Contenu

Question :

Comment est-ce que je configure le Routage à base de règles (PBR) sur un commutateur multicouche ou un routeur de Cisco pour expédier le trafic au WSA ?

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

Quand WSA est configuré en mode transparent utilisant un commutateur L4, aucune configuration n'est nécessaire sur le WSA. La redirection est contrôlée par le commutateur L4 (ou le routeur).

Il est possible d'employer le Routage à base de règles (PBR) pour réorienter le trafic web au WSA. Ceci est réalisé en appariant le trafic correct (basé sur des ports de TCP) et en demandant au routeur/au commutateur pour réorienter ce trafic au WSA.

Dans l'exemple suivant, les données de WSA/interface de proxy (M1 ou P1 selon la configuration) sont sur une interface VLAN dédiée du commutateur multicouche/du routeur (le VLAN 3) et le routeur internet est sur une interface VLAN dédiée aussi bien (Vlan4). Les clients sont sur Vlan1 et Vlan2.

Configuration initiale (seulement éléments pertinents affichés)
interface Vlan1 utilisateur VLAN 1 de desc IP address 10.1.1.1 255.255.255.0 ! interface Vlan2 utilisateur VLAN 2 de desc IP address 10.1.2.1 255.255.255.0 ! interface Vlan3 desc Cisco WSA VLAN dédié IP address 192.168.1.1 255.255.255.252 ! interface Vlan4 routeur internet VLAN dédié de desc IP address 192.168.2.1 255.255.255.252 ! artère 0.0.0.0 0.0.0.0 192.168.2.2 d'IP

Etant donné l'exemple ci-dessus, et Cisco WSA ayant une adresse IP de 192.168.1.2, vous ajouteriez les commandes suivantes d'installer le Routage à base de règles (PBR) :

Étape 1 : Définissez le trafic web
! Le trafic http de correspondance la liste d'accès 100 permettent à TCP 10.1.1.0 0.0.0.255 tout eq 80 la liste d'accès 100 permettent à TCP 10.1.2.0 0.0.0.255 tout eq 80 *! Le trafic de la correspondance HTTPS* la liste d'accès 100 permettent à TCP 10.1.1.0 0.0.0.255 tout eq 443 la liste d'accès 100 permettent à TCP 10.1.2.0 0.0.0.255 tout eq 443
Étape 2 : Définissez un mappage de route pour contrôler où des paquets sont sortis.
autorisation 10 de ForwardWeb de route-map match ip address 100 set ip next-hop 192.168.1.2
Étape 3 : Appliquez le mappage de route à l'interface appropriée.
! Notez que ceci devrait être appliqué à l'interface de source (côté client) interface Vlan1 ip policy route-map ForwardWeb ! interface Vlan2 ip policy route-map ForwardWeb

Remarque: Cette méthode de la redirection du trafic (PBR) a quelques limites. Le problème principal avec cette méthode est que le trafic sera toujours réorienté au WSA même si l'appliance n'est pas accessible (en raison des problèmes de réseau par exemple). Ainsi, il y a aucun basculent l'option.

Au contournement cette insuffisance, vous pouvez configurer l'un ou l'autre de ce qui suit :

1. **PBR avec des options de cheminement** à l'aide des Routeurs de Cisco. Cette caractéristique est utilisée pour vérifier la Disponibilité du prochain saut avant de réorienter 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. En dépistant des options ne soyez pas disponible pour des commutateurs Cisco Catalyst. Cependant, il y a un contournement avancé disponible pour réaliser le même comportement.

   Des détails peuvent être trouvés sur Cisco suivant Wiki :
   Gestion de réseau à base de règles avec le cheminement pour le contournement de commutateur A du Catalyst 3xxx utilisant EEM