Institut de recherches sur la catalyse et l'environnement de Lyon IRCELYON

Authentification et affectation dynamique dans un Vlan

L. Besson

Contexte

- ✓ Institut composé de ~250 personnes
- ✓ 400 postes utilisateurs raccordés dans un même domaine active directory
- ✓ Mouvement de personnels temporaires important (100/ an) et de nombreux thésards qui raccordent leur portable au réseau de l'établissement (avec des systèmes d'exploitation très éclectiques …)
- ✓ des visiteurs (à l'époque (2008) sans accès WIFI)

Dans le cadre d'une nouvelle architecture réseau

Objectif

- Protéger le SI
- Sécuriser l'accès au réseau et affectation automatique dans un VLAN en fonction du profil (personnel/poste utilisateur => quel accès , quel service).

Profil	Quel accès
Postes professionnels	Tout le SI
Portables personnels des non permanents	Quelques subtilités …
Visiteurs	Accès internet uniquement

- Limiter l'impact d'un incident de sécurité par le cloisonnement réseau ((filtrage inter vlan)
- Coût d'exploitation restreint (parc important mais homogène, mouvement de personnels important..)

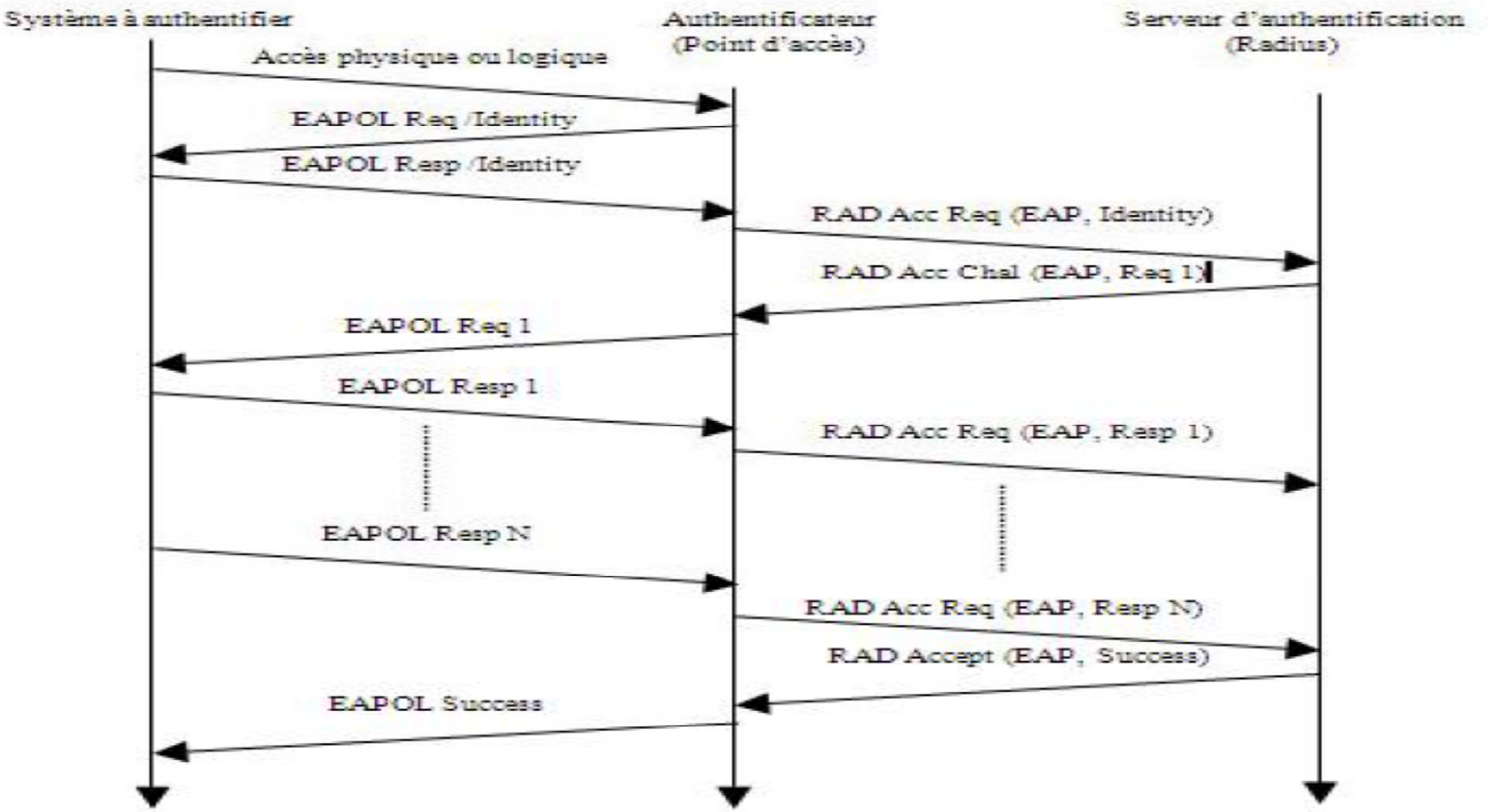
Solution

- Segmentation réseau (**802.1q**)
- Allocation dynamique dans un VLAN en fonction de l'authentification :
  Radius :*centralisation des données d'authentification: une seule base d'utilisateurs*,
  EAP extension radius : Extensible Authentification Radius
  extension du protocole Radius à des types d'authentification plus complexes ((EAP-MD5, EAP-TLS, EAP-TTLS,**EAP-PEAP**)
  Login/mot de passe,
  Certificat,
  Carte à puce ou calculette
