Routeurs virtuels

Vous pouvez créer des routeurs virtuels pour isoler le trafic sur les sous-ensembles d'interfaces les uns des autres.

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.

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.

Pour les politiques qui n'utilisent pas de zones de sécurité, comme la NAT, vous pouvez écrire des règles spécifiques à un routeur virtuel en sélectionnant les interfaces affectées à un seul routeur virtuel comme interfaces de source et de destination. Si vous sélectionnez des interfaces de source et de destination de deux routeurs virtuels distincts, vous devez vous assurer que les routes sont appropriées entre les routeurs virtuels pour que la règle s'applique.

Routage entre routeurs virtuels

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.

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 2110	10
Firepower 2120	20
Firepower 2130	30

Modèle du périphérique	Routeurs virtuels maximums
Firepower 2140	40
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4110	60
Firepower 4112	60
Firepower 4115	80
Firepower 4120	80
Firepower 4125	100
Firepower 4140	100
Firepower 4145	100
Firepower 4150	100
appareil Cisco Firepower de série 9300, tous les modèles	100
Firewall Threat Defense Virtual, toutes les plateformes	30
ISA 3000	10

Lignes directrices pour les routeurs virtuels

Directives relatives aux modèles de périphériques

Vous pouvez configurer des routeurs virtuels sur tous les modèles de périphériques pris en charge, à l'exception des suivants :

- Firepower 1010

Directives supplémentaires

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

  - BGPv6
  - Routage multidiffusion
  - Routage basé sur une stratégie
  - VPN

- Vous pouvez configurer les fonctionnalités suivantes séparément pour chaque routeur virtuel :
  - Routes statiques et leurs moniteurs SLA.
  - OSPFv2
  - BGPv4

- Les fonctionnalités suivantes sont utilisées par le système lors des requêtes ou des communications avec le système distant (trafic initial). Ces fonctionnalités utilisent uniquement les interfaces du routeur virtuel global. Si vous configurez une interface pour cette fonctionnalité, elle doit appartenir au routeur virtuel global. En règle générale, lorsque le système doit rechercher une route pour atteindre un serveur externe à des fins de gestion, il effectue la recherche 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 résoudre des 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 pouvez configurer le VPN uniquement sur des interfaces dans le routeur virtuel global, donc les serveurs AAA externes utilisés pour le VPN, comme Active Directory, doivent être accessibles par l'intermédiaire d'une interface dans le routeur virtuel global.
  - Serveur Syslog.
  - SNMP.

- Dans la NAT, si vous spécifiez des interfaces source et destination associées à des routeurs virtuels différents, la règle NAT détourne le trafic d'un routeur virtuel vers un autre. Assurez-vous de ne pas combiner les interfaces dans les règles de NAT par erreur. Normalement, les interfaces source et destination sont utilisées et la table de routage est ignorée, y compris pour les traductions de destination dans la NAT Toutefois, si la règle NAT doit effectuer une recherche de routage, celle-ci se fait uniquement dans la table VRF de l'interface entrante. Au besoin, définissez les routes statiques dans le routeur virtuel source pour l'interface de destination. Si vous laissez l'interface à **any**, la règle s'applique à toutes les interfaces, quel que soit leur appartenance au routeur virtuel. Lorsque vous utilisez des routeurs virtuels, testez soigneusement vos règles de NAT pour vous assurer d'obtenir le comportement attendu. Si vous omettez de définir une fuite de route nécessaire, il peut arriver que la règle ne corresponde pas à tout le trafic attendu et que la traduction ne soit pas appliquée.
- Si vous configurez des routes entre routeurs virtuels, par exemple en divulguant une route d'un routeur virtuel vers un second, le système effectue la recherche de 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.
- Lorsque vous utilisez des routes entre routeurs virtuels (routes divulguées), par exemple du routeur virtuel 1 vers le routeur virtuel 2, vous n'avez pas à configurer une route miroir (inversée) dans le routeur

virtuel 2 pour permettre le trafic de retour. Toutefois, si vous souhaitez autoriser des connexions dans les deux sens, veillez à divulguer la route dans les deux directions, du routeur virtuel 1 au routeur virtuel 2 et du routeur virtuel 2 au routeur virtuel 1.

- Si vous déplacez une interface d'un routeur virtuel à un autre, toutes les fonctionnalités configurées pour l'interface sont conservées. Examinez la configuration pour vous assurer que les routes statiques, les adresses IP et les autres politiques ont du sens dans le contexte du nouveau routeur virtuel.
- Si vous utilisez des espaces d'adresses qui se chevauchent dans plusieurs routeurs virtuels, sachez que les mappages statiques de balises de groupe de sécurité (SGT) vers des adresses IP téléchargés à partir du Cisco Identity Services Engine (ISE) ne reconnaissent pas les routeurs virtuels. Configurez des domaines d'identité distincts pour chaque 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.
- Si vous utilisez des espaces d'adresses qui se chevauchent dans plusieurs routeurs virtuels, les données du tableau de bord peuvent induire en erreur. Les connexions pour la même adresse IP sont agrégées, de sorte qu'il apparaîtra qu'il y a eu plus de trafic vers ou depuis une adresse donnée lorsqu'elle est partagée par deux points terminaux ou plus. Si vous créez soigneusement vos politiques d'identité à l'aide de domaines d'identité distincts, les statistiques basées sur l'utilisateur devraient être plus exactes.
- Vous ne pouvez pas utiliser des ensembles d'adresses DHCP qui se chevauchent dans des routeurs virtuels distincts.
- Vous pouvez utiliser la configuration automatique du serveur DHCP uniquement sur une interface du routeur virtuel global. La configuration automatique n'est pas prise en charge pour les interfaces affectées à un routeur virtuel défini par l'utilisateur.
- Si vous déplacez une interface d'un routeur virtuel à un autre, y compris du routeur virtuel global vers un nouveau routeur, toutes les connexions existantes par l'intermédiaire de l'interface sont abandonnées.
- 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.

Gestion des routeurs virtuels

Vous pouvez créer plusieurs instances de routage et de transfert virtuels (VRF), appelées routeurs virtuels, pour maintenir 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.

Par défaut, le routage virtuel est désactivé. L'appareil entier utilise un seul ensemble de tables de routage globales, pour le trafic de données (par le biais) et de gestion (vers/à partir du boîtier).

Lorsque vous activez le routage virtuel, la page de routage initiale est une liste des routeurs virtuels définis sur le système. Si vous n'activez pas les routeurs virtuels, la page de routage initiale est une liste des routes statiques définies sur le système.

Il y a toujours un routeur virtuel global. Le routeur global contient toutes les interfaces que vous n'avez pas affectées aux routeurs virtuels individuels.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé du routage (**Routing**).

Étape 2 Si vous n'avez pas encore activé les routeurs virtuels, cliquez sur le lien **Add Multiple Virtual Routers** (Ajouter plusieurs routeurs virtuels), puis sur **Create First Custom Virtual Router** (Créer le premier routeur virtuel personnalisé).

La création du premier routeur virtuel est essentiellement la même que la création de routeurs virtuels supplémentaires. Pour en savoir plus, consultez Créer un routeur virtuel ou modifier les affectations d'interface, à la page 8.

