

Traduction d'adresses réseau (NAT)

Les rubriques suivantes expliquent la traduction d'adresses réseau (NAT) et comment la configurer sur le périphérique.

- Pourquoi utiliser la NAT?, à la page 1
- Principes de base de la NAT, à la page 2
- Directives pour la NAT, à la page 7
- Traduction d'adresses réseau dynamique, à la page 15
- PAT dynamique, à la page 24
- NAT statique, à la page 46
- NAT d'identité, à la page 58
- Surveillance de la NAT, à la page 66
- Historique de la NAT, à la page 66

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 routé 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 (adresse/hôte/réseau/interface réelle) : 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 ».

Types 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 15.
- 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 24.
- 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 46.
- 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 58.

NAT objet de réseau et Twice NAT (NAT en double)

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *network object NAT (NAT objet de réseau)* et *twice NAT (NAT en double)*.

Nous vous recommandons d'utiliser la network object NAT (NAT objet de réseau), sauf si vous avez besoin des fonctionnalités supplémentaires offertes par twice NAT (NAT en double). Il est plus facile de configurer network object NAT (NAT objet de réseau) 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.)

NAT objet de réseau

Toutes les règles NAT configurées comme paramètre d'un objet réseau sont considérées comme des règles *network object NAT (NAT objet de réseau)*. 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.

Après avoir configuré l'objet réseau, vous pouvez identifier l'adresse mappée de cet objet, soit en tant qu'adresse en ligne, soit en tant qu'autre objet de réseau ou groupe d'objets réseau.

Lorsqu'un paquet entre dans une interface, les adresses IP de source et de destination sont vérifiées par rapport aux règles network object NAT (NAT objet de réseau). 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 twice NAT (NAT en double) pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

Twice NAT (NAT en double)

Twice NAT (NAT en double) 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 NAT objet de réseau et Twice NAT (NAT en double)

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

- Votre définition de l'adresse réelle.
  - NAT d'objet réseau : vous définissez la NAT comme paramètre pour un objet réseau. Un objet réseau nomme un hôte, une plage ou un sous-réseau IP afin que vous puissiez ensuite utiliser l'objet dans la configuration NAT au lieu des adresses IP réelles. L'adresse IP de l'objet réseau sert d'adresse réelle. Cette méthode vous permet d'ajouter facilement une NAT à des objets réseau qui peuvent déjà être utilisés dans d'autres parties de votre configuration.
  - Twice NAT (NAT en double) : 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 twice NAT (NAT en double) est plus évolutif.
- Mise en œuvre de la NAT de source et de destination.
  - NAT objet de réseau : 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.
  - Twice NAT (NAT en double) : 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 twice NAT (NAT en double). 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
  - NAT objet de réseau : classés automatiquement dans la table NAT.
  - Twice NAT (NAT en double) : classés manuellement dans la table NAT (avant ou après les règles network object NAT (NAT objet de réseau)).

Ordre des règles NAT

Les règles NAT objet de réseau et twice NAT (NAT en double) 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	Twice NAT (NAT en double)	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 twice NAT (NAT en double) sont ajoutées à la section 1. Par « les règles spécifiques d'abord », nous entendons : • Les règles statiques doivent précéder les règles dynamiques. • Les règles qui incluent la traduction de destination doivent être placées avant les règles ne comprenant que la traduction de la source. 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 de tableau	Type de règle	Ordre des règles dans la section
Section 2	NAT objet de réseau	Si aucune correspondance n'est trouvée dans la section 1, les règles de la section 2 sont appliquées dans l'ordre suivant : **1.** Règles statiques. **2.** Règles dynamiques. **Pour chaque type de règle, les consignes d'ordre suivantes sont utilisées :** **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. **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. **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	Twice NAT (NAT en double)	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)

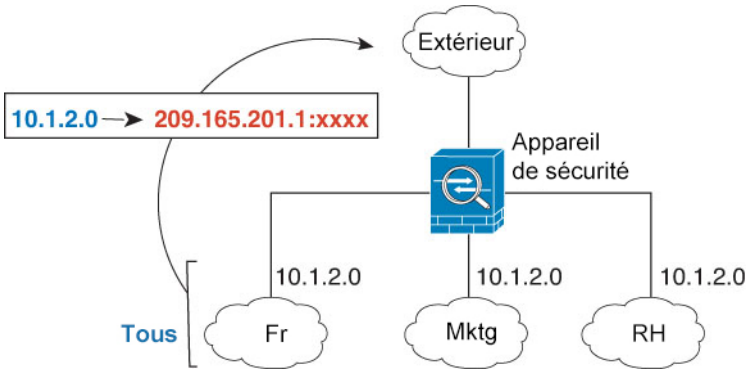
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

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 Internet.

Illustration 1 : 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.

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).

Lignes directrices relatives à la NAT 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. 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 (twice NAT (NAT en double) 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 (twice NAT (NAT en double) 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.

Lignes directrices supplémentaires pour la NAT

- Les règles NAT s'appliquent uniquement au trafic du périphérique. Elles ne s'appliquent pas au trafic initié par le périphérique, comme une authentification RADIUS.
- 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.
- (NAT objet de réseau 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 n'est pas attribuée à plusieurs hôtes.

- Lors de la traduction du trafic SCTP, utilisez uniquement la NAT de l'objet réseau statique. La NAT ou la PAT dynamique ne sont pas autorisées. Bien que vous puissiez configurer deux règles de NAT statique, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue.
- Les objets et les groupes d'objets utilisés dans la NAT ne peuvent pas être non définis; ils doivent inclure des adresses IP.
- 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.
- (Twice NAT (NAT en double) seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « any » (IPv4 ou IPv6) dépend de la règle. Avant que ASA effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, ASA 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.
  - Ensemble d'adresses de VPN existantes
- 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.
- Pour les limites de l'inspection des applications avec NAT ou PAT, consultez Inspections par défaut et limites de la NAT.
- 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. Consultez Routage des paquets NAT pour de plus amples renseignements.
- Si vous activez la commande **arp permit-nonconnected**, le système ne répond pas aux requêtes ARP si l'adresse mappée ne fait partie d'aucun sous-réseau connecté et vous ne spécifiez pas non plus l'interface mappée dans la règle NAT (c'est-à-dire si vous spécifiez « any »). Pour résoudre ce problème, spécifiez l'interface mappée.
- 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 peut se produire si vous utilisez l'option « flat range » pour utiliser les numéros de port les plus élevés si un port de la plage inférieure n'est pas disponible, en particulier si vous ne sélectionnez pas l'option d'inclusion de la plage inférieure dans la plage fixe. 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.
- Vous pouvez améliorer les performances et la fiabilité du système en utilisant le modèle de validation transactionnelle pour la NAT. Pour plus d'informations, consultez le chapitre sur les paramètres de base dans le guide de configuration des opérations générales. L'option se trouve sous **Configurations (Configurations) > Device Management (gestion des périphériques) > Advanced (Avancé) > Rule Engine (moteur de règles)**.
- 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).
- (Twice NAT (NAT en double)) 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.
- DHCP et BOOTP partagent les ports UDP/67-68. Comme BOOTP est obsolète, l'écriture de règles NAT pour le port bootps peut entraîner des problèmes d'allocation de port lors de l'exécution de DHCP. Envisagez d'utiliser le relais DHCP plutôt pour transmettre les demandes DHCP entre les segments de réseau.
- Dans de rares cas, le trafic de retour (serveur à client) avec une traduction existante (xlate) peut être enregistré comme un nouveau flux dans les événements de connexion. Cela peut se produire lorsque le client a déjà mis fin à la connexion et que le serveur envoie un autre paquet qui atteint le périphérique pendant le court intervalle entre la fermeture de la connexion et le retrait de xlate, souvent en raison du

comportement de l'application ou du nettoyage de la pile TCP. Comme le périphérique supprime le xlate uniquement après avoir supprimé la connexion, un paquet de serveur peut arriver pendant que le xlate existe toujours. Si aucune entrée de connexion valide n'est trouvée, le périphérique consigne un événement de connexion distinct en fonction de la règle de politique de contrôle d'accès correspondante.

Lignes directrices de NAT d'objets réseau pour les objets d'adresses mappées

Pour la NAT dynamique, vous devez utiliser un objet ou un groupe pour les adresses mappées. Pour les autres types de NAT, vous pouvez utiliser un objet ou un groupe, ou vous avez la possibilité d'utiliser des adresses en ligne. Les groupes d'objets réseau sont particulièrement utiles pour créer un ensemble d'adresses mappées avec des plages d'adresses IP discontinues ou plusieurs hôtes ou sous-réseaux.

Tenez compte des Lignes directrices suivantes lors de la création d'objets pour les adresses mappées.

- Un groupe d'objets réseau peut contenir des objets ou des adresses en ligne des adresses IPv4 ou IPv6. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- Consultez Lignes directrices supplémentaires pour la NAT, à la page 9 pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules pour nommer un objet réseau ou un ensemble PAT.
- NAT dynamique :
  - Vous ne pouvez pas utiliser une adresse en ligne; vous devez configurer un objet ou un groupe réseau.
  - L'objet ou le groupe ne peut pas contenir de sous-réseau; l'objet doit définir une plage ; le groupe peut inclure des hôtes et des plages.
  - Si un objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.
- PAT dynamique (masquer) :
  - Au lieu d'utiliser un objet, vous pouvez éventuellement configurer une adresse d'hôte en ligne ou préciser l'adresse de l'interface.
  - Si vous utilisez un objet, l'objet ou le groupe ne peut pas contenir de sous-réseau. L'objet doit définir un hôte ou, pour un pool PAT, une plage. Le groupe (pour un ensemble PAT) peut inclure des hôtes et des plages.
- NAT statique ou NAT statique avec traduction de port
  - Au lieu d'utiliser un objet, vous pouvez configurer une adresse en ligne ou préciser l'adresse de l'interface (pour la NAT statique avec traduction de port).
  - Si vous utilisez un objet, l'objet ou le groupe peut contenir un hôte, une plage ou un sous-réseau.
- NAT d'identité
  - Au lieu d'utiliser un objet, vous pouvez configurer une adresse en ligne.

- Si vous utilisez un objet, celui-ci doit correspondre aux adresses réelles que vous souhaitez traduire.

Lignes directrices pour le NAT Twice concernant les objets d'adresses réelles et mappées

Pour chaque règle NAT, configurez jusqu'à quatre objets ou groupes réseau pour :

- Adresse réelle de la source
- Adresse mappée de la source
- Adresse réelle de destination
- Adresse mappée de destination

Les objets sont requis, sauf si vous spécifiez le mot-clé **any** en ligne pour représenter tout le trafic ou, pour certains types de NAT, le mot-clé **interface** pour représenter l'adresse de l'interface. Les groupes d'objets réseau sont particulièrement utiles pour créer un ensemble d'adresses mappées avec des plages d'adresses IP discontinues ou plusieurs hôtes ou sous-réseaux.

Tenez compte des lignes directrices suivantes lors de la création d'objets pour la NAT Twice.

- Un groupe d'objets réseau peut contenir des objets ou des adresses en ligne IPv4 ou IPv6. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- Consultez Lignes directrices supplémentaires pour la NAT, à la page 9 pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules pour nommer un objet réseau ou un ensemble PAT.
- NAT dynamique source :
  - Vous configurez généralement un groupe plus important d'adresses réelles à mapper à un groupe plus restreint.
  - L'objet ou le groupe mappé ne peut pas contenir de sous-réseau; l'objet doit définir une plage; le groupe peut inclure des hôtes et des plages.
  - Si l'objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.
- NAT dynamique source PAT (masquer) :
  - Si vous utilisez un objet, l'objet ou le groupe ne peut pas contenir de sous-réseau. L'objet doit définir un hôte ou, pour un ensemble PAT, une plage. Le groupe (pour un ensemble PAT) peut inclure des hôtes et des plages.
- Source NAT statique ou NAT statique avec traduction de port :
  - L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux.

- Le mappage statique est généralement de type un à un, de sorte que les adresses réelles sont en nombre égal aux adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.

- Source NAT d'identité :
  - Les objets réels et mappés doivent correspondre. Vous pouvez utiliser le même objet pour les deux ou créer des objets distincts qui contiennent les mêmes adresses IP.

- NAT statique de destination ou NAT statique avec traduction de port (la traduction de destination est toujours statique) :
  - Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.
  - Pour la NAT d'identité, les objets réels et mappés doivent correspondre. Vous pouvez utiliser le même objet pour les deux ou créer des objets distincts qui contiennent les mêmes adresses IP.
  - Le mappage statique est généralement de type un à un, de sorte que les adresses réelles sont en nombre égal aux adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.
  - Pour la NAT d'interface statique avec traduction de port (mode routé uniquement), vous pouvez spécifier le mot-clé **interface** au lieu d'un objet ou d'un groupe de réseau pour l'adresse mappée.
  - Vous pouvez utiliser un nom de domaine complet, tel que www.exemple.com, comme destination traduite (mappée). Pour de plus amples renseignements, consultez la section Lignes directrices relatives aux destinations FQDN, à la page 14.

Lignes directrices relatives aux destinations FQDN

Vous pouvez spécifier la destination traduite (mappée) dans une règle twice NAT (NAT en double) 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 de la source traduite et celui de 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 au format IPv4, l'objet FQDN doit spécifier IPv4 comme type d'adresse.

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.

Lignes directrices NAT Twice pour les objets de service pour les ports réels et mappés

Vous pouvez éventuellement configurer des objets de service pour :

- **Port réel source (statique uniquement)** *ou* **port réel de destination**
- **Port mappé source (statique uniquement)** *ou* **port mappé de destination**

Tenez compte des lignes directrices suivantes lors de la création d'objets pour la NAT Twice.

- La NAT prend en charge uniquement les protocoles TCP, UDP et SCTP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Bien que vous puissiez configurer des règles de NAT Twice statiques avec des spécifications de port SCTP, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue. Utilisez plutôt la NAT d'objet statique pour SCTP.
- L'opérateur « non égal » (**neq**) n'est pas pris en charge.
- Pour la traduction de port d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.
- NAT dynamique source : la NAT dynamique source ne prend pas en charge la traduction de port.
- PAT dynamique source (Masquer) : la PAT dynamique source ne prend pas en charge la traduction de port.
- NAT statique source, NAT statique avec traduction de port ou NAT d'identité : un objet de service peut contenir à la fois un port source et un port de destination; toutefois, vous devez préciser *soit* le port source, *soit* le port de destination pour les deux objets de service. Vous ne devez spécifier *les deux*, ports source et de destination, que si votre application utilise un port source fixe (comme certains serveurs DNS) ; mais les ports sources fixes sont rares. Par exemple, si vous souhaitez traduire le port pour l'hôte source, configurez le service source.
- NAT statique de destination ou NAT statique avec traduction de port (la traduction de destination est toujours statique) : pour la NAT source non statique, vous pouvez effectuer une traduction de port uniquement sur la destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré.

Traduction d'adresses réseau dynamique

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

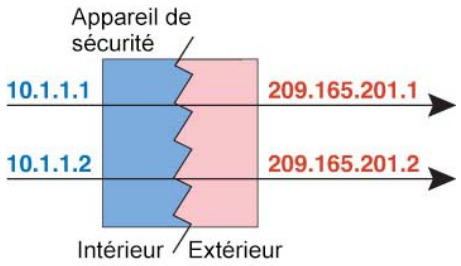
À propos de la NAT dynamique

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.

