . Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

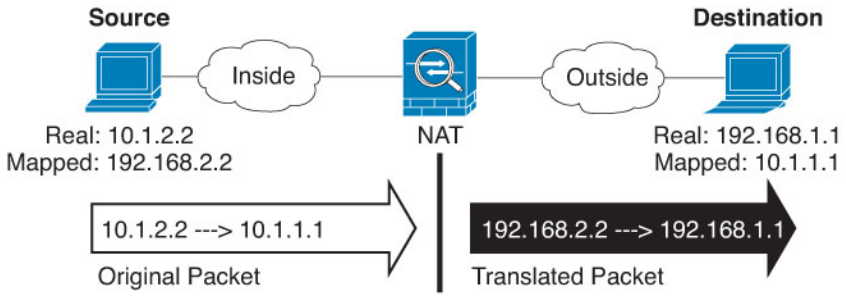
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.




- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

**Étape 6** Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'une des sources suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez **Address** (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

**Étape 7** (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

**Étape 8** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 109. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Mappage de réseau à réseau** : Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy 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 l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées 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.

- **Unidirectionnel** : Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

**Étape 9** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

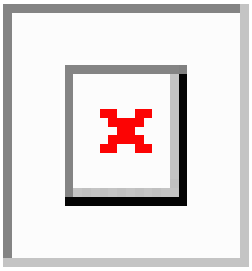
**Étape 10** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

# NAT d'identité

Vous pouvez avoir une configuration NAT dans laquelle vous devez traduire une adresse IP vers elle-même. Par exemple, si vous créez une règle générale qui applique la NAT à tous les réseaux, mais que vous souhaitez exclure un réseau de la NAT, vous pouvez créer une règle NAT statique pour traduire une adresse vers elle-même.

La figure suivante montre un scénario de NAT d'identité typique.

***Illustration 13 : NAT d'identité***



Les rubriques suivantes expliquent comment configurer la NAT d'identité.

## Configurer la NAT automatique d'identité

Utilisez les règles de NAT automatique d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : objet ou groupe réseau ayant exactement le même contenu que l'objet source d'origine. Vous pouvez utiliser le même objet.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Statique**.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Ne configurez pas les options de **port d'origine** et de **port traduit** pour la NAT d'identité.

**Étape 6** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **IPv6** : ne configurez pas cette option pour la NAT d'identité.
- **Mappage réseau à réseau** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy 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 l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées 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.
- **Effectuer une consultation de route pour l'interface de destination**—Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

**Étape 7** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 8** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

## Configurer la NAT manuelle d'identité

Utilisez les règles NAT manuelles d'identité statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. Utilisez les règles NAT d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

### Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : le même objet ou groupe que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle . Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits. Vous pouvez utiliser le même objet pour la NAT d'identité.

### Procédure

**Étape 1** Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

**Étape 2** Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

**Étape 3** Configurez les options des règles de base :

- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.

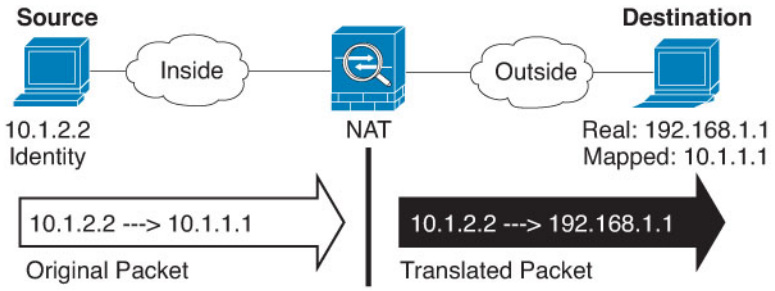
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

**Étape 4** Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

**Étape 5** Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Consultez la figure suivante pour un exemple de paquet d'origine par rapport au paquet traduit dans lequel vous effectuez une NAT d'identité sur l'hôte interne, mais traduit l'hôte externe.




- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Original Destination** (destination d'origine) : (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Objet interface** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

**Étape 6** Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : le même objet ou groupe que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

**Étape 7** (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

**Étape 8** (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy 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 l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées 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.
- **Effectuer une consultation de route pour l'interface de destination**—Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.
- **Unidirectionnel** : Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

**Étape 9** Cliquez sur **Save** (enregistrer) pour ajouter la règle.

**Étape 10** Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

# Propriétés de la règle NAT pour Défense contre les menaces

Utilisez les règles de traduction d'adresses réseau (NAT) pour traduire des adresses IP en d'autres adresses IP. Vous utilisez généralement les règles NAT pour convertir les adresses privées en adresses routables publiquement. La traduction peut se faire d'une adresse à une autre, ou vous pouvez utiliser la traduction d'adresses de port (PAT) pour traduire de nombreuses adresses en une ou quelques adresses, en utilisant les numéros de port pour faire la distinction entre les adresses source.

Les règles NAT comprennent les propriétés de base suivantes. Les propriétés sont les mêmes pour les règles NAT automatique et manuelle, sauf mention contraire.

**Type de NAT**

Si vous souhaitez configurer une **règle NAT manuelle** ou une **règle NAT automatique**. La NAT automatique traduit uniquement l'adresse source et vous ne pouvez pas faire différentes traductions en fonction de l'adresse de destination. La NAT automatique étant plus simple à configurer, utilisez-la sauf si vous avez besoin des fonctionnalités ajoutées de la NAT manuelle. Pour plus d'informations sur les différences, consultez Auto NAT et Manual NAT (NAT manuelle), à la page 5.

**Type**

Si la règle de traduction est **Dynamique** ou **Statique**. La traduction dynamique choisit automatiquement l'adresse mappée dans un ensemble d'adresses ou une combinaison adresse/port lors de la mise en œuvre de la PAT. Utilisez la traduction statique si vous souhaitez définir avec précision l'adresse ou le port mappé.

**Activer (NAT manuelle uniquement)**

Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles. Vous ne pouvez pas désactiver les règles NAT automatique.

**Insérer (NAT manuelle uniquement)**

Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

**Description (facultative) NAT manuelle uniquement.)**

Une description de l'objectif de la règle.

Les rubriques suivantes décrivent les onglets des propriétés des règles NAT.

## Propriétés de la NAT des objets de l'interface

Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. En mode routé, vous pouvez utiliser la valeur par défaut « any » (toute) pour la source et la destination à appliquer à toutes les interfaces de tous les périphériques affectés. Cependant, vous souhaitez généralement sélectionner des interfaces source et destination spécifiques.

**Notes**

- Le concept d'interface « toute » ne s'applique pas aux interfaces des membres des groupes de ponts. Lorsque vous spécifiez une interface « any », toutes les interfaces des membres des groupes de ponts sont exclues. Ainsi, pour appliquer la NAT aux membres du groupe de ponts, vous devez préciser l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface virtuelle de pont (BVI) elle-même, vous pouvez configurer la NAT pour les interfaces membres uniquement.

  Si vous sélectionnez des objets d'interface, une règle NAT sera configurée sur un périphérique affecté uniquement si le périphérique a des interfaces incluses dans tous les objets sélectionnés. Par exemple, si vous sélectionnez des zones de sécurité source et de destination, les deux zones doivent contenir une ou plusieurs interfaces pour un périphérique donné.

- S'il existe plusieurs interfaces dans un objet d'interface sur un périphérique donné, des règles identiques sont créées pour chaque interface. Cela peut devenir un problème pour les règles NAT statiques qui incluent la traduction de destination. Étant donné que les règles NAT sont appliquées en fonction de la règle du premier résultat, seule la règle créée pour la première interface configurée pour l'objet correspond au trafic. Lors de la configuration de la NAT statique avec traduction de destination, utilisez des objets

d’interface qui comprennent au plus une interface par appareil affecté à la politique NAT pour vous assurer d’obtenir les résultats souhaités.

**Source Interface Objects (objets d'interface source), Destination Interface Objects (objets d'interface de destination)**

(obligatoire pour les interfaces membres des groupe de ponts.) Il s’agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l’objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l’appareil. La **destination** est l’objet qui contient l’interface mappée, celle par laquelle le trafic sort de l’appareil. Par défaut, la règle s’applique à toutes les interfaces (**Any**), à l’exception des interfaces membres des groupes de ponts.

## Propriétés de traduction pour la NAT automatique

Utilisez les options de **traduction** pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s’appliquent uniquement à la NAT automatique.

**Source d’origine (toujours obligatoire)**

L'objet réseau qui contient les adresses à traduire. Cela doit être un objet réseau (et non un groupe), et il peut s’agir d’un hôte, d’une plage ou d’un sous-réseau.

Vous ne pouvez pas créer de règles NAT automatique pour les objets any-ipv4 ou any-ipv6 définis par le système.

**Source traduite (généralement requise)**

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s’agir d’un objet ou d’un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu’un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d’hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l’hôte sont utilisées comme PAT de secours.
- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d’interface.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Ne configurez pas un ensemble de PAT.
  - Pour utiliser une adresse unique autre que l’adresse de l’interface de destination, sélectionnez l’objet réseau hôte que vous avez créé à cette fin. Ne configurez pas un ensemble de PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide. Sélectionnez l’objet d'ensemble PAT sur **PAT Pool** (Bassin PAT).
- **NAT statique** : l’une des options suivantes :
  - Pour utiliser un groupe d’adresses défini, sélectionnez **Address** (adresse), puis l’objet ou le groupe de réseau qui contient les adresses mappées. L’objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

- (NAT d’interface statique avec traduction de port.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l’adresse IPv6 de l’interface, vous devez également sélectionner l’option **IPv6** sous l’onglet **Advanced** (Avancé). Cela configure la NAT de l’interface statique avec traduction de port : l’adresse/le port source sont traduits en l’adresse de l’interface et le même numéro de port.

- **NAT d’identité** : le même objet que la source d’origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

**Port d'origine, Port traduit (NAT statique uniquement)**

Si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans **Port d’origine** et saisissez les numéros de port d’origine et traduit. Par exemple, vous pouvez traduire TCP/80 en 8080 au besoin. Ne configurez pas ces options pour la NAT d’identité.

## Propriétés de traduction pour la NAT manuelle

Utilisez les options de **traduction** pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s’appliquent uniquement à la NAT manuelle. Tous ces éléments sont facultatifs, sauf indication contraire.

**Source d’origine (toujours obligatoire)**

L'objet ou le groupe de réseaux qui contient les adresses que vous traduisez. Il peut s’agir d’un objet ou d’un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d’origine, vous pouvez spécifier **Any** (Tout) dans la règle.

**Source traduite (généralement requise)**

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s’agir d’un objet ou d’un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu’un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d’hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l’hôte sont utilisées comme PAT de secours.

- **PAT dynamique** : l'un des éléments suivants :

  - (PAT d’interface.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Ne configurez pas un ensemble de PAT.

  - Pour utiliser une adresse unique autre que l’adresse de l’interface de destination, sélectionnez l’objet réseau hôte que vous avez créé à cette fin. Ne configurez pas un ensemble de PAT.

  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide. Sélectionnez l’objet d'ensemble PAT sur **PAT Pool** (Bassin PAT).

- **NAT statique** : l’une des options suivantes :

  - Pour utiliser un groupe d’adresses défini, sélectionnez **Address** (adresse), puis l’objet ou le groupe de réseau qui contient les adresses mappées. L’objet ou le groupe peut contenir des

hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

- (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, vous devez également sélectionner l'option **IPv6** sous l'onglet **Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.

- **NAT d'identité** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

**Destinations d'origine**

L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

**Destination traduite**

L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Vous pouvez utiliser un objet réseau qui spécifie un nom de domaine complet comme destination traduite; pour en savoir plus, consultez Directives de destination de nom de domaine complet (FQDN), à la page 15.

**Port source d'origine, Port source traduit, Port de destination d'origine, Port de destination traduit**

Les objets de port qui définissent les services de source et de destination pour les paquets d'origine et les paquets traduits. Vous pouvez traduire les ports ou sélectionner le même objet pour rendre la règle sensible au service sans traduire les ports. Gardez les règles suivantes à l'esprit lors de la configuration des services :

- (NAT ou PAT dynamique.) Vous ne pouvez pas effectuer de traduction sur le **port source d' origine** et le **port source traduit**. Vous ne pouvez effectuer la traduction que sur le port de destination.

- La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

## Propriétés NAT de l'ensemble d'adresses PAT

Lorsque vous configurez la NAT dynamique, vous pouvez définir un ensemble d'adresses à utiliser pour la traduction d'adresses de port en utilisant les propriétés de l'onglet **PAT Pool** (Bassin PAT).

**Activer le bassin PAT**

Sélectionnez cette option pour configurer un ensemble d'adresses pour PAT.

**PAT**

Les adresses à utiliser pour l'ensemble PAT, soit l'une des suivantes :

- **Address** (adresse) : L'objet qui définit les adresses de l'ensemble PAT, soit un objet réseau qui comprend une plage, soit un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- **Adresse IP de l'interface de destination** : indique que vous souhaitez utiliser l'interface de destination comme adresse PAT. Pour cette option, vous devez sélectionner un **objet d'interface de destination précis**. vous ne pouvez pas utiliser **Any** (toutes) comme interface de destination. Il s'agit d'une autre façon de mettre en œuvre l'interface PAT.

**Recherche séquentielle**

Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.

**Tableau PAT étendu**

Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.

**Plage de ports non hiérarchique; Inclure les ports réservés**

Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.

**Bloquer l'allocation**

Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec

le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

## Propriétés NAT avancées

Lorsque vous configurez la NAT, vous pouvez configurer les propriétés qui fournissent des services spécialisés dans les options **avancées**. Toutes ces propriétés sont facultatives : ne les configurez que si vous avez besoin du service.

**Traduire les réponses DNS correspondant à cette règle**

Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 109. Cette option n'est pas disponible si vous effectuez une traduction de port dans une règle NAT statique.

**Passage à l'interface PAT (Interface de destination) (NAT dynamique uniquement).**

Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**. Vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas non plus sélectionner l'option si vous configurez un ensemble PAT.

**IPv6**

Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

**Mappage réseau à réseau (NAT statique uniquement).**

Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.

**Ne pas mandater l'ARP sur l'Interface de destination(NAT statique uniquement).**

Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy 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 l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées 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.

**Effectuer une consultation de route pour l'interface de destination (NAT d'identité statique uniquement. Mode routé uniquement.)**

Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

**Unidirectionnel (NAT manuelle uniquement, NAT statique uniquement.)**

Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

# 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 manual NAT (NAT manuelle), 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 manual NAT (NAT manuelle) lorsque vous spécifiez une destination, la création de deux règles auto NAT 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

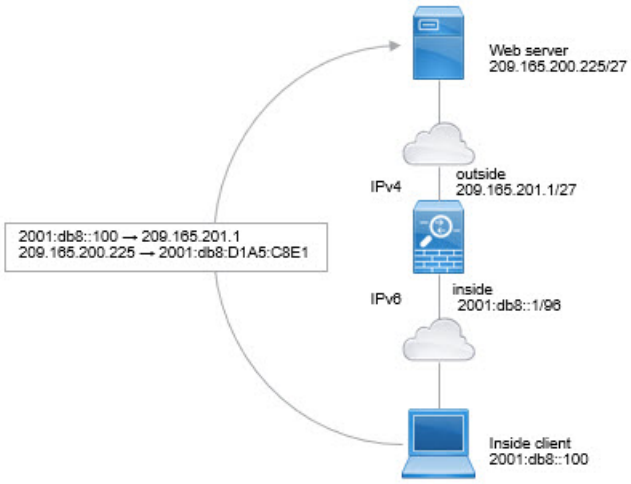
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses 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 manual NAT (NAT manuelle), 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 manual NAT (NAT manuelle) lorsque vous spécifiez une destination, la création de deux règles auto NAT 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 manual NAT (NAT manuelle).



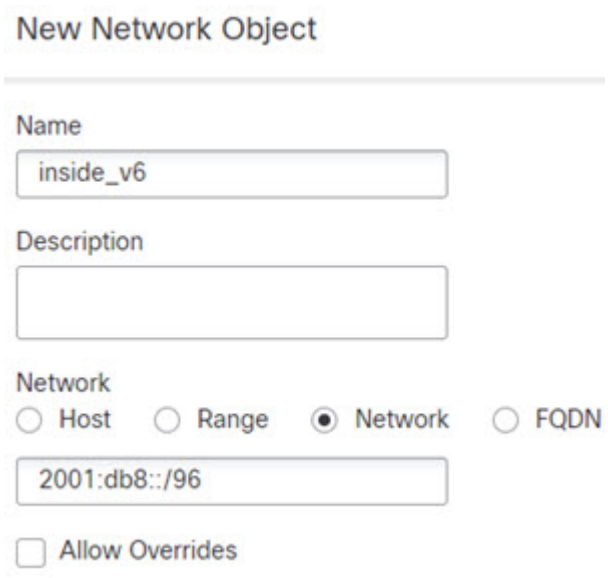

Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne.

### Procédure

**Étape 1** Créez l'objet réseau qui définit le réseau IPv6 interne.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).
c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8::/96.




d) Cliquez sur **Save** (enregistrer).

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

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

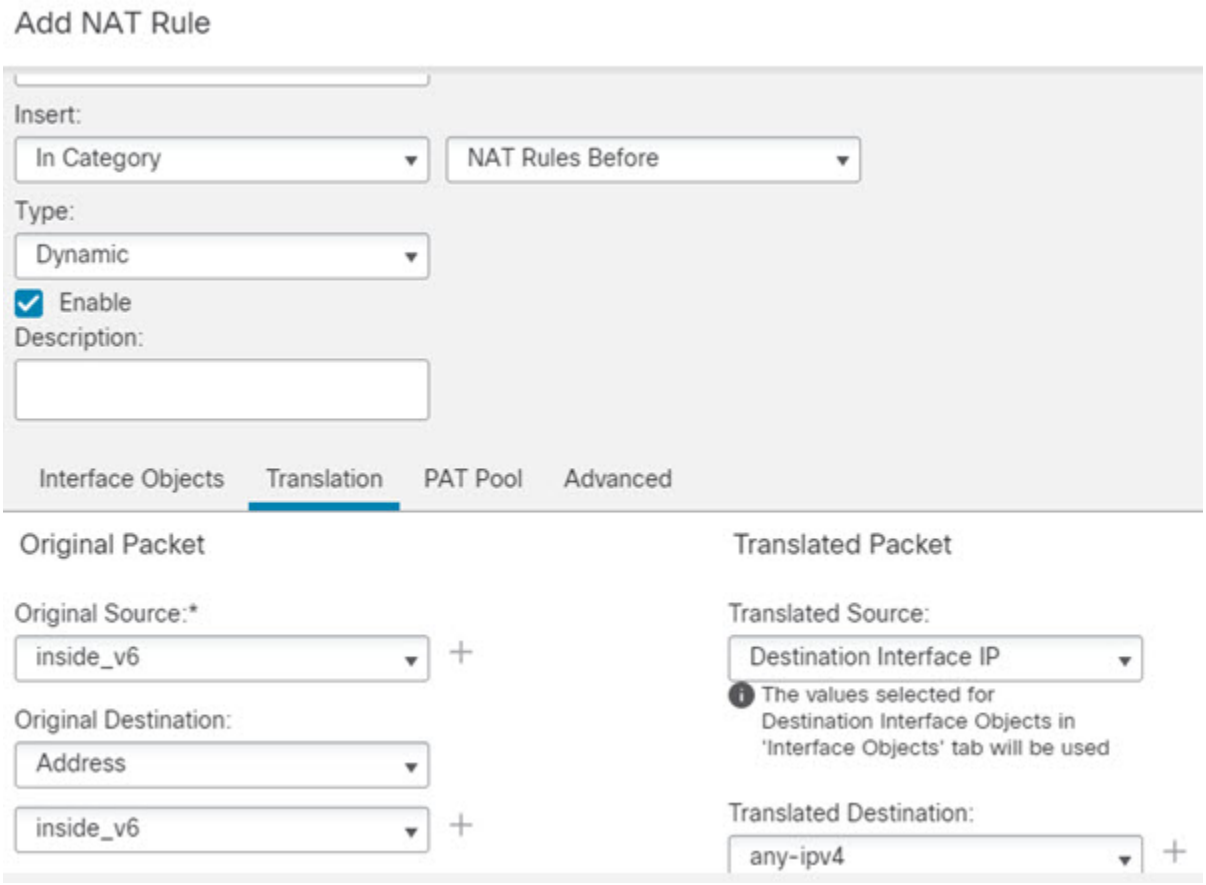
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**).
- **Destination d'origine** = objet réseau interne_v6.
- **Translated Destination** (destination traduite) = any-ipv4 network object.