Étape 3 Effectuez l'une des actions suivantes :

- Pour configurer les paramètres globaux de BGP, qui s'appliquent à tous les routeurs virtuels, cliquez sur le bouton **BGP Global Settings** (Paramètres globaux BGP). Vous configurez ces paramètres à l'aide de l'interface de ligne de commande Smart, qui est expliquée dans Configuration des objets Smart CLI. Configurez les paramètres globaux de BGP uniquement si vous configurez BGP dans un ou plusieurs routeurs virtuels.
- Pour créer un nouveau routeur virtuel, cliquez sur le bouton + au-dessus du tableau.
- Pour modifier les propriétés de routage d'un routeur virtuel, par exemple, pour créer des routes statiques ou définir des processus de routage, cliquez sur l'icône d'affichage ( ) dans la case Action du routeur virtuel.
- Pour modifier le nom, la description ou les affectations d'interface pour un routeur virtuel, cliquez sur l'icône d'affichage ( ) dans la case Action pour le routeur virtuel, puis sélectionnez l'onglet **Virtual Router Properties** (Propriétés du routeur virtuel).
- Pour basculer entre les routeurs virtuels lorsque vous les affichez, cliquez sur la flèche vers le bas à côté du nom du routeur virtuel (au-dessus de la table de routage) et sélectionnez le routeur virtuel souhaité. Vous pouvez revenir à la page de liste en cliquant sur la flèche **Go Back to Virtual Routers** (Revenir aux routeurs virtuels) ( ).
- Pour supprimer un routeur virtuel, cliquez sur l'icône de suppression ( ) dans la case Action du routeur virtuel ou sur l'icône de suppression à côté du nom du routeur virtuel lorsque vous affichez le contenu du routeur virtuel. Lorsque vous supprimez le dernier routeur virtuel (autre que le routeur global, que vous ne pouvez pas supprimer), le VRF est désactivé.
- Pour surveiller le routage dans un routeur virtuel, cliquez sur le lien de l'une des commandes **show** dans le tableau de ce routeur virtuel. Cliquez sur la commande pour ouvrir la console CLI, où vous pouvez examiner le résultat de la commande CLI. Vous pouvez afficher les informations sur les routes, OSPF et les voisins OSPF. Notez que le résultat de la commande est basé sur la configuration déployée ; vous ne verrez rien concernant les modifications non déployées.

  Vous pouvez également exécuter ces commandes en les sélectionnant dans la liste déroulante **Commands** (Commandes) lorsque vous affichez le routeur virtuel.

Créer un routeur virtuel ou modifier les affectations d'interface

Avant de pouvoir configurer des routes statiques ou un processus de routage sur un routeur virtuel, vous devez créer le routeur et lui affecter des interfaces.

Avant de commencer

Accédez à la page **Interfaces** et assurez-vous que chaque interface que vous souhaitez ajouter au routeur virtuel a un nom. Vous ne pouvez pas ajouter d'interface à un routeur virtuel tant qu'il n'a pas de nom.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)** > **Routing (Routage)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Si vous n'avez pas encore créé de routeur virtuel, cliquez sur le lien **Add Multiple Virtual Router**s (Ajouter plusieurs routeurs virtuels), puis sur **Create First Custom Virtual Router** (Créer le premier routeur virtuel personnalisé).
- Cliquez sur le bouton **+** au-dessus de la liste des routeurs virtuels pour en créer un nouveau.
- Cliquez sur l'icône de modification ( ) d'un routeur virtuel afin de modifier ses propriétés et la liste d'interfaces.
- Lorsque vous affichez un routeur virtuel, cliquez sur l'onglet **Virtual Router Properties** (Propriétés du routeur virtuel) pour modifier les propriétés du routeur virtuel affiché.
- Lorsque vous affichez un routeur virtuel, cliquez sur la flèche vers le bas à côté du nom du routeur virtuel, puis cliquez sur**Create New Virtual Router** (Créer un nouveau routeur virtuel).

Étape 3 Configurez les propriétés du routeur virtuel :

- **Name** (Nom) : nom du routeur virtuel.
- **Description** : une description facultative du routeur virtuel.
- **Interfaces** : cliquez sur le signe plus **(+)** pour sélectionner chaque interface qui doit faire partie du routeur virtuel. Pour supprimer une interface, passez le curseur sur l'interface et cliquez sur **X** sur le côté droit de la carte d'interface. Vous pouvez affecter des interfaces physiques, des sous-interfaces, des groupes de ponts et des EtherChannels à un routeur virtuel, mais pas des VLAN.

  La table de routage sera limitée à ces interfaces, sauf si vous communiquez intentionnellement les routes vers d'autres interfaces dans la table de routage virtuelle.

  Vous pouvez attribuer l'interface de diagnostic (Management X/Y) uniquement au routeur virtuel global.

Étape 4 Cliquez sur **OK** ou sur **Save** (Enregistrer).

Vous êtes redirigé vers l'affichage de ce routeur virtuel, où vous pouvez configurer des routes statiques ou des processus de routage.

Configurer Static Routes (routes statiques) et Routing Processes (processus de routage) dans un routeur virtuel

Chaque routeur virtuel possède ses propres routes statiques et processus de routage, qui fonctionnent séparément de ceux définis pour tout autre routeur virtuel.

Lorsque vous configurez des routes statiques, vous pouvez sélectionner des interfaces de destination qui se trouvent à l'extérieur du routeur virtuel. Cela entraîne une fuite de la route dans le routeur virtuel qui contient l'interface de destination. Assurez-vous de ne faire fuiter que les routes nécessaires, afin de ne pas envoyer plus de trafic que vous ne le souhaitez vers l'autre routeur virtuel. Par exemple, si vous disposez d'un seul chemin d'accès à Internet, il est logique de faire fuiter les routes de chaque routeur virtuel vers le routeur virtuel orienté vers Internet pour le trafic destiné à Internet.

Procédure

Étape 1 Choisissez **Device (Appareil)** > **Routing (Routage)**.

Étape 2 Cliquez sur l'icône d'affichage ( ) dans la case Action pour que le routeur virtuel l'ouvre.

Étape 3 Effectuez l'une des actions suivantes :

- Pour configurer des routes statiques, cliquez sur l'onglet **Static Routing** (routage statique), puis créez ou modifiez les routes. Pour de plus amples renseignements, voir Configuration des routes statiques.
- Pour configurer des zones de trafic à coût unique (Equal-Cost Multi-Path, ECMP), cliquez sur l'onglet **ECMP Traffic Zones** (zones de trafic ECMP), puis créez les zones. Pour de plus amples renseignements, voir Configuration des zones de trafic ECMP.
- Pour configurer le processus de routage BGP, cliquez sur l'onglet **BGP**, puis créez l'objet Smart CLI nécessaire pour définir le processus. Pour de plus amples renseignements, voir Protocole de routage BGP.

  Il existe également des paramètres globaux pour BGP qui s'appliquent à tous les routeurs virtuels. Vous devez revenir à la page de liste des routeurs virtuels pour cliquer sur le bouton **BGP Global Settings** (paramètres globaux BGP) pour configurer ces propriétés.
- Pour configurer le processus de routage OSPF, cliquez sur l'onglet **OSPF**, puis créez les objets Smart CLI nécessaires pour définir jusqu'à 2 processus et les configurations d'interface associées. Pour de plus amples renseignements, voir Open Shortest Path First (OSPF).
- (Routeur virtuel global uniquement.) Pour configurer le processus de routage EIGRP, cliquez sur l'onglet **EIGRP**, puis créez l'objet Smart CLI nécessaire pour définir un seul processus. Pour de plus amples renseignements, voir Protocole de routage de passerelle intérieure amélioré (EIGRP).

Supprimer un routeur virtuel

Si vous n'avez plus besoin d'un routeur virtuel, vous pouvez le supprimer. Vous ne pouvez pas supprimer le routeur virtuel global.