  PEAP: tunnel TLS qui permet l'échange d'attributs/valeurs de manière sécurisée.
  Le client est authentifié par l'un des mécanismes classiques (login/mot de passe ou certificat)
  * indépendant du matériel du client Radius,
  * négociation direct avec le « suppliant »
  802.1x extension radius assure une authentification par port pour l'accès à un réseau.
- Filtrage inter vlan

Mécanisme
(sur le réseau filaire)

- ✓ Notion de ports contrôlés par une authentification
- ✓ ports logiques connectés sur un port physique:
  Le 1er port est le port de contrôle : ouvert/fermé,
  Le 2ème port est toujours ouvert, ne laisse passer que du 802.1x, il sert à la négociation.

Mécanisme (suite)



Détail de la solution : équipement réseau (Alcatel)

- **Définition VLAN**

vlan 1762 enable name "utilisateurs"
vlan 1762 authentication enable
vlan 1764 enable name "visiteur"

- **Définition des serveurs radius (je définie un type d'authentification: « Radius »)**

aaa radius-server "poseidon.domaine.fr" host 134.214.x.y key password retransmit 3
timeout 2
auth-port 1812 acct-port 1813

- **Activation de l'authentification du serveur Radius poseidon**

aaa authentication 802.1x "poseidon.domaine.fr"

Détail de la solution : équipement réseau (Alcatel)

Par défaut, les ports des switches sont dans le réseau visiteur (guest vlan)

vlan 1764 port default 1/3

Activation du 802.1x

vlan port mobile 1/3

vlan port 1/3 802.1x enable

Et ...

802.1x 1/3 direction both port-control auto quiet-period 60 tx-period 30 supp-timeout 30 server-timeout 30 max-req 2 re-authperiod 3600 no reauthentication