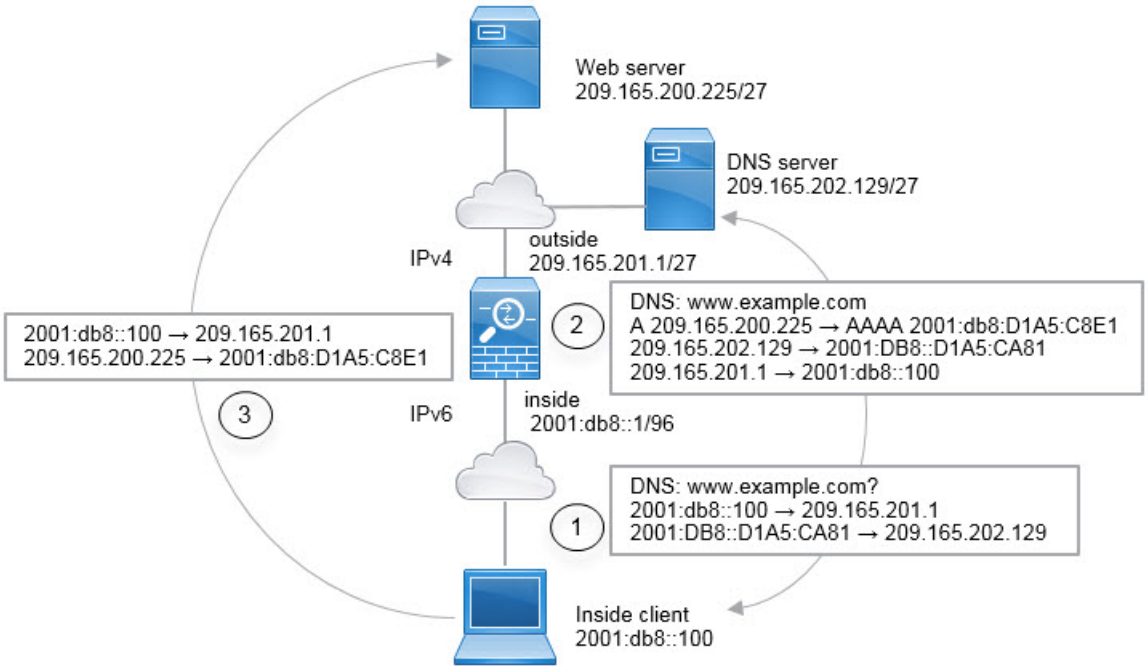

f) Cliquez sur **OK**.

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.

g) Cliquez sur **Save** (Enregistrer) dans la page des règles NAT.

## 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.

### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

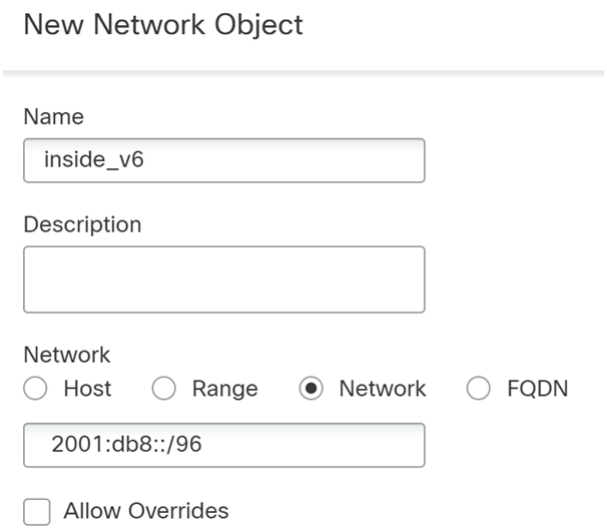
**Étape 1** Créez les objets réseau qui définissent les réseaux IPv6 internes et externes IPv4.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

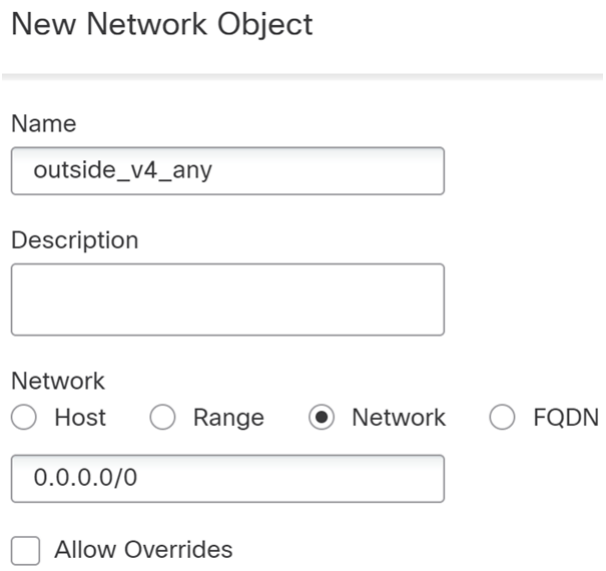
Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8::/96.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau IPv4 externe.

Nommez l'objet réseau (par exemple, Outside_v4_any) et saisissez l'adresse réseau 0.0.0.0/0.




f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle PAT dynamique NAT64 pour le réseau IPv6 interne.

**Étape 3** Configurez la règle NAT46 statique pour le réseau IPv4 externe.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

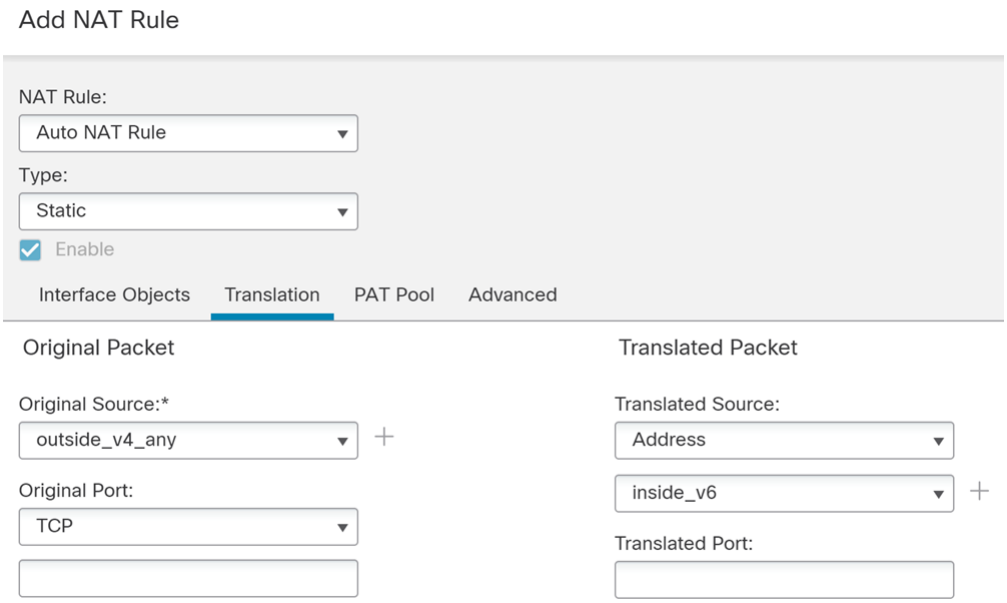
c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = outside_v4_any network object.
- **Translated Source** > **Address** = inside_v6 network object.

e) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).




f) Cliquez sur **OK**.

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.

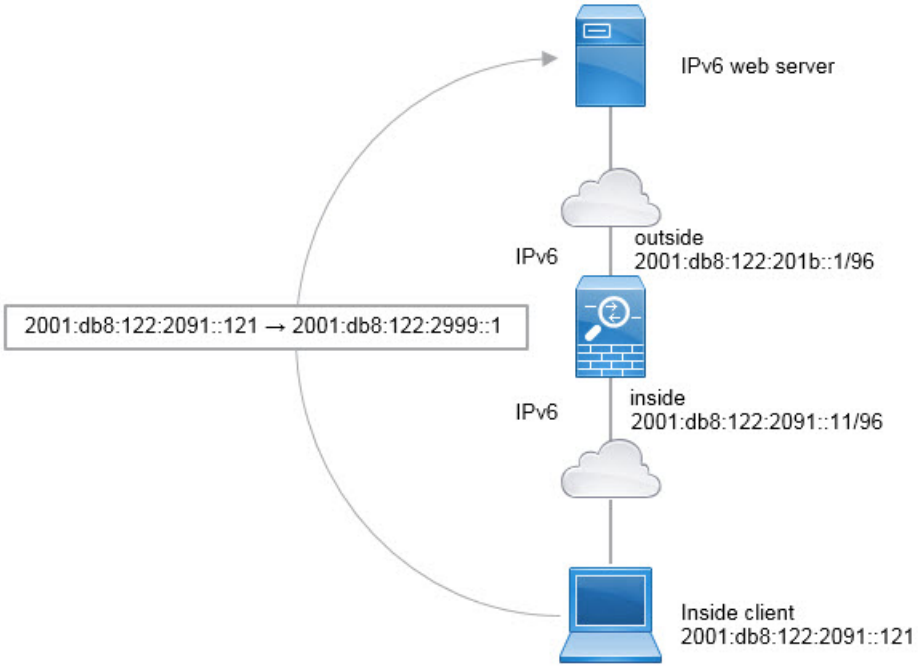
# NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6

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 auto NAT. Toutefois, si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle en utilisant uniquement manual NAT (NAT manuelle).

## Exemple NAT66, de traduction statique entre réseaux

Vous pouvez configurer une traduction statique entre des regroupements d'adresses IPv6 en utilisant auto NAT. 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.




### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

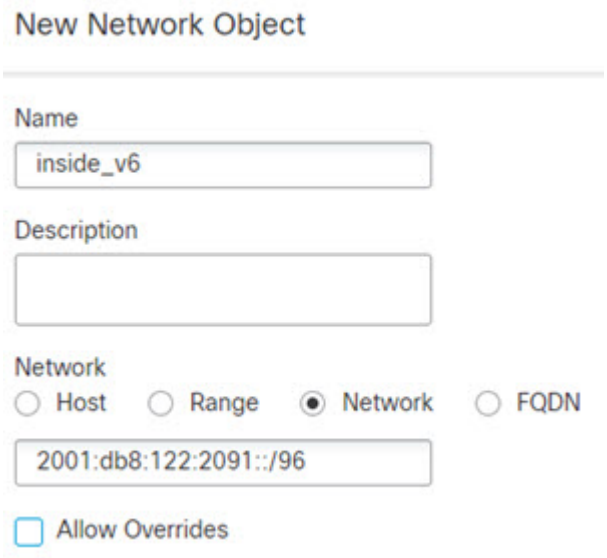
**Étape 1** Créez les objets réseau qui définissent les réseaux NAT IPv6 interne et externe.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

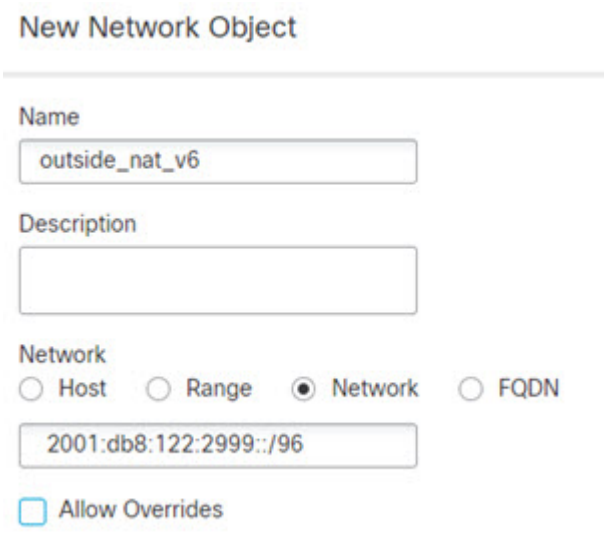
Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8:122:2091::/96.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > ajouter un objet) et définissez le réseau NAT IPv6 externe.

Nommez l'objet réseau (par exemple, Outside_nat_v6) et saisissez l'adresse réseau 2001:db8:122:2999::/96.




f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle NAT statique pour le réseau IPv6 interne.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

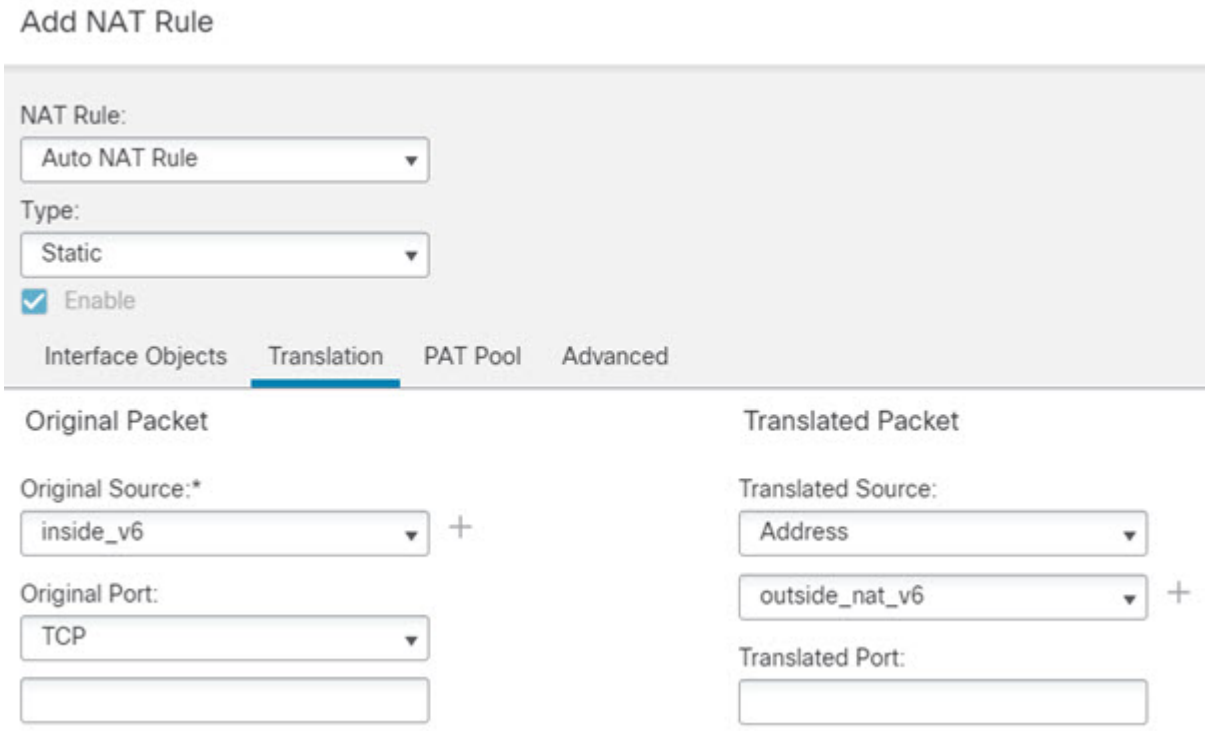
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** > **Address** = outside_nat_v6 network object.



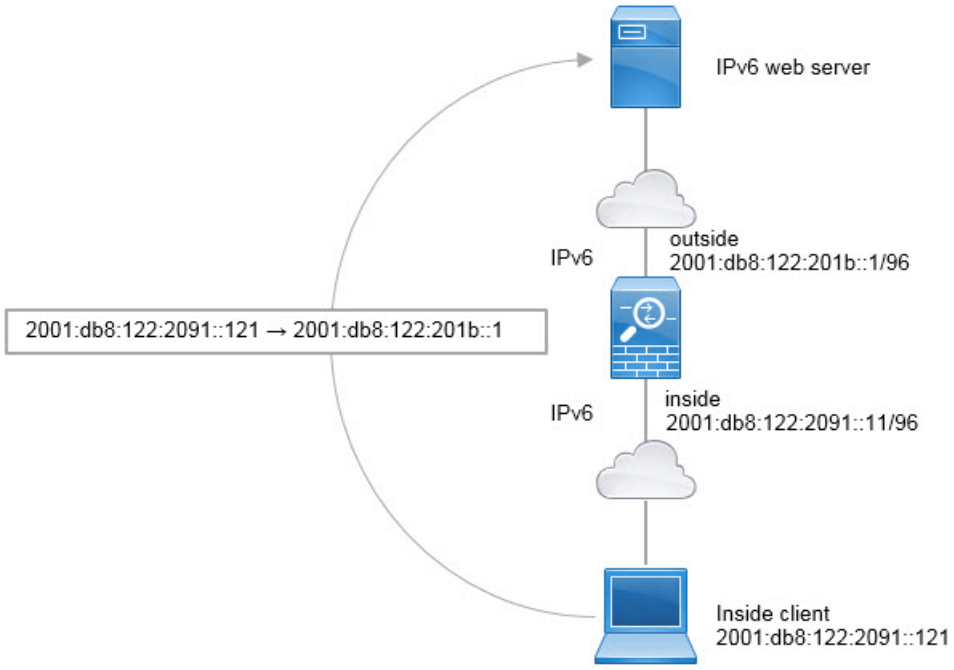

f) Cliquez sur **OK**.

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.




### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

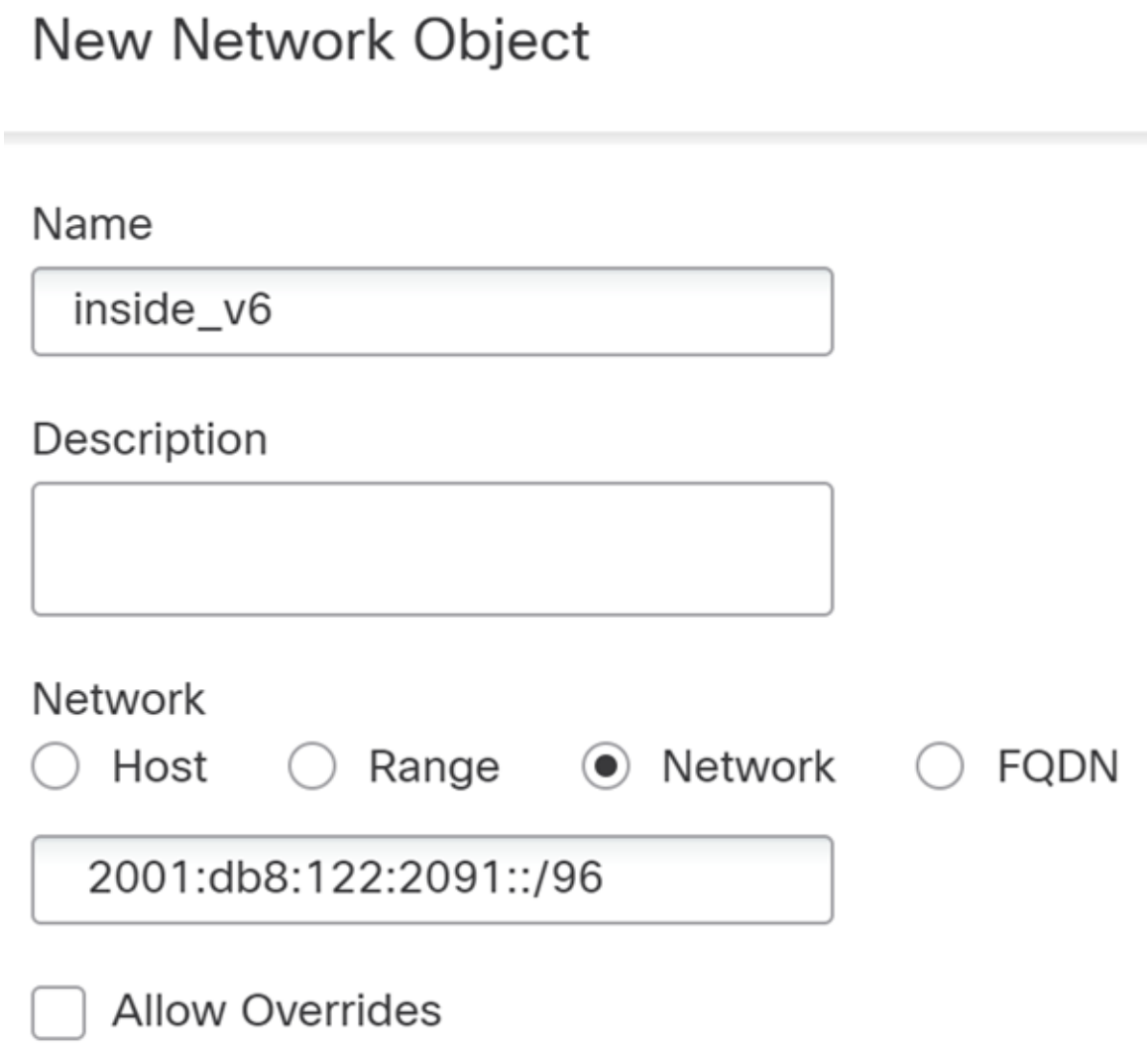
**Étape 1** Créez l'objet réseau qui définit le réseau IPv6 interne.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8:122:2091::/96.




d) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

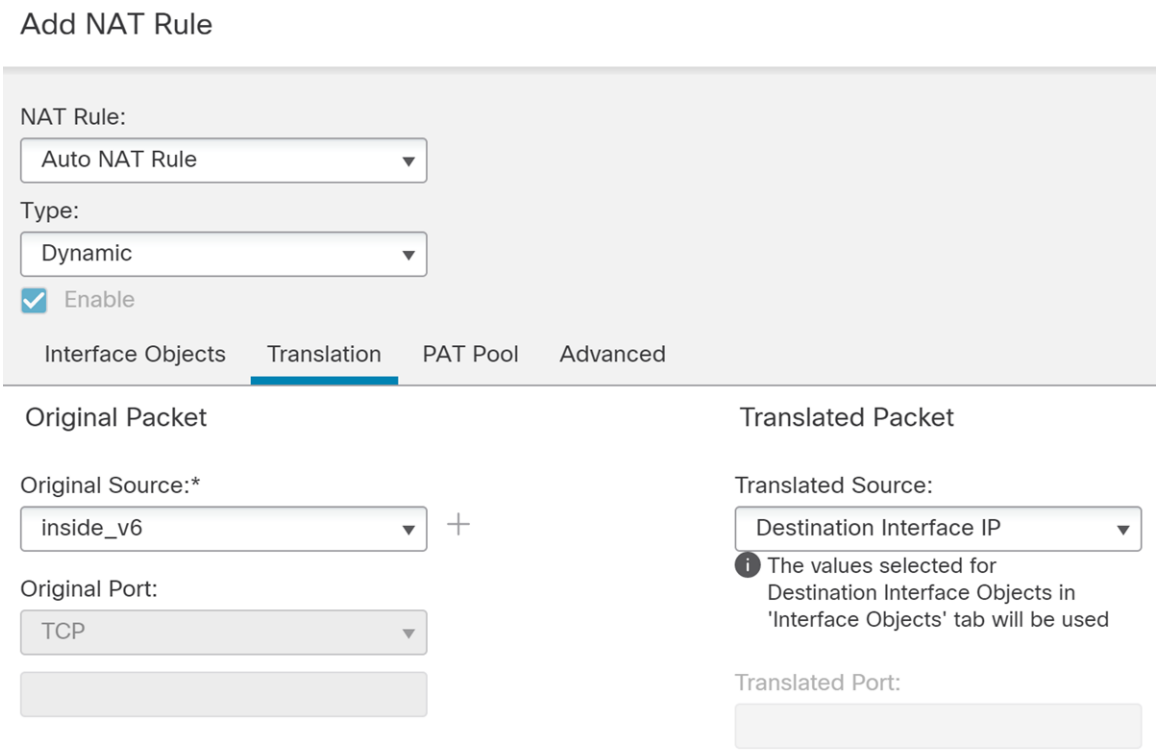
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**).

f) Dans **Avancé**, sélectionnez **IPv6**, ce qui indique que l'adresse IPv6 de l'interface de destination doit être utilisée.




g) Cliquez sur **OK**.

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.

# Surveillance de la NAT

Pour surveiller et dépanner les connexions NAT, connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show nat** affiche les règles NAT et le nombre de résultats par règle. Il existe des mots-clés supplémentaires pour montrer d'autres aspects de la NAT.
- **show xlate** affiche les traductions NAT actuellement actives.

- **clear xlate** vous permet de supprimer une traduction NAT active. Vous devrez peut-être supprimer des traductions actives si vous modifiez les règles NAT, car les connexions existantes continuent d'utiliser l'ancien logement de traduction jusqu'à ce que la connexion se termine. L'effacement d'une traduction permet au système de créer une nouvelle traduction pour un client lors de la prochaine tentative de connexion du client en fonction de vos nouvelles règles.

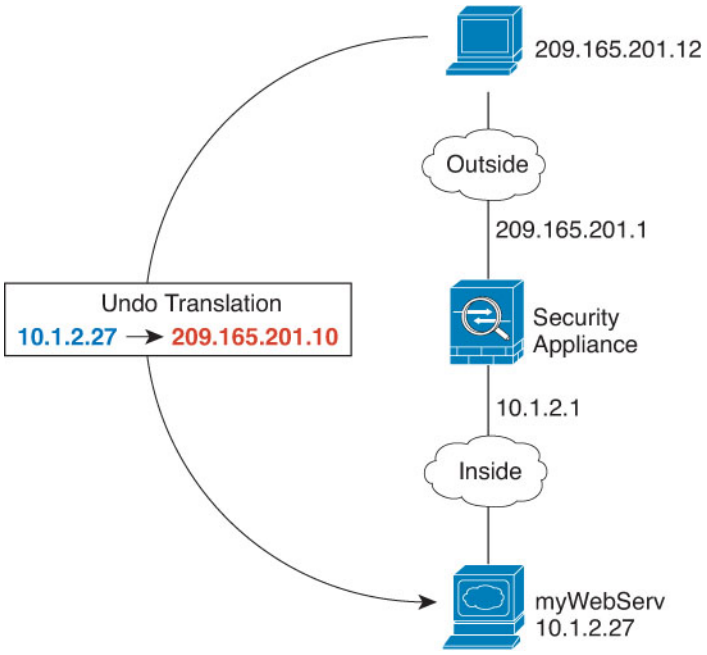
# Exemples relatifs à la NAT

Les rubriques suivantes fournissent des exemples de configuration de la NAT sur les périphériques Threat Defense.

## Fournir l'accès à un serveur Web interne (NAT automatique 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 14 : NAT statique pour un serveur Web interne***




### Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

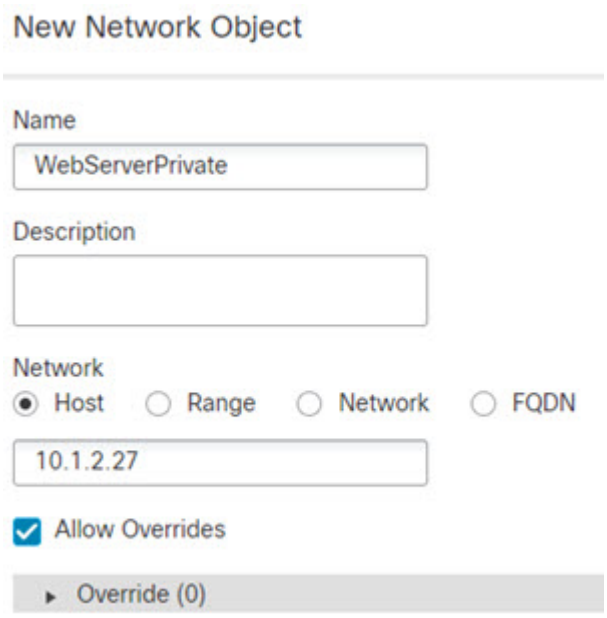
**Étape 1** Créez les objets réseau qui définissent les adresses d'hôte privées et publiques du serveur.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse privée du serveur Web.

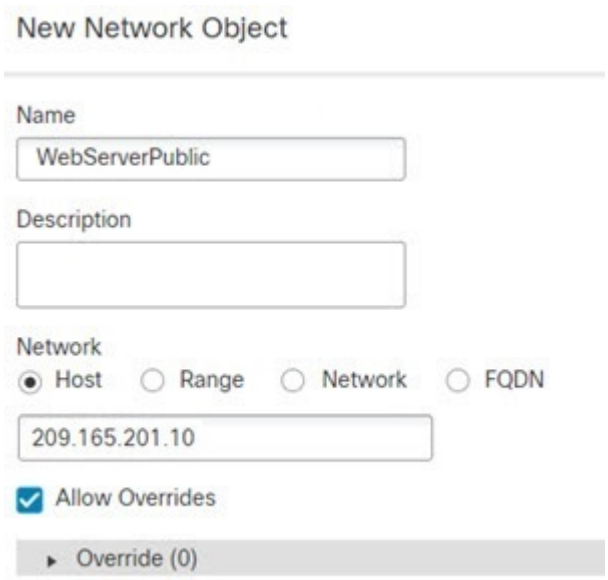
Nommez l'objet réseau (par exemple, WebServerPrivate) et saisissez l'adresse IP réelle de l'hôte, 10.1.2.27.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez l'adresse publique.

Nommez l'objet réseau (par exemple, WebServerPublic) et saisissez l'adresse de l'hôte 209.165.201.10.




f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la NAT statique pour l'objet

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

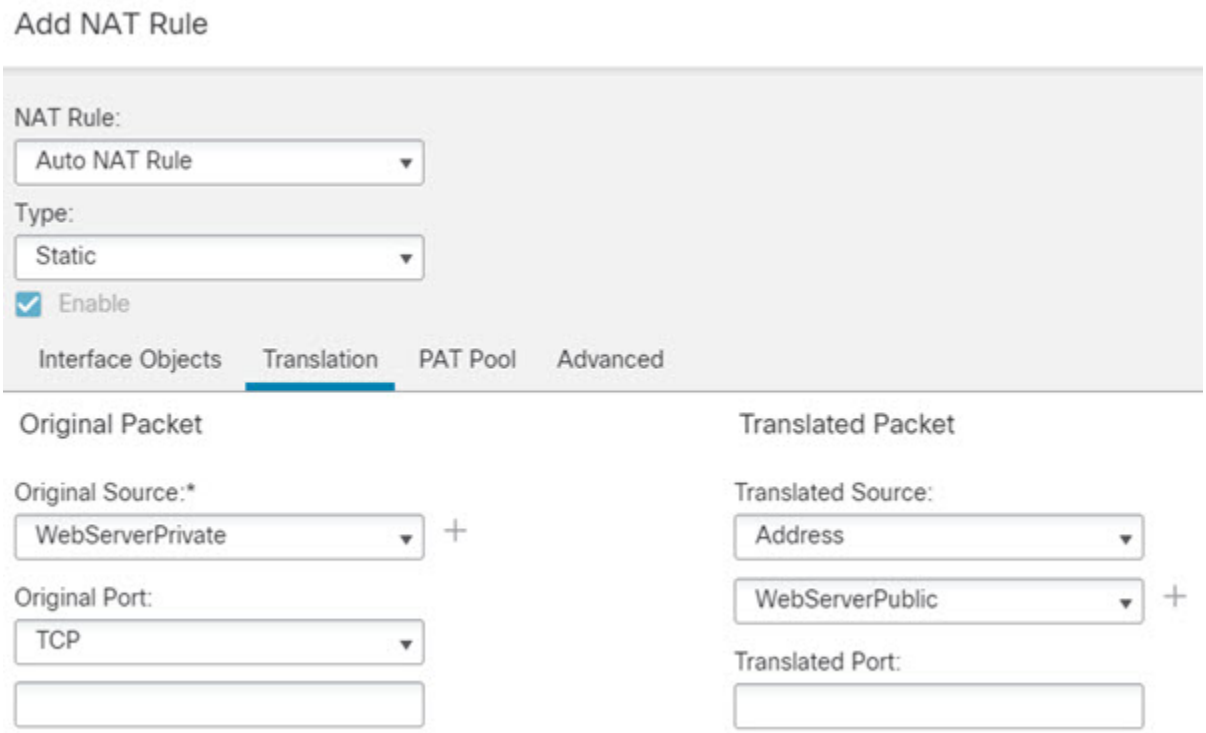
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau WebServerPrivate.
- **Adresse** > **source traduite** = objet réseau WebServerPublic.



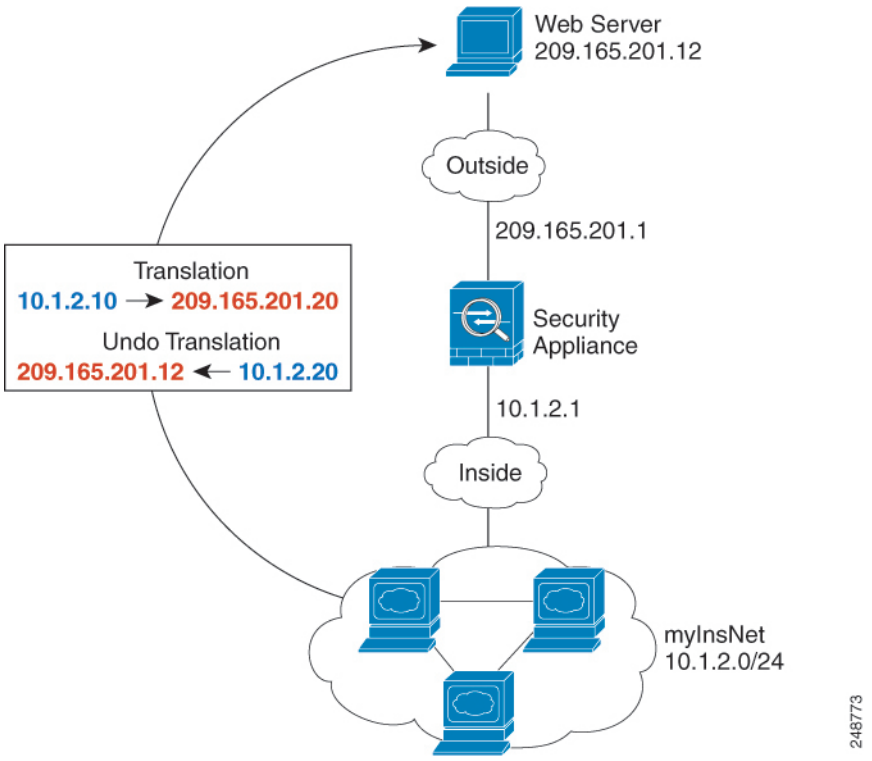

f) Cliquez sur **Save** (enregistrer).

**Étape 3** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# NAT automatique dynamique pour les hôtes internes et NAT statique pour un serveur Web externe

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 15 : NAT dynamique pour l'interne, NAT statique pour le serveur Web externe*




### Avant de commencer

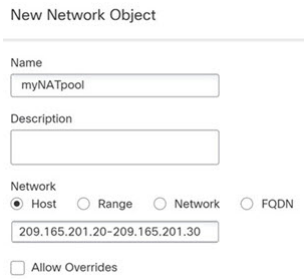
Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

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

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
c) Définissez l'ensemble de NAT dynamique.

Nommez l'objet réseau (par exemple, myNAT Pool) et saisissez la plage réseau 209.165.201.20-209.165.201.30.

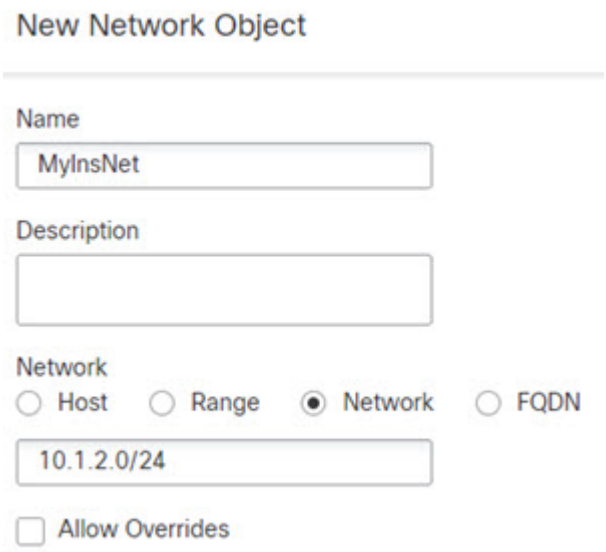



d) Cliquez sur **Save** (enregistrer).

**Étape 2** Créez un objet réseau pour le réseau interne.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, MyInsNet) et saisissez l'adresse réseau 10.1.2.0/24.

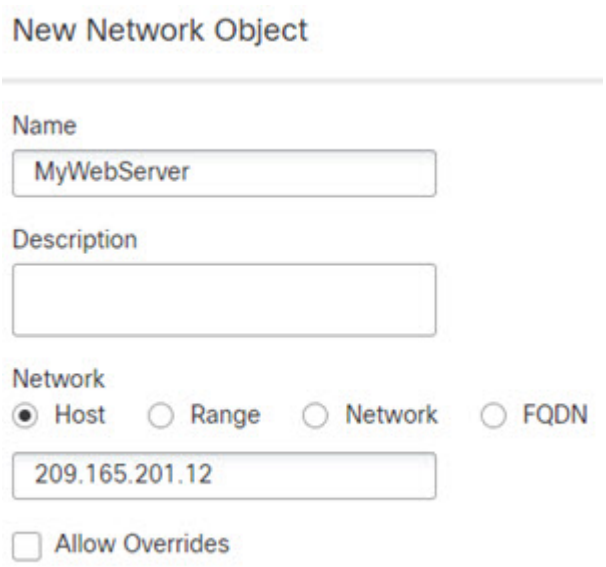



c) Cliquez sur **Save** (enregistrer).

**Étape 3** Créez un objet réseau pour le serveur Web externe.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, MyWebServer) et saisissez l'adresse d'hôte 209.165.201.12.

