Bases de routage et routes statiques

Le système utilise une table de routage pour déterminer l'interface de sortie des paquets qui entrent dans le système. Les rubriques suivantes expliquent les bases du routage et comment configurer le routage statique sur le périphérique.

Bonnes pratiques pour le routage

La conception des processus de routage dans un réseau peut être un processus complexe. Ce chapitre suppose que vous configurez le périphérique Cisco Firewall Threat Defense pour qu'il fonctionne dans un réseau existant et qu'il participe aux processus de routage que vous avez déjà établis dans ce réseau.

Si vous créez plutôt un nouveau réseau, prenez le temps de vous renseigner ailleurs sur les protocoles de routage et sur la façon de concevoir un plan de routage efficace adapté à votre réseau. Ce chapitre ne présente pas de recommandations pour le choix des protocoles et ne détaille pas non plus leur fonctionnement.

Si votre réseau est très petit et que vous vous connectez simplement à un fournisseur de services Internet, vous n'aurez peut-être besoin que de quelques routes statiques et vous n'aurez peut-être pas du tout besoin de mettre en œuvre des protocoles de routage.

Mais si vous configurez un grand réseau qui inclura de nombreux routeurs, vous devrez probablement mettre en œuvre au moins un protocole de routage pour le routage interne, comme OSPF, et possiblement un autre pour le routage externe, comme BGP. Votre fournisseur de services peut vous aider à comprendre quel routage externe pourrait être nécessaire, le cas échéant. S'il s'agit de votre situation, commencez par déterminer quels protocoles de routage vous pouvez configurer à l'aide de Cisco Firewall Threat Defense, puis planifiez votre réseau et, enfin, configurez le périphérique Cisco Firewall Threat Defense en fonction de ce plan.

Aperçu du routage

Les rubriques suivantes décrivent le comportement du routage dans le périphérique Cisco Firewall Threat Defense. Le routage est l'action de déplacer des informations sur un réseau d'une source à une destination. En cours de route, au moins un nœud intermédiaire est généralement rencontré. Le routage comporte deux activités de base : la détermination des chemins de routage optimaux et le transport de paquets dans un réseau.

Protocoles de routage pris en charge

Le tableau suivant explique les protocoles de routage et les technologies que vous pouvez configurer sur un périphérique Firewall Threat Defense à l'aide de Firepower Device Manager, ainsi que la méthode que vous devez utiliser pour terminer la configuration.

Tableau 1 : Protocoles de routage pris en charge

Fonctionnalités de routage	Méthode de configuration	Notes
BGP	Smart CLI	Configurez les objets d'interface de ligne de commande BGP à partir de la page **Device (Périphérique)** > **Routing (Routage).**. Configurez les objets utilisés dans BGP, tels que les cartes de routage, à l'aide d'objets Smart CLI à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
Détection de transfert bidirectionnel (BFD)	FlexConfig	Configurez BFD à l'aide d'objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**. BFD est pris en charge uniquement avec BGP.
EIGRP	Smart CLI	Configurez les objets d'interface de ligne de commande Smart EIGRP à partir de la page **Device (Périphérique)** > **Routing (Routage)**. Configurez les objets utilisés dans EIGRP, comme les route maps, à l'aide d'objets Smart CLI depuis la page**Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
IS-IS	FlexConfig	Configurez IS-IS à l'aide d'objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
Routage multidiffusion	FlexConfig	Configurez le routage multidiffusion à l'aide d'objets FlexConfig depuis la page**Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
OSPFv2	Smart CLI	Configurez les objets Smart CLI OSPFv2 à partir de la page **Device (Périphérique)** > **Routing (Routage)**. Configurez les objets utilisés dans OSPFv2, comme les route maps, à l'aide d'objets Smart CLI depuis la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
OSPFv3	—	La configuration OSPFv3 n'est pas prise en charge.
Routage à base de règles (PBR)	FlexConfig	Configurez le routage à base de règles (PBR) à l'aide d'objets FlexConfig depuis la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Fonctionnalités de routage	Méthode de configuration	Notes
RIP	FlexConfig	Configurez le protocole RIP à l'aide des objets FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
du routage statique;	Firewall Device Manager	Configurez les routes statiques globalement ou par routeur virtuel à partir de la page **Device (Périphérique)** > **Routing (Routage)**.
Routeurs virtuels, VRF	Firewall Device Manager	Configurez les routeurs virtuels à partir de la page **Device (Périphérique)** > **Routing (Routage).**.

Types de route

Il existe deux types principaux de routage : statique ou dynamique.

Les routes statiques sont celles que vous définissez explicitement. Il s'agit de routes stables, normalement de priorité élevée, que vous utiliseriez pour vous assurer que le trafic vers la destination de route est toujours envoyé par la bonne interface. Par exemple, vous créeriez une route statique par défaut pour couvrir tout le trafic qui n'est déjà couvert par aucune autre route, c'est-à-dire 0.0.0.0/0 pour IPv4 ou ::/0 pour IPv6. Un autre exemple serait une route statique vers un serveur syslog interne que vous souhaitez toujours utiliser.

