Routages statiques et par défaut

Ce chapitre décrit comment configurer les routes statiques et par défaut sur l'ASA.

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 ASA 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 ASA 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.

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 ASA.
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.

Routage vers l'interface null0 pour abandonner le trafic indésirable

Les règles d'accès vous permettent de filtrer les paquets en fonction des informations contenues dans leurs en-têtes. Une voie de routage statique vers l'interface null0 est une solution complémentaire aux règles d'accès. Vous pouvez utiliser une route null0 pour transférer le trafic indésirable ou indésirable afin que le trafic soit abandonné.

Les routes statiques Null0 ont un profil de rendement positif. Vous pouvez également utiliser des routes statiques null0 pour éviter les boucles de routage. BGP peut tirer parti de la route statique null0 pour le routage trou noir déclenché à distance.

Priorités de routage

- Les routes qui identifient une destination spécifique prévalent sur la route par défaut.
- Lorsque plusieurs routages existent vers la même destination (statique ou dynamique), la distance administrative du routage détermine la priorité. Les routes statiques sont définies à 1, ce sont donc généralement les routes les plus prioritaires.
- Lorsque vous avez plusieurs routes statiques vers la même destination avec la même distance administrative, consultez Routage à chemins multiples à coûts égaux (ECMP).
- Pour le trafic sortant d'un tunnel avec l'option tunnelisé, cette voie de routage remplace toute autre voie de routage par défaut configurée ou apprise.

Routages en mode de pare-feu transparent et de groupes de ponts

Pour le trafic qui provient du ASA et est destiné à travers une interface membre de groupe de ponts pour un réseau non connecté directement, vous devez configurer une voie de routage par défaut ou des routes statiques pour que l'ASA sache de quelle interface membre de groupe de ponts envoyer trafic. Le trafic provenant de ASA peut inclure des communications avec un serveur syslog ou SNMP. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques. Pour le mode transparent, vous ne pouvez pas spécifier les BVI comme interface de passerelle; seules les interfaces membres peuvent être utilisées. Pour les groupes de ponts en mode routé, vous devez préciser le BVI dans une voie de routage

statique; vous ne pouvez pas définir d'interface membre. Consultez Recherches d'adresse MAC ou de route pour de plus amples renseignements.

Suivi du 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 ASA tombe en panne.

La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. 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.

L'ASA met en œuvre le suivi de route statique en associant une route statique à un hôte cible de surveillance sur le réseau de destination que l'ASA surveille à l'aide des demandes Echo ICMP. Si aucune réponse écho n'est reçue dans un délai donné, l'hôte est considéré comme hors service et la route associée est supprimée de la table de routage. Une route de secours non suivie avec une métrique plus élevée est utilisée à la place de la route supprimée.

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 quel objet réseau de votre choix, mais vous pouvez envisager d'utiliser les objets 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.
- Un serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel l'ASA doit communiquer.
- Un objet réseau persistant sur le réseau de destination

Remarque Un poste de travail qui peut être éteint la nuit n'est pas un bon choix.

Vous pouvez configurer le suivi de routage statique pour les routes définies de manière statique ou pour les routages par défaut obtenus par DHCP ou PPPoE. Vous pouvez uniquement activer les clients PPPoE sur plusieurs interfaces avec le suivi de routage configuré.

Lignes directrices pour les routages statiques et par défaut

Mode de pare-feu et groupes de ponts

- En mode transparent, les routes statiques doivent utiliser l'interface du membre du groupe de ponts comme passerelle; vous ne pouvez pas préciser les BVI.
- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l'interface membre.

- Le suivi de routage statique n'est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

Adresse réseau prise en charge

- Le suivi de routage statique n'est pas pris en charge pour IPv6.
- L'ASA ne prend pas en charge le routage de classe E, donc un réseau de classe E n'est pas routable dans les routes statiques.

Mise en grappe et mode de contexte multiple

- Dans la mise en grappe, le suivi de routage statique n'est pris en charge que sur le nœud de contrôle.
- Le suivi de routage statique n'est pas pris en charge en mode de contexte multiple.

