



## Routeurs virtuels

---

Ce chapitre décrit les concepts sous-jacents des routeurs virtuels et du comportement du routage virtuel dans Cisco Secure Firewall Threat Defense.

- [À propos des routeurs virtuels et du routage et transfert virtuel \(VRF\), à la page 1](#)
- [Nombre maximal de routeurs virtuels par modèle de périphérique, à la page 7](#)
- [Exigences et conditions préalables pour les routeurs virtuels, à la page 9](#)
- [Lignes directrices et limites pour les routeurs virtuels, à la page 9](#)
- [Modifications apportées à l'interface Web Centre de gestion : Page Routage, à la page 11](#)
- [Gérer les routeurs virtuels, à la page 12](#)
- [Créer un routeur virtuel, à la page 12](#)
- [Surveillance des routeurs virtuels, à la page 16](#)
- [Exemples de configuration de routeurs virtuels, à la page 16](#)

## À propos des routeurs virtuels et du routage et transfert virtuel (VRF)

Vous pouvez créer plusieurs routeurs virtuels afin de gérer des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique.

Vous pouvez ainsi fournir une assistance à deux clients distincts ou plus concernant un ensemble d'équipements réseau communs. Vous pouvez également utiliser des routeurs virtuels pour renforcer la séparation entre les éléments de votre propre réseau, par exemple en isolant un réseau de développement de votre réseau d'entreprise général.

Les routeurs virtuels mettent en œuvre la version « allégée » du routage et transfert virtuel, ou VRF-Lite, qui ne prend pas en charge Multiprotocol Extensions for BGP (MBGP).

Lorsque vous créez un routeur virtuel, vous affectez des interfaces au routeur. Vous pouvez affecter une interface donnée à un seul routeur virtuel. Vous devez ensuite définir les routes statiques et configurer les protocoles de routage tels qu'OSPF ou BGP pour chaque routeur virtuel. Vous devez également configurer des processus de routage distincts sur l'ensemble de votre réseau, de sorte que les tables de routage sur tous les périphériques participants utilisent les mêmes processus et tables de routage par routeur virtuel. À l'aide de routeurs virtuels, vous créez des réseaux séparés logiquement sur le même réseau physique pour assurer la confidentialité du trafic qui traverse chaque routeur virtuel.

Comme les tables de routage sont distinctes, vous pouvez utiliser les mêmes espaces adresse ou se chevaucher dans les routeurs virtuels. Par exemple, vous pourriez utiliser l'espace d'adresse 192.168.1.0/24 pour deux routeurs virtuels distincts, pris en charge par deux interfaces physiques distinctes.

Notez qu'il existe des tableaux de gestion et de routage des données distincts par routeur virtuel. Par exemple, si vous affectez une interface de gestion uniquement à un routeur virtuel, la table de routage pour cette interface est distincte des interfaces de données affectées au routeur virtuel.

## Applications des routeurs virtuels

Vous pouvez utiliser des routeurs virtuels pour isoler le réseau sur des ressources partagées et/ou isoler les réseaux avec une politique de sécurité commune. Ainsi, les routeurs virtuels vous aident à réaliser :

- La séparation du trafic pour les clients grâce à des tables de routage dédiées pour chaque client ou pour les différents services.
- Une gestion de la politique de sécurité commune pour les différents services ou réseaux.
- L'accès Internet partagé pour différents services ou réseau.

## Routeurs virtuels globaux et définis par l'utilisateur

### Routeurs virtuels globaux

Pour un périphérique avec une capacité de routage virtuel, le système crée un routeur virtuel global par défaut. Le système affecte toutes les interfaces de votre réseau au routeur virtuel global. Une interface routée peut appartenir à un routeur virtuel défini par l'utilisateur ou à un routeur virtuel global. Lorsque vous mettez à niveau défense contre les menaces vers une version prenant en charge une capacité de routeur virtuel, toutes ses configurations de routage existantes sont intégrées au routeur virtuel global.

### Routeurs virtuels définis par l'utilisateur

Un routeur virtuel défini par l'utilisateur est celui que vous définissez. Vous pouvez créer plusieurs routeurs virtuels sur un périphérique. Cependant, une interface ne peut à tout moment être affectée qu'à un seul routeur virtuel défini par l'utilisateur. Si certaines des fonctionnalités sont prises en charge par les routeurs virtuels définis par l'utilisateur, d'autres ne le sont que par les routeurs virtuels mondiaux. Les routeurs virtuels définis par l'utilisateur prennent en charge le VPN de site à site basé sur le routage (VTI statique) .

### Fonctionnalités prises en charge et politiques de surveillance

Vous ne pouvez configurer le protocole EIGRP que sur le routeur virtuel global.

- OSPFv3
- RIP
- EIGRP
- IS-IS
- Routage multidiffusion
- Routage à base de règles (PBR)

ISIS et PBR sont pris en charge par Flex Config dans centre de gestion (voir [Objets FlexConfig prédéfinis](#)). Configurez uniquement les interfaces de routeur virtuel global pour ces fonctionnalités.

La configuration automatique du serveur DHCP utilise un serveur WINS/DNS ayant fait l'objet d'un apprentissage par une interface. Cette interface ne peut être qu'une interface de routeur virtuel global.

Vous pouvez configurer les fonctionnalités suivantes séparément pour chaque routeur virtuel défini par l'utilisateur :

- Routes statiques et leurs moniteurs SLA
- OSPFv2
- BGPv4/v6
- Routage et pont intégrés (IRB)
- SNMP

Les fonctionnalités suivantes sont utilisées par le système lors des interrogations ou de la communication avec le système distant (trafic initial). Ces fonctionnalités utilisent uniquement les interfaces du routeur virtuel global. Cela signifie que si vous configurez une interface pour la fonctionnalité, elle doit appartenir au routeur virtuel global. En règle générale, si le système doit rechercher une route pour atteindre un serveur externe à des fins de gestion, il le fait dans le routeur virtuel global.

- Serveur DNS, lorsqu'il est utilisé pour résoudre les noms complets utilisés dans les règles de contrôle d'accès ou pour la résolution de noms pour la commande **ping**. Si vous spécifiez **any (tout)** comme interface pour un serveur DNS, le système prend en compte les interfaces uniquement du routeur virtuel global.
- Serveur AAA ou domaine d'identité lorsqu'il est utilisé avec un VPN. Vous ne pouvez configurer le VPN que sur les interfaces appartenant au routeur virtuel global. Ainsi, les serveurs externes AAA utilisés pour le VPN, comme Active Directory, doivent être accessibles par l'intermédiaire d'une interface dans le routeur virtuel global.
- Serveur Syslog.

## Configuration des politiques pour qu'elles soient compatibles avec les routeurs virtuels

Lorsque vous créez un routeur virtuel, la table de routage de ce routeur virtuel est automatiquement séparée du routeur virtuel global ou de tout autre routeur virtuel. Cependant, les politiques de sécurité ne prennent pas automatiquement en charge les routeurs virtuels.

Par exemple, si vous écrivez une règle de contrôle d'accès qui s'applique à « toute » zone de sécurité de source ou de destination, la règle s'appliquera à toutes les interfaces de tous les routeurs virtuels. Cela pourrait en fait être exactement ce que vous voulez. Par exemple, tous vos clients peuvent vouloir bloquer l'accès à une même liste de catégories d'URL répréhensibles.

Toutefois, si vous devez appliquer une politique à l'un des routeurs virtuels mais pas à d'autres, vous devez créer des zones de sécurité qui contiennent les interfaces de ce seul routeur virtuel uniquement. Ensuite, utilisez les zones de sécurité contraintes de virtual-routeur-constrained dans les critères de source et de destination de la politique de sécurité.

En utilisant des zones de sécurité dont les appartenances sont limitées aux interfaces affectées à un seul routeur virtuel, vous pouvez écrire des règles compatibles avec les routeurs virtuels dans les politiques suivantes :

- Politique de contrôle d'accès.
- Politiques de prévention des intrusions et de fichiers.
- Politiques de déchiffrement SSL.
- Politique d'identité et mappages utilisateur-adresse IP. Si vous utilisez des espaces d'adresses qui se chevauchent dans les routeurs virtuels, assurez-vous de créer des domaines distincts pour chaque routeur virtuel et de les appliquer correctement dans les règles de politique d'identité.

Si vous utilisez des espaces adresses qui se chevauchent dans vos routeurs virtuels, vous devez utiliser des zones de sécurité pour vous assurer que les bonnes politiques sont appliquées. Par exemple, si vous utilisez l'espace d'adresse 192.168.1.0/24 dans deux routeurs virtuels distincts, une règle de contrôle d'accès qui spécifie simplement le réseau 192.168.1.0/24 s'appliquera au trafic dans les deux routeurs virtuels. Si ce n'est pas le résultat souhaité, vous pouvez limiter l'application de la règle en spécifiant également les zones de sécurité de source et de destination pour un seul des routeurs virtuels.

## Interconnexion des routeurs virtuels

### Fuite de route statique et dynamique

Vous pouvez configurer le périphérique pour acheminer le trafic entre les routeurs virtuels. Ce processus de fuite de route peut être effectué manuellement en configurant des routes statiques ou dynamiquement via les paramètres de BGP.

### Fuite de route statique

Vous pouvez configurer des routes statiques pour acheminer le trafic entre les routeurs virtuels.

Par exemple, si vous avez l'interface externe dans le routeur virtuel global, vous pouvez configurer des routes statiques par défaut dans chacun des autres routeurs virtuels pour envoyer le trafic vers l'interface externe. Ensuite, tout trafic qui ne peut pas être acheminé dans un routeur virtuel donné est envoyé au routeur global pour le routage ultérieur.

Les routes statiques entre les routeurs virtuels sont appelées fuites de route, car vous faites fuiter du trafic vers un autre routeur virtuel. Lorsque vous communiquez des fuites de routes, par exemple des routages VR1 vers VR2, vous pouvez initier des connexions de VR2 à VR1 uniquement. Pour que le trafic passe de VR1 à VR2, vous devez configurer la route inverse. Lorsque vous créez une voie de routage statique vers une interface dans un autre routeur virtuel, vous n'avez pas besoin de préciser d'adresse de la passerelle. Sélectionnez simplement l'interface de destination.

Pour les routes inter-routeurs virtuels, le système recherche l'interface de destination dans le routeur virtuel source. Ensuite, il recherche l'adresse MAC du prochain saut dans le routeur virtuel de destination. Ainsi, le routeur virtuel de destination doit avoir une route dynamique (acquise) ou statique pour l'interface sélectionnée pour l'adresse de destination.

La configuration de règles NAT qui utilisent des interfaces source et de destination dans différents routeurs virtuels peut également permettre au trafic d'être acheminé entre les routeurs virtuels. Si vous ne sélectionnez pas l'option permettant à la NAT d'effectuer une recherche de routage, la règle enverra simplement le trafic hors de l'interface de destination avec une adresse NATée chaque fois que la traduction de destination se

produit. Cependant, le routeur virtuel de destination doit avoir une voie de routage pour l'adresse IP de destination traduite afin que la recherche du saut suivant puisse réussir.

Bien que la règle NAT entraîne une fuite du trafic d'un routeur virtuel à un autre, pour assurer un routage correct, nous vous recommandons de configurer une fuite de route statique entre ces routeurs virtuels pour le trafic traduit. Sans la fuite de route, la règle peut ne pas correspondre au trafic attendu et la traduction peut ne pas être appliquée.

Le routage virtuel ne prend pas en charge les fuites de routage en série ou en chaîne. Par exemple, supposons que votre défense contre les menaces comporte des routeurs virtuels VR1, VR2 et VR3; VR3 est directement connecté à un réseau – 10.1.1.0/24. Maintenant, supposons que vous configuriez une fuite de route dans VR1 pour le réseau 10.1.1.0/24 par l'interface dans VR2 et que vous définissiez une fuite de route pour la 10.1.1.0/24 par VR3. Cette chaîne de fuites de route ne permettra pas au trafic de passer de VR1 à VR2, puis de sortir de VR3. En cas de fuites de route, les recherches de routage déterminent d'abord l'interface de sortie de la table de routage d'entrée du routeur virtuel, puis examine la sortie de la table de routage du routeur virtuel pour la recherche du saut suivant. L'interface de sortie doit correspondre dans les deux recherches. Dans notre exemple, les interfaces de sortie ne seront pas les mêmes et, par conséquent, le trafic ne passera pas.

Utilisez la route inter-VRF statique avec prudence lorsque le réseau de destination n'est pas un sous-réseau connecté directement du VR en amont (sortant). Par exemple, supposons deux VR : VR1 et VR2. Alors que VR1 gère le trafic sortant qui obtient la voie de routage par défaut de son homologue externe par l'intermédiaire du BGP ou de tout protocole de routage dynamique, et VR2 gère le trafic entrant qui est configuré avec la voie de routage par défaut statique entre VRF avec VR1 comme prochain saut. Lorsque VR1 perd la route par défaut de son homologue, VR2 ne sera pas en mesure de détecter que son VR en amont (sortant) a perdu la route par défaut et le trafic est toujours envoyé vers VR1, qui sera finalement abandonné sans notifications. Dans ce scénario, nous vous recommandons de configurer VR2 avec une fuite de route dynamique par BGP.

### Fuite de route dynamique à l'aide de BGP

Vous pouvez mettre en œuvre une fuite de route entre routeurs virtuels en exportant les routes d'un routeur virtuel source (par exemple VR1) vers la table BGP source à l'aide de la communauté étendue cible de route, puis en important la même communauté étendue cible de route à partir de la table BGP source dans la destination table BGP, qui est utilisée à son tour par le routeur virtuel de destination (par exemple, VR2). Vous pouvez utiliser les cartes de routage pour filtrer les routes. Les routes du routeur virtuel global peuvent également être divulguées vers des routeurs virtuels définis par l'utilisateur et vice versa. La fuite de route entre les routeurs virtuels de BGP prend en charge les préfixes ipv4 et ipv6.

Pour plus de détails sur la configuration de la fuite de route BGP, consultez [Configurer les paramètres d'importation/exportation de routage BGP](#).