Les routes dynamiques sont celles apprises par l'application d'un protocole de routage, tel que OSPF, BGP, EIGRP, IS-IS ou RIP. Vous ne définissez pas les routes directement. Au lieu de cela, vous configurez le protocole de routage, et le système communique ensuite avec les routeurs voisins, en leur transmettant les mises à jour de routage et en recevant les mises à jour de routage.

Les protocoles de routage dynamique ajustent la table de routage aux circonstances changeantes du réseau en analysant les messages de mise à jour de routage entrants. Si le message indique qu'un changement de réseau est survenu, le système recalcule les routes et envoie de nouveaux messages de mise à jour de routage. Ces messages pénètrent dans le réseau, incitant les routeurs à réexécuter leurs algorithmes et à modifier leurs tables de routage en conséquence.

Le routage statique est simple et sert le routage de base. Il fonctionne bien dans des environnements où le trafic réseau est relativement prévisible et où la conception de réseau est relativement simple. Cependant, comme les routes statiques ne peuvent pas changer à moins que vous ne les modifiez, elles ne peuvent pas réagir aux modifications dans le réseau.

Sauf si vous avez un petit réseau, vous combinez généralement des routes statiques avec un ou plusieurs protocoles de routage dynamique. Vous définissez au moins une route statique, comme route par défaut pour tout trafic qui ne correspond pas à une route explicite.

Remarque Vous pouvez utiliser l'interface de ligne de commande Smart pour configurer les protocoles de routage suivants : OSPF, BGP. Utilisez FlexConfig pour configurer d'autres protocoles de routage pris en charge dans le logiciel ASA.

La table de routage et la sélection de route

Lorsque les traductions (xlates) et les règles NAT ne déterminent pas l'interface de sortie, le système utilise la table de routage pour déterminer le chemin d'un paquet.

Les routes dans la table de routage comprennent une métrique appelée « distance administrative » qui fournit une priorité relative à une route donnée. Si un paquet correspond à plus d'une entrée de route, celle ayant la distance la plus faible est utilisée. Les réseaux directement connectés (ceux définis sur une interface) ont la distance 0, ils sont donc toujours privilégiés. Les routes statiques ont une distance par défaut de 1, mais vous pouvez les créer avec n'importe quelle distance comprise entre 1 et 254.

Les routes qui identifient une destination spécifique prévalent sur la route par défaut (la route dont la destination est 0.0.0.0/0 ou ::/0).

Mode de remplissage de la table de routage

La table de routage Firewall Threat Defense peut être remplie par des routes définies de manière statique, des routes connectées directement et des routes découvertes par les protocoles de routage dynamique. Comme le périphérique Firewall Threat Defense peut exécuter plusieurs protocoles de routage en plus d'avoir des routes statiques et connectées dans la table de routage, il est possible qu'une même route soit découverte ou saisie de plusieurs manières. Lorsque deux routes vers la même destination sont mises dans la table de routage, celle qui reste dans la table de routage est déterminée comme suit :

- Si les deux routes ont des longueurs de préfixe de réseau différentes (masques de réseau), les deux routes sont considérées comme uniques et sont entrées dans la table de routage. La logique de transfert de paquets détermine ensuite laquelle des deux utiliser.

  Par exemple, si les processus RIP et OSPF ont découvert les routes suivantes :

  - RIP : 192.168.32.0/24
  - OSPF : 192.168.32.0/19

  Même si les routes OSPF ont la meilleure distance administrative, les deux routes sont installées dans la table de routage, car chacune de ces routes a une longueur de préfixe différente (masque de sous-réseau). Ce sont des destinations considérées comme différentes et la logique de transfert de paquets détermine la route à utiliser.

- Si le périphérique Firewall Threat Defense connaît plusieurs chemins vers la même destination à partir d'un protocole de routage unique, comme RIP, la voie de routage avec la meilleure mesure (déterminée par le protocole de routage) est entrée dans la table de routage.

  Les métriques sont des valeurs associées à des routes spécifiques, de la plus préférée à la moins préférée. Les paramètres utilisés pour déterminer les métriques varient selon le protocole de routage. Le chemin avec la mesure la plus basse est sélectionné comme chemin optimale et installé dans la table de routage. S'il existe plusieurs chemins vers la même destination avec des métriques égales, l'équilibrage de la charge est effectué sur ces chemins de coût égal.

- Si le périphérique Firewall Threat Defense connaît une destination à partir de plus d'un protocole de routage, les distance administratives des routages sont comparées et les routes avec une distance administrative inférieure sont entrées dans la table de routage.

Distances administratives pour les routages

Vous pouvez modifier les distance administratives pour les routages détectés ou redistribués dans un protocole de routage. Si deux routes de deux protocoles de routage différents ont la même distance administrative, la route avec la distance administrative *par défaut* la plus faible est entrée dans la table de routage. Dans le cas des routes EIGRP et OSPF, si la route EIGRP et la route OSPF ont la même distance administrative, la route EIGRP est choisie par défaut.

