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?

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

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

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

Les autres fonctions de la NAT comprennent :

- Sécurité : le fait de garder les adresses IP internes masquées détourne les attaques directes.
- Solutions de routage IP : les adresses IP qui se chevauchent ne sont pas un problème lorsque vous utilisez la NAT.

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

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

Principes de base de la NAT

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

Terminologie NAT

Le présent document utilise les termes suivants :

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

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

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

Type de NAT

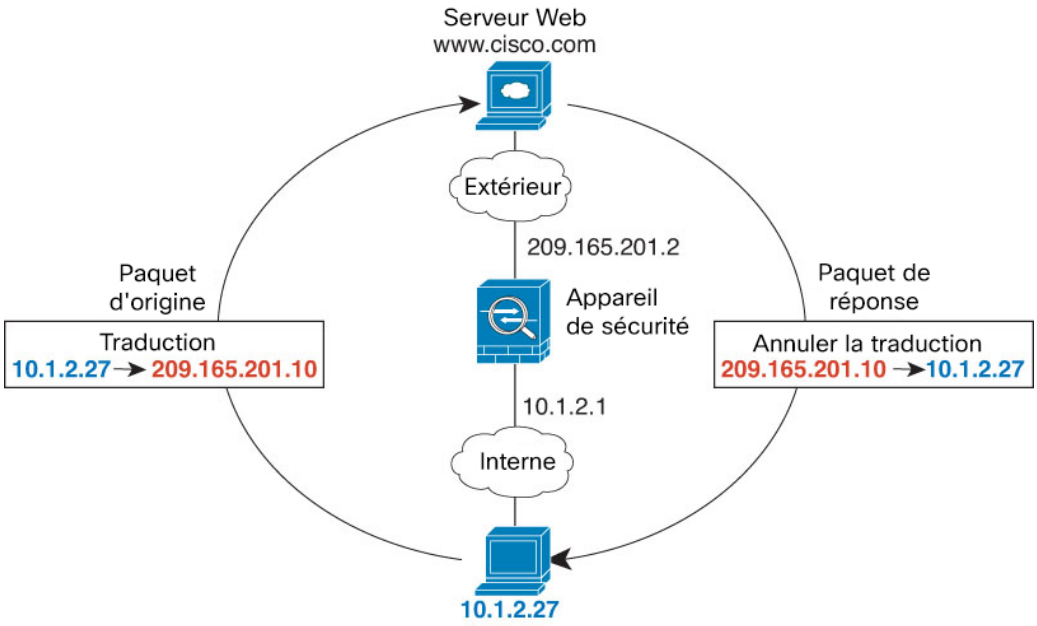
Vous pouvez implémenter la NAT en utilisant les méthodes suivantes :

- NAT dynamique : un groupe d'adresses IP réelles est mappé à un groupe (généralement plus petit) d'adresses IP mappées, selon le principe du premier arrivé, premier servi. Seul l'hôte réel peut initier le trafic. Consultez Traduction d'adresses réseau dynamique, à la page 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 20.
- 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 25.
- 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 34.

NAT en mode routé

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

Illustration 1 : Exemple de NAT : mode routé



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

Auto NAT (NAT automatique) et Manual NAT (NAT manuelle)

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

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

Auto NAT (NAT automatique)

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

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

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

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

Manual NAT (NAT manuelle)

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

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

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

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

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

- Votre définition de l'adresse réelle.

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

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

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

Ordre des règles NAT

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

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

Tableau 1 : Tableau des règles NAT.

Section de tableau	Type de règle	Ordre des règles dans la section
Section 1	Manual NAT (NAT manuelle)	Appliqués lors de la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Étant donné que la première correspondance est appliquée, vous devez vous assurer que les règles spécifiques précèdent les règles plus générales, sans quoi les règles spécifiques pourraient ne pas être appliquées comme vous le souhaitez. Par défaut, les règles manual NAT (NAT manuelle) sont ajoutées à la section 1. 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 2	Auto NAT (NAT automatique)	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	Manual NAT (NAT manuelle)	Si aucune correspondance n'est trouvée, les règles de la section 3 sont appliquées selon la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Cette section devrait contenir vos règles les plus générales. Vous devez également vous assurer que toutes les règles spécifiques de cette section précèdent les règles générales qui s'appliqueraient autrement.

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

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

L'ordre résultant serait le suivant :

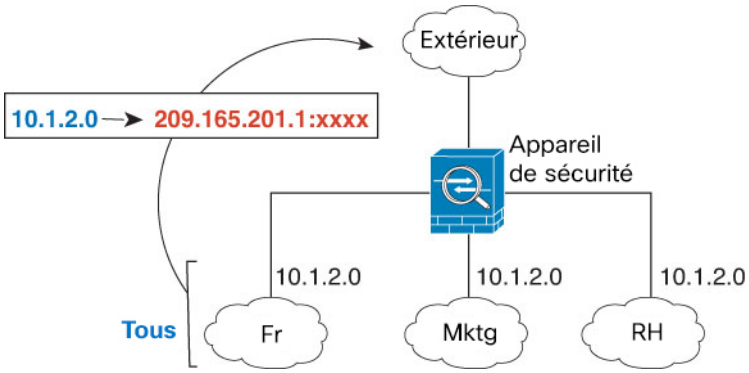
- 192.168.1.1/32 (statique)
- 10.1.1.0/24 (statique)
- 192.168.1.0/24 (statique)
- 172.16.1.0/24 (dynamique) (objet abc)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

Interfaces NAT

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

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

Illustration 2 : 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.

Vous ne pouvez pas configurer la NAT sur des interfaces passives.

Configurer le routage pour la NAT

Le périphérique Cisco Firewall Threat Defense doit être la destination de tous les paquets envoyés à l'adresse traduite (mappée).

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

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

Adresses sur le même réseau que l'interface mappée

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

Adresses sur un réseau unique

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

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

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

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

ARP est prise uniquement en fonction de l'adresse « source »). Si la réponse ARP Firewall Threat Defense est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers Firewall Threat Defense .

Directives pour la NAT

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

Directives relatives à l'interface

La NAT est prise en charge pour les interfaces physiques ou les sous-interfaces routées standard.

Cependant, la configuration de la NAT sur des interfaces membres d'un groupe de pont (interfaces faisant partie d'une Bridge Virtual Interface, ou BVI) est soumise aux 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 la NAT entre des interfaces membres d'un groupe de pont, vous devez préciser les interfaces source et de destination. Vous ne pouvez pas définir « any » comme interface.
- Vous ne pouvez pas configurer la PAT d'interface lorsque l'interface de destination est une interface membre d'un groupe de pont, 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.

Directives pour la NAT pour IPv6

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

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

Prise en charge de la NAT pour les protocoles inspectés

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

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

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

Remarque La réécriture de la NAT est prise en charge sur les ports répertoriés uniquement. Si vous utilisez ces protocoles sur des ports non standard, n'utilisez pas la NAT sur les connexions.

Tableau 2 : Inspection des applications NAT prises en charge

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
DCERPC	TCP/135	No NAT64.	Oui
DNS sur UDP	UDP/53	Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS.	Non
ESMTP	TCP/25	No NAT64.	Non
FTP	TCP/21	Aucune restriction.	Oui
H.323 H.225 (signalisation d'appel) H.323 RAS	TCP/1720 UDP/1718 Pour ARS, UDP/1718-1719	No NAT64.	Oui
ICMP Erreur ICMP	ICMP (Le trafic ICMP dirigé vers une interface de périphérique n'est jamais inspecté.)	Aucune restriction.	Non
Options d'adresse IP	RSVP	No NAT64.	Non
Serveur de noms NetBIOS sur IP	UDP/133, 138 (ports sources)	No NAT64.	Non
RSH	TCP/514	Pas de PAT No NAT64.	Oui
RTSP	TCP/554 (Aucun traitement pour la masquage HTTP.)	No NAT64.	Oui
SIP	TCP/5060 UDP/5060	Pas de PAT étendue. Pas de NAT64 ou NAT46.	Oui
Skinny (SCCP)	TCP/2000	Pas de NAT64, NAT46 ou NAT66.	Oui
SQL*Net (versions 1, 2)	TCP/1521	No NAT64.	Oui
Sun RPC	TCP/111 UDP/111	No NAT64.	Oui
TFTP	UDP/69	No NAT64. Les adresses IP de charge utile ne sont pas traduites.	Oui

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
XDMCP	UDP/177	No NAT64.	Oui

Directives de destination de nom de domaine complet (FQDN)

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

Lorsque vous utilisez un nom de domaine complet, le système obtient la résolution DNS et écrit la règle NAT en fonction de l'adresse renvoyée. Si plusieurs adresses sont obtenues à partir du serveur DNS, l'adresse utilisée est basée sur les éléments suivants :

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

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

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

Directives supplémentaires pour la NAT

- 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.
- (Auto NAT (NAT automatique) seulement.) Vous ne pouvez définir qu'une seule règle NAT pour un objet donné; si vous souhaitez configurer plusieurs règles NAT pour un objet, vous devez créer plusieurs objets avec des noms différents qui spécifient la même adresse IP.
- Si un VPN est défini sur une interface, le trafic ESP entrant sur l'interface n'est pas soumis aux règles de la NAT. Le système autorise le trafic ESP uniquement pour les tunnels VPN établis, abandonnant le trafic non associé à un tunnel existant. Cette restriction s'applique aux ports ESP et UDP 500 et 4500.
- Si vous définissez un VPN de site à site sur un périphérique qui se trouve derrière un périphérique qui applique la PAT dynamique, de sorte que les ports UDP 500 et 4500 ne soient pas ceux réellement utilisés,

vous devez établir la connexion à partir du périphérique qui se trouve derrière le PAT. Le répondeur ne peut pas lancer l'association de sécurité (SA), car il ne connaît pas les bons numéros de port.

- Si vous modifiez la configuration NAT et que vous ne souhaitez pas attendre que les traductions existantes expirent avant d'utiliser la nouvelle configuration NAT, vous pouvez effacer le tableau de traduction à l'aide de la commande **clear xlate** dans la CLI du périphérique . Cependant, l'effacement du tableau de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions.

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

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

- Vous ne pouvez pas utiliser un groupe d'objets avec des adresses IPv4 et IPv6 ; le groupe d'objets ne doit comprendre qu'un seul type d'adresse.
- Un objet réseau utilisé dans la NAT ne peut pas inclure plus de 131 838 adresses IP, explicitement ou implicitement dans une plage d'adresses ou un sous-réseau. Fractionnez l'espace d'adresse en plages plus petites et écrivez des règles distinctes pour les objets plus petits.
- (Manual NAT (NAT manuelle) seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « tout » (IPv4 ou IPv6) dépend de la règle. Avant que Firewall Threat Defense effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, Firewall Threat Defense 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
  - (NAT dynamique.) L'adresse IP de l'interface de secours lorsque le VPN est activé.
- Évitez d'utiliser des adresses qui se chevauchent dans les politiques NAT statiques et dynamiques. Par exemple, avec des adresses qui se chevauchent, une connexion PPTP peut ne pas s'établir si la connexion secondaire pour PPTP atteint le xlate statique au lieu de dynamique.

- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous spécifiez une interface de destination dans une règle, cette interface est utilisée comme interface de sortie plutôt que de rechercher la voie de routage dans la table de routage. Cependant, pour la NAT d'identité, vous avez la possibilité d'utiliser à la place une recherche de route.
- La NAT s'applique uniquement au trafic de transit. Le trafic généré par le système n'est pas soumis à la NAT.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- Vous ne pouvez pas utiliser la NAT sur la charge utile interne des registres PIM (Protocol Independent Multicast).
- (Manual NAT (NAT manuelle)) lors de la rédaction de règles NAT pour une configuration d'interface ISP double (interfaces principale et de secours utilisant les contrats de niveau de service dans la configuration de routage), ne spécifiez pas de critères de destination dans la règle. Assurez-vous que la règle de l'interface principale précède la règle de l'interface de secours. Cela permet au périphérique de choisir la bonne interface de destination NAT en fonction de l'état de routage actuel lorsque le fournisseur de services Internet principal n'est pas disponible. Si vous spécifiez des objets de destination, la règle NAT sélectionnera toujours l'interface principale pour les règles autrement en double.
- Si vous obtenez la raison d'abandon ASP nat-no-xlate-to-pat- Pool pour le trafic qui ne devrait pas correspondre aux règles NAT définies pour l'interface, configurez les règles NAT d'identité pour le trafic affecté afin que le trafic puisse être non traduit.
- Si vous configurez la NAT pour les points terminaux d'un tunnel GRE, vous devez désactiver le maintien de l'activité sur les points terminaux, sinon le tunnel ne pourra pas être établi. Les points terminaux envoient des paquets keepalives aux adresses d'origine.
- 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 la stratégie de contrôle d'accès correspondante.

Configurer la traduction d'adresses réseau (NAT)

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

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

Vous pouvez créer des règles NAT dynamique, PAT dynamique, NAT statique et NAT d'identité. Pour un aperçu, consultez Type de NAT, à la page 2.

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

Pour une comparaison de ces deux options d'implémentation, consultez Auto NAT (NAT automatique) et Manual NAT (NAT manuelle), à la page 4.

Étape 4 Créez les règles, comme expliqué dans les sections suivantes.

- Traduction d'adresses réseau dynamique, à la page 15
- PAT dynamique, à la page 20
- NAT statique, à la page 25
- NAT d'identité, à la page 34

Étape 5 Gérer la politique et les règles NAT

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

- Pour modifier une règle, cliquez sur l'icône de modification () de la règle.
- Pour supprimer une règle, cliquez sur l'icône de suppression () de la règle.

Traduction d'adresses réseau dynamique

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

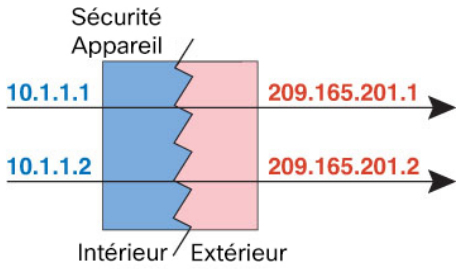
À propos de la NAT dynamique

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.

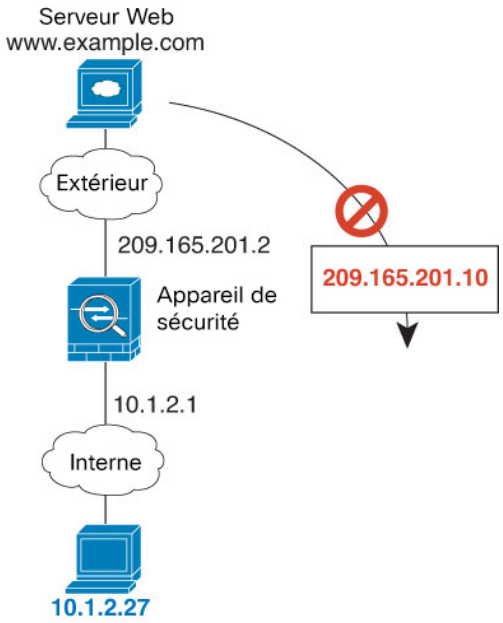
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

Illustration 3 : 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 4 : L'hôte distant tente d'établir une connexion à une adresse mappée



Avantages et désavantages de la NAT dynamique

La NAT dynamique présente les désavantages suivants :

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

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

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

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

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

Configurer la NAT automatique dynamique

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

Avant de commencer

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'objet réseau ou le groupe qui contient les adresses mappées.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 78.
- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts.

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle dynamique

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

Avant de commencer

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

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Adresse source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

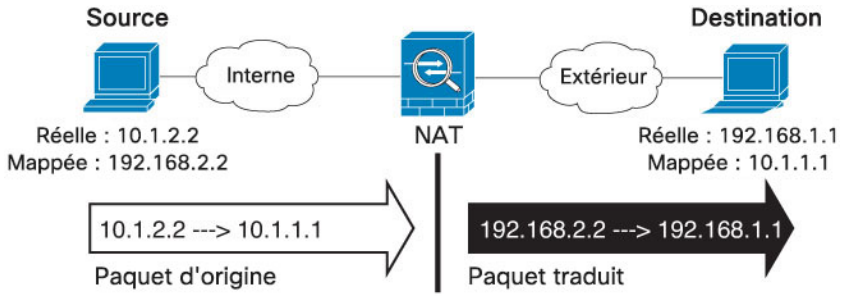
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

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

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



- **Original Source Address** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination Address** (adresse de la destination d'origine) (Facultatif) L'objet réseau qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique

quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

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

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

- **Translated Source Address** (Adresse source traduite) : l'objet réseau ou le groupe qui contient les adresses mappées.
- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **Original Destination Address (Destination d'origine**, vous pouvez configurer l'Identity NAT (NAT d'identité) en sélectionnant le même objet.

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

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

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

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 78.
- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts.

Étape 9 Cliquez sur **OK**.

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

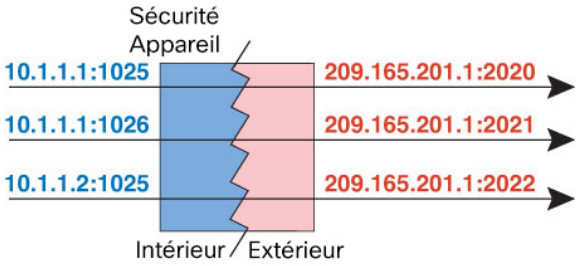
À propos de la PAT dynamique

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 5 : PAT dynamique



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

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

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

Avantages et inconvénients de la PAT dynamique

La PAT dynamique vous permet d'utiliser une seule adresse mappée, préservant ainsi les adresses routables. Vous pouvez même utiliser l'adresse IP de l'interface Firewall Threat Defense comme adresse PAT. Cependant, vous ne pouvez pas utiliser la PAT de l'interface pour les adresses IPv6 sur l'interface.