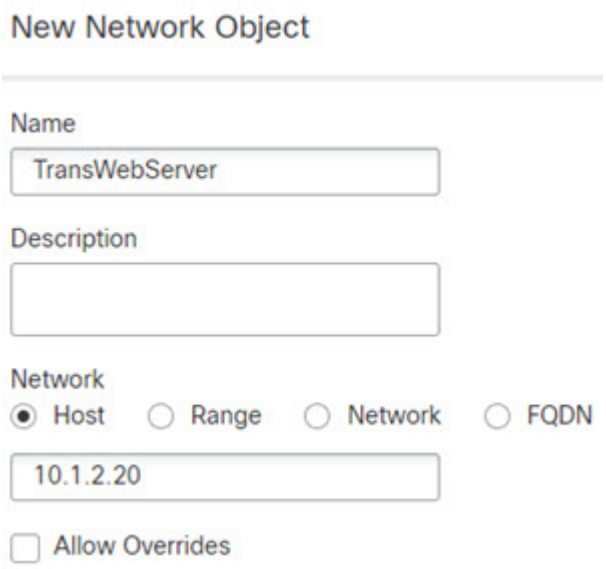



c) Cliquez sur **Save** (enregistrer).

**Étape 4** Créez un objet réseau pour l'adresse traduite du serveur Web.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, TransWebServer) et saisissez l'adresse d'hôte 10.1.2.20.




c) Cliquez sur **Save** (enregistrer).

**Étape 5** Configurez la NAT dynamique pour le réseau interne à l'aide de l'objet ensemble de NAT dynamique.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

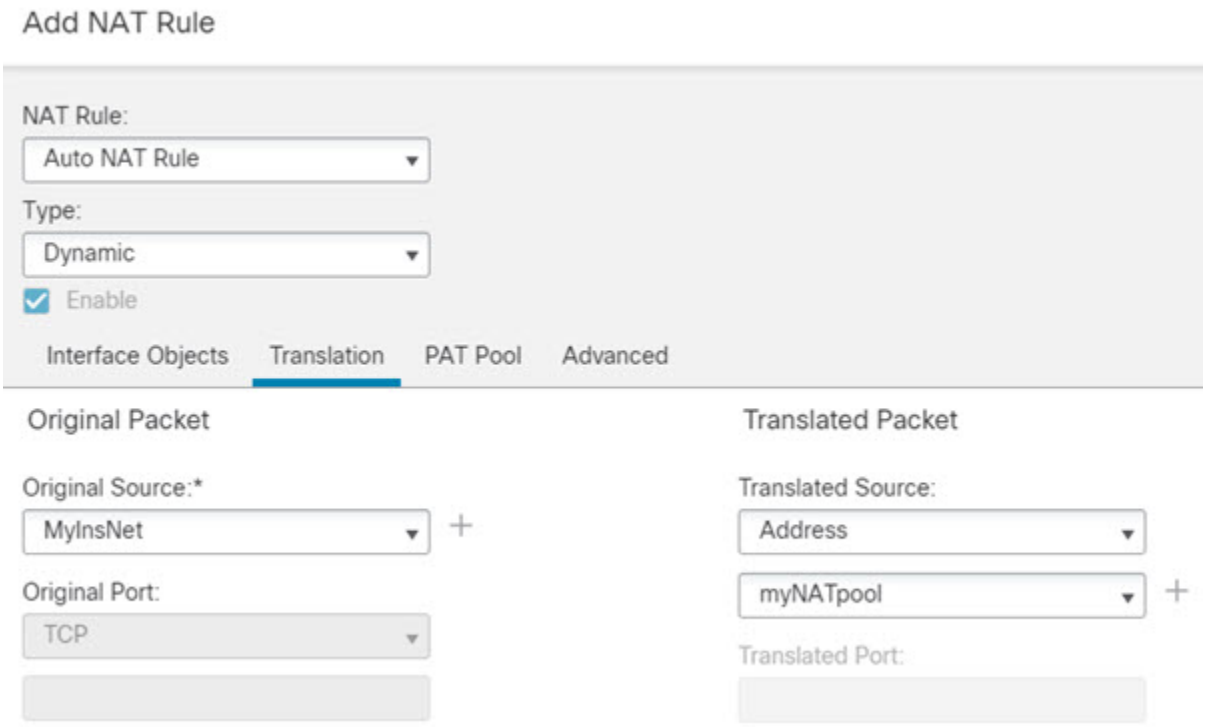
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myInsNet.
- **Adresse** > **source traduite** = groupe de réseaux myNAT Pool.




f) Cliquez sur **Save** (enregistrer).

**Étape 6** Configurez la NAT statique pour le serveur Web.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

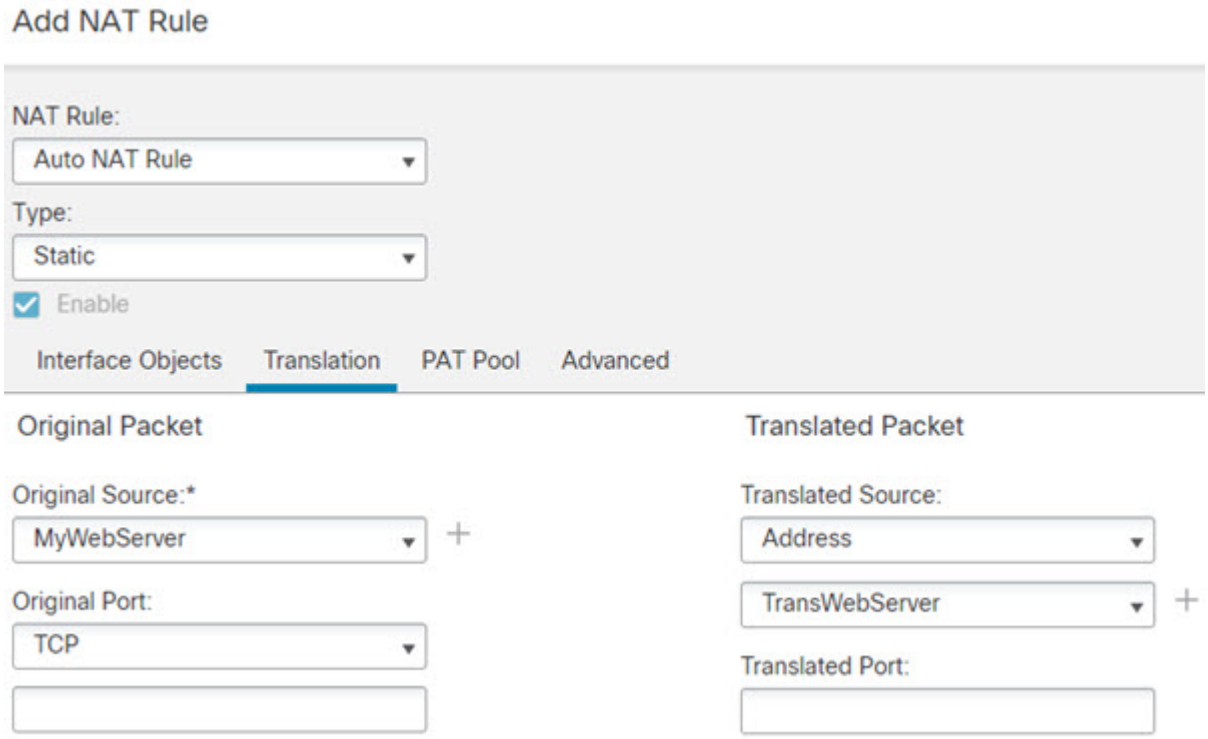
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myWebServer.
- **Adresse** > **source traduite**= objet réseau TransWebServer.



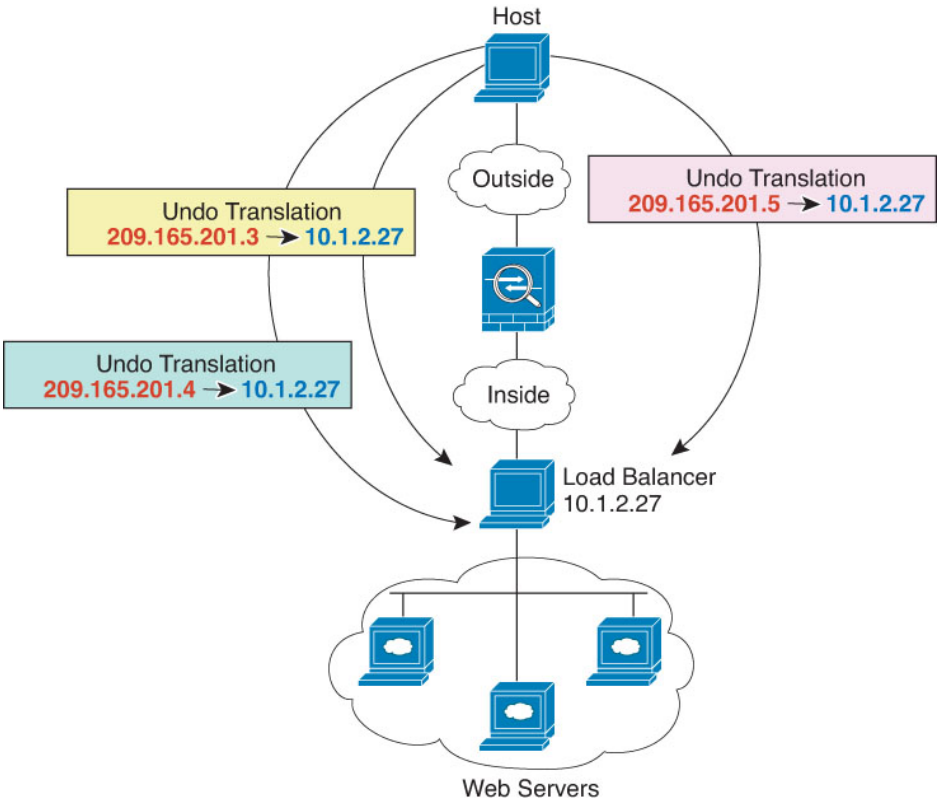

e) Cliquez sur **Save** (enregistrer).

**Étape 7** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# Équilibreur de charge interne avec plusieurs adresses mappées (NAT automatique statique, un vers 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 16 : NAT statique avec règle One-to-Many (un vers plusieurs) pour un équilibreur de charge interne*




### Avant de commencer

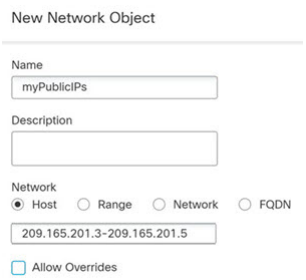
Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

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

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
c) Définissez les adresses.

Nommez l'objet réseau (par exemple, myPublicIPs) et saisissez la plage réseau 209.165.201.3 à 209.165.201.5.

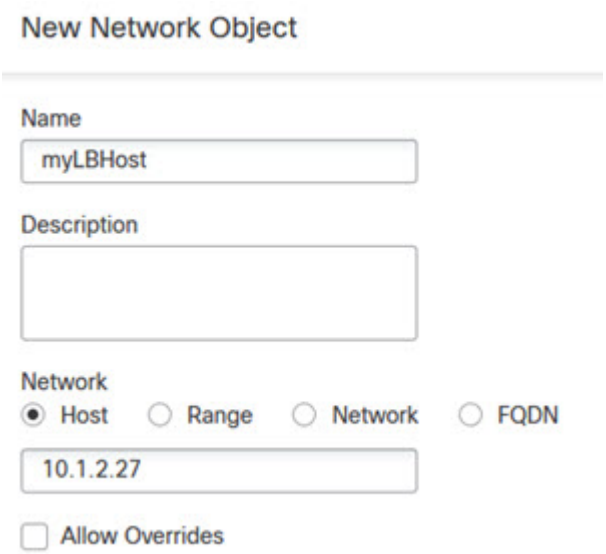



d) Cliquez sur **Save** (enregistrer).

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

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, myLBHost), saisissez l'adresse d'hôte 10.1.2.27.




c) Cliquez sur **Save** (enregistrer).

**Étape 3** Configurez la NAT statique pour l'équilibreur de charge.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

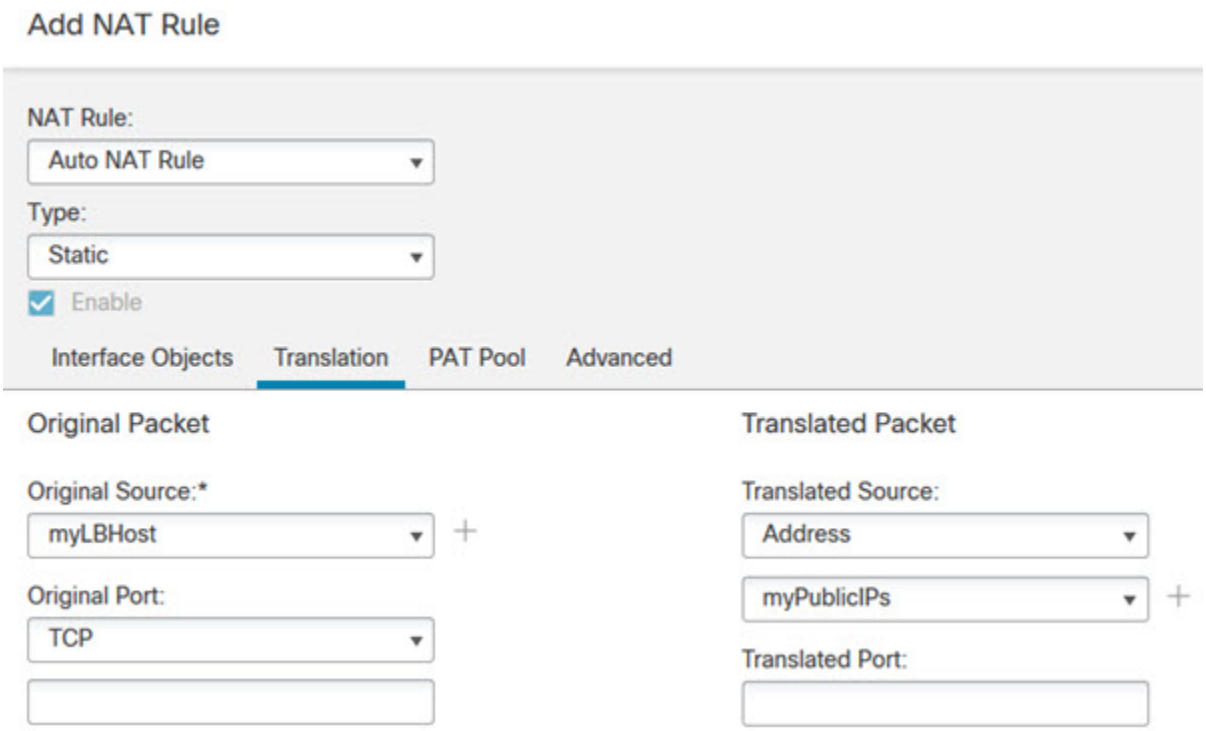
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myLB Host.
- **Adresse** > **source traduite** = groupe de réseaux myPublicIPs.



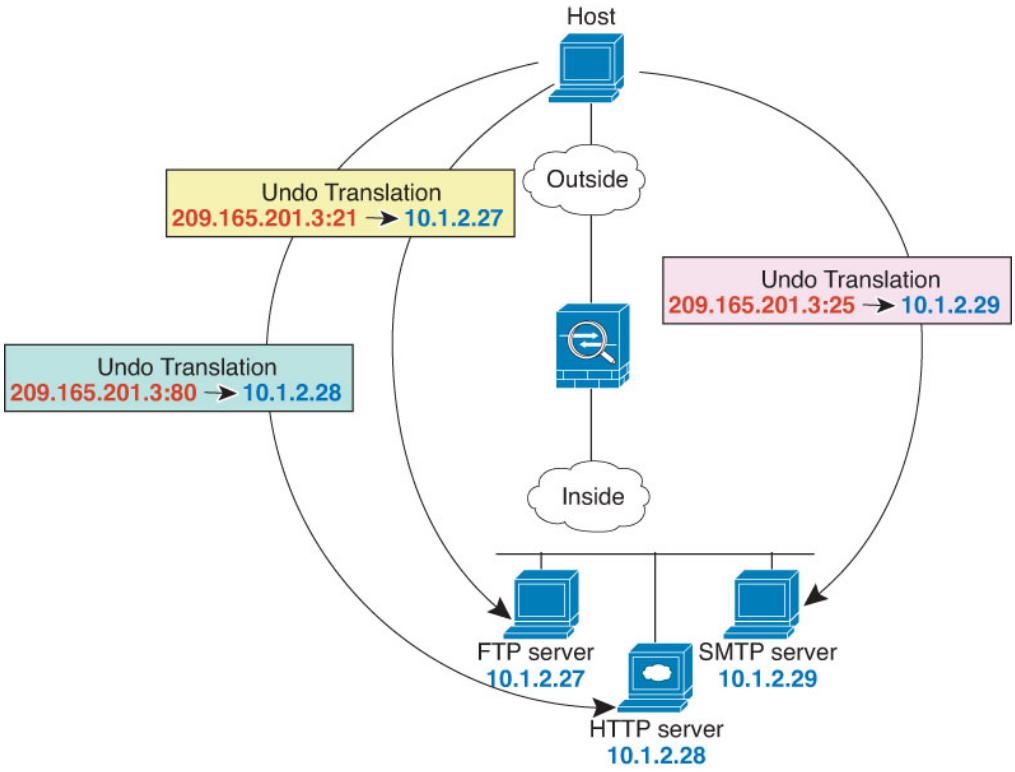

f) Cliquez sur **Save** (enregistrer).

**Étape 4** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# Adresse unique pour FTP, HTTP et SMTP (NAT automatique 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 17 : NAT statique avec traduction de port*



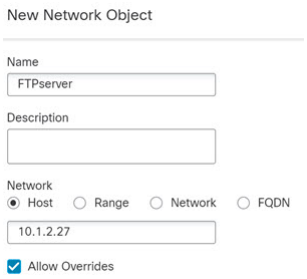

### Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

**Étape 1** Créez un objet réseau pour le serveur FTP.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
c) Nommez l'objet réseau (par exemple, FTPserver) et saisissez l'adresse IP réelle du serveur FTP, 10.1.2.27.

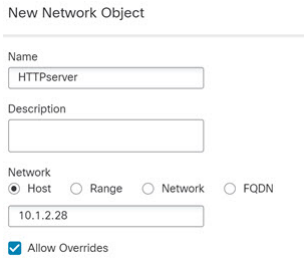



d) Cliquez sur **Save** (enregistrer).

**Étape 2** Créez un objet réseau pour le serveur HTTP.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, HTTPserver), saisissez l'adresse d'hôte 10.1.2.28.

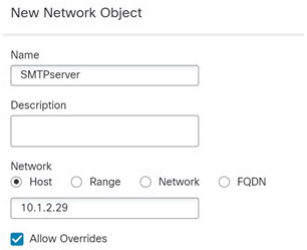



c) Cliquez sur **Save** (enregistrer).

**Étape 3** Créez un objet réseau pour le serveur SMTP.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, SMTPserver), saisissez l'adresse d'hôte 10.1.2.29.

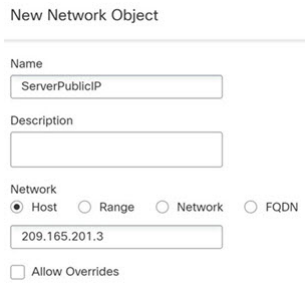



c) Cliquez sur **Save** (enregistrer).

**Étape 4** Créez un objet réseau pour l'adresse IP publique utilisée pour les trois serveurs.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, ServerPublicIP) et saisissez l'adresse d'hôte 209.165.201.3.




c) Cliquez sur **Save** (enregistrer).

