Vous savez déjà créer des utilisateurs sécurisés, mais vous n'allez pas répéter cette opération sur chaque routeur !

Pour conclure cette partie sur la sécurité des appareils CISCO, je vous propose donc de coupler vos routeurs et vos switchs à un serveur permettant de centraliser tous les utilisateurs de votre réseau. Une fois n'est pas coutume, vous n'allez pas, cette fois-ci, installer un serveur CISCO, mais un serveur.

Pourquoi ce changement ?

Car le protocole que vous allez utiliser, RADIUS, est open source et se configure entre un serveur (Linux ou Windows) et vos appareils CISCO. Regardons ensemble comment ça fonctionne.

Centralisez tous vos utilisateurs sur le même serveur

Centraliser tous les utilisateurs sur le même serveur, c'est la mission principale de RADIUS (Remote Authentication Dial-In User Service). Comme évoqué dans l'introduction, en tant qu'administrateur, vous ne voulez pas avoir à créer vos utilisateurs sur un routeur et à répéter l'opération sur chacun de vos appareils. Il faut donc pouvoir centraliser ces données sur un seul serveur.

C'est l'entreprise Livingston Enterprises, Inc qui en 1991 a développé ce protocole. Il a ensuite été standardisé par l'IETF (Internet Engineering Task Force).
RADIUS est ce que l'on appelle un protocole AAA (pour Authentication, Authorization, and Accounting) :

- *Authentication* c'est, vous vous en doutez, le fait de reconnaître un utilisateur et de l'associer à un mot de passe.
- *Authorization* c'est l'action de laisser, ou d'interdire, un utilisateur d'accéder à certaines ressources. Un utilisateur peut avoir accès à certains routeurs, mais pas à d'autres.
- *Accounting* fait référence aux suivis de consommation d'un utilisateur : sur quel routeur il s'est connecté ? Combien de temps s'est-il connecté ? etc.

Voyons un peu plus en détail comment ce protocole fonctionne.

Un client, un serveur et un utilisateur sont dans votre topologie

RADIUS est un protocole client-serveur. Le serveur RADIUS (installé sur Linux dans votre cas) communique avec un client, appelé NAS (network access server). Ce NAS dans votre cas c'est votre routeur CISCO. Il ne manque plus que l'utilisateur, un ordinateur connecté à votre routeur. Regardez comment ils communiquent :

- Le serveur RADIUS et le client NAS échangent un mot de passe privé afin de s'authentifier.
- Le serveur RADIUS possède dans une base de données (MySQL, fichier texte ou autres) les identifiants et mots de passe des utilisateurs.
- Lorsqu'un utilisateur tente de se connecter à un routeur, le routeur transmet les identifiants et mots de passe entrés par l'utilisateur au serveur RADIUS.
- Le serveur RADIUS renvoie un message acceptant ou refusant la connexion au routeur.

Le serveur que vous allez installer n'est donc pas un CISCO mais un serveur sur lequel vous paramétrez le service RADIUS AAA.

Ajoutez un serveur RADIUS à votre topologie

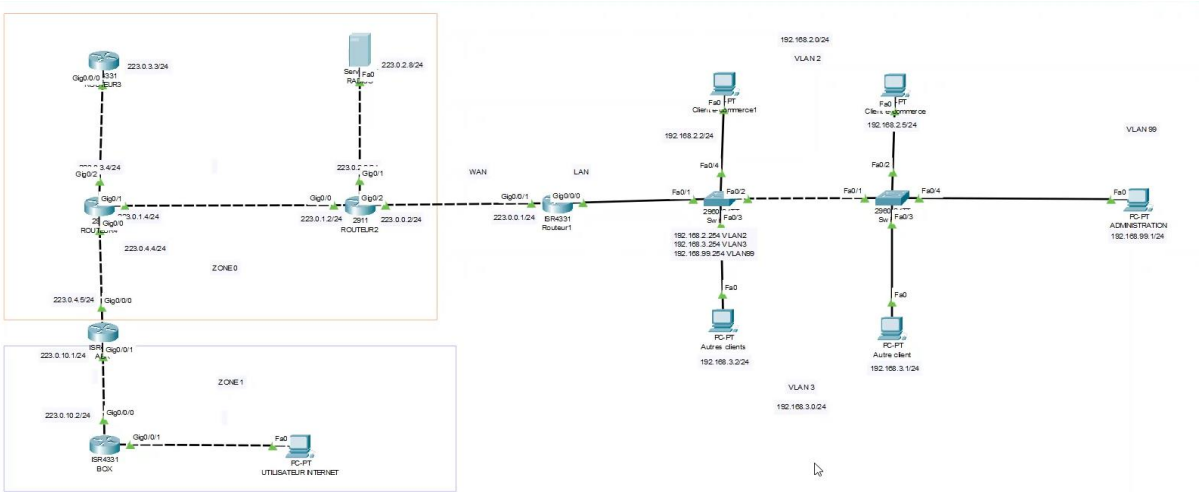
La configuration du serveur RADIUS consiste à :

- Déclarer ses clients (adresses IP), les routeurs ou switchs CISCO, et d'y renseigner le mot de passe partagé ;
- Puis d'enregistrer les utilisateurs avec leur mot de passe.

