Routage basé sur les politiques

Ce chapitre décrit comment configurer Défense contre les menaces pour prendre en charge le routage basé sur les politiques (PBR) à l'aide de la page Policy Based Routing (routage basé sur les politiques) de Centre de gestion. Les sections suivantes décrivent le routage basé sur les politiques, les consignes pour PBR et la configuration pour PBR.

À propos du routage basé sur les politiques

Dans le routage traditionnel, les paquets sont acheminés en fonction de l'adresse IP de destination. Cependant, il est difficile de modifier le routage d'un trafic spécifique dans un système de routage basé sur la destination. Le routage basé sur les politiques (PBR) vous donne plus de contrôle sur le routage en étendant et en complétant les mécanismes existants fournis par les protocoles de routage.

PBR vous permet de définir la priorité IP. Elle vous permet également de préciser un chemin pour certains trafics, tel que le trafic prioritaire sur une liaison onéreuse. PBRvous permet de définir un routage en fonction de critères autres que le réseau de destination, comme le port source, l'adresse de destination, le port de destination, le protocole, les applications ou une combinaison de ces objets.

Vous pouvez utiliser PBR pour classer le trafic réseau en fonction des applications. Cette méthode de routage est applicable dans les scénarios où de nombreux périphériques accèdent à des applications et à des données dans un grand déploiement de réseau. Généralement, les grands déploiements ont des topologies qui transportent tout le trafic réseau vers un concentrateur en tant que trafic chiffré dans un VPN basé sur le routage. Ces topologies entraînent souvent des problèmes tels que la latence des paquets, une bande passante réduite et la perte de paquets. Surmonter ces problèmes nécessite des déploiements et une gestion complexes et coûteux.

La politique PBR vous permet de répartir le trafic en toute sécurité pour des applications spécifiées. Vous pouvez configurer la politique [PBR dans l'interface utilisateur Cisco Secure Firewall Management Center pour autoriser un accès direct aux applications.

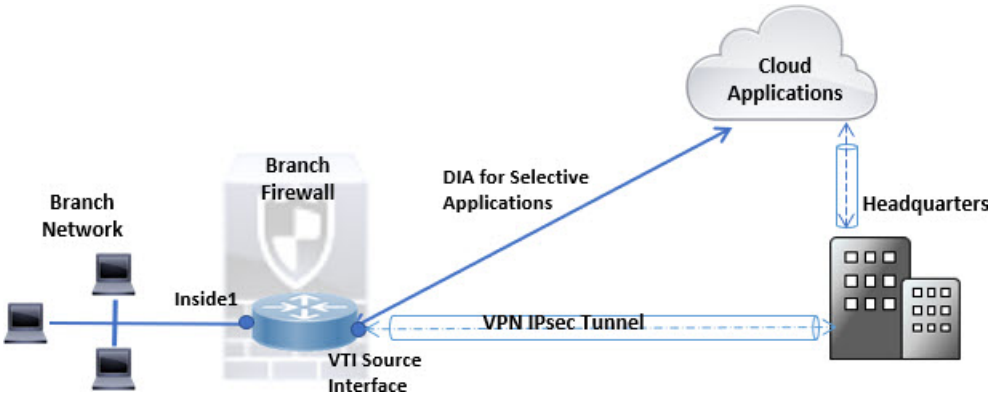
Pourquoi utiliser le routage à base de politiques?

Imaginez une entreprise qui dispose de deux liaisons entre des sites : l'une, une liaison onéreuse à bande passante élevée et à faible délai, et l'autre, à faible bande passante, avec un délai plus élevé et un moindre coût. Lors de l'utilisation de protocoles de routage traditionnels, la liaison à plus grande largeur de bande reçoit la majeure partie, voire la totalité, du trafic qui y est envoyé, en fonction des économies de métriques obtenues grâce aux caractéristiques de la bande passante, du délai ou des deux (avec EIGRP ou OSPF) de la liaison. Avec PBR, vous pouvez acheminer le trafic de priorité supérieure sur la liaison à bande passante élevée/faible délai, tout en envoyant tout le reste du trafic sur la liaison à bande passante faible/délai élevé.

Voici quelques scénarios dans lesquels vous pouvez utiliser le routage basé sur des politiques :

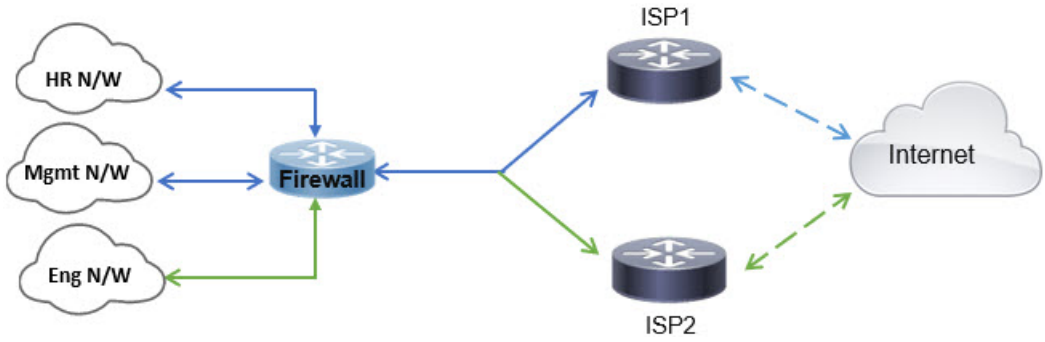
Accès Internet direct

Dans cette topologie, le trafic d'application de la succursale peut être acheminé directement vers Internet plutôt que par le biais du tunnel VPN se connectant au siège social. La succursale défense contre les menaces est configurée avec un point de sortie Internet et la politique PBR est appliquée sur l'interface d'entrée (*Inside 1*) pour identifier le trafic en fonction des applications définie dans la liste de contrôle d'accès. En conséquence, le trafic est acheminé par les interfaces de sortie directement à Internet ou au tunnel VPN IPsec.



Routage à accès égal et sensible à la source

Dans cette topologie, le trafic des réseaux des ressources humaines et de gestion peut être configuré pour passer par FAI1, et le trafic du réseau des ingénieurs peut être configuré pour passer par FAI2. Ainsi, le routage basé sur les politiques permet aux administrateurs réseau de fournir un routage à accès égal et sensible à la source, comme indiqué ici.



Partage de la charge

En plus des fonctionnalités de partage dynamique de charge offertes par l'équilibrage de charge ECMP, les administrateurs réseau peuvent désormais mettre en œuvre des politiques pour répartir le trafic entre plusieurs chemins en fonction des caractéristiques du trafic.

