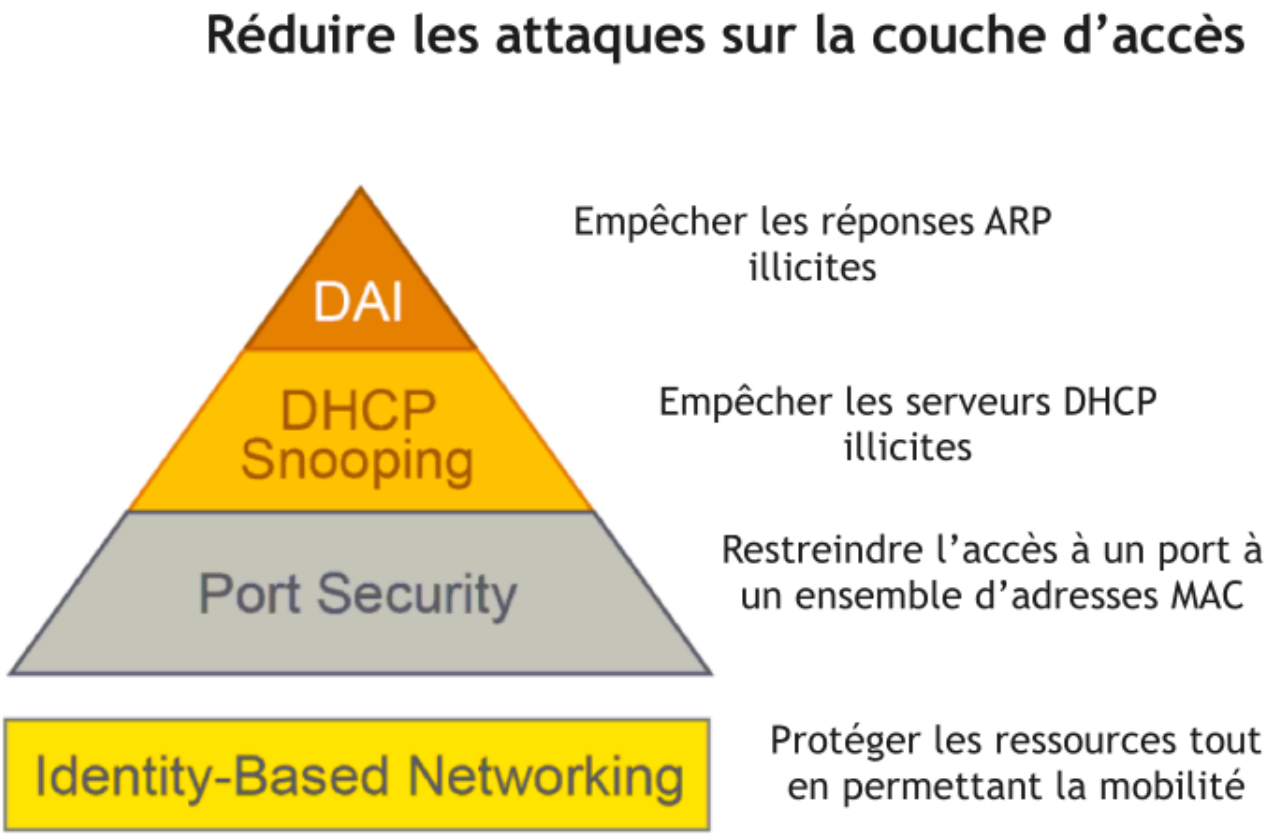
[Cisco] Sécurité des switchs

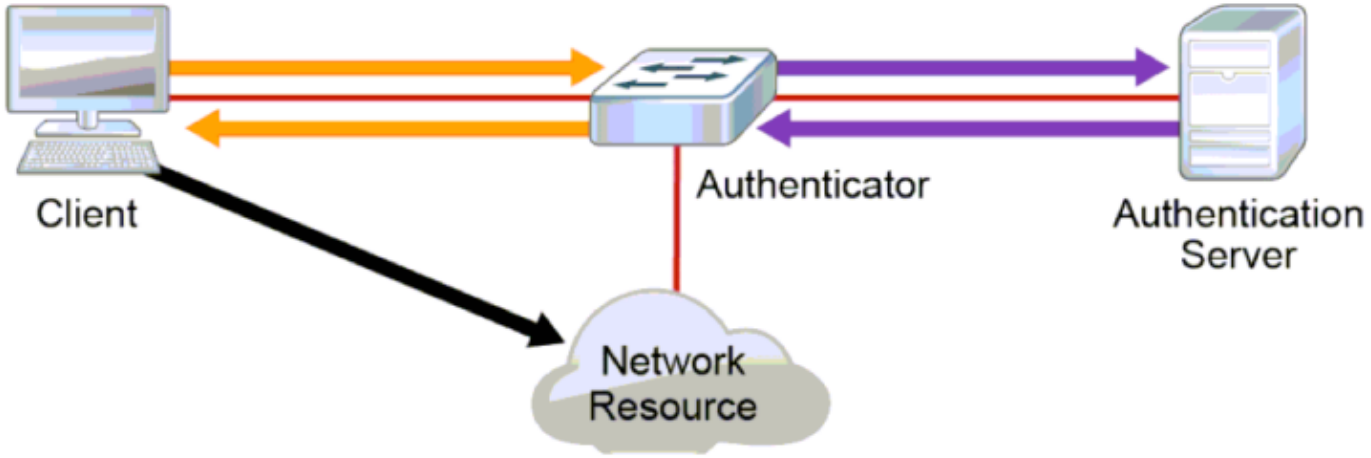
Introduction

Sur les switchs Cisco, il est possible d'activer des options pour renforcer la sécurité des équipements connectés au réseau.



Identify-Based Networking

Basé sur le protocole 802.1x, il permet d'exiger une identification pour accéder au réseau.



Autoriser une adresse MAC manuellement

Après avoir sélectionné l'interface :

```
switchport port-security mac-address <MAC>
```

```
switchport port-security
```

> Il faut autoriser chaque adresse MAC une à une, ce qui peut devenir fastidieux.

Autoriser la première adresse MAC

Après avoir sélectionné l'interface :

```
switchport port-security maximum 1
```

```
switchport port-security
```

> Seulement la première adresse MAC qui se connecte pourra accéder au réseau mais si le courant du switch se coupe et qu'un pirate se connecte, il pourra accéder au réseau.

Autoriser la première adresse MAC + sticky

Après avoir sélectionné l'interface :

```
switchport port-security maximum 1
```

```
switchport port-security mac-address sticky
```

```
switchport port-security
```

> Il s'agit de la méthode la plus recommandée.

Port Security

Shutdown

Avec cette méthode, si l'adresse MAC source d'une trame n'est pas autorisée, **l'interface sera coupée**.

Après avoir sélectionné l'interface :

```
switchport port-security violation shutdown
```

> Il s'agit du mode utilisé par défaut.

Restrict

