Sécuriser un switch Cisco

Sécuriser un switch Cisco

Les mots de passe

Accès par mot de passe

- L'accès au mode Privileged doit être sécurisé par un mot de passe

  host(config)# `enable password` *`mot_de_passe`* ou `enable` *`mot_de_passe`*

  - Solution la moins sécurisé, le mot de passe est stocké en clair

  host(config)# `enable secret ?`

  - 0 : spécifie que le mot de passe qui suit est en clair
  - 5 : spécifie que le mot de passe qui suit est crypté
  - LINE : le mot de passe non crypté

  - Dans tous les cas, le enable secret crypte le mot de passe en utilisant l'algorithme MD5

- Dans le cas de l'utilisation des 2 commandes, c'est le `enable secret` qui sera prioritaire

Sécuriser un switch Cisco

Port Security

Sécuriser l'accès aux ports d'un Cisco 2950

- Pour éviter que n'importe qui se connecte sur les port d'un switch, il est possible de faire un contrôle sur les adresses MAC des machines connectées sur chaque port
- Pour activer cette sécurité sur l'interface concernée :

  Switch(config-if)# `switchport mode access`

  Switch(config-if)# `switchport port-security`
- Définition des adresses MAC autorisées sur un port
  - Adresse MAC fixée

  Switch(config-if)# `switchport port-security mac-address` *`0123.4567.1423.7890`*
  - Ou apprentissage de l'adresse MAC (source) de la première trame qui traversera le port

  Switch(config-if)# `switchport port-security mac-address sticky`
- Par défaut, une seule adresse MAC est autorisée par port. Pour changer ce nombre

  Switch(config-if)# `switchport port-security maximum` *`nombre`*

Politique de sécurité

- Plusieurs politiques de sécurité peuvent être envisagées
- Soit on bloque définitivement le port lors d'une usurpation d'adresse MAC

  Switch(config-if)# `switchport port-security violation shutdown`
- Soit on bloque toutes les trames avec des adresses MAC non connu et on laisse passer les autres

  Switch(config-if)# `switchport port-security violation protect`
- Soit un message dans le syslog et via SNMP sont envoyés. De plus le compteur du nombre de violation est incrémenté.

  Switch(config-if)# `switchport port-security violation restrict`
- Pour réactiver un port désactivé automatiquement, suite à un problème de sécurité faire un `shutdown` suivi d'un `no shutdown`

Information sur les @ MAC et l'état d'un port

- Pour visualiser la politique de sécurité d'une interface

  Switch# `show port-security interface ...`

- Pour visualiser les adresses MAC connues sur les ports

  Switch# `show port-security address`

```
Switch#show port-security interface FastEthernet 0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 1 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0

Switch#
00:02:35: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 02e0.4c39.37dd on port FastEthernet 0/4
```