Entrées de routage ASP et RIB

Tous les routages et leur distance installés sur le périphérique sont capturés dans la table de routage ASP. Cette situation est commune à tous les protocoles de routage statiques et dynamiques. Seule la meilleure distance de routage est saisie dans le tableau RIB.

Configurer les routes par défaut et statiques

Vous devez configurer au moins une route par défaut. Vous devrez peut-être également configurer des routes statiques. Dans cette section, nous allons configurer une route par défaut, configurer une route statique et suivre une route statique.

Configurer une route par défaut

Une voie de routage par défaut est simplement une voie de routage statique avec 0.0.0.0/0 comme adresse IP de destination. Vous devez toujours avoir une route par défaut, soit configurée manuellement avec cette procédure, soit dérivée d'un serveur DHCP ou d'un autre protocole de routage.

Avant de commencer

Consultez les consignes suivantes pour l'option Tunneled (Tunnélisé) :

- N'activez pas la fonction de monodiffusion RPF (commande**ip verify reverse-path**) sur l'interface de sortie d'une route tunnellisée, car ce paramètre entraîne l'échec de la session.
- N'activez pas l'interception TCP sur l'interface de sortie de la route tunnellisée, car ce paramètre fait échouer la session.
- N'utilisez pas les moteurs d'inspection VoIP (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), la plateforme d'inspection DNS ou la plateforme d'inspection d'appel RPC DCE avec des routes tunnellisées, car ces moteurs d'inspection ignorent la route tunnellisée.
- Vous ne pouvez pas définir plusieurs routes par défaut avec l'option tunnellisée.
- ECMP pour le trafic en tunnel n'est pas pris en charge.

- Les routes tunnellisées ne sont pas prises en charge pour les groupes de ponts, qui ne prennent pas en charge la terminaison VPN pour le trafic traversant.

Procédure

Ajoutez une route par défaut :

IPv4 :

route *if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6 :

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

Exemple :

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

L'*if_name* est l'interface par laquelle vous souhaitez envoyer le trafic spécifique. Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

L'argument *distance* correspond à la distance administrative de la route, entre 1 et 254. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une route statique a la même distance administrative qu'une route dynamique, les routes statiques prévalent. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Remarque
Pour le trafic direct, si vous avez deux routes par défaut configurées sur des interfaces différentes qui ont des mesures différentes, la connexion à l'ASA établie à partir de l'interface à mesure supérieure échoue, mais les connexions à l'ASA à partir de l'interface à mesure inférieure réussissent comme prévu. Pour le trafic en provenance de la boîte, si vous avez deux routes par défaut configurées sur différentes interfaces qui ont des mesures différentes, les deux interfaces peuvent être utilisées pour le trafic en provenance de la boîte, selon l'interface qui a été utilisée pour la connexion entrante.

Vous pouvez définir une route par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une route par défaut différente de celle du trafic non VPN à l'aide du mot clé **tunneled**. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une route par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur l'ASA qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette route. Cette option n'est pas prise en charge pour les groupes de ponts.

Astuces

Vous pouvez saisir **0 0** au lieu de **0.0.0.0 0.0.0.0** pour l'adresse réseau de destination et le masque, comme le montre l'exemple suivant : **route outside 0 0 192.168.2.4**

Configurer une route statique

Une voie de routage statique définit où envoyer le trafic pour des réseaux de destination spécifiques.

Procédure

Ajoutez une route statique :

IPv4 :

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6 :

ipv6 route *if_name dest_ipv6_prefix/prefix_length gateway_ip* [**distance**]

Exemple :

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

L'*if_name* est l'interface par laquelle vous souhaitez envoyer le trafic spécifique. Pour abandonner le trafic indésirable, saisissez l'interface **null0**. Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

Les arguments *dest_ip* et *mask* ou *dest_ipv6_prefix/prefix_length* indiquent l'adresse IP du réseau de destination et l'argument *gateway_ip* est l'adresse du routeur de saut suivant. Les adresses que vous spécifiez pour la route statique sont les adresses qui sont dans le paquet avant d'entrer dans l'ASA et d'effectuer la NAT.