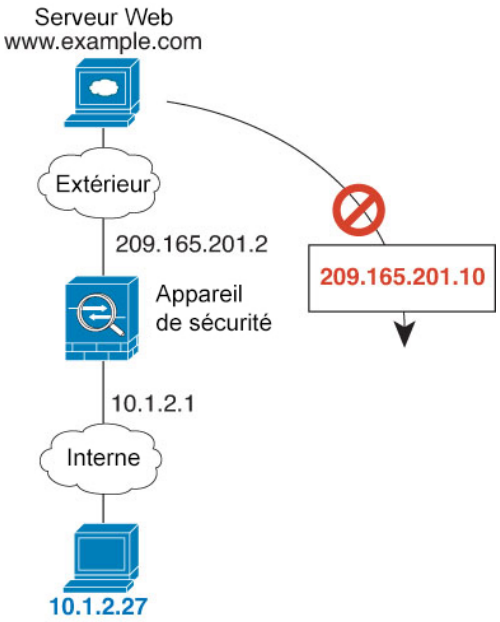
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

Illustration 2 : 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 3 : L'hôte distant tente d'établir une connexion à une adresse mappée



Désavantages et avantages 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 dynamique

Cette section décrit comment configurer la NAT d'objet réseau pour la NAT dynamique.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)**, puis modifiez un objet réseau.

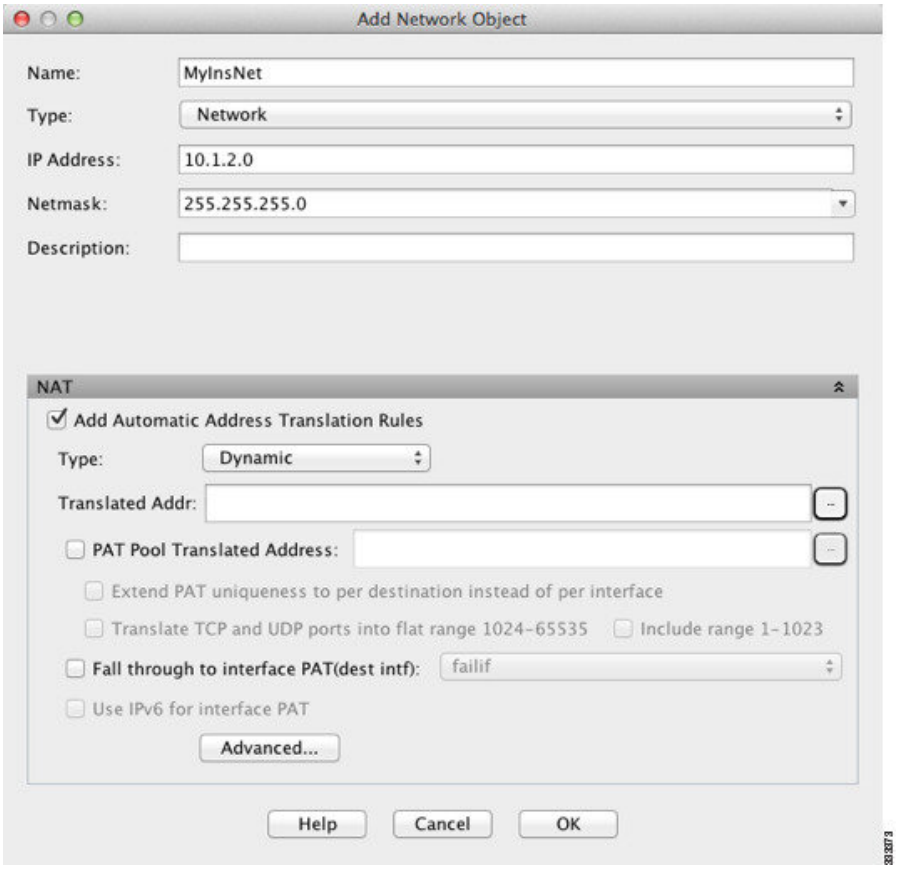
Étape 2 Renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.

b) **Type** : hôte, réseau ou plage.

c) **IP Addresses** (Adresses IP) : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et, pour le sous-réseau, soit une adresse réseau IPv4 et un masque (par exemple, 10.100.10.0 255.255.255.0), soit une adresse IPv6 et une longueur de préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.



Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic** (Dynamique).

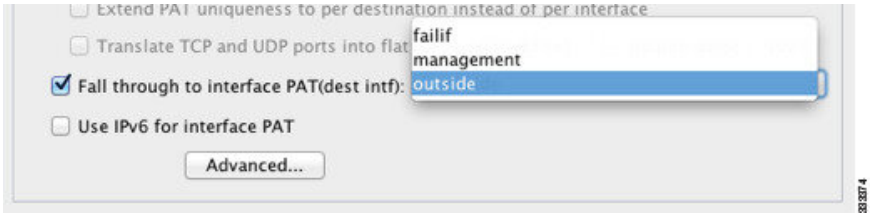
Étape 6 À droite du champ Translated Addr (Adresse traduite), cliquez sur le bouton de navigation et choisissez l'objet réseau ou le groupe d'objets réseau qui contient les adresses mappées.

Vous pouvez créer un nouvel objet si nécessaire.

L'objet ou le groupe ne peut pas contenir 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 objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde lorsque les autres adresses mappées sont déjà allouées, cochez la case **Fall through to interface PAT (dest intf)** (Basculer vers la PAT d'interface [dest intf]) et choisissez l'interface dans la liste déroulante. Pour utiliser l'adresse IPv6 de l'interface, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



Étape 8 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- **Translate DNS replies for rule** (Traduire les réponses DNS pour la règle) : traduit l'adresse IP dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT pour de plus amples renseignements.
- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la NAT Twice dynamique

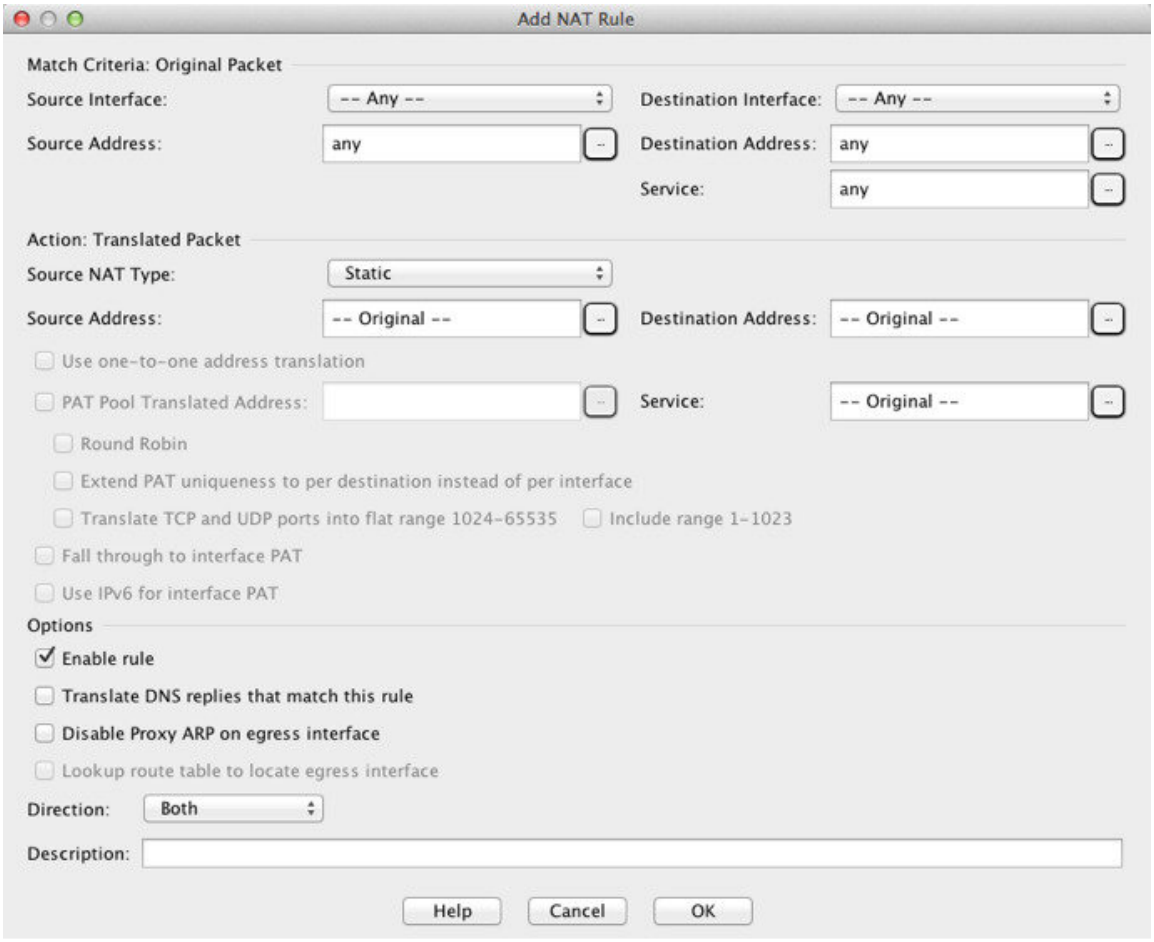
Cette section décrit comment configurer la NAT Twice pour la NAT dynamique.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

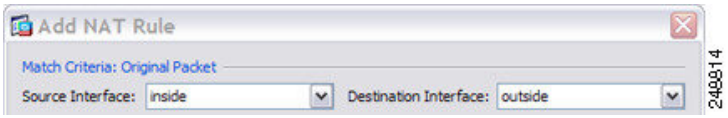


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

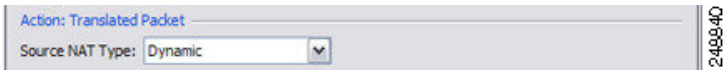
a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet > Destination Interface (Critères de correspondance : paquet d'origine > Interface de destination)**, choisissez l'interface de destination.

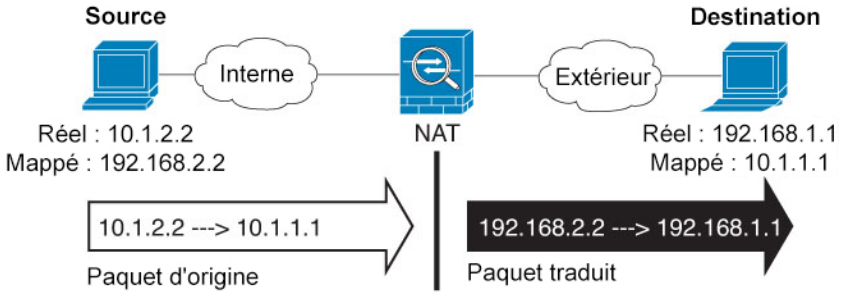


Étape 3 Choisissez **Dynamic** (Dynamique) dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : paquet traduit > Type de NAT source).

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.

b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 47 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action : Paquet traduit > Adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source traduite.

Pour la NAT dynamique, vous configurez généralement un groupe plus important d'adresses source à mapper à un groupe plus restreint.

Si un objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme repli PAT. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Remarque

L'objet ou le groupe ne peut pas contenir de sous-réseau.

b) Pour **l'action : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe de réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

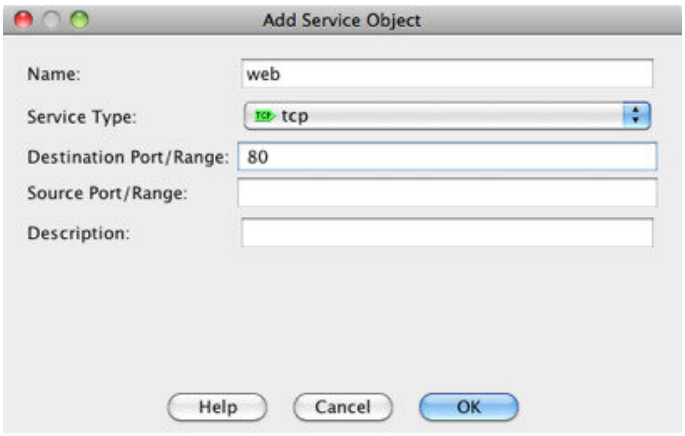
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 46. Consultez Lignes directrices supplémentaires pour la NAT, à la page 9 pour en savoir plus sur les adresses IP mappées non autorisées.

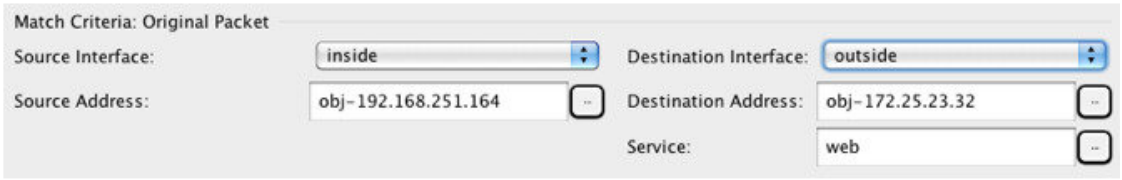
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

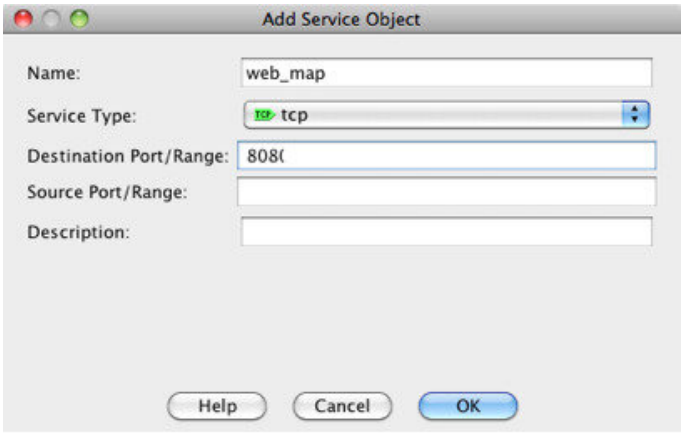
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet > Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :



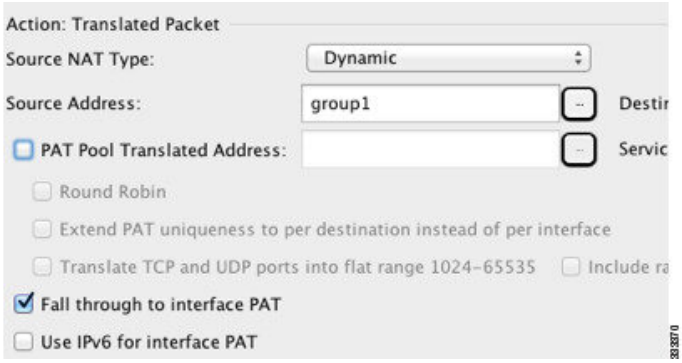






Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde si les autres adresses source mappées sont déjà allouées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT de l'interface). Pour utiliser l'adresse d'interface IPv6, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface).

L'adresse IP de l'interface de destination est utilisée. Cette option est uniquement disponible si vous configurez une interface de destination spécifique.



Étape 8 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement) **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle) : réécrit l'enregistrement DNS A dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer la modification DNS si vous configurez une adresse de destination. Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT pour de plus amples renseignements.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 9 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

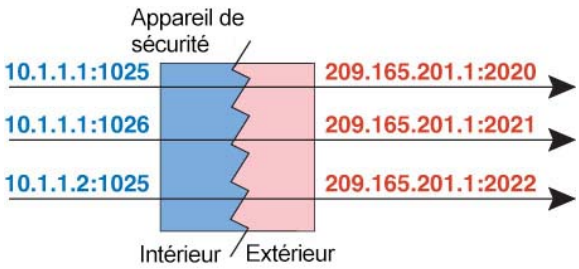
À propos de la PAT dynamique

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 4 : 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. Pour la PAT multisession, le délai d'expiration de la PAT est utilisé, soit 30 secondes par défaut. Pour les PAT par session, le xlate est immédiatement supprimé.

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 ASA 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. Consultez Inspections par défaut et limites de la NAT pour plus d'informations sur la prise en charge de NAT et PAT.

