Le protocole IEEE 802.1x

Situation initiale et objectifs

Constat

Dans le chapitre précédent, nous avons passé en revue un certain nombre de solutions pour protéger les échanges sur la couche 2 du modèle OSI.

Pour être tout à fait exhaustif, résumons dans un tableau les avantages et inconvénients de ces solutions :

Solution	Avantages	Inconvénients
Port security	Une adresse MAC autorisée par port.	Une adresse MAC autorisée par port :-)
	Possibilité de rajouter des adresses MAC	Risque d'être trop laxiste avec le nombre d'adresses autorisées pour ne pas être dérangé trop souvent
	Empêche de squatter toute la plage DHCP	Peu souple ni adapté à un réseau de taille respectable
		Ne protège pas contre l'usurpation préalable de l'adresse MAC autorisée
DHCP Snooping + DAI + IP Source Guard	Solution permettant de contrôler la connexion des hôtes par adresse MAC adresse IP et par port	Contraignants à mettre en place, nécessite un paramétrage avancé et de nombreux ajustements en cours d'exploitation
		Nécessite un serveur DHCP
	Efficace contre le DHCP spoofing	Administration sans souplesse, n'autorise pas les postes de travail nomades non déclarés préalablement
		Ne protège pas contre l'usurpation préalable de l'adresse MAC autorisée
VLAN niveau 1	Permet d'isoler les flux logiquement sans modifier la configuration physique du réseau	Paramétrage long et fastidieux au démarrage et on doit tout de même modifier les branchements sur les commutateurs en cas de modification de la configuration
	Déploiement rapide avec VTP	Quid des PC portables ?
	Routage réglable au cas par cas depuis un routeur compatible 802.1q	Impose un contrôle d'accès aux prises réseaux
VLAN niveau 2	Mêmes avantages avec possibilité d'administrer de manière centralisée la liste des adresses MAC autorisées	Impose l'installation d'au moins un service VMPS sur un hôte du réseau
	Plus besoin de modifier les branchements sur les commutateurs	Ne protège pas contre l'usurpation préalable de l'adresse MAC autorisée...

Force est de constater que l'ensemble de ces solutions n'est pas encore satisfaisant.

Objectifs

Et nous voulons :

- une administration centralisée ; - n'avoir à modifier les branchements qu'exceptionnellement ; - authentifier de manière sûre et identifier avec certitude les hôtes qui se connectent au réseau.

C'est alors que le protocole 802.1x vient répondre à nos attentes.

Fonctionnement du protocole 802.1x

La norme 802.1x [1)] permet l'authentification d'un hôte sur le réseau **avant tout autre échange**, lors de la connexion de l'interface de l'hôte sur un équipement du réseau.

PAE et relais d'authentification

Nous ne sommes plus dans le cas d'une authentification d'interface par adresse MAC mais dans l'authentification d'un utilisateur qui connecte son équipement informatique à un point d'accès au réseau (PAE[2)]).

Dans le cas présent nous le trouverons dans nos commutateurs Cisco 2960 qui jouerons le rôle de relais d'authentification.

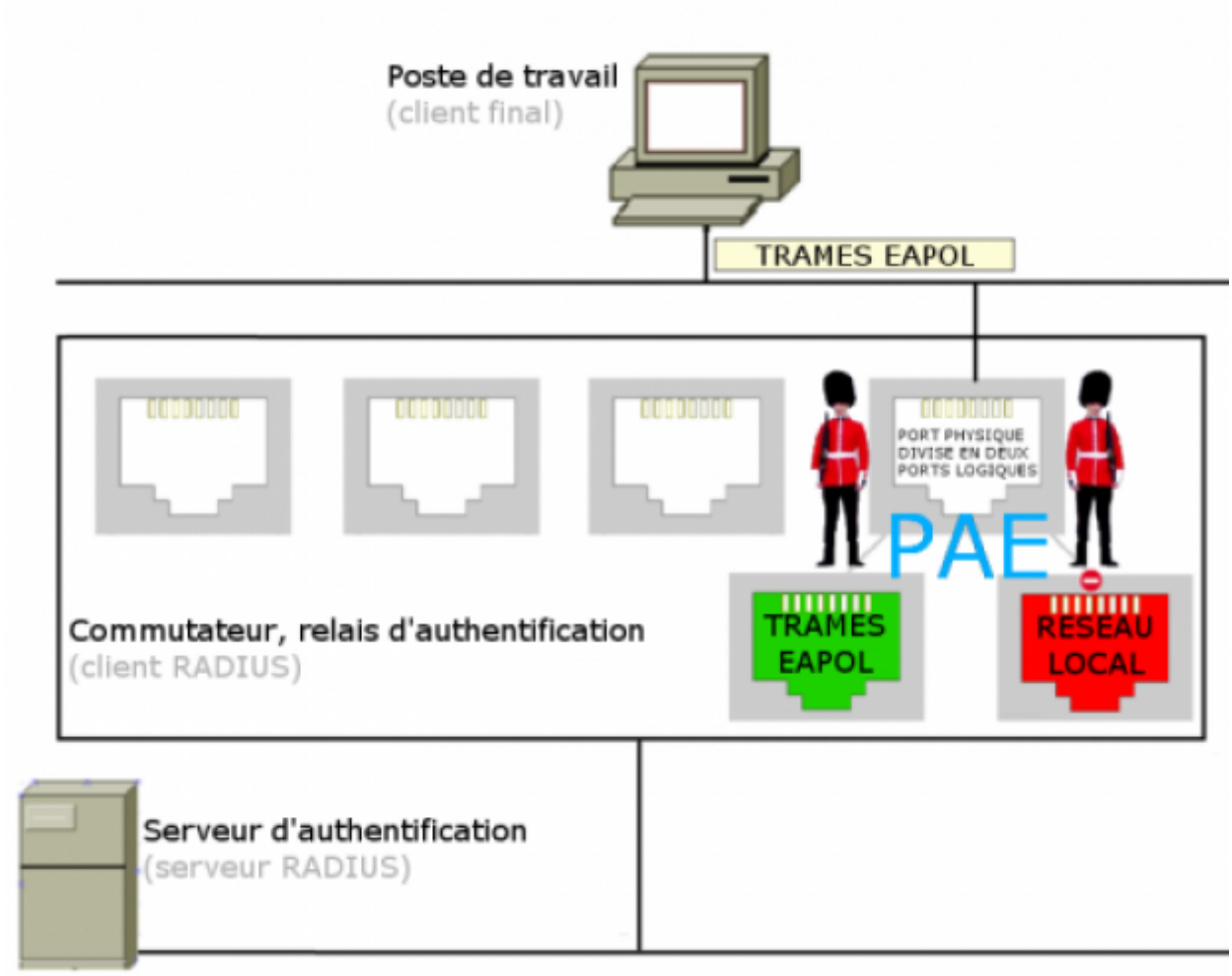
Le port physique d'accès au commutateur ne change pas mais **le PAE “divise” ce port en deux ports logiques** :

- un port permettant l'authentification de l'utilisateur; - un port contrôlé qui bloque ou débloque l'accès au réseau en fonction de l'état de l'authentification.

Pour que cette authentification se réalise, il faudra que le relais d'authentification *(notre commutateur)* soit client d'un serveur d'authentification en mesure de contrôler les accès. Ils communiquent entre eux en s'appuyant sur le protocole EAP[3)] définit par la RFC 3748[4)].

- Les paquets EAP sont transportés dans des trames EAPOL sur la couche 2 Ethernet *(EAP over LAN)* lorsqu'une station de travail se connecte au client RADIUS *(le commutateur)* via sur une prise réseau filaire (à l'exclusion de toute autre trame). - Les paquets EAP sont transportés dans des trames EAP over Radius le client et le serveur RADIUS.

Le schéma suivant résume la connexion d'un hôte au réseau :



Résumé très succinct du mécanisme d'accès au réseau :

1. Branchement physique de l'interface de l'hôte sur une prise réseau murale;
2. Le commutateur détecte le branchement et envoie une requête d'identification à l'hôte;
3. L'hôte transmet son identité au commutateur;
4. Le commutateur en informe le serveur d'authentification;
5. Le serveur d'authentification transmet une requête d'authentification au commutateur qui la transmet à l'hôte;
6. L'hôte comprend cette requête (méthode) sinon on recommence la transaction avec les autres méthodes disponibles;
7. L'hôte envoie ses paramètres d'authentification;
8. Le commutateur envoie ces éléments au serveur d'authentification;
9. Le serveur d'authentification vérifie l'accès et renvoie le résultat au commutateur;
10. Succès de l'authentification : le PAE débloque l'accès au réseau et l'hôte peut communiquer sur le réseau local;
11. (10 bis) Échec de l'authentification : le PAE maintient le blocage du port et on peut définir un temps d'attente avant la prochaine demande de connexion pour se prémunir d'une attaque par force brute;

Dans la suite de ce chapitre, nous allons répondre à ces questions:

- Qu'est ce qu'un serveur d'authentification? - Quelles sont les différentes méthodes d'authentification? - Que se passe-t-il en cas de branchement d'un commutateur sur ce port? Et pour un concentrateur? - Peut-on placer dans un “VLAN pour invités”, des hôtes n'ayant pas d'accès (ex :

attribuer adresse IP et accès vers un portail captif)? - Comment connecter un hôte qui ne gère pas 802.1x (téléphone IP, imprimante *~~ou pire encore: un hôte sous wind~~*... non, rien 😉) - Pourrai-je vérifier les accès dans mon annuaire LDAP? - Y-a-t-il des failles dans 802.1x et le cas échéant, lesquelles et comment s'en prémunir?

Serveur d'authentification

Le serveur d'authentification est capable de vérifier l'authentification d'un hôte sur le réseau: il peut posséder sa propre base de données d'utilisateurs autorisés ou aller chercher ces éléments dans un annuaire.

Pour l'authentification des utilisateurs, nous utiliserons un serveur RADIUS[5] définit par la RFC 2866 *(à la fin de la démonstration on installera un NPS[6] avec Windows Server et un annuaire Active Directory)*.

Configuration des commutateurs clients RADIUS

Nous allons reconfigurer proprement nos commutateurs pour être capable de faire communiquer les hôtes avec le serveur RADIUS:

- Déclaration des VLAN en rajoutant un VLAN spécifique pour la communication avec le serveur RADIUS et un VLAN “poubelle” pour les hôtes qui n'ont pas les droits pour se connecter; - Mise en place de VTP; - Attribuer une adresse IP à l'interface virtuelle 'vlan 50' afin que le commutateur soit reconnu comme client par le serveur RADIUS; - Taguer les ports entre commutateurs; - Paramétrer la connexion avec le serveur RADIUS; - Attribuer automatiquement un VLAN en fonction de l'utilisateur autorisé; - Attribuer un VLAN “voie de garage” pour tous les autres (par précaution car le port reste en réalité désactivé);

Configuration du commutateur SW1 :

```
SW1(config)#vlan 10                                   ! Déclaration des VLAN
SW1(config-vlan)#name secretariat
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name comptabilite
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name direction
SW1(config-vlan)#vlan 40
SW1(config-vlan)#name commerciaux
SW1(config)#vlan 50                                   ! VLAN radius
SW1(config-vlan)#name radius
SW1(config)#vlan 900                                  ! VLAN poubelle
SW1(config-vlan)#name poubelle
SW1(config-vlan)#exit
SW1(config)vtp domain corpora.te                      ! VTP
Changing VTP domain name from NULL to corpora.te

SW1(config)#vtp password zaBTpaYTpo
Setting device VTP password to zaBTpaYTpo
```

```
SW1(config)#vtp mode server
SW1(config)#interface vlan 50                    ! IP sur interface vlan
50
*Mar  1 04:26:21.312: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan50, changed state to down
SW1(config-if)#ip address 10.50.0.1 255.255.0.0
SW1(config-if)#no sh
SW1(config)#interface vlan 10                    ! IP sur interface vlan
10
SW1(config-if)#ip address 10.10.0.1 255.255.0.0
SW1(config-if)#ip helper-address 10.50.19.77          ! On précise
l'adresse du routeur serveur DHCP
SW1(config-if)#no sh
SW1(config)#interface vlan 20                    ! IP sur interface vlan
20
SW1(config-if)#ip address 10.20.0.1 255.255.0.0
SW1(config-if)#ip helper-address 10.50.19.77          ! On précise
l'adresse du routeur serveur DHCP
SW1(config-if)#no sh
SW1(config)#interface vlan 30                    ! IP sur interface vlan
30
SW1(config-if)#ip address 10.30.0.1 255.255.0.0
SW1(config-if)#ip helper-address 10.50.19.77          ! On précise
l'adresse du routeur serveur DHCP
SW1(config-if)#no sh
SW1(config)#interface vlan 40                    ! IP sur interface vlan
40
SW1(config-if)#ip address 10.40.0.1 255.255.0.0
SW1(config-if)#ip helper-address 10.50.19.77          ! On précise
l'adresse du routeur serveur DHCP
SW1(config-if)#no sh
SW1(config-if)#interface fa0/1                   ! Tag des ports reliés
aux commutateurs et au routeur
SW1(config-if)#switchport mode trunk
SW1(config-if)#interface range fa0/23-24
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#exit
SW1(config)#aaa new-model                        ! Activation du protocole
802.1x
SW1(config)#aaa authentication dot1x default group radius
SW1(config)#aaa authorization network default group radius
SW1(config)#dot1x system-auth-control            ! Declaration du serveur
ci-dessous
SW1(config)#radius-server host 10.50.0.10 auth-port 1812 acct-port 1813 key
jpeuxpasjaiponey
SW1(config)interface range fa0/2-22
SW1(config-if-range)switchport mode access
SW1(config-if-range)switchport access vlan 900        ! Tout le monde dans
le VLAN 900 par défaut, aucun droit.
SW1(config-if-range)authentication port-control auto
SW1(config-if-range)dot1x pae authenticator
```

