Cisco : Authentification radius par adresse MAC

>>> Cisco 2960 IOS 15.0

Description :

Le but de cet article est de mettre en place l'authentification radius pour authentifier les machines du réseau afin de les autoriser à accéder au ressources de l'entreprise.

Cisco : Authentification radius par adresse MAC

>>> Cisco 2960 IOS 15.0

Sommaire :

I) Introduction

Nous allons maintenant voir comment authentifier une machine (PC, imprimante, ...) via son adresse MAC. Puis dans un deuxième temps, on fera en sorte qu'une fois authentifiée notre machine soit dans un Vlan particulier.

AAA (Authentication, Authorization and Accounting) est un protocole qui permet de gérer :

- **Authentication** : Authentification consiste à déterminer si l'utilisateur ou l'équipement est bien celui qu'il prêtant être, cela se fait grâce à une authentification nom d'utilisateur/ mot de passe, ou grâce à un certificat.
- **Authorization** : Autorisation consiste à déterminer les droits de l'utilisateur sur les différentes ressources.
- **Accounting** : Compte permet de garder des informations sur l'utilisation des ressources par l'utilisateur.

Voici les informations de notre maquette :

- Le serveur radius :
  - Hostname : Deb-Idum-LAB4
  - Adresse IP : 172.16.1.17/24
  - Port d'auth du service Radius : 1812
  - Port accounting du service Radius : 1813
- Le switch :
  - Hostname : sw-Idum-LAB
  - Adresse IP : 172.16.1.253/24
  - Type de switch : WS-C2960-8TC-L
  - Version IOS : 15.0(2)SE4
  - Key radius : bonjour
- Le PC :
  - Hostname : desktop
  - Adresse IP : DHCP
  - OS : Windows Seven

- Adresse MAC : 00:1c:23:58:2e:ae

II) Configuration du radius

- Éditez le fichier freeradius **"users"**.

```
vim /etc/freeradius/users
```

- Ajoutez un nouvel utilisateur avec les paramètres suivants :
  - Nom : adresse_mac_du_PC
  - Password : adresse_mac_du_PC

```
001c23582eae Cleartext-Password := "001c23582eae"
Service-Type = Framed-User,
```

- Puis rechargez la configuration de **freeradius**.

```
service freeradius reload
```

III) Configuration du switch

1) Configuration de base du switch

- Définissez un hostname :

```
conf t
hostname sw-idum-lab
```

- Définissez un domaine et le serveur de noms de votre réseau. (Dans notre LAB notre serveur radius est aussi serveur DNS)

```
ip domain-name idum.eu
ip name-server 172.16.1.17
```

- Définissez l'adresse IP de votre switch :

```
interface vlan 1
ip address 172.16.1.253 255.255.255.0
exit
ip default-gateway 172.16.1.254
```

- Générer la crypto key pour le SSH (taille 2048) :

```
crypto key generate rsa
```

- Vous devez obtenir ceci :

```
The name for the keys will be: sw-idum-lab.idum.eu
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
```

- Activez la version 2 de SSH :

```
ip ssh vesion 2
```

- Autoriser les connexions SSH :

```
line vty 0 15
transport input ssh
exit
```

- Définissez un utilisateur local, avec les paramètres ci-dessous :

- Nom : admin
- Niveau de droits : 15
- Mot de passe : guten_tag

```
username admin privilege 15 secret guten_tag
```

2) Déclaration du serveur radius

- Tapez les lignes suivantes, pour définir le serveur Radius :

```
radius server deb-idum-lab4
address ipv4 172.16.1.17 auth-port 1812 acct-port 1813
key bonjour
exit
```

- Si vous avez plusieurs interfaces IP de configurée sur le switch, vous devez définir l'interface source pour les requêtes radius.

```
ip radius source-interface vlan 1
```

- Rajoutez la ligne suivante, afin d'éviter des erreurs dans les logs :

```
radius-server attribute 6 on-for-login-auth
```

3) Configuration aaa

- Tapez les commandes suivantes :

```
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius local
```

4) Configuration de l’interface

- Configurez l’interface que vous voulez sécuriser :

```
interface FastEthernet0/1
switchport mode access
switchport nonegotiate
authentication port-control auto
mab
spanning-tree portfast
```

- Vous n’avez plus qu’à connecter votre PC.
- Vous pouvez observer que l’authentification fonctionne bien grâce à la commande :

```
debug radius
```

5) Authentification MAC et VLAN

Nous allons faire en sorte qu’une fois authentifiée notre machine soit dans le vlan 10.

a) Modification du fichier radius "users"

- Modifiez l’utilisateur avec les paramètres suivants :
  - Nom : adresse_mac_du_PC
  - Password : adresse_mac_du_PC
  - Tunnel-private-Group-ID : ID_DU_VLAN

```
001c23582eae Cleartext-Password := "001c23582eae"
Service-Type = Framed-User,
Tunnel-type = VLAN,
Tunnel-Medium-Type = 6,
Tunnel-private-Group-ID = 10
```

- Rechargez la configuration de **freeradius**.

```
service freeradius reload
```

b) Configuration du switch

- Vérifier que le vlan 10 existe, sinon ajoutez le :

```
vlan 10
name test-radius
```

c) Test

- Avant de connecter votre machine, tapez la commande **"show vlan"** afin de vérifier que l’interface fa0/1 est bien dans le Vlan par défaut :

```
sw-idum-lab#sh vlan
```

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Gi0/1
10 test active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

- Connectez votre machine sur le port fa0/1, et retapez la commande afin de confirmer qu'elle est bien dans le vlan 10.

```
sw-idum-lab#sh vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Gi0/1
10 test active Fa0/1
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```