La distance administrative est un paramètre de routage que Firewall Threat Defense utilise pour sélectionner le meilleur chemin lorsqu'il existe deux ou plusieurs itinéraires différents vers la même destination à partir de deux protocoles de routage différents. Puisque les protocoles de routage ont des mesures basées sur des algorithmes différents des autres protocoles, il n'est pas toujours possible de déterminer le meilleur chemin pour deux routages vers la même destination qui ont été générées par différents protocoles de routage.

Chaque protocole de routage est priorisé à l'aide d'une valeur de distance administrative. Le tableau suivant présente les valeurs de distance administrative par défaut pour les protocoles de routage pris en charge par Firewall Threat Defense .

Tableau 2 : Distance administrative par défaut pour les protocoles de routage pris en charge

Source de la route	Distance administrative par défaut
Interface connectée	0
Routage VPN	1
Routage statique	1
Routage résumé EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
Routage EIGRP externe	170
BGP interne et local	200
Inconnu	255

Plus la valeur de la distance administrative est faible, plus la préférence est donnée au protocole. Par exemple, si Le Firewall Threat Defense reçoit une voie de routage vers un certain réseau d'un processus de routage OSPF (distance administrative par défaut - 110) et d'un processus de routage RIP (distance administrative par défaut - 120), le Firewall Threat Defense choisit la voie de routage OSPF, car OSPF a une préférence plus élevée. Dans ce cas, le routeur ajoute la version OSPF de la route à la table de routage.

Une route VPN annoncée (V-Route/RRI) équivaut à une route statique avec la distance administrative par défaut de 1. Mais elle comporte une préférence plus élevée, comme avec le masque de réseau 255.255.255.255.

Dans cet exemple, si la source de routage dérivée OSPF était perdue (par exemple, en raison d'une coupure de courant), le Firewall Threat Defense utiliserait alors le routage dérivé RIP jusqu'à ce que le routage dérivé OSPF réapparaisse.

La distance administrative est un paramètre local. Par exemple, si vous modifiez la distance administrative des routages obtenus par OSPF, cette modification n'affectera que la table de routage du Firewall Threat Defense pour lequel la commande a été saisie. La distance administrative n'est pas annoncée dans les mises à jour de routage.

La distance administrative n'affecte pas le processus de routage. Les processus de routage n'annoncent que les routages détectés par le processus de routage ou redistribués dans le processus de routage. Par exemple, le processus de routage RIP annonce les routes RIP, même si les routes découvertes par le processus de routage OSPF sont utilisées dans la table de routage.

Sauvegarde des routes dynamiques et statiques flottantes

Une route de secours est enregistrée lorsque la tentative initiale d'installation de la route dans la table de routage échoue parce qu'une autre route a été installée à la place. Si la voie de routage qui a été installée dans la table de routage échoue, le processus de maintenance de la table de routage appelle chaque processus de protocole de routage qui a enregistré une voie de routage de secours et lui demande de réinstaller la voie de routage dans la table de routage. S'il existe plusieurs protocoles avec des routes de secours enregistrées pour la voie de routage ayant échoué, la voie de routage préférée est choisie en fonction de la distance administrative.

Grâce à ce processus, vous pouvez créer des routes statiques flottantes qui sont installées dans la table de routage lorsque la route découverte par un protocole de routage dynamique échoue. Une voie de routage statique flottante est tout simplement une voie de routage statique configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique s'exécutant sur Firewall Threat Defense . Lorsque la voie de routage correspondante découverte par un processus de routage dynamique échoue, la voie de routage statique est installée dans la table de routage.

Prise des décisions de transfert

Les décisions de transfert sont prises comme suit :

- Si la destination ne correspond à aucune entrée de la table de routage, le paquet est acheminé par l'intermédiaire de l'interface spécifiée pour la voie de routage par défaut. Si une voie de routage par défaut n'a pas été configurée, le paquet est rejeté.
- Si la destination correspond à une seule entrée dans la table de routage, le paquet est acheminé par l'interface associée à cette voie de routage.
- Si la destination correspond à plus d'une entrée dans la table de routage, le paquet est transféré hors de l'interface associée à la voie de routage qui a la plus grande longueur de préfixe de réseau.

Par exemple, un paquet destiné à 192.168.32.1 arrive sur une interface avec les routes suivantes dans la table de routage :

- Passerelle 192.168.32.0/24 10.1.1.2
- Passerelle 192.168.32.0/19 10.1.1.3

Dans ce cas, un paquet destiné à 192.168.32.1 est dirigé vers 10.1.1.2, car 192.168.32.1 fait partie du réseau 192.168.32.0/24. Il fait également partie de l'autre voie de routage dans la table de routage, mais 192.168.32.0/24 a le préfixe le plus long dans la table de routage (24 bits vers 19 bits). Les préfixes les plus longs sont toujours préférables aux plus courts lors du transfert d'un paquet.

Remarque Les connexions existantes continuent d'utiliser leurs interfaces établies même si une nouvelle connexion similaire entraînerait un comportement différent en raison d'une modification des routages.

Table de routage pour le trafic de gestion

En tant que pratique de sécurité courante, il est souvent nécessaire de séparer et d'isoler le trafic de gestion (provenant du périphérique) du trafic de données. Pour réaliser cet isolement, le périphérique Firewall Threat Defense utilise une table de routage distincte pour le trafic de gestion uniquement par rapport au trafic de données. Des tableaux de routage distincts signifient que vous pouvez créer des routages par défaut distincts pour les données et la gestion.