### Directives sur les fuites de route BGP

- Assurez-vous que toutes les routes nécessaires à la récursivité sont importées et présentes dans la table de routage du routeur virtuel d'entrée.
- ECMP est pris en charge par routeur virtuel. Par conséquent, ne configurez pas un ECMP sur différents routeurs virtuels. Les préfixes qui se chevauchent importés de différents routeurs virtuels ne peuvent pas former un ECMP. C'est-à-dire que lorsque vous tentez d'importer des routages avec des adresses qui se chevauchent de deux routeurs virtuels différents vers d'autres routeurs virtuels (un routeur virtuel global ou un routeur virtuel défini par l'utilisateur), une seule route (selon l'algorithme du meilleur chemin de BGP, la première qui a été annoncé) est importé dans la table de routage virtuelle respective. Par exemple, si un réseau 10.10.0.0/24 connecté à VR1 est annoncé par l'intermédiaire de BGP à un routeur virtuel global d'abord, puis à un autre réseau avec la même adresse 10.10.0.0/24, connecté à VR2 est également

annoncé par BGP à global routeur virtuel, seule la route réseau VR1 est importée dans la table de routage virtuelle globale.

- OSPFv3 n'est pas pris en charge sur les routeurs virtuels définis par l'utilisateur. Par conséquent, ne configurez pas BGPv6 pour divulguer les routeurs virtuels OSPFv3 définis par l'utilisateur vers le routeur virtuel global. Cependant, vous pouvez configurer BGPv6 pour divulguer les routages globaux du routeur virtuel OSPFv3 vers le routeur virtuel défini par l'utilisateur grâce à la redistribution.
- Il est recommandé de garder l'interface VTI et les interfaces internes protégées (interface de boucle avec retour si elle est prise en charge pour le VTI) faire partie du même routeur virtuel pour éviter le besoin d'une fuite de route.

## Chevauchement d'adresses IP

Le routeur virtuel crée plusieurs instances de tables de routage qui sont indépendantes, de sorte que les mêmes adresses IP ou qui se chevauchent peuvent être utilisées sans conflit. Défense contre les menaces permet au même réseau de faire partie de deux routeurs virtuels ou plus. Cela implique que plusieurs politiques soient appliquées au niveau de l'interface ou du routeur virtuel.

À quelques exceptions près, les fonctions de routage et la plupart des capacités NGFW et IPS ne sont pas affectées par le chevauchement des adresses IP. La section suivante décrit les fonctionnalités qui ont des limites en ce qui concerne le chevauchement d'adresses IP, ainsi que les suggestions ou recommandations pour les contourner.

### Limites relatives aux adresses IP se chevauchant

Lorsque vous utilisez une adresse IP en chevauchement dans plusieurs routeurs virtuels, afin d'assurer la bonne application de la politique, vous devez modifier les politiques ou les règles pour certaines fonctionnalités. De telles fonctionnalités exigent que vous utilisiez une interface plus spécifique en divisant la zone de sécurité existante ou en utilisant un nouveau groupe d'interfaces, selon les besoins.

Les fonctionnalités suivantes doivent être modifiées pour fonctionner correctement avec une adresse IP qui se chevauche :

- Network Map (cartographie du réseau) : modifiez la politique de découverte de réseau pour exclure certains segments IP en chevauchement afin d'assurer qu'il n'y a pas d'adresse IP qui se chevauche en cours de mappage.
- Politique d'identité : la source du flux d'identité ne peut pas faire la différence entre les routeurs virtuels; pour contourner cette limitation, mappez les espaces d'adresses qui se chevauchent ou les routeurs virtuels dans différents domaines.

Pour les fonctionnalités suivantes, vous devez appliquer des règles sur des interfaces spécifiques pour vous assurer que différentes politiques sont appliquées sur les segments IP qui se chevauchent :

- Politique d'accès
- Politique de préfiltre
- Limite de QoS/débit
- Politique SSL

### Fonctionnalités non prises en charge avec adresses IP en chevauchement

- Règle basée sur SGT ISE dans la politique d'AC : la balise de groupe de sécurité statique (SGT) avec les mappages d'adresses IP téléchargés à partir du moteur de services de vérification des identités de Cisco (ISE) ne reconnaît pas les routeurs virtuels. Configurez des systèmes ISE distincts par routeur virtuel si vous devez créer différents mappages SGT par routeur virtuel. Cela n'est pas nécessaire si vous souhaitez mettre en correspondance les mêmes adresses IP avec le même numéro SGT dans chaque routeur virtuel.
- Les ensembles de serveurs DHCP qui se chevauchent ne sont pas pris en charge sur les routeurs virtuels.
- Événements et analyses : Plusieurs des analyses centre de gestion dépendent de la cartographie du réseau et des mappages d'identité qui ne peuvent pas faire la différence si la même adresse IP appartient à deux hôtes finaux différents. Par conséquent, ces analyses ne sont pas précises lorsque des segments IP se chevauchent dans le même appareil, mais dans différents routeurs virtuels.

## Configuration de SNMP sur les routeurs virtuels définis par l'utilisateur

En plus de prendre en charge SNMP sur l'interface de gestion et les interfaces de données globales des routeurs virtuels, Cisco Secure Firewall Threat Defense vous permet désormais de configurer l'hôte SNMP sur les routeurs virtuels définis par l'utilisateur.

La configuration d'un hôte SNMP sur les routeurs virtuels définis par l'utilisateur comprend le processus suivant :

1. [Configurez les interfaces du périphérique.](#)
2. [Créer un routeur virtuel](#)
3. [Configurez les hôtes SNMP sur une interface de routeur virtuel.](#)



---

**Remarque** SNMP n'est pas compatible avec les routeurs virtuels. Par conséquent, lors de la configuration du serveur SNMP sur le routeur virtuel défini par l'utilisateur, assurez-vous que l'adresse réseau n'est pas une [Chevauchement d'adresses IP](#).

---

4. [Déployer des configurations vers Cisco Secure Firewall Threat Defense.](#) Une fois le déploiement réussi, les interrogations et les dérouterments de SNMP sont envoyés au poste de gestion réseau par l'interface du routeur virtuel.

## Nombre maximal de routeurs virtuels par modèle de périphérique

Le nombre maximal de routeurs virtuels que vous pouvez créer dépend du modèle de périphérique. Le tableau suivant présente les limites maximales. Vous pouvez vérifier votre système en saisissant la commande **show vrf counters**, qui affiche le nombre maximal de routeurs virtuels définis par l'utilisateur pour cette plateforme, sans compter le routeur virtuel global. Les chiffres dans le tableau ci-dessous comprennent les routeurs utilisateur et globaux. Pour Firepower 4100/9300, ces chiffres s'appliquent au mode natif.

Pour les plateformes qui prennent en charge la capacité d'instances multiples, comme les Firepower 4100/9300, déterminez le nombre maximal de routeurs virtuels par instance de conteneur en divisant le nombre maximal de routeurs virtuels par le nombre de cœurs sur le périphérique, puis en multipliant par le nombre de cœurs affectés à de l'instance, en arrondissant au nombre entier inférieur le plus proche. Par exemple, si la plateforme prend en charge un maximum de 100 routeurs virtuels et qu'elle compte 70 cœurs, chaque cœur prendra en charge un maximum de 1,43 routeur virtuel (arrondi). Ainsi, une instance affectée de 6 cœurs prendrait en charge 8,58 routeurs virtuels, arrondis à 8, et une instance affectée de 10 cœurs prendrait en charge 14,3 routeurs virtuels (arrondis à la valeur inférieure, 14).

Modèle du périphérique	Routeurs virtuels maximums
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower de la série 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Appareils Cisco Firepower de série 9300, tous les modèles	100
Défense contre les menaces virtuelles, toutes les plateformes	30
ISA 3000	10

### Sujets connexes

[Exigences et prérequis pour les instances de conteneur](#)



# Exigences et conditions préalables pour les routeurs virtuels

## Prise en charge des modèles

Défense contre les menaces

## Domaines pris en charge

N'importe quel

## Rôles utilisateur

Admin

Administrateur de réseau

Approbateur de sécurité

# Lignes directrices et limites pour les routeurs virtuels

## Directives sur le mode pare-feu

Les routeurs virtuels sont pris en charge en mode de pare-feu routé uniquement.

## Directives relatives à l'interface

- Vous pouvez affecter une interface à un seul routeur virtuel.
- Un routeur virtuel peut avoir un nombre quelconque d'interfaces qui lui sont affectées.
- Vous pouvez affecter uniquement des interfaces routées avec des noms logiques et des VTI à un routeur virtuel défini par l'utilisateur.
- Si vous souhaitez faire passer l'interface d'un routeur virtuel à un mode sans routage, supprimez l'interface du routeur virtuel, puis modifiez son mode.
- Vous pouvez affecter une interface à un routeur virtuel, soit à partir d'un routeur virtuel global, soit à partir d'un autre routeur virtuel défini par l'utilisateur.
- Les interfaces suivantes ne peuvent pas être affectées à un routeur virtuel défini par l'utilisateur :
  - Interfaces de dépistage.
  - Membres de l'EtherChannel.
  - Membres des Interfaces redondantes.
  - Membres des BVI.
- Le VTI est un VPN basé sur le routage. Ainsi, lorsque le tunnel est établi, le trafic qui utilise VTI pour le chiffrement doit être contrôlé par le routage. Le routage statique, ainsi que le routage dynamique avec BGP, OSPFv2/v3 ou EIGRP sont pris en charge.

- Vous ne pouvez pas utiliser des interfaces qui appartiennent à des routeurs virtuels définis par l'utilisateur dans les VPN de site à site ou d'accès à distance basés sur des politiques.
- Si un routage utilise l'interface qui est déplacée ou si son routeur virtuel est supprimé, existe dans le tableau des routeurs virtuels source ou de destination, supprimez les routages avant le déplacement de l'interface ou la suppression du routeur virtuel.
- Comme des tables de routage distinctes sont conservées pour chaque routeur virtuel, lorsqu'une interface est déplacée d'un routeur virtuel à un autre routeur virtuel, qu'il soit global ou défini par l'utilisateur, le système supprime temporairement l'adresse IP configurée sur l'interface. Toutes les connexions existantes sur l'interface sont arrêtées. Ainsi, le déplacement des interfaces entre les routeurs virtuels a un effet considérable sur le trafic réseau. Prenez donc des mesures de précaution avant de déplacer des interfaces.

### Directives relatives aux routeurs virtuels mondiaux

- Les interfaces qui sont nommées et ne font pas partie d'autres routeurs virtuels font partie du routeur virtuel global.
- Vous ne pouvez pas supprimer les interfaces routées du routeur virtuel global.
- Vous ne pouvez pas modifier le routeur virtuel global.
- En général, après la configuration des interfaces, si vous vous désenregistrez et vous vous réenregistrez sur centre de gestion, la configuration de l'interface est réimportée du périphérique. Avec la prise en charge des routeurs virtuels, il y a une restriction : l'adresse IP pour seules les interfaces de routeur virtuel global est conservée.

### Directives de mise en grappe

- Lorsque la liaison de l'unité de commande échoue en raison de la défaillance de ses interfaces, l'unité supprime de la table de routage globale toutes les routes de routage de ses interfaces et propage les routes connectées inactives et statiques vers les autres unités de la grappe. Cela entraîne la suppression des routages divulgués de la table de routage des autres unités. Ces retraits ont lieu avant qu'une autre unité ne devienne une nouvelle unité de contrôle, ce qui prend environ 500 ms. Lorsqu'une autre unité devient la nouvelle unité de contrôle, ces routes sont apprises et rajoutées aux tables de routage grâce à la convergence de BGP. Ainsi, jusqu'au temps de convergence, environ une minute, les routes divulguées ne sont pas disponibles pour les événements de routage.
- Lorsqu'un changement de rôle de contrôle se produit dans une grappe, les routes divulguées apprises par BGP sont mises à jour avec le meilleur chemin ECMP. Cependant, le chemin ECMP différent du meilleur chemin n'est supprimé de la table de routage de grappe qu'après l'expiration de la minuterie de reconvergence de BGP, soit 210 secondes. Ainsi, jusqu'à l'expiration de la minuterie de reconvergence de BGP, l'ancien chemin ECMP, non le meilleur, persiste comme voie de routage préférée pour le routage des événements.

### Directives supplémentaires

- Lors de la configuration de BGP pour les routeurs virtuels, vous pouvez redistribuer les routes appartenant à différents protocoles au sein des mêmes routeurs virtuels. Par exemple, les routes OSPF VR2 ne peuvent pas être importées dans BGP VR1. Vous pouvez uniquement redistribuer OSPF VR2 dans BGP VR2, puis configurer une fuite de route entre BGP VR2 et BGP VR1.

- Vous ne pouvez pas utiliser la liste de contrôle d'accès IPv6 pour filtrer les routes dans la carte de routage. Seule la liste de préfixes est prise en charge.
- Politique de renseignements sur la sécurité : la politique de renseignements sur la sécurité n'est pas compatible avec les routeurs virtuels. Si vous ajoutez une adresse IP, une URL ou un nom DNS à la liste de blocage, tous les routeurs virtuels le bloqueront. Cette limitation est applicable sur l'interface ayant des zones de sécurité.
- Règles NAT : Ne pas mélanger les interfaces dans les règles NAT. Dans le routage virtuel, si les objets d'interface source et de destination spécifiés (groupes d'interfaces ou zones de sécurité) ont des interfaces qui appartiennent à des routeurs virtuels différents, la règle NAT détourne le trafic d'un routeur virtuel vers un autre routeur virtuel. La NAT effectue la recherche de routage dans la table de routeur virtuel pour l'interface entrante uniquement. Au besoin, définissez les routes statiques dans le routeur virtuel source pour l'interface de destination. Si vous laissez l'interface à **toute**, la règle s'applique à toutes les interfaces, quel que soit l'appartenance au routeur virtuel.
- Relais DHCP : l'interconnexion des routeurs virtuels pour le relais DHCP n'est pas prise en charge. Par exemple, si le client de relais DHCP est activé sur l'interface VR1 et que le serveur de relais DHCP est activé sur l'interface VR2, les demandes DHCP ne seront pas transférées à l'extérieur de l'interface VR2.
- Recréer un routeur virtuel supprimé : Lorsque vous créez un routeur virtuel qui a été supprimé moins de 10 secondes plus tôt, un message d'erreur s'affiche pour indiquer que la suppression du routeur virtuel est en cours. Si vous souhaitez recréer successivement un routeur virtuel supprimé, utilisez un nom différent pour le nouveau routeur virtuel.