Par exemple, dans la topologie décrite dans le scénario de routage à accès égalitaire sensible, un administrateur peut configurer le routage basé sur une politique pour acheminer le trafic du réseau des Ressources humaines par ISP1 et le trafic du réseau Eng par ISP2 et ainsi partager la charge.

Lignes directrices et limites pour le routage basé sur des politiques

Directives sur le mode pare-feu

PBR n'est pris en charge qu'en mode pare-feu routé.

Directives relatives aux périphériques

- Les pages de routage basé sur les politiques dePBR à centre de gestion ne sont prises en charge qu'à partir de la version 7.1 et ultérieures sur centre de gestion comme sur le périphérique.
- Lorsque vous mettez à niveau centre de gestion ou Défense contre les menaces à la version 7.1 ou une version ultérieure, la configuration PBR du périphérique est supprimée. Vous devez configurer à nouveau PBR à l'aide de la page Policy Based Routing (routage basé sur les politiques). Si la version 7.1 du périphérique géré est antérieure, vous devez configurer PBR à nouveau à l'aide de FlexConfig et avec l'option de déploiement définie à « chaque fois ».
- La configuration d'une politique PBR basée sur l'application sur les périphériques de la grappe n'est pas prise en charge.

Directives relatives à l'interface

- Seules les interfaces routées et les interfaces non réservées à la gestion appartenant au routeur virtuel global peuvent être configurées en tant qu'interface d'entrée ou de sortie.
- PBR n'est pas pris en charge par les routeurs virtuels définis par l'utilisateur.
- Seules les interfaces qui ont un nom logique peuvent être définies dans la politique.
- Les VTI statiques peuvent être configurées uniquement en tant qu'interfaces de sortie.
- Avant de procéder à la configuration, assurez-vous que le trafic d'entrée et de sortie de chaque session traverse la même interface destinée au fournisseur de services Internet pour éviter les comportements imprévus causés par le routage dissymétrique, en particulier lorsque la NAT et le VPN sont utilisés.

Prise en charge d'IPv6

PBR prend en charge IPv6.

Configuration DNS et PBR basée sur les applications

- Le PBR basé sur les applications utilise la surveillance DNS pour la détection des applications. La détection de l'application ne réussit que si les demandes DNS passent par défense contre les menaces dans un format de texte en clair; le trafic DNS n'est pas chiffré.
- Vous devez configurer des serveurs DNS de confiance.

Pour en savoir plus sur la configuration des serveurs DNS, consultez DNS.

Politiques PBR non appliquées pour la recherche de route de sortie

Le routage basé sur des règles est une fonction d'entrée uniquement, c'est-à-dire qu'il n'est appliqué qu'au premier paquet d'une nouvelle connexion entrante, et c'est à ce moment-là que l'interface de sortie est sélectionnée pour le tronçon d'aller de la connexion. Notez que PBR ne sera pas déclenché si le paquet entrant appartient à une connexion existante ou si la NAT est appliquée et que cette dernière choisit l'interface de sortie.

Politiques PBR non appliquées pour le trafic amorce

Remarque Il y a connexion amorce lorsque l'établissement de liaison nécessaire entre la source et la destination n'a pas lieu.

Lorsqu'une nouvelle interface interne est ajoutée et qu'une nouvelle politique VPN est créée à l'aide d'un groupement d'adresses unique, le PBR est appliqué à l'interface externe correspondant à la source du nouveau groupement de clients. Ainsi, PBR envoie le trafic du client au prochain saut sur la nouvelle interface. Cependant, PBR n'est pas impliqué dans le trafic de retour d'un hôte qui n'a pas encore établi de connexion avec les nouvelles routes d'interface interne vers le client. Ainsi, le trafic de retour de l'hôte vers le client VPN, en particulier la réponse du client VPN, est abandonné car il n'y a aucune voie de routage valide. Vous devez configurer une voie de routage statique pondérée avec une métrique plus élevée sur l'interface interne.

Directives supplémentaires

- Toutes les restrictions de configuration existantes et les limites de la carte de routage seront reportées.
- Lors de la définition de la liste de contrôle d'accès pour les critères de correspondance de politique, vous pouvez sélectionner plusieurs applications dans une liste d'applications prédéfinies pour former une entrée de contrôle d'accès (ACE). Dans défense contre les menaces , les applications prédéfinies sont stockées en tant qu'objets de service réseau et le groupe d'applications en tant que groupes de services réseau (NSG). Vous pouvez créer un maximum de 1 024 groupes de service réseau L'application ou le groupe de services réseau est détecté par la classification du premier paquet. Actuellement, il n'est pas possible d'ajouter des applications à la liste des applications prédéfinies ou de la modifier.
- Le transfert de chemin inverse de monodiffusion (uRPF) valide l'adresse IP source des paquets reçus sur une interface par rapport à la table de routage et non par rapport à la carte de routage PBR. Lorsque uRPF est activé, les paquets reçus sur une interface par l'intermédiaire de PBR sont abandonnés tels qu'ils sont, sans l'entrée de route spécifique. Par conséquent, lorsque vous utilisez PBR, assurez-vous de désactiver uRPF.

Surveillance des chemins d'accès

La surveillance des chemins, lorsqu'elle est configurée sur des interfaces, dérive des mesures telles que le temps aller-retour (RTT), la gigue, la note moyenne d'opinion (MOS) et les pertes de paquets par interface. Ces mesures sont utilisées pour déterminer le meilleur chemin pour le routage du trafic PBR.

Les mesures sur les interfaces sont collectées dynamiquement à l'aide de messages de sonde ICMP envoyés à la passerelle par défaut de l'interface ou à un homologue distant spécifié.

Minuteries de surveillance par défaut

Pour la collecte et la surveillance des mesures, les minuteurs suivants sont utilisés :

- L'intervalle moyen du moniteur d'interface est de 30 secondes. Cet intervalle indique la fréquence de moyenne des sondes.
- L'intervalle de mise à jour du moniteur d'interface est de 30 secondes. Cet intervalle indique la fréquence à laquelle la moyenne des valeurs collectées est calculée et mise à la disposition de PBR pour déterminer le meilleur chemin de routage.
- L'intervalle de sonde du moniteur d'interface par ICMP est d'une seconde. Cet intervalle indique la fréquence à laquelle un message Ping ICMP est envoyé.

Remarque Vous ne pouvez pas configurer ou modifier l'intervalle de ces minuteries.