Types de trafic pour chaque table de routage

Le trafic de l'appareil utilise toujours la table de routage des données.

Le trafic en provenance du périphérique, selon le type, utilise par défaut la table de tourage réservé à la gestion ou la table de routage des données. Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

- Le trafic du tableau de gestion uniquement en provenance du périphérique comprend les communications du serveur AAA.
- Le trafic du tableau de données du périphérique comprend les recherches de serveur DNS et le DDNS. Une exception est que si vous spécifiez uniquement l'interface de diagnostic pour DNS, le périphérique Firewall Threat Defense utilisera uniquement le tableau de gestion uniquement.

Interfaces incluses dans la table de routage de gestion uniquement

Les interfaces de gestion uniquement comprennent toutes les interfaces x/x Management (gestion) ainsi que toutes les interfaces que vous avez configurées pour être uniquement de gestion.

Remarque L'interface virtuelle de gestion utilise sa propre table de routage Linux qui ne fait pas partie de la recherche de routage Firewall Threat Defense. Le trafic provenant de l'interface de gestion comprend les sessions de gestion Firepower Device Manager, la communication des licences et les mises à niveau de la base de données. L'interface logique de diagnostic, quant à elle, utilise la table de routage de gestion uniquement décrite dans cette section.

Repli vers l'autre table de routage

Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

Utilisation de la table de routage autre que par défaut

Si vous avez besoin que le trafic initial sorte d'une interface qui ne figure pas dans sa table de routage par défaut, vous devrez peut-être spécifier cette interface lorsque vous la configurerez, plutôt que de vous fier à l'autre table. Le Firewall Threat Defense vérifiera uniquement les routes pour l'interface spécifiée. Par exemple, si vous devez communiquer avec un serveur RADIUS sur une interface de données, spécifiez cette interface dans la configuration RADIUS. Sinon, s'il existe une route par défaut dans la table de routage de gestion uniquement, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage des données.

Routage à chemins multiples à coûts égaux (ECMP).

Le Firewall Threat Defense prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

ECMP sur plusieurs interfaces à l'aide de zones de trafic

Si vous configurez des zones de trafic pour contenir un groupe d'interfaces, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au sein de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. Le Firewall Threat Defense équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, le périphérique déplace le flux de manière transparente vers une autre route.

Routes statiques

Vous pouvez créer des routes statiques pour fournir un routage de base à votre réseau.

À propos des routages statiques et par défaut

Pour acheminer le trafic vers un hôte ou un réseau non connecté, vous devez définir une voie de routage vers l'hôte ou le réseau, à l'aide du routage statique ou dynamique. En général, vous devez configurer au moins une route statique : une route par défaut pour tout le trafic qui n'est pas acheminé par d'autres moyens vers une passerelle de réseau par défaut, en général le routeur du saut suivant.

Routage par défaut

L'option la plus simple est de configurer une voie de routage statique par défaut pour envoyer tout le trafic vers un routeur en amont, en se fondant sur le routeur pour acheminer le trafic à votre place. Une voie de routage par défaut identifie l'adresse IP de la passerelle à laquelle Firewall Threat Defense envoie tous les paquets IP pour lesquels il n'a pas de voie de routage statique ou apprise. Une voie de routage statique par défaut est simplement une voie de routage statique avec 0.0.0.0/0 (IPv4) ou::/0 (IPv6) comme adresse IP de destination.

Vous devez toujours définir une voie de routage par défaut.

Comme le périphérique Firewall Threat Defense utilise des tables de routage distinctes pour le trafic de données et le trafic de gestion, vous pouvez éventuellement configurer une voie de routage par défaut pour le trafic de données et une autre voie de routage par défaut pour le trafic de gestion. Notez que le trafic provenant du périphérique utilise par défaut la table de routage de gestion uniquement ou de données, en fonction du type, mais qu'il revient à l'autre table de routage si aucune route n'est trouvée. Les routes par défaut correspondront toujours au trafic et empêcheront un recours à l'autre table de routage. Dans ce cas, vous devez préciser l'interface que vous souhaitez utiliser pour le trafic de sortie si cette interface ne figure pas dans la table de routage par défaut. L'interface de dépistage est incluse dans le tableau des valeurs de gestion uniquement. L'interface de gestion spéciale utilise une table de routage Linux distincte et possède sa propre voie de routage par défaut.

Routes statiques

Vous pourriez souhaiter utiliser des routes statiques dans les cas suivants :

- Vos réseaux utilisent un protocole de découverte de routeur non pris en charge.
- Votre réseau est de petite taille et vous pouvez facilement gérer des routes statiques.
- Vous ne voulez pas associer le trafic ou la surcharge de la CPU aux protocoles de routage.
- Dans certains cas, une route par défaut ne suffit pas. La passerelle par défaut peut ne pas être en mesure d'atteindre le réseau de destination, vous devez donc également configurer des routes statiques plus spécifiques. Par exemple, si la passerelle par défaut est externe, la voie de routage par défaut ne peut pas diriger le trafic vers des réseaux internes qui ne sont pas directement connectés à Firewall Threat Defense .
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.

