Utiliser la liste de contrôle d’accès MAC pour les trames de contrôle de couche 2 sur les commutateurs de la gamme Catalyst 4500

Contenu

Introduction

Ce document décrit le comportement de la liste de contrôle d'accès MAC (MAC ACL) sur le trafic non IP du plan de contrôle sur les commutateurs de la gamme Catalyst 4500. La liste de contrôle d’accès MAC peut être utilisée afin de filtrer le trafic non IP sur un VLAN et sur un port physique de couche 2 (L2).

Pour plus d'informations sur les protocoles non IP pris en charge dans la commande MAC access-list extended, référez-vous à Référence de commande du commutateur de la gamme Catalyst 4500 Cisco IOS®.

Problème

Assumez cette configuration :

```
mac access-list extended udld
 deny any host 0100.0ccc.cccc
 permit any any
!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 mac access-group udld in
!
```

> **Note**: Cette liste de contrôle d'accès ne refuse pas le trafic du plan de contrôle de couche 2, tel que les trames CDP/UDLD/VTP/PAgP avec l'adresse MAC de destination = 0100.0ccc.cccc qui arrive en entrée dans l'interface GigabitEthernet2/4.

Sur les commutateurs Catalyst 4500, il y a une liste de contrôle d'accès intégrée générée par le système qui pond le trafic du plan de contrôle de couche 2 au CPU qui a priorité sur une liste de contrôle d'accès définie par l'utilisateur, afin de classer ce trafic. Par conséquent, une liste de contrôle d’accès définie par l’utilisateur n’atteint pas cet objectif. Ce comportement est spécifique à la plate-forme Catalyst 4500, d'autres plates-formes peuvent avoir des comportements différents.

Solution

Cette méthode peut être utilisée pour supprimer le trafic au niveau du port d'entrée ou du processeur, si nécessaire.

> **Attention** : Les étapes suivantes sont destinées à supprimer toutes les trames dont l'adresse MAC de destination = 0100.0ccc.cccc qui arrivent sur une interface spécifique. Cette adresse MAC est utilisée par les unités de données de protocole (PDU) du plan de contrôle UDLD/DTP/VTP/Pagp.

Si l'objectif est de contrôler ce trafic et de ne pas le supprimer, la réglementation du plan de contrôle est une solution privilégiée. Reportez-vous à Configuration de la réglementation du plan de contrôle sur Catalyst 4500

Étape 1. Activer la qualité de service (QoS) des paquets de contrôle pour cdp-vtp :

```
Catalyst4500(config)#qos control-packets cdp-vtp
```

Cette étape génère une liste de contrôle d'accès générée par le système :

```
Catalyst4500#show run | begin system-control

mac access-list extended system-control-packet-cdp-vtp
 permit any host 0100.0ccc.cccc
```

> **Note**: Une liste de contrôle d'accès MAC nommée définie par l'utilisateur (comme illustré ici) peut également être utilisée à la place d'une liste de contrôle d'accès définie par le système comme générée précédemment. Utilisez une liste de contrôle d'accès générée par le système ou définie par l'utilisateur afin d'enregistrer les ressources TCAM (Ternary Content Addressable Memory).

```
mac access-list extended udld
 permit any host 0100.0ccc.cccc
```

Étape 2. Créez une carte-classe afin de correspondre au trafic qui atteint cette liste de contrôle d'accès :

```
Catalyst4500(config)#class-map cdp-vtp
Catalyst4500(config-cmap)#match access-group name system-control-packet-cdp-vtp
Catalyst4500(config-cmap)#end
Catalyst4500#
```

Étape 3. Créez une carte de stratégie et un trafic de police correspondant à la classe de l'étape 2 avec une action conforme = action de suppression et de dépassement = action de suppression :

```
Catalyst4500(config)#policy-map cdp-vtp-policy
Catalyst4500(config-pmap)#class cdp-vtp
Catalyst4500(config-pmap-c)#police 32000 conform-action drop exceed-action drop
Catalyst4500(config-pmap-c-police)#end
Catalyst4500#
```

Étape 4. Appliquez la carte de stratégie entrante sur le port de couche 2 où ce trafic doit être

abandonné :

```
Catalyst4500(config)#int gigabitEthernet 2/4
Catalyst4500(config-if)#service-policy input cdp-vtp-policy
Catalyst4500(config-if)#end

!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 service-policy input cdp-vtp-policy
end
```

Des listes de contrôle d'accès générées par le système similaires peuvent être utilisées pour d'autres trames de contrôle de couche 2 au cas où elles auraient besoin d'être contrôlées ou abandonnées. Référez-vous à QoS du paquet de contrôle de couche 2 pour plus de détails et comme indiqué dans l'image.

```
Catalyst4500(config)#qos control-packets ?
 bpdu-range       Enable QoS on BPDU-range packets
 cdp-vtp          Enable QoS on CDP and VTP packets
 eapol            Enable QoS on EAPOL packets
 lldp             Enable QoS on LLDP packets
 protocol-tunnel  Enable QoS on protocol tunneled packets
 sstp             Enable QoS on SSTP packets
 <cr>
```

Type of Packet that the Feature is Enabled On	Range of Address the Feature Acts On
BPDU-range	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 EAPOL
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD
LLDP	0180.C200.000E