Surveillance des chemins d'accès

En règle générale, dans PBR, le trafic est acheminé par les interfaces de sortie en fonction de la valeur de priorité (coût d'interface) qui y est configurée. À partir de la version 7.2 du centre de gestion, PBR utilise la surveillance des chemins IP pour recueillir les mesures de performance (RTT, gigue, pertes de paquets et MOS) des interfaces de sortie. PBR utilise les mesures pour déterminer le meilleur chemin (interface de sortie) pour transférer le trafic. La surveillance des chemins informe périodiquement PBR de l'interface surveillée dont la métrique a été modifiée. PBR récupère les dernières valeurs de métrique pour les interfaces surveillées à partir de la base de données de surveillance des chemins et met à jour le chemin d'accès des données.

Vous devez activer la surveillance des chemins pour l'interface et configurer le type de surveillance. La page de politique PBR vous permet de spécifier la mesure souhaitée pour la détermination du chemin. Voir Configurer la politique de routage basée sur les politiques, à la page 6.

Configurer les paramètres de surveillance de chemin d'accès

La politique PBR s'appuie sur des mesures flexibles, telles que le temps aller-retour (RTT), la gigue, le score d'opinion moyen (MOS) et la perte de paquets des interfaces pour identifier le meilleur chemin de routage pour le trafic. La surveillance des chemins collecte ces mesures sur les interfaces spécifiées. Dans la page **Interfaces**, vous pouvez configurer des interfaces avec des paramètres pour la surveillance des chemins d'accès afin d'envoyer les sondes ICMP pour la collecte des métriques.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Path Monitoring** (surveillance des chemins).

Étape 4 Cochez la case **Enable Path Monitoring** (activer la surveillance des chemins d'accès).

Étape 5 Dans la liste déroulante **Monitoring Type** (type de surveillance), sélectionnez l'option appropriée :

- **Auto** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface. Si la passerelle IPv4 n'existe pas, la surveillance de chemin envoie les sondes à la passerelle IPv6 par défaut de l'interface.
- **Homologue IPv4** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, saisissez l'adresse IPv4 dans le champ **Peer IP To Monitor** (Adresse IP de l'homologue à surveiller).
- **Homologue IPv6** : envoie les sondes ICMP à l'adresse IPv6 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, saisissez l'adresse IPv6 dans le champ **Peer IP To Monitor** (Adresse IP de l'homologue à surveiller).
- **Auto IPv4** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface.
- **Auto IPv6** : envoie des sondes ICMP à la passerelle IPv6 par défaut de l'interface.

Remarque
- Les options Auto ne sont pas disponibles pour les interfaces VTI. Vous devez préciser l'adresse de l'homologue.
- Un seul saut suivant est surveillé vers une destination. C'est-à-dire que vous ne pouvez pas spécifier plus d'une adresse homologue pour surveiller une interface.

Étape 6 Cliquez sur **Ok**, et pour enregistrer les paramètres, cliquez sur **Enregistrer**.

Configurer la politique de routage basée sur les politiques

Vous pouvez configurer la politique PBR sur la page de routage basé sur les politiques en précisant les interfaces d'entrée, les critères de correspondance (liste de contrôle d'accès étendue) et les interfaces de sortie.

Avant de commencer

Pour utiliser les métriques de surveillance de chemin d'accès afin de configurer la priorité de transfert du trafic sur les interfaces de sortie, vous devez configurer les paramètres de surveillance de chemin d'accès pour les interfaces. Consultez Configurer les paramètres de surveillance de chemin d'accès, à la page 5.

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 **Routage basé sur les politiques**.

La page Policy Based Routing (Routage basé sur les politiques) affiche la politique configurée. La grille affiche la liste des interfaces d'entrée et une combinaison de la liste d'accès de routage basée sur les politiques et des interfaces de sortie.

Étape 4 Pour configurer la politique, cliquez sur **Add** (Ajouter).

Étape 5 Dans la boîte de dialogue **Add Policy Based Route** (ajouter un routage basé sur les politiques), sélectionnez l'**interface d'entrée** dans la liste déroulante.

Remarque Seules les interfaces qui ont des noms logiques et qui appartiennent à un routeur virtuel global sont répertoriées dans la liste déroulante.

Étape 6 Pour préciser les critères de correspondance et l'action de transfert dans la politique, cliquez sur **Add** (Ajouter).

Étape 7 Dans la boîte de dialogue **Add Forwarding Actions** (Ajouter des actions de transfert), procédez comme suit :

a) Dans la liste déroulante **Match ACL**, choisissez l'objet de liste de contrôle d'accès étendu. Vous pouvez prédéfinir l'objet ACL (voir Configurer les objets ACL étendus) ou cliquer sur l'icône **Ajouter** (+) pour créer l'objet. Dans la zone **New Extended Access List Object** (nouvel objet de liste d'accès étendu), saisissez un nom, cliquez sur **Add** (ajouter) pour ouvrir la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), dans laquelle vous pouvez définir le réseau, le port, ou les critères de correspondance d'application pour la politique PBR.

Remarque L'application et l'adresse de destination ne peuvent pas être définies dans une interface ACE.

Pour appliquer sélectivement le PBR sur l'interface entrante, vous pouvez définir les critères de *blocage* dans l'ACE. Lorsque le trafic correspond à la règle de blocage de l'ACE, le trafic est acheminé vers l'interface de sortie en fonction de la table de routage.

b) Dans la liste déroulante **Send To** (envoyer à) :

- Pour sélectionner les interfaces configurées, choisissez **Egress Interfaces** (interfaces de sortie).
- Pour préciser les adresses du prochain saut IPv4/IPv6, choisissez **IP Address** (Adresse IP). Passez à l'étape 7.e, à la page 8

c) Si vous avez sélectionné **Interfaces de sortie**, dans la liste déroulante **Interface Ordering** (ordre des interfaces), choisissez l'option appropriée :

- Par **priorité d'interface** : le trafic est acheminé en fonction de la priorité des interfaces. Le trafic est acheminé vers l'interface ayant la valeur de priorité la moins élevée en premier. Lorsque l'interface n'est pas disponible, le trafic est ensuite acheminé vers l'interface possédant la prochaine valeur de priorité la plus basse. Par exemple, supposons que *Gig0/1* , *Gig0/2*et *Gig0/3* sont configurés avec les valeurs de priorité *0* ,*1* et *2* respectivement. Le trafic est acheminé vers *Gig0/1*. Si *Gig0/1* devient indisponible, le trafic est ensuite acheminé vers *Gig0/2*.