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 pool d'adresses PAT et utiliser une attribution round-robin des adresses PAT pour atténuer cette situation.

Lignes directrices relatives aux objets de 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 modifiez la limite d'unité de grappe (la taille de la grappe), veillez à effacer les xlates ou à redémarrer les périphériques afin que les ensembles PAT puissent être réaffectés de manière appropriée aux unités de grappe.

- 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. Consultez Inspections par défaut et limites de la NAT pour obtenir une liste complète des inspections non prises en charge.
- 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 l'adresse 10.1.1.1, 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 d'objet réseau dynamique (Masquer)

Cette section décrit comment configurer la NAT d'objet réseau pour la PAT dynamique (Masquer), qui utilise une adresse unique pour la traduction au lieu d'un ensemble de PAT.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

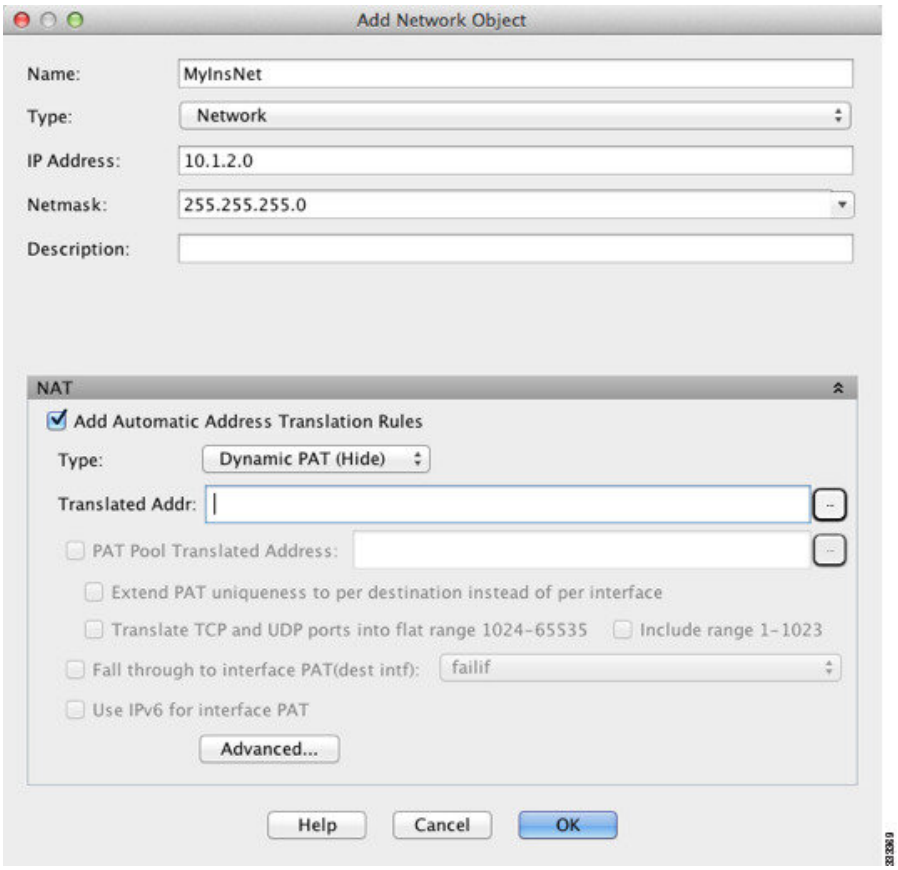
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
b) **Type** : hôte, réseau ou plage.
c) **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

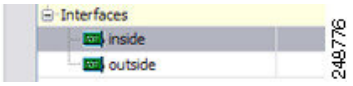
Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic PAT (Hide)** (PAT dynamique [Masquer]).



Étape 6 Précisez une adresse mappée unique. Dans le champ Adresse traduite, spécifiez l'adresse IP mappée en effectuant l'une des opérations suivantes :

- Tapez une adresse IP d'hôte.
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau hôte (ou créez-en un nouveau).
- (Interfaces non membres d'un groupe de ponts uniquement.) Tapez un nom d'interface ou cliquez sur le bouton de navigation, puis choisissez une interface dans la boîte de dialogue Parcourir les adresses traduites.



Si vous spécifiez un nom d'interface, vous activez *l'interface PAT*, où l'adresse IP de l'interface spécifiée est utilisée comme adresse mappée. Pour utiliser l'adresse d'interface IPv6, vous devez également cocher la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface). Avec la PAT d'interface, la règle NAT s'applique uniquement à l'interface mappée spécifiée, qui ne peut pas être membre d'un groupe de ponts. (Si vous n'utilisez pas la PAT d'interface, la règle s'applique à toutes les interfaces par défaut.) Vous ne pouvez pas spécifier d'interface en mode transparent.

Étape 7 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 8 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la PAT d'objet réseau dynamique à l'aide d'un ensemble PAT

Cette section décrit comment configurer la NAT d'objet réseau pour la PAT dynamique à l'aide d'un pool PAT.

Procédure

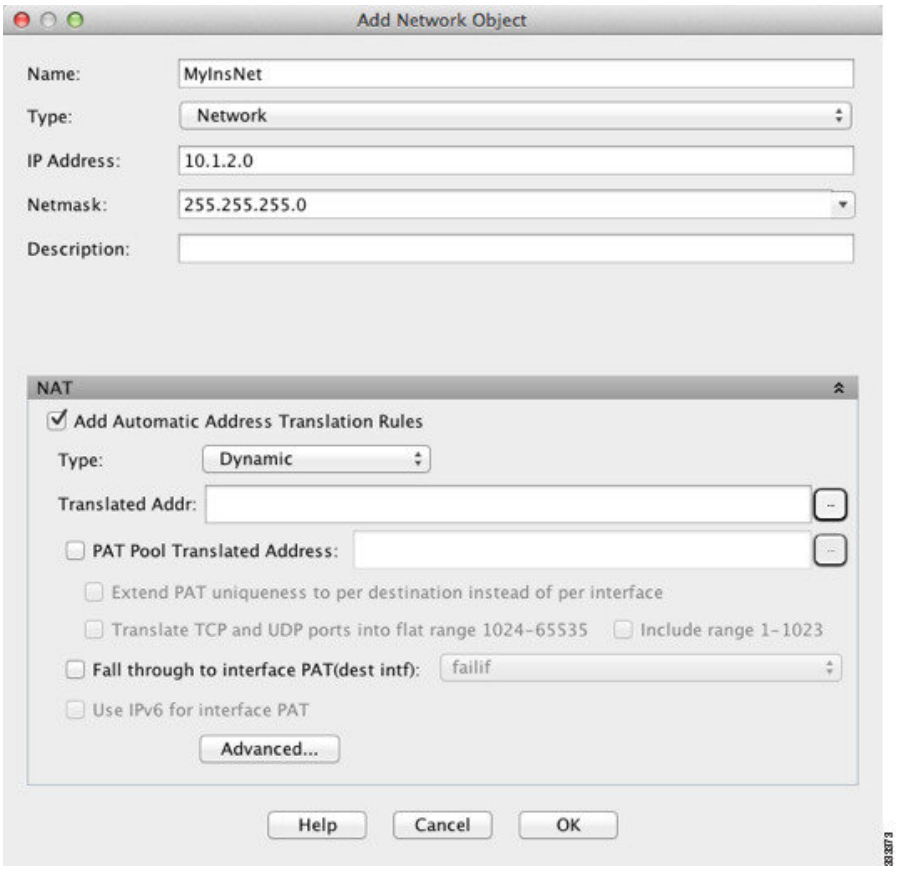
Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter une nouvelle règle NAT d'objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter)** > **Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **Objects** > **(Objets)** > **Network Objects/Groups** > **(Objets/groupes réseau),** puis modifiez un objet réseau.

Étape 2 Pour un nouvel objet, renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
b) **Type** : hôte, réseau ou plage.
c) **IP Addresses** (Adresses IP) : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et, pour le sous-réseau, soit une adresse réseau IPv4 et un masque (par exemple, 10.100.10.0 255.255.255.0), soit une adresse IPv6 et une longueur de préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.



Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic** (Dynamique) même si vous configurez la PAT dynamique avec un pool PAT.

Étape 6 Pour configurer le pool PAT :

a) Ne saisissez pas de valeur pour le champ de l'adresse traduite ; laissez-le vide.

b) Cochez la case **PAT Pool Translated Address** (Adresse traduite du pool PAT), puis cliquez sur le bouton de navigation et choisissez l'objet ou le groupe de réseau qui contient les adresses de pool PAT. Vous pouvez également créer un nouvel objet à partir de la boîte de dialogue Browse Translated PAT Pool Address (Parcourir les adresses de pool PAT traduites).

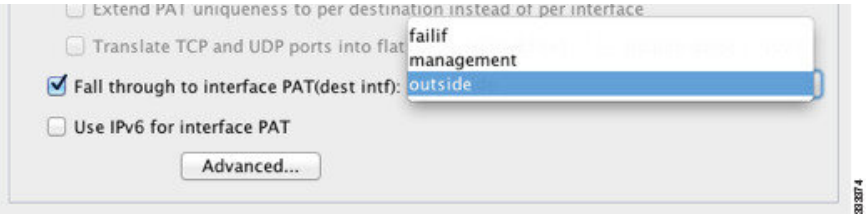
Remarque
L'objet ou le groupe de pool PAT ne peut pas contenir de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.



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

- **Round Robin** : pour attribuer des adresses et 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.
- **Extend PAT uniqueness to per destination instead of per interface** (Étendre l'unicité de la PAT par destination plutôt que par interface) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour utiliser la 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.
- **Include Reserved Ports (1 to 1023)** (Inclure les ports réservés [1 à 1 023]) : comprend les ports réservés, de 1 à 1 023, dans la plage des ports disponibles pour la traduction d'adresses. Si vous ne spécifiez pas cette option, les adresses sont traduites uniquement vers des ports dans la plage de 1 024 à 65 535.
- **Enable Block Allocation** (Activer l'allocation de blocs) (9.5.1 et versions ultérieures) : active l'allocation de blocs 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. 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'allocation de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le PAT étendu. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde lorsque les autres adresses mappées sont déjà attribuées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT d'interface) et choisissez l'interface dans la liste déroulante. Pour utiliser l'adresse IPv6 de l'interface, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



Étape 8 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la PAT Twice dynamique (Masquer)

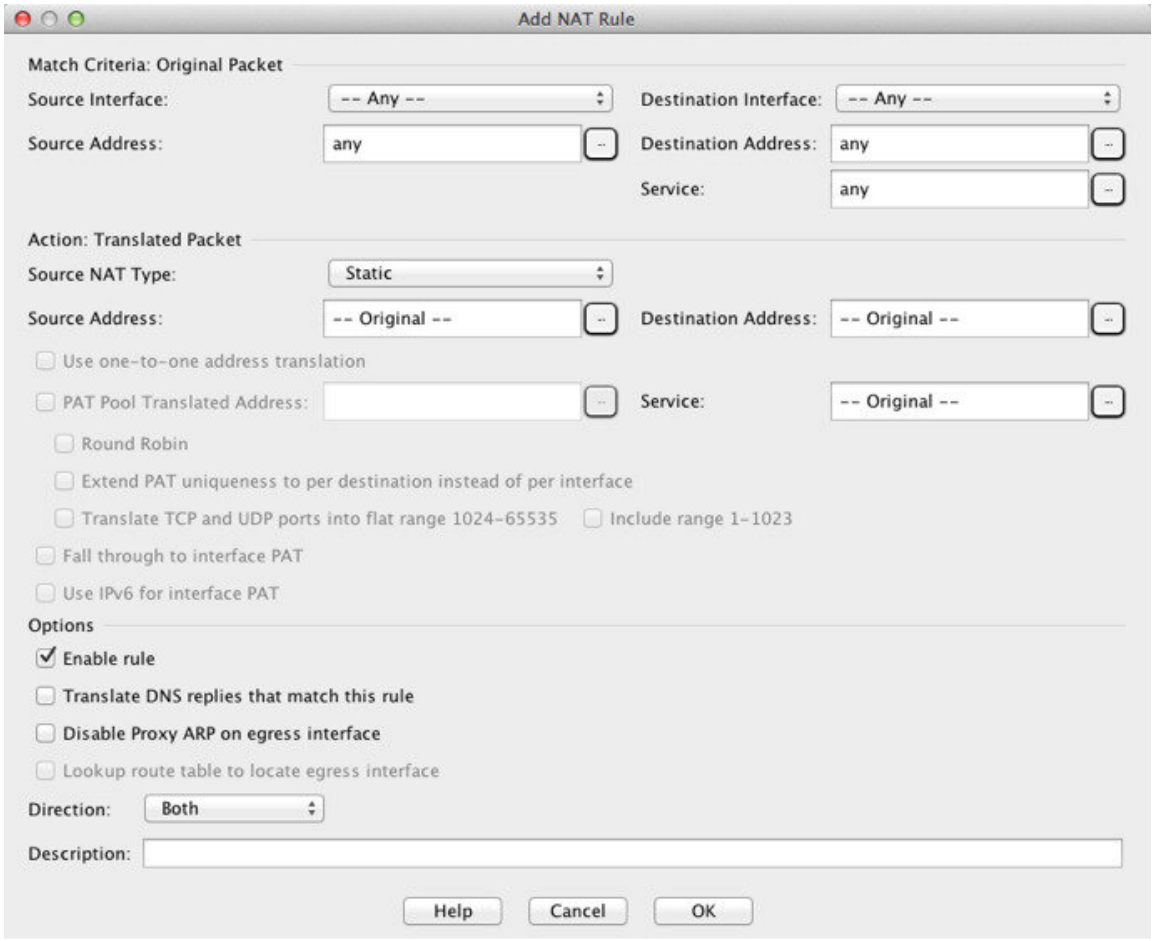
Cette section décrit comment configurer la NAT Twice pour la PAT dynamique (Masquer), qui utilise une adresse unique pour la traduction au lieu d'un pool PAT.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)** , puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

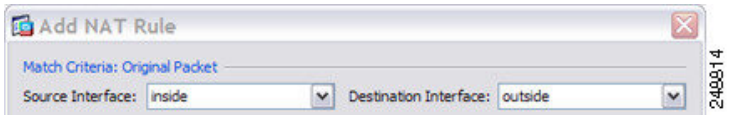


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces de source et de destination.

En mode routé, la valeur par défaut est n'importe quelle interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet > Destination Interface** (Critères de correspondance : Paquet d'origine > Interface de destination), choisissez l'interface de destination.

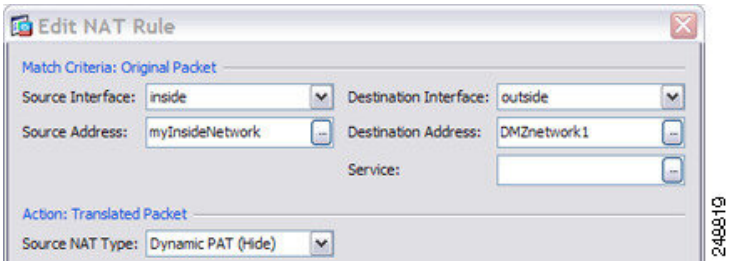


Étape 3 Choisissez **Dynamic PAT (Hide) (PAT dynamique [Masquer])** dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : Paquet traduit > Type de NAT source).