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 entre un membre d'un groupe de ponts et une interface routée standard.

La PAT dynamique ne fonctionne pas avec certaines applications multimédias dont le flux de données est différent de celui du chemin de contrôle. Pour obtenir plus de renseignements, consultez Prise en charge de la NAT pour les protocoles inspectés, à la page 10.

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.

Configurer la PAT automatique dynamique

Utilisez les règles PAT automatiques dynamiques pour traduire les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire en une adresse unique, soit l'adresse de l'interface de destination, soit une autre adresse.

Avant de commencer

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

- **Original Address (**Adresse d'origine) : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Translated Address** (Adresse traduite) : vous avez les options suivantes pour spécifier l'adresse PAT :
  - **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'une des adresses suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Transition vers l'interface PAT** (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas utiliser cette option avec les réseaux IPv6.

Étape 6 Cliquez sur **OK**.

Configurer la PAT manuelle dynamique

Utilisez des règles PAT manuelles dynamiques lorsque la PAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La PAT dynamique traduit les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire en une adresse unique, soit l'adresse de l'interface de destination, soit une autre adresse.

Avant de commencer

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

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Adresse source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :
  - **Destination Interface** (Interface de destination) : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

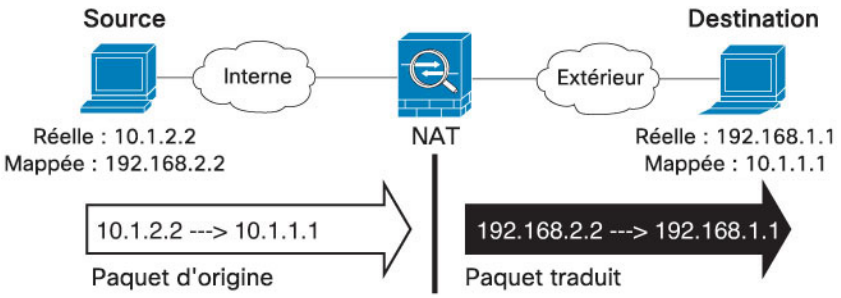
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

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

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



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

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

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

- **Translated Source Address** (Source traduite) : l'une des suivantes :

- (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
- Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.

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

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

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

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

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Transition vers l'interface PAT** (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas utiliser cette option avec les réseaux IPv6.

Étape 9 Cliquez sur **OK**.

NAT statique

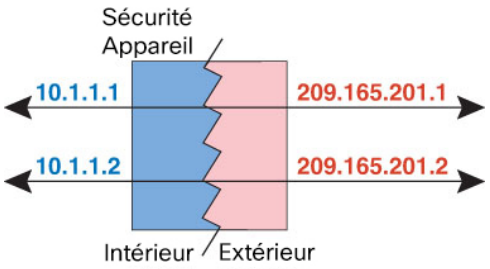
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

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 6 : NAT statique



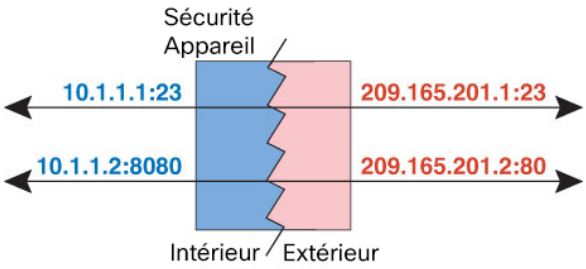
NAT statique avec traduction de port

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 7 : NAT statique typique avec scénario de traduction de port



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

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

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

NAT statique avec traduction de port d'identité

Vous pouvez simplifier l'accès externe aux ressources internes. Par exemple, si vous avez trois serveurs distincts qui fournissent des services sur des ports différents (comme FTP, HTTP et SMTP), vous pouvez donner aux utilisateurs externes une seule adresse IP pour accéder à ces services. Vous pouvez ensuite

configurer la NAT statique avec traduction de port d'identité pour mapper l'adresse IP externe unique avec les adresses IP correctes des serveurs réels en fonction du port auquel ils tentent d'accéder. Vous n'avez pas besoin de modifier le port, car les serveurs utilisent des ports standard (21, 80 et 25, respectivement).

NAT statique avec traduction de port pour les ports non standard

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

NAT d'interface statique avec traduction de port

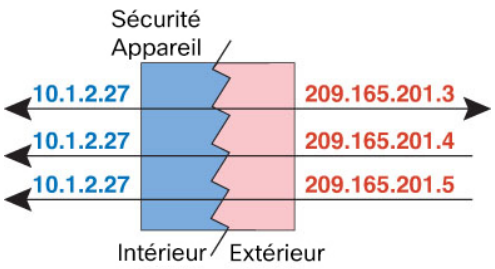
Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec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

NAT statique un vers plusieurs

En règle générale, vous configurez la NAT statique avec un mappage un à un. Cependant, dans certains cas, vous souhaiterez peut-être configurer une seule adresse réelle avec plusieurs adresses mappées (une vers plusieurs). Lorsque vous configurez la NAT statique un-à-plusieurs, lorsque l'hôte réel lance le trafic, il utilise toujours la première adresse mappée. Cependant, pour le trafic initié vers l'hôte, vous pouvez initier le trafic vers n'importe laquelle des adresses mappées, et elles ne seront pas traduites vers l'adresse unique réelle.

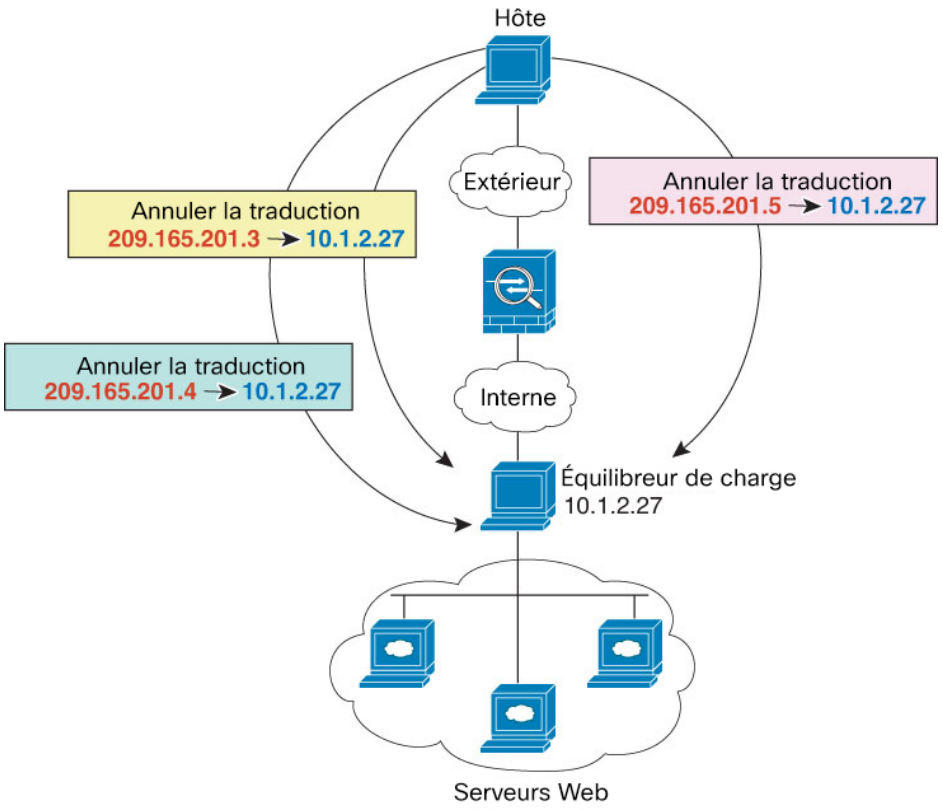
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction IP de l'hôte réel/premier IP mappée est techniquement la seule traduction bidirectionnelle.

Illustration 8 : NAT statique un vers plusieurs



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

Illustration 9 : Exemple de NAT statique un vers plusieurs



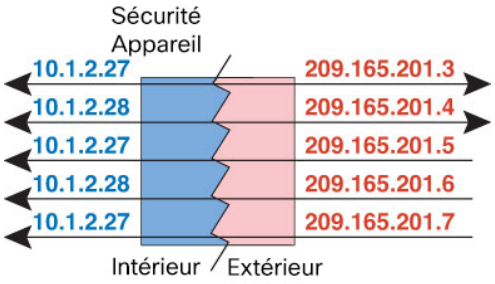
Autres scénarios de mappage (non recommandés)

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 10 : NAT statique quelques-uns vers plusieurs

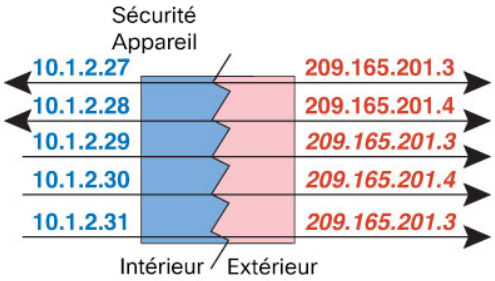


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un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

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

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

Illustration 11 : NAT statique plusieurs à quelques-uns



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

Configurer la NAT statique automatique

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

Avant de commencer

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Statique**.

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Translated Address** (Adresse traduite) : l'une des adresses suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez Address (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.Cela configure la NAT de l'interface

statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.

- (Facultatif) **Original Port (Port d'origine)**, **Translated Port (Port traduit)** : si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans Port d'origine et saisissez les numéros de port d'origine et traduit. Les objets doivent être pour le même protocole. Cliquez sur le lien **Create New Object** (Créer un nouvel objet) si les objets n'existent pas déjà. Par exemple, vous pouvez traduire TCP/80 en TCP/8080 au besoin.

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 78. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle statique

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

Avant de commencer

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

- **Adresse source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Translated Source Address** (Adresse source traduite : vous avez les options suivantes pour spécifier l'adresse traduite :

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

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

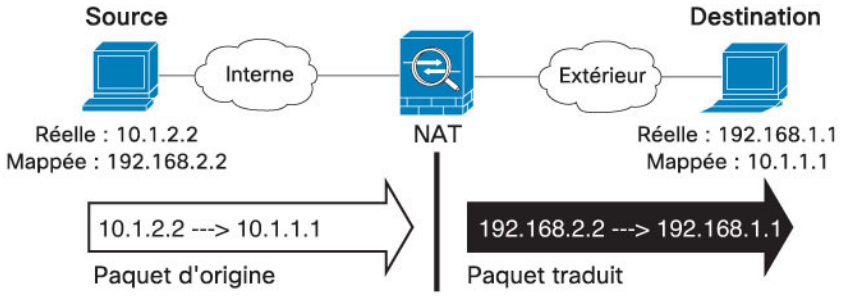
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

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

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



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

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

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

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

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

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

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

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

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 78. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

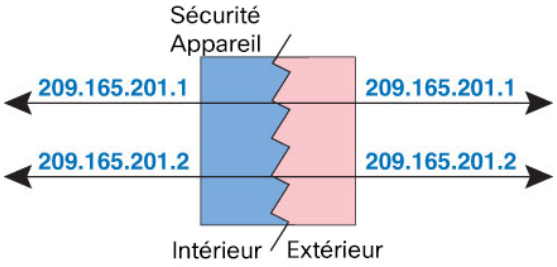
Étape 9 Cliquez sur **OK**.

NAT d'identité

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

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

Illustration 12 : NAT d'identité



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

Configurer la NAT automatique d'identité

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

Avant de commencer

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For** (Créer une règle pour) : sélectionnez **Auto NAT** (NAT automatique).
- **Type** : sélectionnez **Statique**.

Étape 4 Configurez les options de paquets de traduction suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.
- **Original Address** (Adresse d'origine) : l'objet réseau qui contient les adresses que vous traduisez.
- **Adresse traduite** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

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

Étape 5 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage,

car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

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

Étape 6 Cliquez sur **OK**.

Configurer la NAT manuelle d'identité

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

Avant de commencer

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

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

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

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

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **NAT**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification () de la règle.

(Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression de la règle.)

Étape 3 Configurez les options des règles de base :

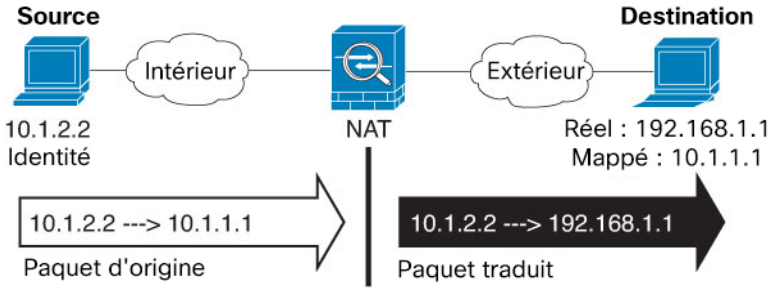
- **Title** (Titre) : entrez un nom pour la règle.
- **Create Rule For**(Créer une règle pour) : sélectionnez **Manual NAT (NAT**manuelle).
- **Rule Placement** (Emplacement des règles) :Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous de la règle de votre choix.
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.

Étape 4 Configurez les options d'interface suivantes :

- **Source Interface (Interface source)**, **Destination Interface (Interface de destination)** : (obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

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

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



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

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

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

- **Translated Source Address** (Adresse source traduite) : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

- **Translated Destination Address** (adresse de destination traduite) : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **Original Destination Address (Destination d'origine**, vous pouvez configurer l'Identity NAT (NAT d'identité) en sélectionnant le même objet.

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

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

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

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

Étape 8 (Facultatif) Cliquez sur le lien **Advanced Options** (Options avancées) et sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.
- **Effectuer une consultation de route pour l'interface de destination** : Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Étape 9 Cliquez sur **OK**.

Propriétés de la règle NAT pour Firewall Threat Defense

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

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

Titre

Entrez un nom pour la règle. Le nom ne peut pas contenir d'espaces.

Create Rule For (Créer une règle pour)

Que la règle de traduction soit **Auto NAT** (NAT automatique) ou **Manual NAT** (NAT manuelle). La NAT automatique est plus simple que la NAT manuelle, mais la NAT manuelle vous permet de créer des traductions distinctes pour une adresse source en fonction de l'adresse de destination.

État

Indique si vous souhaitez que la règle soit active ou désactivée.

Placement (NAT manuelle uniquement)

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

Type

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

Les rubriques suivantes décrivent les propriétés restantes des règles NAT.

Propriétés de traduction de paquets pour la NAT automatique

Utilisez les options **Packet Translation** (Traduction de paquets) pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s'appliquent uniquement à la NAT automatique.

Source Interface (Interface source), Destination Interface (Interface de destination)

(obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Original Address (Adresse d'origine) (toujours obligatoire)

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

Translated Address (Adresse traduite) (généralement requise)

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

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.
- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface**. Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

- Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.

- **NAT statique** : l'une des options suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez l'objet ou le groupe de réseau qui contient les adresses mappées. L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

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

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

Si vous devez traduire un port TCP ou UDP, sélectionnez les objets de port qui définissent les ports d'origine et traduits. Les objets doivent être pour le même protocole. Par exemple, vous pouvez traduire TCP/80 en TCP/8080 au besoin.

Propriétés de traduction de paquets pour la NAT manuelle

Utilisez les options **Packet Translation** (Traduction de paquets) pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s'appliquent uniquement à la NAT manuelle. Tous ces éléments sont facultatifs, sauf indication contraire.

Source Interface (Interface source), Destination Interface (Interface de destination)

(obligatoire pour les interfaces membres des groupe de ponts.) Les interfaces où cette règle NAT s'applique. La **source** est la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Original Source Address (Adresse source d'origine) (toujours obligatoire)

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

Translated Source Address (Adresse source traduite) (généralement requise)

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

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

dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin.
- **NAT statique** : l'une des options suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez l'objet ou le groupe de réseau qui contient les adresses mappées. L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Interface** (Adresse IP de l'interface de destination). Vous devez également sélectionner une interface de destination précise, qui ne peut pas être une interface de membre d'un groupe de ponts. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.
- **NAT d'identité** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Adresse de destination d'origine

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

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

Adresse de destination traduite

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

Vous pouvez utiliser un objet réseau qui spécifie un nom de domaine complet comme destination traduite; pour en savoir plus, consultez Directives de destination de nom de domaine complet (FQDN), à la page 12.

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

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

- (NAT ou PAT dynamique.) Vous ne pouvez pas effectuer de traduction sur le **port source d' origine** et le **port source traduit**. Vous ne pouvez effectuer la traduction que sur le port de destination.
- La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet pour les ports réels et mappés.

Propriétés NAT avancées

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

Traduire les réponses DNS correspondant à cette règle

Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour obtenir plus de renseignements, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 78. Cette option n'est pas disponible si vous effectuez une traduction de port dans une règle NAT statique.

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

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

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

Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

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

Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système

détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Traduction de réseaux IPv6

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

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

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

Remarque NAT46 prend uniquement en charge les mappages statiques.