Remarque Pour configurer la priorité des interfaces, cliquez sur **Configure Interface Priority** (Configurer la priorité des interfaces) dans la page Policy Based Routing (routage basé sur les politiques). Dans la boîte de dialogue, indiquez le numéro de priorité par rapport aux interfaces, puis cliquez sur **Save** (Enregistrer). Vous pouvez également configurer la priorité d'une interface dans les paramètres d'interface.

Lorsque la valeur de priorité est la même pour toutes les interfaces, le trafic est équilibré entre les interfaces.

- Par **ordre** : le trafic est acheminé en fonction de la séquence des interfaces spécifiée ici. Par exemple, supposons que *Gig0/1*, *Gig0/2*et *Gig0/3* sont sélectionnés dans l'ordre suivant, *Gig0/2*, *Gig0/3*, *Gig0/1*. Le trafic est acheminé vers *Gig0/2* d'abord, puis vers *Gig0/3*, quelles que soient leurs valeurs de priorité.
- Par **Gigue minimale** : le trafic est acheminé vers l'interface qui a la valeur de gigue la plus faible. Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs de gigue.
- Par **note d'opinion moyenne maximale** : le trafic est acheminé vers l'interface qui a la note d'opinion maximale moyenne (MOS). Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs MOS.
- Par **temps aller-retour minimal** : le trafic est acheminé vers l'interface qui a le temps aller-retour minimal (RTT). Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs RTT.
- Par **perte de paquets minimale** : le trafic est acheminé vers l'interface qui a le moins de pertes de paquets. Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs de perte de paquets.

d) Dans la zone **available Interfaces** (interfaces disponibles), toutes les interfaces sont répertoriées avec leurs valeurs de priorité. Dans la liste des interfaces, cliquez sur le bouton **Ajouter** (⊕) pour ajouter aux interfaces de sortie sélectionnées. Passez à l'étape 7.k, à la page 9

e) Si vous avez sélectionné **IP Address** (adresse IP), saisissez les adresses IP séparées par des virgules dans les champs **IPv4 Addresses** ou **IPv6 Addresses** (adresses IPv4 ou IPv6).

Remarque Lorsque plusieurs adresses IP de saut suivant sont fournies, le trafic est acheminé selon la séquence des adresses IP spécifiée jusqu'à ce qu'une adresse IP de saut suivant routable soit trouvée. Les prochains sauts configurés doivent être connectés directement.

f) Dans la liste déroulante **Ne pas fragmenter**, sélectionnez Yes, No ou None (Oui, Non ou Aucun). Si l'indicateur DF (Don't Fragment) est défini à *Yes*, les routeurs intermédiaires n'effectuent jamais la fragmentation d'un paquet.

g) Pour spécifier l'interface actuelle par défaut pour le transfert, cochez la case **Default Interface** (interface par défaut).

h) Les onglets **Paramètres IPv4** et **Paramètres IPv6** vous permettent de spécifier les paramètres récursifs et par défaut :

Remarque Pour une carte de routage, vous pouvez uniquement spécifier les paramètres du prochain saut IPv4 ou IPv6.

- **Récursif** : la configuration de la carte de routage est appliquée uniquement lorsque l'adresse de saut suivant et l'adresse de saut suivant par défaut se trouvent sur un sous-réseau directement

connecté. Cependant, vous pouvez utiliser l'option récursive, où l'adresse du saut suivant n'a pas besoin d'être connectée directement. Ici, une recherche récursive est effectuée sur l'adresse de saut suivant, et le trafic correspondant est transmis au saut suivant utilisé par cette entrée de route en fonction du chemin de routage actuel du routeur.

- **Par défaut** : si la recherche de route normale ne parvient pas à correspondre au trafic, le trafic est transféré vers l'adresse IP de saut suivant spécifiée.

i) Cochez la case **Peer Address** (adresse homologue) pour utiliser l'adresse du saut suivant comme adresse homologue.

Remarque Vous ne pouvez pas configurer une carte de routage avec une adresse de saut suivant par défaut et une adresse d'homologue.

j) Pour les paramètres IPv4, vous pouvez vérifier si les prochains sauts IPv4 d'une carte de routage sont disponibles sous **Vérifier la disponibilité** : cliquez sur le bouton **Ajouter** (+) et ajoutez les entrées d'adresses IP du saut suivant :

- **Adresse IP** : saisissez l'adresse IP.
- **Séquence** : les entrées sont évaluées dans l'ordre en utilisant le numéro de séquence. Vérifiez qu'aucun numéro de séquence en double n'est saisi. La plage valide est de 1 à 65 535.
- **Suivi** : saisissez un ID valide. La plage valide est de 1 à 255.

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

Étape 8 Pour enregistrer la politique, cliquez sur **Save** and **Deploy** (enregistrer et déployer).

---

défense contre les menaces utilise les listes de contrôle d'accès pour faire correspondre le trafic et effectuer des actions de routage sur le trafic. En règle générale, vous configurez une carte de routage qui spécifie une liste de contrôle d'accès à laquelle le trafic est comparé, puis vous spécifiez une ou plusieurs actions pour ce trafic. Grâce à la surveillance des chemins, PBR peut désormais sélectionner la meilleure interface de sortie pour acheminer le trafic. Enfin, vous associez la carte de routage à une interface à laquelle vous souhaitez appliquer PBR à tout le trafic entrant.

Ajouter un tableau de bord de supervision du chemin d'accès

Pour afficher les mesures de surveillance de chemin d'accès, vous devez ajouter le tableau de bord de surveillance de chemin d'accès à la page de surveillance de l'intégrité du périphérique.

Procédure

Étape 1 Sélectionnez **System (Système)** > **Health (Intégrité)** > **Monitor (Moniteur)**.

Étape 2 Sélectionnez le périphérique et cliquez sur **Add New Dashboard** (Ajouter un nouveau tableau de bord).

Étape 3 Saisissez un nom pour le tableau de bord personnalisé.

Étape 4 Dans la zone **Metrics** (Mesures), cliquez sur le bouton **Add from Predefined Correlations** (Ajouter à partir de corrélations prédéfinies).

Étape 5 Dans la liste, cliquez sur **Interface - Path Metrics** (interface _ Mesures du chemin d'accès).

Par défaut, les quatre mesures sont sélectionnées pour s'afficher sous forme de portlets dans le tableau de bord avec un champ de mesure supplémentaire. Vous pouvez exclure l'une d'entre elles en cliquant sur **Supprimer** ( ).

Étape 6 Cliquez sur **Add Dashboard** (Ajouter un tableau de bord).