Lorsque vous supprimez un routeur virtuel, vous supprimez également toutes les routes statiques et les processus de routage configurés dans le routeur virtuel.

Toutes les interfaces affectées au routeur virtuel sont réaffectées au routeur global.

Procédure

Étape 1 Choisissez **Device (Périphérique)** > **Routing (Routage)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Dans la liste des routeurs virtuels, cliquez sur l'icône de suppression ( ) dans la colonne Action pour le routeur virtuel.
- Lorsque vous affichez le routeur virtuel que vous souhaitez supprimer, cliquez sur l'icône de suppression ( ) à côté du nom du routeur.

Vous êtes invité à confirmer que vous souhaitez supprimer le routeur virtuel.

Étape 3 Cliquez sur **OK** pour confirmer la suppression.

Exemples pour les routeurs virtuels

Les rubriques suivantes fournissent des exemples d'implémentation de routeurs virtuels.

Sujets connexes

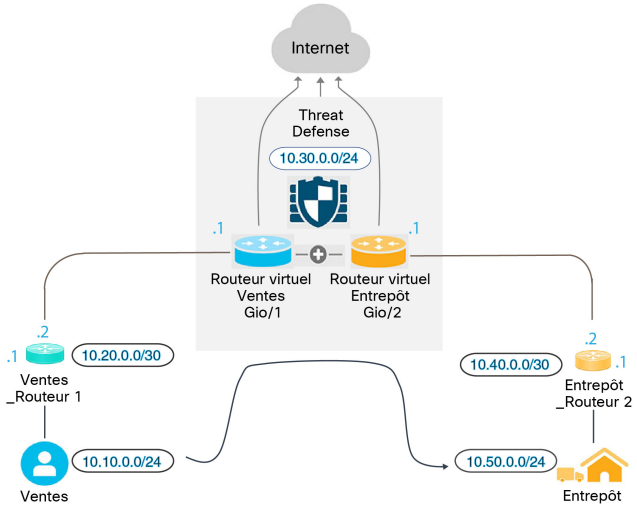
Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels.

Comment effectuer un routage vers un serveur distant à l'aide de routeurs virtuels

Lorsque vous utilisez des routeurs virtuels, vous pouvez avoir une situation où les utilisateurs d'un routeur virtuel ont besoin d'accéder à un serveur qui n'est accessible que par l'intermédiaire d'un routeur virtuel distinct.

Reportez-vous à l'illustration suivante. Les ordinateurs de travail de l'équipe des ventes sont connectés au routeur virtuel des ventes. Les serveurs d'entrepôt sont connectés par l'intermédiaire du routeur virtuel de l'entrepôt. Si l'équipe de vente doit rechercher des informations sur le serveur de l'entrepôt dont l'adresse IP est 10.50.0.5/24, vous devez divulguer une route du routeur virtuel des ventes vers le routeur virtuel de l'entrepôt. Le routeur virtuel de l'entrepôt doit également avoir une voie de routage vers le serveur de l'entrepôt, qui se trouve de plusieurs sauts derrière le routeur de l'entrepôt 2.



Avant de commencer

Cet exemple suppose que vous avez déjà configuré :

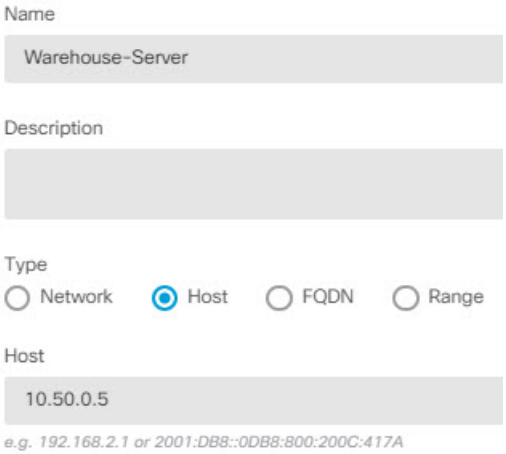
- Les routeurs virtuels Ventes et Entrepôt sur le périphérique Firewall Threat Defense, avec GigabitEthernet 0/1 attribué aux Ventes et GigabitEthernet 0/2 attribué à l'Entrepôt.
- Le routeur de ventes 1 a une route statique ou dynamique qui enverra le trafic vers 10.50.0.5/24 à partir de l'interface 10.20.0.1/30.

Procédure

Étape 1 Créez l'objet réseau pour 10.50.0.5/24 ou 10.50.0.0/24. Créez également l'objet pour la passerelle, 10.40.0.2/30.

Si vous souhaitez limiter le routage à l'adresse IP unique du serveur d'entrepôt, utilisez un objet hôte pour définir 10.50.0.5. Sinon, si l'équipe de vente doit avoir accès à d'autres systèmes dans l'entrepôt, créez un objet réseau pour le réseau 10.50.0.0/24. Dans cet exemple, nous créerons une route vers l'adresse IP de l'hôte.

a) Choisissez **Objects** (Objets), puis **Networks** (Réseaux) dans la table des matières.
b) Cliquez sur +, puis complétez les propriétés d'objet pour le serveur d'entrepôt :



c) Cliquez sur **OK**.

d) Cliquez sur **+**, puis complétez les propriétés d'objet pour la passerelle du routeur vers le réseau de l'entrepôt :

e) Cliquez sur **OK**.

Étape 2 Définissez la fuite de route dans Ventes qui pointe vers l'interface Gi0/2 dans le routeur virtuel de l'entrepôt.

Dans cet exemple, Gi0/1 est nommé inside, et Gi0/2 est nommé inside-2.

a) Sélectionnez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé **Routing** (Routage).

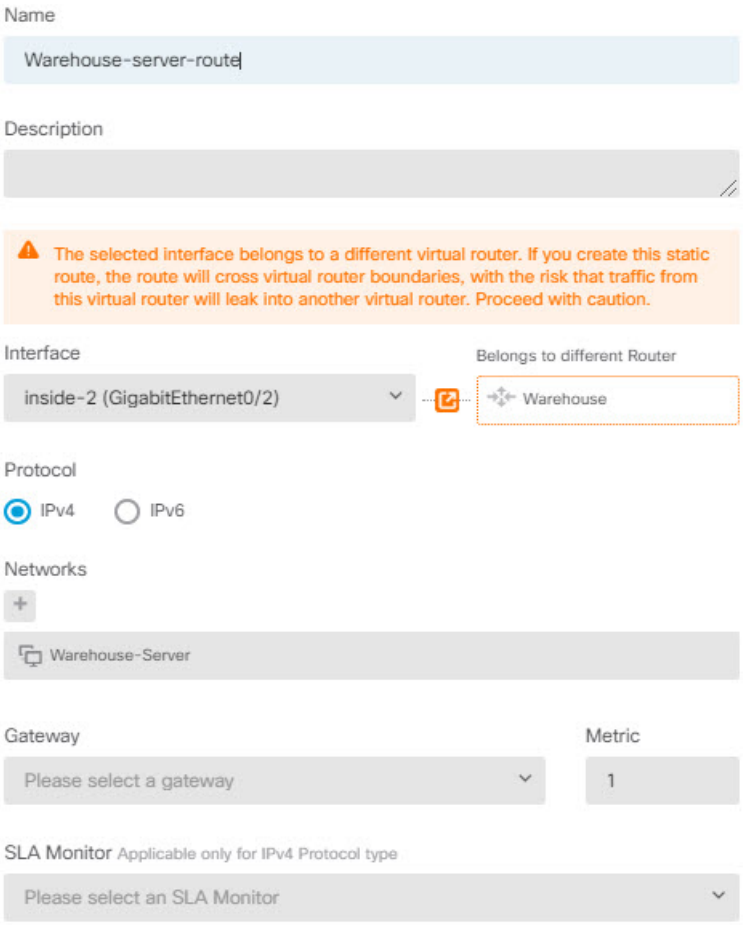
b) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'action du routeur virtuel de ventes.

c) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (Nom) : tout nom convient, par exemple Entrepôt-serveur-route.
- **Interface** : sélectionnez **inside-2**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**. Vous pouvez également utiliser des adresses IPv6 pour mettre en œuvre cet exemple.