## Modifications apportées à l'interface Web Centre de gestion : Page Routage

Les périphériques antérieurs à défense contre les menaces 6.6 et à quelques modèles de périphériques ne sont pas pris en charge avec la capacité de routage virtuel. L'interface Web centre de gestion affiche la même page de routage de centre de gestion 6.5 ou version antérieure pour les périphériques non pris en charge. Pour connaître les périphériques et la plateforme pris en charge pour le routage virtuel, consultez [Nombre maximal de routeurs virtuels par modèle de périphérique](#).

Vous pouvez configurer des routeurs virtuels dans la page de routage d'un périphérique pris en charge :

1. Accédez à **Périphériques** > **Gestion des périphériques** et modifiez le périphérique compatible avec les routeurs virtuels.
2. Cliquez sur **Routing** (routage) pour accéder à la page des routeurs virtuels.

Pour les périphériques utilisant le routage virtuel, le volet gauche de la page Routing (routage) affiche les éléments suivants :

- **Gérer les routeurs virtuels** : vous permet de créer et de gérer des routeurs virtuels.
- Liste des protocoles de routage virtuels : répertorie les protocoles de routage que vous pouvez configurer pour les routeurs virtuels.
- **Paramètres généraux** : vous permet de configurer les paramètres généraux de BGP applicables à tous les routeurs virtuels. Cochez la case **Enable BGP** (activer BGP) afin de définir d'autres paramètres BGP.

Pour configurer d'autres paramètres BGP pour un routeur virtuel, accédez à **BGP** dans les protocoles de routage virtuel .

## Gérer les routeurs virtuels

Lorsque vous cliquez sur **Manage Virtual Routeurs** (Gérer les routeurs virtuels) dans le volet Virtual Routers, la page Manage Virtual Routers s'affiche. Cette page affiche les routeurs virtuels existants sur le périphérique et les interfaces associées. Dans cette page, vous pouvez **Ajouter un routeur virtuel** (+) sur le périphérique. Vous pouvez également **Edit** (✎) et **Supprimer** (🗑) sur les routeurs virtuels définis par l'utilisateur. Vous ne pouvez pas modifier ou supprimer un routeur virtuel global. Vous pouvez uniquement **Afficher** (🔍) les détails d'un routeur virtuel global.

## Créer un routeur virtuel

### Procédure

- 
- Étape 1** Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
  - Étape 2** Cliquez sur **Routing** (Routage).
  - Étape 3** Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).
  - Étape 4** Cliquez sur **Ajouter un routeur virtuel** (+).
  - Étape 5** Dans la zone Add Virtual Router (ajouter un routeur virtuel), saisissez un nom et une description pour le routeur virtuel.

**Remarque** Si vous créez un routeur virtuel qui a été supprimé il y a moins de 10 secondes, un message d'erreur s'affiche pour indiquer que la suppression du routeur virtuel est en cours. Si vous souhaitez recréer un routeur virtuel supprimé, utilisez un nom différent pour le nouveau routeur virtuel.

- Étape 6** Cliquez sur **Ok**.  
La page Routing (routage) apparaît, affichant la page du routeur virtuel nouvellement créée.
- 

### Prochaine étape

- [Configurer un routeur virtuel](#).

## Configurer un routeur virtuel

Vous pouvez affecter des interfaces à un routeur virtuel défini par l'utilisateur et configurer les politiques de routage pour le périphérique. Bien que vous ne puissiez pas ajouter ou supprimer manuellement des interfaces pour un routeur virtuel global, vous pouvez configurer les politiques de routage pour les interfaces de périphérique.

### Avant de commencer

- Pour configurer des politiques de routage pour un routeur virtuel défini par l'utilisateur, ajoutez un routeur. Consultez [Créer un routeur virtuel](#), à la page 12.
- Tous les paramètres de configuration de routage d'un périphérique non compatible avec le routage virtuel sont également disponibles pour un routeur virtuel global. Pour en savoir plus sur les paramètres, consultez [Paramètres de routage](#).
- Seuls des protocoles de routage limités sont pris en charge pour un routeur virtuel défini par l'utilisateur.

### Procédure

- Étape 1** Dans la page **Devices > Device Management** (Périphériques > Gestion des périphériques), modifiez le périphérique virtual-router pris en charge. Accédez à **Routage**. Pour en savoir plus sur les modifications apportées à la page de routage, consultez [Modifications apportées à l'interface Web Centre de gestion : Page Routage](#), à la page 11.
- Étape 2** Dans la liste déroulante, sélectionnez le routeur virtuel souhaité.
- Étape 3** Dans la page **Virtual Router Properties** (propriétés du routeur virtuel), vous pouvez modifier la description.
- Étape 4** Pour associer des interfaces, sélectionnez-les dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).
- N'oubliez pas les éléments suivants :
- Seules les interfaces avec un nom logique sont répertoriées dans la zone **Interfaces disponibles**. Vous pouvez modifier l'interface et fournir un nom logique dans **Interfaces**. N'oubliez pas d'enregistrer les modifications pour que les paramètres prennent effet.
  - Seules les interfaces des routeurs virtuels mondiaux sont disponibles pour l'attribution; la zone **Interfaces disponibles** répertorie uniquement les interfaces qui ne sont affectées à aucun autre routeur virtuel défini par l'utilisateur. Vous pouvez affecter des interfaces physiques, des sous-interfaces, des interfaces redondantes, des groupes de ponts, des VTI et des EtherChannels à un routeur virtuel, mais pas à leurs interfaces membres. Comme les interfaces membres ne peuvent pas être nommées, elles ne peuvent pas être utilisées dans le routage virtuel.
- Vous ne pouvez attribuer l'interface de dépistage qu'au routeur virtuel global.
- Étape 5** Pour enregistrer les paramètres, cliquez sur **Enregistrer**.
- Étape 6** Pour configurer la politique de routage du routeur virtuel, cliquez sur les noms respectifs pour ouvrir la page des paramètres correspondantes :
- **OSPF** : seul OSPFv2 est pris en charge sur le routeur virtuel défini par l'utilisateur. Tous les autres paramètres pour OSPFv2 sont aussi applicables que pour une interface non compatible avec les routeurs virtuels, sauf que **Interface** vous permet de sélectionner uniquement les interfaces du routeur virtuel que vous configurez. Vous pouvez définir les politiques de routage OSPFv3 et OSPFv2 pour un routeur virtuel global. Pour en savoir plus sur les paramètres OSPF, consultez [OSPF](#).
  - **IP** : vous pouvez configurer les politiques de routage du RP uniquement pour un routeur virtuel global. Pour en savoir plus sur les paramètres IPS, consultez [RIP](#).
  - **BGP** : cette page affiche les paramètres généraux de BGP que vous avez configurés dans **Paramètres** :

- Vous ne pouvez modifier aucun de ces paramètres généraux sur cette page, à l'exception des paramètres d'ID du routeur. Vous pouvez remplacer les paramètres d'ID du routeur qui ont été définis dans la page **Settings** (Paramètres) en les modifiant sur cette page.
- Pour configurer d'autres paramètres BGP IPv4 ou IPv6, vous devez activer l'option BGP dans la page **BGP** sous **Paramètres généraux**.
- La configuration BGP pour les familles d'adresses IPv4 et IPv6 est prise en charge pour le routeur global et le routeur virtuel défini par l'utilisateur.

Pour en savoir plus sur la configuration des paramètres de BGP, consultez [BGP](#).

- **Route statique** utilisez ce paramètre pour définir l'endroit où envoyer le trafic pour un réseau de destination spécifique. Vous pouvez également utiliser ce paramètre pour créer une voie de routage statique entre les routeurs virtuels. Vous pouvez créer une fuite de route connectée ou statique en utilisant les interfaces des routeurs virtuels définis par l'utilisateur ou mondiaux. **Préfixes FMC** à une interface pour indiquer qu'elle appartient à un autre routeur virtuel et peut être utilisée pour une fuite de route. Pour que la fuite de route réussisse, ne spécifiez pas la passerelle du saut suivant.

Le tableau Static Route (routage statique) affiche le routeur virtuel dont l'interface est utilisée pour une fuite de route dans la colonne **Fuite du routeur virtuel**. S'il ne s'agit pas d'une fuite de route, la colonne affiche S/O (N/A).

Indépendamment du routeur virtuel auquel la route statique appartient, une interface Null0 est répertoriée avec les interfaces du même routeur virtuel auquel la route statique appartient.

Pour en savoir plus sur les paramètres de routage statique, consultez [Routages statiques et par défaut](#).

- **Multidiffusion** : vous pouvez configurer des politiques de routage de multidiffusion uniquement pour un routeur virtuel global. Pour en savoir plus sur les paramètres de multidiffusion, consultez [Multicast \(multidiffusion\)](#).

**Étape 7** Pour enregistrer les paramètres, cliquez sur **Enregistrer**.

---

#### Prochaine étape

- [Modifier un routeur virtuel](#).
- [Supprimer des routeurs virtuels](#)

## Modifier un routeur virtuel


Vous pouvez modifier la description et les autres politiques de routage d'un routeur virtuel.


#### Procédure

---

- Étape 1** Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
- Étape 2** Cliquez sur **Routing** (Routage).
- Étape 3** Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).

Tous les routeurs virtuels et les interfaces attribuées s'affichent dans la page **Virtual Routeurs** (Routeurs virtuels).

**Étape 4** Pour modifier un routeur virtuel, cliquez sur **Edit** () à côté du routeur virtuel souhaité.

**Remarque** Vous ne pouvez pas modifier les paramètres généraux du routeur virtuel global. Par conséquent, le routeur global ne peut pas être modifié ; en revanche, il est possible d'afficher les paramètres à l'aide de **Afficher** ()

**Étape 5** Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

---

#### Prochaine étape

- [Supprimer des routeurs virtuels](#)

## Supprimer des routeurs virtuels

#### Avant de commencer

- Vous ne pouvez pas supprimer le routeur virtuel global. Par conséquent, l'option de suppression n'est pas disponible pour le routeur virtuel global.
- Vous pouvez supprimer plusieurs routeurs virtuels à la fois.
- Toutes les politiques de routage du routeur virtuel supprimé sont également supprimées.
- Toutes les interfaces du routeur virtuel supprimé sont déplacées vers le routeur virtuel global.
- S'il existe des restrictions de mouvement des interfaces, telles qu'un chevauchement d'adresses IP, des conflits de routage, etc., vous ne pouvez supprimer le routeur qu'après avoir résolu les conflits.

#### Procédure


---

**Étape 1** Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

**Étape 2** Cliquez sur **Routing** (Routage).

**Étape 3** Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).

Tous les routeurs virtuels ainsi que les interfaces mappées sont affichés dans la page **Virtual Routers** (Routeurs virtuels).

**Étape 4** Pour supprimer un routeur virtuel, cliquez sur **Supprimer** () à côté du routeur virtuel souhaité.

**Étape 5** Pour supprimer plusieurs routeurs, tout en maintenant la touche CTRL enfoncée, cliquez sur les routeurs virtuels que vous souhaitez supprimer. Effectuez un clic droit, puis cliquez sur **Supprimer**.

**Étape 6** Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

---

## Surveillance des routeurs virtuels

Pour surveiller et dépanner des routeurs virtuels, connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes :

- **show vrf** : affiche les détails des routeurs virtuels et de leurs interfaces associées.
- **show route vrf <vrf\_name>** : affiche les détails de routage d'un routeur virtuel.
- **show run router bgp all** : affiche les détails de routage BGP de tous les routeurs virtuels.
- **show run router bgp vrf [vrf\_name]** : affiche les détails de routage de BGP d'un routeur virtuel.

## Exemples de configuration de routeurs virtuels

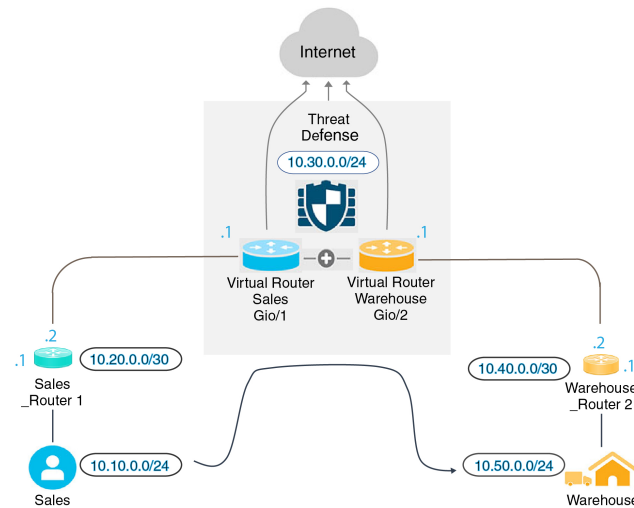
### Effectuer un routage vers un serveur distant à l'aide de routeurs virtuels

Dans le routage virtuel, vous pouvez créer plusieurs routeurs virtuels pour maintenir des tables de routage distinctes pour les groupes d'interfaces, ce qui permet de séparer les réseaux. Dans certains cas, vous pouvez avoir besoin d'accéder à un serveur qui n'est accessible que par l'intermédiaire d'un routeur virtuel distinct. Cet exemple montre la procédure qui interconnecte les routeurs virtuels pour atteindre un hôte situé à plusieurs sauts.

Prenons l'exemple d'un membre du service des ventes d'une entreprise de vêtements qui souhaite consulter le stock géré par le service d'entrepôt de son unité de production. Dans un environnement de routage virtuel, vous avez besoin d'une fuite de route entre des routeurs virtuels dont la destination (le service d'entrepôt) est éloignée de plusieurs sauts du service des ventes. Cette fuite de route se fait en ajoutant une fuite de route à sauts multiples, où vous configurez une route statique dans le routeur virtuel des ventes (source) vers une interface dans le routeur virtuel de l'entrepôt (destination). Comme le réseau de destination est éloigné de plusieurs sauts, vous devez également configurer le routeur virtuel de l'entrepôt avec la route vers le réseau de destination, à savoir 10.50.0.0/24.



Illustration 1 : Interconnexion de deux routeurs virtuels - Exemple



### Avant de commencer

Cet exemple suppose que vous avez déjà configuré Sales\_Router1 pour acheminer le trafic de l'interface 10.20.0.1/30 vers l'interface 10.50.0.5/24.