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

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

NAT64/46 : traduction d'adresses IPv6 en IPv4

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

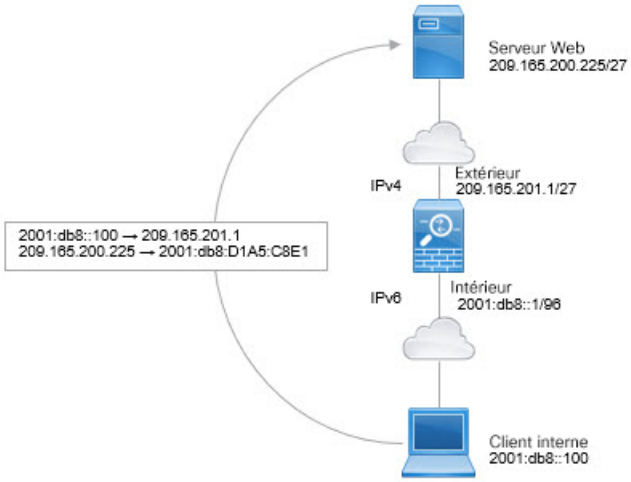
- L'ensemble d'adresses IPv4 pour la règle NAT64 est normalement de petite taille et peut généralement ne pas avoir assez d'adresses pour un mappage individuel avec les adresses client IPv6. La PAT dynamique pourrait plus facilement répondre au plus grand nombre possible d'adresses de clients IPv6 par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

Vous devez définir deux politiques, une pour le réseau IPv6 source et une pour le réseau IPv4 de destination. Bien que vous puissiez accomplir cela à l'aide d'une seule règle manual NAT (NAT manuelle), si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne

pouvez pas activer la réécriture DNS sur une règle manual NAT (NAT manuelle) lorsque vous spécifiez une destination, la création de deux règles auto NAT est la meilleure solution.

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

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



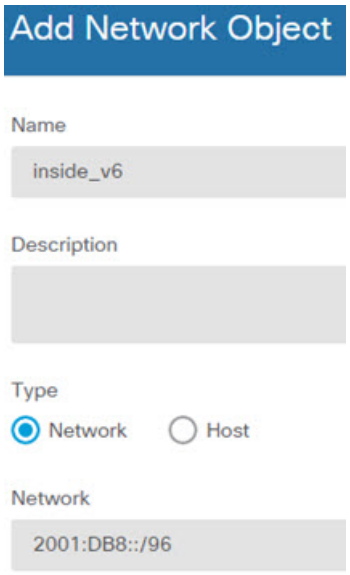
Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne.

Procédure

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

a) Choisissez **Objects** (Objets).
b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.
c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:db8::/96.

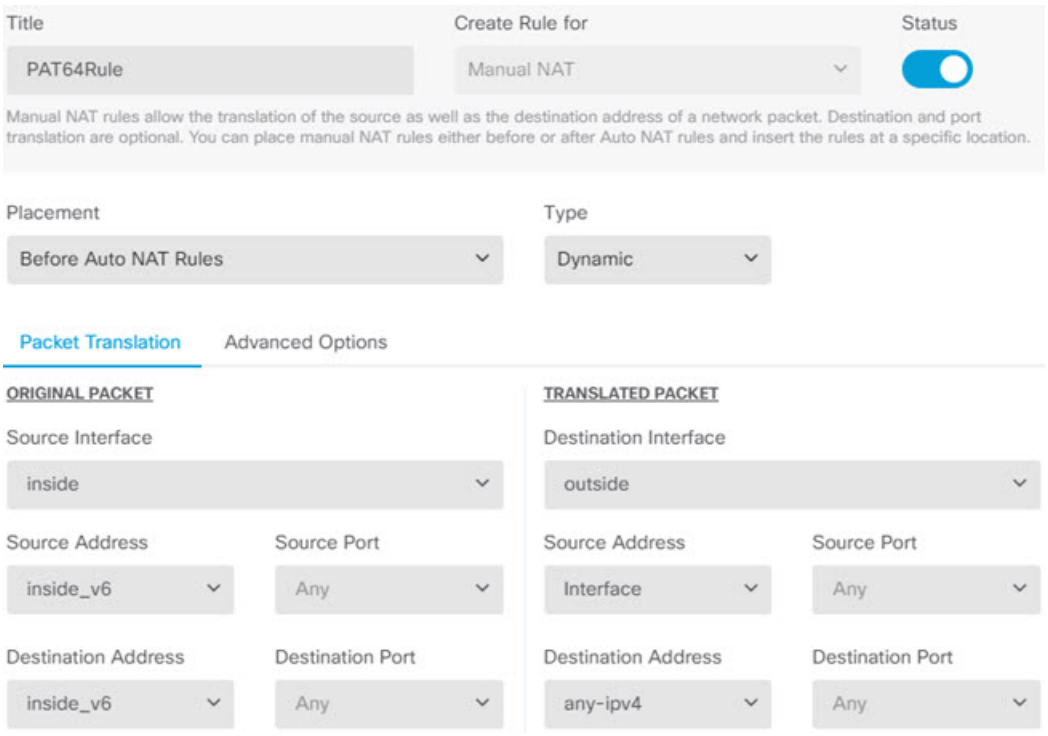


d) Cliquez sur **OK**.

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

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = **Manual NAT** (NAT manuelle).
- **Placement** (emplacement) = **Before Auto NAT Rules** (avant les règles NAT automatiques)
- **Type** = **Dynamic** (dynamique).
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Packet Source Address** (adresse source de paquet d'origine) = objet réseau inside_v6.
- **Translated Packet Source Address (adresse source de paquet traduite)** = Interface. Cette option utilise l'adresse IPv4 de l'interface de destination comme adresse PAT.
- **Original Packet Destination Address** (adresse de destination de paquet d'origine) = objet réseau inside_v6.
- **Translated Packet Destination Address** (adresse de destination de paquet traduite) = objet réseau any-ipv4.

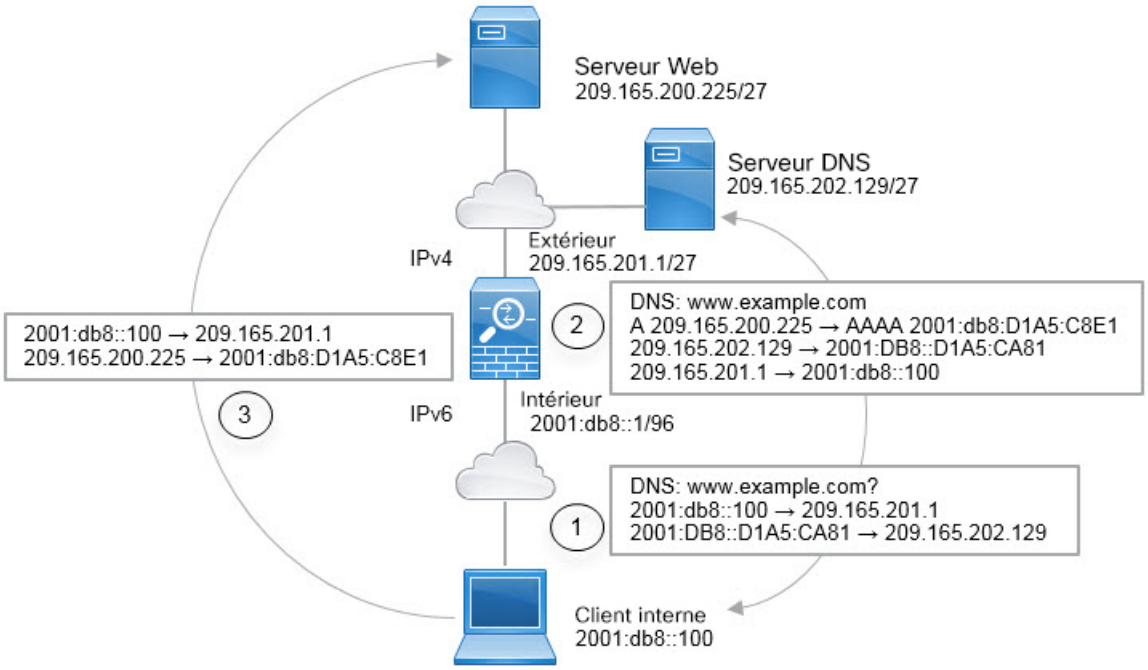


d) Cliquez sur **OK**.

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

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

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



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

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

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

La procédure suivante explique comment configurer cet exemple.

Procédure

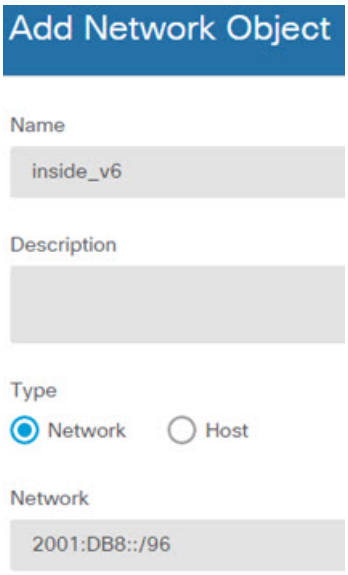
Étape 1 Créez les objets réseau qui définissent les réseaux IPv6 internes et externes IPv4.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez le réseau IPv6 interne.

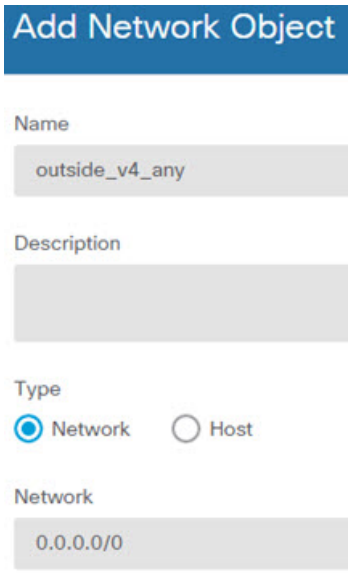
Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:db8::/96.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez le réseau IPv4 externe.

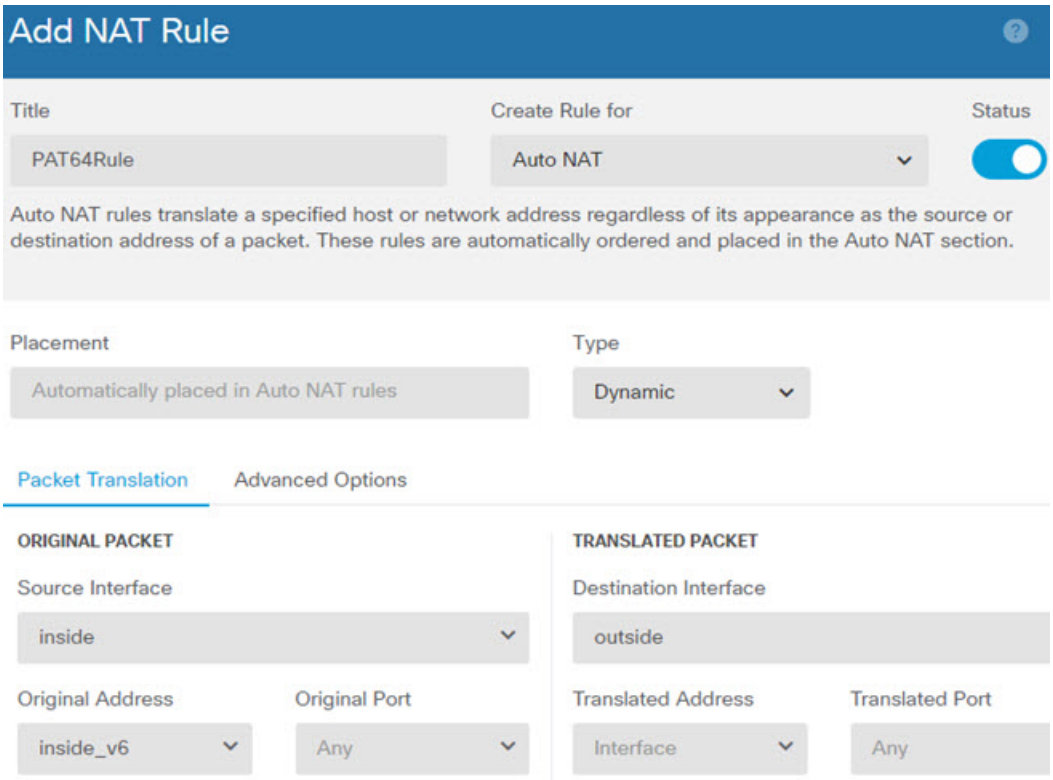
Nommez l'objet réseau (par exemple, outside_v4_any), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 0.0.0.0/0.



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

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Translated Address** (Adresse traduite) = **Interface**. Cette option utilise l'adresse IPv4 de l'interface de destination comme adresse PAT.



d) Cliquez sur **OK**.

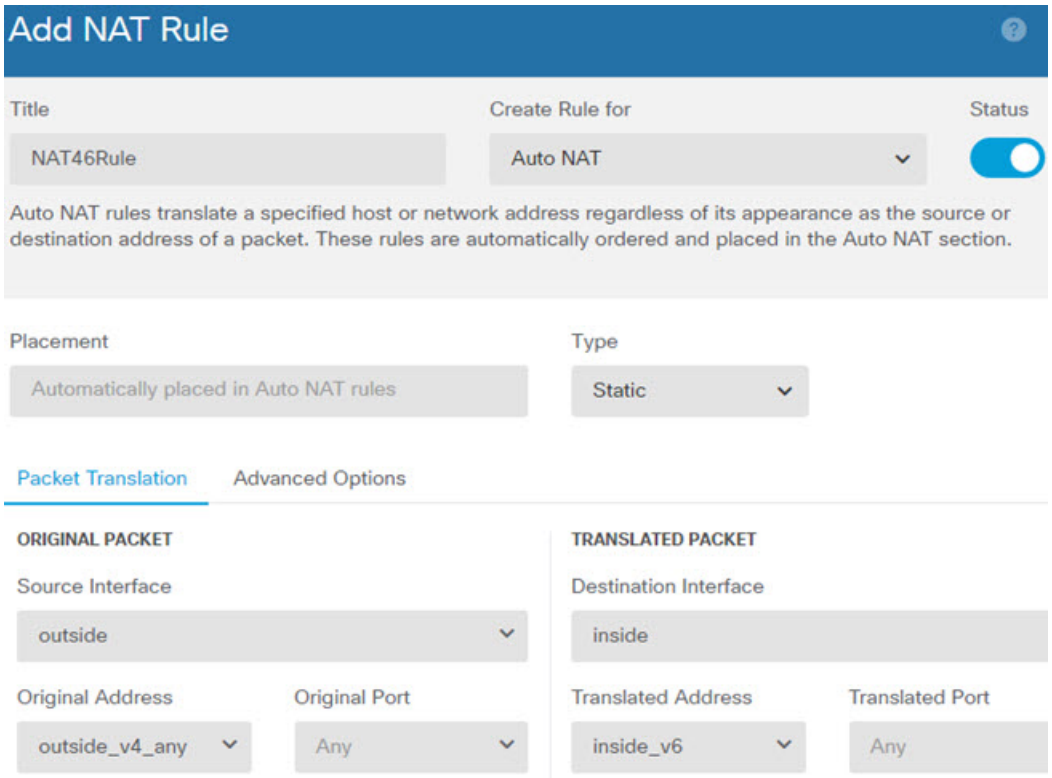
Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe.

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

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Title** (Titre) = NAT46Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Original Address** (Adresse d'origine) = outside_v4_any network object.
- **Translated Address** (Adresse traduite) = inside_v6 network object.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



c) Cliquez sur **OK**.

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

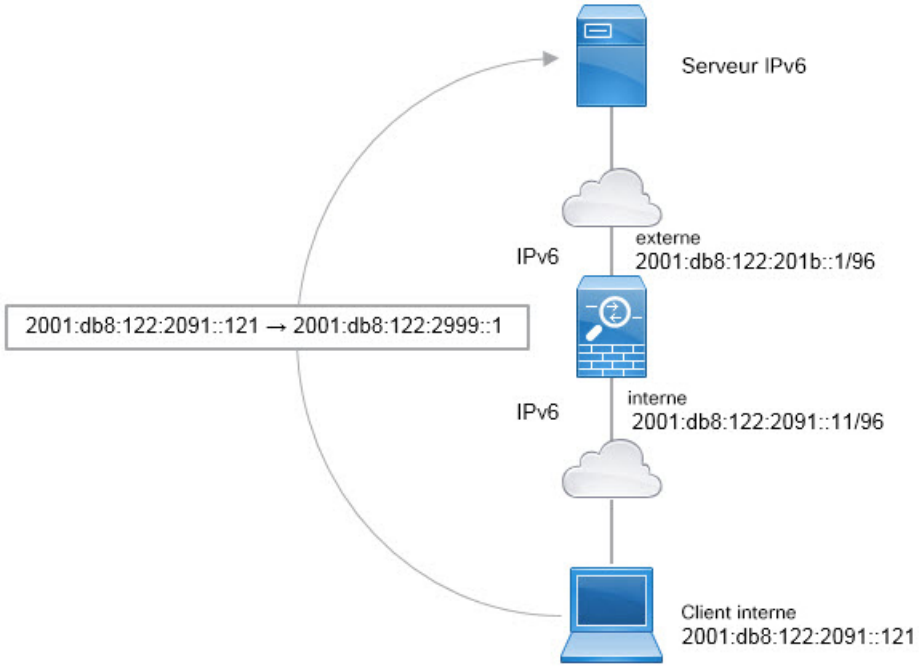
NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6

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

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

Exemple NAT66, de traduction statique entre réseaux

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



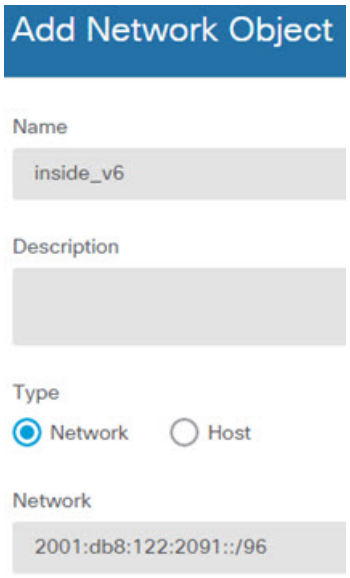
Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

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

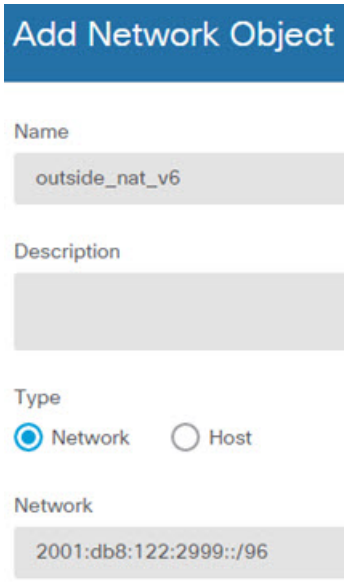
a) Choisissez **Objects** (Objets).
b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.
c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **OK**.
e) Cliquez sur + et définissez le réseau NAT IPv6 externe.