- **Networks** (Réseaux) : 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.

La boîte de dialogue doit ressembler à ce qui suit :

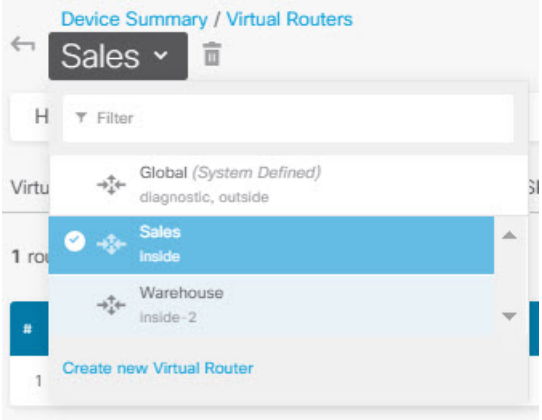


d) Cliquez sur **OK**.

Étape 3 Dans le routeur virtuel de l'entrepôt, définissez la route qui pointe vers la passerelle du routeur de l'entrepôt 2.

Sinon, cela peut être fait en configurant un protocole de routage qui découvrirait dynamiquement la route à partir du routeur de l'entrepôt 2. Pour cet exemple, nous définirons la route statique.

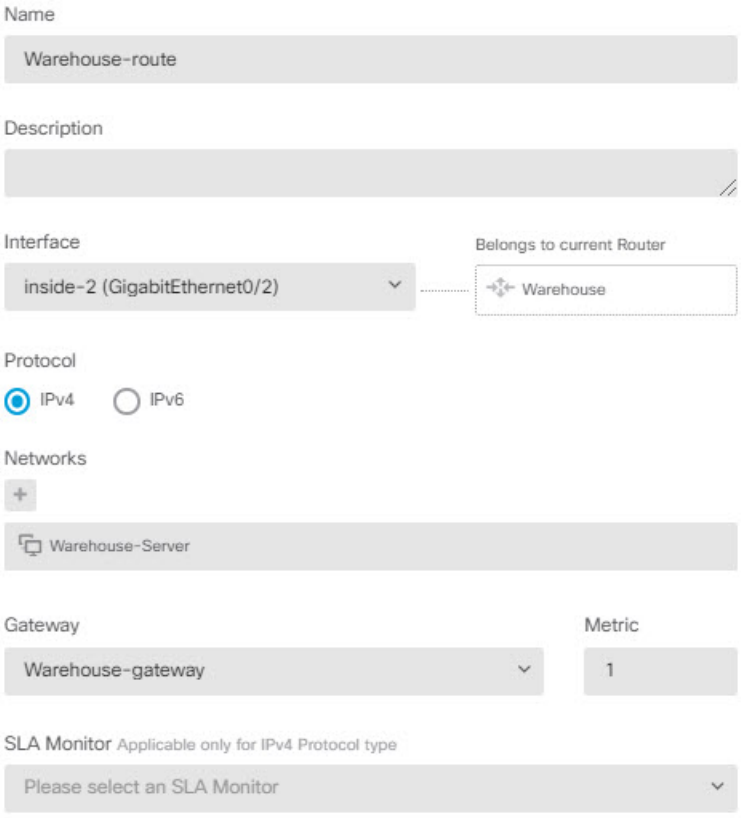
a) Dans la liste déroulante du routeur virtuel qui indique actuellement Ventes, sélectionnez le routeur virtuel de l'entrepôt pour changer de routeur.



b) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (Nom) : tout nom convient, par exemple Route de l'entrepôt.
- **Interface** : sélectionnez **inside-2**.
- **Protocole** : sélectionnez **IPv4**.
- **Networks** (Réseaux) : sélectionnez l'objet Warehouse-Server.
- **Gateway** (Passerelle) : Sélectionnez l'objet Warehouse-Gateway.

La boîte de dialogue doit ressembler à ce qui suit :

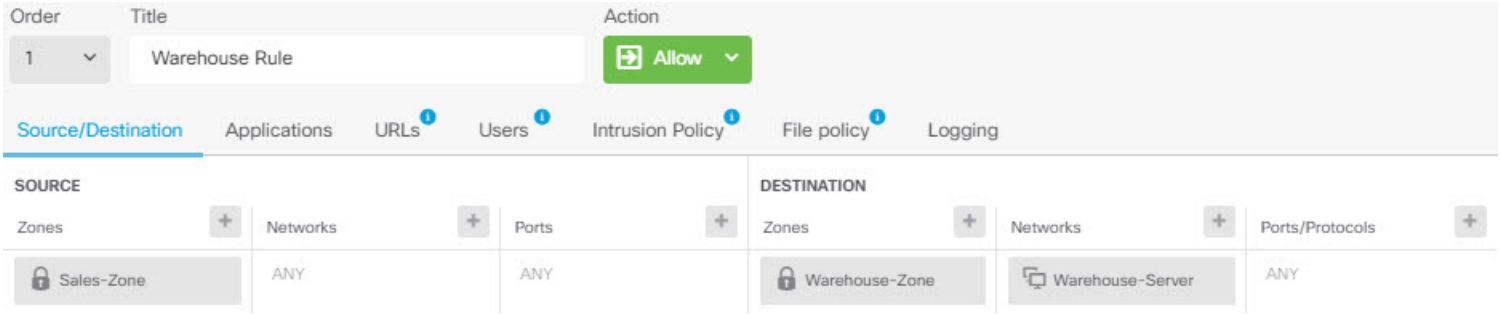


c) Cliquez sur **OK**.

Étape 4 Assurez-vous qu'il existe une règle de contrôle d'accès qui permet l'accès au serveur d'entrepôt.

La règle la plus simple permettrait 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. Vous pouvez appliquer l'inspection de prévention des intrusions au trafic comme vous le souhaitez.

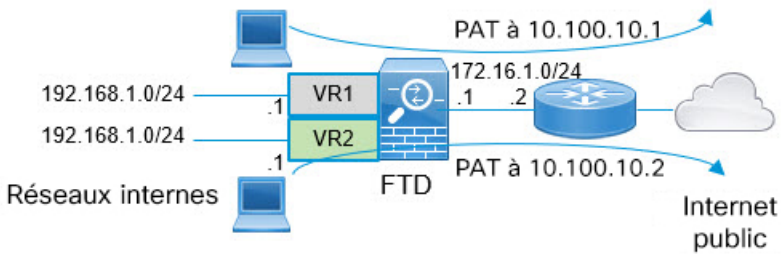
Par exemple, si les interfaces dans Sales se trouvent dans la zone de sécurité Sales-Zone et que celles de l'entrepôt sont dans la zone de sécurité Warehouse-Zone, la règle de contrôle d'accès ressemblera à ce qui suit :



Fournir un accès Internet à plusieurs routeurs virtuels 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. 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. Cependant, comme les adresses IP acheminées dans ces routeurs virtuels distincts sont identiques, vous devez gérer avec soin le trafic qui quitte les routeurs virtuels pour vous assurer que le trafic de retour se dirige vers la bonne destination.