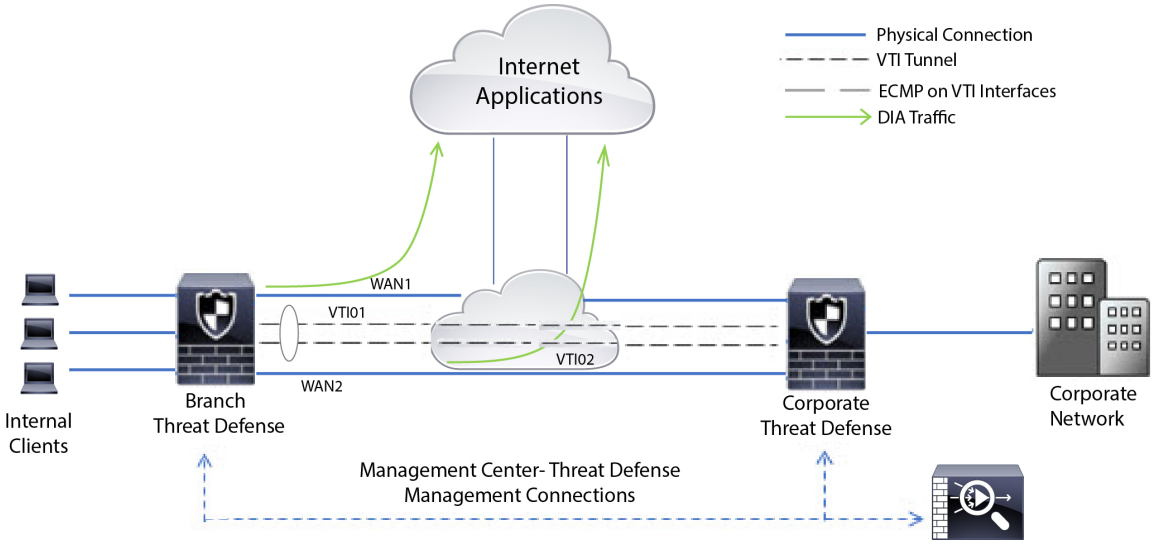
Exemple de configuration pour le routage basé sur les politiques

Voici un scénario de réseau d'entreprise typique dans lequel tout le trafic du réseau de succursale passe par un VPN du réseau d'entreprise basé sur le routage et diverge vers l' extranet, au besoin. L'accès aux applications Web qui traitent des opérations quotidiennes par le biais du réseau de l'entreprise entraîne des coûts d'expansion et de maintenance considérables. Cet exemple illustre la procédure de configuration PBR pour un accès Internet direct.

La figure suivante montre la topologie d'un réseau d'entreprise. Le réseau de la succursale est connecté au réseau d'entreprise par un VPN basé sur le routage. Habituellement, le défense contre les menaces d'entreprise est configuré pour gérer le trafic interne et externe de la succursale. Avec la politique PBR, la succursale défense contre les menaces est configurée avec une politique qui achemine un trafic particulier vers le réseau étendu plutôt que vers les tunnels virtuels. Le reste du trafic passe par le VPN basé sur le routage, comme d'usage.

Cet exemple illustre également la configuration des interfaces WAN et VTI avec les zones ECMP pour réaliser l'équilibrage de la charge.

Illustration 1 : Configuration du routage basé sur les politiques sur la succursale Défense contre les menaces dans Centre de gestion



Avant de commencer

Cet exemple suppose que vous avez déjà configuré les interfaces WAN et VTI pour la succursale défense contre les menaces dans centre de gestion.

Procédure

Étape 1 Configurez le routage basé sur les politiques pour la succursale défense contre les menaces , sélectionnez les interfaces d'entrée :

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

b) Choisissez **Routing (Routage)** > **Policy Based Routing**et dans la page **Policy Based Routing** (routage basé sur les politiques), cliquez sur **Add** (ajouter).

c) Dans la boîte de dialogue **Add Policy Based Route** (ajouter une route basée sur les politiques), sélectionnez les interfaces (disons, *Inside1* et *Inside2*) dans la liste déroulante **interface d'entrée**.

Étape 2 Précisez les critères de correspondance :

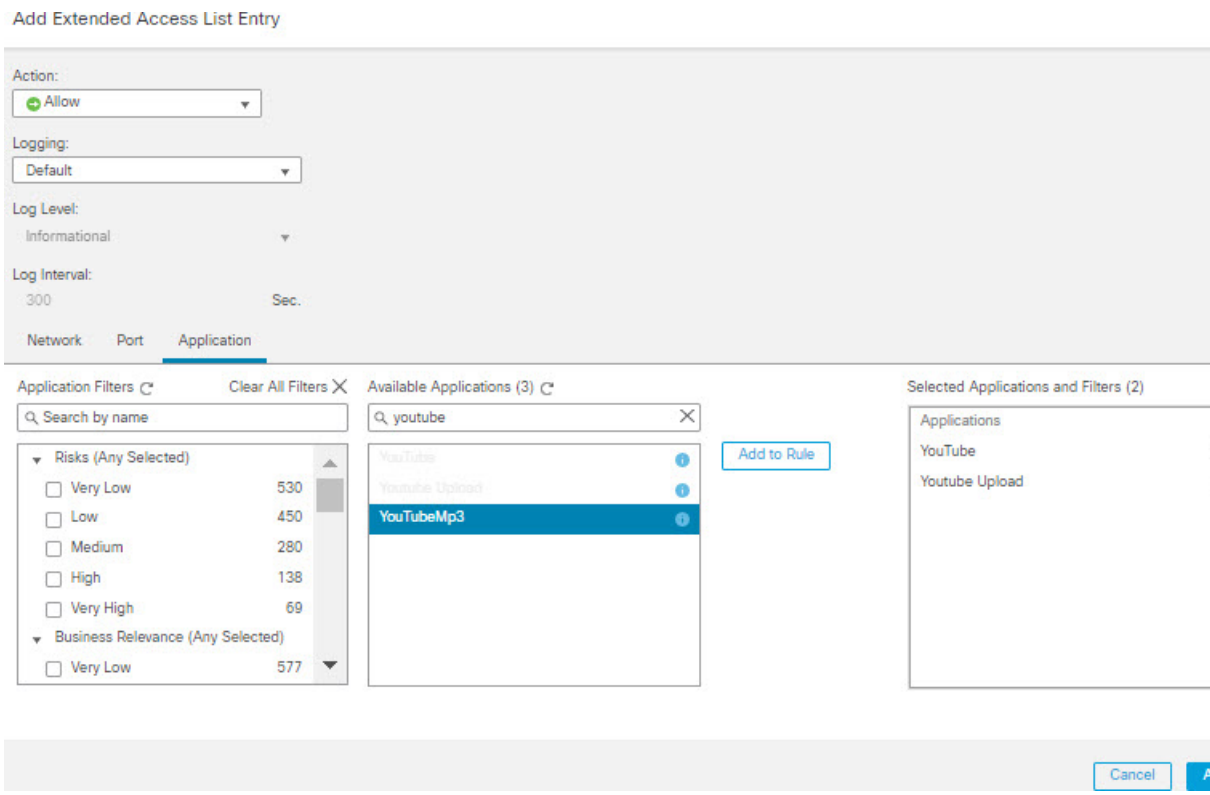
a) Cliquez sur **Add** (ajouter).