Nommez l'objet réseau (par exemple, outside_nat_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 2001:db8:122:2999::/96.

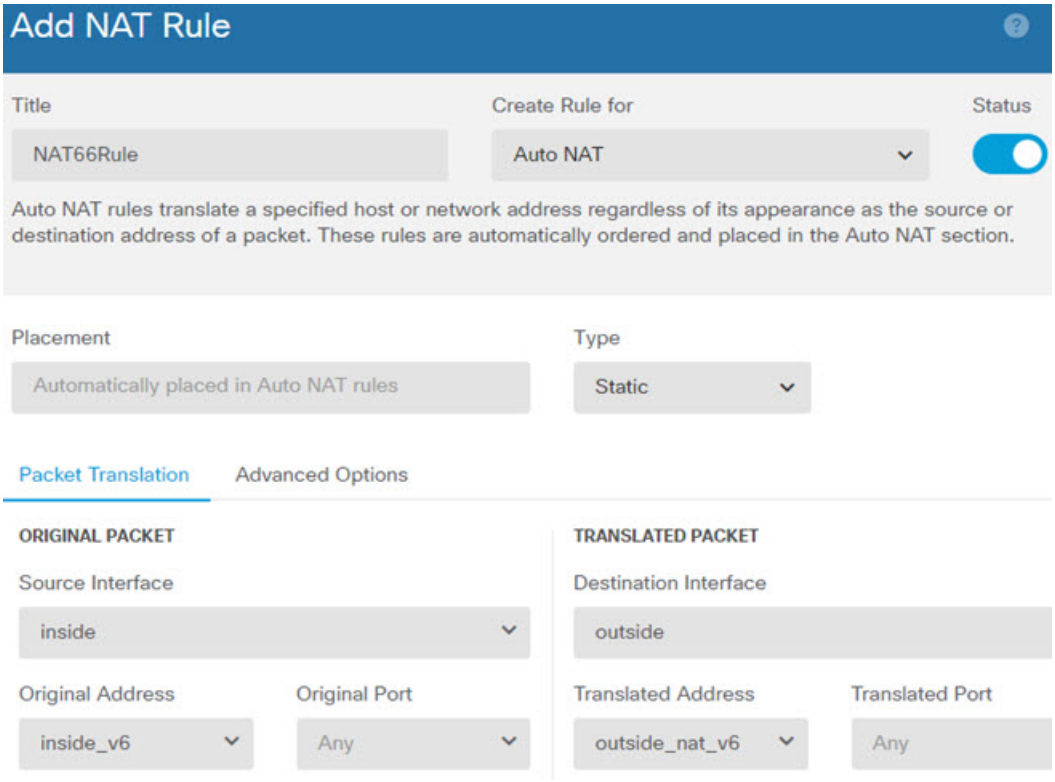


Étape 2 Configurez la règle NAT statique pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = NAT66Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Adresse traduite** = objet réseau outside_nat_v6.



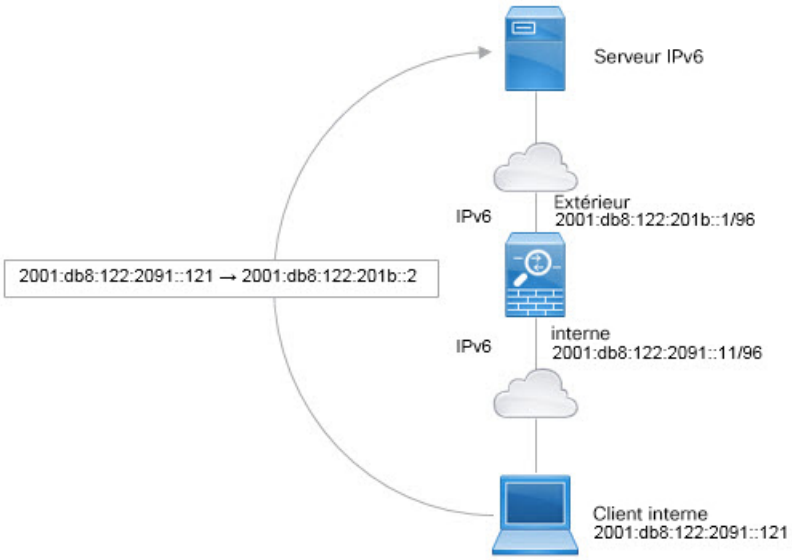
d) Cliquez sur **OK**.

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

Exemple de NAT66, PAT d'interface IPv6 simple

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

Cependant, vous ne pouvez pas configurer l'interface PAT en utilisant l'adresse IPv6 d'une interface à l'aide de la commande Firepower Device Manager. Au lieu de cela, utilisez une seule adresse libre sur le même réseau qu'un ensemble de PAT dynamique.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

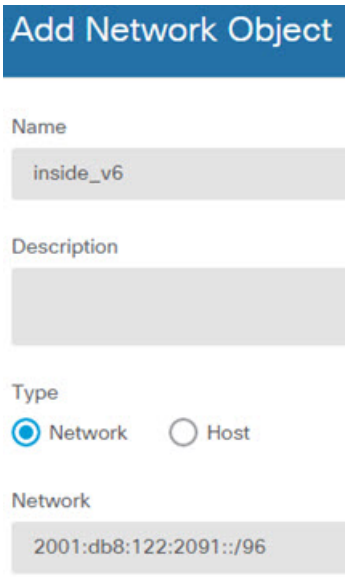
Étape 1 Créez les objets réseau qui définissent le réseau IPv6 interne et l'adresse IPv6 PAT.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **OK**.
e) Cliquez sur le signe + et définissez l'adresse PAT IPv6 externe.

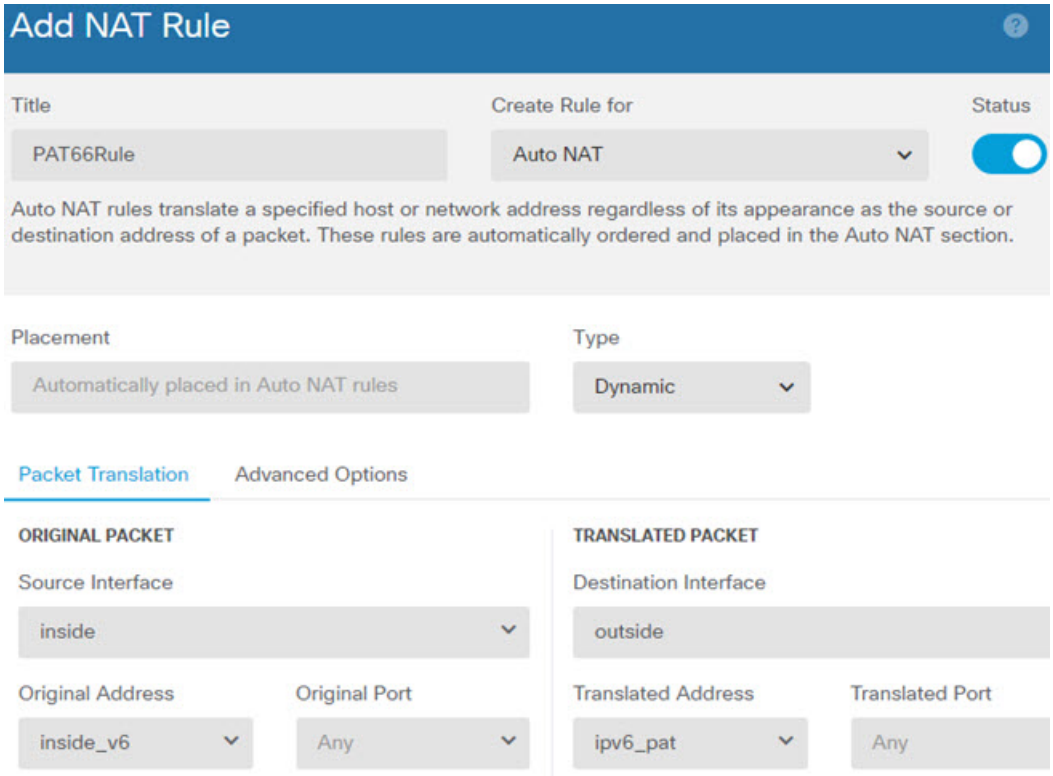
Nommez l'objet réseau (par exemple, ipv6_pat), sélectionnez **Host** (Hôte) et saisissez l'adresse de l'hôte 2001:db8:122:201b::2.

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

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Title** (Titre) = PAT66Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Translated Address** (Adresse traduite) = ipv6_pat network object.



d) Cliquez sur **OK**.

Avec cette règle, tout trafic provenant du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne vers l'interface externe reçoit une traduction dynamique PAT66 vers un port sur 2001:db8:122:201b::2.

Surveillance de la NAT

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

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

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

Exemples relatifs à la NAT

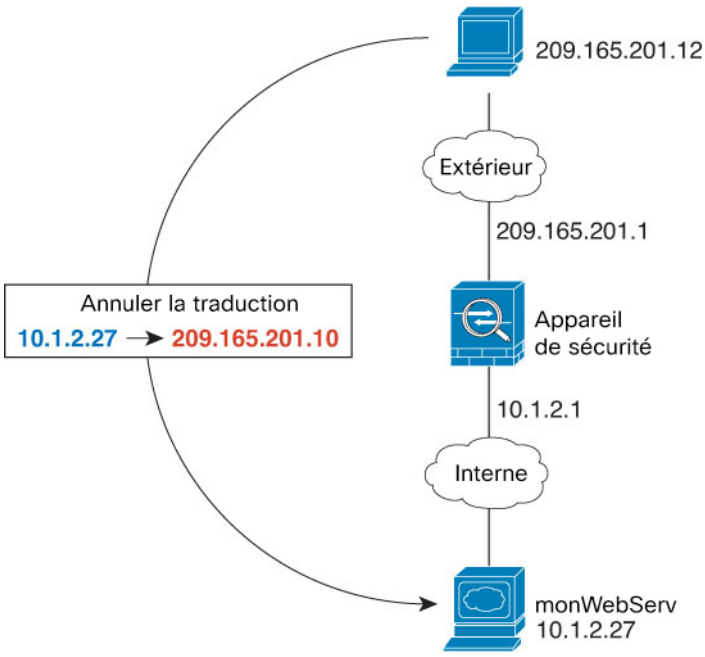
Les rubriques suivantes fournissent des exemples de configuration de la NAT sur les périphériques Threat Defense.

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

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

Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, sélectionnez l'interface de membre du groupe de ponts à laquelle le serveur Web est relié, par exemple, inside1_3.

Illustration 13 : NAT statique pour un serveur Web interne



Procédure

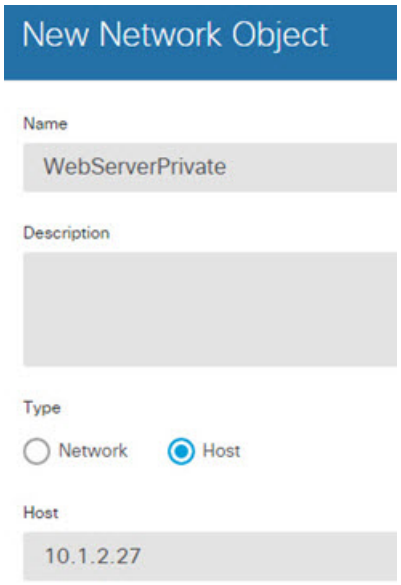
Étape 1 Créez les objets réseau qui définissent les adresses d'hôte privées et publiques du serveur.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez l'adresse privée du serveur Web.

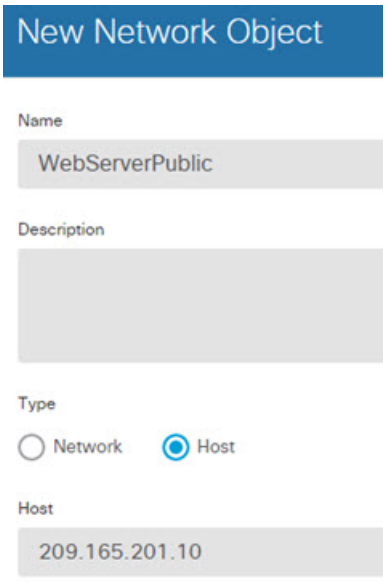
Nommez l'objet réseau (par exemple, WebServerPrivate), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 10.1.2.27.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez l'adresse publique.

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

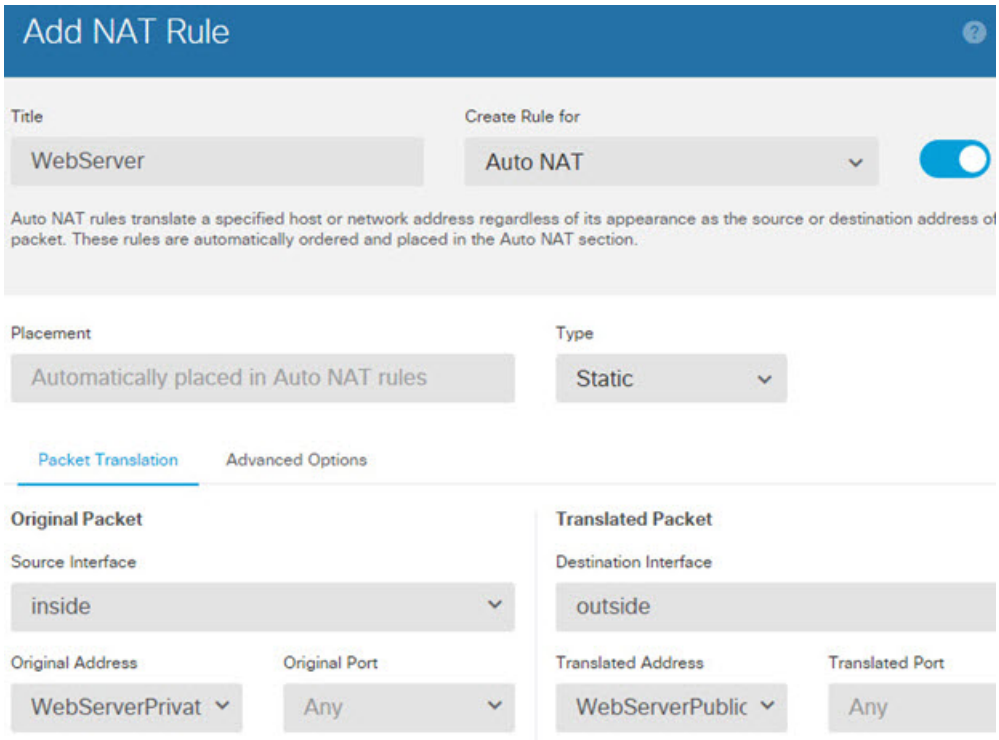


f) Cliquez sur **OK**.

Étape 2 Configurez la NAT statique pour l'objet

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = WebServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Address (**Adresse d'origine) = objet réseau WebServerPrivate.
- **Translated Address** (Adresse traduite) = objet réseau WebServerPublic.