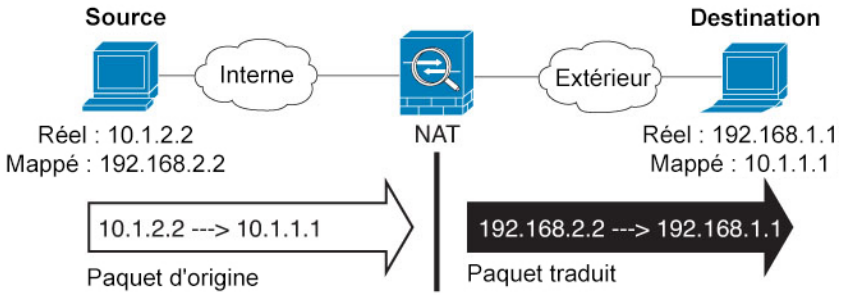
Ce paramètre s'applique uniquement à l'adresse source ; la traduction de destination est toujours statique.

Remarque

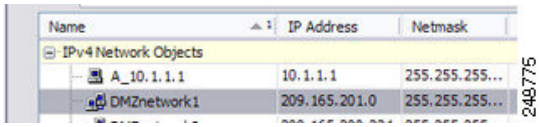
Pour configurer la PAT dynamique à l'aide d'un pool PAT, choisissez **Dynamic** (Dynamique) au lieu de Dynamic PAT (Hide) (PAT dynamique [Masquer]) ; consultez Configurer la PAT Twice dynamique à l'aide d'un ensemble PAT, à la page 37.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **Match Criteria: Original Packet > Source Address** (Critères de correspondance : Paquet d'origine > Adresse source), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.



b) (Facultatif) Pour **Match Criteria: Original Packet > Destination Address** (Critères de correspondance : Paquet d'origine > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface existants (interfaces non membres de groupes de ponts uniquement), ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine). Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

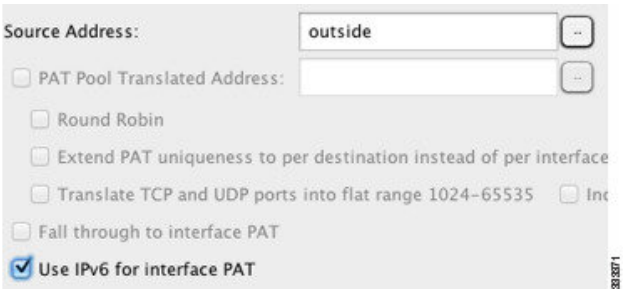
Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse. Vous pouvez configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 47 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action: Translated Packet > Source Address** (Action : Paquet traduit > Adresse source), cliquez sur le bouton de navigation et choisissez un objet réseau existant qui définit une adresse d'hôte, ou une interface, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite). L'interface ne peut pas faire partie d'un groupe de pont.

Si vous souhaitez utiliser l'adresse IPv6 de l'interface, cochez la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



b) (Facultatif) Pour **Action: Translated Packet > Destination Address** (Action : Paquet traduit > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated Destination Address (Parcourir l'adresse de destination traduite). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

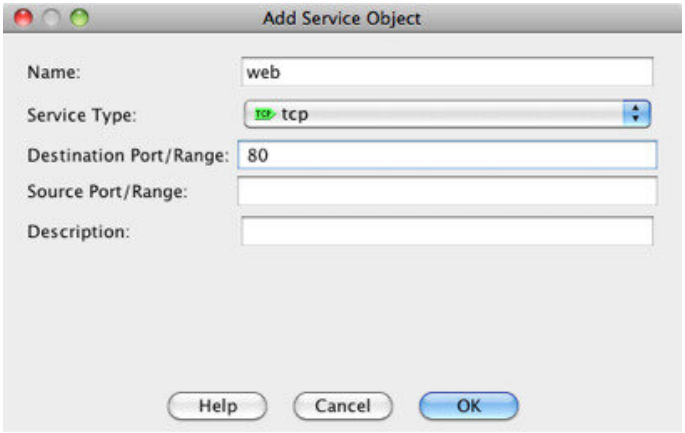
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 46. Consultez Directives pour la NAT, à la page 7 pour en savoir plus sur les adresses IP mappées non autorisées.

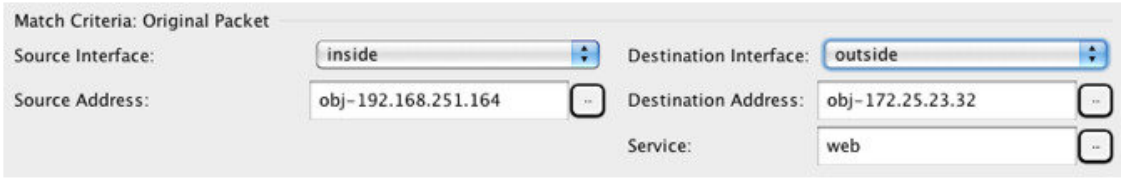
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

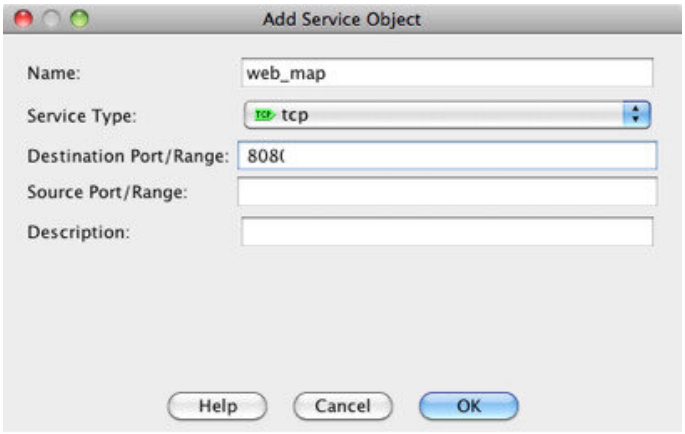
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet > Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :

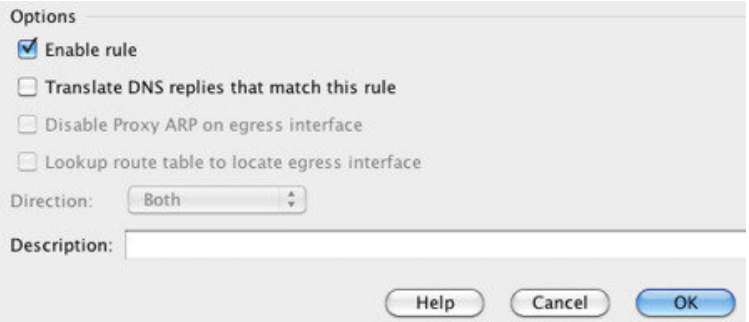








Étape 7 (Facultatif) Configurez les options de NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. Cette fonction est activée par défaut.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 8 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer la PAT Twice dynamique à l'aide d'un ensemble PAT

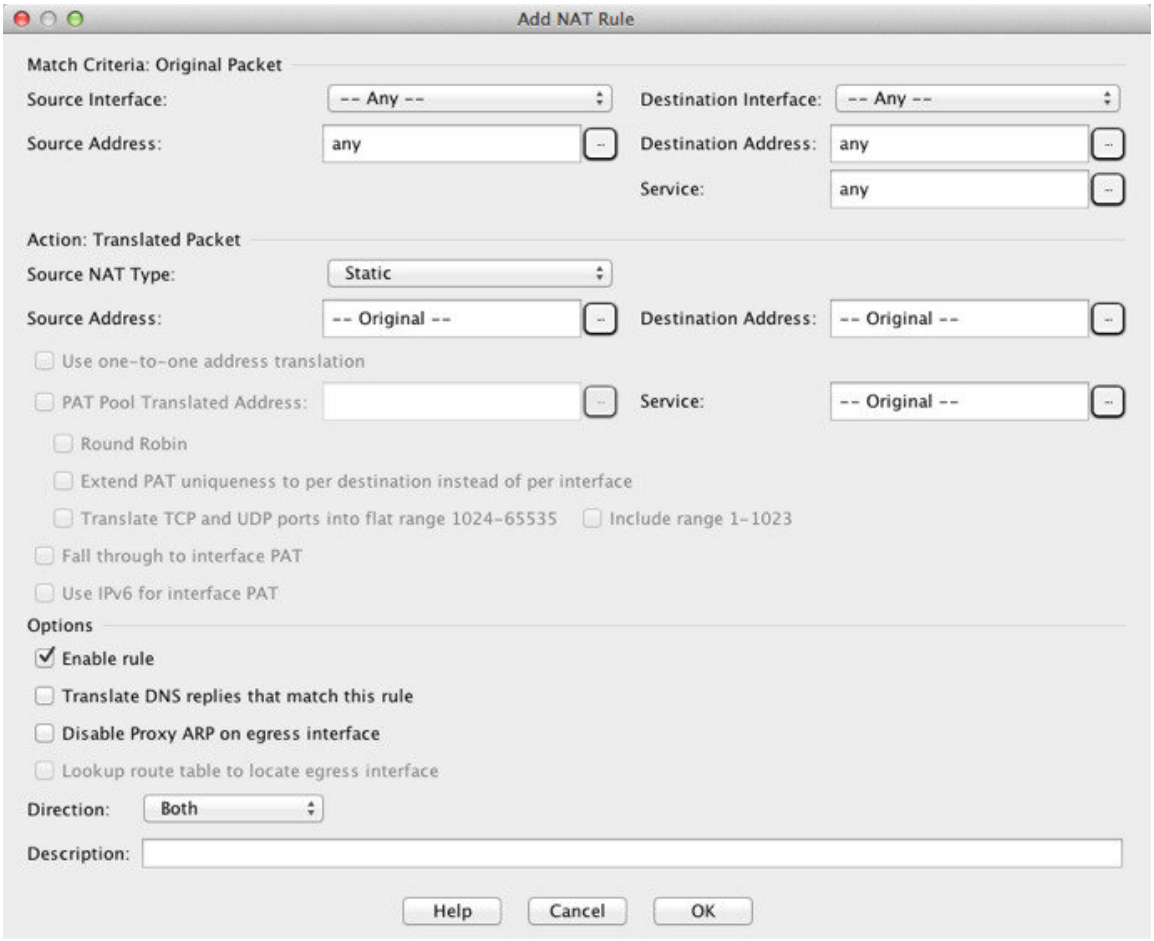
Cette section décrit comment configurer la NAT Twice pour la PAT dynamique à l'aide d'une réserve PAT.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add** NAT **Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add** NAT **Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.



Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts; « any » n'inclut pas ces interfaces.

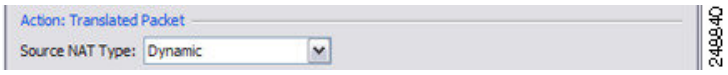
a) Dans la liste déroulante **Match Criteria: Original Packet** > **Source Interface** (Critères de correspondance : paquet d'origine > Interface source), choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet** > **Destination Interface** (Critères de correspondance : paquet d'origine > Interface de destination), choisissez l'interface de destination.

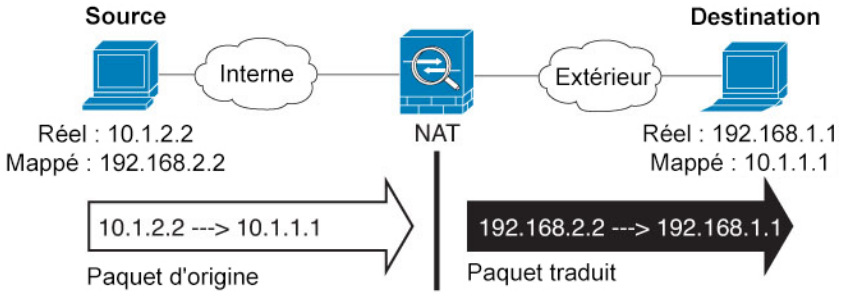


Étape 3 Choisissez **Dynamic** (Dynamique) dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : paquet traduit > Type de NAT source).

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **Match Criteria: Original Packet** > **Source Address** (Critères de correspondance : paquet d'origine > Adresse source), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.

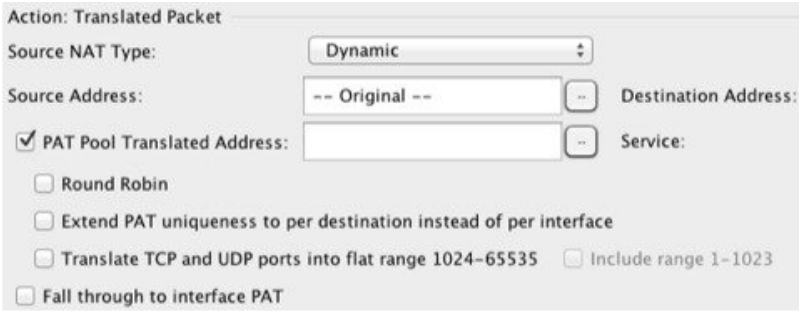
b) (Facultatif) Pour **Match Criteria: Original Packet** > **Destination Address** (Critères de correspondance : paquet d'origine > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface existant (interfaces qui ne sont pas membres d'un groupe de ponts uniquement), ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine). Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 47 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Cochez la case **PAT Pool Translated Address** (Adresse traduite du pool PAT), puis cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated PAT Pool Address (Parcourir l'adresse du pool PAT traduit). **Remarque :** laissez le champ Adresse source vide.



Remarque
L'objet ou le groupe ne peut pas contenir de sous-réseau.

b) (Facultatif) Pour **Action: Translated Packet** > **Destination Address** (Action : paquet traduit > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated Destination Address (Parcourir l'adresse de destination traduite).

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

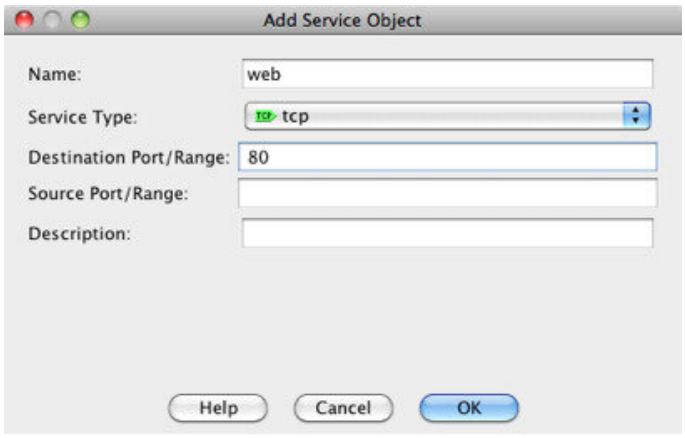
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 46. Consultez Directives pour la NAT, à la page 7 pour en savoir plus sur les adresses IP mappées non autorisées.

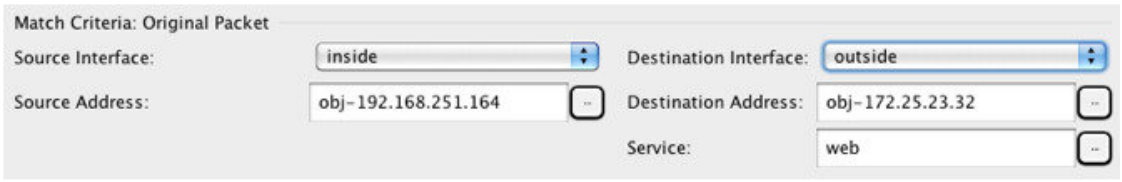
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

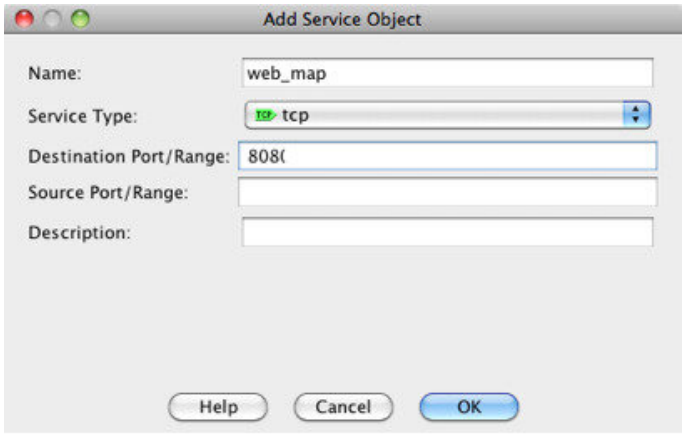
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet** > **Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet** > **Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :









Étape 7 (Facultatif) Pour un pool PAT, configurez les options suivantes selon les besoins :

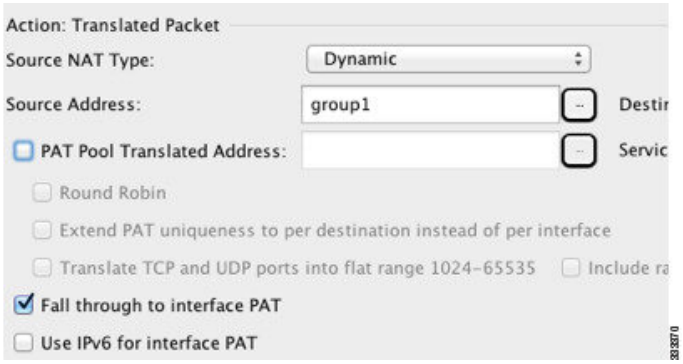
- **Round Robin** (Tourniquet) : permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
- **Extend PAT uniqueness to per destination instead of per interface** (Étendre l'unicité de la PAT par destination plutôt que par interface) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour

utiliser la 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.