Pour autoriser l'accès Internet à partir de deux routeurs virtuels qui utilisent le même espace d'adresses, vous devez appliquer les règles NAT séparément aux interfaces de chaque routeur virtuel, idéalement en utilisant des pools NAT ou PAT distincts. Vous pouvez utiliser PAT pour traduire les adresses sources de virtual router 1 en 10.100.10.1 et, pour celles de virtual router 2, 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 explicitement sélectionnée, car l'utilisation de « any » comme interface source empêche le système d'identifier correctement la source, étant donné que la même adresse IP peut exister sur deux interfaces différentes.



Remarque Cet exemple est simplifié : chaque routeur virtuel contient une seule interface. Si un routeur virtuel « interne » possède plusieurs interfaces, vous devez créer les règles NAT pour chaque interface « interne ». Même si certaines interfaces dans les routeurs virtuels n'utilisent pas des espaces d'adresses en chevauchement, sélectionner explicitement l'interface source dans les règles NAT peut faciliter le dépannage et assurer une séparation plus nette du trafic Internet sortant des routeurs virtuels.

Procédure

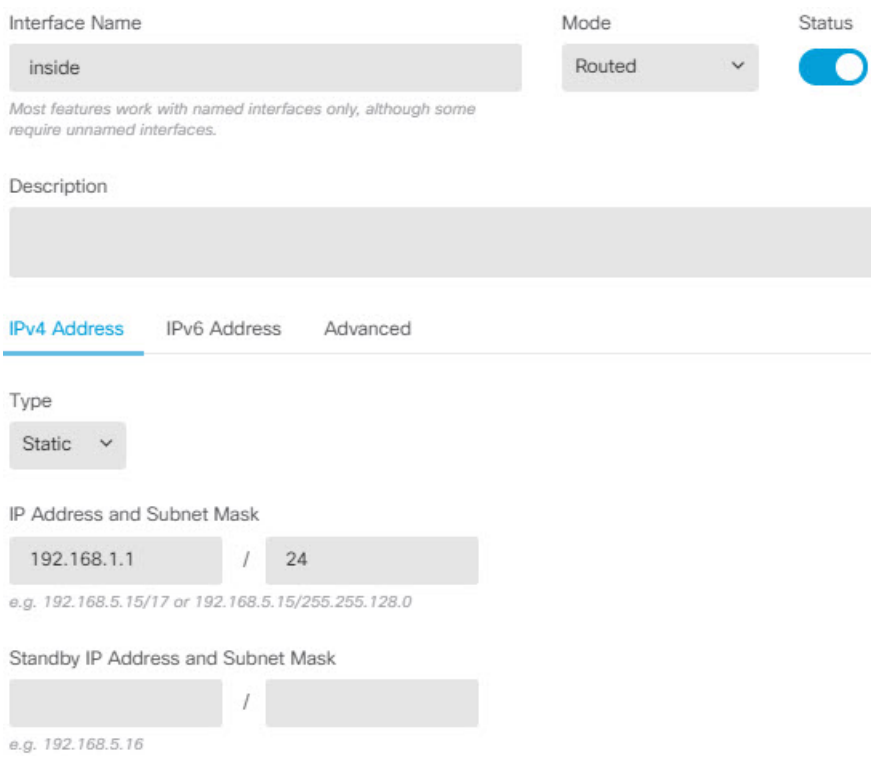
Étape 1 Configurez l'interface interne pour le routeur virtuel 1 (VR1).

a) Cliquez sur **Device** (appareil), puis sur **View All Interfaces** (afficher toutes les interfaces) dans le résumé **Interface**.

b) Cliquez sur l'icône de modification ( ) dans la colonne Action de l'interface que vous affecterez à VR1.

c) Configurez au moins les propriétés suivantes :

- **Name**(nom) : pour cet exemple, **inside**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : activez l'interface.
- **Type** > **d'adresse IPv4** : sélectionnez **Static** (statique).
- **Adresse IPv4 et masque de sous-réseau** : saisissez 192.168.1.1/24.



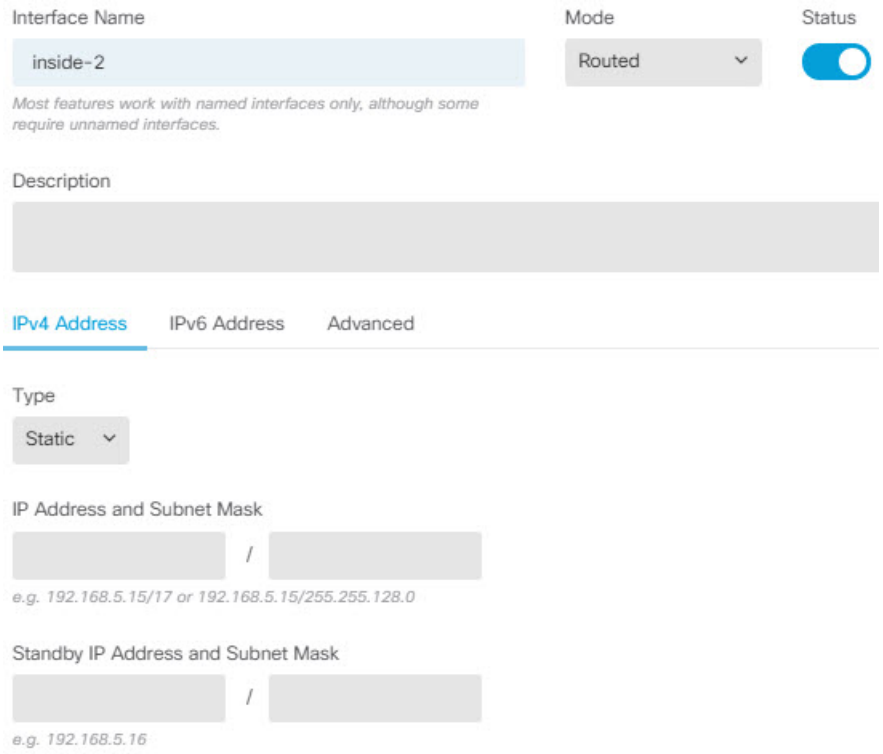
d) Cliquez sur **OK**.

Étape 2 Configurez l'interface interne-2 pour le routeur virtuel 2 (VR2), mais ne spécifiez pas l'adresse IP.

a) Sur la page de liste des interfaces, cliquez sur l'icône de modification ( ) dans la colonne Action de l'interface que vous affecterez à VR2.

b) Configurez au moins les propriétés suivantes :

- **Name** (nom) : pour cet exemple, **inside_2**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : activez l'interface.
- **Type** > **d'adresse IPv4** : sélectionnez **Static** (statique).
- **Adresse IPv4 et masque de sous-réseau** : laissez ces champs vides. Si vous essayez de configurer la même adresse que l'interface interne à ce stade, le système affiche un message d'erreur et vous empêche de créer une configuration non fonctionnelle. Vous ne pouvez pas acheminer le trafic vers le même espace d'adresse en utilisant différentes interfaces sur le même routeur.



c) Cliquez sur **OK**.

Étape 3 Configurez le routeur virtuel VR1, y compris la fuite de route statique par défaut vers l'interface externe.

a) Choisissez **Device** (appareil), cliquez sur **View Configuration** (afficher la configuration) dans le résumé de **Routing** (routage).

b) Cliquez sur **Add Multiple Virtual Routers** (ajouter plusieurs routeurs virtuels) en haut de la page de routage.

c) Dans le coin inférieur droit du panneau explicatif, cliquez sur **Create First Custom Virtual Router** (créer le premier routeur virtuel personnalisé).

d) Remplissez les propriétés du routeur virtuel VR1.

