

Routage basé sur une stratégie

Ce chapitre décrit comment configurer l'ASA pour prendre en charge le routage basé sur les politiques (BPR). Les sections suivantes décrivent le routage basé sur les politiques, les lignes directrices relatives au PBR et la configuration du PBR.

- À propos du routage basé sur les politiques, à la page 1
- Lignes directrices pour le routage basé sur des politiques, à la page 3
- Configurer le routage basé sur les politiques, à la page 5
- Historique du routage basé sur des politiques, à la page 8

À propos du routage basé sur les politiques

Le routage traditionnel est basé sur la destination, ce qui signifie que 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. Avec le routage basé sur les politiques (PBR), vous pouvez définir le routage en fonction de critères autres que le réseau de destination. Le PBR vous permet d'acheminer le trafic en fonction de l'adresse source, du port source, de l'adresse de destination, du port de destination, du protocole ou d'une combinaison de ces éléments.

Routage basé sur les politiques :

- Vous permet de fournir une qualité de service (QoS) à un trafic différencié.
- Vous permet de répartir le trafic interactif et par lots sur des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé.
- Permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies.

Le routage basé sur les politiques peut mettre en œuvre la QoS en classant et en marquant le trafic à la périphérie du réseau, puis en utilisant le PBR dans tout le réseau pour acheminer le trafic marqué le long d'un chemin spécifique. Cela permet le routage de paquets provenant de différentes sources vers différents réseaux, même lorsque les destinations sont les mêmes, et cela peut être utile pour interconnecter plusieurs réseaux privés.

Pourquoi utiliser le routage basé sur des politiques?

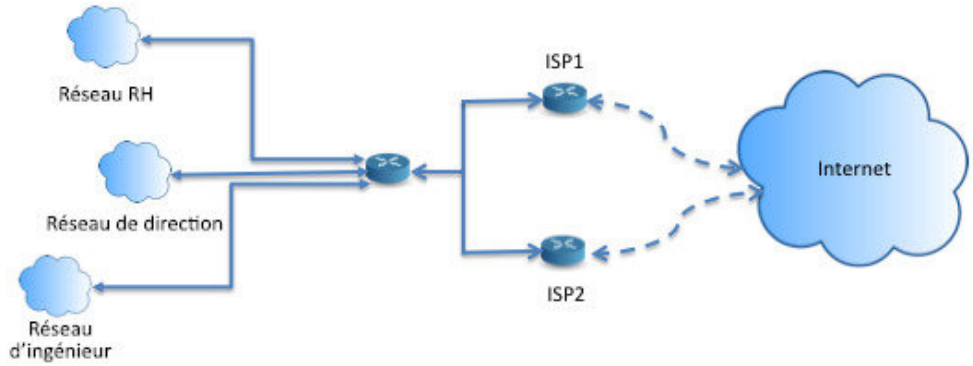
Imaginez une entreprise qui dispose de deux liaisons entre des sites : l'une, une liaison onéreuse à bande passante élevée et à faible délai, et l'autre, à faible bande passante, avec un délai plus élevé et un moindre

coût. Lors de l'utilisation de protocoles de routage traditionnels, la liaison à plus grande largeur de bande recevrait 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 et/ou du délai (avec EIGRP ou OSPF) de la liaison. PBR vous permet d'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.

Certaines applications du routage basé sur les politiques sont les suivantes :

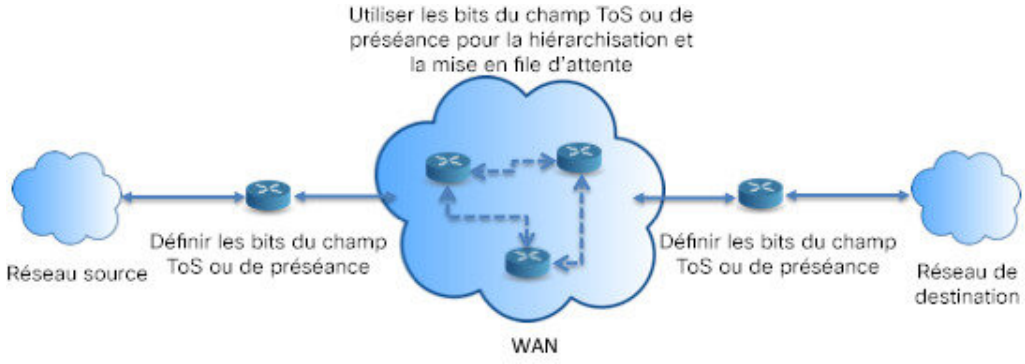
Routage à accès égal et sensible à la source