**Étape 5** Configurez la NAT statique avec la traduction de port pour le serveur FTP, en mappant le port FTP sur lui-même.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

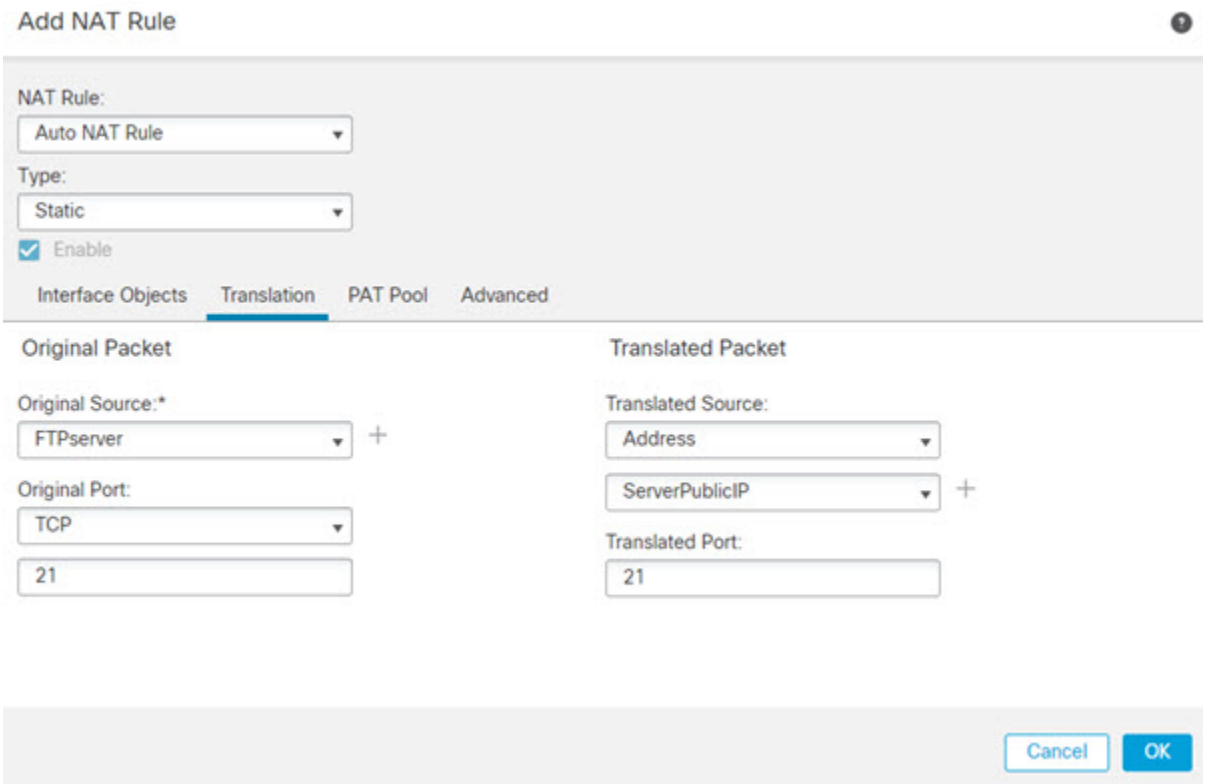
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur FTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 21.
- **Port traduit** = 21.




f) Cliquez sur **Save** (enregistrer).

**Étape 6** Configurez la NAT statique avec la traduction de port pour le serveur HTTP, en mappant le port HTTP sur lui-même.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

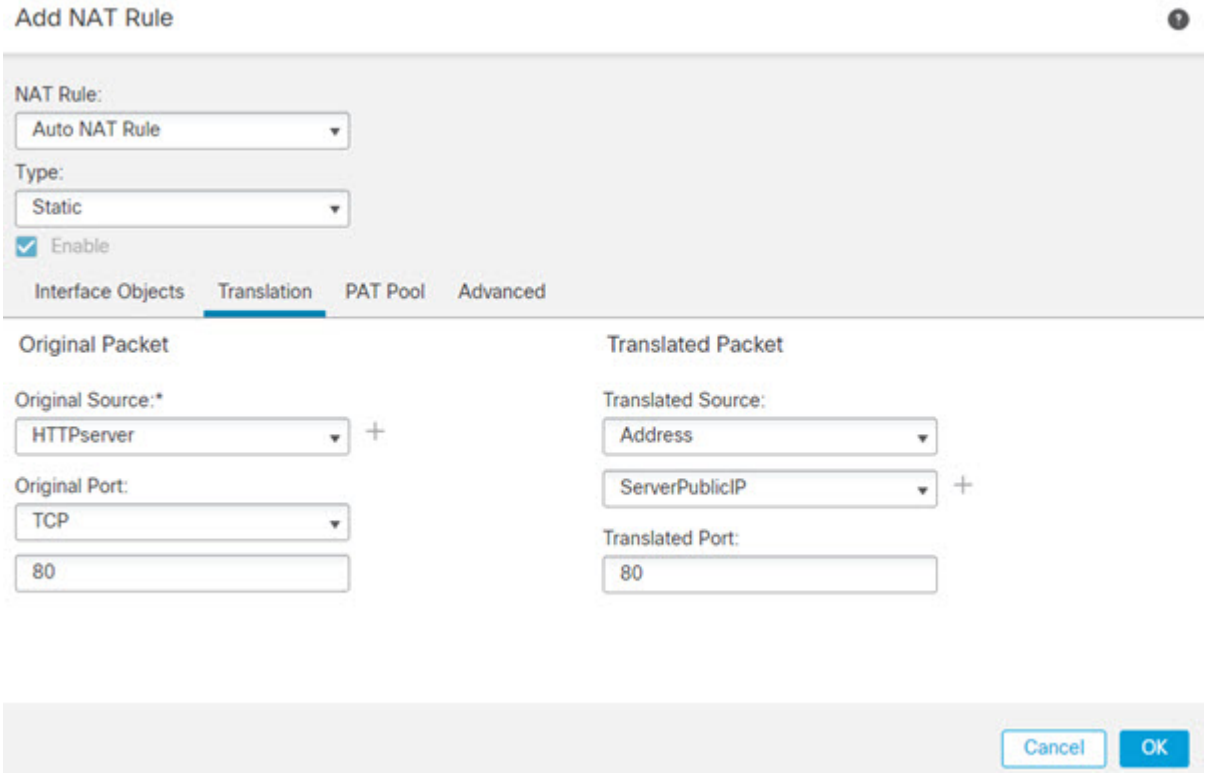
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur HTTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 80.
- **Port traduit** = 80.




e) Cliquez sur **Save** (enregistrer).

**Étape 7** Configurez la NAT statique avec la traduction de port pour le serveur SMTP, en mappant le port SMTP sur lui-même.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

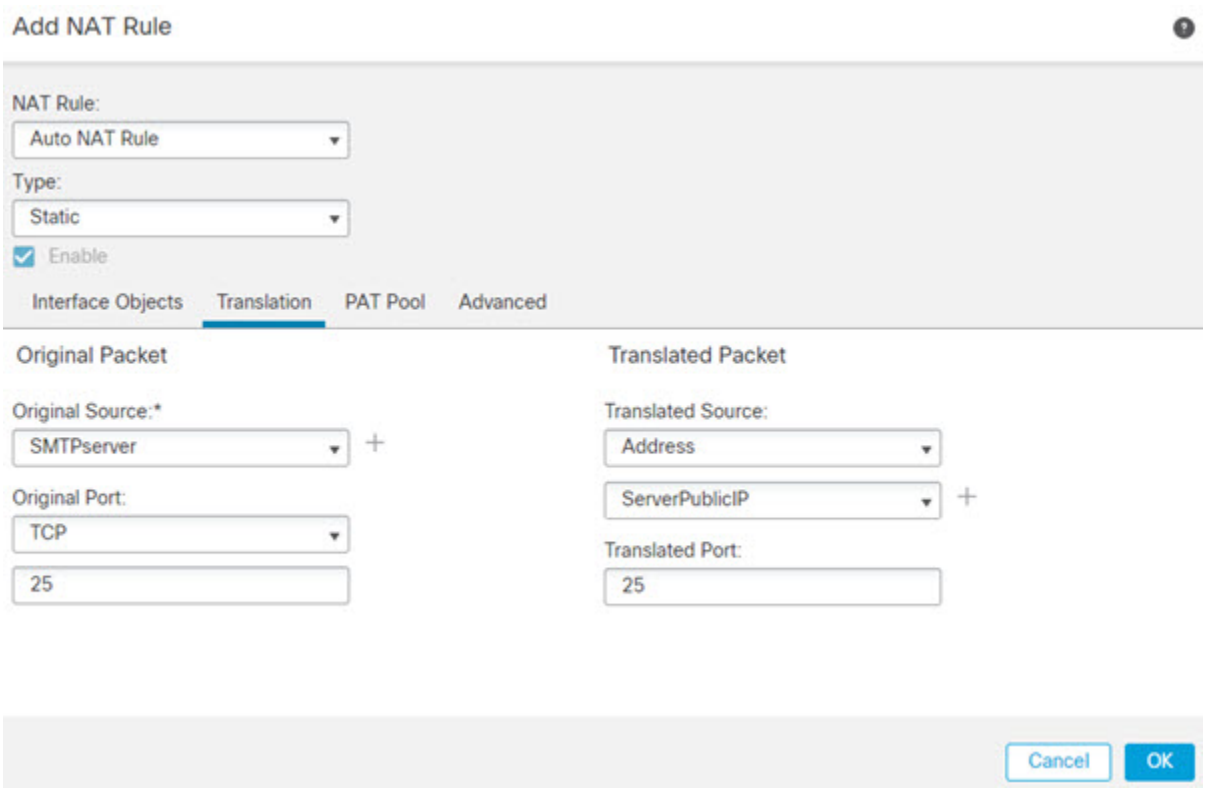
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur SMTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 25.
- **Port traduit** = 25.



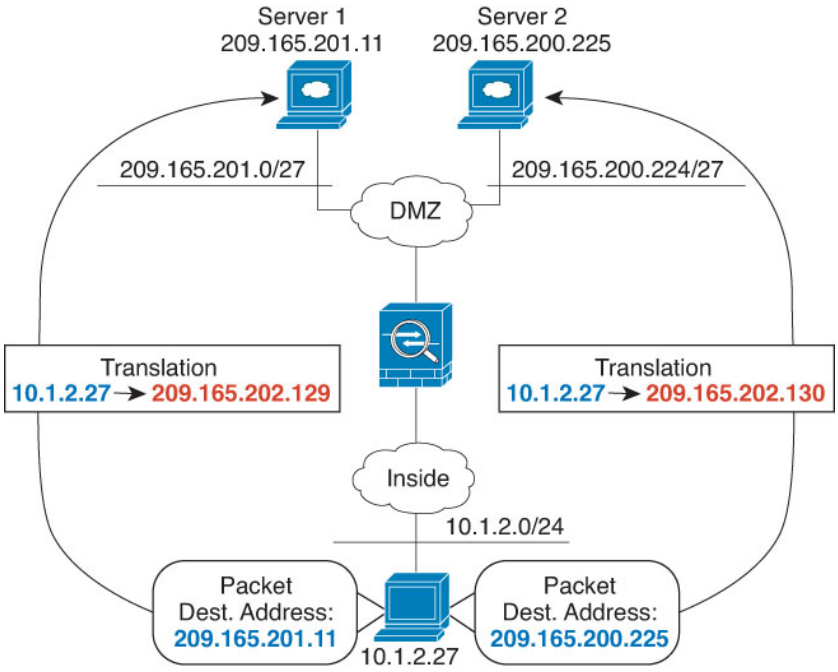

e) Cliquez sur **Save** (enregistrer).

**Étape 8** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# 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 18 : NAT manuelle avec différentes adresses de destination*




### Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **interne** et **dmz**. Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

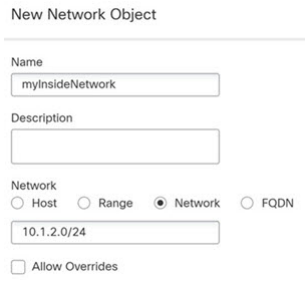
### Procédure

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

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Nommez l'objet réseau (par exemple, myInsideNetwork) et saisissez l'adresse réseau réelle, soit 10.1.2.0/24.




d) Cliquez sur **Save** (enregistrer).

**Étape 2** Créer un objet réseau pour le réseau DMZ 1.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

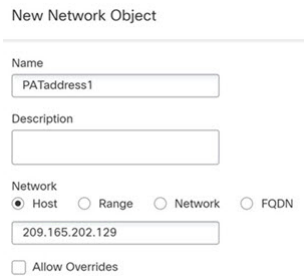
b) Nommez l'objet réseau (par exemple, DMZnetwork1) et saisissez l'adresse réseau 209.165.201.0/27 (masque de sous-réseau 255.255.255.224).


c) Cliquez sur **Save** (enregistrer).

**Étape 3** Créez un objet réseau pour l'adresse PAT du réseau DMZ 1.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress1) et saisissez l'adresse d'hôte 209.165.202.129.

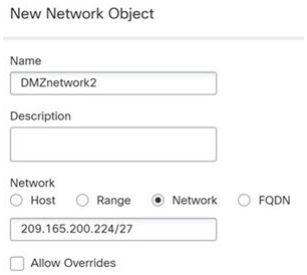



c) Cliquez sur **Save** (enregistrer).

**Étape 4** Créez un objet réseau pour le réseau DMZ 2.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, DMZnetwork2) et saisissez l'adresse réseau 209.165.200.224/27 (masque de sous-réseau 255.255.255.224).



c) Cliquez sur **Save** (enregistrer).

**Étape 5** Créez un objet réseau pour l'adresse PAT du réseau DMZ 2.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress2) et saisissez l'adresse d'hôte 209.165.202.130.


c) Cliquez sur **Save** (enregistrer).

**Étape 6** Configurez la PAT manuelle dynamique pour le réseau DMZ 1.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

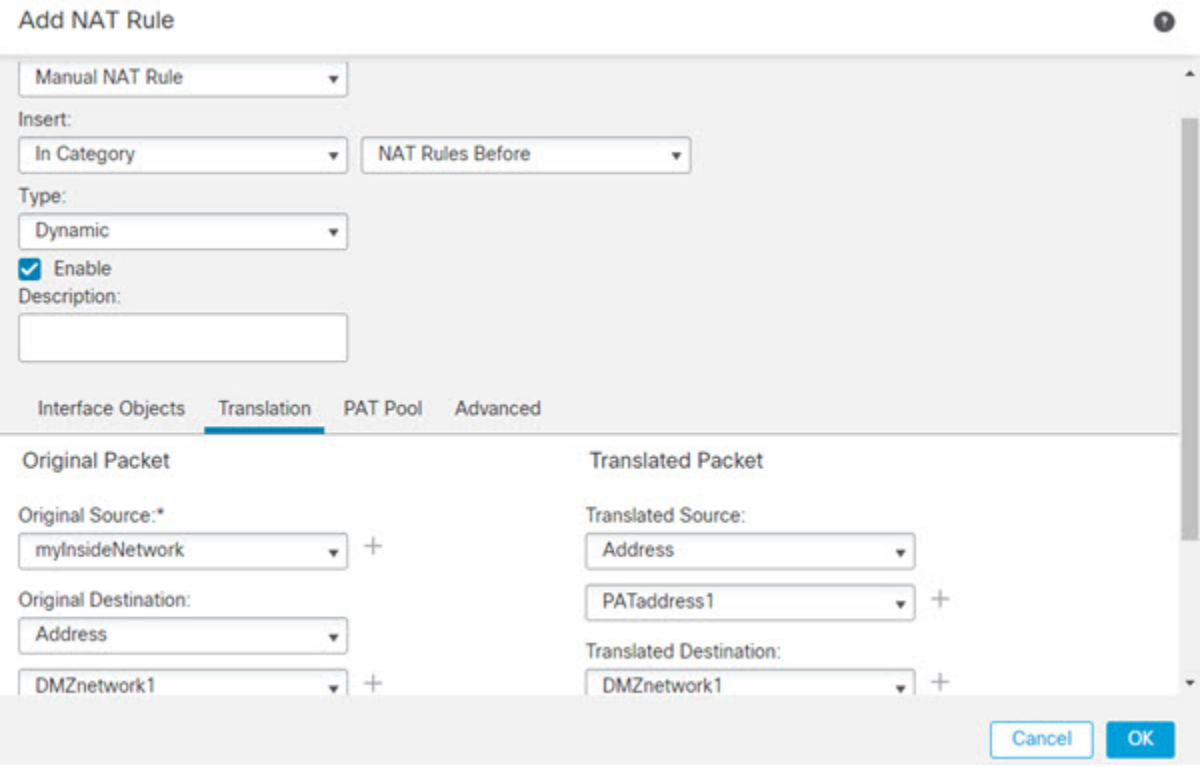
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress1.
- **Adresse** > **destination d'origine** = objet réseau DMZnetwork1.
- **Destination traduite** = objet réseau DMZnetwork1.

**Remarque** 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. Laissez tous les champs de port vides.




f) Cliquez sur **Save** (enregistrer).

**Étape 7** Configurez la PAT manuelle dynamique pour le réseau DMZ 2.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

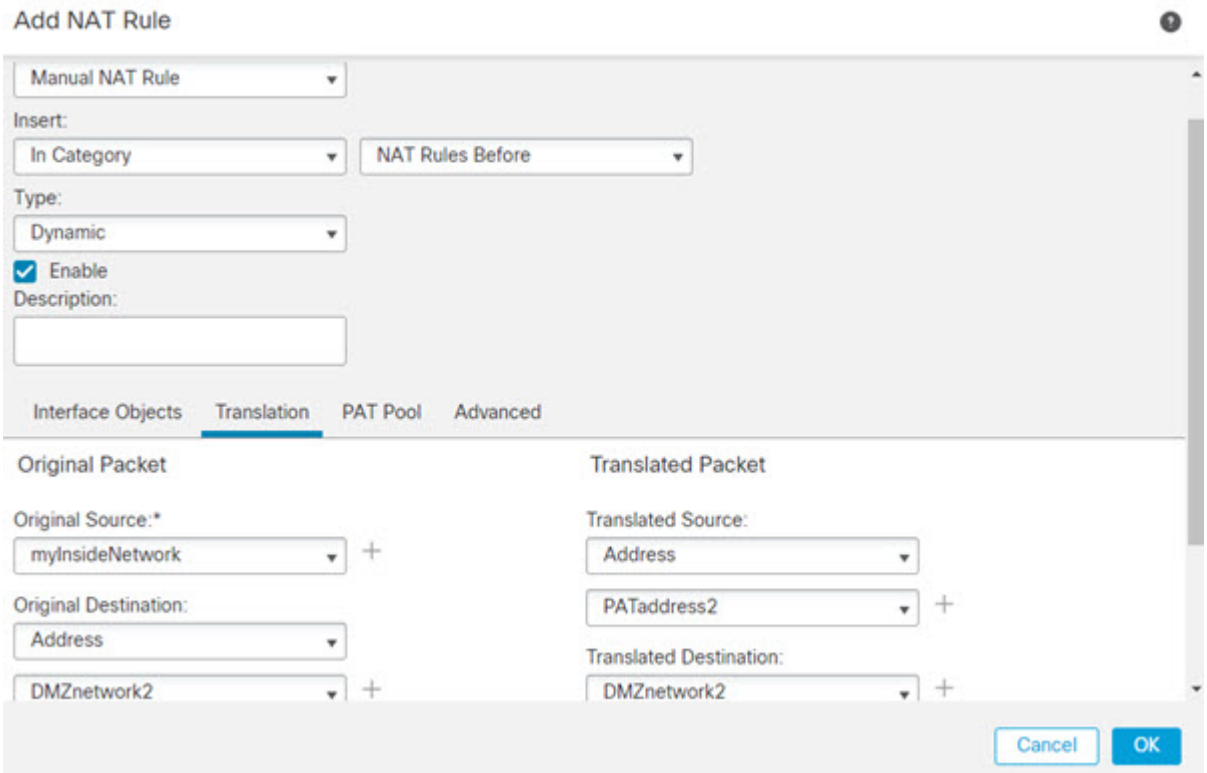
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress2.
- **Adresse** > **destination d'origine** = objet réseau DMZnetwork2.
- **Destination traduite** = objet réseau DMZnetwork2.