- **Name** (nom) : saisissez VR1 ou un autre nom de votre choix.
- **Interfaces** : cliquez sur **+**, sélectionnez **inside**, puis cliquez sur **OK**.

e) Cliquez sur **OK**.

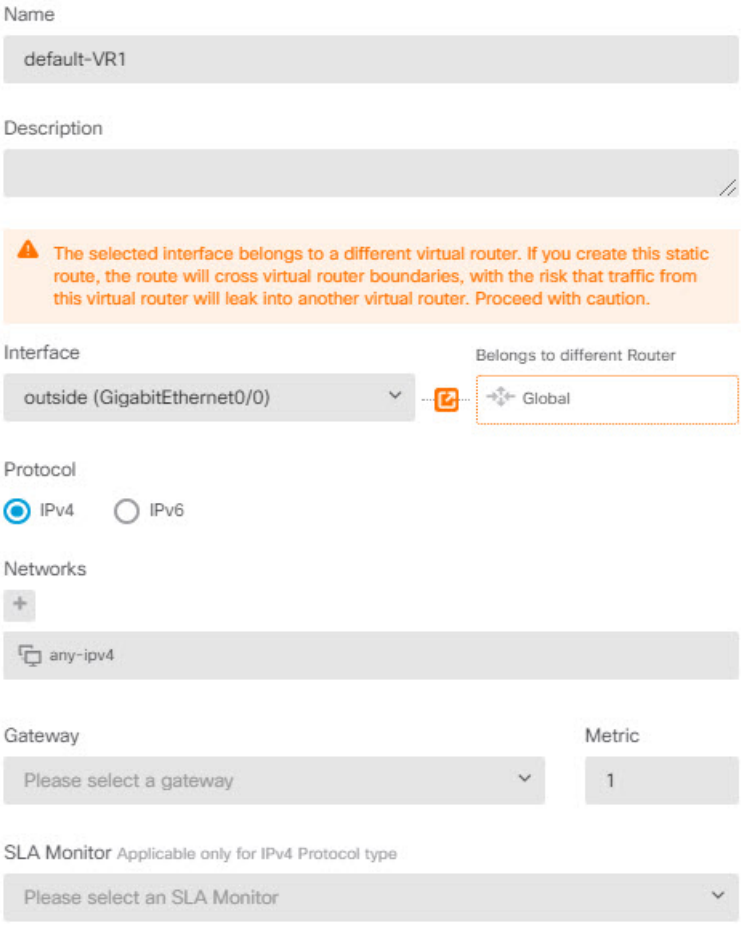
La boîte de dialogue se ferme et la liste des routeurs virtuels s'affiche.

f) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'actions pour le routeur virtuel VR1.

g) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que **default-VR1**.
- **Interface** : sélectionnez **outside**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Ce sera 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 vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



h) Cliquez sur **OK**.

Étape 4 Configurez le routeur virtuel VR2, y compris la fuite de route statique par défaut vers l'interface externe.

a) Lorsque vous affichez VR1, cliquez sur le bouton de retour (⇦) pour revenir à la liste des routeurs virtuels.
b) Cliquez sur + en haut de la liste.
c) Remplissez les propriétés du routeur virtuel VR2.

- **Name** (nom) : saisissez VR2 ou un autre nom de votre choix.
- **Interfaces** : cliquez sur +, sélectionnez **inside-2**, puis cliquez sur **OK**.

d) Cliquez sur **OK**.

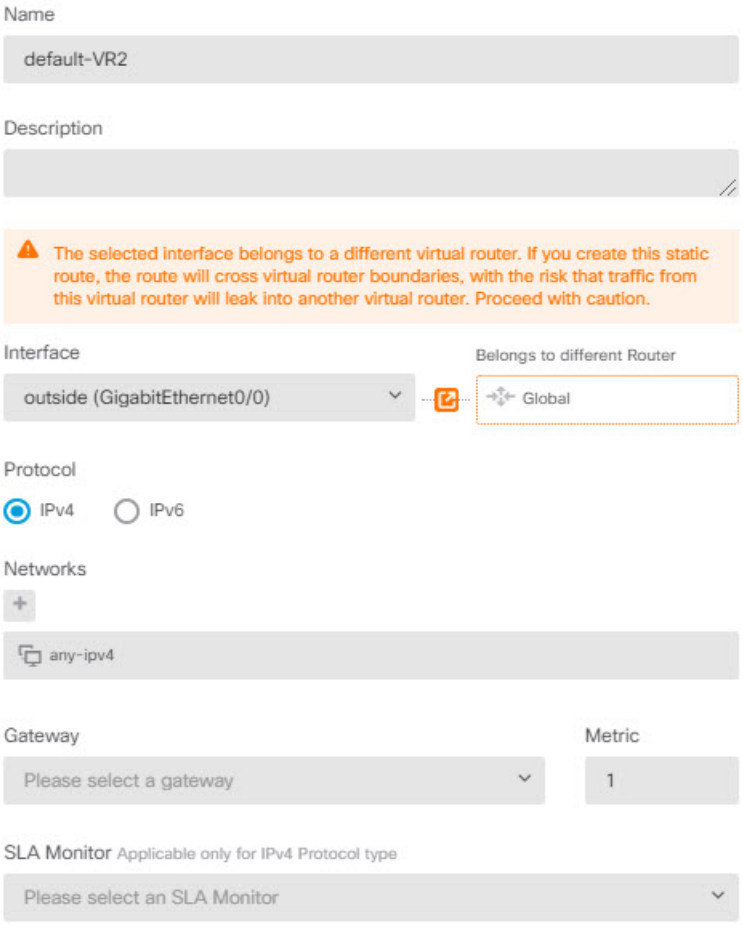
La boîte de dialogue se ferme et la liste des routeurs virtuels s'affiche.

e) Dans la liste des routeurs virtuels, cliquez sur l'icône d'affichage ( ) dans la colonne d'actions pour le routeur virtuel VR2.

f) Dans l'onglet **Static Routing** (routage statique), cliquez sur le signe **plus (+)** et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que **default-VR2**.
- **Interface** : sélectionnez **outside**. Vous verrez un avertissement indiquant que l'interface se trouve dans un autre routeur et que vous créez une fuite de route. C'est l'action souhaitée.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Ce sera 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 route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



g) Cliquez sur **OK**.

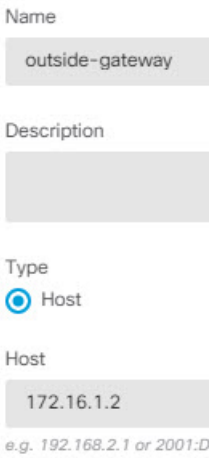
Étape 5 Ajoutez la voie de routage par défaut dans le routeur global vers l'interface externe.

Le but de ce routage est d'affecter la passerelle correcte au trafic fuité des deux routeurs virtuels vers l'interface outside (externe) du routeur virtuel global.