“aaa” pour “Authentication, Authorization & Accounting”

Il nous reste à faire de même sur SW2 et SW3!… Pour le commutateur SW2 :

```
SW2(config)vtp domain corpora.te                    ! VTP
Changing VTP domain name from NULL to corpora.te

SW2(config)#vtp password zaBTpaYTpo
Setting device VTP password to zaBTpaYTpo
SW2(config)#vtp mode client
SW2(config)#interface fastEthernet 0/2              ! Attribution du VLAN 50
au port connecté au serveur RADIUS
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 50
SW2(config-if)#interface fa0/1                      ! Tag des ports reliés
aux commutateurs
SW2(config-if)#switchport mode trunk
SW2(config-if)#interface fa0/24
SW2(onfig-if)#switchport mode trunk
SW2(config-if)#interface vlan 50                    ! IP sur interface vlan
50
*Mar  1 04:45:22.117: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan50, changed state to down

SW2(config-if)#ip address 10.50.0.2 255.255.0.0
SW2(config-if)#no sh
SW2(config-if)#ip helper-address 10.50.19.77
SW2(config)#interface vlan 10                       ! IP sur interface vlan
10
SW2(config-if)#ip address 10.10.0.1 255.255.0.0
SW2(config-if)#ip helper-address 10.50.19.77
SW2(config-if)#no sh
SW2(config)#interface vlan 20                       ! IP sur interface vlan
20
SW2(config-if)#ip address 10.20.0.1 255.255.0.0
SW2(config-if)#ip helper-address 10.50.19.77
SW2(config-if)#no sh
SW2(config)#interface vlan 30                       ! IP sur interface vlan
30
SW2(config-if)#ip address 10.30.0.1 255.255.0.0
SW2(config-if)#ip helper-address 10.50.19.77
SW2(config-if)#no sh
SW2(config)#interface vlan 40                       ! IP sur interface vlan
40
SW2(config-if)#ip address 10.40.0.1 255.255.0.0
SW2(config-if)#ip helper-address 10.50.19.77
SW2(config-if)#no sh
SW2(config-if)#exit
SW2(config)#aaa new-model                           ! Activation du protocole
802.1x
SW2(config)#aaa authentication dot1x default group radius
```

```
SW2(config)#aaa authorization network default group radius
SW2(config)#dot1x system-auth-control              ! Declaration du serveur
ci-dessous
SW2(config)#radius-server host 10.50.0.10 auth-port 1812 acct-port 1813 key
jpeuxpasjaiponey
SW2(config)interface range fa0/3-22
SW2(config-if-range)switchport mode access
SW2(config-if-range)switchport access vlan 900          ! Tout le monde dans
le VLAN 900 par défaut, aucun droit.
SW2(config-if-range)authentication port-control auto
SW2(config-if-range)dot1x pae authenticator
```

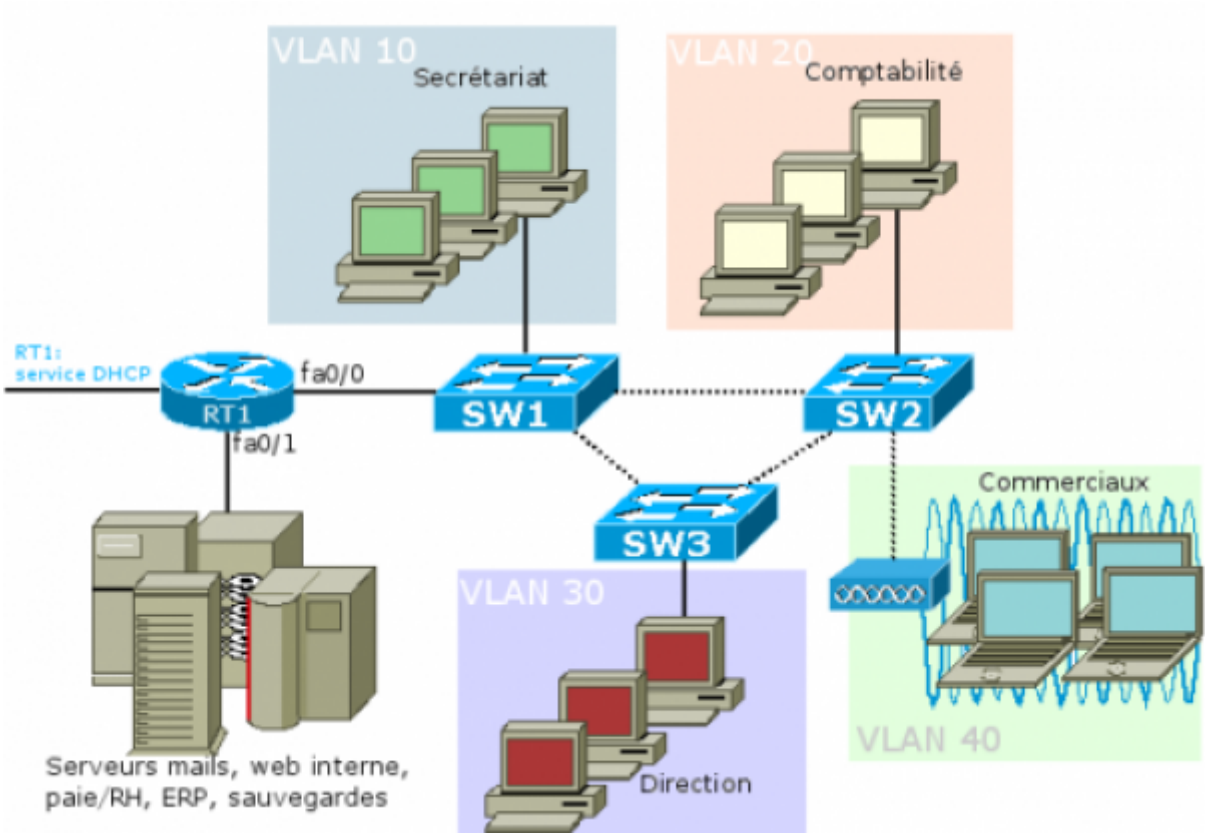
Et enfin pour le commutateur SW3 :

```
SW3(config)vtp domain corpora.te                    ! VTP
Changing VTP domain name from NULL to corpora.te

SW3(config)#vtp password zaBTpaYTpo
Setting device VTP password to zaBTpaYTpo
SW3(config)#vtp mode client
SW3(config-if)#interface fa0/1                      ! Tag des ports reliés
aux commutateurs
SW3(config-if)#switchport mode trunk
SW3(config-if)#interface fa0/24
SW3(onfig-if)#switchport mode trunk
SW3(config-if)#interface vlan 50                    ! IP sur interface vlan
50
*Mar  1 04:48:41.103: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan50, changed state to down

SW3(config-if)#ip address 10.50.0.3 255.255.0.0
SW3(config-if)#no sh
SW3(config)#interface vlan 10                       ! IP sur interface vlan
10
SW3(config-if)#ip address 10.10.0.1 255.255.0.0
SW3(config-if)#ip helper-address 10.50.19.77
SW3(config-if)#no sh
SW3(config)#interface vlan 20                       ! IP sur interface vlan
20
SW3(config-if)#ip address 10.20.0.1 255.255.0.0
SW3(config-if)#ip helper-address 10.50.19.77
SW3(config-if)#no sh
SW3(config)#interface vlan 30                       ! IP sur interface vlan
30
SW3(config-if)#ip address 10.30.0.1 255.255.0.0
SW3(config-if)#ip helper-address 10.50.19.77
SW3(config-if)#no sh
SW3(config)#interface vlan 40                       ! IP sur interface vlan
40
SW3(config-if)#ip address 10.40.0.1 255.255.0.0
SW3(config-if)#ip helper-address 10.50.19.77
```

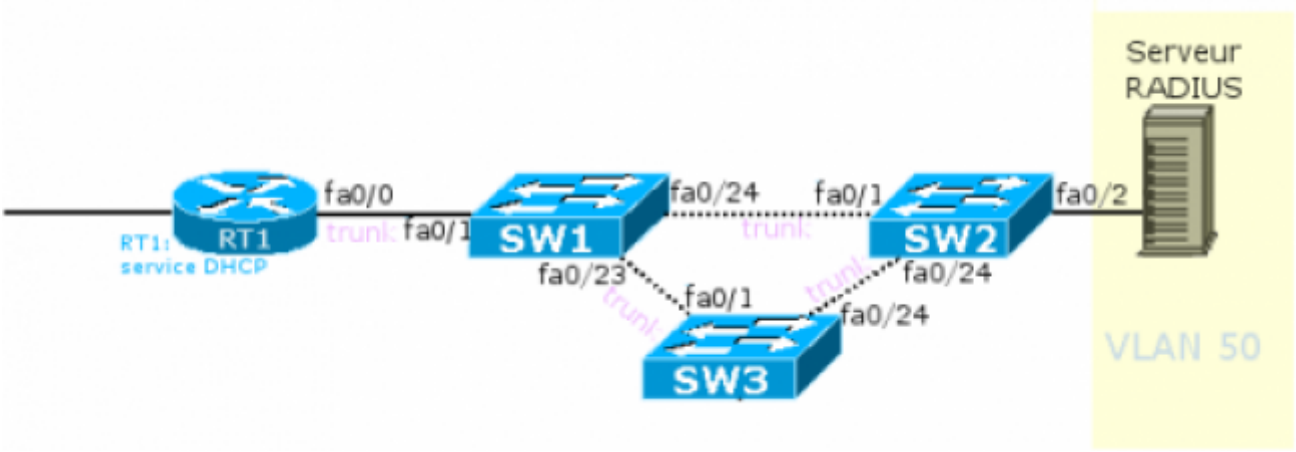
```
SW3(config-if)#no sh
SW3(config-if)#exit
SW3(config)#aaa new-model                              ! Activation du protocole
802.1x
SW3(config)#aaa authentication dot1x default group radius
SW3(config)#aaa authorization network default group radius
SW3(config)#dot1x system-auth-control                  ! Declaration du serveur
ci-dessous
SW3(config)#radius-server host 10.50.0.10 auth-port 1812 acct-port 1813 key
jpeuxpasjaiponey
SW3(config)interface range fa0/2-23
SW3(config-if-range)switchport mode access
SW3(config-if-range)switchport access vlan 900          ! Tout le monde dans
le VLAN 900 par défaut, aucun droit.
SW3(config-if-range)authentication port-control auto
SW3(config-if-range)dot1x pae authenticator
```

La configuration (running conf) de SW1 à copier/coller se trouve sur ce lien.
La configuration (running conf) de SW2 à copier/coller se trouve sur ce lien.
La configuration (running conf) de SW3 à copier/coller se trouve sur ce lien

Nous avions ça :



Nous avons maintenant configuré les commutateurs et allons installer le serveur RADIUS pour obtenir ça :



Installation et configuration du serveur RADIUS

Installation

FreeRadius[7] est un outil OpenSource[8] relativement simple à mettre en place. Nous allons l'installer sur un serveur Debian 8 qui nous servait précédemment de serveur DHCP *(service maintenant délivré par le routeur RT1)*

Pour l'installer, on récupère et décompresse la dernière version de FreeRadius:

```
#mkdir radius && cd radius
#wget
ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.12.tar.gz
Ouverture de session en anonymous...Session établie!
==> SIZE freeradius-server-3.0.12.tar.gz ... 4767418
==> PASV ... complété.    ==> RETR freeradius-server-3.0.12.tar.gz ...
complété.
Taille: 4767418 (4,5M) (non certifiée)
100%
[=====================================================================>]
4 767 418   --.-K/s   ds 0,06s
#tar xfz *gz
#cd freeradius-server-3.0.12
```

Puis l'installation se fait traditionnellement avec `./configure` puis `make` et `make install` (installer les éventuelles dépendances manquantes (*elles seront précisées lors de l'installation)*.

Configuration

Chez corpora.te tous les hôtes sont sous Windows  ... nous allons faire en sorte qu'ils puissent se connecter avec un login et un mot de passe *(différent dans un premier temps de leur mot de passe de session)*.

Nous avons 4 fichiers à configurer dans `/etc/freeradius` : `radiusd.conf` pour le serveur lui-même, `users` pour la liste des utilisateurs, `clients.conf` pour la liste des clients RADIUS et enfin

eap.conf pour la méthode d'authentification utilisée par les hôtes :

Configuration de `clients.conf`:

```
client 10.50.0.1 {
       shortname = SW1
       secret = jpeuxpasjaiponey
       shortname = LAN
}
  client 10.50.0.2 {
       shortname = SW2
       secret = jpeuxpasjaiponey
       shortname = LAN
}
client 10.50.0.3 {
       shortname = SW3
       secret = jpeuxpasjaiponey
       shortname = LAN
}
```

Remarque : Nous aurions pu désigner les clients RADIUS avec leur réseau commun 10.50.0.0/16 dans la mesure où ils partagent la même clé secrète mais je préfère rester parcimonieux.