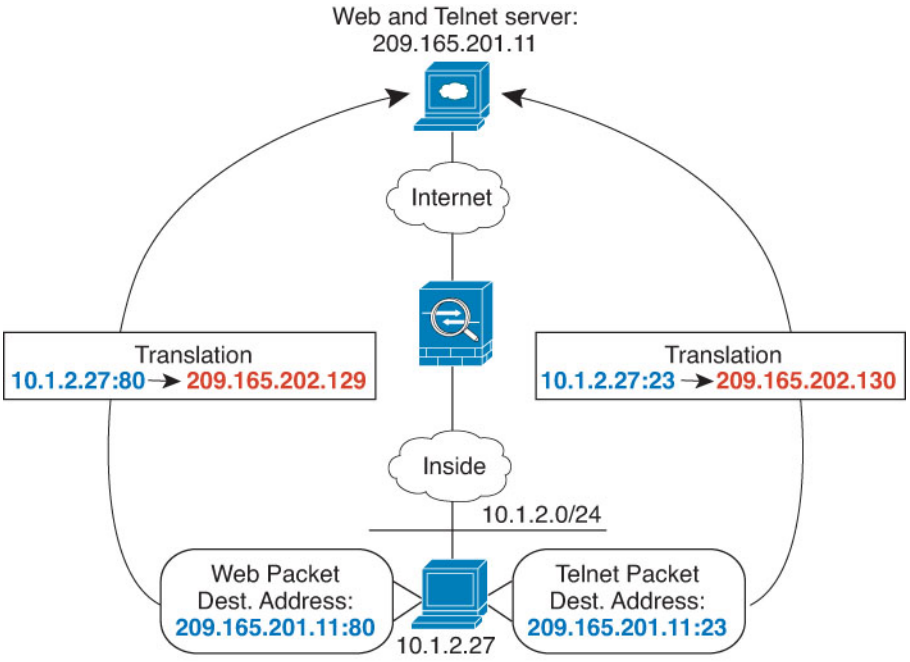

e) Cliquez sur **Save** (enregistrer).

**Étape 8** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# Traduction différente selon l'adresse et le port de destination (PAT manuelle 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 19 : NAT manuelle avec différents ports de destination*




### Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **interne** et **dmz**. Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

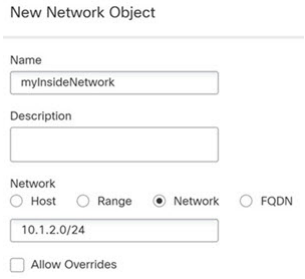
### Procédure

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

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Nommez l'objet réseau (par exemple, myInsideNetwork) et saisissez l'adresse réelle du réseau, soit 10.1.2.0/24.




d) Cliquez sur **Save** (enregistrer).

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

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

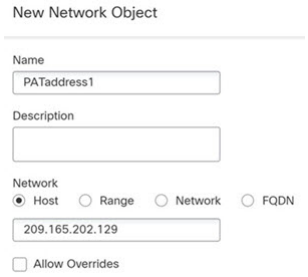
b) Nommez l'objet réseau (par exemple, TelnetWebServer) et saisissez l'adresse d'hôte 209.165.201.11.


c) Cliquez sur **Save** (enregistrer).

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

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress1) et saisissez l'adresse d'hôte 209.165.202.129.




c) Cliquez sur **Save** (enregistrer).

**Étape 4** Créez un objet réseau pour l'adresse PAT lorsque vous utilisez HTTP.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress2) et saisissez l'adresse d'hôte 209.165.202.130.


c) Cliquez sur **Save** (enregistrer).

**Étape 5** Configurez la PAT manuelle dynamique pour l'accès Telnet.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

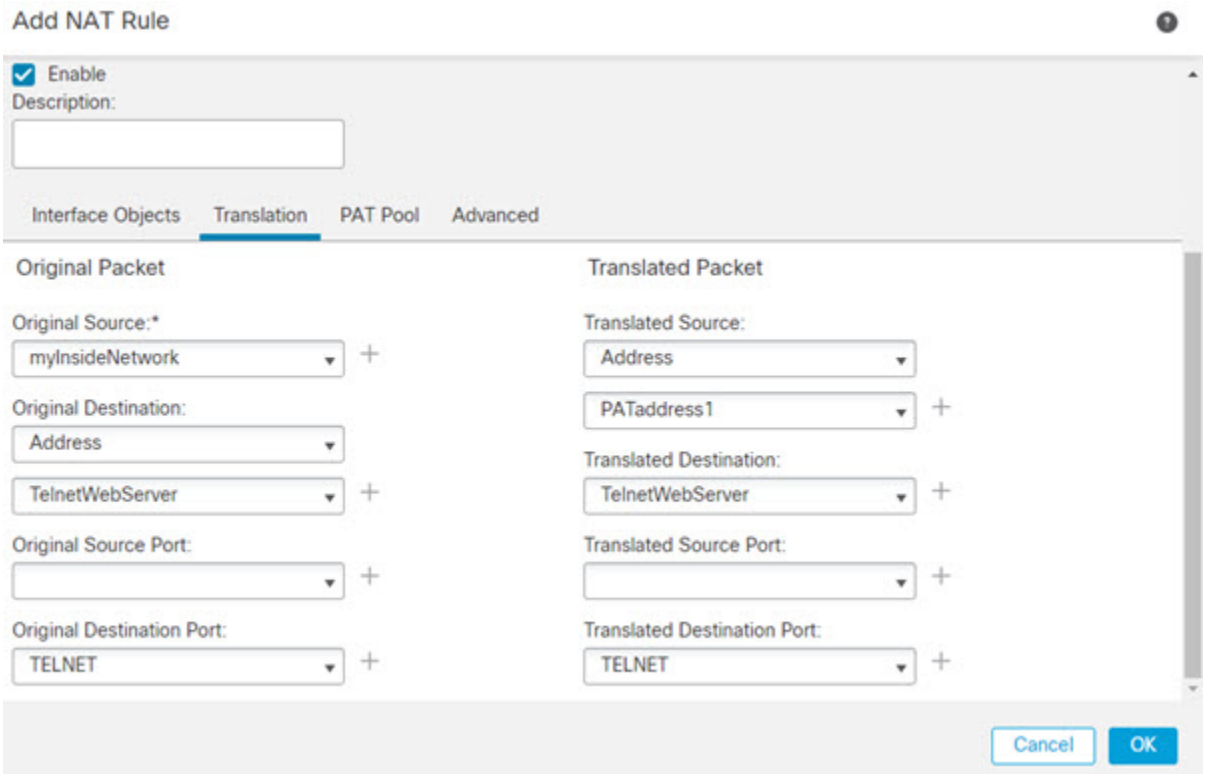
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress1.
- **Adresse** > **destination d'origine** = objet réseau TelnetWebServer.
- **Destination traduite** = objet réseau TelnetWebServer.
- **Port de destination d'origine** = objet de port TELNET (défini par le système).
- **Port de destination traduit** = objet de port TELNET (défini par le système).

**Remarque** Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour cette adresse en spécifiant la même adresse pour les adresses de destination d'origine et traduites, et le même port pour le port d'origine et traduit.




f) Cliquez sur **Save** (enregistrer).

**Étape 6** Configurez la PAT manuelle dynamique pour l'accès Web.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

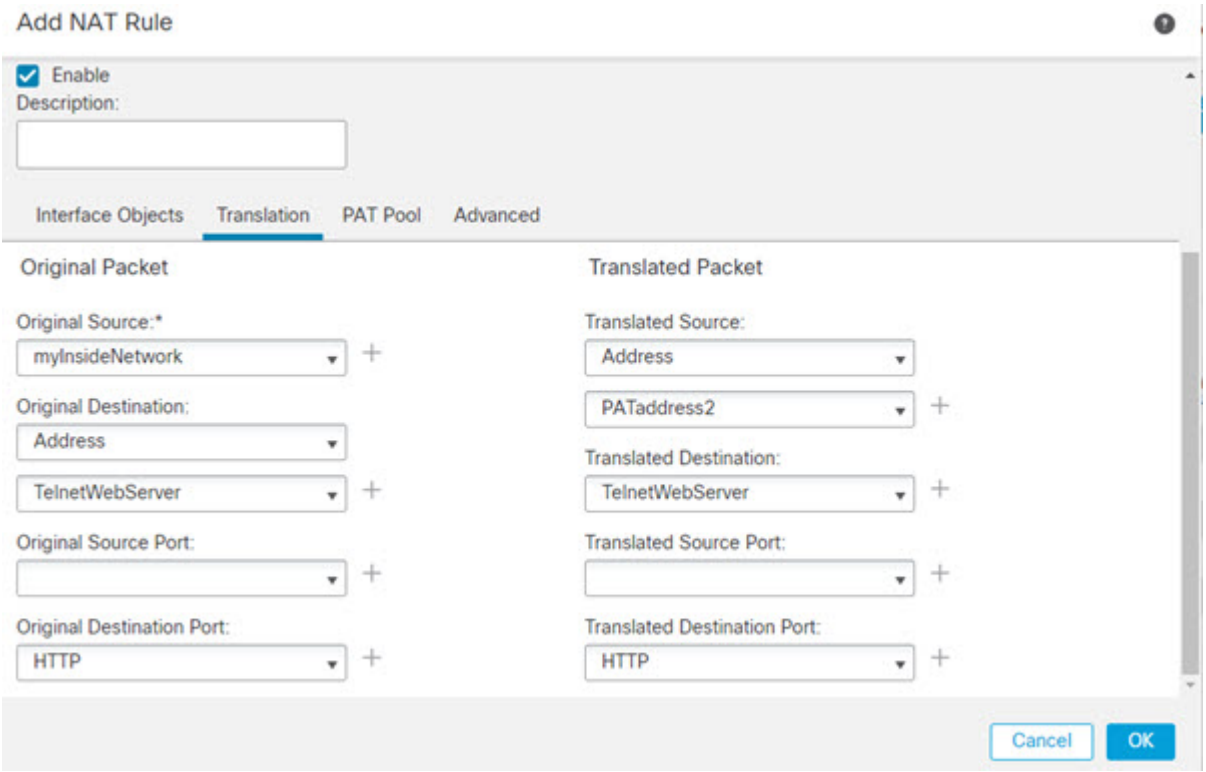
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress2.
- **Adresse** > **destination d'origine** = objet réseau TelnetWebServer.
- **Destination traduite** = objet réseau TelnetWebServer.
- **Port de destination d'origine** = objet de port HTTP (défini par le système).
- **Port de destination traduit** = objet de port HTTP (défini par le système).



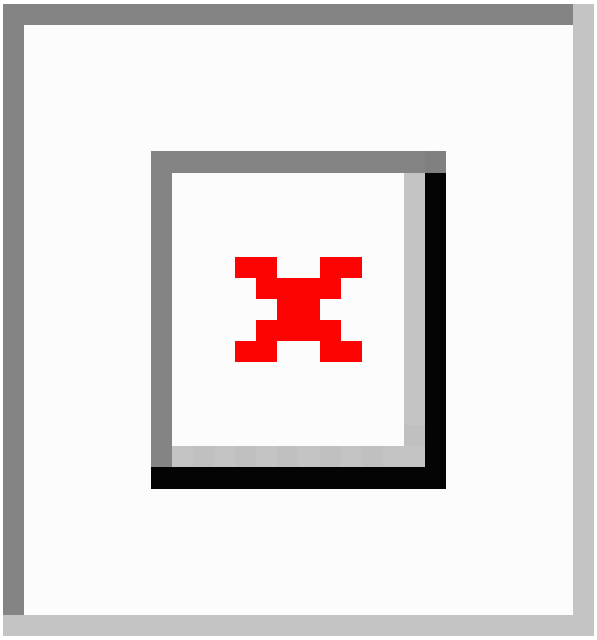

e) Cliquez sur **Save** (enregistrer).

**Étape 7** Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

# 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 20 : PAT d'interface et NAT d'identité pour le VPN de site à site***



L'exemple suivant explique la configuration de Firewall1 (Boulder).

### Avant de commencer

Assurez-vous de disposer d'objets d'interface (zones de sécurité ou groupes d'interfaces) qui contiennent les interfaces des périphériques dans le VPN. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **inside-boulder** et **outside-boulder** pour les interfaces Firewall1 (Boulder). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)** , puis sélectionnez **Interfaces**.

### Procédure

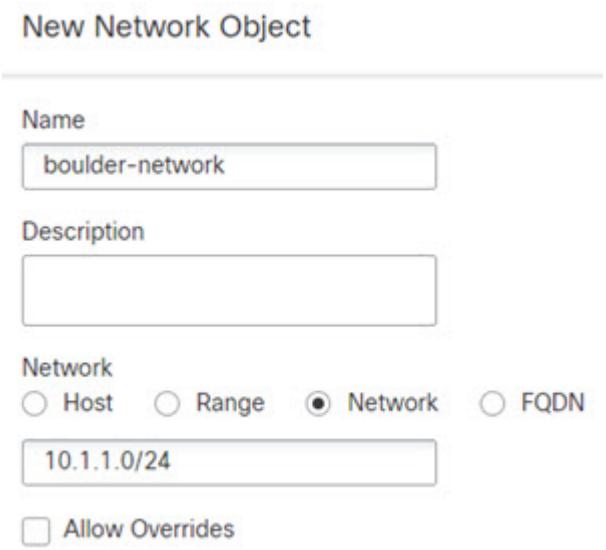
**Étape 1** Créez les objets pour définir les différents réseaux.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Repérez le réseau interne Boulder.

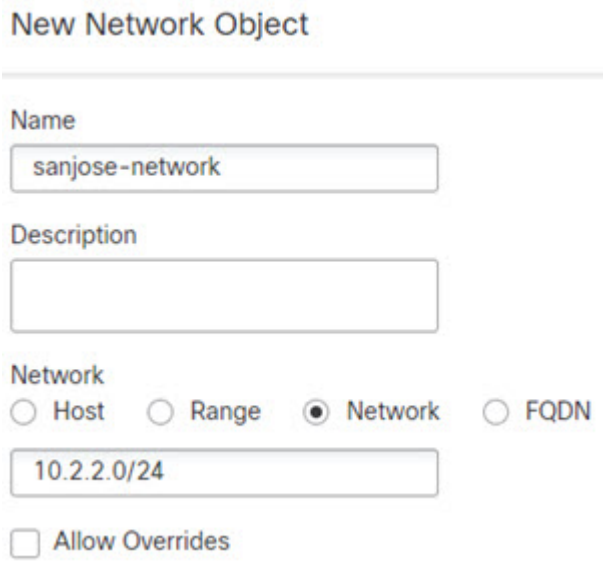
Nommez l'objet réseau (par exemple, boulder-network) et saisissez l'adresse réseau, 10.1.1.0/24.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau San Jose interne.

Nommez l'objet réseau (par exemple, sanjose-network) et saisissez l'adresse réseau 10.2.2.0/24.

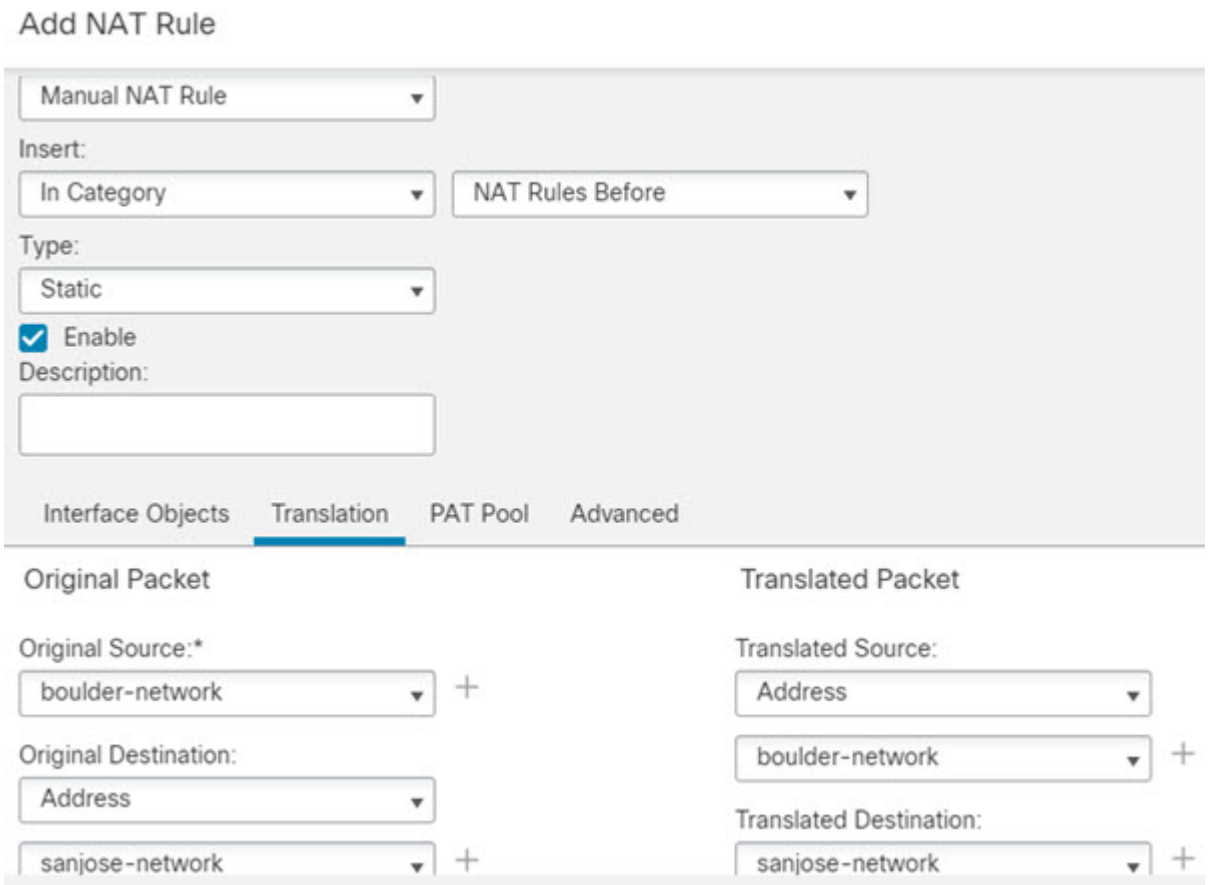



f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurer la NAT d'identité manuelle pour le réseau Boulder lorsqu'il passe par le VPN vers San Jose sur le Firewall1 (Boulder).

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :
   - **Règle NAT** = Règle NAT manuelle.
   - **Type** = Statique.
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :
   - **Source Interface Objects** (Objets de l'interface source) = inside-boulder.
   - **Destination Interface Objects** (Objets de l'interface de destination) = outside-boulder.
e) Pour **Translation** (traduction), configurez les options suivantes :
   - **Original Source** (Source d'origine) = objet boulder-network.
   - **Translated Source** > **Address** (adresse traduite de la source) = boulder-network object.
   - **Original Destination** > **Address** (adresse de destination d'origine) = sanjose-network object.
   - **Translated Destination** (destination traduite) = sanjose-network object.

   **Remarque** 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. Laissez tous les champs de port vides. Cette règle configure la NAT d'identité pour la source et la destination.
f) Pour **Advanced** (avancé), sélectionnez **Do not proxy ARP on Destination interface** (Ne pas utiliser le mandataire ARP sur l'interface de destination).




g) Cliquez sur **Save** (enregistrer).