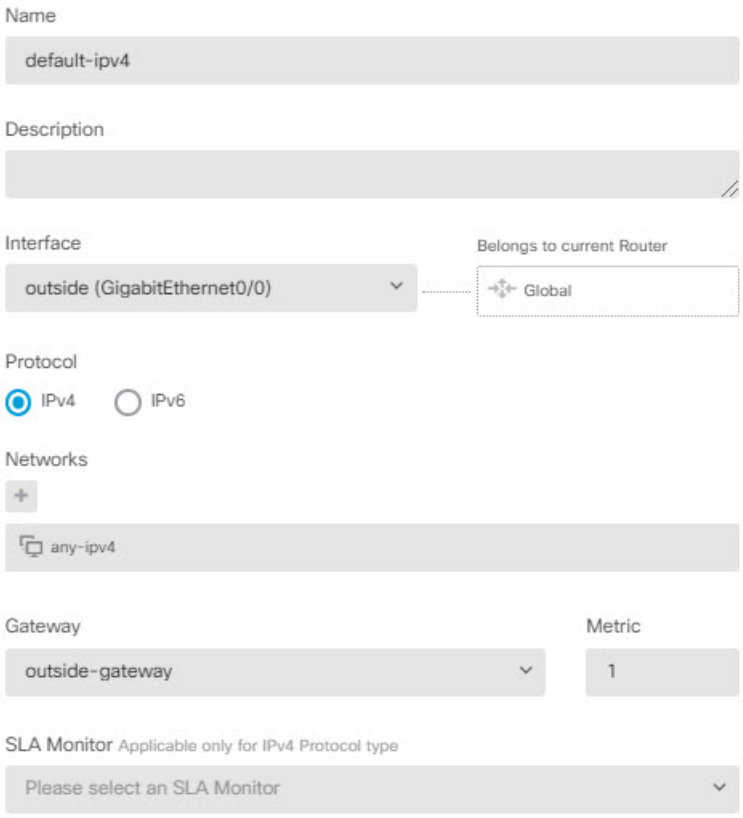
a) Lorsque vous affichez VR2, cliquez sur le nom de VR2 en haut de la page pour ouvrir la liste des routeurs virtuels, puis sélectionnez le routeur Global.

b) Dans l'onglet Static Routing (routage statique) du routeur Global, cliquez sur + et configurez le routage :

- **Name** (nom) : n'importe quel nom suffit, tel que par défaut-ipv4.
- **Interface** : sélectionnez **outside**.
- **Protocole** : pour cet exemple, utilisez **IPv4**.
- **Réseaux** : sélectionnez l'objet **any-ipv4**. Il s'agira de la voie de routage par défaut pour tout trafic IPv4.
- **Gateway** (passerelle) : si l'objet n'existe pas encore, cliquez sur **Create New Network Object** (Créer un nouvel objet réseau, puis définissez un objet hôte pour l'adresse IP de la passerelle à l'autre extrémité du lien réseau sur l'interface outside (externe), dans cet exemple 172.16.1.2. Après avoir créé l'objet, sélectionnez-le dans le champ Gateway (passerelle) du routage statique.



La boîte de dialogue doit ressembler à ce qui suit :



c) Cliquez sur **OK**.

Étape 6 Revenez à la page **Interfaces** et ajoutez l'adresse IP à inside-2.

a) Cliquez sur **Device** (appareil), puis sur **View All Interfaces** (afficher toutes les interfaces) dans le résumé **Interface**.

b) Cliquez sur l'icône de modification ( ) dans la colonne Action pour l'interface inside-2 que vous avez affectée à VR2.

c) Dans l'onglet **IPv4 Address** (adresse IPv4), saisissez 192.168.1.1/24 comme adresse IP et masque de sous-réseau.

d) Cliquez sur **OK**.

Vous n'obtenez pas d'erreur d'adresse IP en double cette fois, car les interfaces inside et inside-2 se trouvent désormais dans des routeurs virtuels distincts.

Étape 7 Créez la règle NAT pour appliquer la PAT de inside (interne) vers outside (externe) vers 10.100.10.1.

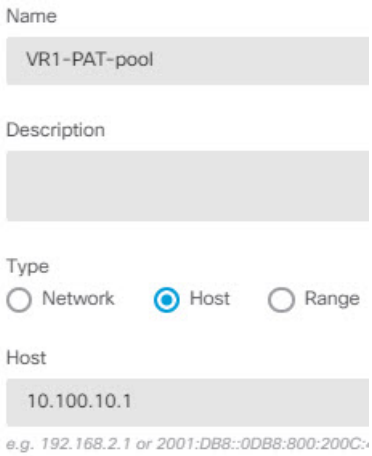
a) Choisissez **Policies** (politiques), puis cliquez sur **NAT**.

b) S'il existe déjà une règle NAT manuelle nommée InsideOutsideNatRule pour l'interface inside (interne) → outside (externe) appliquant la PAT d'interface, cliquez sur l'icône de modification ( ) pour la règle. Sinon, cliquez sur le signe **plus (+)** pour créer une nouvelle règle.

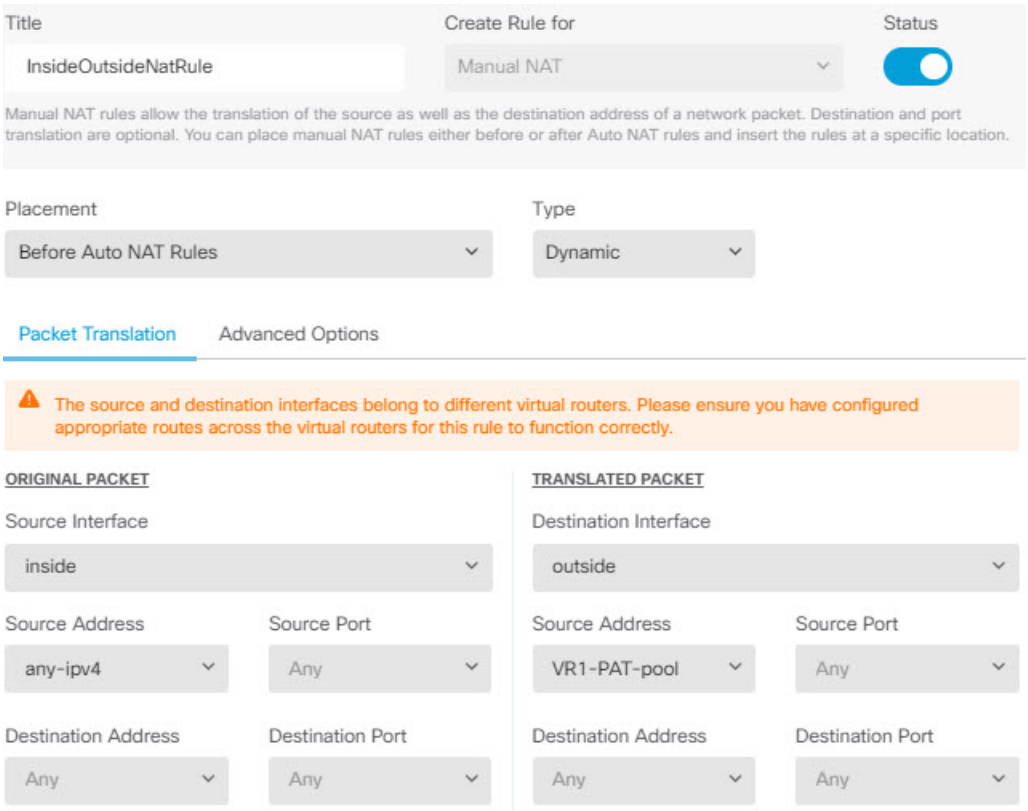
Si vous modifiez une règle existante, notez qu'un avertissement indique que les interfaces source et destination se trouvent dans des routeurs virtuels différents et que vous devez définir des routes. C'est ce que vous avez effectué plus tôt dans la procédure.

c) Si vous modifiez une règle existante, cliquez sur la flèche déroulante de **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)**, puis cliquez sur **Create New Network** (Créer un nouveau réseau) (en supposant que vous n'avez pas encore d'objet hôte définissant 10.100.10.1).