Routes statiques de sauvegarde et suivi de routage statique

L'un des problèmes des routes statiques est qu'il n'y a pas de mécanisme inhérent pour déterminer si la route est active ou inactive. Les routes statiques restent dans la table de routage même si la passerelle du saut suivant n'est plus disponible. Les routes statiques ne sont supprimées de la table de routage que si l'interface associée tombe en panne.

En mettant en œuvre le suivi de routage, à l'aide d'un moniteur de contrat de niveau de service (SLA), vous pouvez suivre la disponibilité d'un routage statique et installer automatiquement un routage de secours en cas de défaillance du routage principal. Par exemple, vous pouvez définir une route par défaut vers une passerelle de FAI et une route de secours par défaut vers un FAI secondaire au cas où le FAI principal deviendrait indisponible.

Lorsque vous utilisez le suivi de routage, vous associez une adresse IP cible sur le réseau de destination au routage suivi. Le système utilise ensuite les requêtes d'écho ICMP pour vérifier périodiquement que l'adresse est accessible. Si le système ne reçoit pas de réponse d'écho dans le délai que vous spécifiez, l'hôte est estimé comme inaccessible et le système supprime la route associée de la table de routage. Le système peut alors utiliser une route de secours non suivie avec une mesure plus élevée à la place de la route supprimée.

Ainsi, pour utiliser une route statique de secours pour une destination donnée, y compris pour une route par défaut, vous devez procéder comme suit :

1. Créez un moniteur SLA qui surveillera une adresse IP fiable sur le réseau de destination, comme une passerelle ou un serveur permanent (comme un serveur Web ou un serveur Syslog). Ne surveillez pas l'adresse IP d'un système qui pourrait être mis hors ligne alors que le réseau de destination reste sain et disponible. Consultez Configurer les objets du moniteur SLA, à la page 12.

2. Créez la route principale vers la destination et sélectionnez le moniteur SLA pour la route. La métrique pour cette route doit généralement être 1. Consultez Configuration des routes statiques, à la page 11.
3. Créez la route statique de secours qui sera utilisée en cas de défaillance de la route principale. Cette route doit avoir une métrique plus grande que la route principale. Par exemple, si la route principale est 1, la route de secours pourrait être 10. Vous devez également normalement sélectionner une interface différente pour la route de secours.

Lignes directrices relatives au routage statique

Groupes de ponts

- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l'interface membre.
- Pour le trafic qui provient du Firewall Threat Defense (comme syslog ou SNMP) et qui doit traverser une interface membre d'un groupe de ponts vers un réseau non directement connecté, vous devez configurer soit une route par défaut, soit des routes statiques, afin que le Firewall Threat Defense sache par quelle interface membre du groupe de ponts envoyer le trafic. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques.
- Le suivi de routage statique n'est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

IPv6

- Le suivi de routage statique (surveillance SLA) n'est pas pris en charge pour IPv6.

Zones de trafic à chemins multiples (ECMP) à coût égal

- Conservez les interfaces membres d'une zone de trafic ECMP dans la même zone de sécurité pour éviter que différentes critères d'accès, SSL ou d'identité ne soient appliquées à ces interfaces.
- Vous pouvez avoir jusqu'à 8 routes à coût égal pour un réseau dans une zone de trafic ECMP donnée.
- Vous pouvez créer jusqu'à 256 zones de trafic ECMP, avec jusqu'à 8 interfaces par zone.
- Les zones de trafic ECMP peuvent contenir des interfaces physiques, des sous-interfaces et des EtherChannels nommés. Elles ne peuvent pas contenir les éléments suivants :
  - Un groupe de ponts (BVI) ou ses membres
  - Interfaces membre EtherChannel
  - Interfaces HA (basculement ou liaisons d'état)
  - Interfaces de gestion uniquement
  - Interfaces utilisées pour les connexions VPN de site à site ou VPN d'accès à distance.
  - Interfaces de tunnel virtuel (VTI) ou leurs interfaces source.
  - Interfaces configurées pour l'accès de gestion VPN.

- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone.

Configuration des routes statiques

Définissez des routes statiques pour indiquer au système où envoyer les paquets qui ne sont pas liés aux réseaux directement connectés aux interfaces du système.

Vous avez besoin d'au moins une route statique, la route par défaut, pour le réseau 0.0.0.0/0. Cette route définit où envoyer les paquets dont l'interface de sortie ne peut pas être déterminée par les xlates NAT existants (traductions) ou les règles NAT statiques, ou d'autres routage statiques.

Vous pourriez avoir besoin d'autres routages statiques si la passerelle par défaut ne peut pas être utilisée pour accéder à tous les réseaux. Par exemple, le routeur par défaut est généralement un routeur en amont sur l'interface externe. S'il existe d'autres réseaux internes qui ne sont pas directement connectés au périphérique et qu'ils ne sont pas accessibles au moyen de la passerelle par défaut, vous avez besoin de routages statiques pour chacun de ces réseaux internes.