### Procédure

#### Étape 1

Configurez l'interface interne (Gi0/1) du périphérique à affecter au routeur virtuel des ventes :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces(interfaces)**.
- b) Modifiez l'interface Gi0/1 :
  - **Name** (Nom) : Pour cet exemple, Ventes-VR.
  - Cochez la case **Enable** (Activer).
  - Dans **IPv4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **IP Address** (adresse IP) : Saisissez 10.30.0.1/24.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

#### Étape 2

Configurez l'interface interne (Gi0/2) du périphérique à affecter au routeur virtuel de l'entrepôt :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces(interfaces)**.
- b) Modifiez l'interface Gi0/2 :
  - **Name** (Nom) : Pour cet exemple, Entrepôt-VR.
  - Cochez la case **Enable** (Activer).
  - Dans **IPv4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).

- **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP (10.30.0.1/24), car vous devez encore créer les routeurs virtuels définis par l'utilisateur.

- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

**Étape 3**

Créer des routeurs virtuels Ventes et Entrepôt et attribuer leurs interfaces :

- Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
- Choisissez **Routing > Manage Virtual Routes (gestion des routeurs virtuels)**.
- Cliquez sur **Add Virtual Router** (Ajouter un serveur virtuel) et créez Sales (ventes).
- Cliquez sur **Add Virtual Router** (Ajouter un serveur virtuel) et créez Warehouse (entrepôt).
- Dans les propriétés du routeur virtuel, sélectionnez Sales (ventes) dans la liste déroulante **Virtual Router Properties** (Propriétés du routeur virtuel), ajoutez VR-Sales comme **interface sélectionnée** et enregistrez.
- Dans les propriétés du routeur virtuel, sélectionnez Warehouse (entrepôt) dans la liste déroulante **Virtual Router Properties** (Propriétés du routeur virtuel), ajoutez VR-Warehouse comme **interface sélectionnée** et enregistrez.

**Étape 4**

Revoquez la configuration de l'interface VR-Warehouse :

- Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
- Cliquez sur **Edit** (modifier) dans l'interface VR-WareHouse. Spécifiez l'adresse IP 10.30.0.1/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP de VR-Sales, car les interfaces sont affectées séparément à deux routeurs virtuels différents.
- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

**Étape 5**

Créez des objets réseau pour le serveur d'entrepôt (10.50.0.0/24) et pour la passerelle d'entrepôt (10.40.0.2/30) :

- Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
- Choisissez **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** :
  - **Name** (nom) : Pour cet exemple, Entrepôt-Serveur.
  - **Network** (Réseau) : Cliquez sur Réseau et saisissez 10.50.0.0/24.
- Cliquez sur **Save** (enregistrer).
- Choisissez **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** :
  - **Name** (nom) : Pour cet exemple, Warehouse-Gateway.
  - **Network** (réseau) : Cliquez sur Host (Hôte), puis saisissez 10.40.0.2.
- Cliquez sur **Save** (enregistrer).

**Étape 6**

Définissez la fuite de route dans Ventes qui pointe vers l'interface VR-Warehouse :

- Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
- Choisissez **Routage**.
- Choisissez Sales virtual router (routeur virtuel de ventes) dans la liste déroulante, puis cliquez sur **Static Route** (route statique).

- d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
- **Interface** : Sélectionnez VR-Warehouse.
  - **Network** (réseau) : Sélectionnez l'objet Warehouse-Server.
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
VR-Warehouse

Available Network  +  
Search

any-ipv4  
IPv4-Benchmark-Tests  
IPv4-Link-Local  
IPv4-Multicast  
IPv4-Private-10.0.0.0-8  
IPv4-Private-172.16.0.0-12

Add

Selected Network  
Warehouse-Server

Gateway\*  
 +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
 +

Cancel OK

- e) Cliquez sur **Ok**.
- f) Cliquez sur **Save** (enregistrer).

## Étape 7

Dans le routeur virtuel de l'entrepôt de données, définissez la voie de routage qui pointe vers la passerelle du routeur de l'entrepôt de données 2 :

- Choisissez Routeur virtuel de l'entrepôt dans la liste déroulante, puis cliquez sur **Static Route** (Route statique).
- Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : Sélectionnez VR-Warehouse.
  - **Network** (réseau) : Sélectionnez l'objet Warehouse-Server.
  - **Gateway** (Passerelle) : Sélectionnez l'objet Warehouse-Gateway.

### Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
VR-Warehouse

Available Network  +

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Add

Selected Network  
Warehouse-Server

Ensure that egress virtualrouter has route to that destination

Gateway  
Warehouse-Gateway +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
+

Cancel OK

- c) Cliquez sur **Ok**.  
d) Cliquez sur **Save** (enregistrer).

**Étape 8** Configurez la règle de contrôle d'accès qui permet l'accès au serveur d'entrepôt. Pour créer la règle de contrôle d'accès, vous devez créer des zones de sécurité. Utilisez **Objects (objets) > Object Management (gestion des objets) > Interfaces**. Choisissez **Add (Ajouter) > Security Zone** (zones de sécurité) et créez des zones de sécurité pour VR-Sales et VR-Warehouse; pour l'objet réseau Warehouse-Server, créez un groupe d'interfaces Warehouse-Server (choisissez **Add (Ajouter) > Interface Group (Groupe d'interfaces)**).

**Étape 9** Choisissez **Policies (Politiques) > Access Control** (Contrôle d'accès) et configurez une règle de contrôle d'accès pour autoriser le trafic des interfaces source du routeur virtuel des ventes vers les interfaces de destination du routeur virtuel d'entrepôt pour l'objet réseau de destination Warehouse-Server.

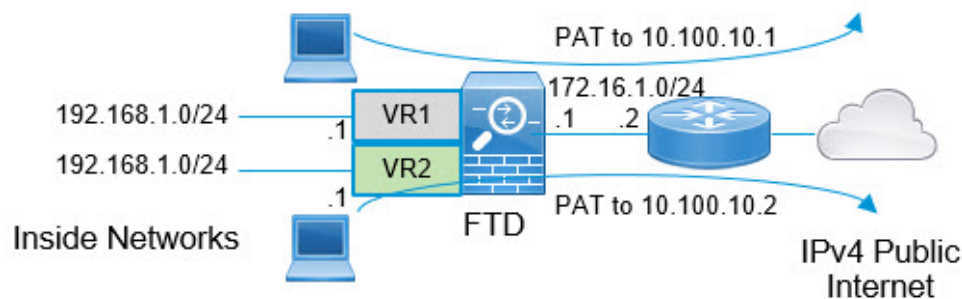
Par exemple, si les interfaces dans Sales se trouvent dans la zone de sécurité Sales-Zone et que celles de l'entrepôt sont dans la zone de sécurité Warehouse-Zone, la règle de contrôle d'accès ressemblera à ce qui suit :

SalesWarehouse														Analyze Hit Counts
Enter Description														
Rules														Inheritance Settings   Policy
Security Intelligence														Prefilter Policy: Default Prefilter Policy
HTTP Responses														SSL Policy: None
Logging														Id
Advanced Settings														
Filter by Device														Search Rules
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	
Mandatory - SalesWarehouse (1-1)														
1	Warehouse-Rule	Sales-Zone	Warehouse-Zone	Any	10.50.0.5	Any	Any	Any	Any	Any	Any	Any	Allow	

## Fournir un accès Internet avec des espaces d'adresses en chevauchement

Lorsque vous utilisez des routeurs virtuels, vous pouvez avoir la même adresse réseau pour les interfaces qui résident dans des routeurs distincts. Cependant, comme les adresses IP acheminées dans ces routeurs virtuels distincts sont les mêmes, appliquez les règles NAT/PAT pour chaque interface avec des pools NAT/PAT distincts pour vous assurer que le trafic de retour va vers la bonne destination. Cet exemple fournit la procédure à suivre pour configurer les routeurs virtuels et les règles NAT/PAT pour gérer les espaces adresses qui se chevauchent.

Par exemple, les interfaces vr1-inside et vr2-inside sur FTD sont définies pour utiliser l'adresse IP 192.168.1.1/24 et gérer les points de terminaison sur leur segment dans le réseau 192.168.1.0/24. Pour autoriser l'accès Internet à partir de deux routeurs virtuels qui utilisent le même espace d'adresse, vous devez appliquer les règles NAT séparément aux interfaces de chaque routeur virtuel, préférablement en utilisant des pools NAT ou PAT distincts. Vous pouvez utiliser PAT pour traduire les adresses sources de VR1 en 10.100.10.1 et, pour celles de VR2, en 10.100.10.2. L'illustration suivante montre cette configuration, où l'interface externe accessible à Internet fait partie du routeur global. Vous devez définir les règles NAT/PAT avec l'interface source (vr1-inside et vr2-inside) explicitement sélectionnée : l'utilisation de « any » comme interface source empêche le système d'identifier la bonne source, car la même adresse IP pourrait exister sur deux interfaces différentes.



### Remarque

Même si certaines interfaces dans les routeurs virtuels n'utilisent pas d'espaces d'adresses qui se chevauchent, définissez la règle NAT avec l'interface source pour faciliter le dépannage et pour assurer une séparation plus nette entre le trafic et le trafic des routeurs virtuels. lié à Internet.

## Procédure

---

### Étape 1

Configurez l'interface interne du périphérique pour VR1 :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces(interfaces)**.
- b) Modifiez les interfaces que vous souhaitez affecter à VR1 :
  - **Nom** : pour cet exemple, vr1-inside.
  - Cochez la case **Enable (Activer)**.
  - Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **Adresse IP** : saisissez 192.168.1.1/24.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

### Étape 2

Configurez l'interface interne du périphérique pour VR2 :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces(interfaces)**.
- b) Modifiez les interfaces que vous souhaitez affecter à VR2 :
  - **Nom** : pour cet exemple, vr2-inside.
  - Cochez la case **Enable (Activer)**.
  - Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP, car vous devez encore créer les routeurs virtuels définis par l'utilisateur.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

### Étape 3


Configurez VR1 et la fuite de route statique par défaut vers l'interface externe :


- a) Sélectionnez **Devices (périphériques) > Device Management (gestion des périphériques)**, et modifiez le périphérique FTD.
- b) Choisissez **Routing > Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel) et créez VR1.
- c) Pour VR1, dans **les propriétés du routeur virtuel**, affectez vr1-inside et enregistrez.
- d) Cliquez sur **Static Route** (Routage statique).
- e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : Sélectionnez l'interface externe du routeur global.
  - **Réseau** : sélectionnez l'objet any-ipv4. Ce réseau est la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR1.
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route dans un autre routeur virtuel, ne fournissez pas de passerelle.

### Add Static Route Configuration


Type:  IPv4  IPv6

Interface\*

(Interface starting with this icon  signifies it is available for route leak)

Available Network  + Selected Network

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

any-ipv4 

Ensure that egress virtualrouter has route to that destination

Gateway

Metric:

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

- f) Cliquez sur **Ok**.
- g) Cliquez sur **Save** (enregistrer).

#### Étape 4

Configurez VR2 et la fuite de route statique par défaut vers l'interface externe :

- a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
- b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel) et créez VR2.
- c) Pour VR2, dans **les propriétés du routeur virtuel**, affectez vr2-inside et enregistrez.
- d) Cliquez sur **Static Route** (Routage statique).
- e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :


- **Interface** : Sélectionnez l'interface externe du routeur global.


- **Réseau** : sélectionnez l'objet any-ipv4. Ce réseau est la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR2.
- **Gateway (Passerelle)** : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas la passerelle.

Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
outside


(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Selected Network

any-ipv4 

Ensure that egress virtualrouter has route to that destination

Gateway  +

Metric:  
  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  +

- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

### Étape 5

Configurez la route statique par défaut IPv4, soit 172.16.1.2, sur l'interface externe du routeur global :

- Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
- Choisissez **Routing** (routage) et modifiez les propriétés globales du routeur.
- Cliquez sur **Static Route** (Routage statique).
- Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :




- **Interface** : Sélectionnez l'interface externe du routeur global.
- **Réseau** : sélectionnez l'objet any-ipv4. Il s'agira de la voie de routage par défaut pour tout trafic IPv4.
- **Passerelle** : si elle est déjà créée, sélectionnez le nom d'hôte dans la liste déroulante. Si l'objet n'est pas encore créé, cliquez sur **Add** (ajouter) et définissez l'objet hôte pour l'adresse IP de la passerelle à l'autre extrémité du lien de réseau sur l'interface externe, dans cet exemple, 172.16.1.2. Après avoir créé l'objet, sélectionnez-le dans le champ Gateway (Passerelle).

Add Static Route Configuration ?

Type:  IPv4  IPv6

Interface\*

(Interface starting with this icon  signifies it is available for route leak)

Available Network +

Add

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12

Selected Network

Gateway\*  
 +

Metric:

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

- e) Cliquez sur **Ok**.
- f) Cliquez sur **Save** (enregistrer).

### Étape 6

Revoquez la configuration de l'interface vr2-inside :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces).
- b) Cliquez sur **Edit** (Modifier) par rapport à l'interface vr2-inside. Spécifiez l'adresse IP au format 192.168.1.1/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP de vr1-inside, car les interfaces sont affectées séparément à deux routeurs virtuels différents.

- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

**Étape 7**

Créez la règle NAT pour le trafic PAT de l'intérieur vers l'extérieur de VR1 à 10.100.10.1.

- a) Choisissez **Périphériques** > **NAT**.
- b) Cliquez sur **New Policy (Nouvelle politique)** > **Threat Defense NAT**.
- c) Saisissez **InsideOutsideNATRule** comme nom de politique NAT et sélectionnez le périphérique **FTD**. Cliquez sur **Save** (enregistrer).
- d) Dans la page **InsideOutsideNATRule**, cliquez sur **Add Rule** (ajouter une règle) et définissez les éléments suivants :
  - **NAT Rule** (règle NAT) sélectionnez **Manuel NAT Rule** (règle NAT manuelle).
  - **Type** : sélectionnez **Dynamique**.
  - **Insérer** : ci-dessus, s'il existe une règle NAT dynamique.
  - Cliquez sur **Enabled** (Activé).
  - Dans **Interface Objects**, sélectionnez **vr1-interface object** et cliquez sur **Add to Source** (Ajouter à la source) (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**), puis sélectionnez **outside** comme **Add to Destination** (ajouter à la destination).
  - Dans **Traduction**, pour **Source originale**, sélectionnez **any-ipv4**. Pour la **source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet hôte **VR1-PAT-Pool** avec **10.100.10.1**. Sélectionnez **VR1-PAT-Pool**, comme le montre la figure ci-dessous :

- e) Cliquez sur **Ok**.
- f) Cliquez sur **Save** (enregistrer).