Configuration de `users` *(un seul utilisateur pour l'instant, le directeur Monsieur Pignon, auquel est affécté le VLAN 30)* :

```
f.pignon Cleartext-Password := "motdepassereseau"
         Tunnel-Type = VLAN,
         Tunnel-Medium-Type = IEEE802,
         Tunnel-Private-Group-ID = 30
         Reply-Message = "Bienvenue chez corpora.te !!"
```

Pour la configuration de `radius.conf`, nous vérifions la présence de ces options pour loguer les tentatives d'accès :

```
stripped_named = yes
auth = yes
auth_badpass= yes
auth_goodpass = yes
```

Configuration de `eap.conf` : on va s'assurer que les blocs commençant par `eap`, `md5` et `ttls` ne sont pas commentés pour permettre l'établissement d'un tunnel chiffré *(garantissant que le mot de passe ne transite pas en clair)*. On rajoutera également ce bloc pour utiliser la méthode PEAP que nous allons voir avec la configuration de l'hôte plus loin dans le chapitre :

```
peap {
       default_eap_type = mschapv2
       copy_request_to_tunnel = yes
       user_tunneled_reply = yes
       virtual_server = "inner-tunnel"
```

```
        }
```

Nous n'avons plus qu'à démarrer notre serveur : `service freeradius start`

Configuration d'un hôte

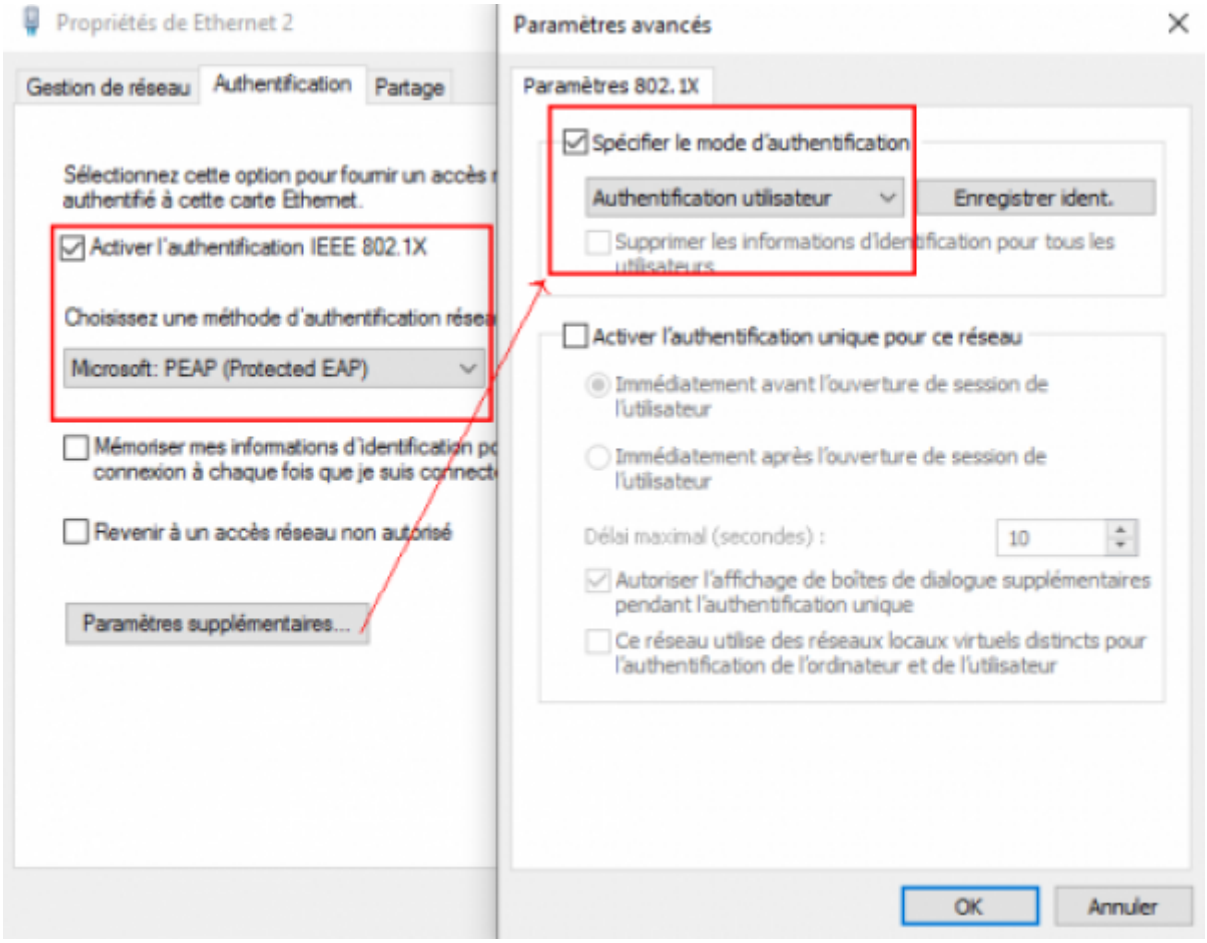
Nous allons tenter de connecter l'ordinateur de Monsieur Pignon au réseau local depuis un bureau du secrétariat.

Méthode MSCHAPv2 et PEAP

La méthode MSchapv2 est un échange entre le serveur RADIUS et l'hôte permettant une authentification au moyen d'un identifiant de session, du login et mot de passe de l'hôte et de hachage de chaînes aléatoires. PEAP sécurise le transfert de ces informations sans utiliser de certificat.

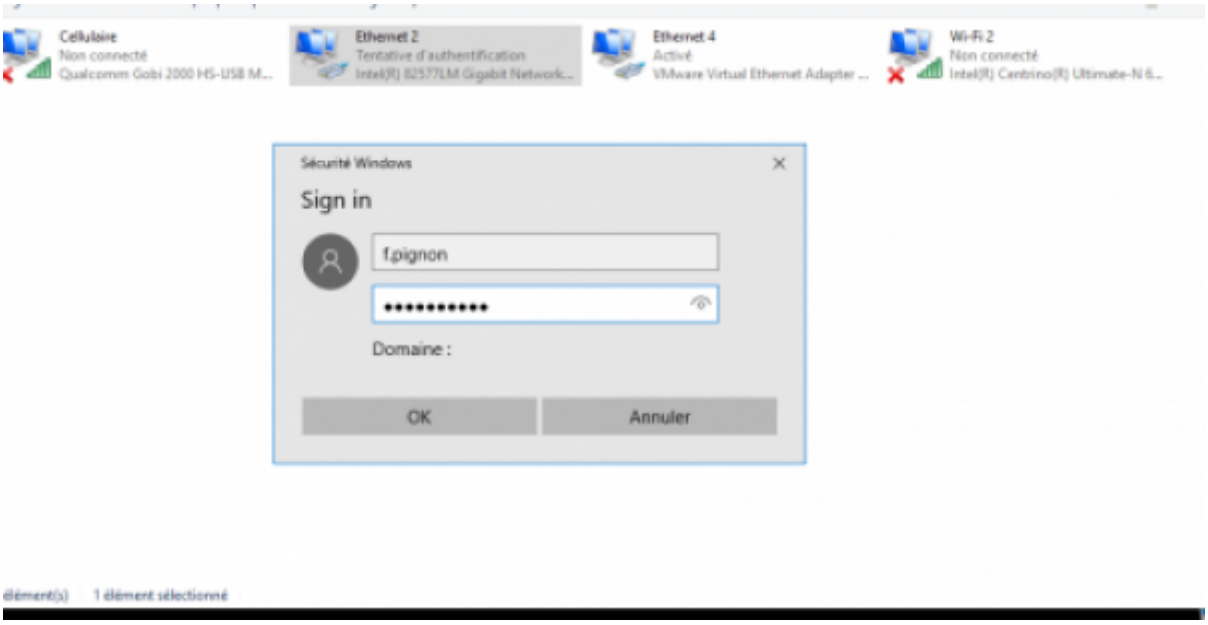
Nous allons configurer l'hôte de cette manière:

- Dans les services (services.msc), démarrer le service “configuration automatique de réseau câblé”; - Régler les propriétés de l'interface réseau comme suit (sans modifier la configuration automatique DHCP)



Nous connectons l'ordinateur à la prise murale et une boîte de dialogue apparaît dans laquelle M.

Pignon rentre ses identifiants:



et voici Monsieur Pignon connecté au réseau, dans le VLAN 30 comme on peut le voir sur le commutateur simultanément :

```
SW1>
*Mar  1 04:56:22.925: %DOT1X-5-SUCCESS: Authentication successful for client
(f0de.f157.d739) on Interface Fa0/5 AuditSessionID 0A320100000000026010E6D37
*Mar  1 04:56:22.925: %AUTHMGR-7-RESULT: Authentication result 'success'
from 'dot1x' for client (f0de.f157.d739) on Interface Fa0/5 AuditSessionID
0A320100000000026010E6D37
*Mar  1 04:56:22.925: %AUTHMGR-5-VLANASSIGN: VLAN 30 assigned to Interface
Fa0/5 AuditSessionID 0A320100000000026010E6D37
*Mar  1 04:56:22.950: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan30, changed state to up
*Mar  1 04:56:23.957: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(f0de.f157.d739) on Interface Fa0/5 AuditSessionID 0A320100000000026010E6D37
```

Vérifions sur les logs du serveur RADIUS :

```
[eap] Request found, released from the list
[eap] EAP/mschapv2
[eap] processing type mschapv2
[mschapv2] # Executing group from file /etc/freeradius/sites-enabled/inner-
tunne
[mschapv2] +group MS-CHAP {
[mschap] Creating challenge hash with username: f.pignon
[mschap] Client is using MS-CHAPv2 for f.pignon, we need NT-Password
[mschap] adding MS-CHAPv2 MPPE keys
....
....
[peap] Got tunneled reply RADIUS code 2
      Tunnel-Type:0 = VLAN
      Tunnel-Medium-Type:0 = IEEE-802
```

```
      Tunnel-Private-Group-Id:0 = "30"
      MS-MPPE-Encryption-Policy = 0x00000001
      MS-MPPE-Encryption-Types = 0x00000006
      MS-MPPE-Send-Key = 0x79363c02b8f595f211b2778eccb656d5
      MS-MPPE-Recv-Key = 0x1f1fbab78c2035f57329333ad7f2be3d
      EAP-Message = 0x03090004
      Message-Authenticator = 0x00000000000000000000000000000000
      User-Name = "f.pignon"
[peap] Tunneled authentication was successful.
[peap] SUCCESS
```

Méthode par certificat

Nous allons générer un certificat avec Windows Server dans la section suivante.

802.1x et Active Directory

Organisation de l'annuaire

Corporate a évolué et s'est doté d'un contrôleur de domaine Windows Server 2003 (*serv-win.corpora.te*) qui fera office de serveur RADIUS. Il conserve l'adresse de l'ancien serveur freeradius (10.50.0.10). Le contrôleur de domaine dispose d'un service d'annuaire comportant :

- Les utilisateurs du domaine se trouvent dans l'OU *Utilisateurs* puis dans les “sous-unités”:
  - Direction
  - Comptabilite
  - Secretariat
  - Commerciaux
- Les utilisateurs du domaines sont également respectivement membres des groupes direction,comptabilité,secretariat ou commerciaux afin d'affecter un VLAN par groupe par la suite.

Configuration du serveur

Contrairement à ce qui a été dit plus haut, nous n'utiliserons pas un service NPS (à partir de Windows server 2008) mais IAS (Internet Access Service) à cause du niveau fonctionnel de notre forêt (Windows server 2003). Globalement nous allons faire la même chose : être le “fournisseur d'accès” réseau de nos hôtes.

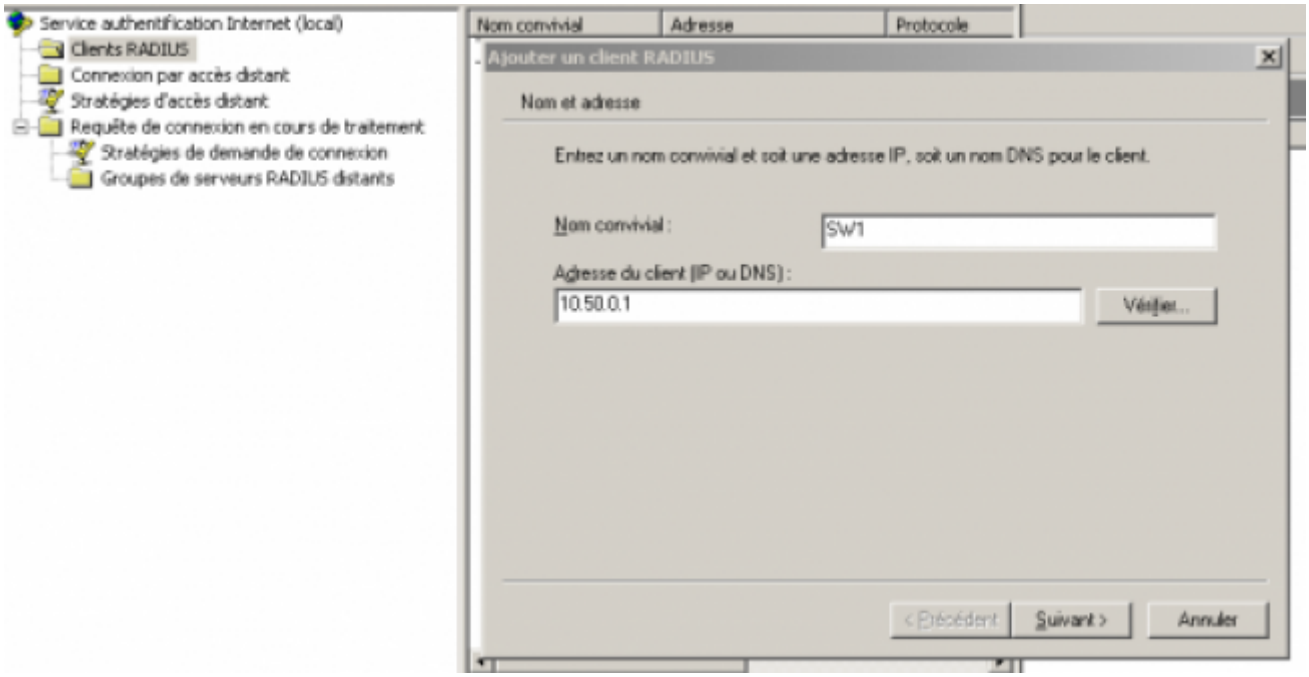
Internet Authentication Service

Notre serveur va donc fournir un service d'accès réseau. Au préalable nous allons générer un