Vous ne pouvez pas définir de routages statique pour les réseaux qui sont directement connectés aux interfaces du système. Le système crée automatiquement ces routes.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur le lien dans le sommaire de **Routing (routage)**.

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez une route statique.

Étape 3 Sur la page de **routage statique**, effectuez l'une des opérations suivantes :

- Pour ajouter une nouvelle route, cliquez sur **+**.
- Cliquez sur l'icône de modification ( ) de la route que vous souhaitez modifier.

Si vous n'avez plus besoin d'un routage, cliquez sur l'icône de la corbeille pour le supprimer.

Étape 4 Configurer les propriétés du routage

- **Name (nom)** : nom d'affichage du routage.
- **Description** : une description facultative de l'objectif du routage.
- **Interface** : sélectionnez l'interface par laquelle vous souhaitez envoyer le trafic. L'adresse de la passerelle doit être accessible au moyen de cette interface.

  Pour les groupes de pontage, vous configurez la route pour l'interface de groupe de pontage (BVI), pas pour les interfaces membres.

  Si vous avez activé le routage et le transfert virtuels, vous pouvez sélectionner une interface qui appartient à un autre routeur virtuel. Si vous créez un routage statique dans un routeur virtuel pour une interface dans un routeur virtuel différent, la route franchira les limites du routeur virtuel, avec le risque que le trafic de ce routeur virtuel se répande dans un autre routeur virtuel. Cela peut être le résultat souhaité, mais déterminez avec soin que vous avez besoin de cette fuite de routage. Lorsque vous sélectionnez des interfaces, le nom du routeur virtuel auquel appartient l'interface s'affiche à droite de l'interface.
- **Protocol (Protocole)**— Sélectionnez si la route est pour une adresse **IPv4** or **IPv6** address.

- **Networks (réseaux)** : sélectionnez les objets réseau qui identifient les réseaux de destination ou les hôtes qui doivent utiliser la passerelle dans ce routage.

  Pour définir une route par défaut, utilisez les objets réseau prédéfinis any-ipv4 ou any-ipv6, ou créez un objet pour le réseau 0.0.0.0/0 (IPv4) ou ::/0 (IPv6).

- **Passerelle** : sélectionnez l'objet réseau hôte qui identifie l'adresse IP de la passerelle. Le trafic est envoyé à cette adresse. Vous ne pouvez pas utiliser la même passerelle pour les routages sur plusieurs interfaces.

  Si vous définissez un routage dans un routeur virtuel et que l'interface appartient à un autre routeur virtuel, vous devez laisser la passerelle vide. Le système acheminera le trafic vers ces réseaux vers l'autre routeur virtuel, puis utilisera la table de routage du routeur virtuel cible pour déterminer la passerelle.

- **Métrique** : la distance administrative pour la route, entre 1 et 254. La valeur par défaut pour les routes statiques est 1. S'il y a des routeurs supplémentaires entre l'interface et la passerelle, saisissez le nombre de sauts comme distance administrative.

  La distance administrative est un paramètre utilisé pour comparer les routages. Plus le nombre est bas, plus la priorité est donnée au routage. Les routages connectés (réseaux directement connectés à une interface sur le périphérique) ont toujours la priorité sur les routages statiques.

Étape 5 (Facultatif; routages IPv4 uniquement.) Sélectionnez le **moniteur SLA** qui doit suivre la viabilité de ce routage.

Un moniteur SLA peut vérifier qu'un hôte toujours disponible sur le réseau cible est accessible. S'il devient inaccessible, le système peut installer un routage de secours. Par conséquent, si vous configurez un moniteur SLA, vous devez également configurer un autre routage statique, avec une mesure plus importante, pour ce réseau. Par exemple, si ce routage a la métrique 1, créez un routage de secours avec la métrique 10. Pour en savoir plus, consultez Routes statiques de sauvegarde et suivi de routage statique, à la page 9.

Si l'objet SLA Monitor n'existe pas encore, cliquez sur le lien **Create SLA Monitor (créez un moniteur SLA)** en bas de la liste et créez-le maintenant.

Remarque
Si un routage surveillé est supprimé parce que l'adresse surveillée ne peut pas faire l'objet d'un ping, le routage est indiqué dans la table de routage statique avec un avertissement indiquant que la route est inaccessible. Déterminez si le problème est temporaire ou si vous devez reconfigurer le routage. Envisagez la possibilité que le routage soit viable, mais que l'adresse surveillée ne soit pas suffisamment fiable.

Étape 6 Cliquez sur **OK**.

Configurer les objets du moniteur SLA

Configurer les objets du moniteur de contrat par niveau de service (SLA) pour une utilisation avec des routes statiques. À l'aide d'un moniteur SLA, vous pouvez suivre l'intégrité d'un routage statique et remplacer automatiquement un routage défaillant par un nouveau. pour obtenir plus de renseignements sur le suivi de routage, consultez Routes statiques de sauvegarde et suivi de routage statique, à la page 9.

Lorsque vous sélectionnez une cible de surveillance, vous devez vous assurer qu'elle peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quelle adresse IP, définie dans un objet réseau hôte, mais vous devriez envisager d'utiliser les éléments suivants :

- L'adresse de la passerelle du FAI, pour la prise en charge du double FAI.
- L'adresse de passerelle du saut suivant, si vous êtes préoccupé par la disponibilité de la passerelle.

- Serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel le système doit communiquer.
- Une adresse IP persistante sur le réseau de destination. Un poste de travail qui peut être fermé la nuit n'est pas un bon choix.

Procédure

Étape 1 Select **Objects (objets)**, then select **SLA Monitors** from the table of contents.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Définissez les options requises pour le moniteur SLA :

- **Monitor Address (adresse de surveillance)** : sélectionnez l'objet réseau hôte qui définit l'adresse à surveiller sur le réseau de destination. Vous pouvez cliquer sur **Create New Network (créer un nouveau réseau)** si l'objet dont vous avez besoin n'existe pas.

  Cette adresse est surveillée uniquement si vous connectez le moniteur SLA à une route statique.

- **Target interface interface cible)** : sélectionnez l'interface par laquelle envoyer les paquets de demande d'écho. Il s'agit normalement de l'interface sur laquelle vous allez définir la route statique. L'adresse source de l'interface est utilisée comme adresse source dans les paquets de demande d'écho.

Étape 5 (Facultatif) Ajustez les **options d'écho IP ICMP**.

Toutes les options ICMP ont des valeurs par défaut qui sont appropriées dans la plupart des cas, mais vous pouvez les régler en fonction de vos besoins.

- **Threshold (Seuil)** : le nombre de millisecondes pour qu'un seuil croissant soit déclaré, de 0 à 2147483647. La valeur par défaut est 5000 (5 secondes). Cette valeur ne doit pas être supérieure à la valeur définie pour le délai d'expiration. La valeur de seuil est uniquement utilisée pour indiquer les événements de dépassement de seuil, qui ne touchent pas l'accessibilité. Vous pouvez utiliser la fréquence des événements de seuil pour évaluer le paramètre de délai d'expiration.
- **Timeout (délai d'expiration)** : le temps, en millisecondes, pendant lequel l'opération de surveillance du routage doit attendre une réponse des paquets de demande, est compris entre 0 et 60 480 000 millisecondes (7 jours). La valeur par défaut est de 5 000 millisecondes (5 secondes). Si le moniteur ne reçoit pas de réponse à au moins une demande d'écho pendant cette période, le processus installe la route de secours.
- **Frequency (fréquence)** : le nombre de millisecondes entre les sondes SLA, de 1 000 à 60 480 000, en multiples de 1 000. Vous ne pouvez pas définir une fréquence inférieure à la valeur du délai d'expiration. La valeur par défaut est de 60 000 millisecondes (60 secondes).
- **Type of Service (type de service)** : un entier qui définit le type de service (toS) dans l'en-tête IP du paquet de requête d'écho ICMP, de 0 à 255. La valeur par défaut est 0.

- **Number of Packets (nombre de paquets)** : nombre de paquets à envoyer avec chaque interrogation, de 1 à 100. La valeur par défaut est 1 paquet.
- **Data Size (taille des données)** : taille de la charge utile de données à utiliser dans les paquets de demande d'écho, de 0 à 16 384 octets. La valeur par défaut est 28. Ce paramètre spécifie la taille de la charge utile uniquement; il ne spécifie pas la taille du paquet entier.

Étape 6 Cliquez sur **OK**.

Vous pouvez désormais utiliser l'objet moniteur SLA dans une route statique.

Configuration des zones de trafic ECMP

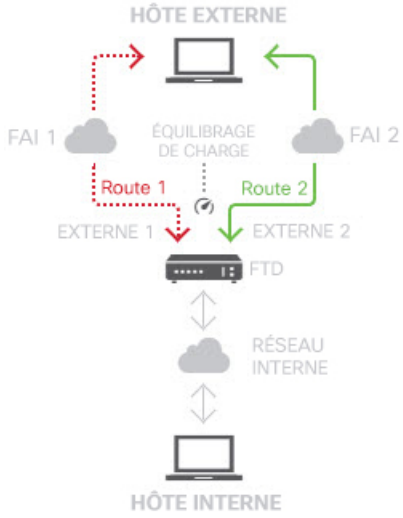
Normalement, pour configurer plusieurs routes pour un préfixe réseau donné, avec la même métrique de routage, vous devez configurer les routes sur la même interface. Ainsi, le système utilise le routage ECMP (Equal-Cost Multi-Path) pour équilibrer la charge du trafic envoyé par l'interface vers les passerelles.

Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles, et cette configuration est autorisée sans modifications supplémentaires.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

Vous pouvez également utiliser ECMP pour équilibrer le trafic sur plusieurs interfaces (au sein d'un routeur virtuel) pour le même préfixe de réseau et la même métrique de routage. Cette configuration est nécessaire si les passerelles sont accessibles par des interfaces distinctes. Par exemple, si vous avez deux fournisseurs de services Internet et que vous souhaitez équilibrer la charge entre eux, sans diviser vos espaces d'adresses internes entre les passerelles ISP. Un fournisseur de services Internet est accessible par l'interface outside1 et l'autre par l'interface outside2. Pour ce faire, vous devez créer une zone de trafic de routage qui contient les interfaces outside1 et outside2.

```
isp-zone containing outside1 and outside2
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.1.1.3
```



Remarque Une zone de trafic de routage ECMP n'est pas liée aux zones de sécurité. La création d'une zone de sécurité qui contient les interfaces outside1 et outside2 ne met pas en œuvre une zone de trafic à des fins de routage ECMP.