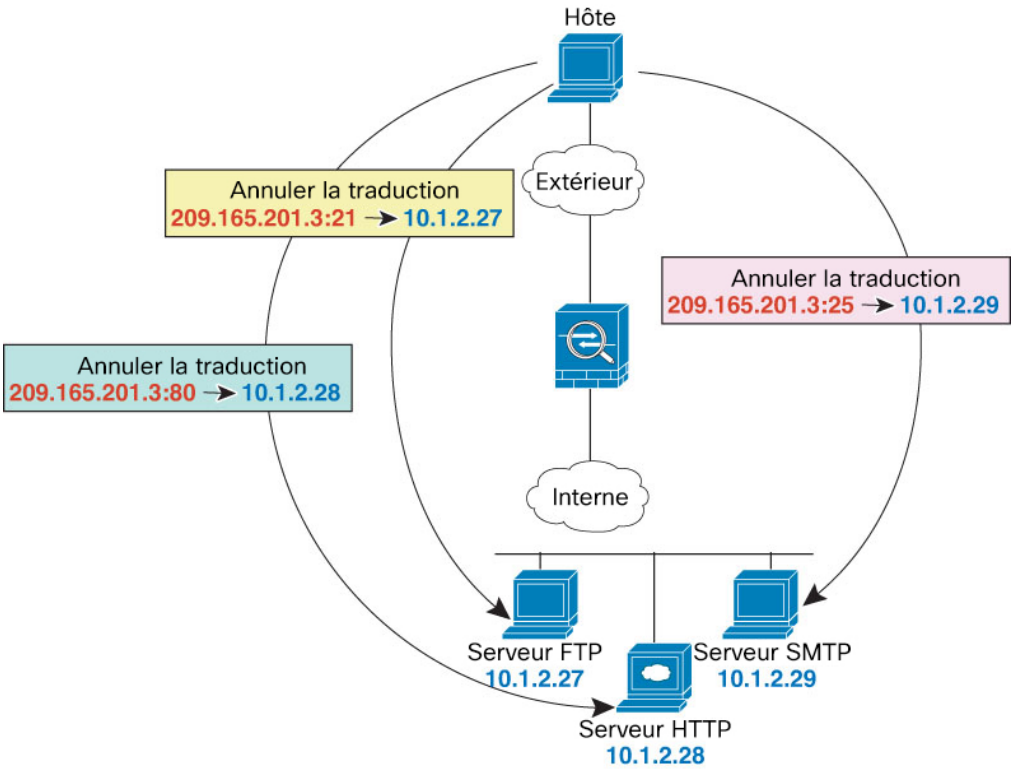
d) Cliquez sur **OK**.

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

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

Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec les serveurs connectés au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que les serveurs sont associés à des interfaces de membre de groupe de ponts distinctes, sélectionnez l'interface de membre spécifique à laquelle chaque serveur est associé pour la règle correspondante. Par exemple, les règles peuvent avoir inside1_2, inside1_3 et inside1_4 pour l'interface source plutôt que inside.

Illustration 14 : NAT statique avec traduction de port



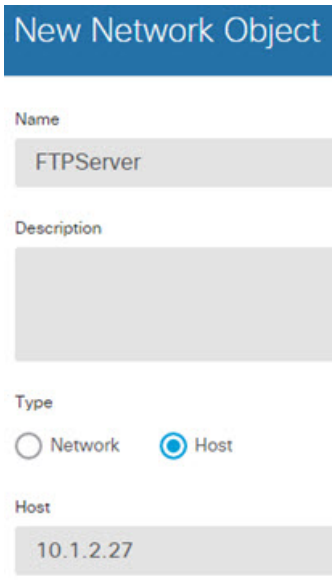
Procédure

Étape 1 Créez un objet réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

c) Nommez l'objet réseau (par exemple, FTPserver), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle du serveur FTP, 10.1.2.27.

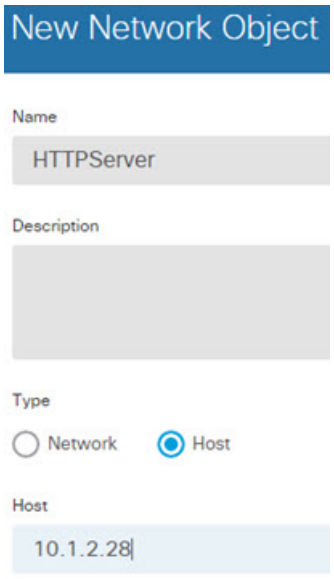


d) Cliquez sur **OK**.

Étape 2 Créez un objet réseau pour le serveur HTTP.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, HTTPserver), sélectionnez **Host** (Hôte), et saisissez l'adresse d'hôte 10.1.2.28.

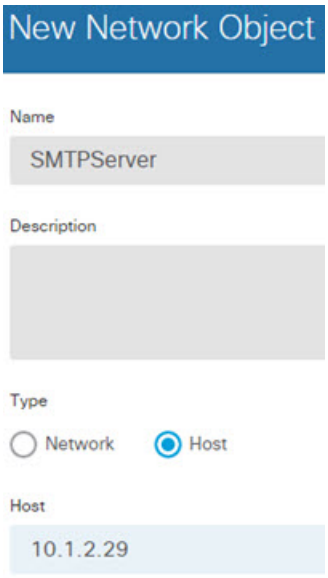


c) Cliquez sur **OK**.

Étape 3 Créez un objet réseau pour le serveur SMTP.

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, SMTPserver), sélectionnez **Host (Hôte)**, et saisissez l'adresse d'hôte 10.1.2.29.

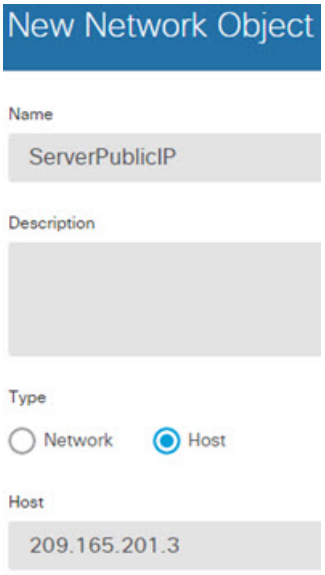


c) Cliquez sur **OK**.

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

a) Cliquez +.

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



c) Cliquez sur **OK**.

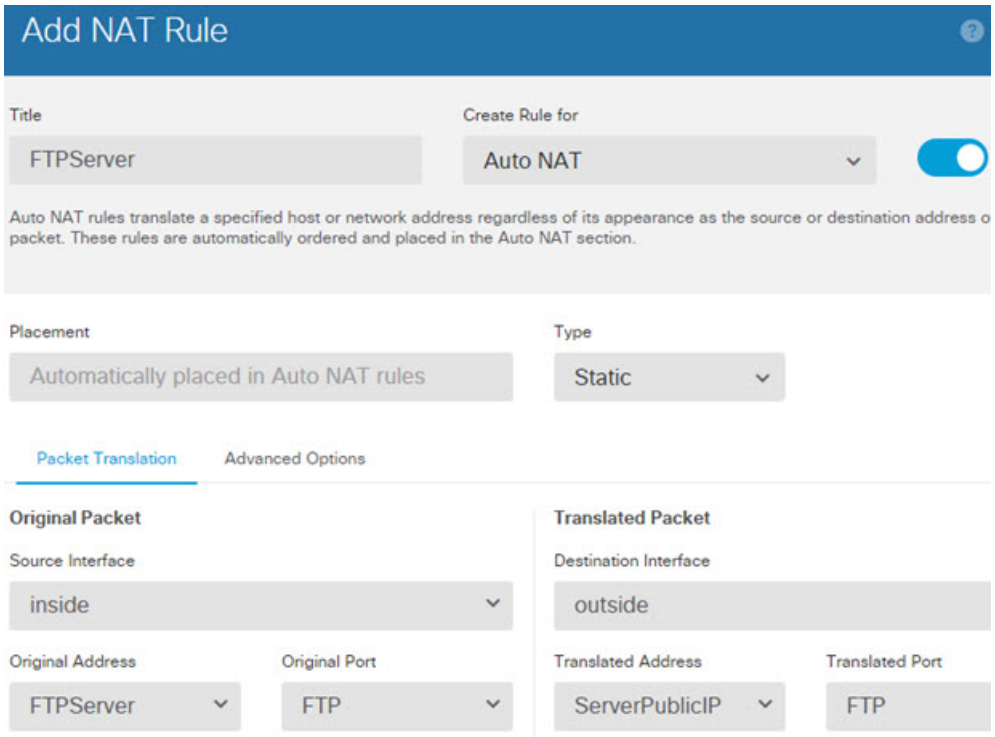
Étape 5 Configurez la NAT statique avec la traduction de port pour le serveur FTP, en mappant le port FTP sur lui-même.

a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau FTPserver.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port FTP.
- **Port traduit** = objet de port FTP.



d) Cliquez sur **OK**.

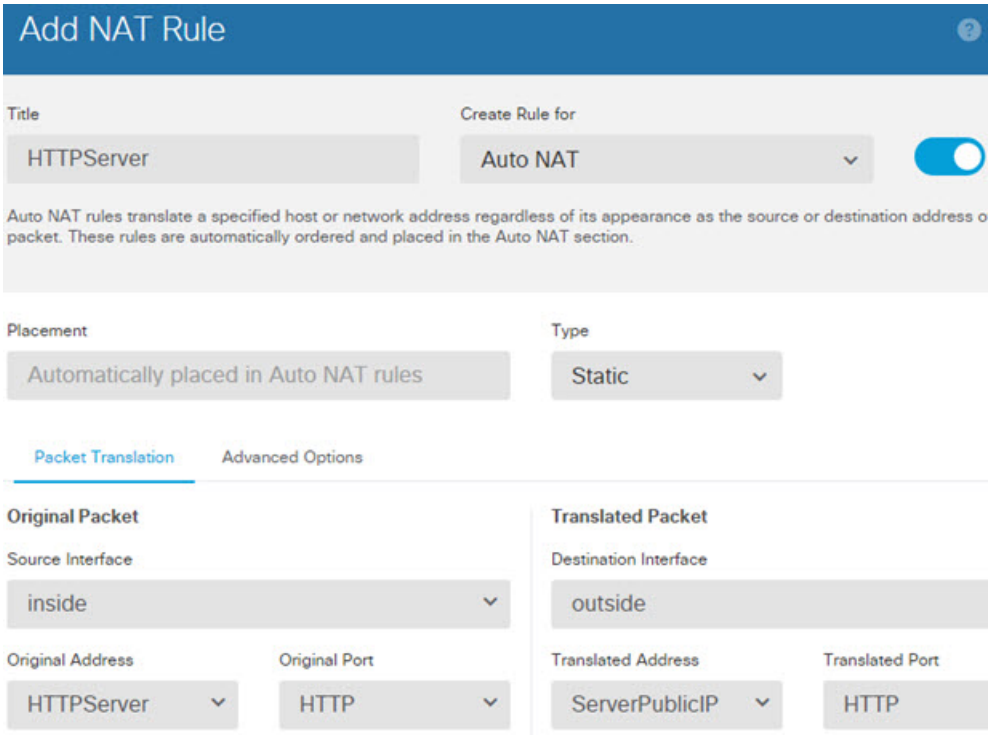
Étape 6 Configurez la NAT statique avec la traduction de port pour le serveur HTTP, en mappant le port HTTP sur lui-même.

a) Cliquez sur le bouton **+**.

b) Configurez les propriétés suivantes :

- **Titre** = HTTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.

- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau HTTPserver.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port HTTP.
- **Port traduit** = objet de port HTTP.



c) Cliquez sur **OK**.

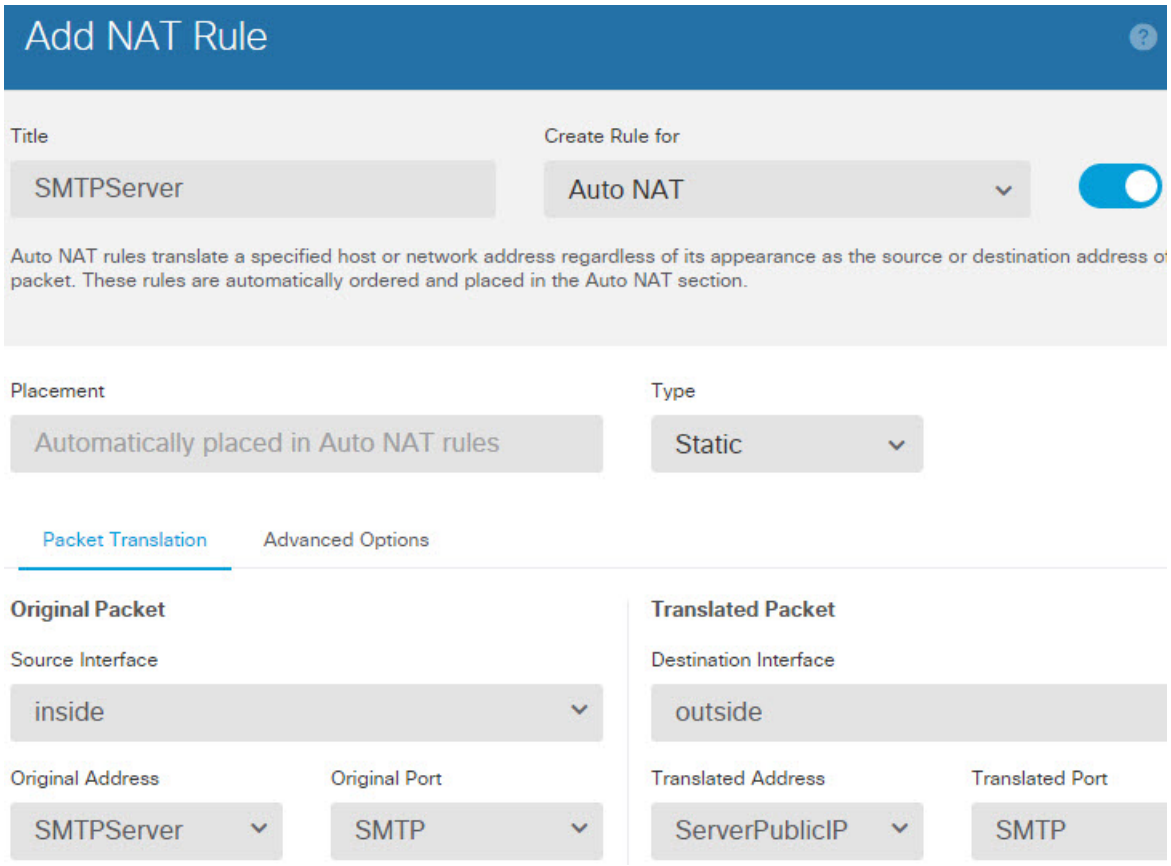
Étape 7 Configurez la NAT statique avec la traduction de port pour le serveur SMTP, en mappant le port SMTP sur lui-même.

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Titre** = SMTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse d'origine** = objet réseau du serveur SMTP.
- **Adresse traduite** = objet réseau ServerPublicIP.
- **Port d'origine** = objet de port SMTP.

- **Port traduit** = objet de port SMTP.



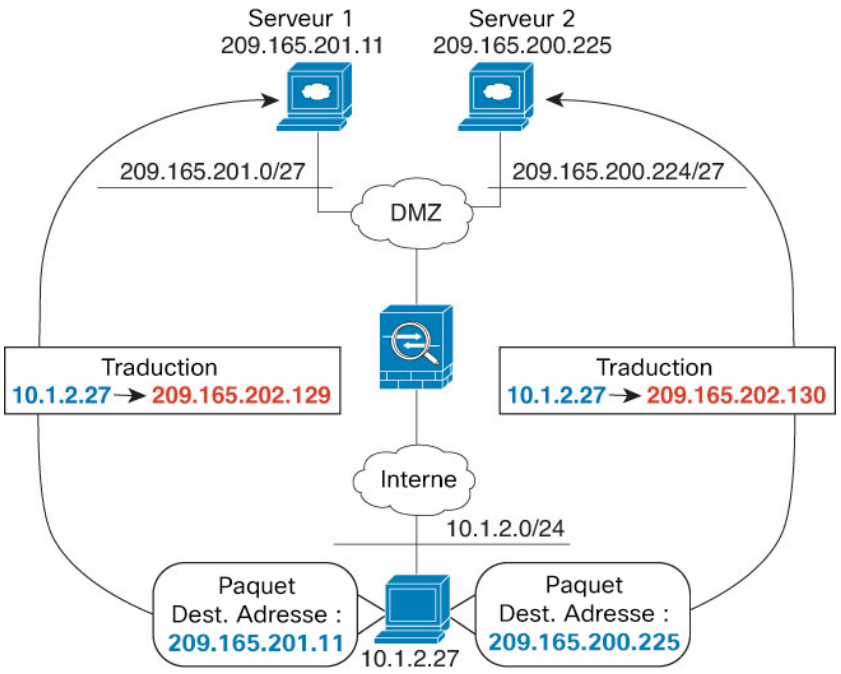
c) Cliquez sur **OK**.

Traduction différente selon la destination (PAT manuelle dynamique)

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

Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec les serveurs connectés au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que les serveurs sont associés à des interfaces de membre de groupe de ponts distinctes, sélectionnez l'interface de membre spécifique à laquelle chaque serveur est associé pour la règle correspondante. Par exemple, les règles peuvent avoir interne1_2 et interne1_3 pour l'interface source plutôt que interne.

Illustration 15 : NAT manuelle avec différentes adresses de destination



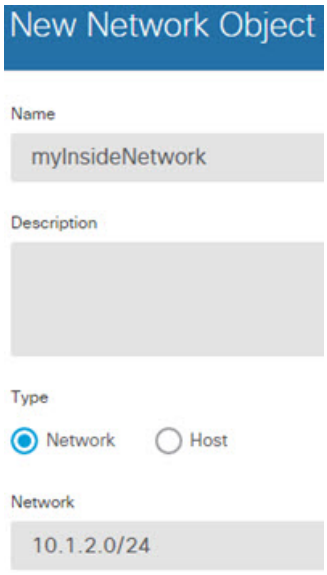
Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

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

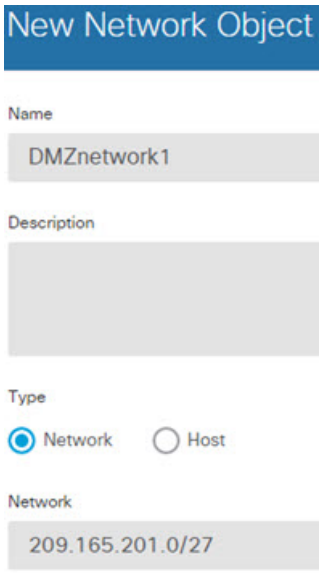


d) Cliquez sur **OK**.