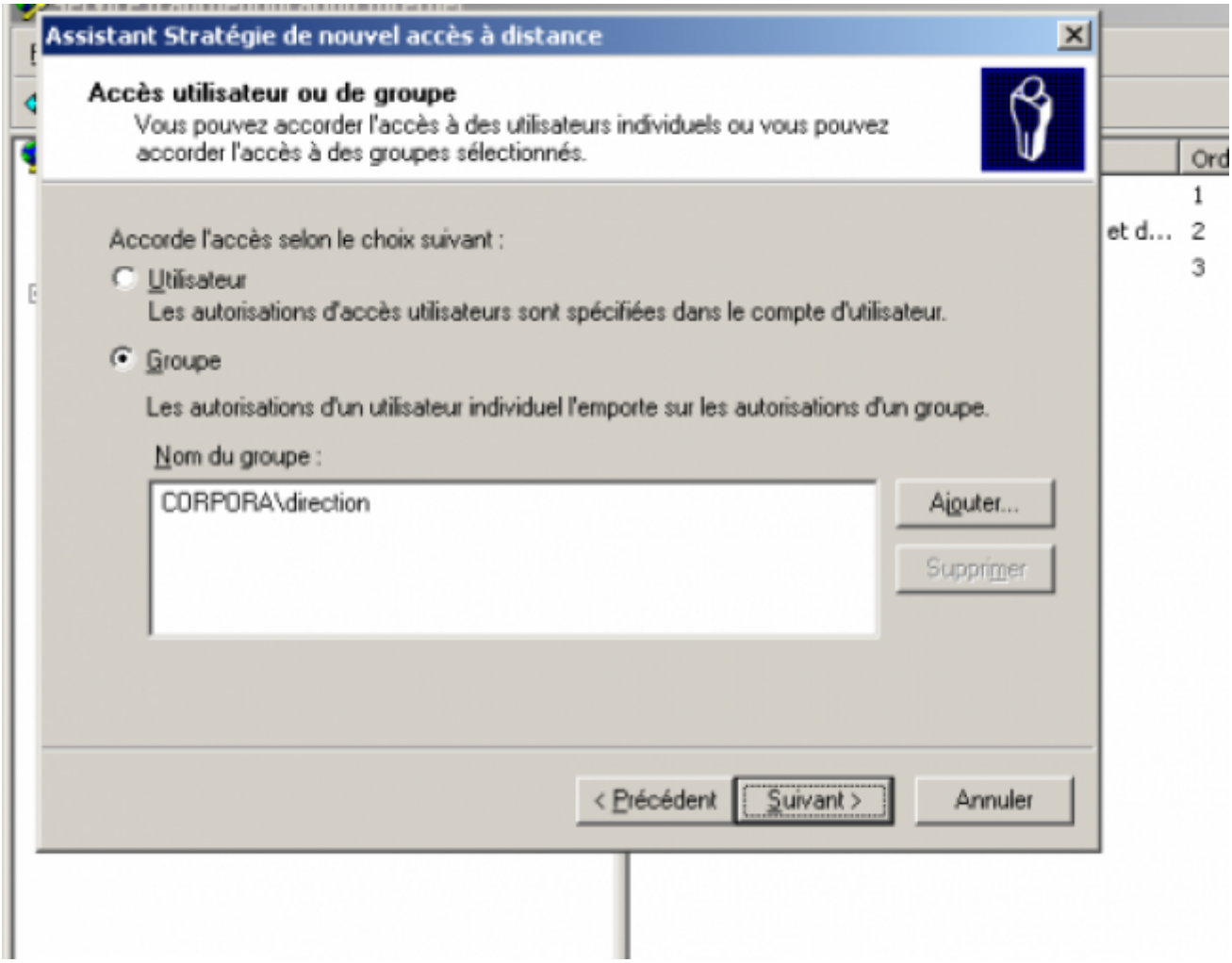
certificat d'une durée d'un an (décidée aribitrairement, 5 jours par défaut) afin d'identifier le serveur auprès de ses futurs clients :

```
selfssl /t /v:365
(on choisit le seul serveur disponible le %1).
```

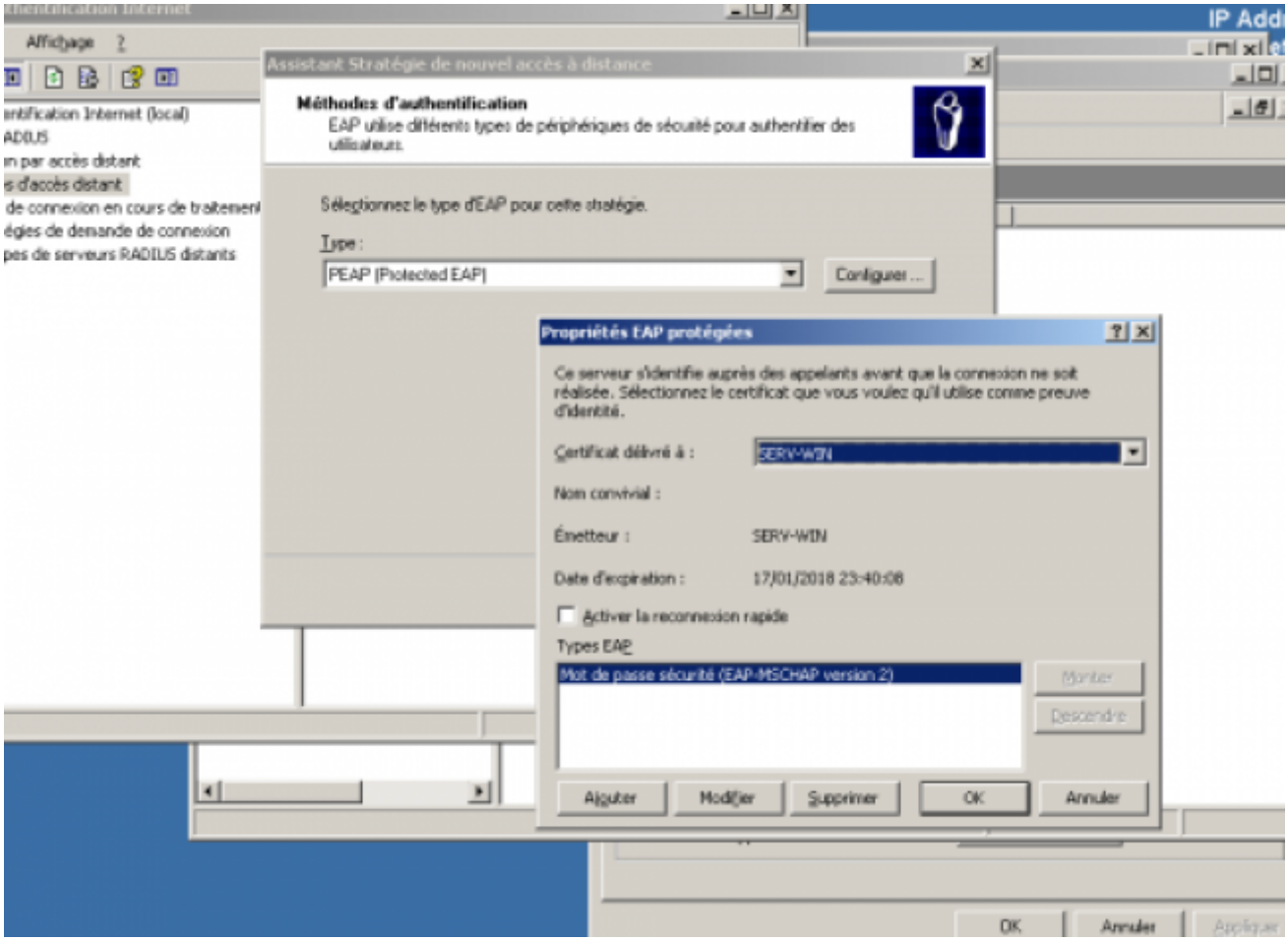
Nous allons maintenant configurer le service. Dans les outils d'administration, choisir Internet Authentification Service, puis déclarer les 3 clients RADIUS à savoir les commutateurs SW1, SW2 et SW3 :



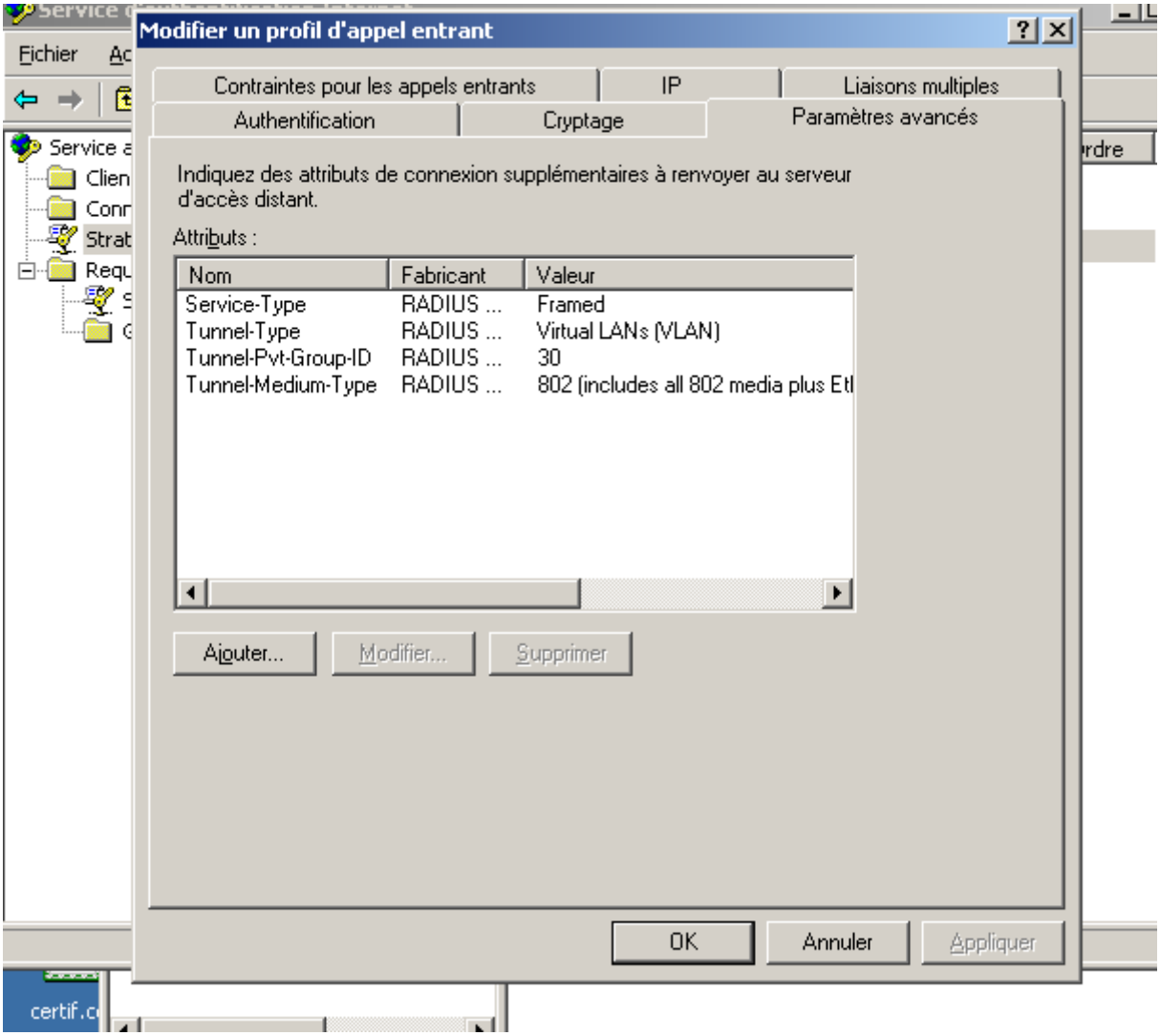
Nous allons ensuite créer autant de stratégie de connexion distante qu'il y a de VLAN. Pour la direction :