- **Translate TCP or UDP ports into flat range (1024-65535)** (Traduire les ports TCP ou UDP en plage continue [1024 à 65 535]) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour utiliser la plage de ports de 1 024 à 65 535 comme plage continue unique lors de l'allocation de ports. Lorsque vous choisissez le numéro de port mappé pour une traduction, l'ASA 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 65 535, cochez également la case **Include range 1 to 1 023** (Inclure la plage de 1 à 1 023).
- **Include Reserved Ports (1 to 1023)** (Inclure les ports réservés [1 à 1 023]) : comprend les ports réservés, de 1 à 1 023, dans la plage des ports disponibles pour la traduction d'adresses. Si vous ne spécifiez pas cette option, les adresses sont traduites uniquement vers des ports dans la plage de 1 024 à 65 535.
- **Enable Block Allocation** (Activer l'allocation de blocs) (9.5.1 et versions ultérieures) : active l'allocation de blocs 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. 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'allocation de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le PAT étendu. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 8 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde si les autres adresses source mappées sont déjà allouées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT de l'interface). Pour utiliser l'adresse d'interface IPv6, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface).

L'adresse IP de l'interface de destination est utilisée. Cette option est uniquement disponible si vous configurez une interface de destination spécifique.



Étape 9 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 10 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

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. Il existe des blocs distincts pour les connexions TCP, UDP et ICMP, et ces blocs peuvent se chevaucher. 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 **Round Robin** (Round-robin), mais vous ne pouvez pas inclure les options permettant d'étendre l'unicité PAT, ou de basculer vers la PAT d'interface. 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. Cependant, lorsque vous fonctionnez dans une grappe, vous devez recharger la grappe pour que les unités puissent distribuer correctement les blocs.

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 pat-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 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)** et configurez les paramètres suivants :

- **Size of the block** (Taille du bloc) : nombre de ports dans chaque bloc. La plage est de 32 à 4096. La valeur par défaut est 512.

  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.

- **Maximum block allocation per host** (Allocation maximale de blocs par hôte) : nombre maximal de blocs pouvant être alloués par hôte. 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.

- **PBA Interim Logging** (Journalisation intermédiaire PBA) : si vous saisissez une valeur, le système active la journalisation intermédiaire. 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*

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

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**.
b) Ajoutez ou modifiez une règle NAT d'objet ou de NAT Twice.
c) Configurez au moins les options suivantes :

- (NAT Twice.) Sélectionnez l'objet qui définit l'adresse source dans **Original Packet (Paquet d'origine)** > **Source Address (Adresse source)**.

- **Type** = **Dynamic** (dynamique).

- **PAT Pool Translated Address** (Adresse traduite du pool PAT). Sélectionnez un objet réseau qui définit le réseau de pool PAT.
- **Enable Block Allocation** (Activer l'allocation de blocs).

d) Cliquez sur **OK**.

Configurer la PAT par session ou la PAT multi-session (version 9.0(1) et versions ultérieures)

Par défaut, tout le trafic PAT TCP et tout le trafic DNS UDP utilisent une PAT par session. Pour utiliser la PAT multi-session pour le trafic, vous pouvez configurer des règles PAT par session : une règle d'autorisation utilise la PAT par session, et une règle de refus utilise la PAT multi-session.

La PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multi-sessions doivent être transférées au nœud de contrôle et détenues par celui-ci. À la fin d'une session PAT par session, l'ASA envoie une réinitialisation et supprime immédiatement le xlate. Cette réinitialisation force le nœud terminal à libérer immédiatement la connexion, évitant l'état TIME_WAIT. La PAT multi-session, en revanche, utilise le délai d'expiration PAT, par défaut de 30 secondes.

Pour le trafic « hit-and-run », comme HTTP ou HTTPS, la PAT par session peut augmenter considérablement le débit de connexion pris en charge par une adresse. Sans la PAT par session, le débit de connexion maximal pour une adresse pour un protocole IP est d'environ 2 000 par seconde. Avec la PAT par session, le débit de connexion pour une adresse pour un protocole IP est de 65 535/*average-lifetime*.

Pour le trafic qui peut bénéficier de la PAT multi-session, comme H.323, SIP ou Skinny, vous pouvez désactiver la PAT par session en créant une règle de refus par session. Toutefois, si vous souhaitez également utiliser la PAT par session pour les ports UDP utilisés par ces protocoles, vous devez créer les règles d'autorisation pour ceux-ci.

Avant de commencer

Par défaut, les règles suivantes sont installées :

- Autoriser le protocole TCP depuis n'importe quelle adresse (IPv4 et IPv6) vers n'importe quelle adresse (IPv4 et IPv6).
- Autoriser le protocole UDP depuis n'importe quelle adresse (IPv4 et IPv6) vers le port de domaine.

Ces règles ne s'affichent pas dans le tableau.

Vous ne pouvez pas supprimer ces règles, et elles existent toujours après toute règle créée manuellement. Comme les règles sont évaluées dans l'ordre, vous pouvez remplacer les règles par défaut. Par exemple, pour annuler complètement ces règles, vous pouvez ajouter les éléments suivants :

- Refuser le protocole TCP depuis n'importe quelle adresse (IPv4 et IPv6) vers n'importe quelle adresse (IPv4 et IPv6).
- Refuser le protocole UDP depuis n'importe quelle adresse (IPv4 et IPv6) vers le port de domaine.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Per-Session NAT Rules (Règles NAT par session)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Add Per-Session NAT Rule (Ajouter une règle NAT par session)**.
- Sélectionnez une règle et cliquez sur **Edit** (Modifier).

Étape 3 Configurez la règle :

- **Action** : cliquez sur **Permit** (Autoriser) ou **Deny** (Refuser). Une règle d'autorisation utilise la PAT par session ; une règle de refus utilise la PAT multi-session.
- Source : spécifiez l'adresse source en tapant une adresse ou en cliquant sur le bouton **...** pour choisir un objet. Pour le service, sélectionnez UDP ou TCP. Vous pouvez éventuellement préciser un port source, bien que, normalement, vous ne précisiez que le port de destination. Saisissez UDP/*port* ou TCP/*port*, ou cliquez sur le bouton**...** pour sélectionner une valeur commune ou un objet.
- Destination : spécifiez l'adresse de destination, soit en saisissant une adresse, soit en cliquant sur le bouton **...** pour choisir un objet. Pour le service, sélectionnez UDP ou TCP; il doit correspondre au service source. Vous pouvez éventuellement préciser un port de destination. Saisissez UDP/*port* ou TCP/*port*, ou cliquez sur le bouton**...** pour sélectionner une valeur commune ou un objet. Vous pouvez utiliser les opérateurs != (non égal à), > (supérieur à), < (inférieur à) ou spécifier une plage à l'aide d'un tiret, par exemple, 100-200.

Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

NAT statique

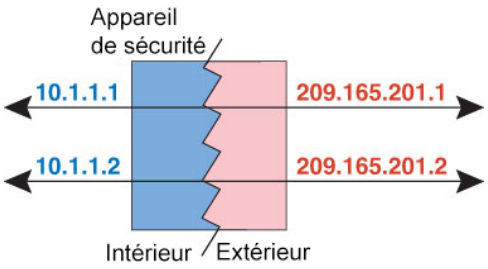
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

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 5 : NAT statique



Remarque Vous pouvez désactiver la bidirectionnalité si vous le souhaitez.

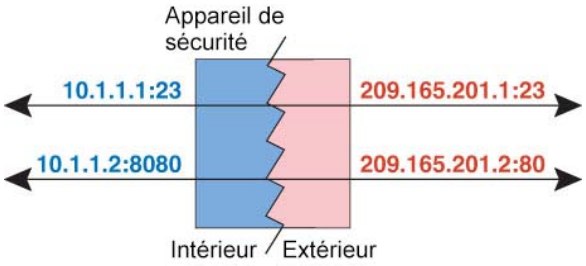
NAT statique avec traduction de port

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 6 : 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 twice NAT (NAT en double), 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). Pour plus de détails sur la façon de configurer cet exemple, consultez Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port).

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

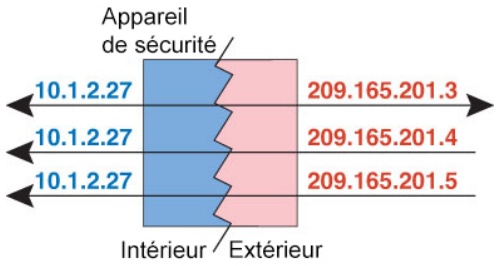
Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec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

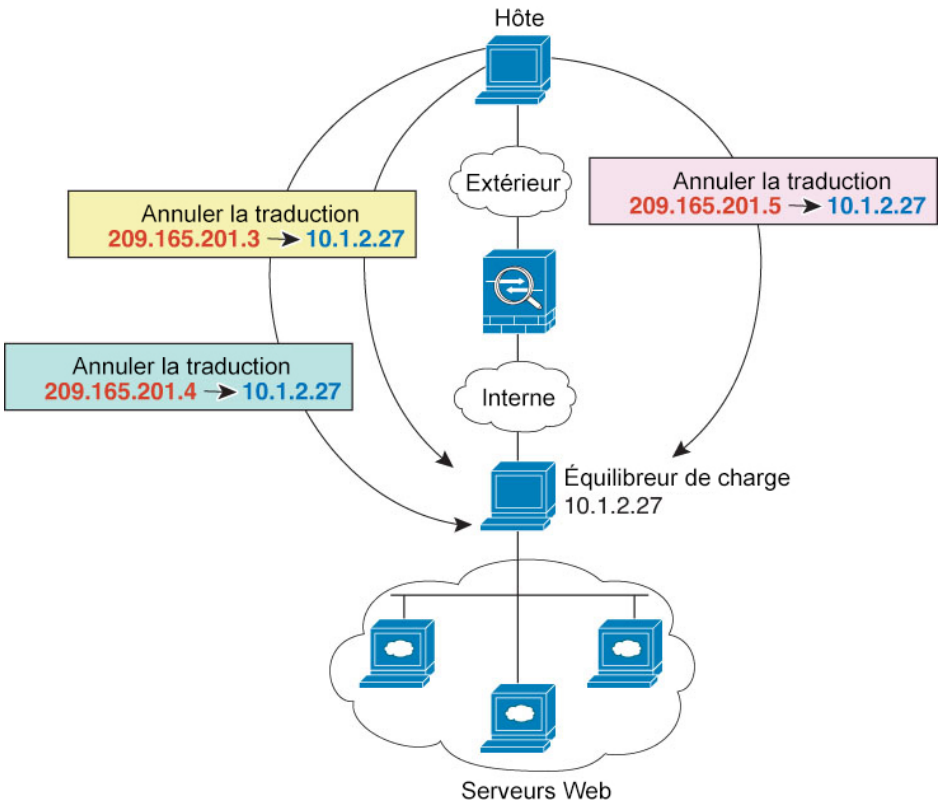
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction entre l'adresse IP de l'hôte réel et la première adresse IP mappée est techniquement la seule traduction bidirectionnelle.

Illustration 7 : 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. Pour plus de détails sur la façon de configurer cet exemple, consultez Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs) .

Illustration 8 : Exemple de NAT statique un vers plusieurs



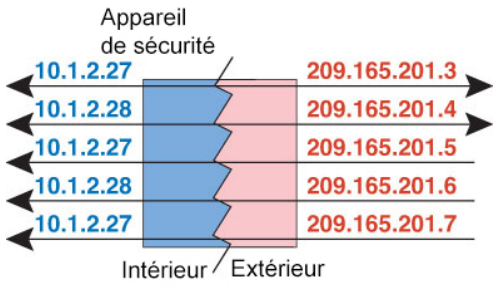
Autres scénarios de mappage (non recommandés)

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 9 : NAT statique quelques-uns vers plusieurs

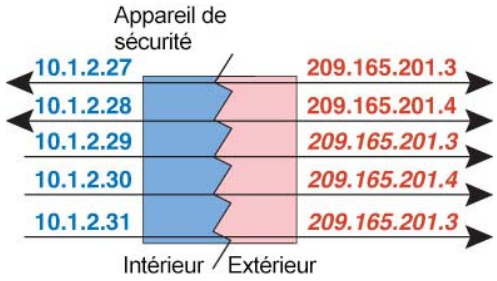


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un 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, protocole) 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 10 : 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 d'objet réseau statique ou la NAT statique avec traduction de port

Cette section décrit comment configurer une règle de NAT statique à l'aide de la NAT d'objet réseau.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

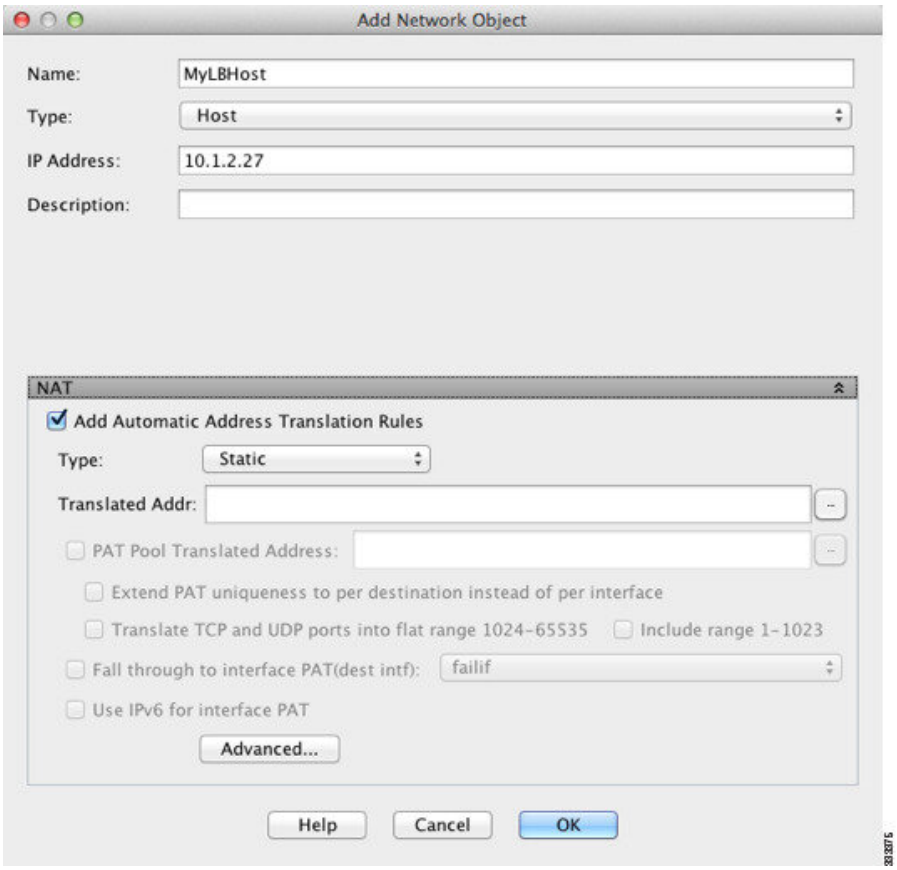
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

- **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
- **Type** : hôte, réseau ou plage.
- **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

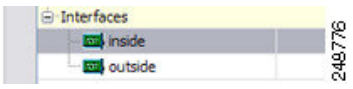
Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Static** (Statique).