802.1x 1/3 captive-portal session-limit 12 retry-count 3

802.1x 1/3 captive-portal inactivity-logout disable

802.1x 1/3 supp-polling retry 2

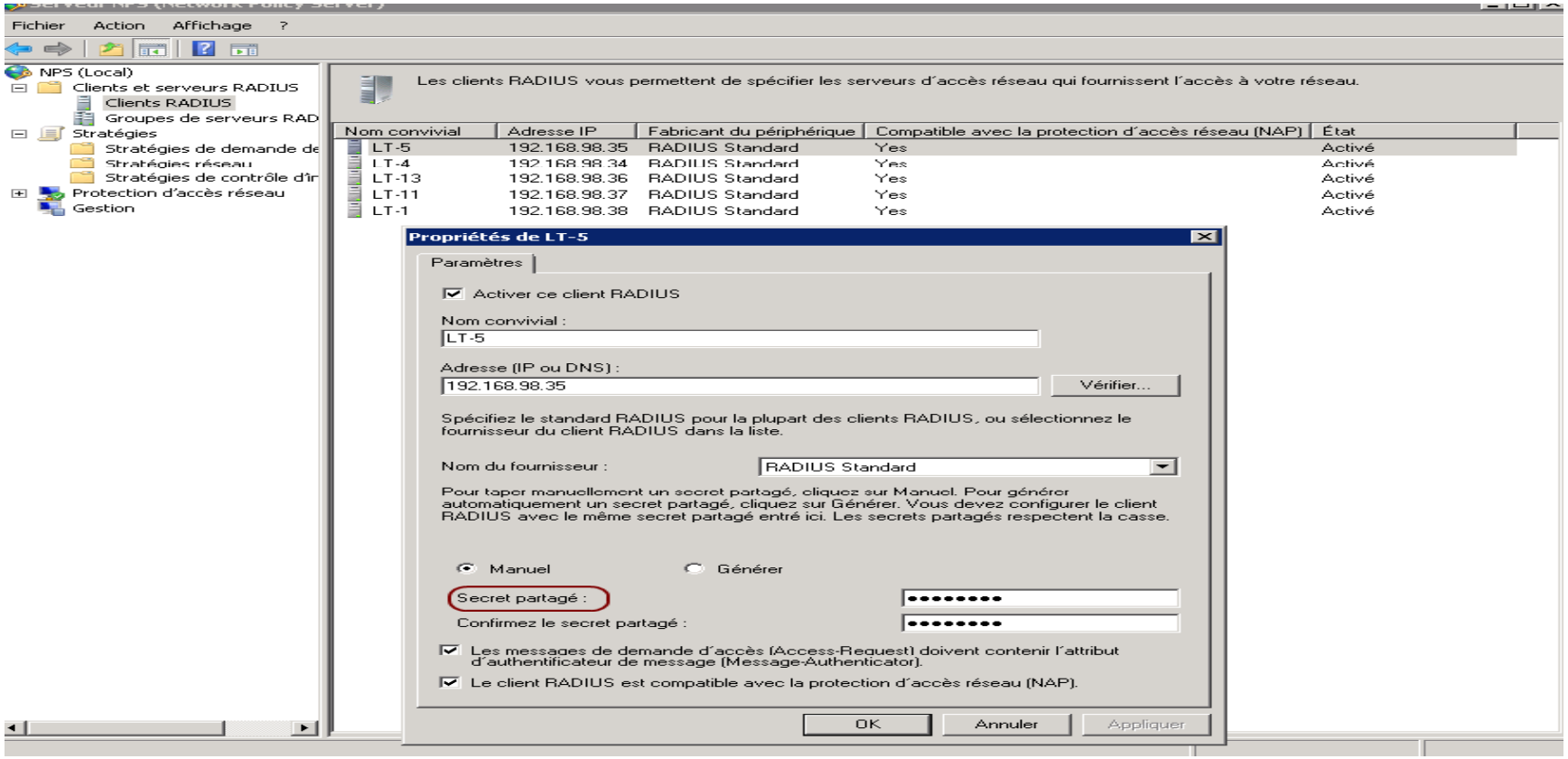
802.1x 1/3 supplicant policy authentication pass group-mobility default-vlan fail vlan 1764 block (on négocie l'authentification et en cas d'echec ...)

802.1x 1/3 non-supplicant policy default-vlan (si l'équipement ne demande pas a être authentifié)