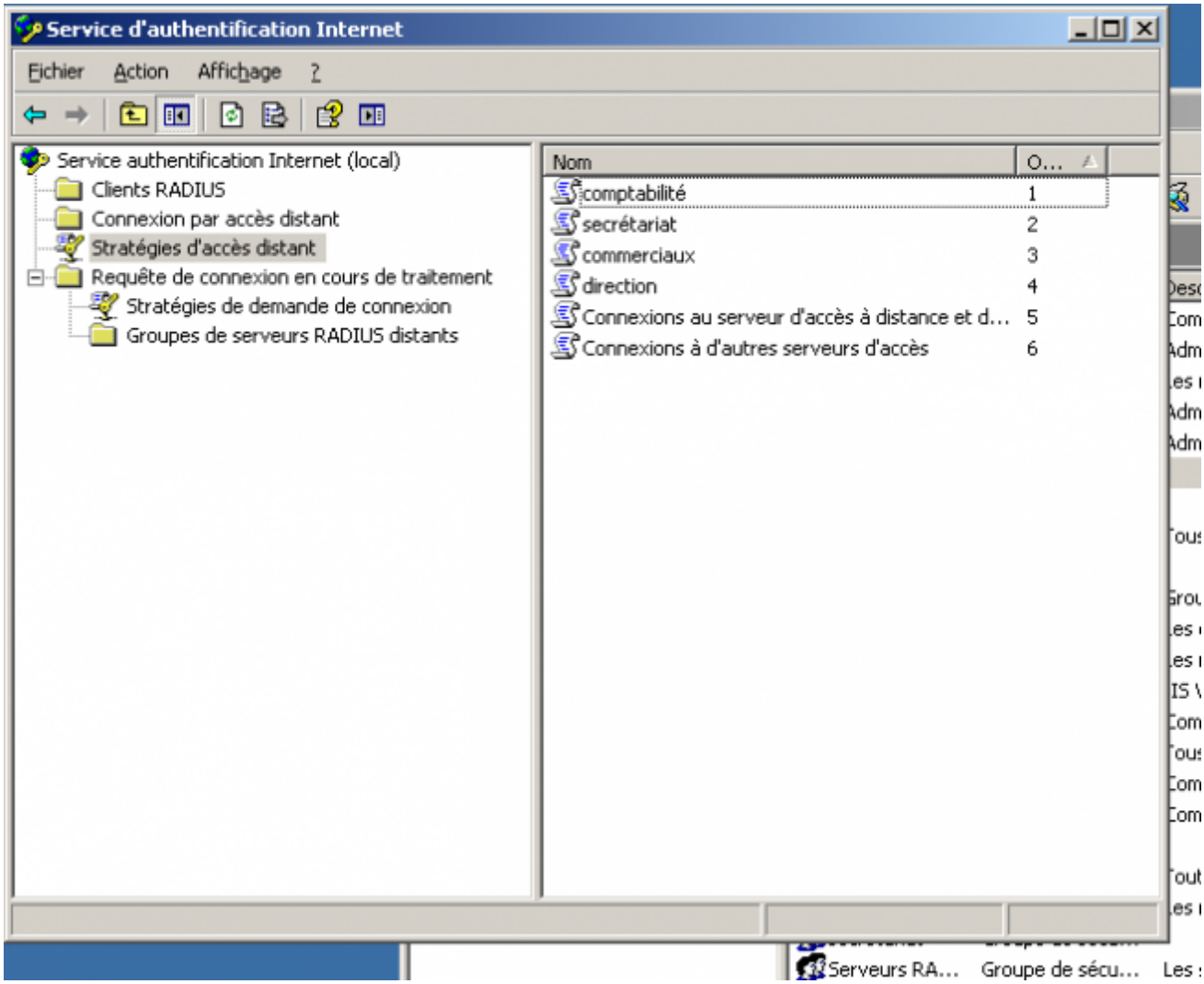
Nous choisissons ensuite la méthode PEAP avec certificat pour la connexion des clients en désignant le certificat que l'on a créé:



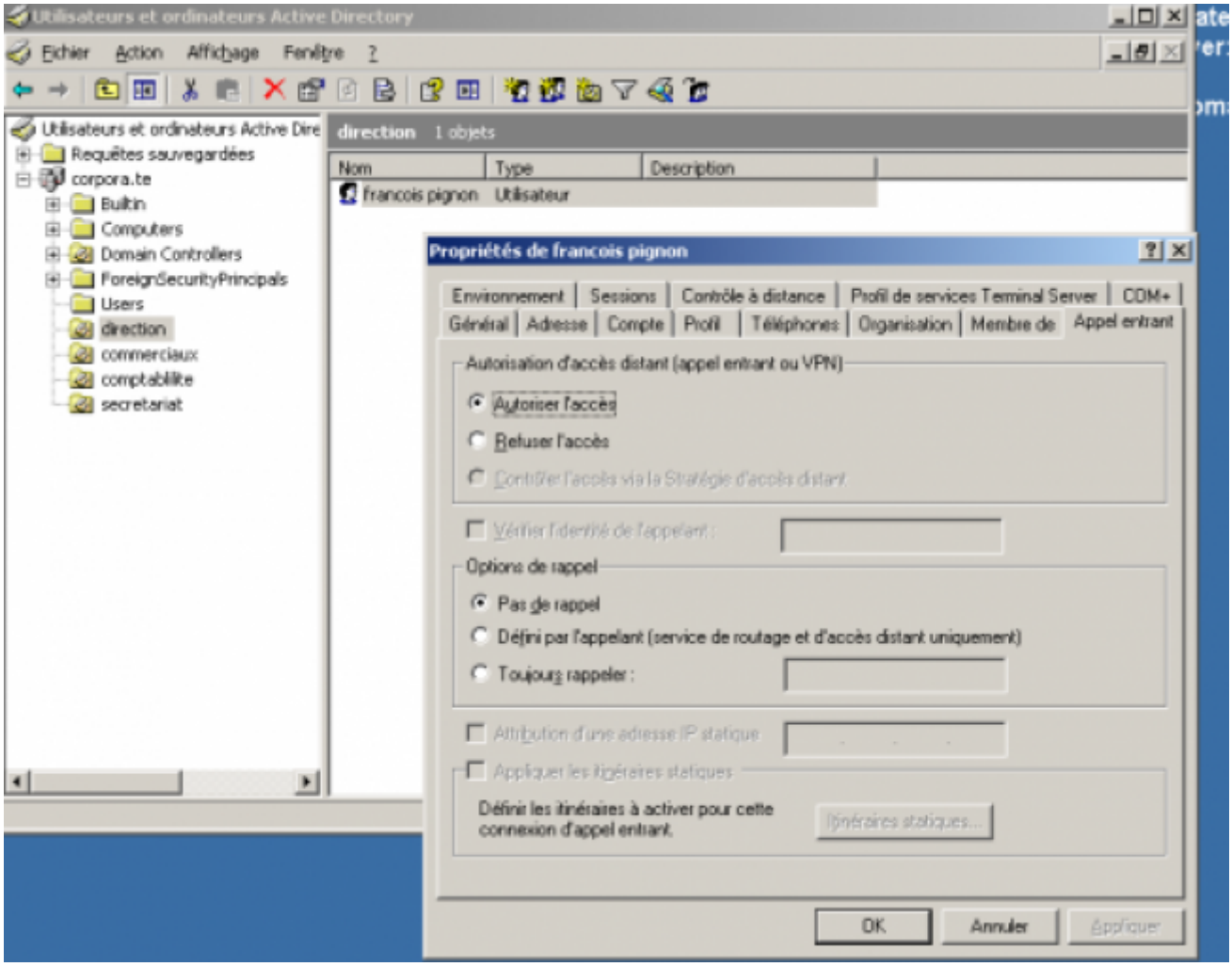
Enfin, nous rajoutons les options suivantes pour que les utilisateurs du groupe direction soient connectés au VLAN 30 :



Faire de même avec les groupes commerciaux pour le VLAN 20, le groupe secretariat pour le VLAN 10 et le groupe commerciaux pour le VLAN 40 :



Il ne faudra pas oublier de permettre à chaque utilisateur de se connecter en activant cette option dans l'annuaire :

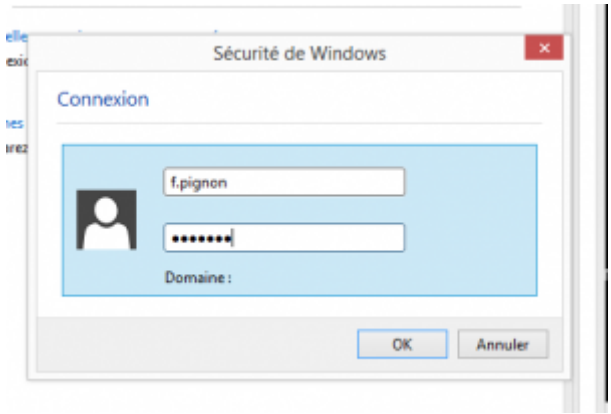


Configuration de l'hôte

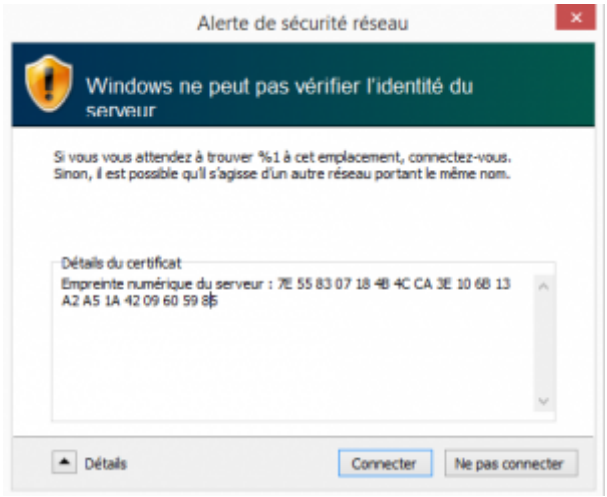
Rien d'autre à faire que précédemment (sauf que n'ayant pas installé le certificat au préalable pour notre client lors de cette démonstration, nous allons recevoir une alerte).

Demonstration

Le directeur de l'entreprise allume son PC de bon matin et pour obtenir l'accès au réseau il va devoir s'authentifier avec son login et mot de passe de session lorsque ce message va apparaître :



Une fois cela fait, il reçoit une alerte car le certificat délivré par le serveur n'est pas installé dans son magasin de certificats faisant autorité:

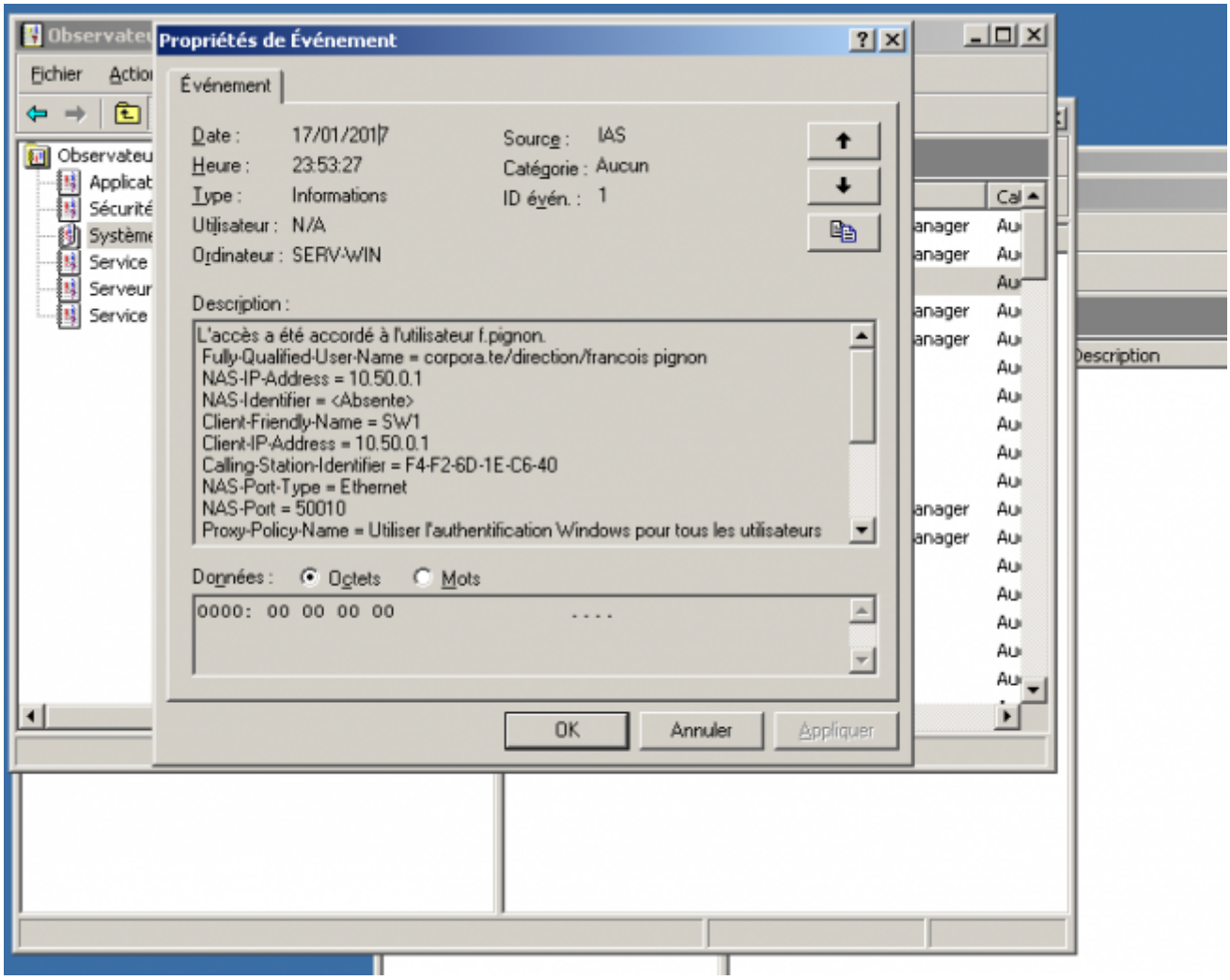


Il accepte la connexion, et on peut voir le résultat sur le commutateur :

```
*Mar  1 02:04:26.934: %AUTHMGR-5-START: Starting 'dot1x' for client
(f4f2.6d1e.c640) on Interface Fa0/10 AuditSessionID 0A32000A0000000C0071EEE5
*Mar  1 02:04:27.219: %DOT1X-5-SUCCESS: Authentication successful for client
(f4f2.6d1e.c640) on Interface Fa0/10 AuditSessionID 0A32000A0000000C0071EEE5
*Mar  1 02:04:27.219: %AUTHMGR-7-RESULT: Authentication result 'success'
from 'dot1x' for client (f4f2.6d1e.c640) on Interface Fa0/10 AuditSessionID
0A32000A0000000C0071EEE5
*Mar  1 02:04:27.219: %AUTHMGR-5-VLANASSIGN: VLAN 30 assigned to Interface
Fa0/10 AuditSessionID 0A32000A0000000C0071EEE5
*Mar  1 02:04:27.865: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(f4f2.6d1e.c640) on Interface Fa0/10 AuditSessionID 0A32000A0000000C0071EEE5
*Mar  1 02:04:28.721: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed
state to up
*Mar  1 02:04:29.728: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/10, changed state to up
```