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

a) Cliquez +.

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

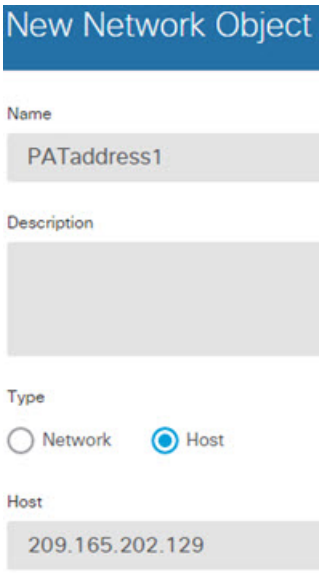


c) Cliquez sur **OK**.

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

a) Cliquez +.

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

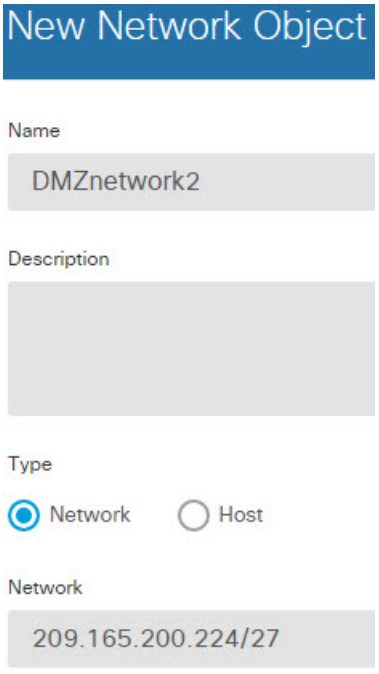


c) Cliquez sur **OK**.

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

a) Cliquez +.

b) Nommez l'objet réseau (par exemple, DMZnetwork2), sélectionnez **Network (Réseau)**, et saisissez l'adresse réseau 209.165.201.0/27 (masque de sous-réseau 255.255.255.224).

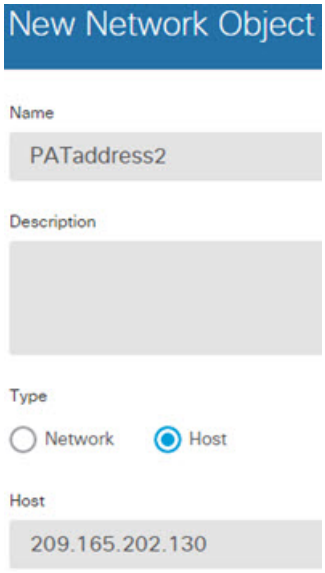


c) Cliquez sur **OK**.

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

a) Cliquez +.

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



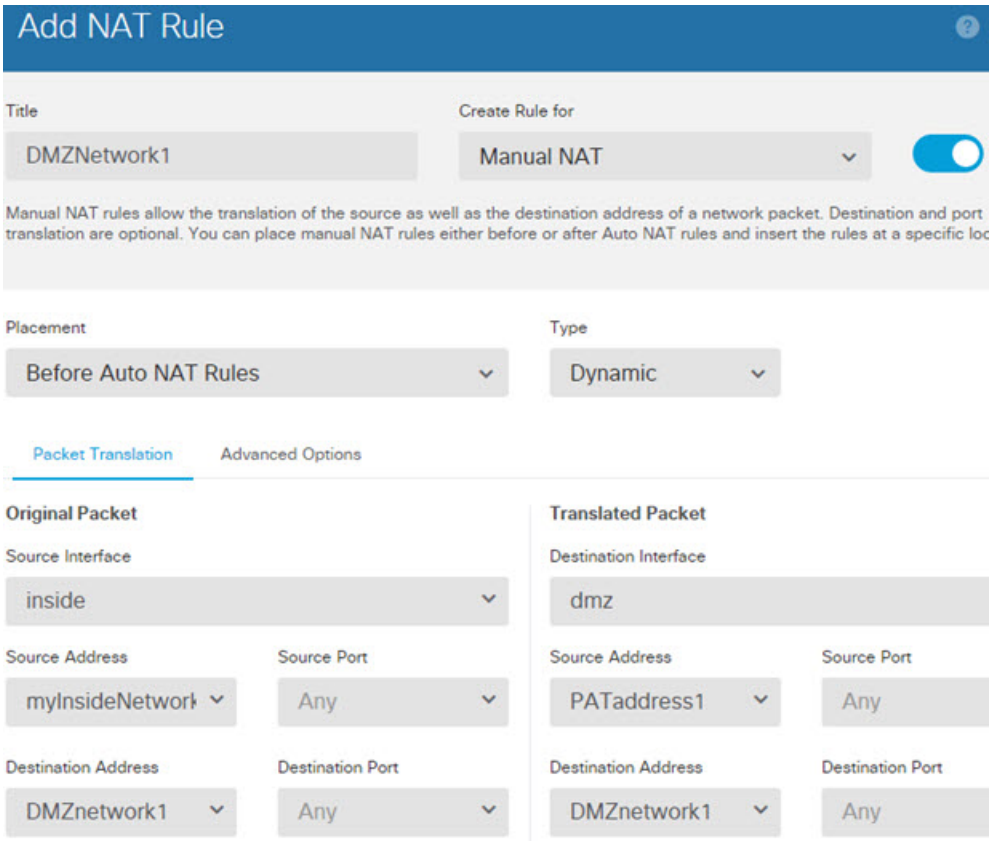
c) Cliquez sur **OK**.

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

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Title** (Titre) = DMZNetwork1 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- Adresse **source traduite** = objet de réseau PATaddress1.
- **Adresse de destination d'origine** = objet réseau DMZnetwork1.
- **Adresse de destination traduite** = objet réseau DMZnetwork1.

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



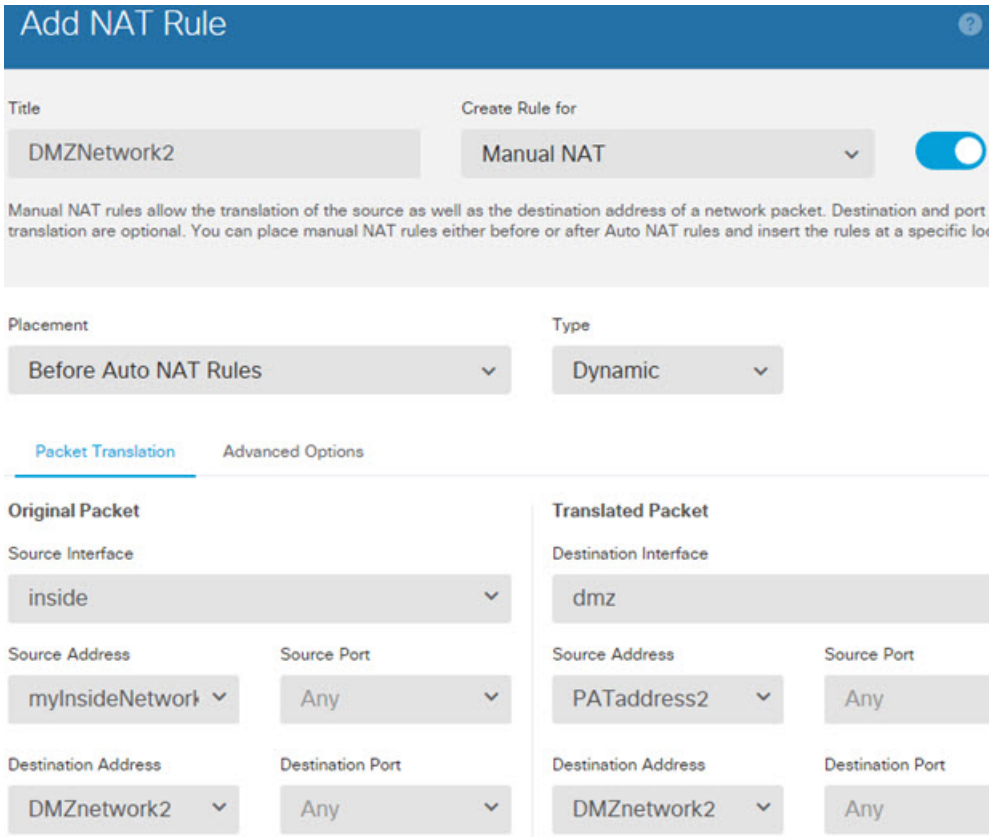
d) Cliquez sur **OK**.

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

a) Cliquez sur le bouton +.

b) Configurez les propriétés suivantes :

- **Title** (Titre) = DMZNetwork2 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress2.
- **Adresse de destination d'origine** = objet réseau DMZnetwork2.
- **Adresse de destination traduite** = objet réseau DMZnetwork2.



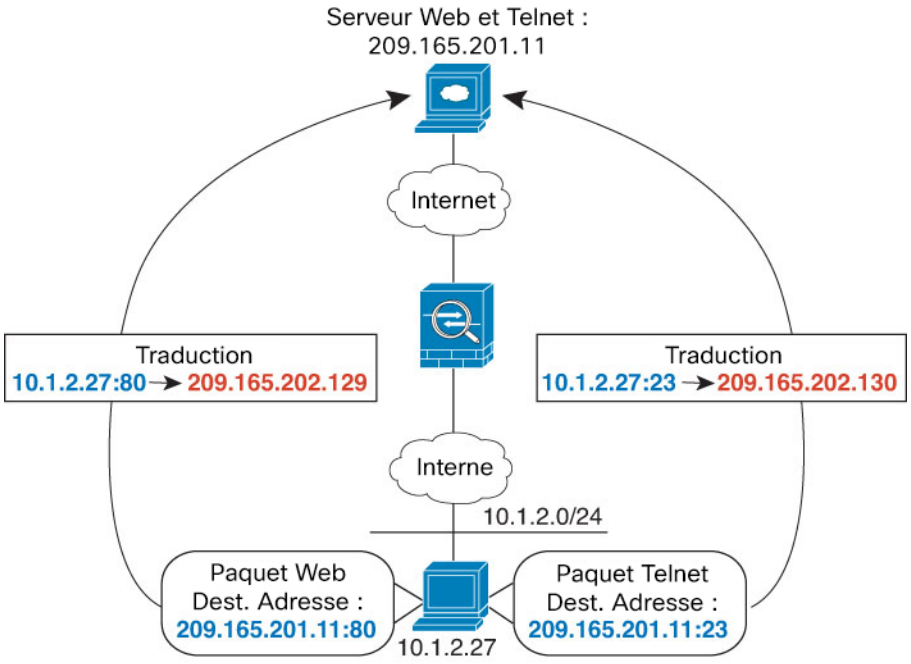
c) Cliquez sur **OK**.

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

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

Remarque Cet exemple suppose que l'interface interne est une interface routée standard connectée à un commutateur, avec le serveur connecté au commutateur. Si votre interface interne est une interface de groupe de ponts (BVI) et que le serveur est associé à une interface de membre de groupe de ponts, sélectionnez l'interface de membre spécifique à laquelle le serveur est associé. Par exemple, la règle peut avoir inside1_2 pour l'interface source plutôt que inside.

Illustration 16 : NAT manuelle avec différents ports de destination



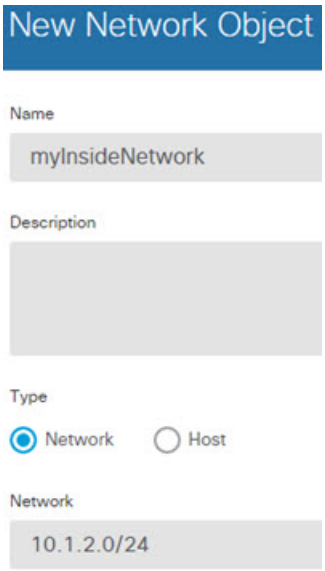
Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

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

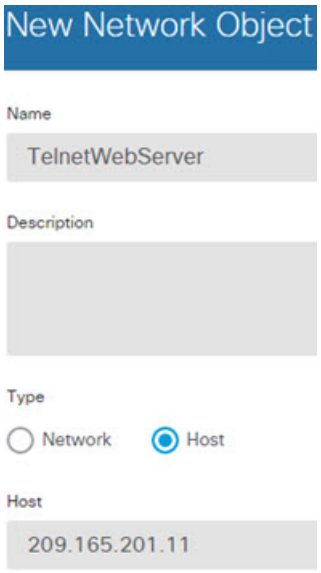


d) Cliquez sur **OK**.

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

a) Cliquez +.

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

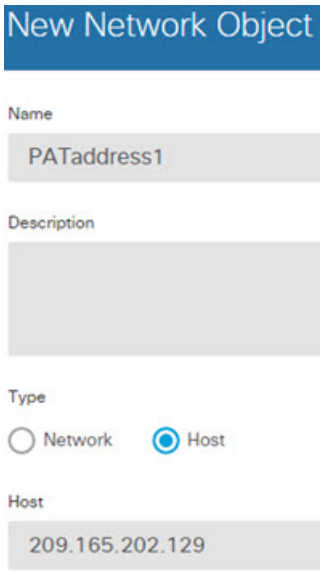


c) Cliquez sur **OK**.

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

a) Cliquez +.

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

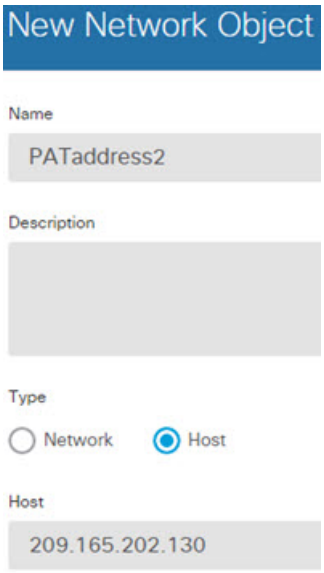


c) Cliquez sur **OK**.

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

a) Cliquez +.

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



c) Cliquez sur **OK**.

Étape 5 Configurez la PAT manuelle dynamique pour l'accès Telnet.

a) Sélectionnez **Policies (Politiques)** > **NAT**.

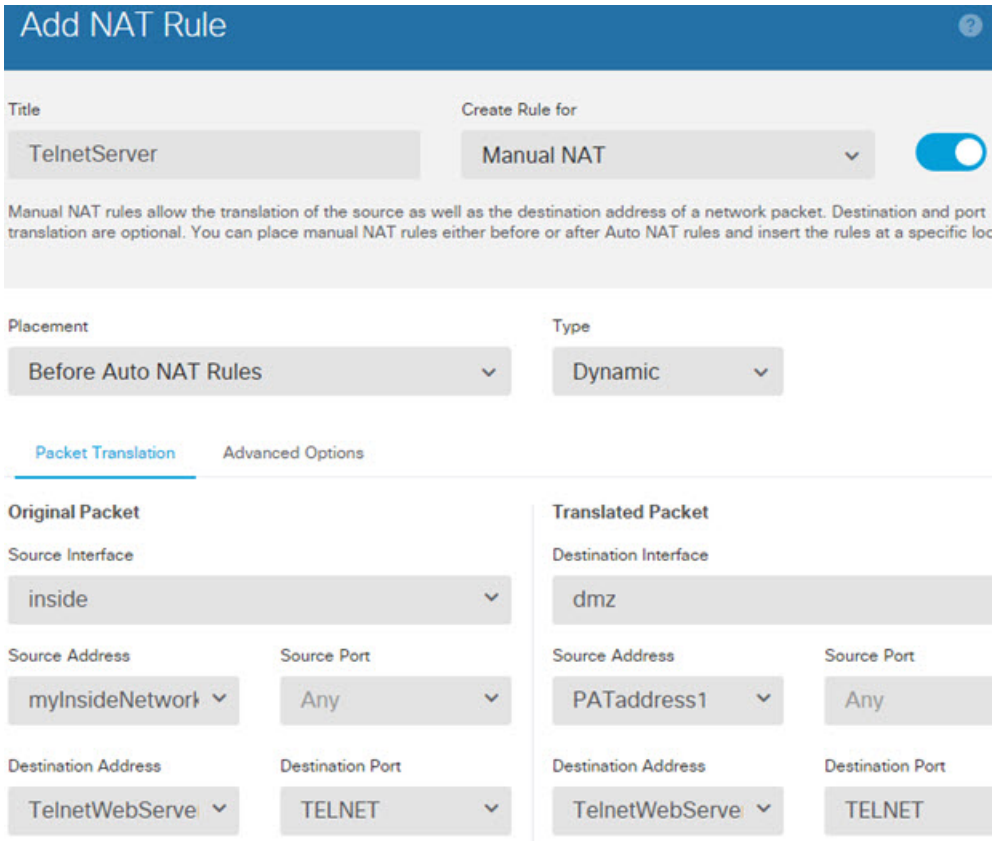
b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Title** (Titre) = TelnetServer (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress1.
- **Original Destination Address**s (Adresse de destination d'origine) = objet réseau TelnetWebServer.
- **Translated Destination Address** (Adresse de destination traduite) = objet réseau TelnetWebServer.
- **Original Destination Port** (Port de destination d'origine) = objet de port TELNET.
- **Translated Destination Port** (Port de destination traduit) = objet de port TELNET.

Remarque

Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour cette adresse en spécifiant la même adresse pour les adresses de destination d'origine et traduites, et le même port pour le port d'origine et traduit.



d) Cliquez sur **OK**.

