NE424 – TP n° 3 – Serveur PPP et Radius

Christophe Deleuze

ESISAR – 2022/2023

1 Introduction

Lors de la séance précédente vous avez étudié PPP vu du côté utilisateur. Cette séance sera consacrée au côté fournisseur d'accès. Essentiellement, vous configurerez votre machine dans le rôle du NAS (network access server) d'un point d'accès.

Les indications données ici sont valables pour l'image Deb-CD-radius-2018.

Des étapes pour valider votre configuration sont données au fil du sujet. Vous devez exécuter **sur votre machine** la commande donnée avec les bons arguments. En cas de succès, une clé à mentionner dans votre rapport vous est indiquée. En cas d'échec, il faut déterminer ce qui ne va pas (la plupart du temps une analyse avec wireshark devrait vous permettre de déterminer ce qui ne se passe pas correctement).

2 Serveur PPP

P Parcourez les pages de manuel de pppoe et `pppoe-server` et déterminez comment respectivement sélectionner (côté client) et fixer (côté serveur) le nom du concentrateur d'accès. Notez aussi comment empêcher le serveur de devenir un *démon*.

Installez et configurez un serveur PPP(oE) sur votre station. [1] Comme chaque binome fera de même, il y aura plusieurs serveurs PPPoE dans la salle. Votre serveur pourra être identifié par son "nom de concentrateur d'accès" (`nomAC` dans la suite) pour lequel vous utiliserez votre login agalan (un par binome suffira). Vérifiez les logins connus dans la liste disponible en tapant `netcat 192.168.130.210 9999`. Autorisez l'accès à l'utilisateur du TP2 (`tpne424` et `motdepasse`).

Lancez le serveur par la commande `pppoe-server` en lui passant les options fixant son nom, une adresse IP autre que l'adresse par défaut 10.0.0.1, et le maintenant au premier plan (au lieu de devenir un *démon*). Vous pouvez observer ses messages de log dans le fichier `syslog` (`tail -f /var/log/syslog`).

Utilisez la machine `test` (par ssh, on vous donnera son adresse IP) pour tester votre serveur. Vous devrez fournir le nom du concentrateur d'accès, ce qui peut se faire avec l'incantation suivante :

```
pppd pty 'pppoe -C nomAC' noauth user tpne424 nodetach
```

Si cela réussit, vous pouvez mettre fin à la session en interrompant le processus par CTRL-c.

Validation 1. Configurez le serveur pour qu'il impose au client de s'authentifier avec PAP. Validez avec `tptest 1 nomAC`.

Validation 2. Configurez le serveur pour qu'il impose au client de s'authentifier avec EAP. Validez avec `tptest 2 nomAC`.

1. Le paquet debian pppoe contient à la fois un client et un serveur mais la commande pppoeconf est conçue pour configurer un client.

Validation 3. Configurez le serveur pour qu'il accepte de s'authentifier avec EAP uniquement. Validez avec `tptest 3 nomAC`. Votre serveur a les mêmes infos d'authentification que le serveur du TP2, il faut préciser son nom par l'option `user` dans le fichier de configuration.

Résumez dans votre rapport les configurations effectuées.

3 Serveur radius

P Parcourez le RFC2865. Dans le contexte de RADIUS, qu'appelle-t-on un *client* ? un *user* ? À quoi sert l'attribut `Framed-IP-Address` ?

Dans un `Access-Request`, comment le mot de passe du *user* (attribut `User-Password`) est-il protégé ?

3.1 Serveur de la salle

Un serveur radius est installé sur la machine 192.168.130.210, avec les informations d'authentification de différents utilisateurs. Configurez votre serveur PPP pour qu'il délègue l'authentification au serveur radius. Le mot de passe de ce serveur est `toto`.

Vous devrez pour cela :

— installer le paquet `libfreeradius-client2`[2],

— éditer le fichier `/etc/radiusclient/radiusclient.conf` pour indiquer l'adresse IP du serveur radius (`authserver`),

— éditer le fichier `/etc/radiusclient/servers` pour mettre sur une ligne l'adresse IP du serveur et son mot de passe,

— configurer le serveur PPP pour qu'il confie l'authenfication au serveur radius (voir la page de manuel `pppd-radius`). Pour cela il faut simplement ajouter l'option `plugin radius.so` dans le fichier d'options qui vous semble approprié...