Dans cette topologie, le trafic provenant du réseau RH et du réseau 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.



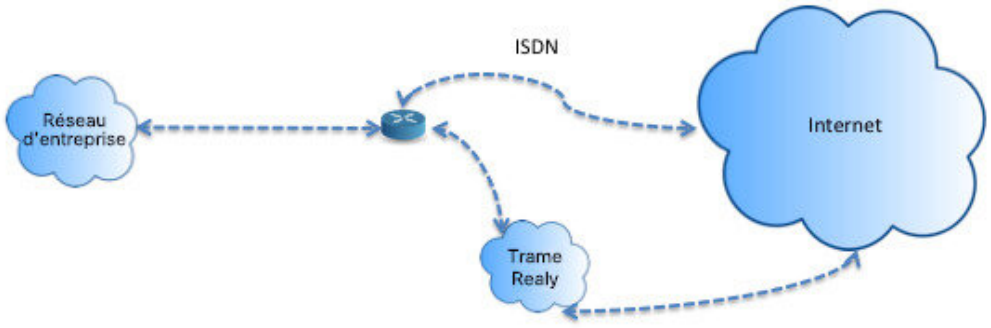
Qualité de service

En balisant les paquets avec le routage basé sur les politiques, les administrateurs réseau peuvent classer le trafic réseau au périmètre du réseau pour différentes classes de service, puis mettre en œuvre ces classes de service au cœur du réseau à l'aide de la mise en file d'attente de priorité, personnalisée ou pondérée (comme indiqué dans la figure ci-dessous). Cette configuration améliore les performances du réseau en éliminant le besoin de classer le trafic explicitement sur chaque interface WAN au cœur du réseau fédérateur.



Réduction des coûts

Une organisation peut diriger le trafic en bloc associé à une activité spécifique pour utiliser un lien à haute bande passante à coût élevé pendant une durée courte et maintenir la connectivité de base sur un lien à faible coût à bande passante inférieure pour le trafic interactif en définissant la topologie, 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 partager la charge du trafic provenant du réseau des Ressources humaines par ISP1 et du trafic provenant du réseau Eng par ISP2.

Mise en œuvre de PBR

L'ASA utilise les ACL pour faire correspondre le trafic et effectuer des actions de routage sur le trafic. Plus précisément, vous configurez une carte de routage qui spécifie une ACL pour la correspondance, puis vous spécifiez une ou plusieurs actions pour ce trafic. Enfin, vous associez la carte de routage à une interface sur laquelle vous souhaitez appliquer le PBR à tout le trafic entrant.

Remarque 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 asymétrique, en particulier lorsque la NAT et le VPN sont utilisés.

Lignes directrices pour le routage basé sur des politiques

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Routage par flux

Étant donné que l'ASA effectue le routage par flux, le routage des politiques est appliqué sur le premier paquet et la décision de routage qui en résulte est stockée dans le flux créé pour le paquet. Tous les paquets suivants appartenant à la même connexion correspondent simplement à ce flux et sont acheminés de manière appropriée.

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.

Mise en grappe

- La mise en grappe est prise en charge.
- Dans un scénario de grappe, sans routes statiques ou dynamiques, et avec la commande ip-verify-reverse path activée, le trafic asymétrique peut être abandonné. Il est donc conseillé de désactiver ip-verify-reverse path.

Prise en charge d'IPv6

IPv6 est pris en charge.