b) Pour définir les critères de correspondance, cliquez sur le bouton **Ajouter** (+).

c) Dans **le nouvel objet de liste d'accès étendu**, saisissez le nom de la liste d'accès (ACL) (disons, *DIA-FTD-Branch*) et cliquez sur **Add** (Ajouter).

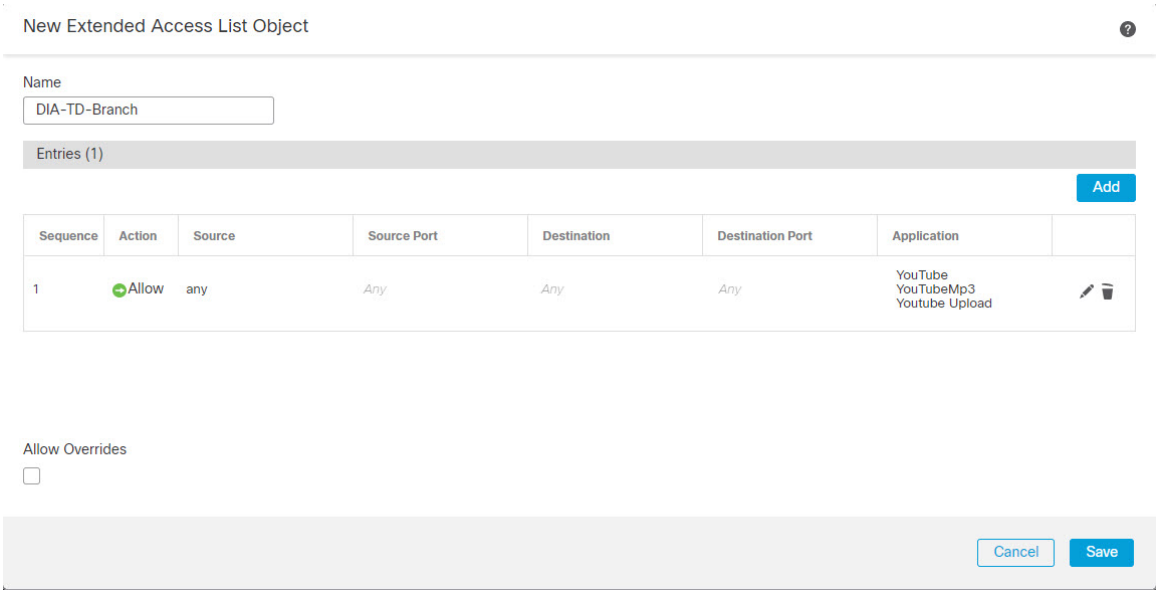
d) Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionnez les applications Web requises dans l'onglet **Application** :

Illustration 2 : Onglet Applications



Sur défense contre les menaces , le groupe d'applications d'une ACL est configuré en tant que groupe de service réseau et chaque application en tant qu'objet de service réseau.

Illustration 3 : Liste de contrôle d'accès étendue



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

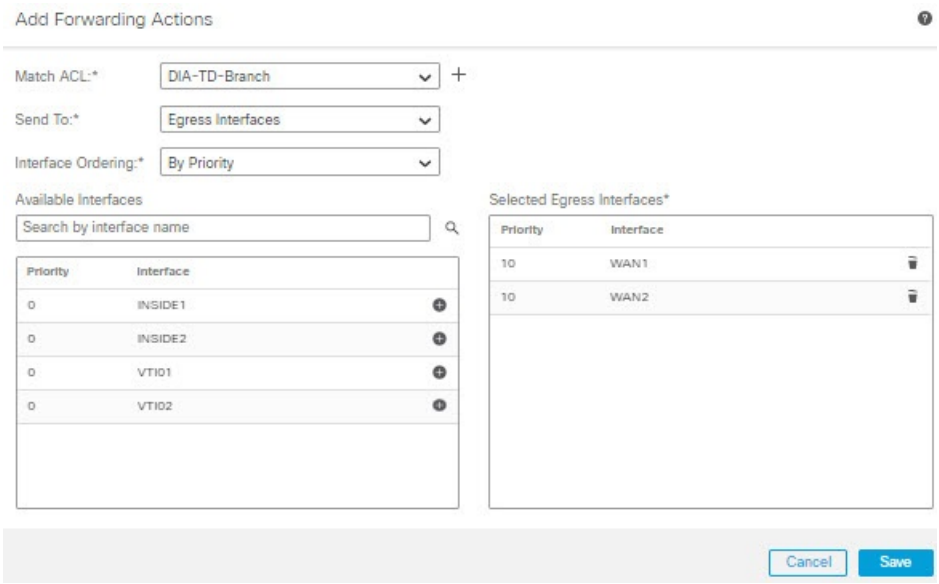
f) Sélectionnez *DIA-FTD-Branch* dans la liste déroulante **Match ACL** (Liste de contrôle d'accès de correspondance).