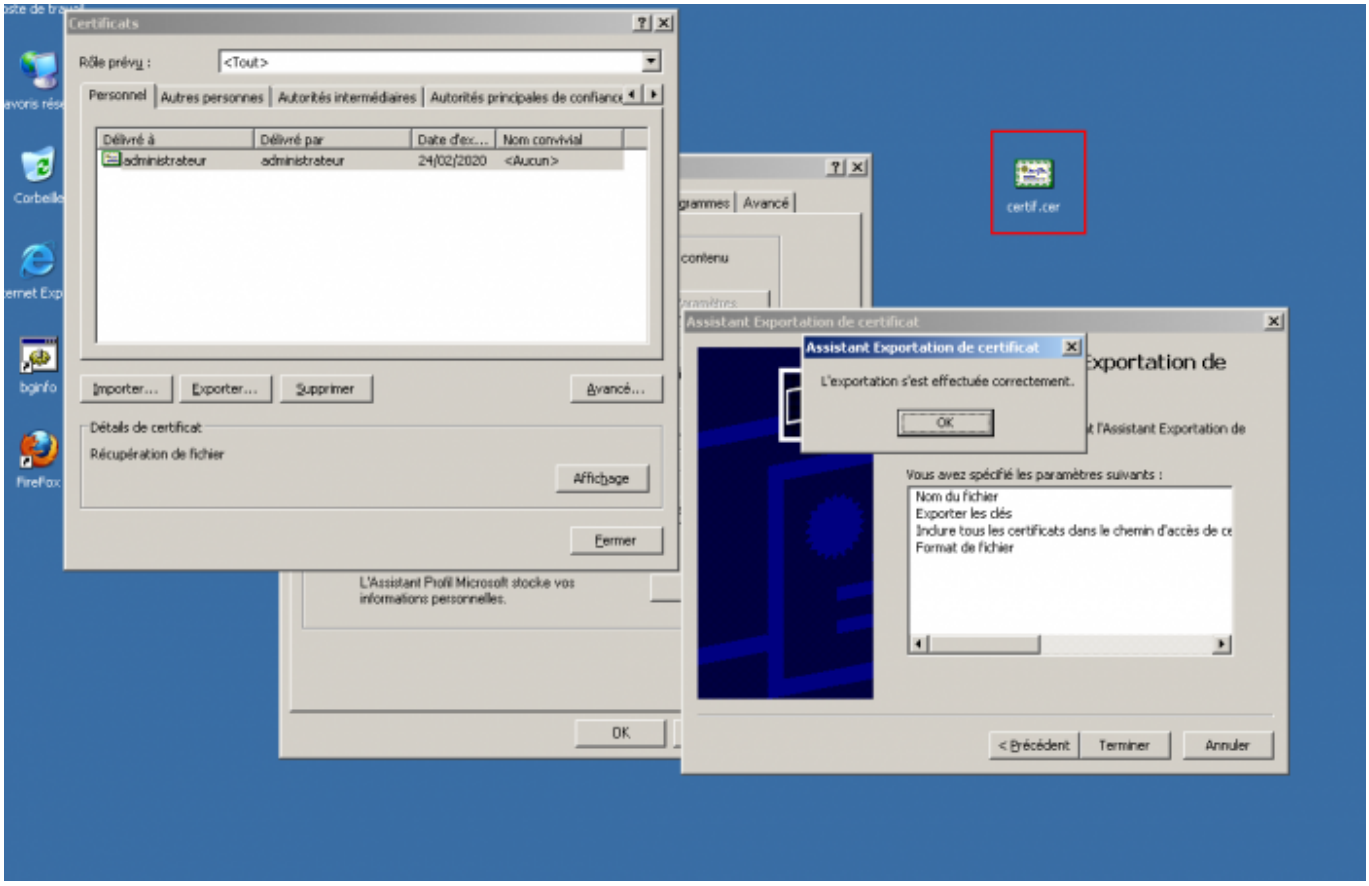
Et le VLAN 30 est attribué au port.

On peut constater le succès de la connexion dans l'observateur d'évènements:

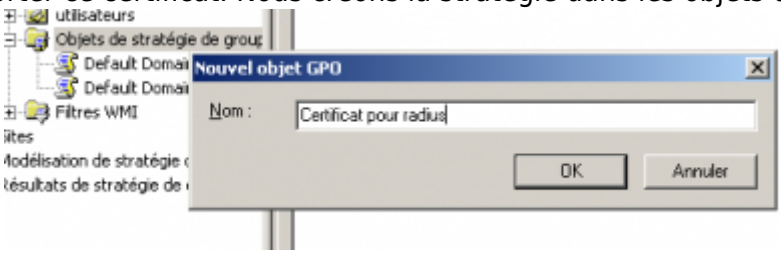


Envoi du certificat par GPO

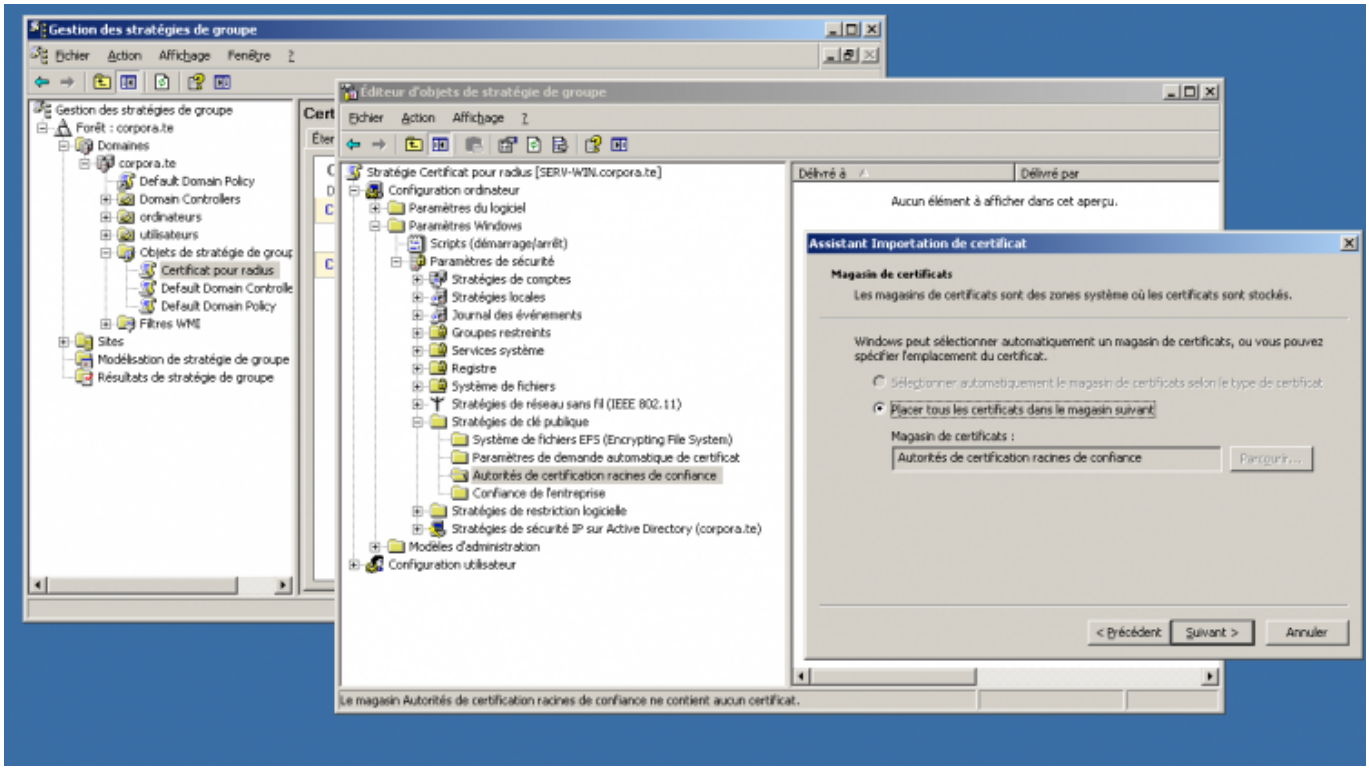
Pour ne plus recevoir l'alerte au sujet du certificat lors des prochaines connexions, nous allons le transmettre par stratégie de groupe sur les PC situés dans l'OU “Ordinateurs”. Pour ce faire, nous exportons le certificat dans un fichier nommé “certif.cer” par exemple :



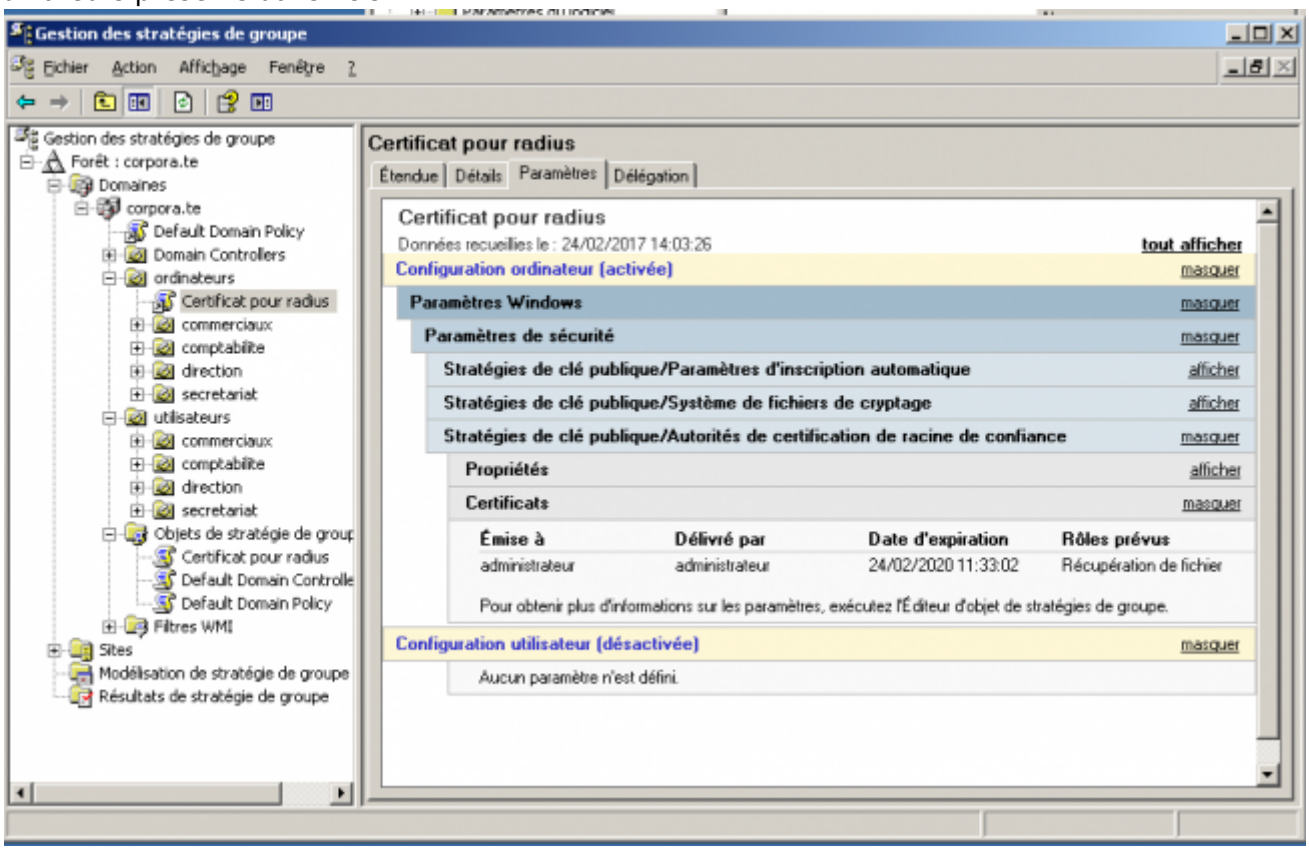
Nous allons créer une stratégie de groupe pour imposer à tous les ordinateurs situés dans l'OU “Ordinateurs” d'importer ce certificat. Nous créons la stratégie dans les objets de stratégie de groupe:



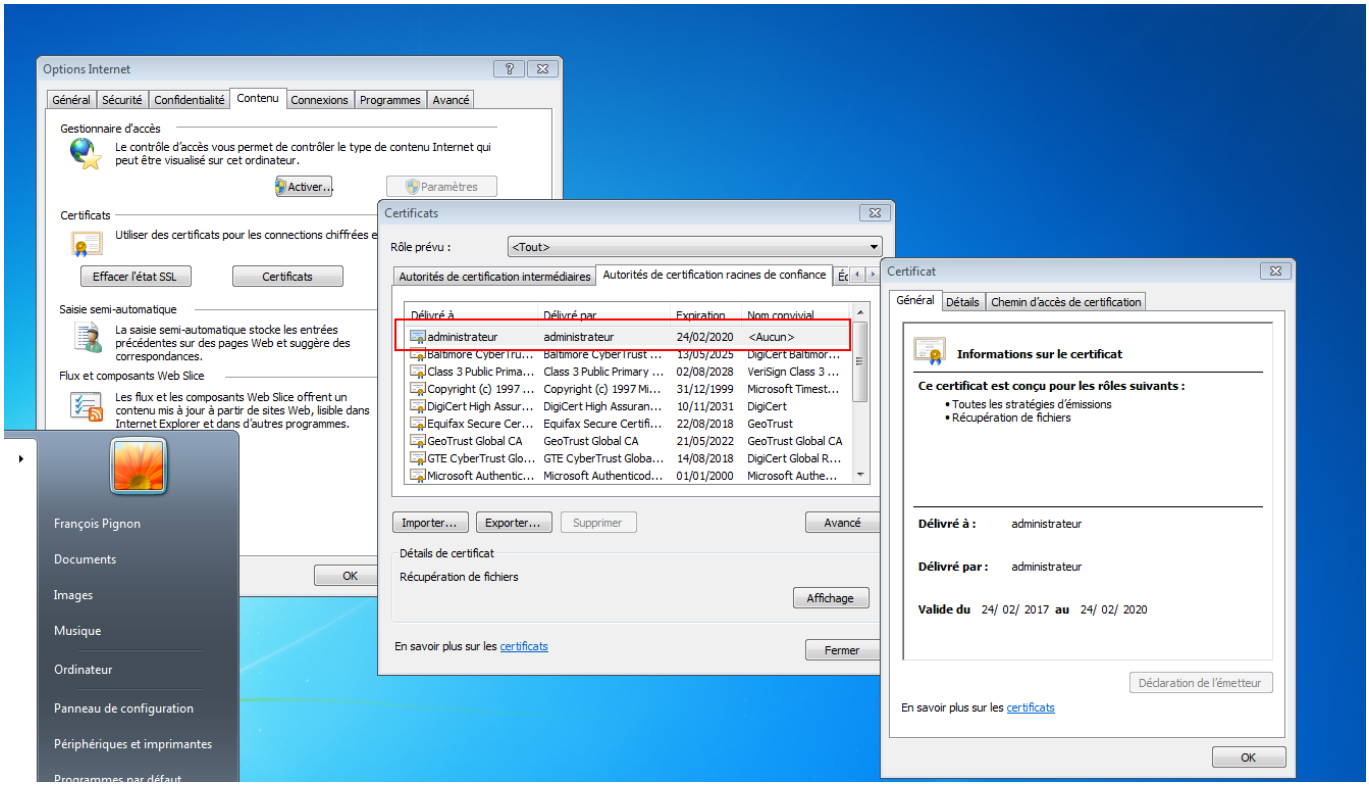
et nous allons importer le certificat “certif.cer” dans le magasin des Autorités de certification racines de confiance des ordinateurs situés dans l'OU Ordinateurs :



Il ne nous reste plus qu'à lier la GPO à l'OU “Ordinateurs” et d'attendre la propagation de la règle aux ordinateurs présents dans l'OU:



Après avoir connecté l'ordinateur appelé “Directeur” avec l'utilisateur f.pignon, on constate que notre certificat est bien installé dans le magasin “Autorités de certification racines de confiance” :



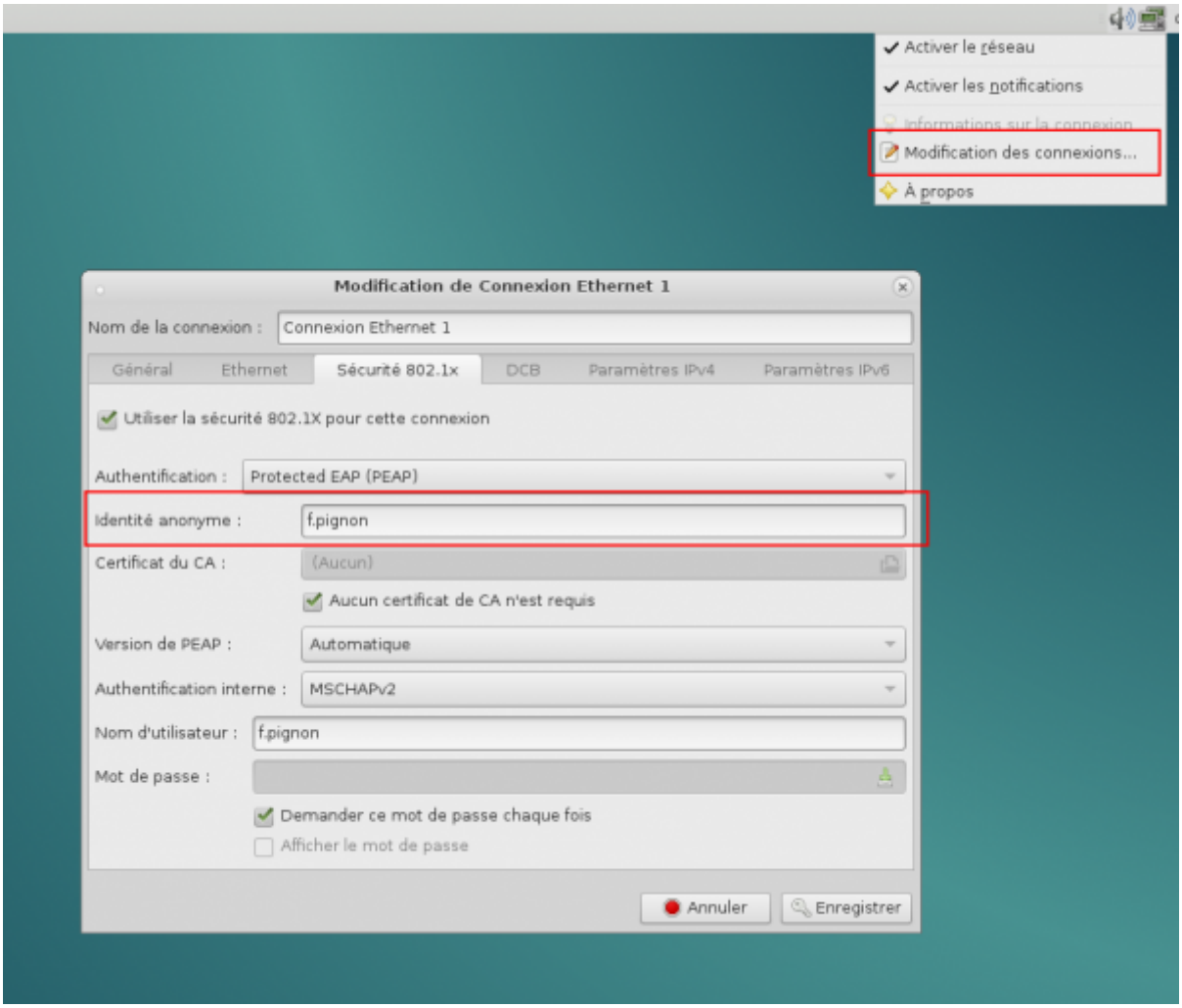
Hôte sous Linux

Nous allons voir la configuration d'un hôte sous linux pour se connecter au réseau en utilisant 802.1x.

En mode graphique

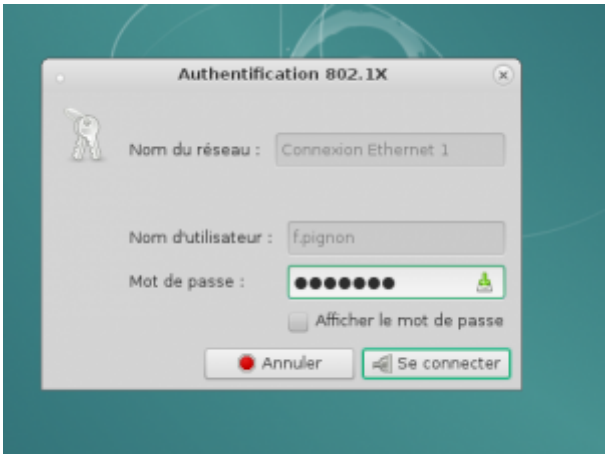
oui, ça existe ! 😳

L'application NetworkManager nous permet de nous connecter très simplement sur le réseau filaire en renseignant les éléments suivants dans la partie 802.1x :



Il convient de préciser le nom d'utilisateur dans le champ “identité anonyme”.

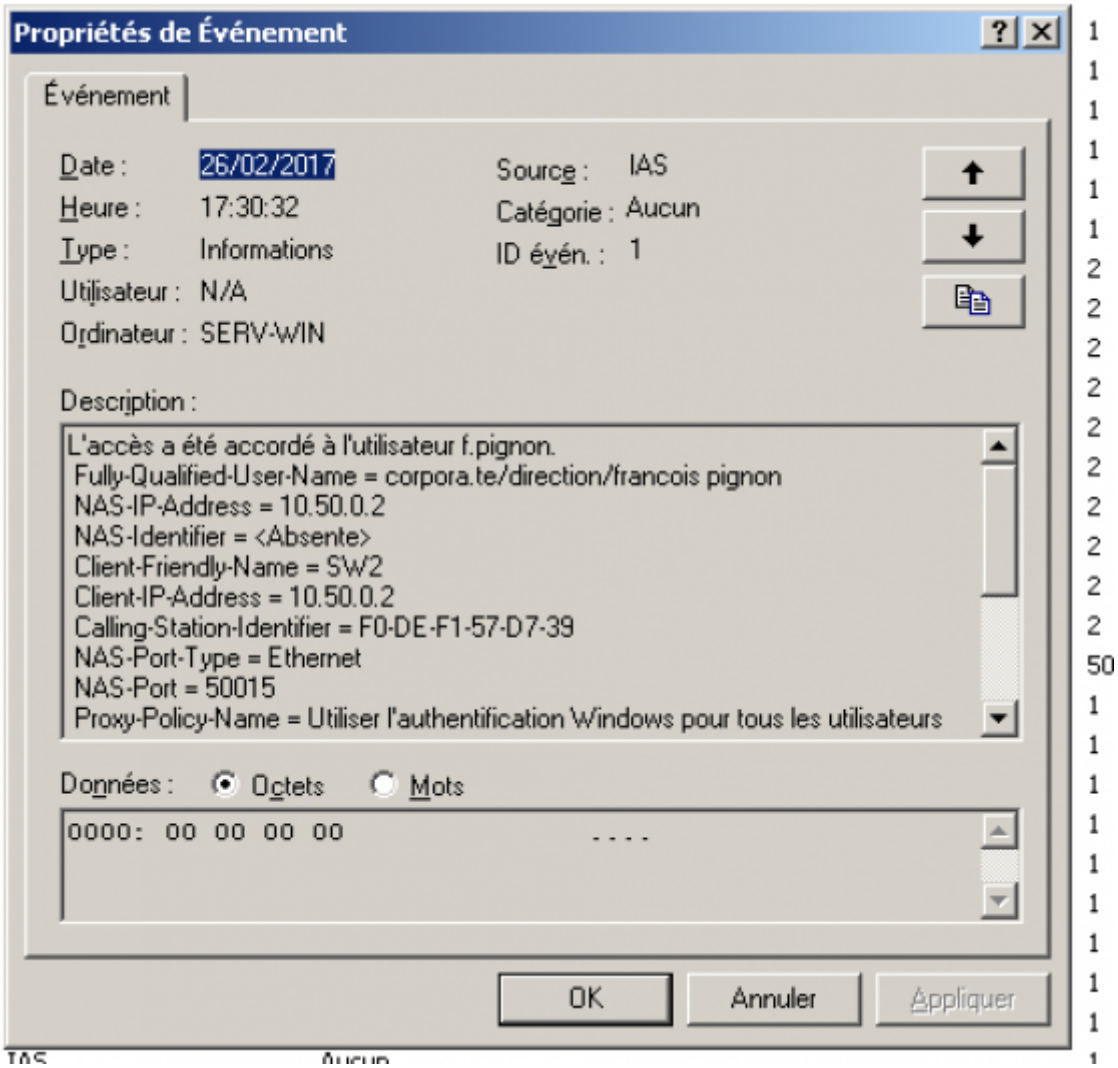
Le système nous demande notre mot de passe et nous sommes connectés :



Aperçu de la sortie sur le commutateur :

```
%AUTHMGR-5-START: Starting 'dot1x' for client (f0de.f       ) on Interface Fa0/15 AuditSessionID 0A3200020000008100B5ED28
%DOT1X-5-SUCCESS: Authentication successful for client (f0de.f157.    ) on Interface Fa0/15 AuditSessionID 0A3200020000008100B5ED28
```

Log du serveur Windows Server 2003 :



Voici le fichier de configuration de la connexion, `/etc/NetworkManager/system-connections/Ethernet` :

```
[ethernet]
duplex=full
mac-address=F0:DE:D1:57:C8:39

[connection]
id=Connexion Ethernet 1
type=ethernet

[ipv6]
method=auto
ip6-privacy=0

[802-1x]
eap=peap;
identity=f.pignon
anonymous-identity=f.pignon
phase2-auth=mschapv2
password-flags=3
```

```
[ipv4]
method=auto
```

Hôtes incompatibles avec 802.1x

Que faire du matériel incompatible avec la norme?

Changez-en! 😉

Sinon, plusieurs possibilités s'offrent à nous afin de connecter nos imprimantes par exemple :

VLAN invité

Il est possible de créer un VLAN destiné aux hôtes qui ne prennent pas en compte 802.1x. Nous avons créé le VLAN 900 qui va nous servir à cela:

```
SW2(config)#interface range fa0/3-22
SW2(config-if-range)#authentication event no-response action authorize vlan
900
```

On branche l'interface de l'imprimante de la comptabilité sur la prise murale correspondant au port fa0/15 du commutateur SW2 et on constate qu'elle a bien été placée dans le VLAN 900 et peut communiquer avec les autres hôtes qui s'y trouvent :

```
SW2#
SW2#
*Mar  1 00:28:01.295: %LINK-3-UPDOWN: Interface FastEthernet0/15, changed state to up
*Mar  1 00:28:02.301: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to up
SW2#
*Mar  1 00:29:31.908: %DOT1X-5-FAIL: Authentication failed for client (Unknown MAC) on Interface Fa0/15 AuditSessionID 0A3200010000000E00199FC2
*Mar  1 00:29:31.908: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (Unknown MAC) on Interface Fa0/15 AuditSessionID 0A32
*Mar  1 00:29:31.908: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (Unknown MAC) on Interface Fa0/15 AuditSessionID 0A3200010000000E00199FC2
*Mar  1 00:29:31.908: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (Unknown MAC) on Interface Fa0/15 AuditSessionID 0A3200010
*Mar  1 00:29:32.521: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (Unknown MAC) on Interface Fa0/15 AuditSessionID 0A3200010000000E00199FC2
SW2#
```

On placera judicieusement le serveur d'impression dans un réseau sécurisé pouvant communiquer avec ce VLAN au moyen d'un routeur filtrant.