Lignes directrices relatives à la surveillance des chemins d'accès

Voici les lignes directrices pour configurer la surveillance des chemins d'accès sur les interfaces :

- Les interfaces doivent avoir un nom d'interface.
- Les interfaces de gestion uniquement ne peuvent pas être configurées avec la surveillance des chemins d'accès. Pour configurer la surveillance des chemins d'accès, vous devez décocher la case **Dedicate this interface to management only** (Dédier cette interface à la gestion uniquement).
- La surveillance des chemins d'accès n'est pas prise en charge sur les périphériques en mode de système transparent ou de contexte multiple.

- Les types de surveillance automatique (auto, auto4 et auto6) ne sont pas pris en charge pour les interfaces de tunnel.
- La surveillance des chemins d'accès ne peut pas être configurée pour les interfaces suivantes :
  - BVI
  - Boucle avec retour
  - DVTI

Directives supplémentaires

- Toutes les restrictions et limites de configuration existantes liées aux cartes de routage seront conservées.
- N'utilisez pas de cartes de routage contenant des listes de correspondance de politiques pour le routage basé sur des politiques. La liste de politiques de correspondance est uniquement utilisée pour le BGP.
- 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.

Configurer le routage basé sur les politiques

Une carte de routage est composée d'une ou de plusieurs instructions route-map. Chaque instruction a un numéro de séquence, ainsi qu'une clause allow ou deny. Chaque instruction route-map contient des commandes match et set. La commande match indique les critères de correspondance à appliquer au paquet. La commande set indique l'action à entreprendre sur le paquet.

- Lorsqu'une carte de routage est configurée avec des clauses match/set IPv4 et IPv6 ou lorsqu'une ACL unifiée faisant correspondre le trafic IPv4 et IPv6 est utilisée, les actions définies seront appliquées en fonction de la version IP de destination.
- Lorsque plusieurs interfaces ou sauts suivants sont configurés en tant qu'action définie, toutes les options sont évaluées l'une après l'autre jusqu'à ce qu'une option utilisable valide soit trouvée. Aucun équilibrage de charge ne sera effectué parmi les multiples options configurées.
- L'option verify-availability n'est pas prise en charge en mode de contexte multiple.

Procédure

Étape 1 Dans ASDM, configurez une ou plusieurs ACL standard ou étendues pour identifier le trafic sur lequel vous souhaitez effectuer le routage basé sur les politiques. Voir **Configuration de** > **gestionnaire avancé d'ACL du** > **pare-feu** > .

Étape 2 Choisissez **Configuration** > **Device Setup (Configuration des périphériques)** > **Routing (routage)** > **Route Maps (carte de routage)**, et cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Route map** (Ajouter une carte de routage) apparaît.

Étape 3 Saisissez le nom et le numéro de séquence de la carte de routage. Vous utiliserez ce même nom pour des instructions de carte de routage supplémentaires facultatives. Le numéro de séquence est l'ordre dans lequel ASA évalue les cartes de routage.

Étape 4 Cliquez sur **Deny** (Refuser) ou **Allow** (Autoriser).

La liste de contrôle d'accès comprend également ses propres instructions d'autorisation et de refus. Pour les correspondances Autoriser/Autoriser entre la carte de routage et la liste de contrôle d'accès, le traitement de routage basé sur les politiques se poursuit. Pour les correspondances Autoriser/refuser, le traitement se termine pour cette carte de routage et les autres cartes de routage sont vérifiées. Si le résultat est toujours Autoriser/refuser, la table de routage normale est utilisée. Pour les correspondances refus/refus, le traitement de routage basé sur les politiques se poursuit.

Étape 5 Cliquez sur l'onglet **Map Clause** (Clause relative à la carte) pour identifier les listes de contrôle d'accès que vous avez créées.

Dans la section **IPv4**, choisissez **Access List** (liste d'accès) dans le menu déroulant, puis sélectionnez une ou plusieurs ACL standard ou étendues dans la boîte de dialogue.