**Étape 3** Configurez manuellement l'interface dynamique PAT lors de la connexion à Internet pour le réseau interne Boulder sur Firewall1 (Boulder).

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

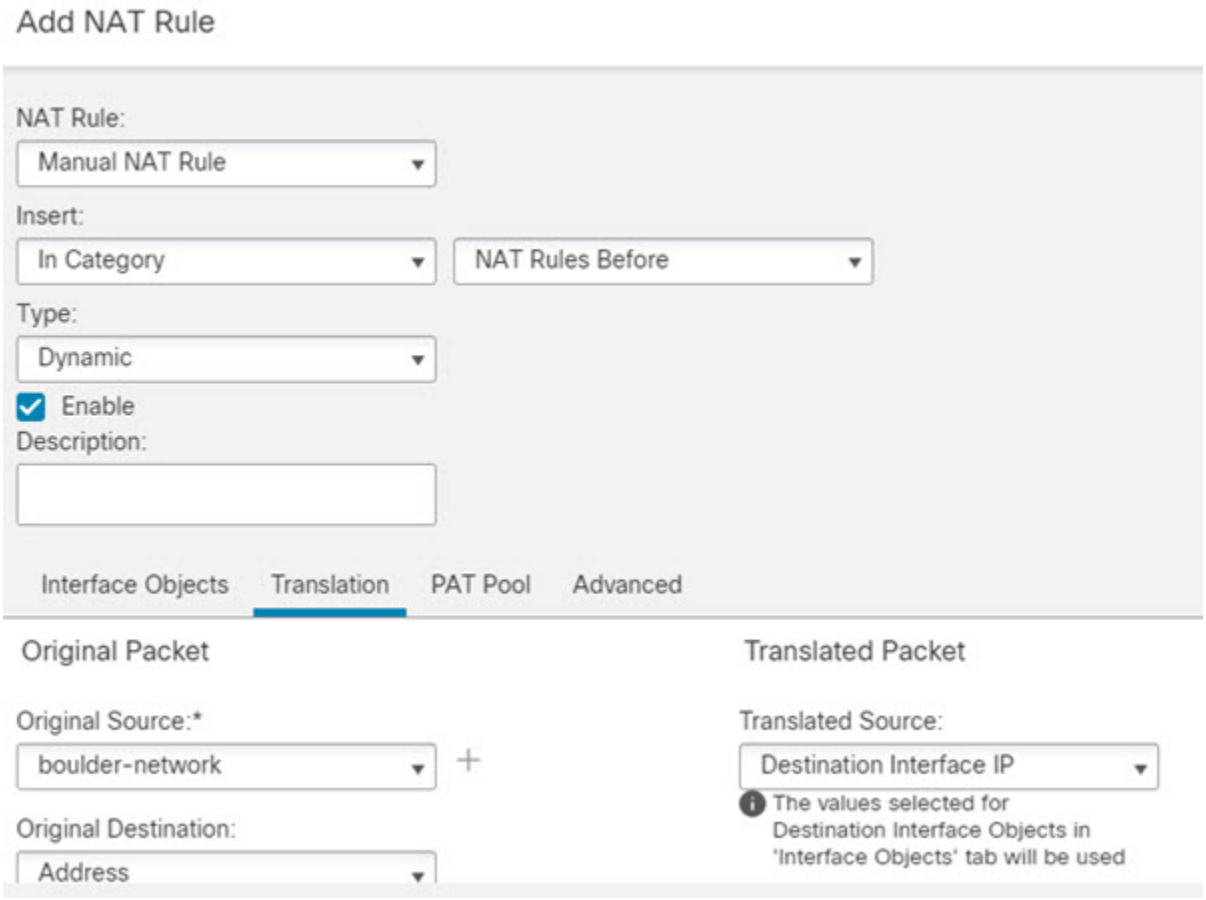
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.
- **Insert Rule** (Insérer une règle) = n'importe quelle position après la première règle Étant donné que cette règle s'applique à toute adresse de destination, la règle qui utilise sanjose-network comme destination doit précéder cette règle, sinon la règle sanjose-network ne sera jamais mise en correspondance. La procédure par défaut est de placer les nouvelles règles NAT manuelles à la fin de la section « NAT Rules Before Auto NAT ».

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** (Objets de l'interface source) = inside-boulder.
- **Destination Interface Objects** (Objets de l'interface de destination) = outside-boulder.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) = objet boulder-network.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**). Cette option configure l'interface PAT à l'aide de l'interface contenue dans l'objet d'interface de destination.
- **Original Destination** > **Address** (adresse de destination d'origine) = n'importe laquelle (laissez vide).
- **Translated Destination** (Destination traduite) = n'importe laquelle (laissez vide).




e) Cliquez sur **Save** (enregistrer).

**Étape 4** Si vous gérez également Firewall2 (San Jose), vous pouvez configurer des règles similaires pour ce périphérique.

- La règle de la NAT d'identité manuelle serait pour sanjose-network lorsque la destination est boulder-network. Créez de nouveaux objets d'interface pour Firewall2 , à l'intérieur et à l'extérieur des réseaux.
- La règle PAT de l'interface dynamique manuelle serait pour sanjose-network lorsque la destination est « any » (Toute).

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

Vous devrez peut-être configurer l'appareil de défense contre les menaces  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 :

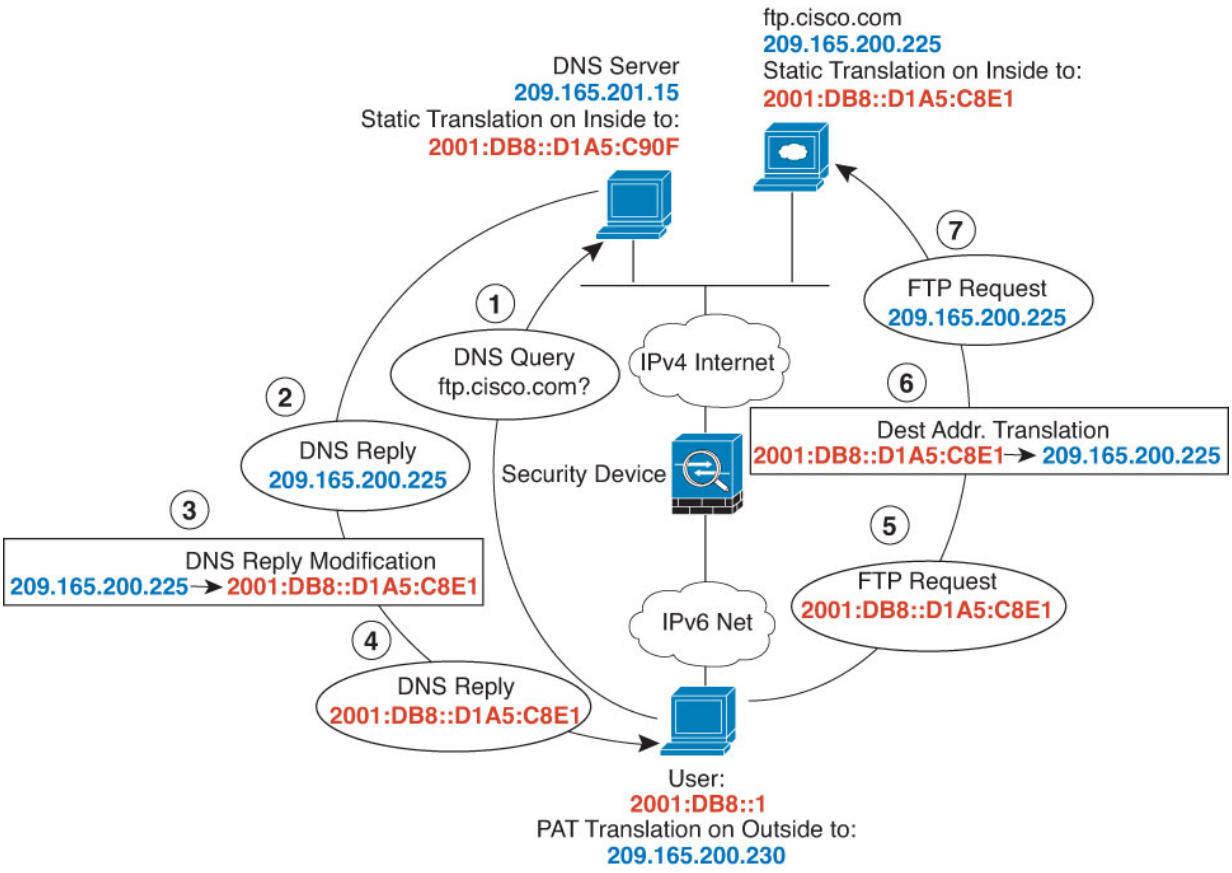
- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle manual NAT (NAT manuelle), vous ne pouvez pas configurer la modification DNS si vous spécifiez l'adresse 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 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.




### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

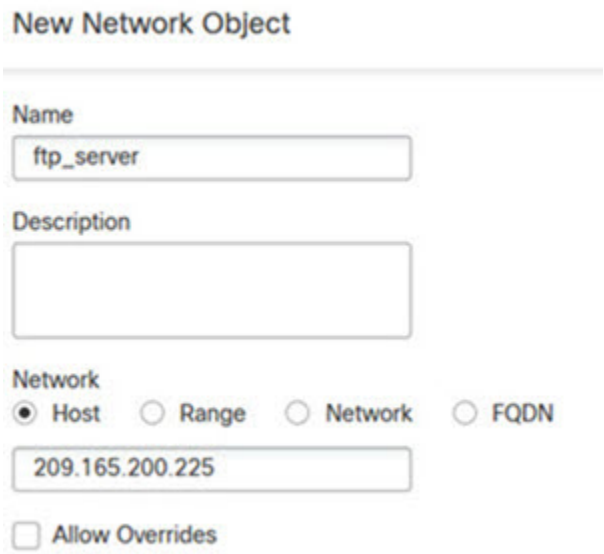
**Étape 1** Créez les objets réseau pour le serveur FTP, le serveur DNS, le réseau interne et l'ensemble PAT.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

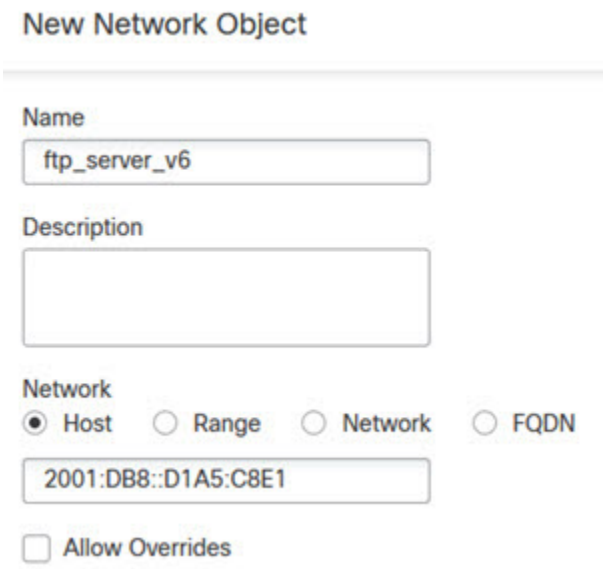
Nommez l'objet réseau (par exemple, ftp_server) et saisissez l'adresse de l'hôte, 209.165.200.225.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un objet réseau) et définissez l'adresse IPv6 traduite du serveur FTP.

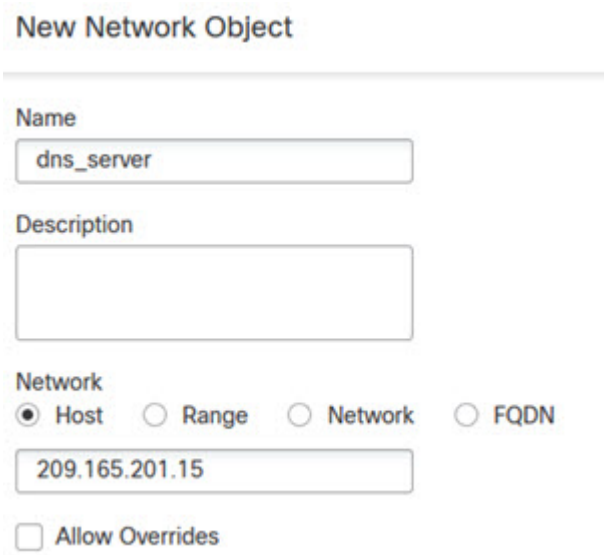
Nommez l'objet réseau (par exemple, ftp_server_v6) et saisissez l'adresse de l'hôte, 2001:DB8::D1A5:C8E1.




f) Cliquez sur **Save** (enregistrer).

g) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse réelle du serveur DNS.

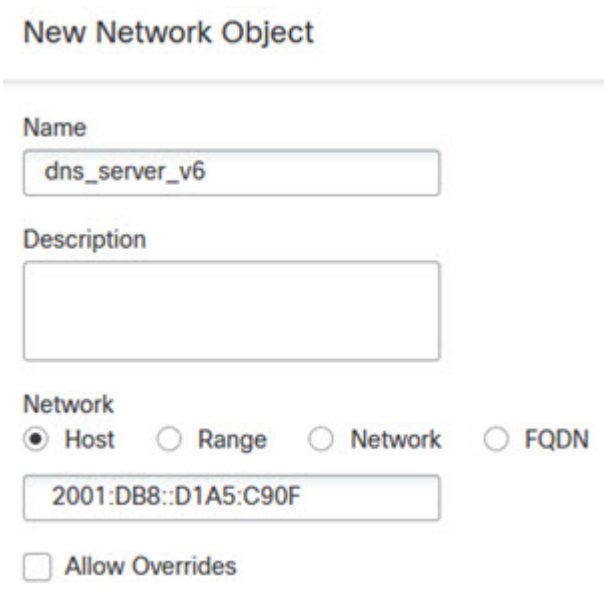
Nommez l'objet réseau (par exemple, dns_server) et saisissez l'adresse de l'hôte, 209.165.201.15.




h) Cliquez sur **Save** (enregistrer).

i) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse IPv6 traduite du serveur DNS.

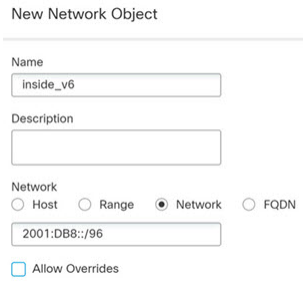
Nommez l'objet réseau (par exemple, dns_server_v6) et saisissez l'adresse de l'hôte, 2001:DB8::D1A5:C90F (où D1A5:C90F est l'équivalent IPv6 de 209.165.201.15).




j) Cliquez sur **Save** (enregistrer).

k) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau IPv6 interne.

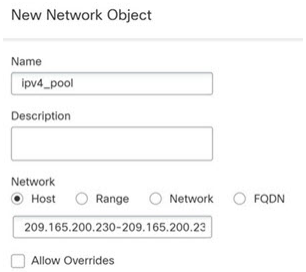
Nommez l'objet réseau (par exemple, inside_v6) et saisissez l'adresse réseau, 2001:DB8::/96.




l) Cliquez sur **Save** (enregistrer).

m) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez l'ensemble PAT IPv4 pour le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, ipv4_ pool) et saisissez la plage 209.165.200.230 à 209.165.200.238.




n) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

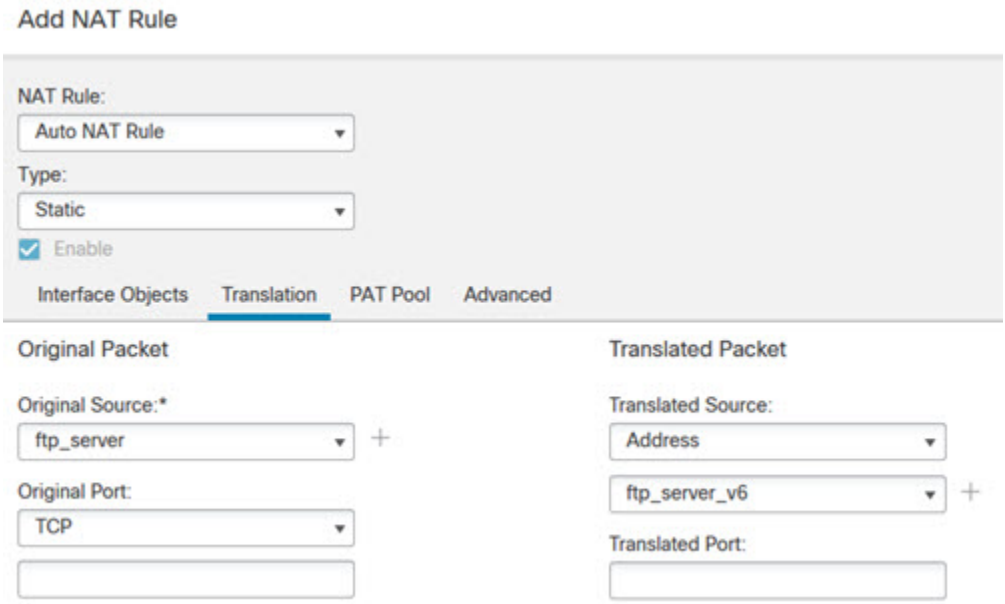
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau ftp_server.
- **Adresse** > **source traduite** = objet de réseau ftp_server_v6.




f) Dans **Avancé**, sélectionnez les options suivantes :

- **Traduire les réponses DNS correspondant à cette règle**
- **Net to Net Mapping** (Mappage net à net), car il s'agit d'une traduction NAT46 un à un.

g) Cliquez sur **OK**.

**Étape 3** Configurez la règle NAT statique pour le serveur DNS.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

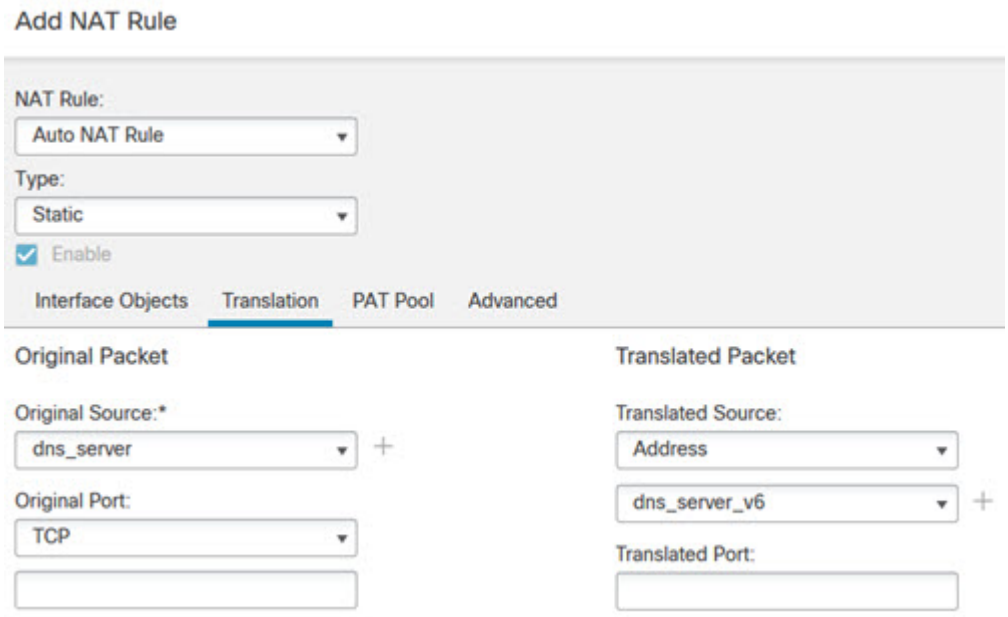
c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau dns_server.
- **Adresse** > **source traduite** = objet de réseau dns_server_v6

e) Dans **Avancé**, sélectionnez **Net to Net Mapping** (Mappage net à net), car il s'agit d'une traduction NAT46 un à un.




f) Cliquez sur **OK**.