**Étape 8**

Ajoutez une règle NAT au trafic PAT de l'intérieur vers l'extérieur de VR2 vers la version 10.100.10.2.

- a) Choisissez **Périphériques** > **NAT**.
- b) Modifiez InsideOutsideNATRule pour définir la règle de NAT VR2 :
  - **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
  - **Type** : sélectionnez Dynamique.
  - **Insérer** : ci-dessus, s'il existe une règle NAT dynamique.
  - Cliquez sur **Enabled** (Activé).
  - Dans **Objets d'interface**, sélectionnez vr2-interface object et cliquez sur **Add to Source** (ajouter à la source) (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**) et sélectionnez outside comme **Add to Destination** (ajouter à la destination).
  - Dans **Traduction**, pour **Source originale**, sélectionnez any-ipv4. Pour **Translated Source**, cliquez sur **Add** (Ajouter) et définissez l'objet hôte VR2-PAT-Pool avec 10.100.10.2. Sélectionnez VR2-PAT-Pool, comme le montre la figure ci-dessous :

- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

### Étape 9

Pour configurer la politique de contrôle d'accès qui permet le trafic des interfaces v1-inside et vr2-inside vers l'interface externe, vous devez créer des zones de sécurité. Utilisez **Objects (objets)** > **Object Management (gestion des objets)** > **Interfaces**. Choisissez **Add (Ajouter)** > **Security Zone (Zones de sécurité)** et créez des zones de sécurité pour les interfaces v1-inside, vr2-inside et externe.

### Étape 10

Choisissez **Politiques** > **Contrôle d'accès** et configurez une règle de contrôle d'accès pour autoriser le trafic de vr1-inside-zone et vr2-inside-zone vers Outside-zone.

En supposant que vous créez des zones nommées d'après les interfaces, une règle de base qui permet à tout le trafic d'acheminer vers Internet ressemblera à ce qui suit. Vous pouvez appliquer d'autres paramètres à cette politique de contrôle d'accès :

### Add Rule

Name:   Enabled Insert:

Action:  Time Range:

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes

Available Zones

- outside-zone
- vr1-inside-zone
- vr2-inside-zone

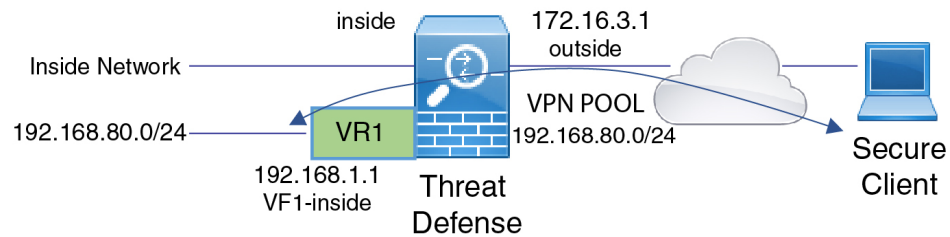
Source Zones (2)

- vr1-inside-zone
- vr2-inside-zone

## Autoriser l'accès au VPN d'accès distant aux réseaux internes dans le routage virtuel

Sur les périphériques activés pour le routage virtuel, de VPN d'accès à distance est pris en charge uniquement sur les interfaces du routeur virtuel global. Cet exemple décrit la procédure qui permet à votre utilisateur Secure Client (services client sécurisés) de se connecter aux réseaux de routeurs virtuels définis par l'utilisateur.

Dans l'exemple suivant, l'utilisateur de VPN d'accès à distance (Secure Client (services client sécurisés)) se connecte à l'interface externe de défense contre les menaces à l'adresse 172.16.3.1 et reçoit une adresse IP dans le pool de 192.168.80.0/24. L'utilisateur peut accéder au réseau interne du routeur virtuel global uniquement. Pour permettre au trafic de circuler dans le réseau du routeur virtuel défini par l'utilisateur VR1, à savoir 192.168.1.0/24, diffusez la route en configurant les routes statiques sur global et VR1.



### Avant de commencer

Cet exemple suppose que vous avez déjà configuré de VPN d'accès à distance, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

### Procédure

#### Étape 1

Configurez la fuite de route du routeur virtuel global vers le VR1 défini par l'utilisateur :

- Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
- Cliquez sur **Routing** (Routage). Par défaut, la page des propriétés de routage global s'affiche.
- Cliquez sur **Static Route** (Routage statique).
- Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : sélectionnez l'interface interne du VR1.
  - **Network** (réseau) : sélectionnez l'objet réseau du routeur virtuel VR1. Vous pouvez en créer un à l'aide de l'option **Add Object** (ajouter un objet).
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionne pas la passerelle.

Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
vr1-inside

Available Network  +

- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anycast
- nw-192.168.1.0**

Add

Selected Network  
nw-192.168.1.0

Gateway\*

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

Cancel OK

La fuite de route permet aux adresses IP Secure Client (services client sécurisés) attribuées dans l'ensemble d'adresses du VPN d'accéder au réseau 192.168.1.0/24 du routeur virtuel VR1.

e) Cliquez sur **Ok**.

## Étape 2

Configurez la fuite de route de VR1 vers le routeur virtuel global :

- a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
- b) Cliquez sur **Routing** (routage) et dans la liste déroulante, sélectionnez VR1.
- c) Cliquez sur **Static Route** (Routage statique).
- d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : Sélectionnez l'interface externe du routeur global.
  - **Network (réseau)** : Sélectionnez l'objet de réseau du routeur virtuel global.
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionne pas la passerelle.

Add Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
outside

Available Network  +

- outside-gateway
- vpn-pool**
- vr1-inside
- VR1-PAT-Pool
- vr2-inside
- VR2-PAT-Pool

Selected Network  
vpn-pool

Gateway\*

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

Cancel OK

La voie de routage statique configurée permet aux points terminaux sur le réseau 192.168.1.0/24 (VR1) d'établir des connexions avec les adresses IP attribuées à Secure Client (services client sécurisés) dans l'ensemble d'adresses du VPN.

e) Cliquez sur **Ok**.

### Prochaine étape

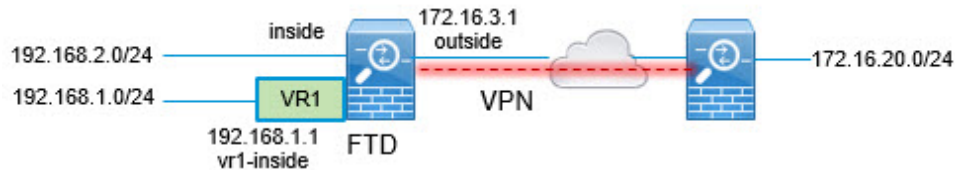
Si l'ensemble d'adresses du VPN d'accès à distance et les adresses IP du routeur virtuel défini par l'utilisateur se chevauchent, vous devez également utiliser des règles NAT statiques sur les adresses IP pour permettre un routage approprié. Vous pouvez également modifier votre ensemble d'adresses de VPN d'accès à distance afin qu'il n'y ait pas de chevauchement.

## Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Sur les périphériques activés pour le routage virtuel, le VPN de site à site est pris en charge uniquement sur les interfaces de routeur virtuel global. Vous ne pouvez pas la configurer sur une interface qui appartient à un routeur virtuel défini par l'utilisateur. Cet exemple indique la procédure qui vous permet de sécuriser les connexions depuis ou vers les réseaux hébergés dans des routeurs virtuels définis par l'utilisateur sur le VPN

de site à site. Vous devez également mettre à jour la connexion VPN de site à site pour inclure les réseaux de routage virtuels définis par l'utilisateur.

Considérons un scénario dans lequel un VPN de site à site est configuré entre un réseau de succursale et un réseau du siège social d'une entreprise; FTD de la succursale dotée de routeurs virtuels. Dans ce cas, le VPN de site à site est défini sur l'interface externe de la succursale à l'adresse 172.16.3.1. Ce VPN comprend le réseau interne 192.168.2.0/24 sans configuration supplémentaire, car l'interface interne fait également partie du routeur virtuel global. Mais, pour fournir des services VPN de site à site au réseau 192.168.1.0/24, qui fait partie du routeur virtuel VR1, vous devez divulguer la voie de routage en configurant les routes statiques sur global et VR1, et ajouter le réseau VR1 à la configuration VPN de site à site.



### Avant de commencer

Cet exemple suppose que vous avez déjà configuré le VPN de site à site entre le réseau local 192.168.2.0/24 et le réseau externe 172.16.20.0/24, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

### Procédure

#### Étape 1

Configurez la fuite de route du routeur virtuel global vers le VR1 défini par l'utilisateur :

- a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
- b) Cliquez sur **Routing** (Routage). Par défaut, la page des propriétés de routage global s'affiche.
- c) Cliquez sur **Static Route** (Routage statique).
- d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : sélectionnez l'interface interne du VR1.
  - **Network** (réseau) : sélectionnez l'objet réseau du routeur virtuel VR1. Vous pouvez en créer un à l'aide de l'option **Add Object** (ajouter un objet).
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.



Add Static Route Configuration ?

Type:  IPv4  IPv6

Interface\*  
vr1-inside

Available Network +

Search

IPv4-Private-10.0.0.0-8  
IPv4-Private-172.16.0.0-12  
IPv4-Private-192.168.0.0-16  
IPv4-Private-All-RFC1918  
IPv6-to-IPv4-Relay-Anycast  
**nw-192.168.1.0**

Add

Selected Network

nw-192.168.1.0

Gateway\*  
+

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
+

Cancel OK

La fuite de route permet aux points terminaux protégés par l'extrémité externe (distant) du VPN de site à site d'accéder au réseau 192.168.1.0/24 dans le routeur virtuel VR1.

e) Cliquez sur **Ok**.

## Étape 2


Configurez la fuite de route de VR1 vers le routeur virtuel global :

- a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
- b) Cliquez sur **Routing** (routage) et dans la liste déroulante, sélectionnez VR1.
- c) Cliquez sur **Static Route** (Routage statique).
- d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : Sélectionnez l'interface externe du routeur global.
  - **Network (réseau)** : Sélectionnez l'objet de réseau du routeur virtuel global.
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

Add Static Route Configuration

Type:  IPv4  IPv6


Interface\*  
outside

Available Network  +

Search

any-ipv4  
default-ipv4  
**external-vpn-nw**  
inside  
IPv4-Benchmark-Tests  
IPv4-Link-Local

Add

Selected Network  
external-vpn-nw 

Gateway\*  
+

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
+

Cancel OK

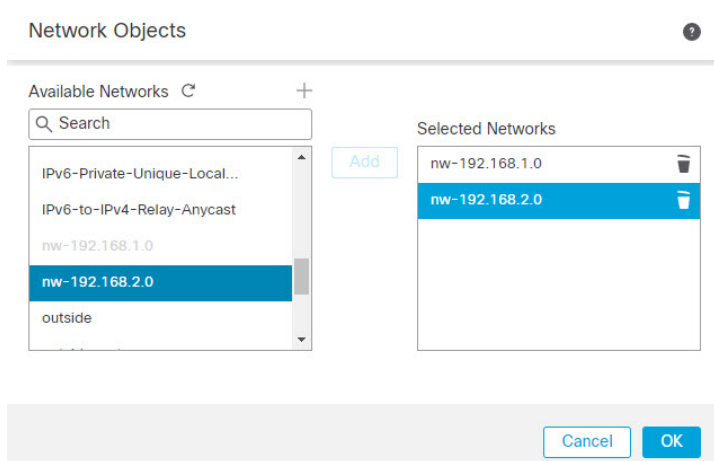
Cette voie de routage statique permet aux points terminaux sur le réseau 192.168.1.0/24 (VR1) d'établir des connexions qui traverseront le tunnel VPN de site à site. Pour cet exemple, le point terminal distant qui protège le réseau 172.16.20.0/24.

e) Cliquez sur **Ok**.

### Étape 3

Ajoutez le réseau 192.168.1.0/24 au profil de connexion VPN de site à site :

- Choisissez **Devices > VPN > Site to Site to**(périphériques VPN de site à site) et modifiez la topologie VPN.
- Dans **Endpoints** (points terminaux), modifiez le point terminal du nœud A.
- Dans le champ **Edit Endpoint** (Modifier les points terminaux), cliquez sur **Add New Network Object** (Ajouter un nouvel objet réseau) dans le champ **Protected Networks** (Réseaux protégés).
- Ajoutez l'objet réseau VR1 avec le réseau 192.168.1.0 :

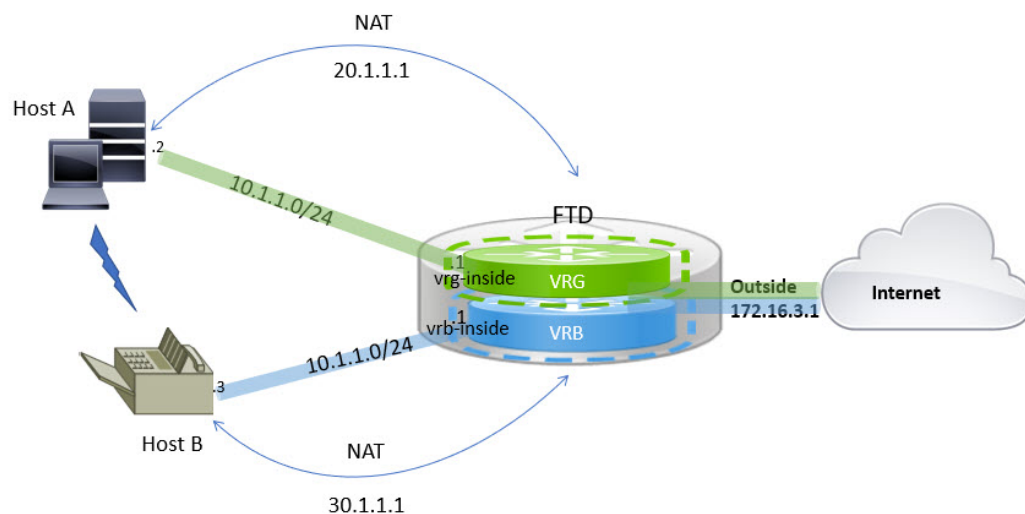


e) Cliquez sur **OK** et enregistrez la configuration.

## Acheminer le trafic entre deux hôtes réseau en chevauchement dans un routage virtuel

Vous pouvez configurer des hôtes sur les routeurs virtuels qui ont la même adresse réseau. Si les hôtes veulent communiquer, vous pouvez configurer deux fois la NAT. Cet exemple décrit la procédure à suivre pour configurer les règles NAT pour gérer l'hôte réseau en chevauchement.