Étape 3 Précisez les interfaces de sortie :

a) Dans les listes déroulantes **Send To** (Envoyer à) et **Interface Ranking** (Ordre des interfaces), choisissez Interfaces de sortie et Par priorité respectivement.

b) Sous **Availability Interfaces** (interfaces disponibles), cliquez sur le bouton ⊕ à côté des noms d'interface respectifs pour ajouter *le WAN1* et *WAN2* :

Illustration 4 : Configurer le routage basé sur les politiques



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

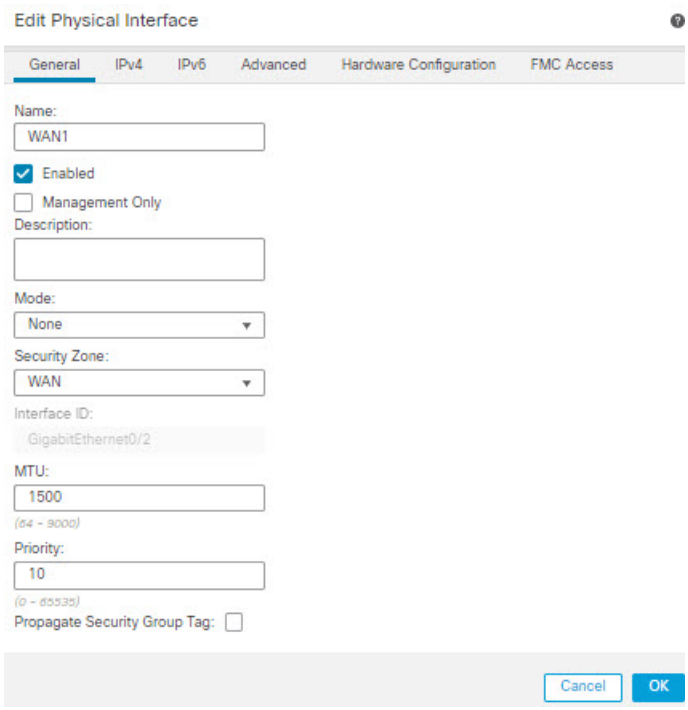
Étape 4 Configuration de la priorité des interfaces :

Vous pouvez définir la valeur de priorité des interfaces dans la page **Edit Physique Interface** (Modifier la priorité des interfaces) ou dans la page **Policy Based Routing** (Routage basé sur les politiques (**Configure Interface Priority**) (Configurer la priorité des interfaces). Dans cet exemple, la méthode de modification de l'interface physique est décrite.

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

b) Définissez la priorité des interfaces. Cliquez sur **Edit**(Modifier) en regard de l'interface et saisissez la valeur de priorité :

Illustration 5 : Définir la priorité de l'interface



c) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

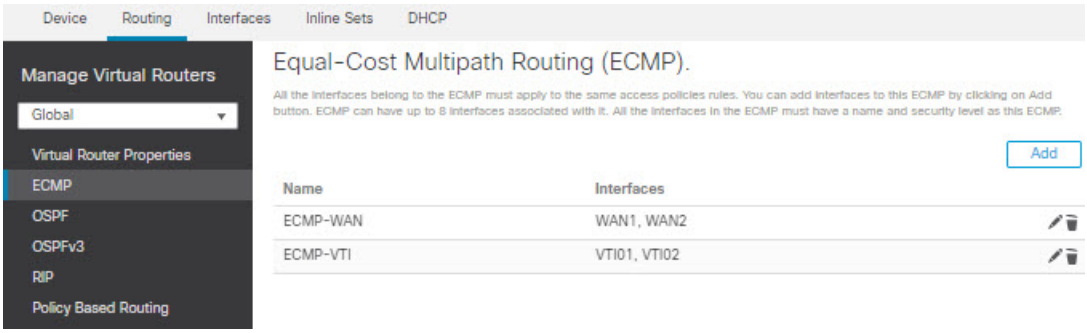
Étape 5 Créer des zones ECMP pour l'équilibrage de la charge :

a) Dans la page **Routing** (routage), cliquez sur **ECMP**.

b) Pour associer des interfaces à la zone ECMP, cliquez sur **Add** (Ajouter).

c) Sélectionnez *WAN 1* et *WAN 2* et créez une zone ECMP : *ECMP-WAN*. De même, ajoutez *VTI01* et *VTI02* et créez une zone ECMP : *ECMP-VTI* :

Illustration 6 : Association des interfaces à la zone ECMP

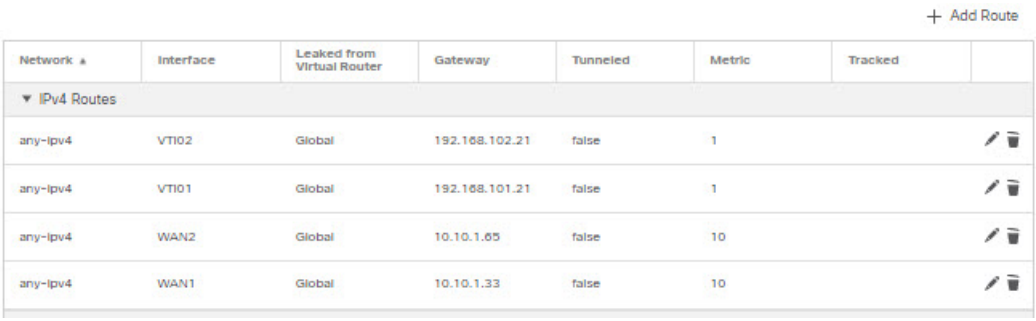


Étape 6 Configurez les routes statiques pour les interfaces de zone aux fins d'équilibrage de la charge :

a) Dans la page **Routing** (routage), cliquez sur **Static Route** (Route statique).

b) Cliquez sur **Add** (ajouter) et spécifiez les routes statiques pour *WAN1*, *WAN2*, *VTI01*et *VTI02*. Assurez-vous de spécifier la même valeur de métrique pour les interfaces appartenant aux mêmes zones ECMP (Étape 5) :

Illustration 7 : Configuration des routes statiques pour les interfaces de zone ECMP



Remarque Assurez-vous que les interfaces de zone ont la même adresse de destination et la même métrique, mais des adresses de passerelle différentes.

Étape 7 Configurez un DNS de confiance sur les objets WAN de la succursale défense contre les menaces pour sécuriser le flux de trafic vers Internet :

a) Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créer une politique DNS sur la succursale défense contre les menaces .

b) Pour spécifier le DNS de confiance, **modifiez** la politique et cliquez sur **DNS**.

c) Pour préciser les serveurs DNS que la résolution DNS doit utiliser par les objets WAN, dans l'onglet **DNS Settings** (Paramètres DNS) , fournissez les détails du groupe de serveurs DNS et sélectionnez WAN dans les objets de l'interface.

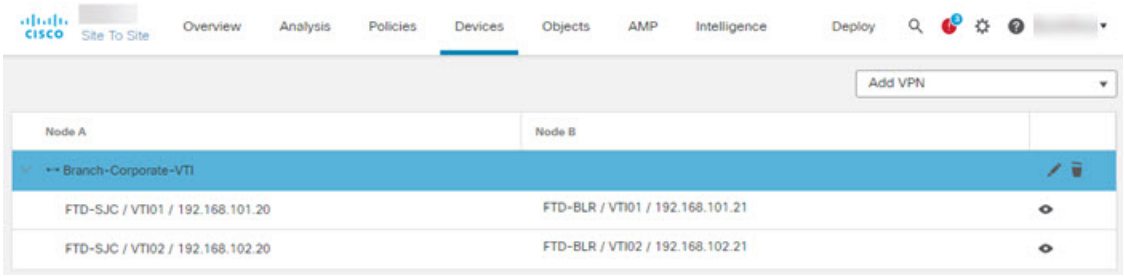
d) Utilisez l'onglet **Trusted DNS Servers** (Serveurs DNS de confiance) pour fournir des serveurs DNS spécifiques en lesquels vous faites confiance pour la résolution DNS.