Étape 6 Dans le champ Adresse traduite, spécifiez l'adresse IP mappée comme suit. 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. Pour en savoir plus, consultez NAT statique, à la page 46.

- Tapez une adresse IP d'hôte. Il s'agit d'un mappage un à un pour les objets hôtes. Pour les objets de sous-réseau, le même masque réseau est utilisé pour l'adresse de l'hôte en ligne, et vous obtenez des traductions un à un pour les adresses dans le sous-réseau de l'hôte en ligne mappé. Pour les objets de plage, l'adresse mappée comprend le même nombre d'hôtes que dans l'objet de plage, en commençant par l'adresse d'hôte mappée. Par exemple, si l'adresse réelle est définie comme une plage comprise entre 10.1.1.1 et 10.1.1.6, et que vous spécifiez 172.20.1.1 comme adresse mappée, la plage mappée inclura 172.20.1.1 à 172.20.1.6. Pour les traductions NAT46 ou NAT66, il peut s'agir d'une adresse réseau IPv6.
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau (ou créez-en un nouveau). Pour effectuer un mappage un à un pour une plage d'adresses IP, sélectionnez un objet qui contient une plage avec le même nombre d'adresses.
- (Pour NAT statique avec traduction de port uniquement.) Tapez un nom d'interface ou cliquez sur le bouton de navigation, puis choisissez une interface dans la boîte de dialogue Parcourir les adresses traduites. Vous ne pouvez pas sélectionner une interface membre d'un groupe de ponts.



Pour utiliser l'adresse d'interface IPv6, vous devez également cocher la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface). Assurez-vous de cliquer également sur **Advanced**

(Avancé) et de configurer une traduction de port de service. (Vous ne pouvez pas spécifier d'interface en mode transparent.)

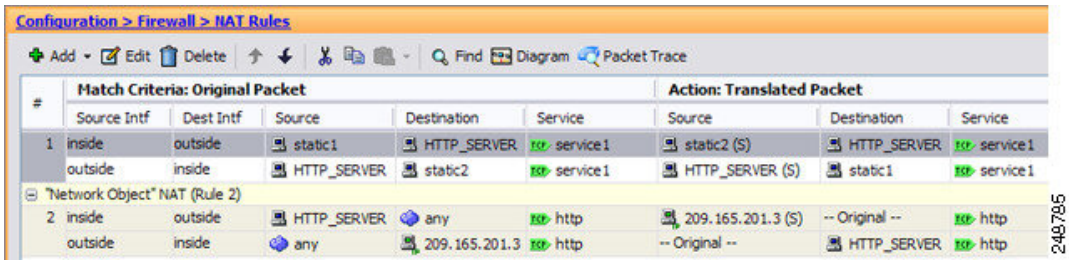
Étape 7 (Facultatif) Pour NAT46, cochez **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un). Pour NAT46, spécifiez un à un pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, et ainsi de suite. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.

Étape 8 (Facultatif) Cliquez sur **Avancé**, configurez les options suivantes dans la boîte de dialogue des paramètres NAT avancés, puis cliquez sur **OK**.

- **Traduire les réponses DNS pour la règle**—Traduit l'adresse IP dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT pour de plus amples renseignements.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Pour en savoir plus sur les conditions qui peuvent nécessiter la désactivation du proxy ARP, consultez Adresses mappées et routage.
- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.
- **Service** : configure la NAT statique avec traduction de port. Choisissez le protocole, puis saisissez le port réel et le port mappé. Vous pouvez utiliser des numéros de port ou un nom de port bien connu tel que http.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Comme les règles statiques sont bidirectionnelles (permettant l'initiation vers et depuis l'hôte réel), le tableau NAT Rules (Règles NAT) affiche deux lignes pour chaque règle statique, une pour chaque direction.



Configurer la NAT statique Twice ou la NAT statique avec traduction de port

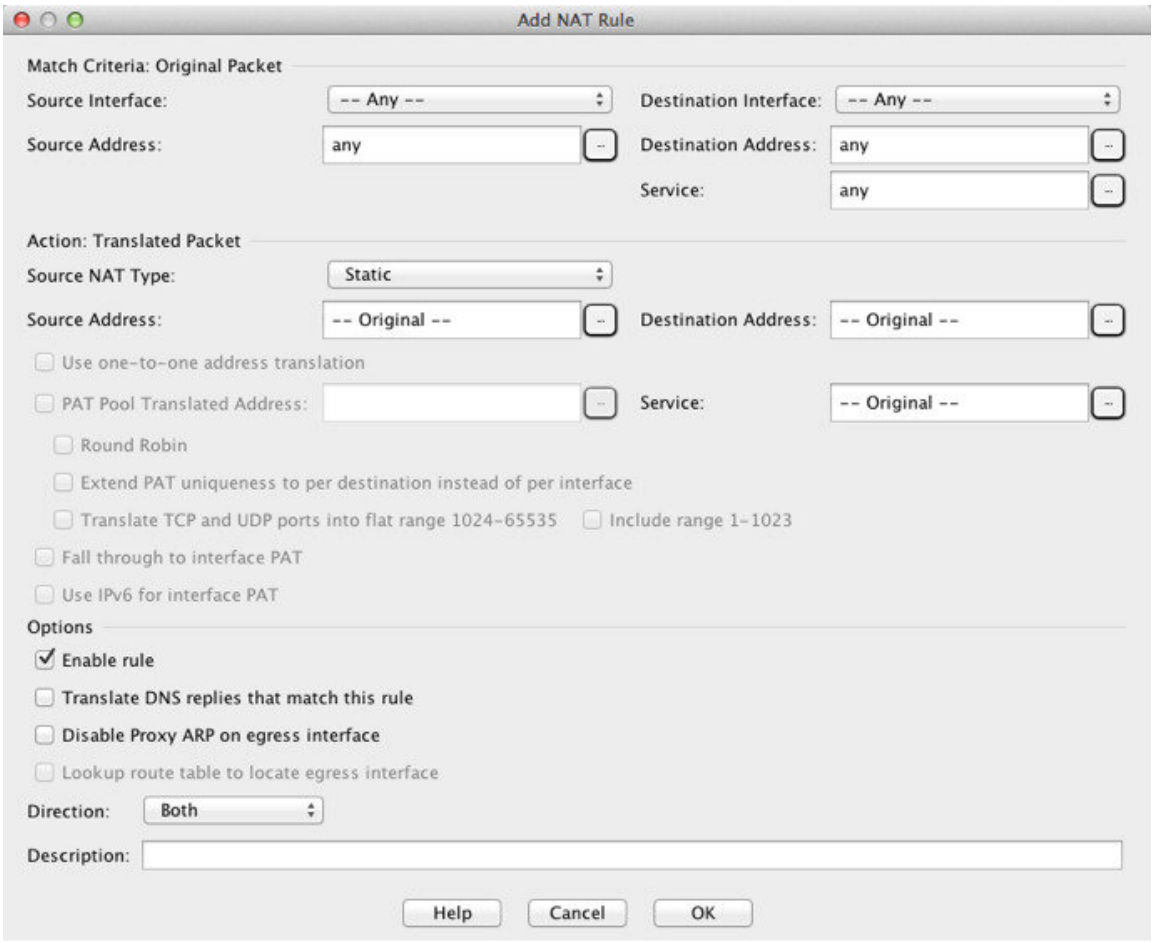
Cette section décrit comment configurer une règle de NAT statique à l'aide de la NAT Twice.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

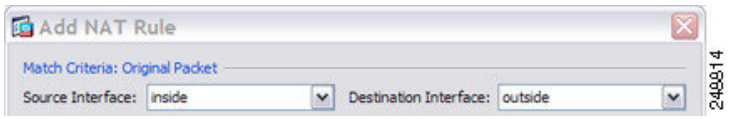


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est n'importe quelle interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts; « any » n'inclut pas ces interfaces.

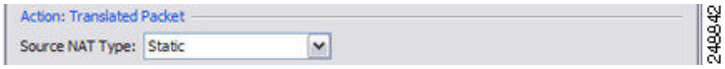
a) Dans la liste déroulante **Critères de correspondance : Paquet original > Interface source**, choisissez l'interface source.

b) Dans la liste déroulante **Correspondance des critères : paquet d'origine > interface de destination**, choisissez l'interface de destination.

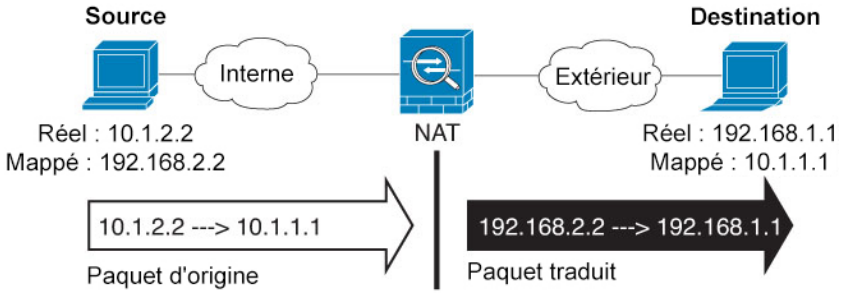


Étape 3 Choisissez **Static** (Statique) dans la liste déroulante **Action > Translated Packet** > **Source NAT Type** (Action > Paquet traduit > Type de NAT source). Statique est le paramètre par défaut.

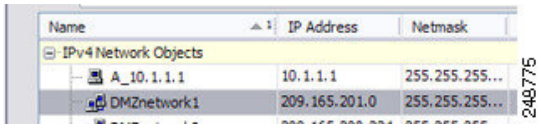
Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6; c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (l'*adresse source réelle* et l'*adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **Any**, mais n'utilisez pas cette option, sauf pour la NAT d'identité.



b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine.

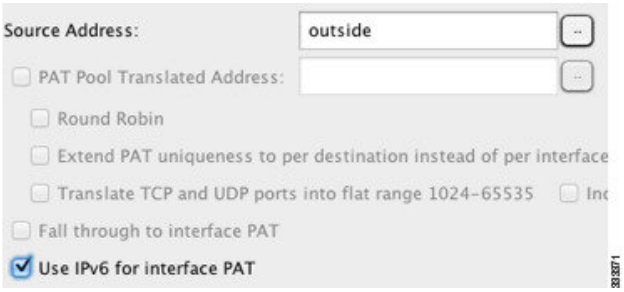
Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse. Vous pouvez configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action : Paquet traduit > Adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source traduite.

Pour la NAT statique, le mappage est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.

Pour la NAT d'interface statique avec traduction de port, vous pouvez préciser l'interface au lieu d'un objet ou d'un groupe de réseau pour l'adresse mappée. Si vous souhaitez utiliser l'adresse IPv6 de l'interface, cochez la case **Utiliser IPv6 pour la PAT de l'interface**. Vous ne pouvez pas sélectionner un membre d'interface de groupe de pont.



Pour en savoir plus, consultez NAT statique avec traduction de port, à la page 47. Consultez Directives pour la NAT, à la page 7 pour en savoir plus sur les adresses IP mappées non autorisées.

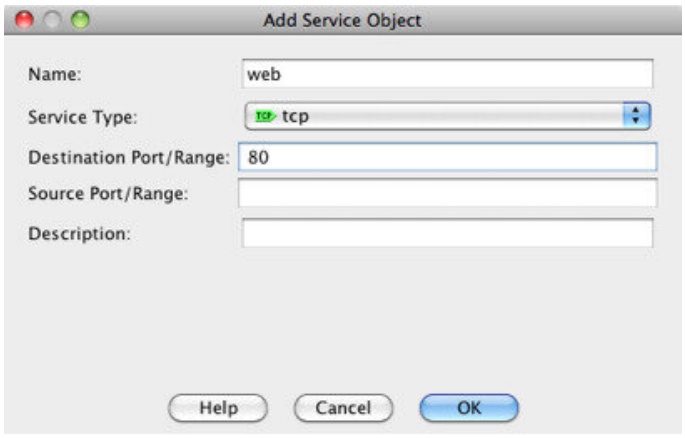
b) (Facultatif) Pour **l'action : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe de réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

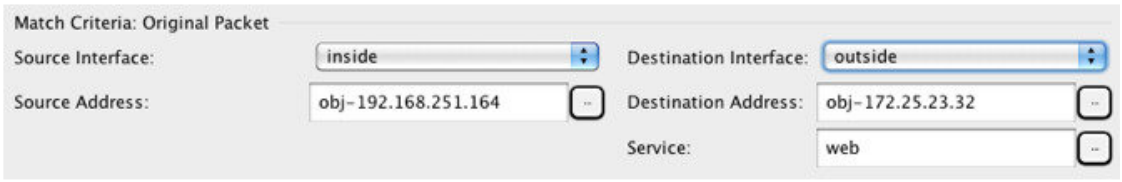
Étape 6 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

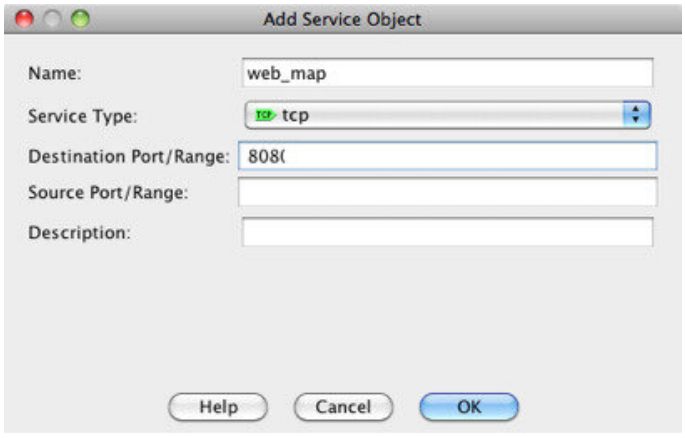
- Déterminez le port source ou de destination du paquet d'origine (le *port source réel* **ou** le *port de destination mappé*). Pour **les critères de correspondance : Paquet d'origine > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports ou créez un nouvel objet dans la boîte de dialogue Parcourir le service d'origine.
- Identifiez le port source ou de destination du paquet traduit (le *port source mappé* **ou** le *port de destination réel*). Pour **Action : Paquet traduit > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie des ports, ou créez un nouvel objet à partir de la boîte de dialogue Parcourir le service traduit.

Un objet de service peut contenir à la fois un port source et un port de destination. Vous devez préciser *soit* le port source *soit* le port de destination pour les objets de service réels et mappés. Vous ne devez spécifier *les deux* ports source et de destination que si votre application utilise un port source fixe (comme certains serveurs DNS); mais les ports sources fixes sont rares. Dans le cas rare où vous spécifiez les deux ports source et de destination dans l'objet, l'objet du service de paquets d'origine contient le port source réel/port de destination mappé; l'objet de service de paquets traduit contient le port source mappé/port de destination réel. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (par exemple, TCP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés. L'opérateur "pas égal" (**!=**) n'est pas pris en charge.