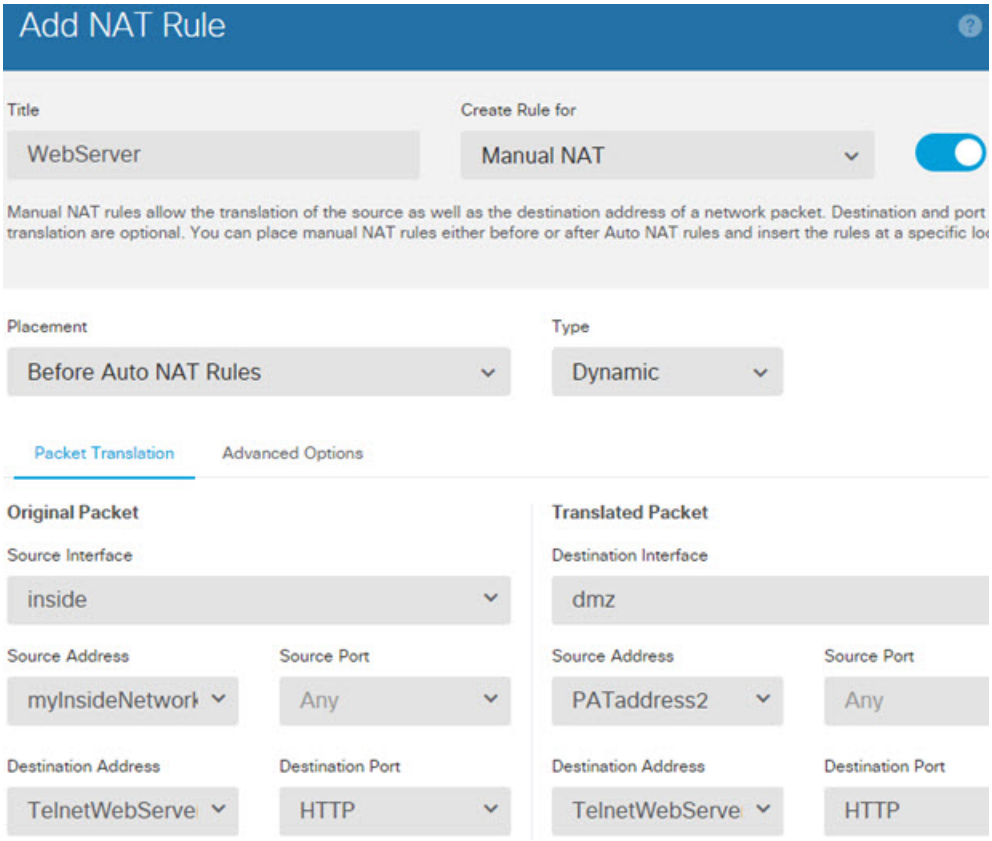
Étape 6 Configurez la PAT manuelle dynamique pour l'accès Web.

a) Cliquez sur le bouton **+**.

b) Configurez les propriétés suivantes :

- **Titre** = WebServer (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = dmz.
- **Original Source Address** (Adresse source d'origine) = objet de réseau myInsideNetwork.
- **Translated Source Address** (Adresse source traduite) = objet de réseau PATaddress2.
- **Original Destination Addres**s (Adresse de destination d'origine) = objet réseau TelnetWebServer.
- **Translated Destination Address** (Adresse de destination traduite) = objet réseau TelnetWebServer.

- **Original Destination Port** (Port de destination d'origine) = objet de port HTTP.
- **Translated Destination Port** (Port de destination traduit) = objet de port HTTP.



c) Cliquez sur **OK**.

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

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

Cette fonctionnalité réécrit l'adresse dans les requêtes DNS et les réponses qui correspondent à une règle NAT (par exemple, l'enregistrement A pour IPv4, l'enregistrement AAAA pour IPv6 ou l'enregistrement PTR pour les requêtes DNS inversées). Pour les réponses DNS passant d'une interface mappée à toute autre interface, l'enregistrement est réécrit de la valeur mappée à la valeur réelle. Inversement, pour les réponses DNS traversant une interface vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette fonctionnalité fonctionne avec NAT44, NAT 66, NAT46 et NAT64.

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

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

Limites de réécriture DNS

Voici quelques limites concernant la réécriture DNS :

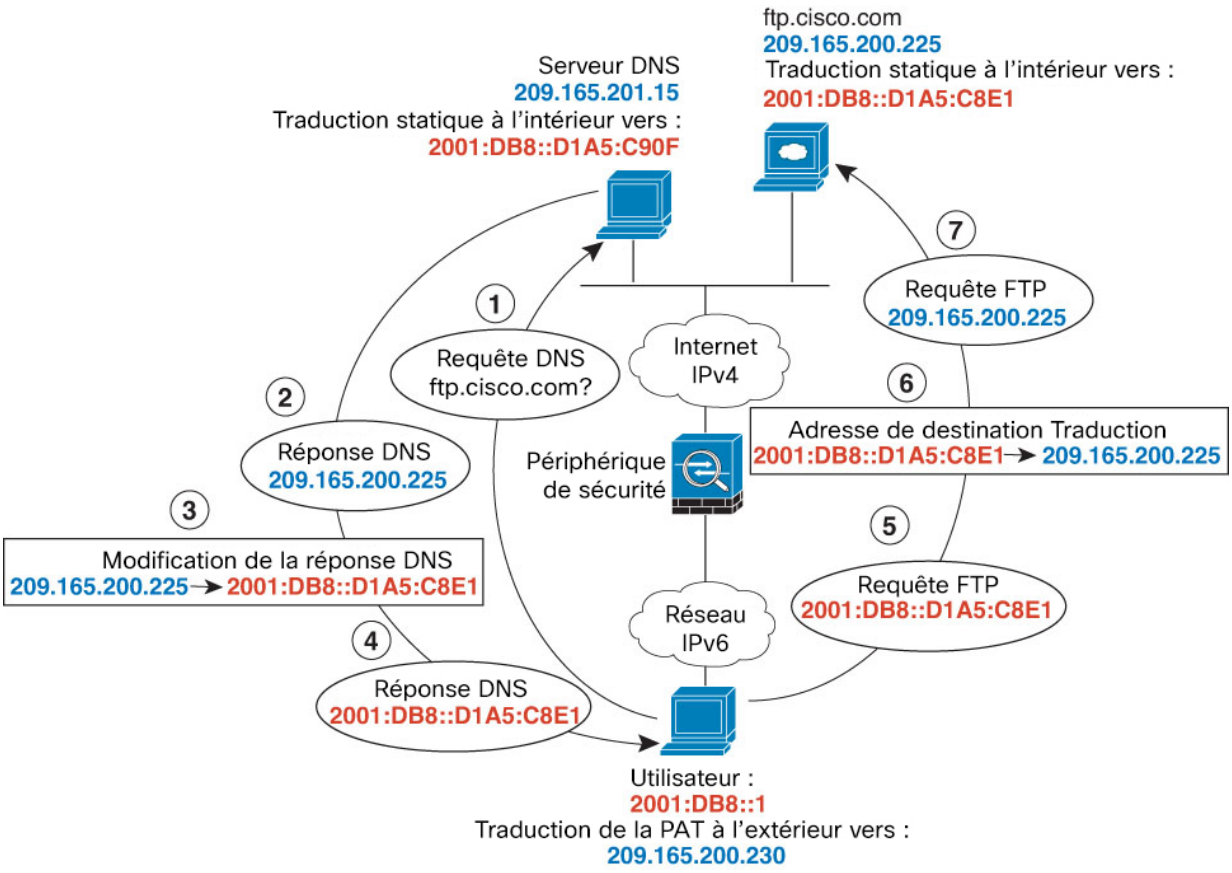
- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle manual NAT (NAT manuelle), vous ne pouvez pas configurer la modification DNS si vous spécifiez l'adresse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

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

Modification de la réponse DNS64

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

Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (2001:DB8::D1A5:C8E1, où D1A5:C8E1 est l'équivalent IPv6 de 209.165.200.225), vous devez configurer la modification de la réponse DNS pour la traduction statique. Cet exemple comprend également une traduction NAT statique pour le serveur DNS et une règle PAT pour les hôtes IPv6 internes.



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

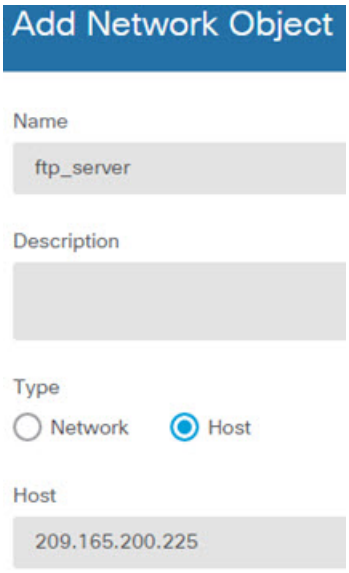
Étape 1 Créez les objets réseau pour le serveur FTP, le serveur DNS, le réseau interne et l'ensemble PAT.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Définissez l'adresse réelle du serveur FTP.

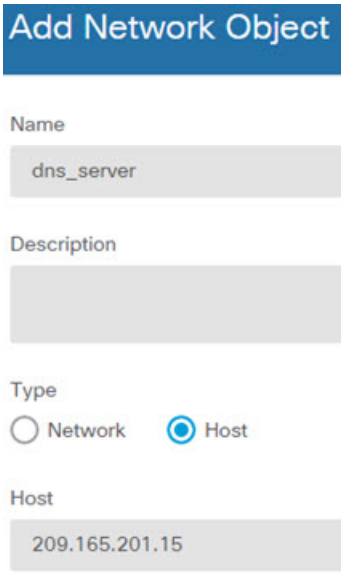
Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 209.165.200.225.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez l'adresse réelle du serveur DNS.

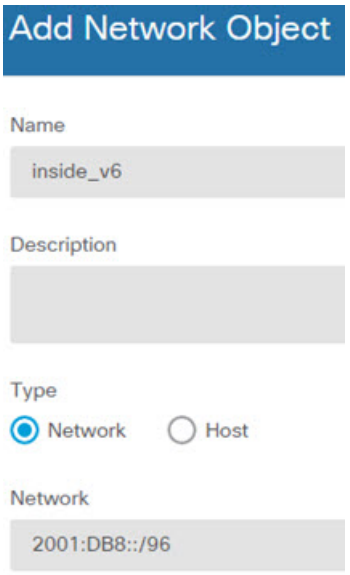
Nommez l'objet réseau (par exemple, dns_server), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 209.165.201.15.



f) Cliquez sur **OK**.

g) Cliquez sur + et définissez le réseau IPv6 interne.

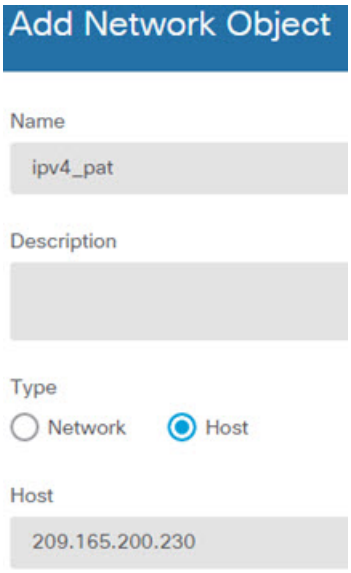
Nommez l'objet réseau (par exemple, inside_v6), sélectionnez **Network** (réseau), puis saisissez l'adresse réseau 2001:DB8::/96.



h) Cliquez sur **OK**.

i) Cliquez sur + et définissez l'adresse PAT IPv4 pour le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, ipv4_pat), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 209.165.200.230.



j) Cliquez sur **OK**.

Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

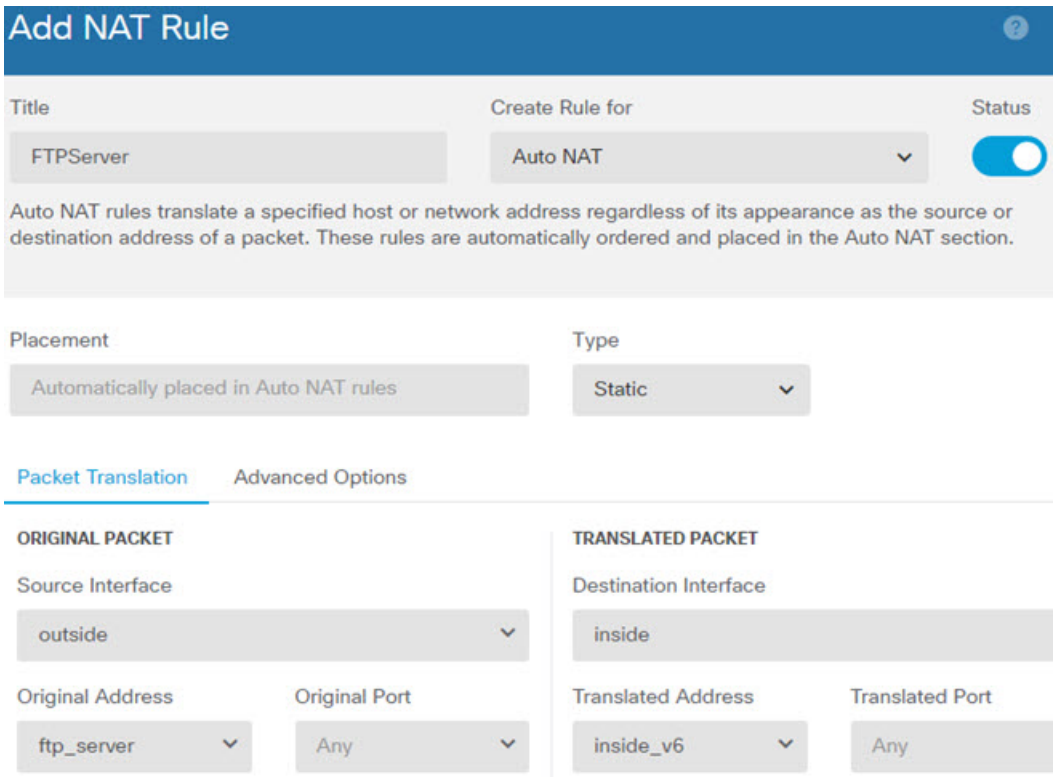
a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).

- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau ftp_server.
- **Adresse traduite** = objet réseau inside_v6. Comme la méthode d'adresse intégrée IPv4 est utilisée lors de la conversion d'IPv4 en adresses IPv6, 209.165.200.225 est converti en équivalent IPv6 D1A5:C8E1 et le préfixe de réseau est ajouté pour obtenir l'adresse complète, 2001:DB8::D1A5:C8E1.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



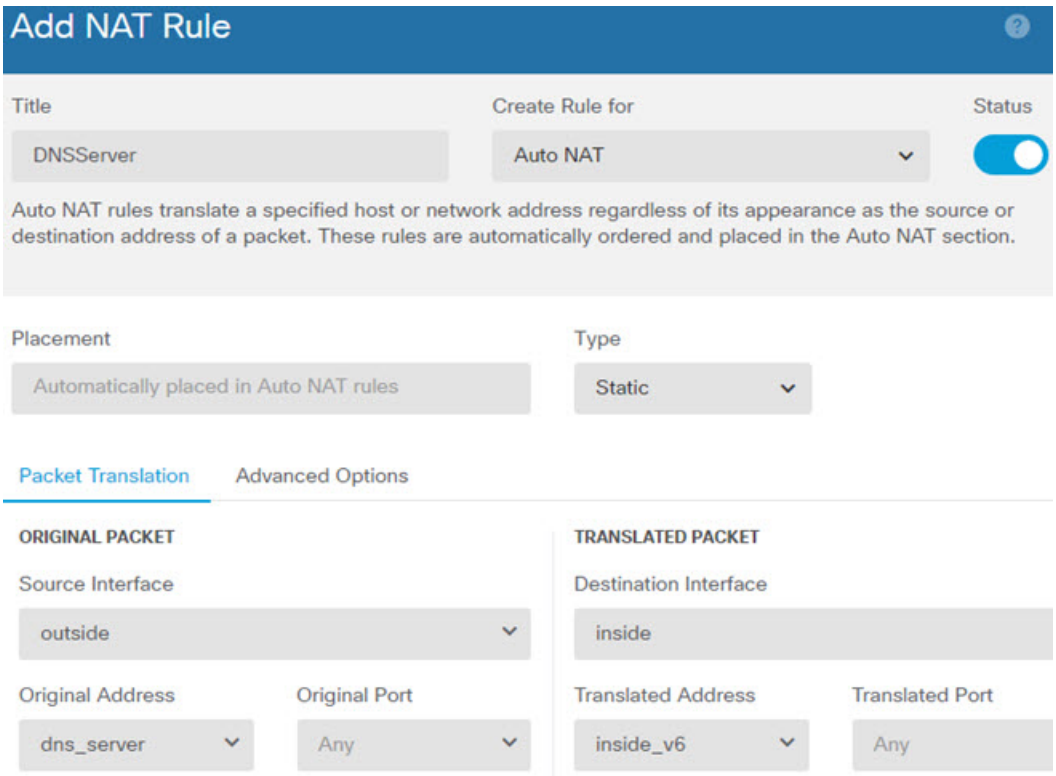
d) Cliquez sur **OK**.

Étape 3 Configurez la règle NAT statique pour le serveur DNS.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton **+**.
c) Configurez les propriétés suivantes :

- **Titre** = DNSServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Statique.

- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau dns_server.
- **Adresse traduite** = objet réseau inside_v6. Comme la méthode d'adresse intégrée IPv4 est utilisée lors de la conversion d'IPv4 en adresses IPv6, 209.165.201.15 est converti en équivalent IPv6 D1A5:C90F et le préfixe de réseau est ajouté pour obtenir l'adresse complète, 2001:DB8::D1A5:C90F.