Étape 8 **Enregistrez** et **déployez**.

Toutes les demandes d'accès liées à *YouTube* et en provenance de la succursale *INSIDE1* ou *INSIDE2* du réseau sont acheminées vers *WAN1* ou *WAN2* car elles correspondraient à la liste de contrôle d'accès (ACL

) DIA-FTD-Branch. Toute autre demande, par exemple *google.com*, est acheminée par *VTI01* ou *VTI02* comme configuré dans les paramètres VPN de site à site :

Illustration 8 : Paramètres VPN de site à site



Une fois ECMP configuré, le trafic réseau est équilibré en toute transparence.

Exemple de configuration pour PBR avec supervision du chemin d'accès

Cet exemple détaille la configuration de PBR avec surveillance de chemin pour les applications suivantes avec des mesures flexibles :

- Applications audio ou vidéo sensibles (par exemple, Webex Meetings) avec gigue.
- Application en nuage (par exemple, Office365) avec RTT.
- Contrôle d'accès basé sur le réseau (avec une source et une destination spécifiques) avec perte de paquets.

Avant de commencer

1. Cet exemple suppose que vous connaissez les étapes de configuration de base pour le système PBR.
2. Vous avez configuré des interfaces d'entrée et de sortie avec des noms logiques. Dans cet exemple, l'interface d'entrée est nommée *Inside1*et les interfaces de sortie sont nommées *ISP01*, *ISP02*et *ISP03*.

Procédure

Étape 1 Configuration de la surveillance des chemins sur les interfaces *ISP01*, *ISP02* et *ISP03* :

Pour la collecte de mesures sur les interfaces de sortie, vous devez activer et configurer la surveillance des chemins sur celles-ci.

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
b) Sous l'onglet **Interfaces** (interfaces), modifiez l'interface (dans notre exemple, *ISP01*)
c) Cliquez sur l'onglet **Path Monitoring** (surveillance des chemins), cochez la case **Enable Path Monitoring** (Activer la surveillance des chemins), puis spécifiez le type de surveillance (voir Configurer les paramètres de surveillance de chemin d'accès, à la page 5).
d) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

e) Répétez les mêmes étapes et configurez les paramètres de surveillance de chemin d'accès pour *ISP02* et *ISP03*.

Étape 2 Configurer le routage basé sur les politiques pour une succursale dans une organisation défense contre les menaces , sélectionnez les interfaces d'entrée :

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

b) Choisissez **Routing (Routage)** > **Policy Based Routing**et dans la page **Policy Based Routing** (routage basé sur les politiques), cliquez sur **Add** (ajouter).

c) Dans la boîte de dialogue **Add Policy Based Route** (ajouter une route basée sur les politiques), sélectionnez *Inside 1* dans la liste déroulante **Ingress Interface** (Interfaces d'entrée).

Étape 3 Précisez les critères de correspondance :

a) Cliquez sur **Add** (ajouter).

b) Pour définir les critères de correspondance, cliquez sur le bouton **Ajouter** (+).

c) Dans **le nouvel objet de liste d'accès étendu**, saisissez le nom de la liste d'accès (ACL) (par exemple, *PBR-Webex*) et cliquez sur **Add**(ajouter).

d) Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionnez les applications Web requises (par exemple, Webex Meetings) sous l'onglet **Application**.

Rappel Sur défense contre les menaces , le groupe d'applications d'une ACL est configuré en tant que groupe de service réseau et chaque application en tant qu'objet de service réseau.

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

f) Sélectionnez *PBR-Webex* dans la liste déroulante **match ACL** (ACL de correspondance).

Étape 4 Précisez les interfaces de sortie :

a) Dans la liste déroulante **Send To** (Envoyer à), choisissez Egress Interfaces (Interfaces de sortie).

b) Dans la liste déroulante **InterfaceOrdering** (Ordre d'interface), choisissez By Minimum jitter (Par gigue minimale).

c) Sous **Available Interfaces** (Interfaces disponibles) , cliquez sur le bouton **Flèche droite** (>) en regard des noms d'interface respectifs pour ajouter *ISP01*, *ISP02*, et *ISP03*.

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

Étape 5 Répétez les étapes 2 et 3 pour créer des PBR pour la même interface (*Inside1*) afin d'acheminer le trafic d' Office365 et de contrôle d'accès basé sur le réseau :

a) Créez un objet de critères de correspondance, par exemple *PBR- Office365*, et sélectionnez l'application Office365 dans l'onglet **Application** (application).

b) Dans la liste déroulante **Interface Ordering** (Ordre d'interface), choisissez By Minimal Round Trip Time (En réduisant au minimum la durée de l'aller-retour.)

c) Précisez les interfaces de sortie *ISP01*, *ISP02*et *ISP03*, puis cliquez sur **Save**(Enregistrer).

d) À présent, créez un objet de critères de correspondance, example *PBR-networks*, et spécifiez l'interface de source et de destination dans l'onglet **Network** (réseau).

e) Dans la liste déroulante **Interface Ordering** (Ordre d'interface), choisissez By Minimum Packet Loss (perte de paquets minimale).

f) Précisez les interfaces de sortie *ISP01*, *ISP02*et *ISP03*, puis cliquez sur **Save**(Enregistrer).

Étape 6 **Enregistrez** et **déployez**.

Étape 7 Pour afficher les métriques de surveillance des chemins, choisissez **Devices** > **Device Management**(gestion des périphériques) et, dans la zone **Plus** (⋮), cliquez sur **Health Monitor** (Surveillance de l'intégrité). Pour

afficher les détails de la métrique pour les interfaces du périphérique, vous devez ajouter le tableau de bord des métriques de chemin. Pour de plus amples renseignements, consultez la section Ajouter un tableau de bord de supervision du chemin d'accès , à la page 9.

Le trafic de Webex, Office365 et les ACL basées sur les réseaux sont acheminés par la meilleure route dérivée de la valeur des métriques collectées sur *ISP01*, *ISP02*et *ISP03*.

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.