L'argument *distance* correspond à la distance administrative de la route. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une voie de routage statique a la même distance administrative qu'une voie de routage dynamique, la voie statique prévaut. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Exemple

L'exemple suivant montre les routes statiques pour trois réseaux qui vont à la même passerelle et un autre réseau qui va à une passerelle distincte :

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
```

```
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

Configurer le suivi de route statique

Pour configurer le suivi des routes statiques, procédez comme suit.

Procédure

Étape 1 Configurez la route statique pour l'interface (externe 1) utilisée pour atteindre le réseau :

```
ciscoasa(config)# route outside1 172.29.139.134 255.255.255.255 10.0.0.1
```

Étape 2 Définissez le processus de surveillance :

sla monitor sla_id

Exemple :

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

Étape 3 Spécifiez le protocole de surveillance, l'hôte cible sur le réseau suivi et l'interface par laquelle vous accédez au réseau :

type echo protocol ipicmpecho target_ip **interface** if_name

Exemple :

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134 interface outside1
ciscoasa(config-sla-monitor-echo)#
```

L'argument *target_ip* est l'adresse IP de l'objet réseau dont le processus de suivi surveille la disponibilité. Pendant que cet objet est disponible, la route du processus de suivi est installée dans la table de routage. Lorsque cet objet n'est plus disponible, le processus de suivi supprime la route et la route de secours est utilisée à sa place.

Étape 4 (Facultatif) Configurez les options de surveillance. Consultez la référence de commande pour les commandes suivantes : **frequency, num-packets, request-data-size, threshold, timeout** et **tos**.

Étape 5 Planifiez le processus de surveillance :

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

Exemple :

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

En règle générale, vous utiliserez la commande **sla monitor schedule** *sla_id* **life forever start-time now** pour le calendrier de surveillance et permettrez à la configuration de surveillance de déterminer la fréquence des tests.

Cependant, vous pouvez planifier ce processus de surveillance pour qu'il commence dans le futur et qu'il se produise uniquement à des heures spécifiées.

Étape 6 Associez une route statique suivie au processus de surveillance du SLA :

track track_id **rtr** sla_id **reachability**

Exemple :

```
ciscoasa(config)# track 6 rtr 5 reachability
```

L'argument *track_id* est un numéro de suivi que vous attribuez avec cette commande. L'argument *sla_id* est le numéro d'identifiant du processus SLA.

Étape 7 Suivez l'un des types de route suivants :

- Route statique :

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  Exemple :

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  Vous ne pouvez pas utiliser l'option **tunneled**.

- Route par défaut obtenue par DHCP :

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- Route par défaut obtenue par PPPoE :

  ```
  interface interface_id
    pppoe client route track track_id
    ip address pppoe setroute
  ```

Étape 8 Créez une route de secours non suivie.

La route de secours est une route statique vers la même destination que la route suivie, mais via une interface ou une passerelle différente. Vous devez attribuer à cette route une distance administrative (mesure) plus élevée que votre route suivie.

Supervision d'une route statique ou par défaut

- **afficher route**

Affiche la table de routage.

Exemples de routes statiques ou par défaut

L'exemple suivant montre comment créer une route statique qui envoie tout le trafic destiné à 10.1.1.0/24 au routeur 10.1.2.45, qui est connecté à l'interface interne, définit trois routes statiques à coût égal qui dirigent le trafic vers trois passerelles différentes sur l'interface DMZ, et ajoute une route par défaut pour le trafic tunnelé et une autre pour le trafic normal.

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

Historique des routes statiques et par défaut

Tableau 1 : Historique des fonctionnalités pour les routes statiques et par défaut

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Suivi du routage statique	7.2(1)	La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Nous avons ajouté les commandes suivantes : **clear configure sla, frequency, num-packets, request-data-size, show sla monitor, show running-config sla, sla monitor, sla monitor schedule, threshold, timeout, tos, track rtr**
Route statique null0 pour abandonner le trafic	9.2(1)	L'envoi du trafic vers une interface null0 entraîne l'abandon des paquets destinés au réseau spécifié. Cette fonctionnalité est utile dans la configuration de Remotely Triggered Black Hole (RTBH) pour BGP. Nous avons modifié la commande suivante : **route**.

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.