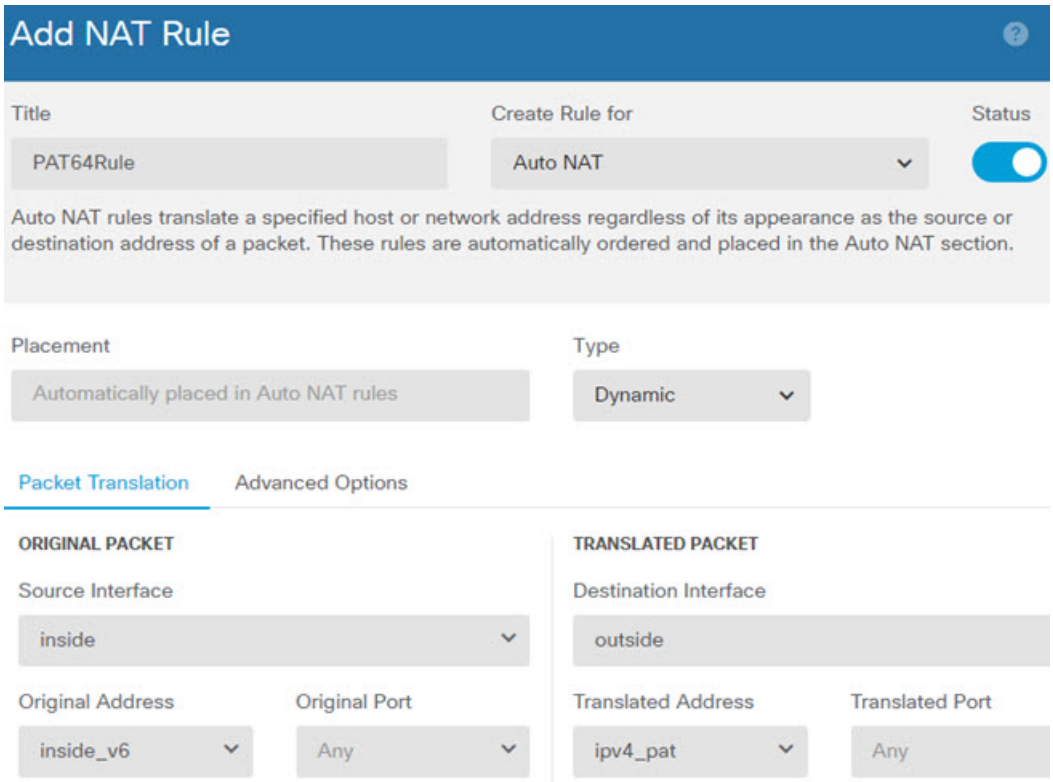


d) Cliquez sur **OK**.

Étape 4 Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = PAT64Rule (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.
- **Type** = Dynamique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Adresse originale** = inside_v6 network object.
- **Adresse traduite** = ipv4_pat network object.



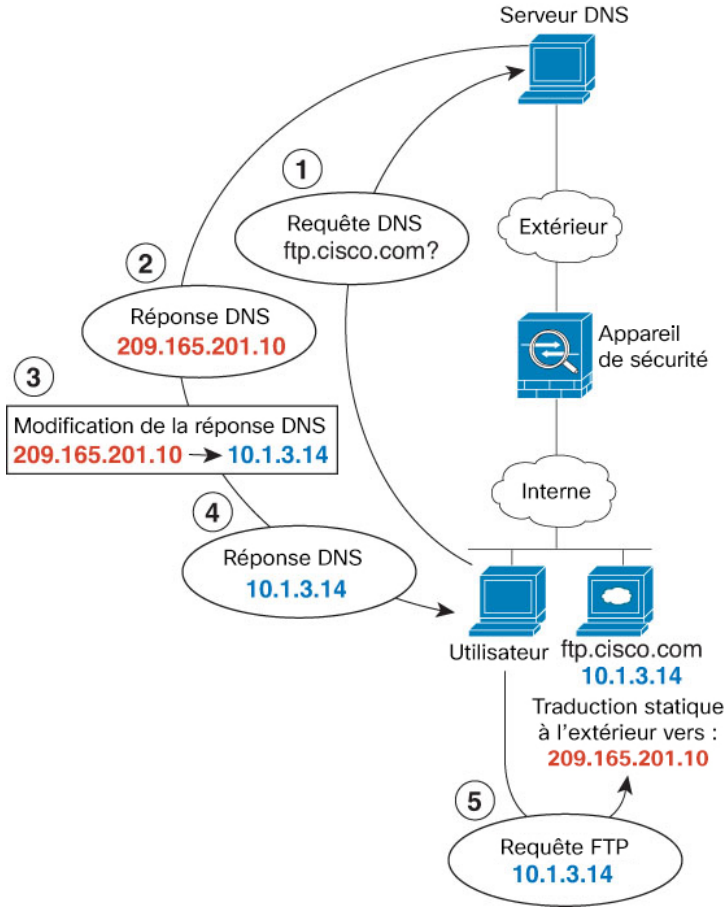
d) Cliquez sur **OK**.

Modification de la réponse DNS, serveur DNS externe

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

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

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



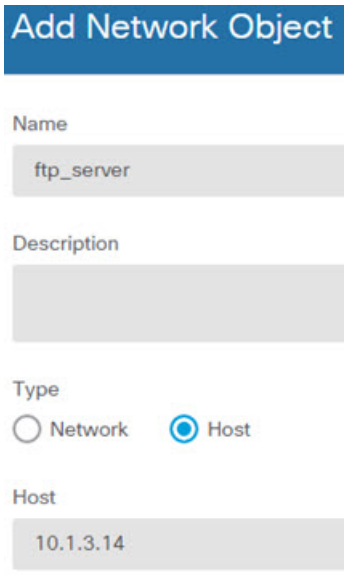
Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).
b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.
c) Définissez l'adresse réelle du serveur FTP.

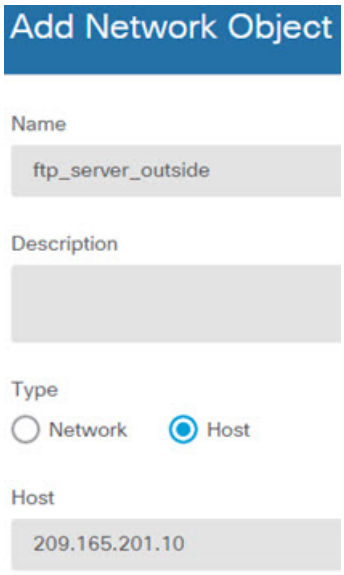
Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 10.1.3.14.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_outside), sélectionnez **Host** (Hôte), puis saisissez l'adresse de l'hôte, 209.165.201.10.



Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

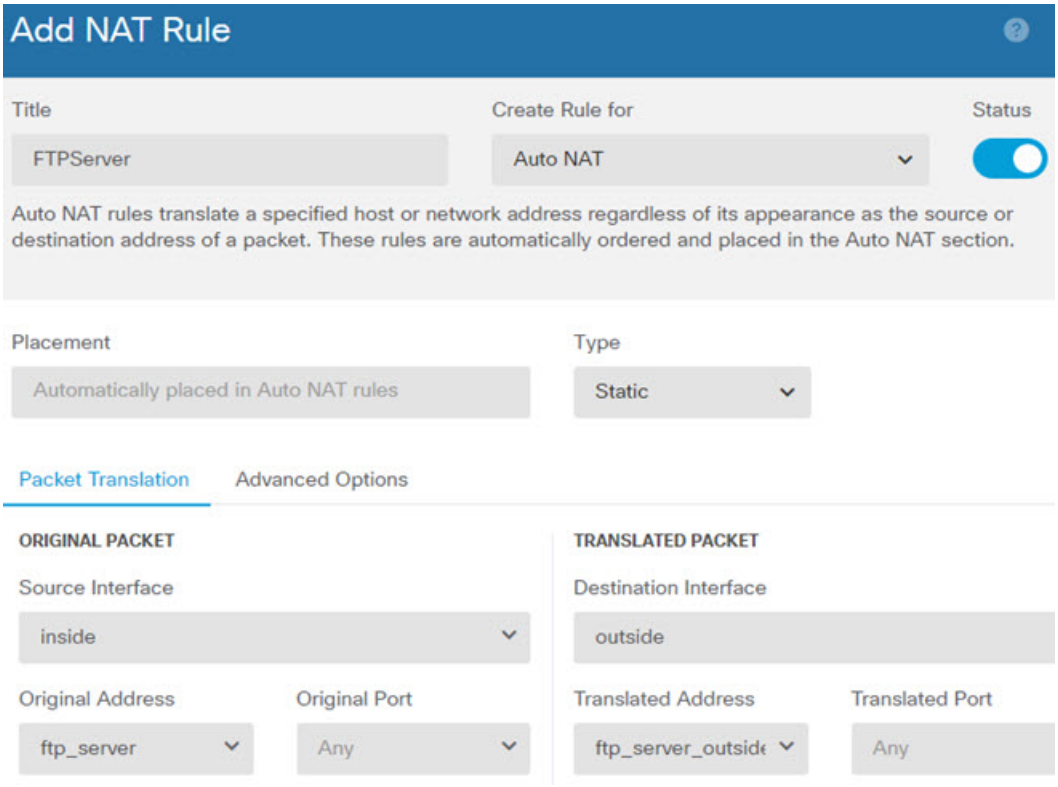
a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

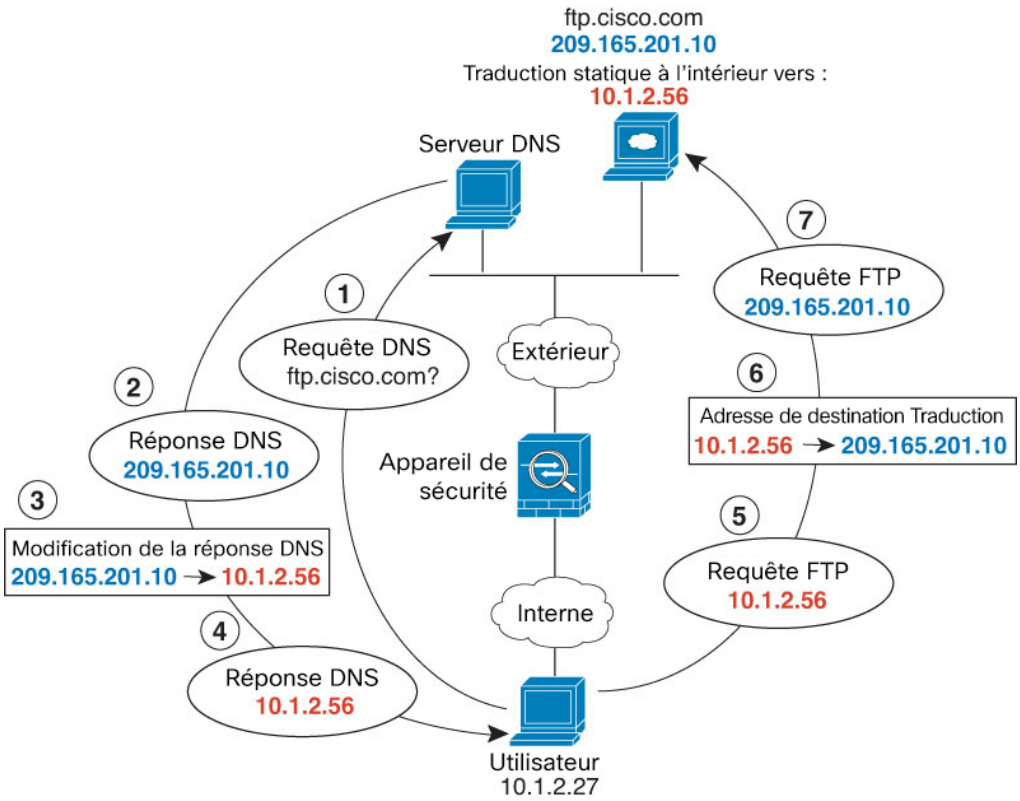
- **Type** = Statique.
- **Interface source** = interne.
- **Interface de destination** = externe.
- **Original Address (Adresse d'origine)** = objet réseau ftp_server.
- **Translated Address (Adresse traduite)** = objet réseau ftp_server_outside.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).



d) Cliquez sur **OK**.

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

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



Remarque Cet exemple suppose que l'interface interne n'est pas une interface de groupe de ponts (BVI), mais une interface routée standard. Si l'interface interne est un BVI, vous devez dupliquer les règles pour chaque interface membre.

Procédure

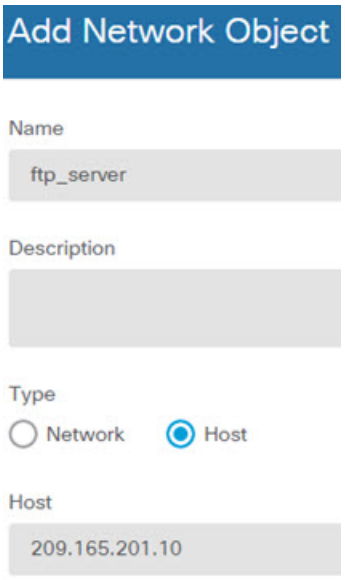
Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur **+**.

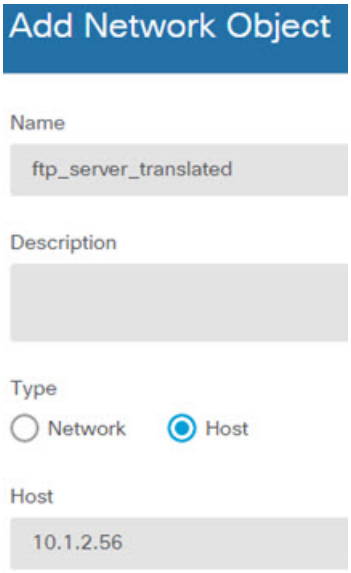
c) Définissez l'adresse réelle du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server), sélectionnez **Host** (Hôte), et saisissez l'adresse IP réelle de l'hôte, 209.165.201.10.



d) Cliquez sur **OK**.
e) Cliquez sur + et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_translated), sélectionnez **Host** (Hôte), et saisissez l'adresse de l'hôte, 10.1.2.56.

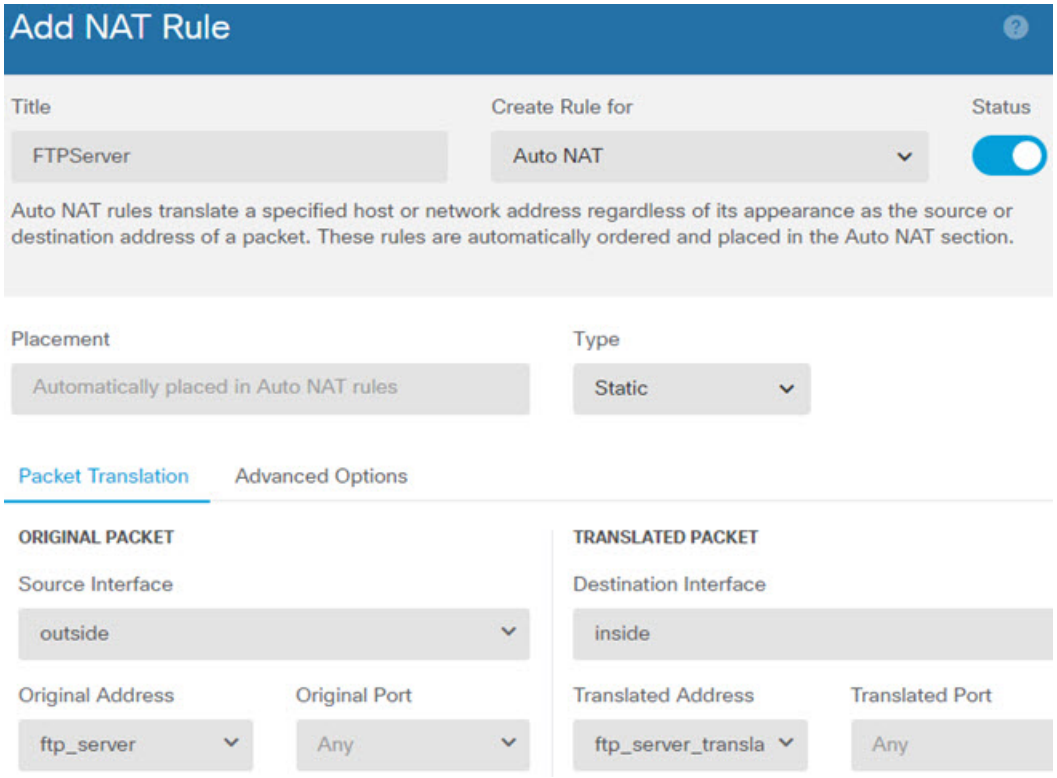


Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Policies (Politiques)** > **NAT**.
b) Cliquez sur le bouton +.
c) Configurez les propriétés suivantes :

- **Titre** = FTPServer (ou un autre nom de votre choix).
- Sélectionnez **Create Rule For** (Créer une règle pour) = Auto NAT.

- **Type** = Statique.
- **Interface source** = externe.
- **Interface de destination** = interne.
- **Adresse d'origine** = objet réseau ftp_server.
- **Adresse traduite** = objet réseau ftp_server_translated.
- Dans l'onglet **Advanced Options** (Options avancées), sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).



d) Cliquez sur **OK**.

À propos de la traduction

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