La procédure suivante explique comment configurer les zones ECMP pour profiter du traitement ECMP sur l'ensemble des interfaces.

Procédure

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

Étape 2 Si vous avez activé les routeurs virtuels, cliquez sur l'icône d'affichage ( ) pour le routeur dans lequel vous configurez une route statique.

Étape 3 Cliquez sur l'onglet **ECMP Traffic Zones** (Zones de trafic ECMP).

Étape 4 Sur la page **ECMP Traffic Zones** (Zones de trafic ECMP), effectuez l'une des opérations suivantes :

- Pour ajouter une nouvelle zone, cliquez sur **+**, ou **Add ECMP Traffic Zone** (Ajouter une zone de trafic ECMP).
- Cliquez sur l'icône de modification ( ) de la zone que vous souhaitez modifier.

Si vous n'avez plus besoin d'une zone, cliquez sur l'icône de la corbeille pour la supprimer. Vous devez supprimer toutes les routes statiques qui dépendent d'une zone avant de pouvoir supprimer la zone.

Étape 5 Entrez un **Name** (Nom) pour la zone et, facultativement, une description.

Étape 6 Sélectionnez jusqu'à 8 **Interfaces** à inclure dans la zone :

- Cliquez sur **+** pour ajouter une interface.
- Cliquez sur **x** à droite d'une interface pour la supprimer.

Lors de la sélection des interfaces, gardez les restrictions suivantes à l'esprit :

- Vous pouvez sélectionner des interfaces physiques, des sous-interfaces et des canaux EtherChannel.
- Une zone de trafic ECMP ne peut pas inclure les types d'interfaces suivants : un groupe de ponts (BVI) ou ses membres, des interfaces membres EtherChannel, des interfaces de haute disponibilité (basculement ou liens d'état), des interfaces réservées à la gestion, ou des interfaces configurées pour accéder à la gestion du VPN.
- Vous ne pouvez pas inclure d'interfaces utilisées dans des connexions VPN d'accès à distance ou de site à site.
- Vous ne pouvez pas sélectionner d'interfaces activées pour le relais DHCP, que ce soit comme serveur ou comme agent.
- Les interfaces doivent être attribuées au même routeur virtuel.
- Une interface ne peut se trouver que dans une seule zone de trafic.

Étape 7 Cliquez sur **OK**.

Prochaine étape

Vous pouvez maintenant accéder à l'onglet Static Routes (Routes statiques) et créer des routes à coût égal par l'intermédiaire de ces interfaces pour la même destination. Sinon, vos protocoles de routage dynamique peuvent configurer automatiquement des routes à coût égal si elles sont distribuées dans le système.

Surveillance du routage

Pour surveiller et dépanner le routage, 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 route** affiche la table de routage des interfaces de données, y compris les routes pour les réseaux directement connectés.
- **show ipv6 route** affiche la table de routage IPv6 pour les interfaces de données, y compris les routes pour les réseaux directement connectés.
- **show network** affiche la configuration de l'interface de gestion virtuelle , y compris la passerelle de gestion. Le routage via l'interface de gestion virtuelle n'est pas géré par la table de routage de l'interface de données, sauf si vous spécifiez des interfaces de données comme passerelle de gestion.
- **show network-static-routes** affiche les routes statiques configurées pour l'interface de gestion virtuelle à l'aide de la commande **configure network static-routes** . Normalement, il n'y aura pas de routes statiques, car la passerelle de gestion est suffisante pour le routage de gestion dans la plupart des cas. Ces routes ne sont pas disponibles pour le trafic sur les interfaces de données. Cette commande n'est pas disponible dans la console d'interface de ligne de commande.
- **show ospf** affiche des informations sur les processus OSPF et les routes apprises. Utilisez **show ospf ?** pour obtenir la liste des options que vous pouvez inclure afin d'afficher des informations précises sur OSPF.

- **show bgp** affiche des informations sur les processus BGP et les routes apprises. Utilisez **show bgp ?** pour obtenir une liste d'options que vous pouvez inclure pour afficher des informations spécifiques sur BGP.
- **show eigrp** *option* affiche des informations sur les processus EIGRP et les routes apprises. Utilisez **show eigrp ?** pour obtenir une liste d'options que vous pouvez inclure ; vous devez fournir une option.
- **show isis** *option* affiche des informations sur les processus IS-IS et les routes apprises. Utilisez **show isis ?** pour obtenir une liste d'options que vous pouvez inclure; vous devez fournir une option.
- **show rip database** affiche des renseignements sur les processus RIP et les routes apprises.
- **show vrf** affiche les renseignements sur les routeurs virtuels définis sur le système.
- **show zone** affiche les informations sur les zones de trafic ECMP, y compris les interfaces qui font partie de chaque zone.

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.