Par exemple :



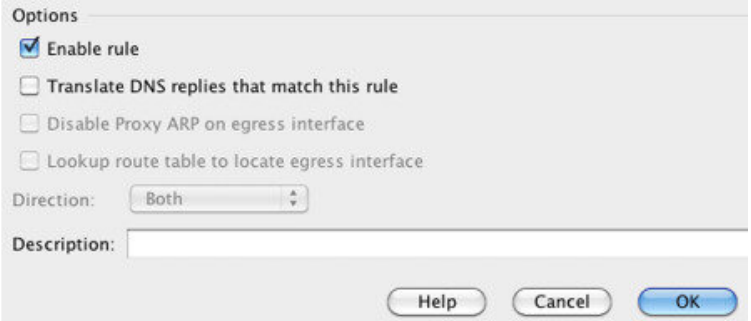






Étape 7 (Facultatif) Pour NAT46, cochez la case **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un). Pour NAT46, spécifiez un à un pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, et ainsi de suite. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.

Étape 8 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement.) **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle) : réécrit l'enregistrement DNS A dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer la modification DNS si vous configurez une adresse de destination. Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT pour de plus amples renseignements.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Consultez Adresses mappées et routage pour de plus amples renseignements.
- **Direction** : pour rendre la règle unidirectionnelle, choisissez **Unidirectional** (Unidirectionnel). La valeur par défaut est les deux. Rendre la règle unidirectionnelle empêche les adresses de destination d'établir des connexions avec les adresses réelles.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

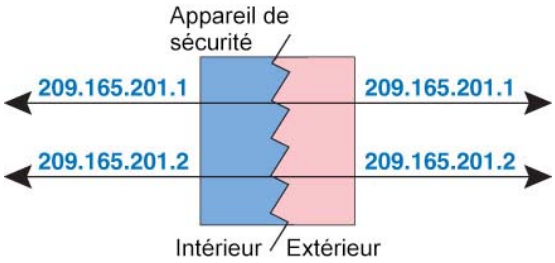
Étape 9 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

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 ce réseau vers lui-même. La NAT d'identité est nécessaire pour le VPN d'accès à distance, lorsque vous devez exclure le trafic client de la NAT.

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

Illustration 11 : NAT d'identité



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

Configurer la NAT d'objet de réseau d'identité

Cette section décrit comment configurer une règle d'identité NAT à l'aide de la NAT d'objet réseau.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

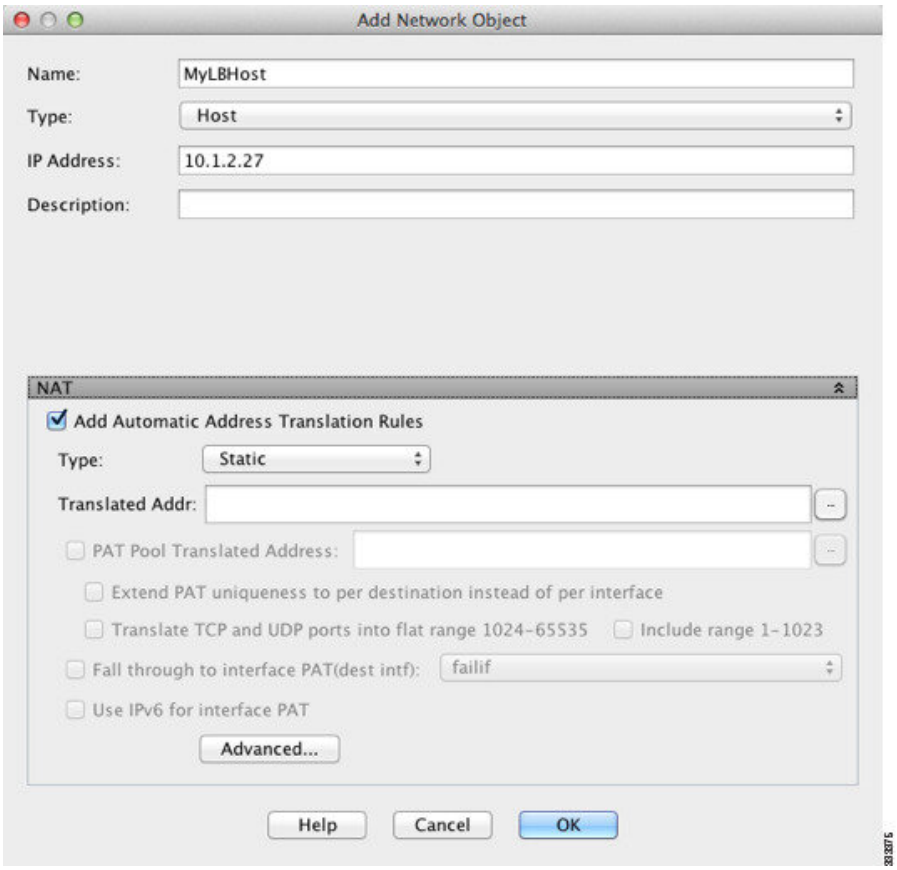
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

- **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
- **Type** : hôte, réseau ou plage.
- **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Static** (Statique).



Étape 6 Dans l'adresse traduite , effectuez l'une des opérations suivantes :

- Pour les objets hôtes, saisissez la même adresse. Pour les objets de plage, saisissez la première adresse dans la plage réelle (le même nombre d'adresses dans la plage sera utilisée). Pour les objets de sous-réseau, saisissez n'importe quelle adresse dans le sous-réseau réel (toutes les adresses du sous-réseau seront utilisées).
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau (ou créez-en un nouveau). Utilisez cette option lors de la configuration de la NAT d'identité pour une plage d'adresses.

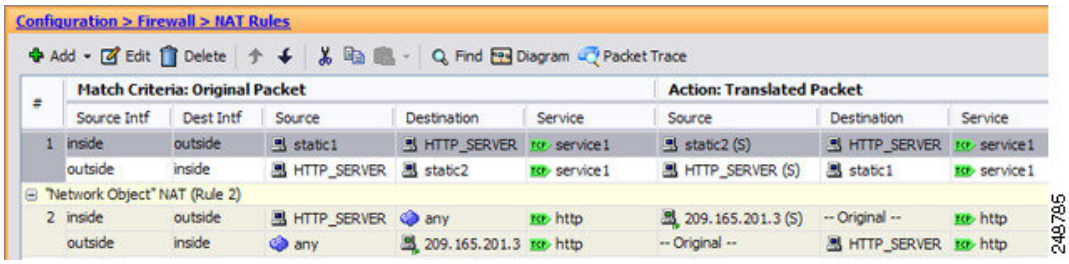
Étape 7 (Facultatif) Cliquez sur **Avancé**, configurez les options suivantes dans la boîte de dialogue des paramètres NAT avancés, puis cliquez sur **OK**.

- **Translate DNS replies for rule** (Traduire les réponses DNS pour la règle) : ne configurez pas cette option pour la NAT d'identité.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Pour en savoir plus sur les conditions qui peuvent nécessiter la désactivation du proxy ARP, consultez Adresses mappées et routage.
- (Mode routé ; interfaces précisées.) **Lookup route table to locate egress interface** (Rechercher la table de routage pour localiser l'interface de sortie) : détermine l'interface de sortie à l'aide d'une recherche de routage au lieu d'utiliser l'interface spécifiée dans la commande NAT. Consultez Détermination de l'interface de sortie pour de plus amples renseignements.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.
- **Service** : ne configurez pas cette option pour la NAT d'identité.

Étape 8 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Comme les règles statiques sont bidirectionnelles (permettant l'établissement de connexions vers et à partir de l'hôte réel), le tableau NAT Rules (Règles NAT) affiche deux lignes pour chaque règle statique, une pour chaque direction, sauf si vous sélectionnez l'option de recherche de routage.



Configurer la NAT d'identité Twice

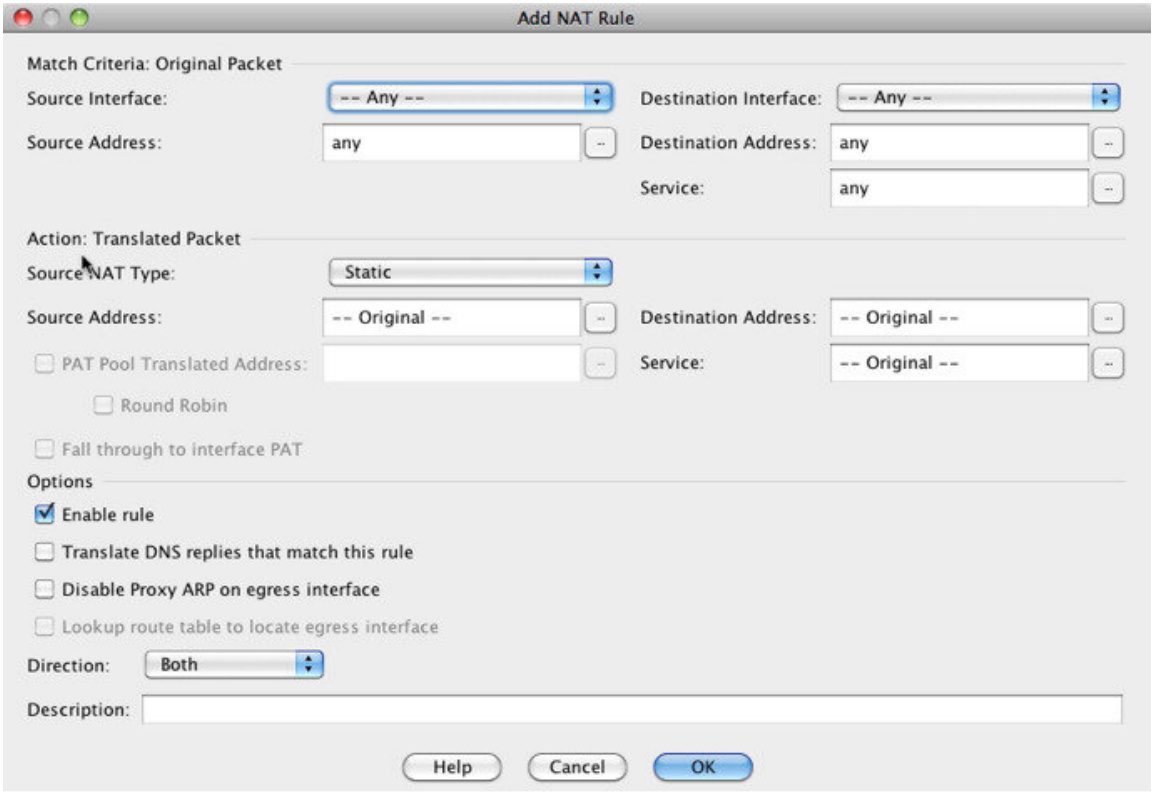
Cette section décrit comment configurer une règle de NAT d'identité à l'aide de la NAT Twice.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

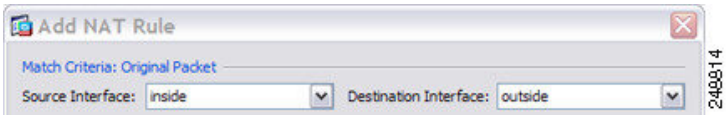


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routage, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

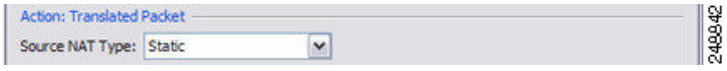
a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Correspondance des critères : paquet d'origine > interface de destination**, choisissez l'interface de destination.



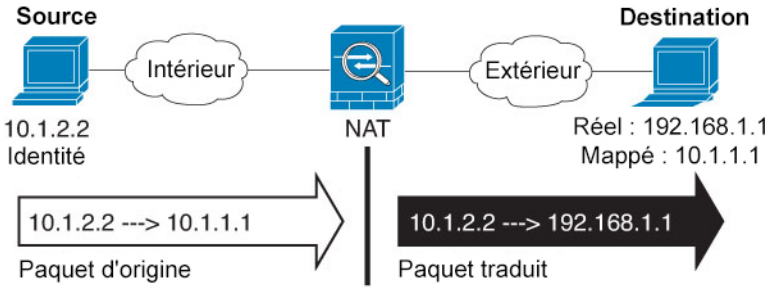
Étape 3 Choisissez **Static** (Statique) dans la liste déroulante **Action > Translated Packet** > **Source NAT Type** (Action > Paquet traduit > Type de NAT source). Statique est le paramètre par défaut.

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.

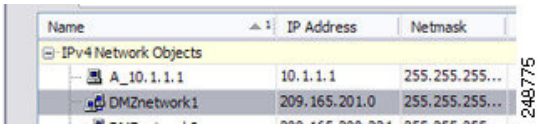


Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination*

mappée). 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.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **Any**; Utilisez uniquement cette option lorsque vous définissez l'adresse mappée sur **Any**.



b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 4.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface. Si vous spécifiez une interface, veillez à configurer une traduction de service. Pour en savoir plus, consultez NAT statique avec traduction de port, à la page 47.

Étape 5 Identifiez les adresses de paquets traduites, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination (l'*adresse source mappée* et l'*adresse de destination réelle*).

a) Pour **Action: Translated Packet > Source Address** (Action : Paquet traduit > Adresse source), cliquez sur le bouton de navigation et choisissez le même objet ou groupe réseau dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite) que vous avez choisi pour l'adresse source réelle. Utilisez **any** si vous avez spécifié **any** pour l'adresse réelle.

b) Pour **les critères de correspondance : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

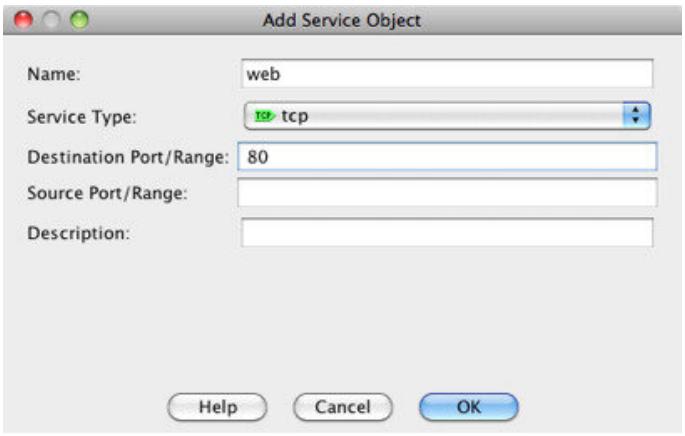
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 46. Consultez Directives pour la NAT, à la page 7 pour en savoir plus sur les adresses IP mappées non autorisées.

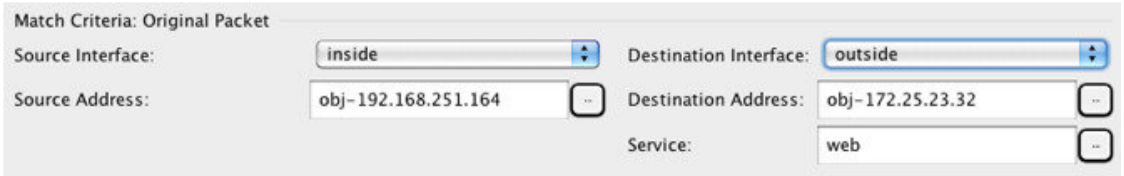
Étape 6 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

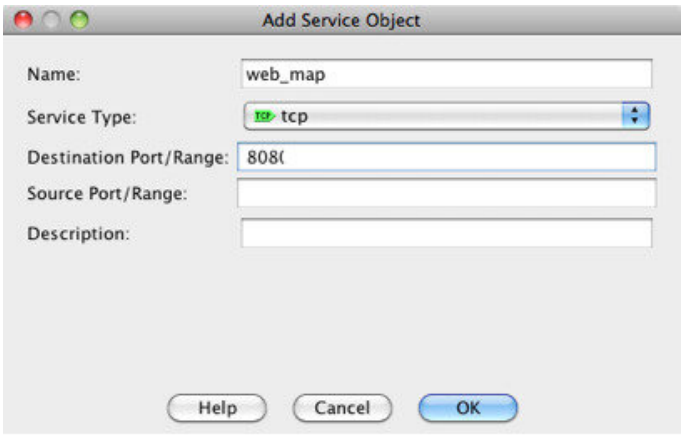
- Déterminez le port source ou de destination du paquet d'origine (le *port source réel* **ou** le *port de destination mappé*). Pour **les critères de correspondance : Paquet d'origine > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports ou créez un nouvel objet dans la boîte de dialogue Parcourir le service d'origine.
- Identifiez le port source ou de destination du paquet traduit (le *port source mappé* **ou** le *port de destination réel*). Pour **Action : Paquet traduit > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie des ports, ou créez un nouvel objet à partir de la boîte de dialogue Parcourir le service traduit.