Dans l'exemple suivant, deux hôtes, l'hôte A et l'hôte B, appartiennent à différents routeurs virtuels : VRG (interface vrg-inside) et VRB (interface vrb-inside), respectivement, avec le même sous-réseau 10.1.1.0/24. Pour que les deux hôtes communiquent, il faut créer une politique NAT où l'objet d'interface VRG-Hôte utiliserait une adresse NAT mappée – 20.1.1.1, et l'objet d'interface VRB-Hôte utiliserait une adresse NAT mappée – 30.1.1.1. Ainsi, l'hôte A utilise la version 30.1.1.1 pour communiquer avec l'hôte B; L'hôte B utilise la version 20.1.1.1 pour atteindre l'hôte A.



### Avant de commencer

Cet exemple suppose que vous avez déjà configuré :

- Les interfaces vrg-inside et vrb-inside sont associées aux routeurs virtuels : VRG et VRB respectivement et les interfaces vrg-inside et vrb-inside configurées avec la même adresse de sous-réseau (disons, 10.1.1.0/24).
- Les zones d'interface VRG-Inf, VRB-Inf ont été créées avec des interfaces vrg-inside et vrb-inside respectivement.
- hôte A dans VRG avec vrg-inside comme passerelle par défaut; Hôte B dans VRB avec vrb-inside comme passerelle par défaut

### Procédure

- 
- Étape 1** Créez la règle NAT pour gérer le trafic de l'hôte A vers l'hôte B. Choisissez **Devices > NAT**.
- Étape 2** Cliquez sur **New Policy (Nouvelle politique) > Threat Defense NAT**.
- Étape 3** Saisissez un nom de politique NAT et sélectionnez le périphérique défense contre les menaces . Cliquez sur **Save** (enregistrer).
- Étape 4** Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :
- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
  - **Type** : sélectionnez Statique.
  - **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
  - Cliquez sur **Enabled** (Activé).
  - Dans **Objets de l'interface**, sélectionnez l'objet VRG-Inf et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Object > Object Management > Interface**), et sélectionnez VRB-Inf objet et cliquez sur **Ajouter à la destination**.
  - Dans **Traduction**, sélectionnez les options suivantes :
    - **Source d'origine**, sélectionnez vrg-inside.
    - **Destination d'origine**, cliquez sur **Add** (ajouter) et définissez l'objet VRB-Mapped-Host avec 30.1.1.1. Sélectionnez VRB-Mapped-Host.
    - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRG-Mapped-Host avec la version 20.1.1.1. Sélectionnez VRG-Mapped-Host.
    - **Destination traduite**, sélectionnez vrb-inside, comme le montre la figure suivante :

Add NAT Rule ?

NAT Rule:  
Manual NAT Rule

Insert:  
In Category NAT Rules Before

Type:  
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:\*  
vrg-inside +

Original Destination:  
Address  
VRB-Mapped-Host +

Original Source Port:  
+

Original Destination Port:  
+

Translated Packet

Translated Source:  
Address

Translated Destination:  
VRG-Mapped-Host +  
vrb-inside +

Translated Source Port:  
+

Translated Destination Port:  
+

Lorsque vous exécutez la commande **show nat detail** sur le périphérique défense contre les menaces , vous verrez un résultat semblable à celui-ci :

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

### Étape 5

Cliquez sur **Ok**.

### Étape 6

Cliquez sur **Save** (enregistrer).

La règle NAT ressemble à ceci :

Host2Host Show Warnings

Enter Description

Rules Policies

[Filter by Device](#)

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before											
1		Static	VRG-Inf	VRB-Inf	vrg-inside	VRB-Mapped-Host		VRG-Mapped-Host	vrb-inside		Dns
Auto NAT Rules											
NAT Rules After											

Lorsque vous déployez la configuration, un message d'avertissement s'affiche :

Validation Messages: [View All \(1\)](#) ✕

---

**1 total** | 0 errors | 1 warning | 0 infos

**ManualNat64Rule: Host2Host**

▼ Warning: [ManualNatRule 1] The NAT rule has source and destination interfaces belonging to different Virtual Routers, the traffic will be able to leak between Virtual Routers without explicit route leak configuration whenever destination translation happens. If you intent to apply this NAT rule even when destination translation is not happening, create a static route leak explicitly. The rule involves interfaces from [VRG] to [VRB]

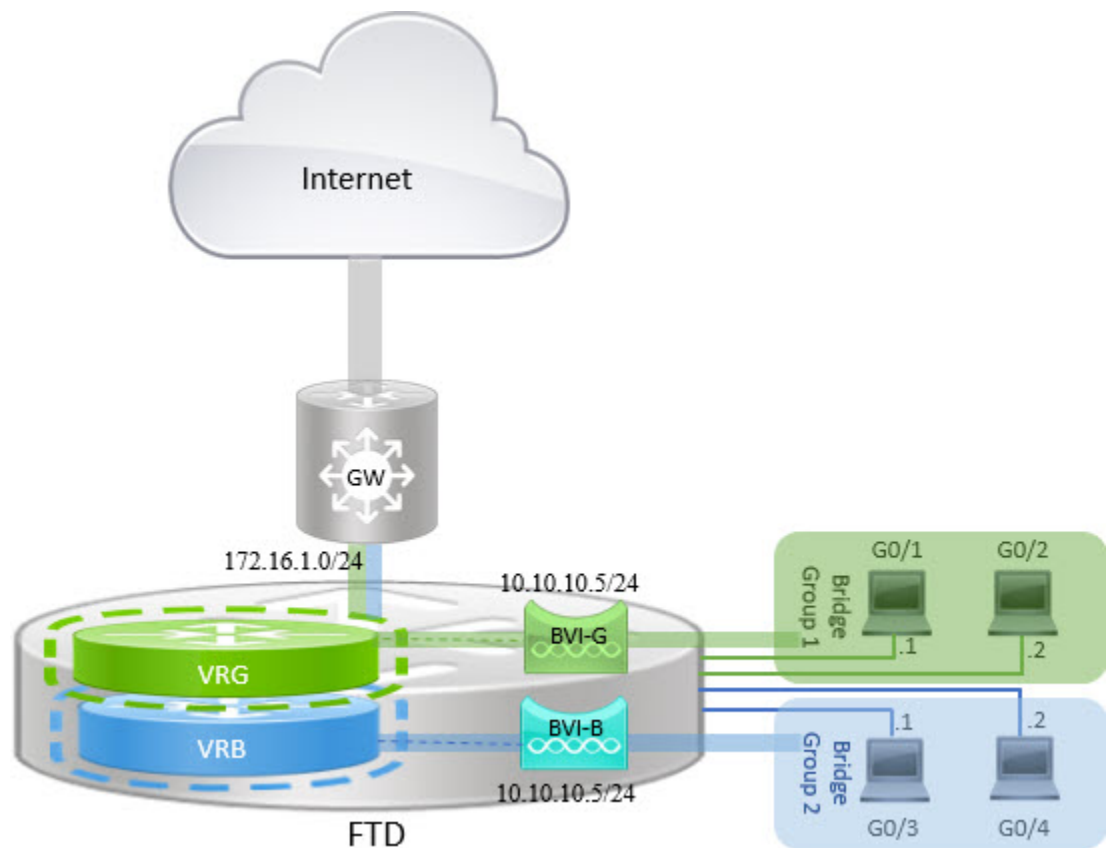
---

## Gérer les segments qui se chevauchent en mode de pare-feu routé avec des interfaces BVI

Vous pouvez déployer un seul FTD entre plusieurs réseaux qui se chevauchent de manière transparente et/ou déployer le pare-feu entre les hôtes d'un même réseau. Pour réaliser ce déploiement, configurez les BVI par routeur virtuel. La procédure de configuration des BVI dans le routeur virtuel est expliquée ici.

BVI est une interface virtuelle dans un routeur qui agit comme une interface routée normale. Il ne prend pas en charge le pont, mais représente le groupe de ponts comparable avec les interfaces routées dans le routeur. Tous les paquets entrant ou sortant de ces interfaces ponts passent par l'interface BVI. Le numéro d'interface des BVI est le numéro du groupe de ponts que l'interface virtuelle représente.

Dans l'exemple suivant, BVI-G est configuré dans VRG et le groupe de ponts 1 est l'interface routée pour les interfaces G0/1 et G0/2. De même, BVI-B est configuré dans VRB et le groupe de ponts 2 est l'interface routée pour les interfaces G0/3 et G0/4. Considérez que les deux BVI ont la même adresse IP de sous-réseau, disons 10.0.10.5/24. À cause des routeurs virtuels, le réseau est isolé sur les ressources partagées.



### Procédure

- Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**. Modifiez le périphérique requis.
- Étape 2** Dans **Interfaces( Interfaces)**, choisissez **Add Interfaces > Bridge Group Interface** (Ajouter des interfaces > interface de groupe de ponts).
- a) Saisissez les informations suivantes pour BVI-G :
- **Nom** : dans cet exemple, BVI-G.
  - **ID de groupe de ponts** : dans cet exemple, 1.
  - **Interface disponible** : Sélectionnez les interfaces.
  - Dans **IPv4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **Adresse IP** : saisissez 10.0.10.5/24.

Add Bridge Group Interface

Interfaces IPv4 IPv6

Name:  
BVI-G

Description:

Bridge Group ID \*:  
1

(1 - 250)

Available Interfaces

Search

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2**
- GigabitEthernet0/3
- GigabitEthernet0/4
- GigabitEthernet0/5

Add

Selected Interfaces

- GigabitEthernet0/1
- GigabitEthernet0/2

Cancel OK

- b) Cliquez sur **Ok**.
- c) Cliquez sur **Save** (enregistrer).
- a) Saisissez les informations suivantes pour BVI-G :
- **Nom** : dans cet exemple, BVI-G.B
  - **ID de groupe de ponts** : dans cet exemple, 2.
  - **Interface disponible** : sélectionnez les sous-interfaces.
  - Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **Adresse IP** : laissez ce champ vide, car le système ne permet pas que deux interfaces aient des adresses IP qui se chevauchent. Vous pouvez revoir le groupe de ponts et fournir la même adresse IP après l'avoir alignée sous un routeur virtuel.



Add Bridge Group Interface ?

Interfaces IPv4 IPv6

Name:

Description:

Bridge Group ID \*:  
  
(1 - 250)

Available Interfaces ↻

Search

- GigabitEthernet0/0
- GigabitEthernet0/3
- GigabitEthernet0/4
- GigabitEthernet0/5
- GigabitEthernet0/6
- GigabitEthernet0/7

Selected Interfaces

- GigabitEthernet0/3 ✕
- GigabitEthernet0/4 ✕

- b) Cliquez sur **Ok**.
- c) Cliquez sur **Save** (enregistrer).

### Étape 3

Créez un routeur virtuel, disons VRG, et sélectionnez BVI-G comme étant son réseau :

- a) Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- b) Modifiez le périphérique et choisissez **Routage > Gérer les routeurs virtuels**.
- c) Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel). Saisissez un nom pour le routeur virtuel et cliquez sur **OK**.
- d) Dans **Propriétés de routage virtuel**, sélectionnez **BVI-G** et cliquez sur **Add** (ajouter).

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers

VRG ▼

Virtual Router Properties

OSPF

▼ BGP

IPv4

Static Route

General Settings

BGP

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name:

Description:

Select Interface:

Available Interface\*

- BVI-G
- BVI-B
- vrg-inside

Selected Interfaces

- BVI-G ✕

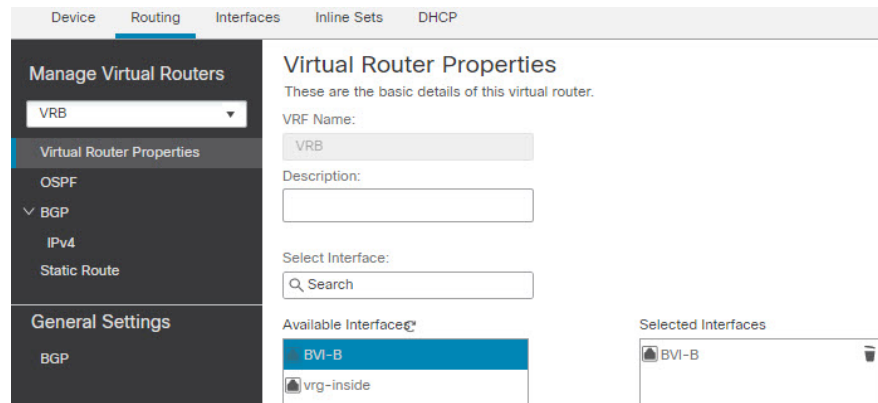
- e) Cliquez sur **Save** (enregistrer).

### Étape 4

Créez un routeur virtuel, disons VRB, et sélectionnez BVI-B comme étant son réseau :

- a) Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- b) Modifiez le périphérique et choisissez **Routage > Gérer les routeurs virtuels**.

- c) Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel). Saisissez un nom pour le routeur virtuel et cliquez sur **OK**.
- d) Dans **Propriétés de routage virtuel**, sélectionnez **BVI-B** et cliquez sur **Add** (Ajouter).