Remarque Vérifiez que la liste d'accès ne contient aucune règle inactive. Vous ne pouvez pas définir une correspondance ACL avec les règles inactives sur un PBR.

Si vous utilisez une liste de contrôle d'accès standard, la mise en correspondance s'effectue uniquement pour l'adresse de destination. Si vous utilisez une liste de contrôle d'accès étendue, vous pouvez mettre en correspondance la source, la destination ou les deux.

Utilisez la section IPv4 pour les listes de contrôle d'accès IPv4 et IPv6. Pour la liste de contrôle d'accès étendue, vous pouvez spécifier les paramètres IPv4, IPv6, Identity Firewall ou Cisco TrustSec. Vous pouvez également inclure des objets de service réseau. Pour obtenir la syntaxe complète, consultez la référence de commande ASA.

Étape 6 Cliquez sur l'onglet **Policy Based Routing** (Routage basé sur des politiques) pour définir la politique à appliquer aux flux de trafic.

Cochez une ou plusieurs des actions suivantes à effectuer pour les flux de trafic correspondants :

- **Définir l'adresse IP de saut suivant PBR** : Pour IPv4 et IPv6, vous pouvez configurer plusieurs adresses IP de saut suivant, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une adresse IP de saut suivant routable soit trouvée. Les prochains sauts configurés doivent être connectés directement; Sinon, l'action définie ne sera pas appliquée.
- **Définir l'adresse IP du saut suivant par défaut :** pour IPv4 et IPv6, si la recherche normale de route échoue pour le trafic correspondant, l'ASA transfère le trafic en utilisant cette adresse IP de saut suivant spécifiée.
- **Trouver et définir de manière récursive l'adresse IP de saut suivant** : l'adresse de saut suivant et l'adresse de saut suivant par défaut exigent que le prochain saut se trouve sur un sous-réseau directement connecté. Avec cette option, l'adresse de saut suivant n'a pas besoin d'être connectée directement. Au lieu de cela, 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 routage en fonction du chemin de routage utilisé sur le routeur.
- **Configuration de la vérifiabilité du saut suivant** : vérifie si les prochains sauts IPv4 d'une carte de routage sont disponibles. Vous pouvez configurer un objet de suivi de moniteur SLA pour vérifier

l'accessibilité du prochain saut. Cliquez sur **Add** pour ajouter des entrées d'adresse IP du saut suivant et spécifiez les informations suivantes.

- **Numéro de séquence** : les entrées sont évaluées dans l'ordre à l'aide du numéro de séquence.
- **Adresse IP** : saisissez l'adresse IP.
- **ID d'objet de suivi** : saisissez un ID valide.

- **Définir les interfaces** : cette option configure l'interface par laquelle le trafic correspondant est acheminé. Vous pouvez configurer plusieurs interfaces, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une interface valide soit trouvée. Lorsque vous spécifiez **null0**, tout le trafic correspondant à la carte de routage sera abandonné. Il doit y avoir une voie de routage pour la destination qui peut être acheminée par l'interface spécifiée (statique ou dynamique).
- **Définir la clause** > **Coût de l'interface adaptative** : cette option se trouve dans l'onglet Set Clause (Définir a clause) plutôt que dans l'onglet **Policy Based Routing** (Routage basé sur une politique). Cette option définit l'interface de sortie en fonction de son coût. Cliquez dans le champ **Available Interfaces** (interfaces disponibles) et sélectionnez les interfaces à prendre en compte. L'interface de sortie est sélectionnée dans la liste des interfaces. Si les coûts des interfaces sont les mêmes, il s'agit d'une configuration active-active et les paquets sont équilibrés (round robin) sur les interfaces de sortie. Si les coûts sont différents, l'interface avec le coût le plus faible est sélectionnée. Les interfaces ne sont prises en compte que si elles sont actives.
- **Définir l'interface null0 comme interface par défaut** : si une recherche de route normale échoue, l'ASA transfère le trafic null0 et le trafic sera abandonné.
- **Définir le bit de non-fragmentation sur 1 ou 0**) : sélectionnez le bouton radio approprié.
- **Définir la valeur du point de code de service différentiel (DSCP) en bits de QoS** : sélectionnez une valeur dans la liste déroulante IPv4 ou IPv6.