— créer un fichier vide `/etc/radiusclient/port-id-map`.

Validation 4. `tptest 4 nomAC` permet de tester que vous déléguez correctement l'authentification. Relevez le diagramme d'échange montrant les interactions entre le client PPP, le serveur PPP et le serveur radius. Quel est l'utilisateur qui s'authentifie ?

Validation 5. `tptest 5 nomAC` fait la même chose pour un utilisateur qui fournit un mauvais mot de passe. Relevez le diagramme d'échange. Vous est-il possible de déterminer quel mot de passe est utilisé ?

Note : l'implémentation du serveur PPP que vous utilisez refuse obstinément de déléguer l'authentification au serveur radius dans le cas du protocole EAP... assurez-vous donc d'utiliser un autre protocole !

3.2 Serveur radius local

P Parcourez la page de manuel de l'outil `radtest`. Quelle valeur faut-il donner à l'argument `nas-port-number` ?

Installez maintenant un serveur radius sur votre machine. Résumé des opérations :

2. Ce paquet n'est plus disponible dans la distribution debian, mais vous pouvez le rapatrier à `http://192.168.130.202/~deleuzec/NE424-Radius/libfreeradius-client2_1.1.6-7_amd64.deb` et l'installer ensuite avec `dpkg -i libfreeradius-client2...`

— installer le paquet `freeradius`,
— le fichier `/etc/freeradius/3.0/clients.conf` liste les clients radius acceptés par le serveur et leurs mots de passe,
— le fichier `/etc/freeradius/3.0/users` contient les informations d'authentification et d'autorisation sur les utilisateurs (inspirez-vous du compte `steve`, les trois premières lignes suffisent).

Pour le tester, vous pouvez décommenter l'entrée `steve` dans `/etc/freeradius/3.0/users` et utiliser l'outil `radtest`. Ensuite, configurez le serveur PPP pour qu'il délègue l'authentification à votre serveur radius et créez l'utilisateur `tpne424` pour tester l'intégration.

Vous pouvez avoir intérêt à surveiller le fichier `/var/log/freeradius/radius.log`. Ne pas oublier de redémarrer freeradius avec `/etc/init.d/freeradius restart` !

Note : comme les deux serveurs sont sur la même machine, le trafic radius passera sur l'interface `lo` et non pas `eth0` (utiliser pour la capture la pseudo interface `any`).

Validation 6. `tptest 6 nomAC IPdevotremachine` permet de valider le bon fonctionnement. Pour que ce test fonctionne vous devez commencer par changer dans la section `log` du fichier `/etc/freeradius/3.0/radiusd.conf` le `auth=no` en `auth=yes`.

Le serveur radius peut-il fixer l'adresse IP qu'aura le user ? Montrez comment.

Note : si le serveur radius refuse votre configuration, une bonne façon de localiser l'erreur est de taper `freeradius -X`.

3.3 Délégation radius

Configurez maintenant votre serveur radius pour qu'il délègue l'authentification au serveur radius de la machine 192.168.130.210 dans le cas où l'utilisateur cherchant à s'authentifier est dans le *royaume* (realm) `prof.com`. Par exemple, le login de l'utilisateur sera `tpne424@prof.com`.

Pour cela vous devez éditer le fichier `/etc/freeradius/3.0/proxy.conf` et créer :
— un `home_server` pour le serveur radius 210,
— un `home_server_pool` contenant ce serveur,
— un royaume `prof.com` associé à ce *pool*.

Il y a beaucoup de paramètres possibles, ne mettez à priori que ceux qui vous semblent indispensables en vous inspirant des configurations existantes.

Validation 7. `tptest 7 nomAC` permet de tester que vous déléguez correctement l'authentification pour un utilisateur du royaume `prof.com`. Dessinez le diagramme d'échanges de paquets montrant les échanges entre :
— le client PPP
— le serveur PPP
— le serveur radius local
— le serveur radius de la salle

Validation 8. `tptest 8 nomAC` fait la même chose pour un utilisateur qui fournit un mauvais mot de passe. Faites la aussi le relevé.

3.4 Délégation radius encore (BONUS)

Associez vous à un (ou plusieurs) autre binome, créez chacun un royaume avec des utilisateurs et faites en sorte que les utilisateurs de chaque royaume puissent se connecter indifféremment à chaque point d'accès.