**Étape 4** Configurez la NAT dynamique avec une règle d'ensemble PAT pour le réseau IPv6 interne.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

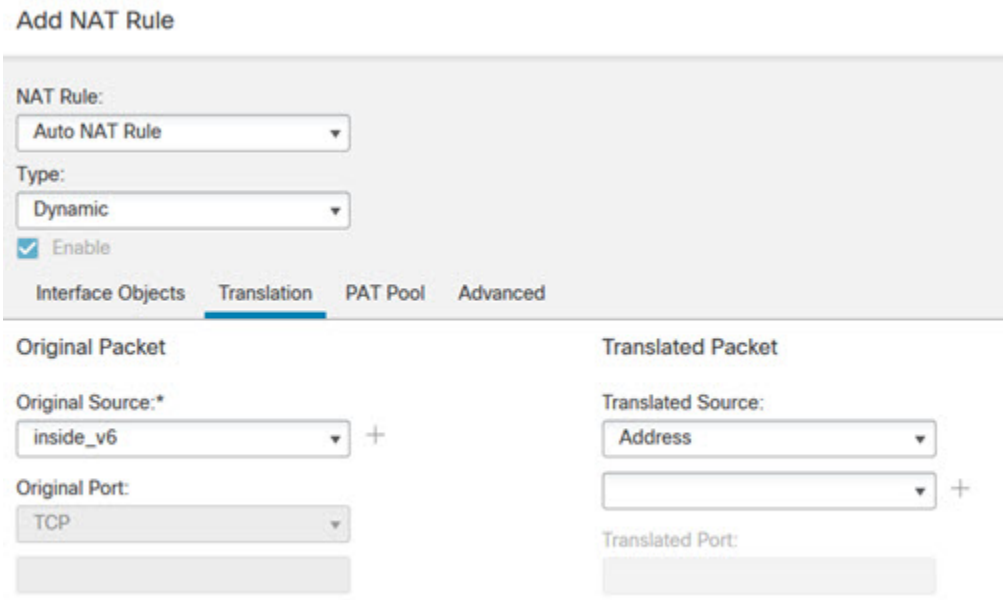
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

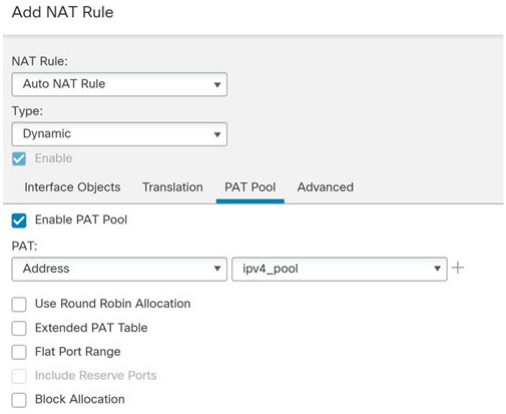
d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Adresse** > **source traduite** = laissez ce champ vide.




e) Dans **PAT Pool** (Bassin PAT), configurez les éléments suivants :

- **Enable PAT Pool** (activer l'ensemble PAT) = sélectionner cette option.
- **Adresse** > **source traduite** = objet réseau ipv4_ pool



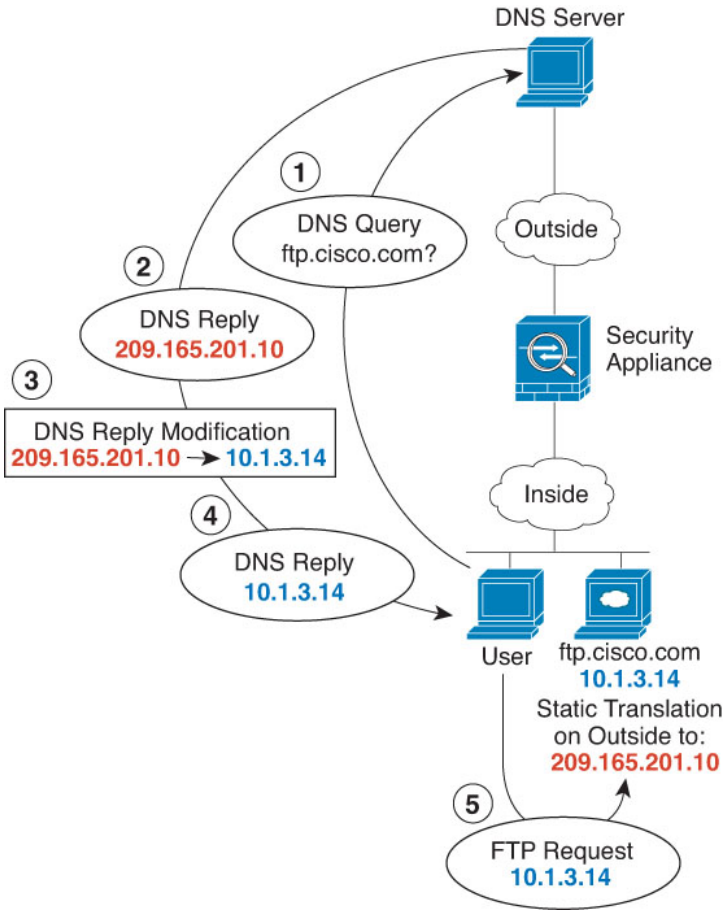

f) Cliquez sur **OK**.

## 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.




### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

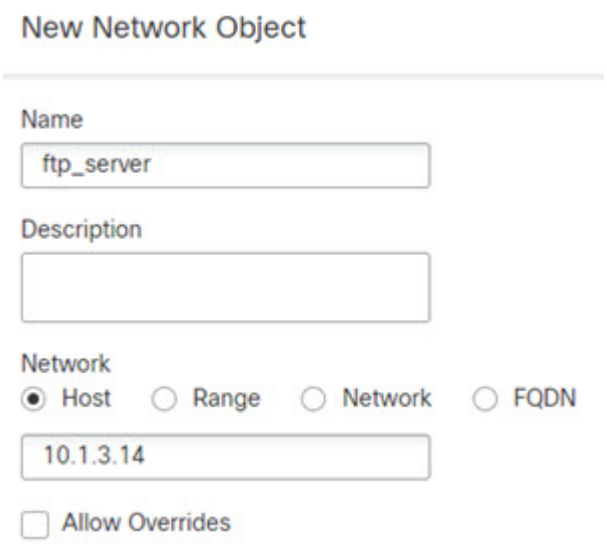
**Étape 1** Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

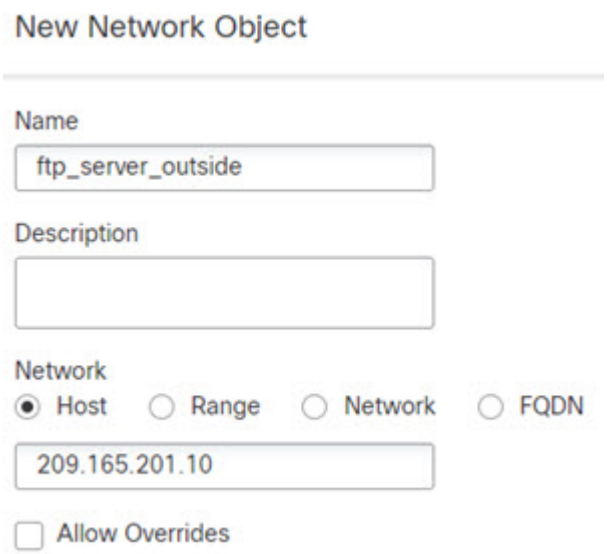
Nommez l'objet réseau (par exemple, ftp_server) et saisissez l'adresse de l'hôte, 10.1.3.14.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse traduite du serveur FTP.

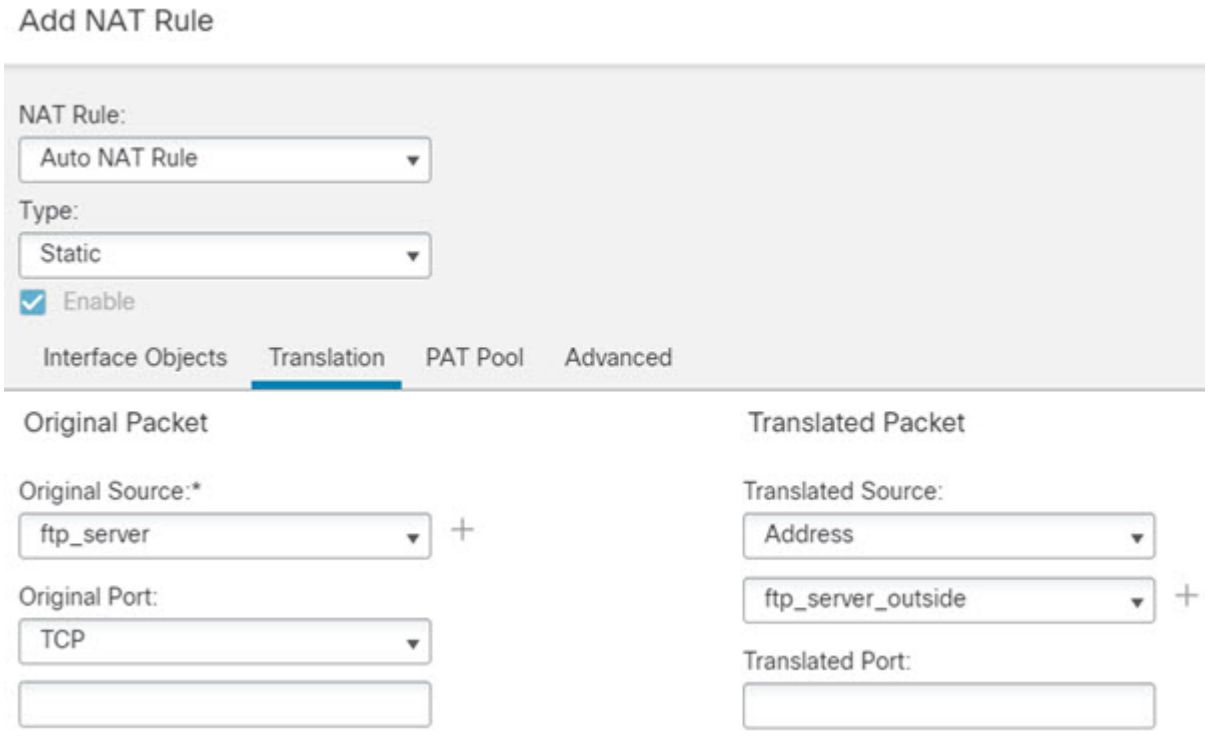
Nommez l'objet réseau (par exemple, ftp_server_outside) et saisissez l'adresse de l'hôte, 209.165.201.10.




f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

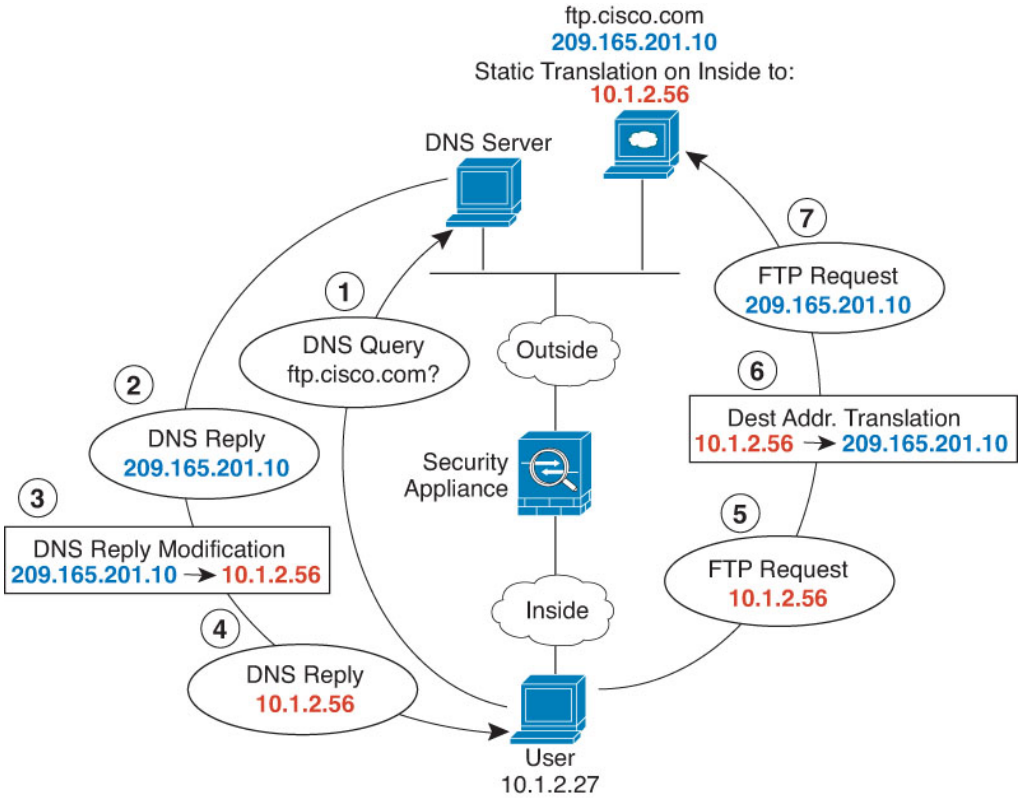
a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :
   - **NAT Rule** = Auto NAT Rule.
   - **Type** = Statique.
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :
   - **Source Interface Objects** = inside.
   - **Destination Interface Objects** = outside.
e) Pour **Translation** (traduction), configurez les options suivantes :
   - **Source d'origine** = objet réseau ftp_server.
   - **Adresse** > **source traduite** = objet réseau ftp_server_outside.
f) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).




g) Cliquez sur **OK**.

# 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.




### Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

### Procédure

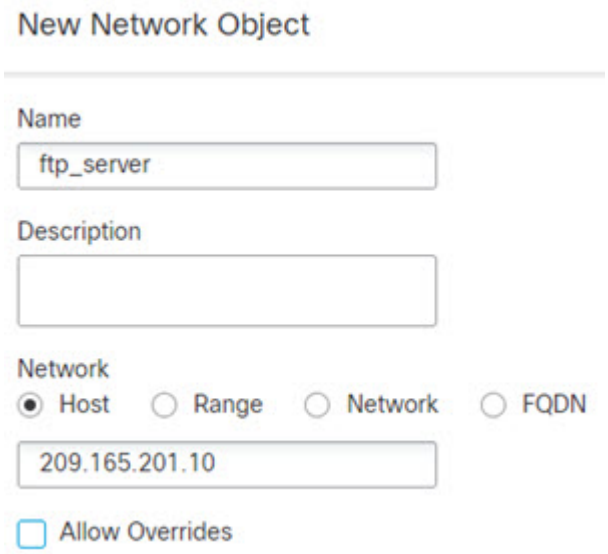
**Étape 1** Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

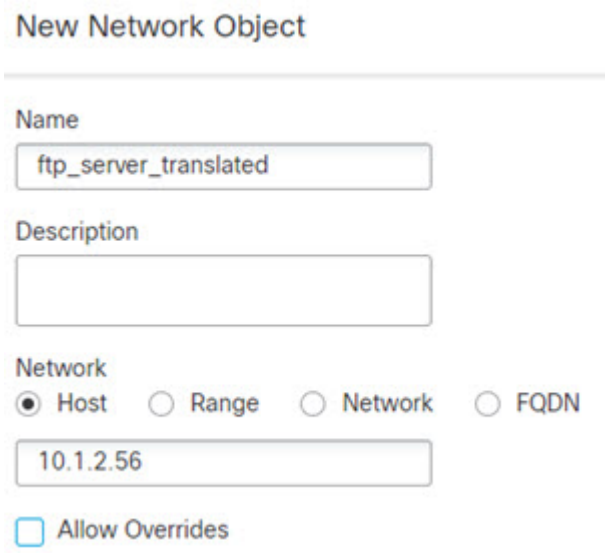
Nommez l'objet réseau (par exemple, serveur_ftp) et saisissez l'adresse de l'hôte, 209.165.201.10.




d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_translated) et saisissez l'adresse de l'hôte, 10.1.2.56.




f) Cliquez sur **Save** (enregistrer).

**Étape 2** Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

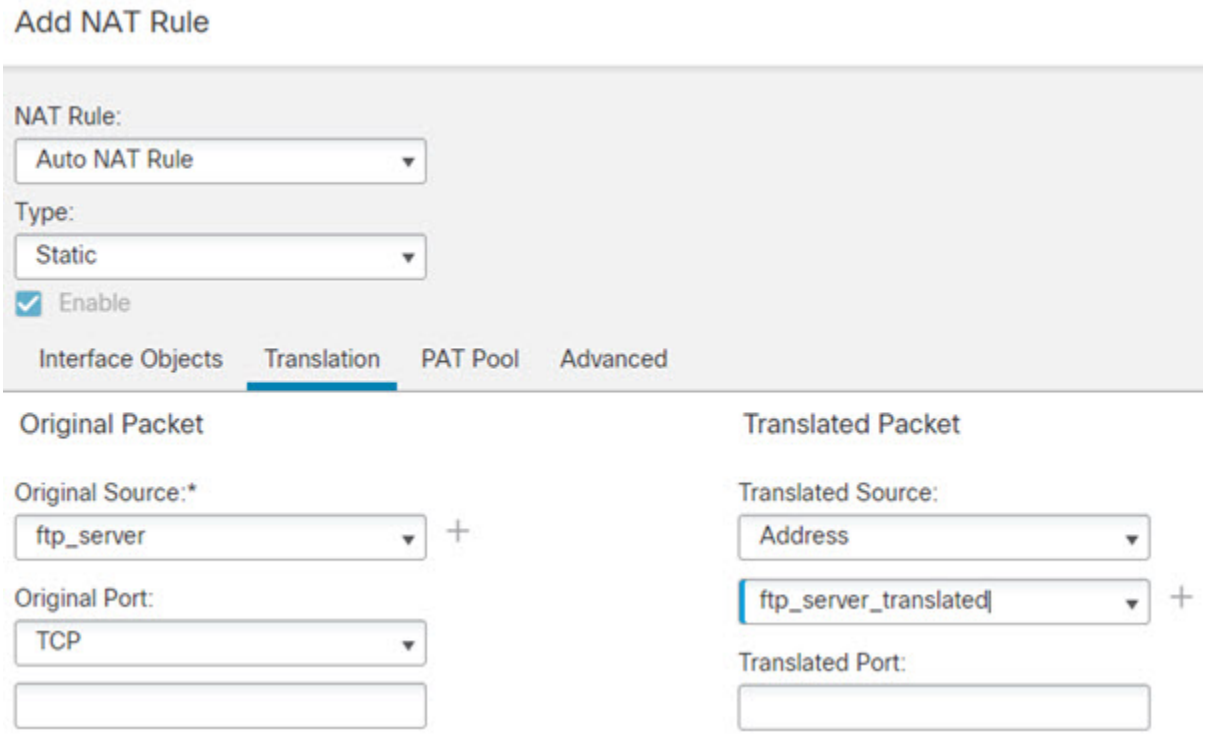
- **NAT Rule** = Auto NAT Rule.

- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :
   - **Source Interface Objects** = outside.
   - **Destination Interface Objects** = inside.

e) Pour **Translation** (traduction), configurez les options suivantes :
   - **Source d'origine** = objet réseau ftp_server.
   - **Adresse source** > **traduite** = ftp_server_translated network object.

f) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).




g) Cliquez sur **OK**.

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.