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

### Étape 5

Réexaminez la configuration de BVI-B :

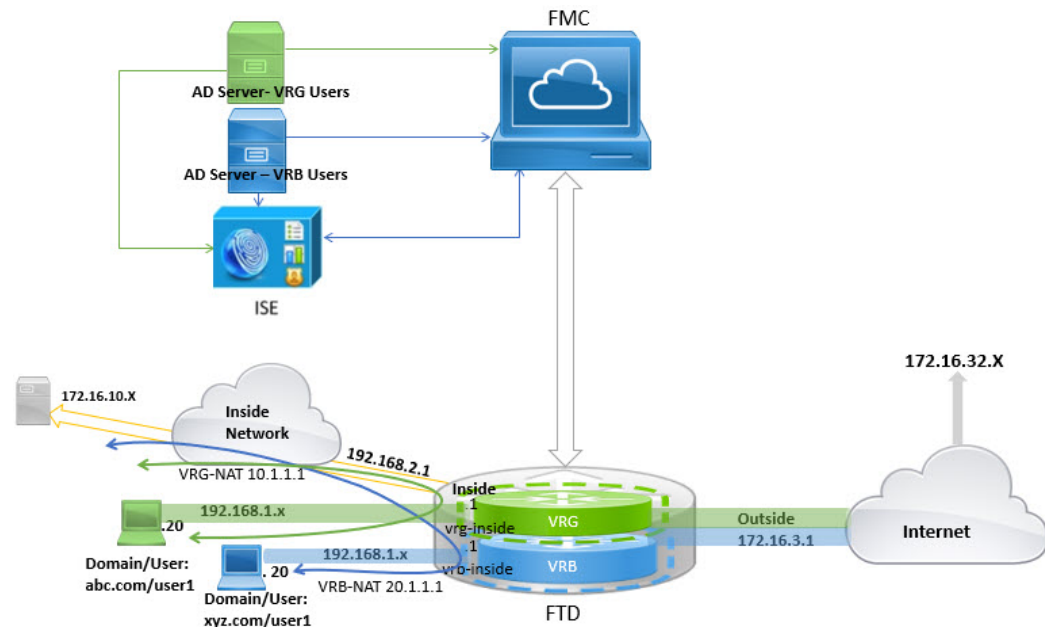
- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces).
- b) Cliquez sur **Edit** (Modifier) en regard de l'interface BVI-B. Spécifiez l'adresse IP au format 10.10.10.5/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP que BVI-G, car les interfaces sont affectées séparément à deux routeurs virtuels différents.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

Si vous souhaitez activer la communication entre BVI, utilisez un routeur externe comme passerelle par défaut. Dans les scénarios de chevauchement BVI, comme dans cet exemple, utilisez un routeur externe double NAT comme passerelle pour établir le trafic inter-BVI. Lors de la configuration de la NAT pour les membres d'un groupe de ponts, vous spécifiez l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface de groupe de ponts (BVI) elle-même. Lorsque vous effectuez une NAT entre des interfaces de membres de groupes de ponts, vous devez préciser les adresses réelles et mappées. Vous ne pouvez pas définir « any » comme interface.

## Configurer l'authentification des utilisateurs en cas de chevauchement de réseaux

Dans le routage virtuel, vous pouvez configurer plusieurs routeurs virtuels avec des adresses IP et des utilisateurs qui se chevauchent. Dans l'exemple, VRG et VRB sont les routeurs virtuels dont les adresses IP se chevauchent : 192.168.1.1/24. Les utilisateurs de deux domaines différents ont également un réseau IP 192.168.1.20 qui se chevauche. Pour que les utilisateurs de VRG et de VRB accèdent au serveur partagé 172.16.10.X, les routes de fuite vers le routeur virtuel global. Utilisez le NAT source pour gérer les adresses IP en chevauchement. Pour contrôler l'accès des utilisateurs de VRG et de VRB, vous devez définir l'authentification des utilisateurs dans FMC. FMC utilise des domaines, des répertoires actifs, une source d'identité et des règles et politiques d'identité pour authentifier l'identité des utilisateurs. Puisque FTD ne joue pas de rôle direct dans l'authentification des utilisateurs, l'accès des utilisateurs est géré uniquement par la politique de contrôle

d'accès. Pour contrôler le trafic des utilisateurs qui se chevauchent, utilisez la politique et les règles d'identité pour créer une politique de contrôle d'accès.



### Avant de commencer

Cet exemple suppose que vous disposez de :

- Deux serveurs AD pour les utilisateurs VRG et VRB.
- ISE avec les deux serveurs AD ajoutés.

### Procédure

#### Étape 1

Configurez l'interface interne du périphérique pour VRG :

- Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces).
- Modifiez les interfaces que vous souhaitez affecter à VRG :
  - **Nom** : dans cet exemple, VRG-inside.
  - Cochez la case **Enable** (Activer).
  - Dans **IPv4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **Adresse IP** : saisissez 192.168.1.1/24.
- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

#### Étape 2

Configurez l'interface interne du périphérique pour VRB :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces).
- b) Modifiez les interfaces que vous souhaitez affecter à VRB :
  - **Nom** : dans cet exemple, VRB-inside.
  - Cochez la case **Enable** (Activer).
  - Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
  - **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP, car vous devez encore créer les routeurs virtuels définis par l'utilisateur.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

### Étape 3

Configurez VRG et la fuite de route statique par défaut vers l'interface interne du routeur global pour que les utilisateurs de VRG accèdent au serveur commun 172.16.10.1 :

- a) Sélectionnez **Devices (périphériques) > Device Management** (gestion des périphériques), et modifiez le périphérique FTD.
- b) Choisissez **Routing > Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (ajouter un routeur virtuel) et créez le VRG.
- c) Pour VRG, dans **les propriétés du routeur virtuel**, affectez VRG-inside et enregistrez.

The screenshot displays the 'Virtual Router Properties' configuration page. The left sidebar shows a navigation menu with 'Manage Virtual Routers' selected, and a dropdown menu for 'VRG'. The main content area is titled 'Virtual Router Properties' and includes the following fields and sections:

- VRF Name:** VRG
- Description:** (empty text box)
- Select Interface:** A search box with 'VRG-inside' selected.
- Available Interfaces:** A list of interfaces: VRG-inside (highlighted), VRB-inside, inside, and outside.
- Selected Interfaces:** A list containing VRG-inside.

- d) Cliquez sur **Static Route** (Routage statique).
- e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : sélectionnez l'interface interne du routeur global.

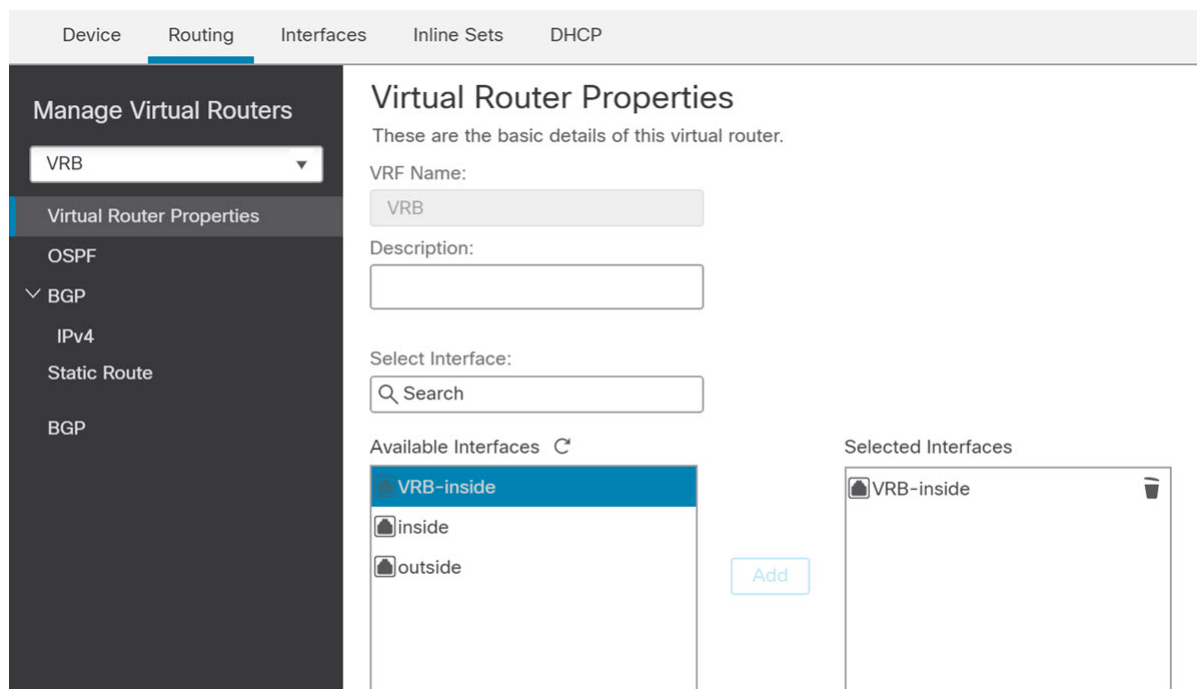
- **Réseau** : sélectionnez l'objet any-ipv4.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas de passerelle.

- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

#### Étape 4

Configurez VRB et la fuite de route statique par défaut vers l'interface interne du routeur global pour que les utilisateurs de VRB accèdent au serveur partagé 172.16.10.x :

- Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
- Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (ajouter un routeur virtuel) et créez un VRB.
- Pour VRB, dans **les propriétés du routeur virtuel**, affectez VRB-inside et enregistrez.



- Cliquez sur **Static Route** (Routage statique).
- Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
  - **Interface** : sélectionnez l'interface interne du routeur global.
  - **Réseau** : sélectionnez l'objet any-ipv4.
  - **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas de passerelle.
- Cliquez sur **Ok**.
- Cliquez sur **Save** (enregistrer).

#### Étape 5

Revoquez la configuration de l'interface VRB-inside :

- a) Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces).
- b) Cliquez sur **Edit** (modifier) en regard de l'interface VRB-inside. Spécifiez l'adresse IP au format 192.168.1.1/24. Le système vous permet maintenant d'utiliser la même adresse IP que celle du VRG-inside, car les interfaces sont affectées séparément à deux routeurs virtuels différents.
- c) Cliquez sur **Ok**.
- d) Cliquez sur **Save** (enregistrer).

**Étape 6**

Ajoutez des règles NAT pour les objets source VRG et VRB. Cliquez sur **Périphériques > NAT**.

**Étape 7**

Cliquez sur **New Policy (Nouvelle politique) > Threat Defense NAT**.

**Étape 8**

Saisissez un nom de politique NAT et sélectionnez le périphérique FTD. Cliquez sur **Save** (enregistrer).

**Étape 9**

Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez la NAT source suivante pour VRG :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Statique.
- **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
- Cliquez sur **Enabled** (Activé).
- Dans **Objets de l'interface**, sélectionnez l'objet VRG-Inside et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Objet > Gestion des objets > Interface**), sélectionnez Global-Inside Object et cliquez sur **Ajouter à la destination**.
- Dans **Traduction**, sélectionnez les options suivantes :
  - **Source d'origine**, sélectionnez VRG-Users.
  - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRG-NAT avec 10.1.1.1. Sélectionnez VRG-NAT, comme le montre la figure suivante :

## Add NAT Rule

NAT Rule:  
Manual NAT Rule

Insert:  
In Category NAT Rules Before

Type:  
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* VRG-Users +	Translated Source: Address
Original Destination: Address +	Translated Destination: VRG-NAT +
Original Source Port:	Translated Source Port:

Cancel OK

**Étape 10**

Cliquez sur **Ok**.

**Étape 11**

Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez la NAT source suivante pour VRB :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Statique.
- **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
- Cliquez sur **Enabled** (Activé).
- Dans les **objets de l'interface**, sélectionnez VRB-Inside et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Objet > Gestion des objets > Interface**), sélectionnez objet Global-Inside et cliquez sur **Ajouter à la destination**.
- Dans **Traduction**, sélectionnez les options suivantes :
  - **Source d'origine**, sélectionnez VRB-Users.
  - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRB-NAT avec la version 20.1.1.1. Sélectionnez VRB-NAT, comme le montre la figure suivante :

## Add NAT Rule

NAT Rule:  
Manual NAT Rule

Insert:  
In Category NAT Rules Before

Type:  
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* VRB-Users +	Translated Source: Address
Original Destination: Address +	Translated Destination: VRB-NAT +
Original Source Port:	Translated Source Port:

Cancel OK

## Étape 12

Cliquez sur **Save** (enregistrer).

La règle NAT ressemble à ceci :

Rules

[Filter by Device](#)

					Original Packet	
#	Direction	Type	Source Interface	Destination Interface	Original Sources	Original Destinations
NAT Rules Before						
1	↔	St...	any	any	VRG-Users	
2	↔	St...	any	any	VRB-Users	
Auto NAT Rules						

## Étape 13

Ajoutez les deux serveurs AD uniques dans FMC, un pour chaque utilisateur de VRG et VRB : choisissez **Système > Intégration > Domaines**.



- Étape 14** Cliquez sur **Nouveau domaine** et remplissez les champs. Pour de plus amples renseignements, sur les champs, voir [Champs de domaine](#).
- Étape 15** Pour contrôler l'accès des utilisateurs de VRG et de VRB, définissez deux ActiveDirectory [Créer un domaine LDAP](#) ou un [domaine Active Directory et un répertoire de domaine](#), consultez [Champs Répertoire de domaine et Synchroniser](#)
- Étape 16** Ajoutez ISE dans FMC : choisissez **Système > Intégration > Sources d'identité**.
- Étape 17** Cliquez sur **Identity Services Engine** (moteur de services d'identité) et remplissez les champs. Pour de plus amples renseignements, sur les champs, voir [Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine](#).
- Étape 18** Créez une politique d'identité et des règles, puis définissez une politique de contrôle d'accès pour contrôler l'accès des utilisateurs qui se recoupent à partir de VRG et de VRB.
- 

## Interconnecter des routeurs virtuels à l'aide de BGP

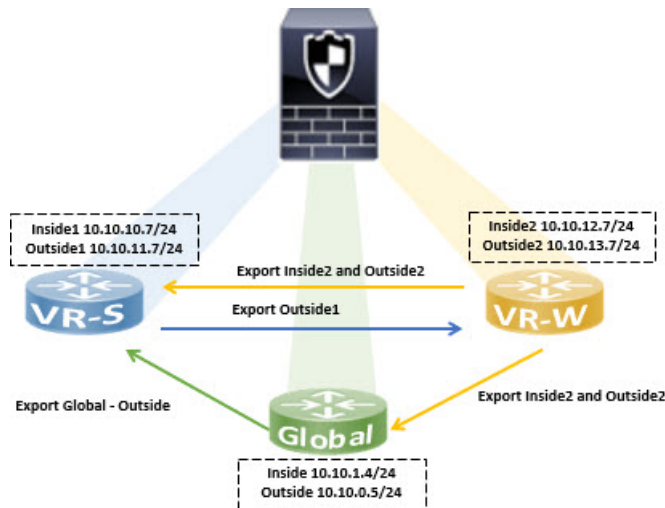
Vous pouvez maintenant configurer les paramètres de BGP sur un périphérique pour transmettre les routes entre les routeurs virtuels (routeurs virtuels mondiaux et définis par l'utilisateur). La cible de routage du routeur virtuel source est exportée vers la table BGP, qui, à son tour, est importée dans le routeur virtuel de destination. La carte de routage est utilisée pour partager les routes virtuelles globales avec les routeurs virtuels définis par l'utilisateur et vice versa. Notez que toutes les importations ou exportations des routes vers la table BGP sont configurées au niveau du routeur virtuel défini par l'utilisateur, y compris les routes virtuelles globales.

