

Comment configurer le routage basé sur les politiques (PBR) sur un commutateur ou un routeur multicouche Cisco pour transférer le trafic vers le WSA ?

Table des matières

[Question :](#)

Question :

Comment configurer le routage basé sur les politiques (PBR) sur un commutateur ou un routeur multicouche Cisco pour transférer le trafic vers le WSA ?

Environnement : appareil de sécurité Web Cisco (WSA), mode transparent - commutateur L4

Lorsque WSA est configuré en mode transparent à l'aide d'un commutateur de couche 4, aucune configuration n'est nécessaire sur le WSA. La redirection est contrôlée par le commutateur L4 (ou le routeur).

Il est possible d'utiliser le routage PBR (Policy Based Routing) pour rediriger le trafic Web vers le WSA. Pour ce faire, il faut faire correspondre le trafic correct (en fonction des ports TCP) et demander au routeur/commutateur de rediriger ce trafic vers le WSA.

Dans l'exemple suivant, l'interface de données/proxy de WSA (M1 ou P1 selon la configuration) se trouve sur une interface VLAN dédiée du commutateur/routeur multicouche (Vlan 3) et le routeur Internet se trouve également sur une interface VLAN dédiée (Vlan4). Les clients se trouvent sur Vlan1 et Vlan2.

Configuration initiale (seules les pièces pertinentes sont affichées)

```
interface Vlan1
desc User VLAN 1
ip address 10.1.1.1 255.255.255.0
!
interface Vlan2
desc User VLAN 2
ip address 10.1.2.1 255.255.255.0
```

```
!  
interface Vlan3  
desc VLAN dédié Cisco WSA  
adresse ip 192.168.1.1 255.255.255.252  
!  
interface Vlan4  
desc Routeur Internet VLAN dédié  
adresse ip 192.168.2.1 255.255.255.252  
!  
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Dans l'exemple ci-dessus, et Cisco WSA ayant l'adresse IP 192.168.1.2, vous ajouteriez les commandes suivantes pour configurer le routage basé sur les politiques (PBR) :

Étape 1 : Définissez le trafic Web

```
! Correspondance du trafic HTTP  
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 80  
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 80  
! Correspondance du trafic HTTPS  
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 443  
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 443
```

Étape 2 : définissez une carte de route pour contrôler l'emplacement de sortie des paquets.

```
route-map ForwardWeb permit 10  
match ip address 100  
set ip next-hop 192.168.1.2
```

Étape 3 : appliquez la carte de routage à l'interface appropriée.

```
!Notez que ceci doit être appliqué à l'interface source (côté client)  
interface Vlan1  
ip policy route-map ForwardWeb  
!  
interface Vlan2  
ip policy route-map ForwardWeb
```

Remarque : cette méthode de redirection du trafic (PBR) présente certaines limitations. Le principal problème avec cette méthode est que le trafic sera toujours redirigé vers le WSA même si l'appliance n'est pas accessible (en raison de problèmes réseau par exemple). Il n'y a donc pas d'option de basculement.

Pour remédier à cette lacune, vous pouvez configurer l'un des éléments suivants :

1. PBR avec options de suivi lorsque vous utilisez des routeurs Cisco. Cette fonctionnalité permet de vérifier la disponibilité du tronçon suivant avant de rediriger le trafic.

Plus de détails sur l'article suivant :

[Exemple de configuration de routage fondé sur la stratégie avec la fonction d'options de suivi multiples](#)

2. Les options de suivi ne sont pas disponibles pour les commutateurs Cisco Catalyst. Cependant, une solution de contournement avancée est disponible pour obtenir le même comportement.

Pour plus d'informations, consultez le wiki Cisco suivant :

[Routage PBR \(Policy-Based Routing\) avec suivi pour les commutateurs Catalyst 3xxx - Solution de contournement utilisant EEM](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.