Port security sans 802.1x

Une autre solution consiste à s'affranchir simplement de 802.1x et de se contenter de port security sur le port voulu et de mettre ce port dans le VLAN invité. L'idée étant que même en cas d'usurpation d'adresse MAC, l'attaquant n'ira pas plus loin que le VLAN invité dans lequel se trouvera ce port.

Wi-Fi et portail captif

Pour les utilisateurs dont les appareils ne pourraient pas se connecter avec 802.1x, il reste la possibilité de rendre une attaque compliquée grâce à une connexion Wi-Fi sécurisée et un portail captif nécessitant l'authentification de l'utilisateur (au moyen du même Active Directory que celui utilisé par le serveur radius).

Nous verrons comment utiliser 802.1x avec le Wi-Fi dans la suite du chapitre.

802.1x et la téléphonie IP

On peut intégrer un VLAN propre à la voix sur IP sur les ports que l'on souhaite affecter aux téléphones IP. Nous allons créer un VLAN 700 appelé “telephonie” et permettre au port fa0/12 du commutateur SW2 de recevoir un téléphone IP:

```
SW2(config)#vlan 700
SW2(config-vlan)#name telephonie
SW2(config-vlan)#exit
SW2(config)#int fa0/12
SW2(config-if)#switchport voice vlan 7
```

Si on souhaite que les données relatives à la téléphonie sur IP soient prioritaires, on peut activer la priorité entre les différents vlan en activant 802.1p[9] :

```
SW2(config-if)#switchport voice vlan dot1p
```

Nous ne traiterons pas le sujet plus en avant, bien trop vaste et un peu hors sujet…

802.1x et le Wifi

Les commerciaux et leurs portables

Mise en place de 802.1x sur le point d'accès sans fil

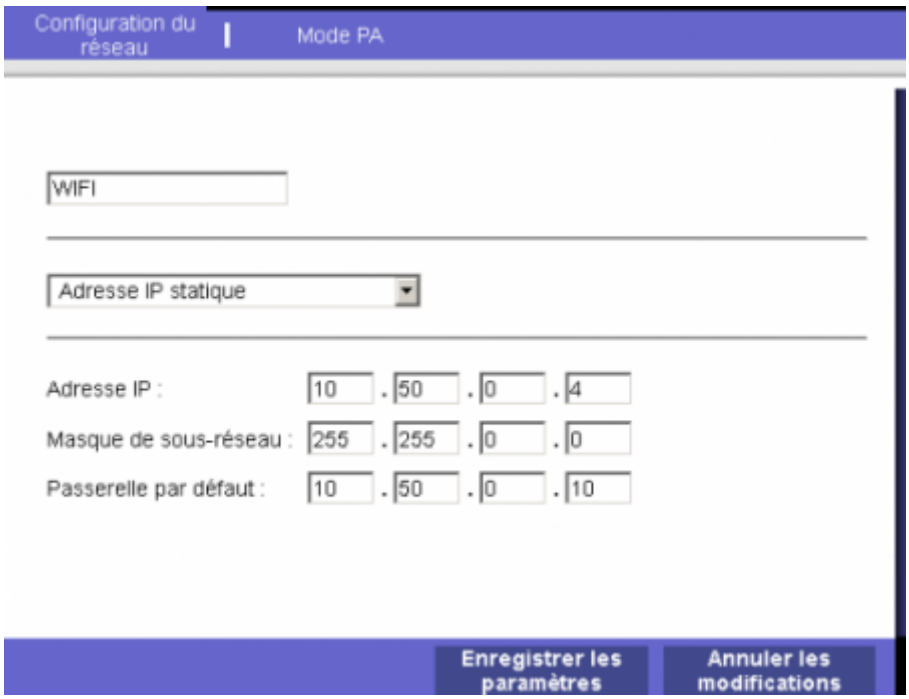
Nos commerciaux vont avoir un point d'accès Wifi leur permettant de se connecter au réseau. Du point de vue du serveur, on va rajouter une stratégie d'accès distant en prenant en compte l'acces 802.11 à la place d'Ethernet.

On évitera donc les points d'accès non compatibles 802.1x … Nous utilisons un Point d'accès Linksys WAP54G, comptabible 802.1x:

Configuration

Sous windows serveur 2003, nous ne modifions que le paramètre Ethernet en “Sans fil” pour la stratégie d'accès “commerciaux”.

Nous paramétrons la configuration de base du point d'accès Linksys et précisons que l'authentification sera en WPA Entreprise en indiquant l'adresse du serveur RADIUS :

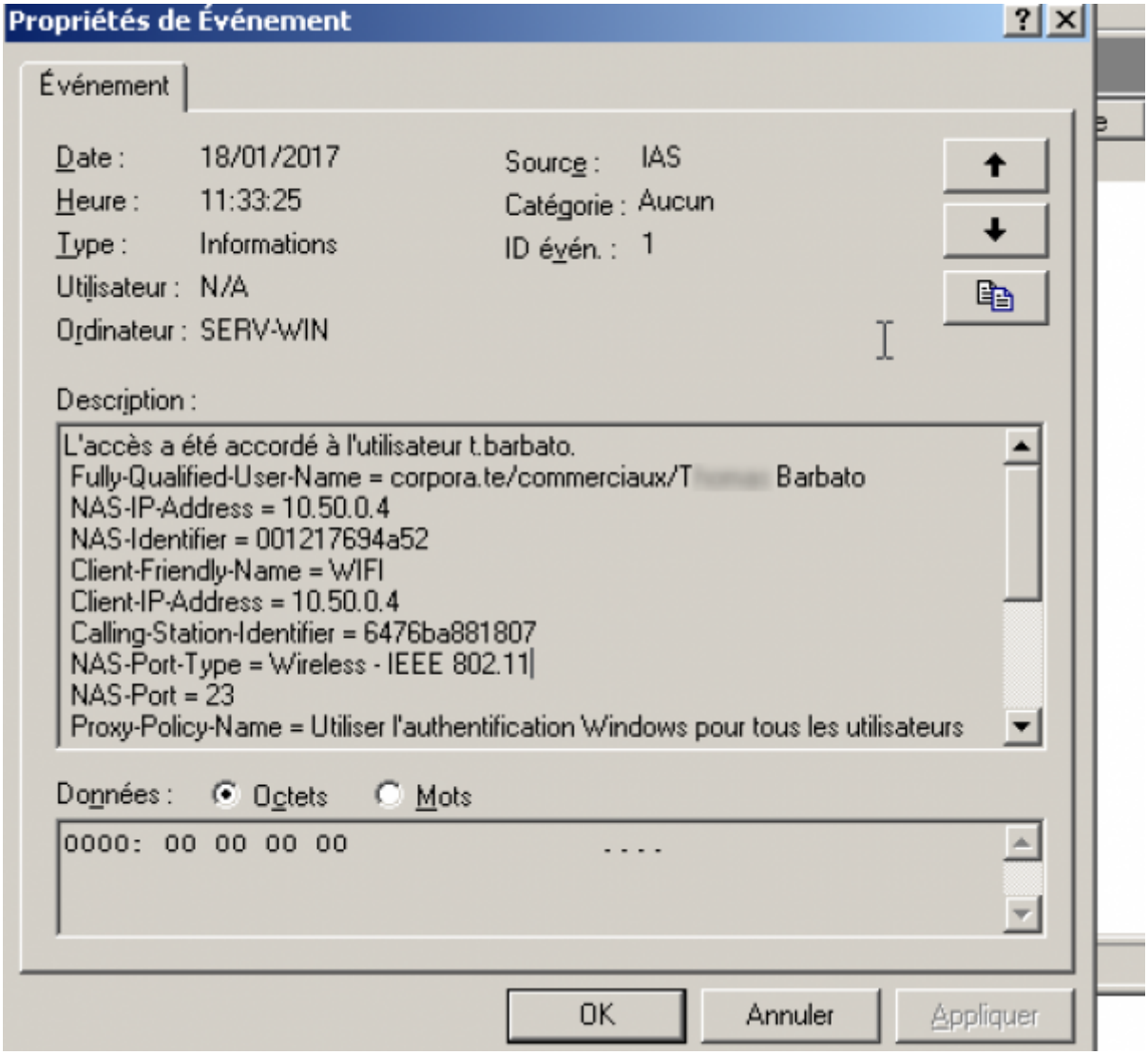


(la passerelle par défaut est le routeur RT1 auquel nous avons ajouté l'adresse 10.50.19.77 dans le VLAN 50)

Démonstration

T. Barbato, commercial dans l'entreprise Corpora.te, va tenter de se connecter avec son téléphone en wifi au réseau de l'Entreprise. Il doit renseigner un login et un mot de passe et le point d'accès lui remet le certificat du serveur qu'il doit accepter (le certificat n'est pas installé par défaut dans son téléphone):

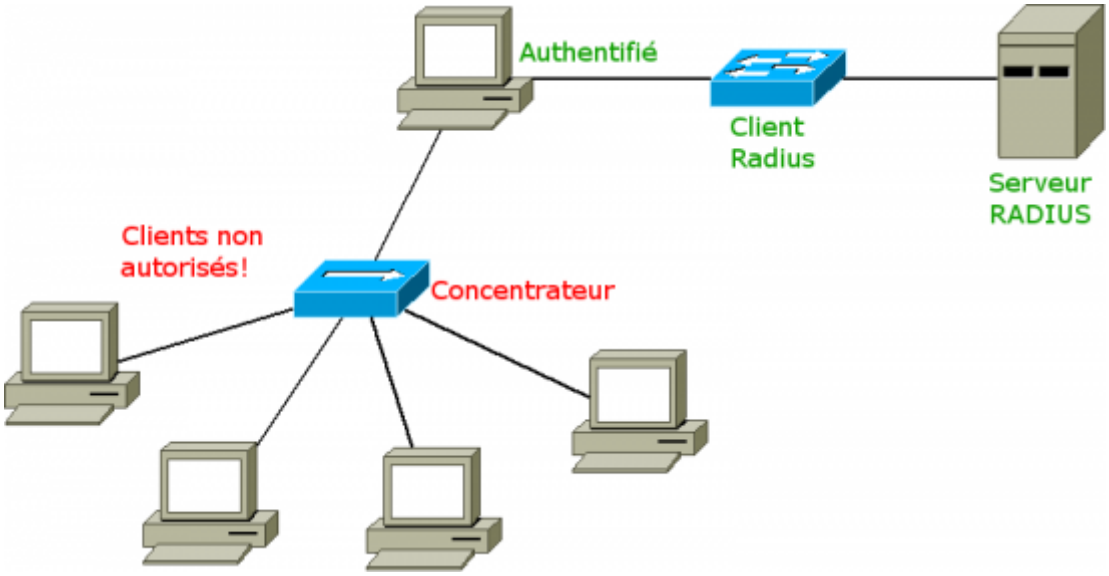
Le succès de la connexion apparaît dans l'observateur d'évènements :



Les failles

Branchement d'un concentrateur pour partager une connexion

Il suffit qu'un hôte soit authentifié pour que d'autres puissent passer par lui:



Pour contrer ce désagrément, on activera port security pour empêcher que plusieurs interfaces utilisent le même port du client Radius (dans le cas présent, le commutateur). On se référera au chapitre précédent pour son fonctionnement.

Man In The Middle (encore lui!)

L'activation de port security couplé à 802.1x interdit tout rejeu de paquet par un hôte préalablement authentifié (le port sera désactivé au changement d'adresse MAC).

Wifi

On utilisera les solutions de chiffrement plus efficaces que MD5 susceptible de faire l'objet d'un bruteforce par dictionnaire, comme EAP-TLS pour renforcer la sécurité des connexions.

On pourra également rajouter un portail captif sur un VLAN existant pour avoir une double sécurité sur certaines connexions wifi.

Bonus

Vous trouverez une présentation amusante et très instructive en vidéo sur ce lien (Black Hat 2014). Et sur celui-ci, vous pouvez suivre la présentation sur un pdf de 42 pages.

Conclusions, remarques et critiques

Nous arrivons au terme de ce projet dans lequel nous avons pu étudier différentes solutions de sécurité de la couche 2.

Pour conclure, 802.1x est une solution de sécurité robuste mais lourde à mettre en place, en particulier dans un environnement comportant de nombreux hôtes et une infrastructure complexe.

Nous n'avons pas tout traité, le sujet est bien trop vaste, il aurait fallu faire de longues démonstrations (attaques par bruteforce avec des dictionnaires par exemple).

Basé sur port-security, 802.1x fait de notre réseau un bastion presque “imprenable”, si l'on ne tient pas compte de l'erreur humaine (mot de passe sur un post-it ou vol par social engineering couplé à une usurpation d'adresse MAC). Il est donc fondamental de sensibiliser les utilisateurs aux fondamentaux de la sécurité au delà de tous les aspects techniques vus dans ce projet.

Voilà c'est la fin de ce cas pratique issu de mon imagination mais basé sur des cas bien concrets/vécus.
Toute technologie évolue, il est probable que lorsque vous aurez lu ceci,tout ne sera déjà plus d'actualité mais les fondamentaux ne changent pas beaucoup ;)

1)
IEEE 802.1x
2)
Port Access Entity
3)
Extensible Authentication Protocol
4)
https://tools.ietf.org/html/rfc3748
5)
Remote Authentication Dial-In User Service
6)
Network Policy Server
7)
http://freeradius.org/
8)
Redistribution sans restrictions, accès libre au code source et usage indirect autorisé pour la création d'autres projets
9)
http://standards.ieee.org/getieee802/download/802.1D-2004.pdf