d) Configurez l'objet réseau hôte pour l'adresse PAT. L'objet doit ressembler à ce qui suit :



e) Sélectionnez le nouvel objet comme **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)**. La règle NAT doit ressembler à ce qui suit :



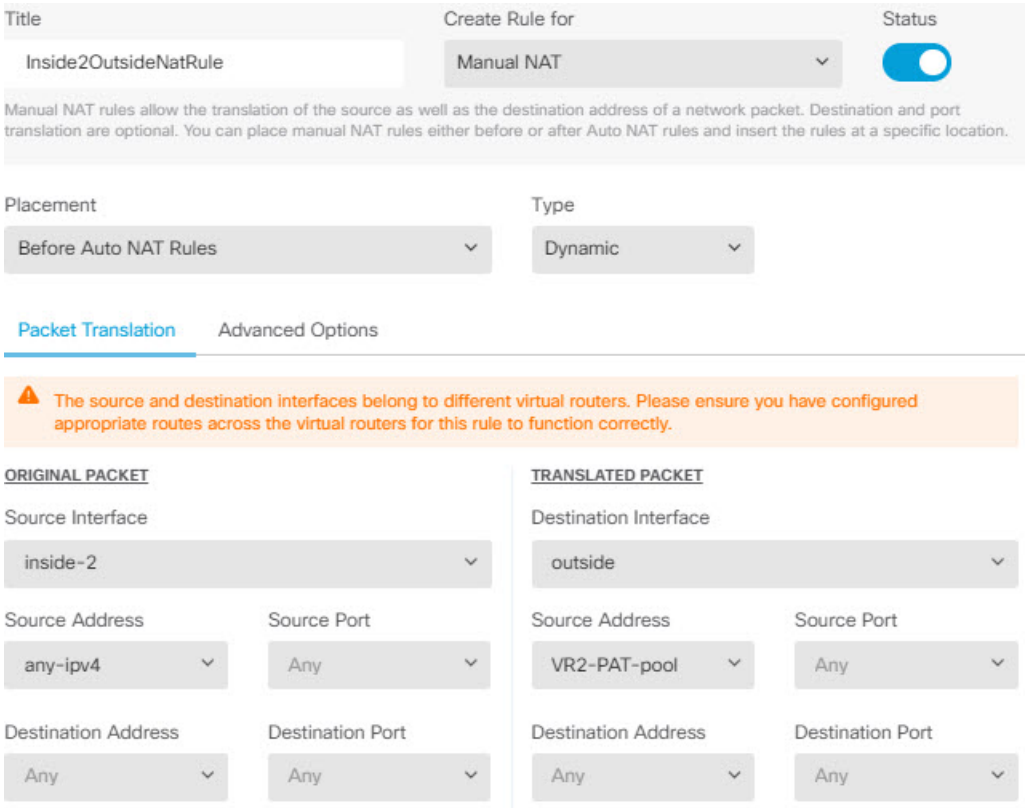
f) Cliquez sur **OK**.

Étape 8 Créez la règle NAT pour appliquer la PAT de inside-2 (interne-2) vers outside (externe) à 10.100.10.2.

Cette règle ressemblera exactement à celle de VR1, avec les exceptions suivantes :

- **Name (nom)** : il doit être unique, par exemple, Inside2OutsideNatRule.
- **Original Packet (Paquet d'origine)** > **Source Interface (Interface source)** : sélectionnez inside-2.
- **Translated Packet (Paquet traduit)** > **Source Address (Adresse source)** : créez un nouvel objet réseau d'hôte pour 10.100.10.2.

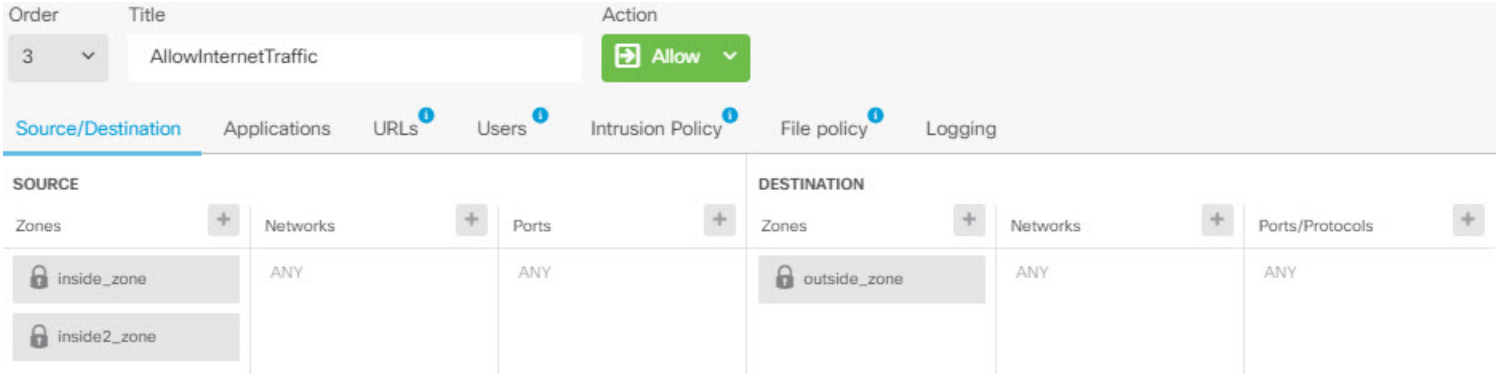
La règle devrait ressembler à ce qui suit :



Étape 9 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** et configurez une règle de contrôle d'accès pour autoriser le trafic de inside_zone et inside2_zone vers outside_zone.

Enfin, vous devez configurer la politique de contrôle d'accès pour permettre le trafic des interfaces inside et inside-2 vers l'interface outside (externe). Comme la règle de contrôle d'accès nécessite des zones de sécurité, vous devez créer des zones pour chacune de ces interfaces. Vous pouvez aussi créer une zone unique pour inclure inside et inside-2, mais il est probable que vous souhaiterez créer des règles supplémentaires, ici ou dans d'autres politiques, afin de différencier le traitement du trafic dans ces routeurs.

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 une politique de prévention des intrusions à cette règle selon vos besoins. Vous pouvez définir des règles supplémentaires pour bloquer le trafic indésirable, par exemple pour appliquer un filtrage d'URL.



Surveillance des routeurs virtuels

Pour surveiller et dépanner les routeurs virtuels, ouvrez la console de l'interface de ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes. Vous pouvez également sélectionner certaines de ces commandes dans le menu **Commands** (Commandes) sur la page Routing (Routage).

- **show vrf** affiche les renseignements sur les routeurs virtuels définis sur le système.
- **show ospf** [**vrf** *name* | **all**]

  Affiche les informations sur le processus OSPF dans un routeur virtuel. Vous pouvez spécifier un routeur virtuel pour voir les informations sur le processus dans ce routeur virtuel uniquement, ou omettre l'option afin de voir les informations sur VRF sur tous les routeurs virtuels. Utilisez **show ospf ?** pour voir les options supplémentaires.
- **show bgp** [**vrf** *name* | **all**]

  Affiche les informations sur le processus BGP dans un routeur virtuel. Vous pouvez spécifier un routeur virtuel pour voir les informations sur le processus dans ce routeur virtuel uniquement, ou omettre l'option afin de voir les informations sur VRF sur tous les routeurs virtuels. Utilisez **show bgp ?** pour voir les options supplémentaires.
- **show eigrp** *option*

  Affiche les renseignements sur le processus EIGRP. Utilisez **show eigrp ?** pour voir les options disponibles.

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.