Étape 7 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 8 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** (Configuration > Configuration du périphérique > paramètres de l'interface > Interfaces) et configurez les interfaces d'entrée qui doivent appliquer cette carte de routage pour déterminer les interfaces de sortie.

a) Sélectionnez une interface d'entrée , puis cliquez sur **Edit** Modifier).
b) Dans **Route Map**, sélectionnez la carte de routage basée sur les politiques qui doit être appliquée.
c) Si vous avez utilisé le **coût d'interface adaptatif** pour sélectionner l'interface de sortie dans la carte de routage, définissez la valeur du **coût** sur l'interface.

   La valeur peut être 1 à 65535. La valeur par défaut est 0, que vous pouvez réinitialiser en supprimant la valeur de ce champ. Plus le numéro de priorité est faible, plus la priorité est élevée. Par exemple, 1 a priorité sur 2.

d) Pour que PBR utilise des mesures flexibles pour identifier le meilleur chemin pour le routage des paquets, dans la liste déroulante **Path Monitoring** (surveillance des chemins), sélectionnez le type de surveillance approprié :

   - **auto** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface, si elle existe (identique à Auto IPv4). Sinon, envoie à la passerelle par défaut IPv6 de l'interface (identique à Auto IPv6).
   - **ipv4** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, le champ adjacent est activé. Saisissez l'adresse IPv4 dans le champ.

- **ipv6** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, le champ adjacent est activé. Saisissez l'adresse IPv4 dans le champ.
- **auto4** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface.
- **auto6** : envoie des sondes ICMP à la passerelle par défaut IPv6 de l'interface.
- **Aucune** : pour désactiver la surveillance des chemins pour l'interface.

e) Cliquez sur **OK**, puis sur **Apply**(appliquer).

Historique du routage basé sur des politiques

Tableau 1 : Historique des cartes de routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Indicateurs de supervision des chemins d'accès dans PBR.	9.18(1)	PBR utilise les mesures pour déterminer le meilleur chemin (interface de sortie) pour transférer le trafic. La supervision 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. Écrans nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage basé sur les politiques	9.4(1)	Le routage basé sur les politiques (PBR) est un mécanisme par lequel le trafic est acheminé par des chemins spécifiques avec une QoS spécifiée à l'aide d'ACL. Les ACL permettent de classer le trafic en fonction du contenu des en-têtes de couche 3 et de couche 4 du paquet. Cette solution permet aux administrateurs de fournir une QoS à un trafic différencié, de répartir le trafic interactif et par lots entre des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé, et permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies. Nous avons mis à jour les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Policy Based Routing (Routage basé sur les politiques), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Interface Settings (Paramètres d'interface) > Interfaces
Prise en charge d'IPv6 pour le routage basé sur les politiques	9.5(1)	Les adresses IPv6 sont désormais prises en charge pour le routage basé sur les politiques. Nous avons modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Map (Ajouter une carte de routage) > Policy Based Routing (Routage basé sur les politiques) Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Maps (Ajouter des cartes de routage) > Match Clause (Clause de correspondance)**
Prise en charge de VXLAN pour le routage basé sur les politiques	9.5(1)	Vous pouvez maintenant activer le routage basé sur les politiques sur une interface VNI. Nous avons modifié l'écran suivant : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage basé sur les politiques pour le pare-feu d'identité et Cisco TrustSec	9.5(1)	Vous pouvez configurer le pare-feu d'identité et Cisco TrustSec, puis utiliser les ACL du pare-feu d'identité et Cisco TrustSec dans les cartes de routage basées sur les politiques. Nous avons modifié l'écran suivant : **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > Route Maps (Cartes de routage) > Add Route Maps (Ajouter des cartes de routage) > Match Clause (Clause de correspondance)**

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.