N'oubliez pas que pour pouvoir communiquer avec le serveur RADIUS, votre routeur doit pouvoir l'atteindre. Il ne doit pas forcément être sur le même réseau pour autant.

Configurez votre serveur RADIUS

Commencez par ajouter un serveur à votre topology et donnez lui une adresse IP, dans notre exemple nous lui donnons l'adresse IP 223.0.2.8/24, et l'avons raccorder au routeur 2.



Topology avec un serveur RADIUS

Ajoutez vos clients au serveur RADIUS

Il est assez simple de comprendre que vos clients, c'est-à-dire vos routeurs, doivent être renseignés sur votre serveur, il faut donc entrer leurs informations dans le service AAA de notre serveur.

Ainsi nous allons indiquer le nom du routeur ainsi que son adresse IP dans les champs prévus, puis nous allons entrer un mot de passe, par exemple Cisco1234.

N'oubliez pas de cliquer sur ADD pour enregistrer vos paramètres.

Avec cette configuration, vous venez d'ajouter le routeur 2 avec comme mot de passe secret : Cisco1234. Il faudra renseigner de la même façon ce mot de passe dans le routeur.

Il ne vous manque plus qu'à ajouter des utilisateurs et les autoriser à se connecter au routeur.

Ajoutez des utilisateurs au serveur RADIUS

C'est la section suivante qui nous permet d'entrer les utilisateurs du serveur Radius.

Ici, nous créons un utilisateur ainsi que son mot de passe. Pour notre exemple, nous choisissons un login/mot de passe simple : root

N'oubliez pas de cliquer sur ADD pour enregistrer vos paramètres.

Avec cette configuration, vous venez d'ajouter un utilisateur nommé "root" avec comme mot de passe : root

Votre serveur RADIUS est désormais configuré, il ne vous manque plus qu'à configurer votre routeur en tant que client afin qu'il considère les utilisateurs de RADIUS comme les siens.

Configurez votre routeur comme client

Pour configurer votre routeur comme client, vous devez :

- Activer AAA ;
- Puis configurer le serveur Ubuntu comme étant votre serveur RADIUS.

La commande suivante va vous permettre d'activer AAA.

```
routeur1(config)# aaa new-model
```

Ensuite, vous allez renseigner l'adresse du serveur RADIUS et le mot de passe configuré dessus.

```
routeur1(config)#radius-server host 223.0.2.8 key Cisco1234
```

Vous devez également configurer le routeur de sorte qu'il vous permette d'utiliser l'authentification AAA, associée au groupe RADIUS avec la commande :

```
routeur1(config)#aaa authentication login default group radius local
```
Enfin, vous devez l’associer à une ou plusieurs lignes en mode configuration de lignes :

```
routeur2(config)#line vty 0 15 routeur2(configure-line)# login authentication default
```

Vérifiez votre configuration

Comme toujours, il est essentiel de vérifier vos configurations. Vous pouvez les vérifier dans votre running-config en tapant ces commandes :

```
routeur1# show run | in radius
```
Ça vous montre la partie RADIUS de votre configuration.

```
routeur1# show run | in aaa
```
Ça vous montre la partie AAA de votre configuration.

Il ne vous reste plus qu’à faire le test en vous reconnectant à votre routeur en indiquant l’identifiant et le mot de passe configuré sur le serveur Radius (dans notre exemple).

Et voilà ! N’hésitez pas à configurer l'authentification sur d’autres routeurs.

La prise en main, le réseau local puis les protocoles de routage et enfin la sécurité. BRAVO. La fin de cette partie marque aussi la fin de ce cours. Maîtriser les concepts que nous avons vus ensemble vous ouvre déjà de nombreuses perspectives, qu’elles soient professionnelles ou scolaires.

Quant à moi, j’espère vous retrouver dans un prochain cours, à bientôt.

En résumé

- RADIUS vous permet de centraliser vos identifiants et mots de passe.
- Il s’agit d’un protocole client/serveur. Le serveur, RADIUS, gère les authentifications pour ses clients, routeurs et switchs.
- Il s’agit aussi d’un protocole AAA, qui signifie :
    - Authentification
    - Autorisation
    - Accounting (compte)
- Pour configurer RADIUS, il faut créer sur le serveur :
    - Un client
    - Un utilisateur
- Pour configurer RADIUS sur vos appareils CISCO, il faut :
    - Activer AAA

```
routeur2(config)# aaa new-model
```

    - Configurer le serveur RADIUS

```
routeur2(config)#radius-server host 223.0.2.8 key Cisco1234
```

Créer un groupe RADIUS

```
routeur2(config)#aaa authentication login default group radius local
```

Et pour finir, l'associer à une ligne

```
routeur2(config)#line vty 0 15 routeur2(configure-line)# login authentication default
```