Considérez que le périphérique de pare-feu d'une usine est configuré avec les routeurs virtuels et les interfaces suivants :

- Le routeur virtuel global est configuré avec Inside (10.10.1.4/24) et Outside (10.10.0.5/24)
- Le routeur virtuel VR-S (ventes) est configuré avec Inside1 (10.10.10.8/24) et Outside1 (10.10.11.7/24)
- Le routeur virtuel VR-W (entrepôt) est configuré avec Inside2 (10.10.12.7/24) et Outside2 (10.10.13.7/24)

Supposons que vous souhaitez que les routes de l'entrepôt (VR-W) soient divulguées avec les ventes (VR-S) et globales, et les routes d'interface externe de VR-S à VR-W. De même, vous souhaitez que les routes de l'interface externe du routeur global soient divulguées aux ventes (VR-S). Cet exemple montre la procédure de configuration BGP pour interconnecter les routeurs :

Illustration 2 : Interconnecter les routeurs virtuels à l'aide des paramètres de BGP



### Avant de commencer

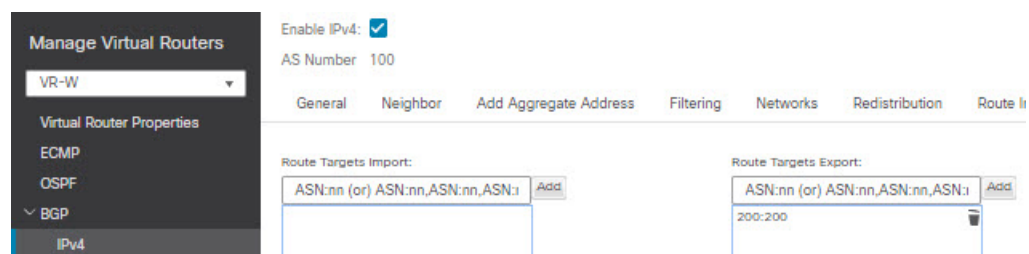
- Créer un routeur virtuel, VR-S et VR-W.
- Activez BGP et configurez BGP pour chaque routeur virtuel pour la redistribution des routes connectées.

### Procédure

#### Étape 1

Configurez VR-W pour exporter ses routages en les marquant d'une balise avec une cible de routage vers le VR-S :

- Sélectionnez **Devices (Périphériques) > Device Management (gestion des périphériques)**, modifiez le périphérique, puis cliquez sur l'onglet **Routage**.
- Dans la liste déroulante du routeur virtuel, sélectionnez VR-W.
- Cliquez sur **BGP > IPv4 > Importation/exportation de routage**.
- Pour une fuite des routes VR-W vers le VR-S, balisez les routes avec une cible de route, de sorte que les routes du VR-W soient exportées vers sa table BGP avec la cible de route marquée dessus. Dans le champ **Route Targets Export** (exportation des cibles de routage), saisissez une valeur, par exemple **200:200**. Cliquez sur **Add** (Ajouter).



- Dans la liste déroulante du routeur virtuel, sélectionnez VR-S.
- Cliquez sur **BGP > IPv4 > Importation/exportation de routage**.

- g) Pour recevoir les routes de fuite de VR-W, configurez Import Route Target (importation de cible de routage) pour importer les routes VR-W marquées avec la cible de route du tableau BGP (homologue ou redistribué). Dans le champ **Route Targets Import** (importation de cibles de routage), saisissez la valeur de la cible de routage que vous avez configurée pour VR-W, *200:200*. Cliquez sur **Add** (ajouter).

The screenshot shows the configuration interface for a virtual router. On the left, a sidebar lists various configuration options, with 'BGP' and 'IPv4' selected. The main area shows 'Enable IPv4' checked and 'AS Number' set to 100. Below, there are two input fields for 'Route Targets Import' and 'Route Targets Export'. The 'Import' field contains '200:200' and has an 'Add' button next to it. The 'Export' field is currently empty.

**Remarque** Si vous souhaitez conditionner la fuite des routes à partir de VR-W, vous pouvez spécifier les critères de correspondance dans l'objet de carte de routage et le choisir dans la carte de routage **d'exportation de routeur virtuel de l'utilisateur**. De même, si vous souhaitez conditionner les routes à importer dans VR-S à partir du tableau BGP, vous pouvez utiliser la **carte de routage d'importation de routeur virtuel de l'utilisateur**. Cette procédure est expliquée à l'étape 3.

## Étape 2

Configurez VR-W pour exporter ses routages vers le routeur virtuel global :

- Vous devez créer une carte de routage qui permette d'exporter les routes VR-W vers la table de routage globale. Choisissez **Objects (objets) > Object Management (gestion des objets) > Route Map (carte de routage)**.
- Cliquez sur **Add Route Map** (Ajouter ne carte de routage), donnez un nom, par exemple *Export-to-Global*, puis cliquez sur **Add** (Ajouter).
- Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution** :

The screenshot shows the 'New Route Map Object' configuration window. The 'Name' field contains 'Export-to-Global'. Below it, there is a section for 'Entries (1)' with an 'Add' button. A table lists the entries:

Sequence No	Redistribution
1	Allow

At the bottom, there is an 'Allow Overrides' checkbox which is unchecked, and 'Cancel' and 'Save' buttons.

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

Dans cet exemple, toutes les routes VR-W sont des routes de fuite vers la table de routage globale. Par conséquent, aucun critère de correspondance n'est configuré pour la carte de routage.

- Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-W. Cliquez sur **BGP > IPv4 > Route Import/Export (importation/exportation de route)**.

- f) Dans la liste déroulante **Global Virtual Router Export Route Map** (carte de routage d'exportation globale du routeur virtuel), choisissez Export-to-Gobal :

Enable IPv4:

AS Number: 100

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Route Targets Import:

ASN:nn (or) ASN:nn,ASN:nn,ASN:nn Add

User Virtual Router

Import Route Map: --select--

Global Virtual Router

Import Route Map: --select--

Route Targets Export:

ASN:nn (or) ASN:nn,ASN:nn,ASN:nn Add

200:200

User Virtual Router

Export Route Map: --select--

Global Virtual Router

Export Route Map: Export-to-Global

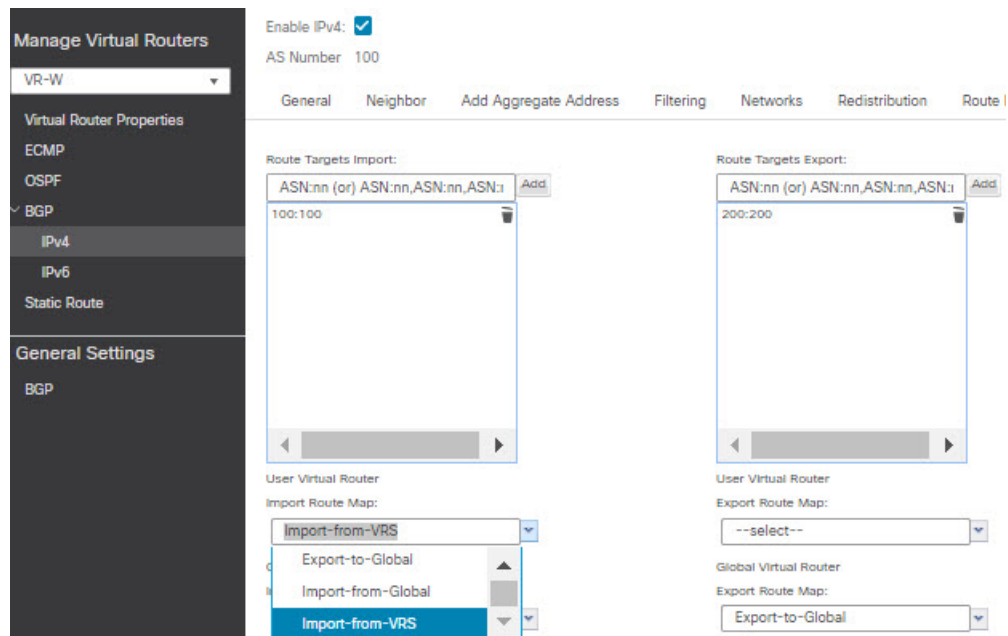
Export-to-Global

### Étape 3

Pour diffuser uniquement les routes Outside1 de VR-S vers VR-W :

- a) Dans la liste déroulante du routeur virtuel, sélectionnez VR-S.
- b) Cliquez sur **BGP > IPv4 > Importation/exportation de routage**.
- c) Pour fuiter les routes VR-S vers le VR-W, balisez les routes avec une cible de route, de sorte que les routes du VR-S soient exportées vers sa table BGP avec la cible de route marquée dessus. Dans le champ **Route Targets Export** (exportation des cibles de routage), saisissez une valeur, par exemple *100:100*. Cliquez sur **Add** (ajouter).
- d) Dans la liste déroulante du routeur virtuel, sélectionnez VR-W et **BGP > IPv4 > Route Import/Export (Importation/exportation de routage)**.
- e) Pour recevoir les fuites de routes de VR-S, configurez Import Route Target (importation cible de route) de façon à importer les routes VR-S marquées avec la cible de route du tableau BGP (homologue ou redistribué). Dans le champ **Route Targets Import** (importation des cibles de routage), saisissez la valeur de la cible de route VR-S, *100:100*. Cliquez sur **Add** (ajouter).
- f) Maintenant, vous devez conditionner que seules les routes Outside1 de VR-S soient fuitées vers VR-W. Choisissez **Object > Object Management > Prefix List > IPv4 Prefix List (liste des préfixes IPv4)**.
- g) Cliquez sur **Add IPv4 Prefix List** (Ajouter une liste de préfixes IPv4), donnez un nom, par exemple *VRS-Outside1-Only*, puis cliquez sur **Add** (Ajouter).
- h) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.
- i) Saisissez l'adresse IP (deux premiers octets) de l'interface VR-S Outside1.
- j) Cliquez sur **Save** (enregistrer).
- k) Créez une carte de routage avec la clause de correspondance avec la liste de préfixes. Cliquez sur **Route Map** (carte de routage). Cliquez sur **Add Route Map** (Ajouter une carte de routage), donnez un nom, par exemple *Import-from-VRS*, puis cliquez sur **Add** (Ajouter).

- l) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.
- m) Dans l'onglet **match Clause** (clause de correspondance), cliquez sur **IPv4**. Sous l'onglet **Address** (Adresse), cliquez sur **Prefix List** (Liste de préfixes).
- n) Sous **liste des préfixes IPv4 disponibles**, sélectionnez VRS-Outside1-Only et cliquez sur **Add** (Ajouter).
- o) Cliquez sur **Save** (enregistrer).
- p) Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-W. Cliquez sur **BGP** > **IPv4** > **Route Import/Export (importation/exportation de route)**.
- q) Dans la liste déroulante **Global Virtual Router Import Route Map** (Carte de routage d'importation du routeur virtuel global), choisissez Import-from-VRS :



**Étape 4** Configurez VR-S pour importer les routes externes du routeur virtuel global :

**Remarque** Pour utiliser des routes de fuite des routages vers ou à partir d'un routeur virtuel global, vous devez configurer respectivement le routeur virtuel source ou de destination défini par l'utilisateur. Ainsi, dans cet exemple, VR-S est le routeur de destination qui importe les routes de l'interface externe du routeur virtuel global.

- a) Choisissez **Object** > **Management** > **Prefix List** > **IPv4 Prefix List** (Objets > Gestion des objets > Liste de préfixes > Liste de préfixes IPv4).
- b) Cliquez sur **Add IPv4 Prefix List** (Ajouter une liste de préfixes IPv4), donnez un nom, par exemple *Global-Outside-Only*, puis cliquez sur **Add** (Ajouter).
- c) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.
- d) Saisissez l'adresse IP (deux premiers octets) de l'interface externe globale :

Add Prefix List Entry ?

Action:

Sequence No:  
  
Range: 1-4294967295

IP Addresses: (Limit 250) Address:  
  
Format: ipaddr/len (len<=32)

Min Prefix Length:  
  
Range: 1 - 32

Max Prefix Length:  
  
Range: 1 - 32

- e) Cliquez sur **Save** (enregistrer).
- f) Cliquez sur **Route Map** (carte de routage). Cliquez sur **Add Route Map** (ajouter une carte de routage), donnez un nom, par exemple *Import-from-Global*, puis cliquez sur **Add** (ajouter).
- g) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.
- h) Dans l'onglet **match Clause** (clause de correspondance), cliquez sur **IPv4**. Sous l'onglet **Address** (Adresse), cliquez sur **Prefix List** (Liste de préfixes).
- i) Sous **available IPv4 Prefix List** (Liste de préfixes IPv4 disponibles), sélectionnez Global-Outside-Only, puis cliquez sur **Add**(ajouter) :

Add Route Map Entry

Sequence No:

Redistribution:

Match Clauses    Set Clauses

Security Zones

- IPv4**
- IPv6
- BGP
- Others

Address (2)    Next Hop (0)    Route Source (0)

Select addresses to match as access list or prefix list addresses of route.

Access List

Prefix List

Available Access Lists :

Available IPv4 Prefix List

Selected IPv4 Prefix List

- j) Cliquez sur **Save** (enregistrer).
- k) Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-S. Cliquez sur **BGP > IPv4 > Route Import/Export** (importation/exportation de route) .
- l) Dans la liste déroulante **Global Virtual Router Export Route Map** (carte de routage d'exportation globale du routeur virtuel), choisissez Import-from-Gobal :

Manage Virtual Routers

VR-S

Virtual Router Properties

ECMP

OSPF

BGP

IPv4

IPv6

Static Route

General Settings

BGP

Enable IPv4:

AS Number 100

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route li

Route Targets Import:

ASN:nn (or) ASN:nn,ASN:nn,ASN:1 Add

200:200

Route Targets Export:

ASN:nn (or) ASN:nn,ASN:nn,ASN:1 Add

User Virtual Router

Import Route Map: --select--

Global Virtual Router

Import Route Map: Import-from-Global

Export-to-Global

Import-from-Global

User Virtual Router

Export Route Map: --select--

Global Virtual Router

Export Route Map: --select--

## Étape 5 Enregistrez et déployez.





## 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.