Un objet de service peut contenir à la fois un port source et un port de destination. Vous devez préciser *soit* le port source *soit* le port de destination pour les objets de service réels et mappés. Vous ne devez spécifier *les deux* ports source et de destination que si votre application utilise un port source fixe (comme certains serveurs DNS) ; mais les ports sources fixes sont rares. Dans le cas rare où vous spécifiez les deux ports source et de destination dans l'objet, l'objet du service de paquets d'origine contient le port source réel/port de destination mappé; l'objet de service de paquets traduit contient le port source mappé/port de destination réel. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :









Étape 7 (Facultatif) Configurez les options de NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement.) **Traduire les réponses DNS qui correspondent à cette règle** : bien que cette option soit disponible si vous ne configurez pas d'adresse de destination, elle ne s'applique pas à la NAT d'identité, car vous traduisez l'adresse en elle-même, de sorte que la réponse DNS ne nécessite pas de modification.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Consultez Adresses mappées et routage pour de plus amples renseignements.
- (Mode routé ; interfaces précisées.) **Lookup route table to locate egress interface** (Rechercher la table de routage pour localiser l'interface de sortie) : détermine l'interface de sortie à l'aide d'une recherche de routage au lieu d'utiliser l'interface spécifiée dans la commande NAT. Consultez Détermination de l'interface de sortie pour de plus amples renseignements.
- **Direction** : pour rendre la règle unidirectionnelle, choisissez **Unidirectional** (Unidirectionnel). La valeur par défaut est Both (Les deux). Rendre la règle unidirectionnelle empêche le trafic d'établir des connexions avec les adresses réelles. Vous pouvez utiliser ce paramètre à des fins de test.

- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 8 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Surveillance de la NAT

Vous pouvez afficher les graphiques liés à la NAT à partir des pages suivantes :

- **Monitoring (Surveillance) > Properties (Propriétés) > Connection Graphs (Graphiques de connexion) > Xlates** : sélectionnez le graphique Xlate Utilization (Utilisation de Xlate) pour afficher les xlates en cours d'utilisation et les plus utilisés. Cela équivaut à la commande **show xlate**.
- **Monitoring (Surveillance) > Properties (Propriétés) > Connection Graphs (Graphiques de connexion) > Perfmon** : sélectionnez le graphique Xlate Perfmon (Perfmon Xlate) pour afficher les informations sur les performances de la NAT. Cela équivaut aux informations xlate de la commande **show perfmon**.

Historique de la NAT

Nom de la caractéristique	Versions de plateforme	Description
NAT d'objet réseau	8.3(1)	Configure la NAT pour une ou plusieurs adresses IP d'objet réseau. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT); Configuration (Configuration) > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)
NAT Twice	8.3(1)	NAT Twice vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle. Nous avons modifié l'écran suivant : Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT).

Nom de la caractéristique	Versions de plateforme	Description
Recherche de routage et d'ARP configurable pour la NAT d'identité	8.4(2)/8.5(1)	Dans les versions précédentes de la NAT d'identité, le proxy ARP était désactivé et une recherche de routage était toujours utilisée pour déterminer l'interface de sortie. Vous ne pouviez pas configurer ces paramètres. Dans les versions 8.4(2) et ultérieures, le comportement par défaut de la NAT d'identité a été modifié pour correspondre à celui des autres configurations NAT statiques : le proxy ARP est activé et la configuration NAT détermine l'interface de sortie (si spécifiée) par défaut. Vous pouvez laisser ces paramètres tels quels, ou les activer ou les désactiver discrètement. Notez que vous pouvez désormais désactiver le proxy ARP pour la NAT statique normale. Pour les configurations antérieures à la version 8.3, la migration des règles d'exemption de NAT (la commande nat **0 access-list**) vers la version 8.4(2) et les versions ultérieures comprend désormais les mots-clés suivants pour désactiver le proxy ARP et utiliser une recherche de routage : **no-proxy-arp** et **route-lookup**. Le mot-clé **unidirectionnal** qui a été utilisé pour la migration vers les versions 8.3(2) et 8.4(1) n'est plus utilisé pour la migration. Lors de la mise à niveau vers la version 8.4(2) à partir des versions 8.3(1), 8.3(2) et 8.4(1), toutes les configurations NAT d'identité incluront désormais les mots clés **no-proxy-arp** et **route-lookup**, pour maintenir les fonctionnalités existantes. Le mot clé **unidirectional** est supprimé. Nous avons modifié les écrans suivant : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau) > Advanced NAT Settings (Paramètres NAT avancés); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT).

Nom de la caractéristique	Versions de plateforme	Description
Affectation d'adresses de pool PAT et round-robin	8.4(2)/8.5(1)	Vous pouvez désormais spécifier un pool d'adresses PAT au lieu d'une adresse unique. Vous pouvez également éventuellement activer l'affectation round-robin des adresses PAT au lieu d'utiliser d'abord tous les ports d'une adresse PAT avant d'utiliser l'adresse suivante dans le regroupement. Ces fonctionnalités aident à éviter qu'un grand nombre de connexions à partir d'une seule adresse PAT ne semble faire partie d'une attaque DoS et facilitent la configuration d'un grand nombre d'adresses PAT. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT).
L'allocation de pool PAT round-robin utilise la même adresse IP pour les hôtes existants	8.4(3)	Lors de l'utilisation d'un pool PAT avec affectation round-robin, si un hôte a une connexion existante, les connexions suivantes de cet hôte utiliseront la même adresse IP PAT si des ports sont disponibles. Nous n'avons pas modifié d'écrans. *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*
Plage uniforme de ports PAT pour un pool PAT	8.4(3)	S'il est disponible, le numéro de port source réel est utilisé pour le port mappé. 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 1 024 à 65 535. Par conséquent, les ports inférieurs à 1024 ont seulement un petit pool PAT. Si une grande partie du trafic utilise les plages de ports inférieures, lors de l'utilisation d'un pool PAT, vous pouvez désormais spécifier une plage uniforme de ports à utiliser au lieu des trois niveaux de taille inégal: 1024 à 65 535 ou 1 à 65 535. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*

Nom de la caractéristique	Versions de plateforme	Description
PAT étendu pour un pool PAT	8.4(3)	Chaque adresse IP PAT permet jusqu'à 65 535 ports. Si 65 535 ports ne fournissent pas assez de traductions, vous pouvez maintenant activer la PAT étendue pour un pool PAT. 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. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*

Nom de la caractéristique	Versions de plateforme	Description
Règles de NAT automatiques pour traduire l'adresse IP locale d'un homologue de VPN en adresse IP réelle de l'homologue	8.4(3)	Dans de rares cas, vous pouvez utiliser l'adresse IP réelle d'un homologue VPN sur le réseau interne au lieu d'une adresse IP locale attribuée. Normalement avec le VPN, l'homologue reçoit une adresse IP locale attribuée pour accéder au réseau interne. Cependant, vous pouvez traduire l'adresse IP locale en adresse IP publique réelle de l'homologue si, par exemple, vos serveurs internes et la sécurité du réseau sont basés sur l'adresse IP réelle de l'homologue. Vous pouvez activer cette fonctionnalité sur une interface par groupe de tunnels. Les règles de NAT d'objet sont ajoutées et supprimées dynamiquement lorsque la session VPN est établie ou déconnectée. Vous pouvez afficher les règles à l'aide de la commande **show nat** . En raison de problèmes de routage, nous ne recommandons pas l'utilisation de cette fonctionnalité, sauf si vous savez que vous en avez besoin; communiquez avec le centre d'assistance technique Cisco pour confirmer la compatibilité de la fonctionnalité avec votre réseau. Voir les limitations suivantes : • Ne prend en charge que Cisco IPsec et Secure Client. • Le trafic de retour vers les adresses IP publiques doit être acheminé vers l'ASA pour que la politique de NAT et la politique de VPN puissent être appliquées. • Ne prend pas en charge l'équilibrage de la charge (en raison de problèmes de routage). • Ne prend pas en charge l'itinérance (modification d'adresse IP publique). ASDM ne prend pas en charge cette commande; entrez la commande à l'aide de Command Line Tool (Outil de ligne de commande).
Prise en charge de la NAT pour IPv6	9.0(1)	La NAT prend désormais en charge le trafic IPv6 ainsi que la traduction entre IPv4 et IPv6. La traduction entre IPv4 et IPv6 n'est pas prise en charge en mode transparent. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Group (Objets/groupe réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT).
Prise en charge de la NAT pour les recherches DNS inversées	9.0(1)	La NAT prend maintenant en charge la traduction de l'enregistrement DNS PTR pour les recherches DNS inversées lors de l'utilisation de la NAT IPv4, de la NAT IPv6 et de NAT64 avec l'inspection DNS activée pour la règle NAT.

Nom de la caractéristique	Versions de plateforme	Description
PAT par session	9.0(1)	La fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque unité membre de détenir des connexions PAT ; les connexions PAT multi-session doivent être transférées et détenues par l'unité de contrôle. À la fin d'une session PAT par session, l'ASA envoie une réinitialisation et supprime immédiatement le xlate. Cette réinitialisation force le nœud terminal à libérer immédiatement la connexion, en évitant l'état TIME_WAIT. La PAT multi-session, en revanche, utilise le délai d'expiration PAT, par défaut de 30 secondes. Pour le trafic « hit-and-run », comme HTTP ou HTTPS, la fonctionnalité par session peut augmenter considérablement le débit de connexion pris en charge par une adresse. Sans la fonctionnalité par session, le débit de connexion maximal pour une adresse pour un protocole IP est d'environ 2 000 par seconde. Avec la fonctionnalité par session, le débit de connexion pour une adresse pour un protocole IP est de 65535/*average-lifetime* . Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent une xlate PAT par session. Pour le trafic qui nécessite une PAT multi-session, comme H.323, SIP ou Skinny, vous pouvez désactiver la PAT par session en créant une règle de refus par session. Nous avons introduit l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Per-Session NAT Rules (Règles NAT par session).
Modèle de validation transactionnelle sur le moteur de règles NAT	9.3(1)	Lorsque cette option est activée, une mise à jour de règle NAT est appliquée une fois la compilation de la règle terminée; sans affecter la performance de correspondance de la règle. Nous avons ajouté la NAT à l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles).
Améliorations de la NAT de niveau opérateur	9.5(1)	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). Nous avons ajouté la commande suivante : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)**. Nous avons ajouté les boîtes de dialogue **Enable Block Allocation** (Activer l'allocation de blocage) pour l'objet NAT et la NAT Twice.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de la NAT pour SCTP	9.5(2)	Vous pouvez maintenant spécifier les ports SCTP dans les règles NAT des objets réseau statiques. L'utilisation de SCTP dans la NAT Twice statique n'est pas recommandée. La NAT/PAT dynamique ne prend pas en charge SCTP. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **NAT** Add/Edit static network object NAT rule (Ajouter/Modifier une règle NAT d'objet réseau statique), boîte de dialogue **Advanced NAT Settings** (Paramètres NAT avancés).
Journalisation provisoire pour l'allocation de bloc de ports NAT.	9.12(1)	Lorsque vous activez l'allocation de bloc de ports pour la NAT, le système génère des messages de journal système lors de la création et de la suppression d'un bloc de port. Si vous activez la journalisation provisoire, le système génère le message 305017 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. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)** .

Nom de la caractéristique	Versions de plateforme	Description
Modifications apportées à l'attribution d'adresses PAT dans la mise en grappe. L'option **flat** de l'ensemble PAT est désormais activée par défaut et n'est pas configurable.	9.15(1)	La façon dont les adresses PAT sont distribuées aux membres d'une grappe est modifiée. Auparavant, les adresses étaient distribuées aux membres de la grappe, de sorte que votre ensemble de PAT avait besoin d'au moins une adresse par membre de la grappe. Désormais, l'unité de contrôle divise plutôt chaque adresse de pool PAT en blocs de ports de taille égale et les répartit entre les membres de la grappe. Chaque membre dispose de blocs de ports pour les mêmes adresses PAT. Ainsi, vous pouvez réduire la taille de l'ensemble PAT, même à une seule adresse IP, en fonction du nombre de connexions généralement nécessaires à PAT. Les blocs de ports sont attribués en blocs de port 512 uniquement dans la plage de 1024 à 65535. Vous pouvez éventuellement inclure les ports réservés, 1 à 1023, dans cette allocation de bloc lorsque vous configurez les règles de l'ensemble PAT. Par exemple, dans une grappe de 4 nœuds, chaque nœud reçoit 32 blocs, avec lesquels il sera en mesure de gérer 16 384 connexions par adresse IP d'ensemble PAT, contre un seul nœud pouvant gérer les 65 535 connexions par adresse IP d'ensemble PAT. Dans le cadre de ce changement, les regroupements de PAT pour tous les systèmes, qu'ils soient autonomes ou en grappe, utilisent désormais une plage de ports uniforme de 1023 à 65 535. Auparavant, vous pouviez éventuellement utiliser une plage à plat en incluant le mot clé **flat** dans une règle d'ensembles de PAT. Le mot clé **flat** n'est plus pris en charge : l'ensemble de PAT est désormais toujours à plat. Le mot clé **include-reserve** , qui était auparavant un sous-mot clé de **flat** , est maintenant un mot clé indépendant dans la configuration de l'ensemble de PAT. Cette option vous permet d'inclure la plage de 1 à 1 023 ports dans l'ensemble de PAT. Notez que si vous configurez l'allocation de bloc de ports (l'option d'ensemble de PAT **block-allocation**), la taille de votre allocation de bloc est utilisée plutôt que le bloc de 512 ports par défaut. En outre, vous ne pouvez pas configurer la PAT étendue pour un ensemble PAT pour les systèmes d'une grappe. Écrans nouveaux ou modifiés : configuration de l'ensemble de PAT NAT.

Nom de la caractéristique	Versions de plateforme	Description
Nouvelle section 0 pour les règles NAT définies par le système.	9.16(1)	Une nouvelle section 0 a été ajoutée au tableau de règles NAT. Cette section est destinée exclusivement à l'utilisation du système. Toutes les règles NAT dont le système a besoin pour le fonctionnement normal sont ajoutées à cette section, et ces règles ont priorité sur toutes les règles que vous créez. Auparavant, les règles définies par le système étaient ajoutées à la section 1, et les règles définies par l'utilisateur pouvaient interférer avec le bon fonctionnement du système. Vous ne pouvez pas ajouter, modifier ou supprimer les règles de la section 0, mais vous les verrez dans la sortie de la commande **show nat detail** .
Prise en charge de la NAT Twice pour les objets de nom de domaine complet (FQDN) en tant que destination (mappée) de la traduction.	9.17(1)	Vous pouvez utiliser un objet de réseau FQDN, par exemple spécifiant www.exemple.com, comme adresse de destination (mappée) de la traduction dans les règles NAT doubles. Le système configure la règle en fonction de l'adresse IP renvoyée par le serveur DNS.

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.