Avec cette méthode, si l'adresse MAC source de la trame n'est pas autorisée, il **supprime la trame** et en **informe** l'administrateur.

Après avoir sélectionné l'interface :

```
switchport port-security violation restrict
```

Protect

Avec cette méthode, si l'adresse MAC source de la trame n'est pas autorisée, il **supprime la trame sans informer** l'administrateur.

Après avoir sélectionné l'interface :

```
switchport port-security violation protect
```

DHCP snooping

L'objectif est d'empêcher un pirate de mettre son propre serveur DHCP sur le réseau ou de DOS votre serveur DHCP.

Interface trusted

L'objectif va être de définir les ports sur lesquels les serveurs DHCP légitimes sont présents.

Tout d'abord, activez le DHCP snooping :

```
ip dhcp snooping
```

On peut aussi l'activer sur un VLAN spécifique :

```
ip dhcp snooping vlan <VLAN_ID>
```

Ensuite, sélectionnez l'interface sur laquelle le serveur DHCP est présent puis faite :

```
ip dhcp snooping trust
```

Vérifier les interfaces de confiance

```
show ip dhcp snooping
```

DAI

L'objectif va être d'empêcher l'ARP spoofing.

Pour cela, le DHCP snooping doit être configuré pour fonctionner.

Configurer une correspondance MAC/IP

Tout d'abord définissez une liste d'accès :

```
arp access-list <NAME>
```

Puis lancez la commande suivante :

```
permit ip host <IP> mac host <MAC>
```

Et enfin :

```
ip arp inspection filter <NAME> vlan <VLAN_ID>
```

Revision #2
Created 24 January 2024 12:14:04 by Elieroc
Updated 19 March 2024 07:05:00 by Elieroc