802.1x 1/3 captive-portal policy authentication pass default-vlan fail block

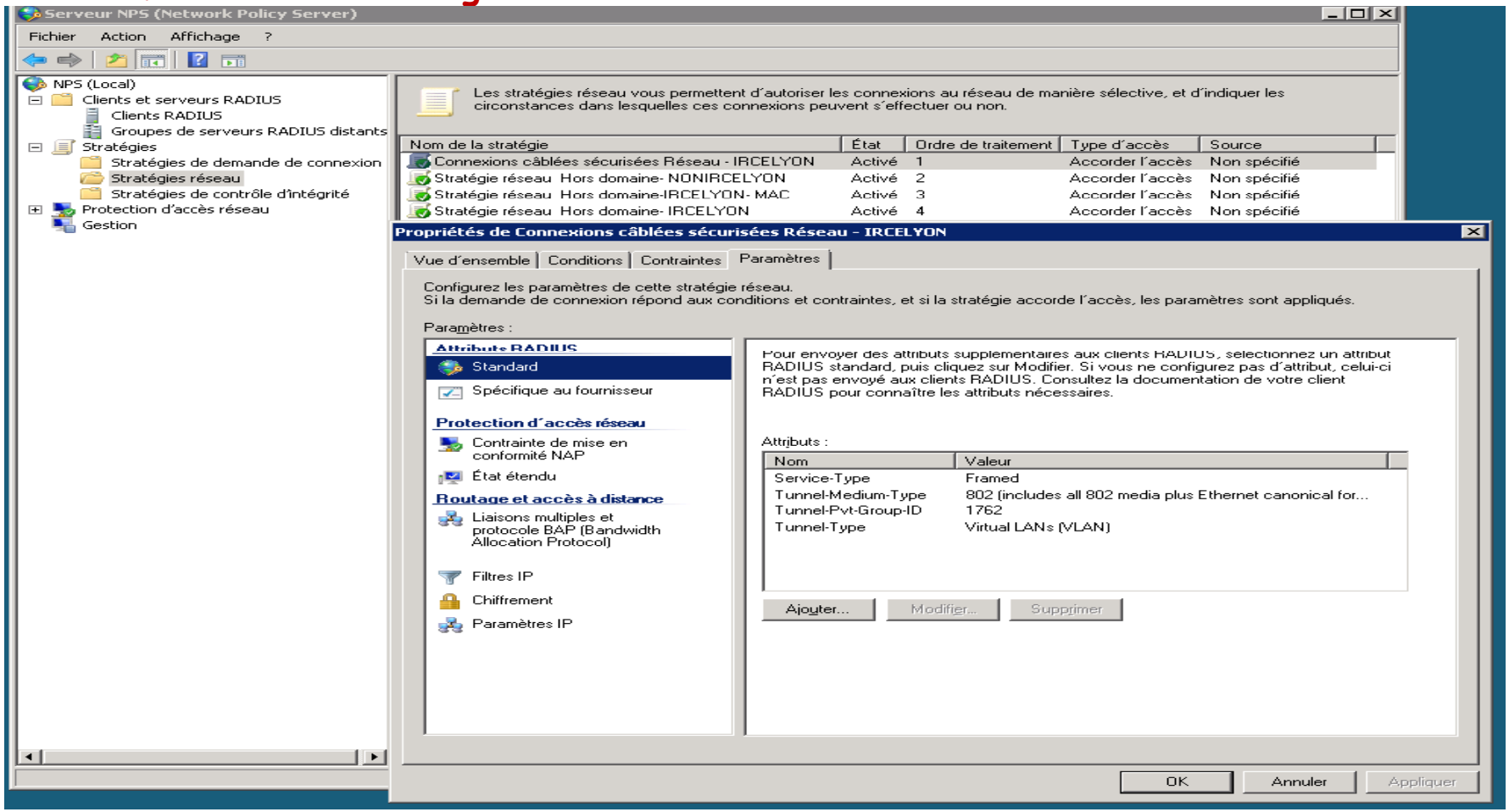
Détail de la solution : server Radius(NPS) 1/2

- **Définition des clients Radius** (l'ensemble des commutateurs qui demandent une authentification radius) (secret partagé)



Détail de la solution : partie server Radius(NPS) 2/2

- **Définition des stratégies**



Détail de la solution : les clients

PEAP: authentification avec certificat

- La gestion des certificats est réalisé grâce à la mise en service d'une autorité de certification interne.
- Le déploiement se fait soit par le domaine active directory (postes en domaines) soit https://autorité_de_certification/cetsrv pour les autres

Bilan du contrôle d'accès sur le réseau filaire

- Objectif de réduire les coûts d'exploitation atteint
- Le contrôle d'accès ca peut aussi servir pour..:
  - Un contrôle d'accès selon une plage horaire,
  - Un contrôle d'accès selon un système d'exploitation :
    par exemple : depuis l'arrêt de la maintenance XP , utilisation de radius pour confiner ces postes dans un vlan d'adresses IP privées.

- *Et un bon entrainement pour se préparer aux nouveaux usages nomadismes et BYOD (Smartphones, Tablettes)*
  - *Contrôle d'accès pour l'accès au Wifi,*
  - *Délégation d'authentification (Eduroam)*
    Nos chercheurs en déplacement …
    Les chercheurs accueillis au sein de l'établissement

Contrôle d'accès au réseau Wifi

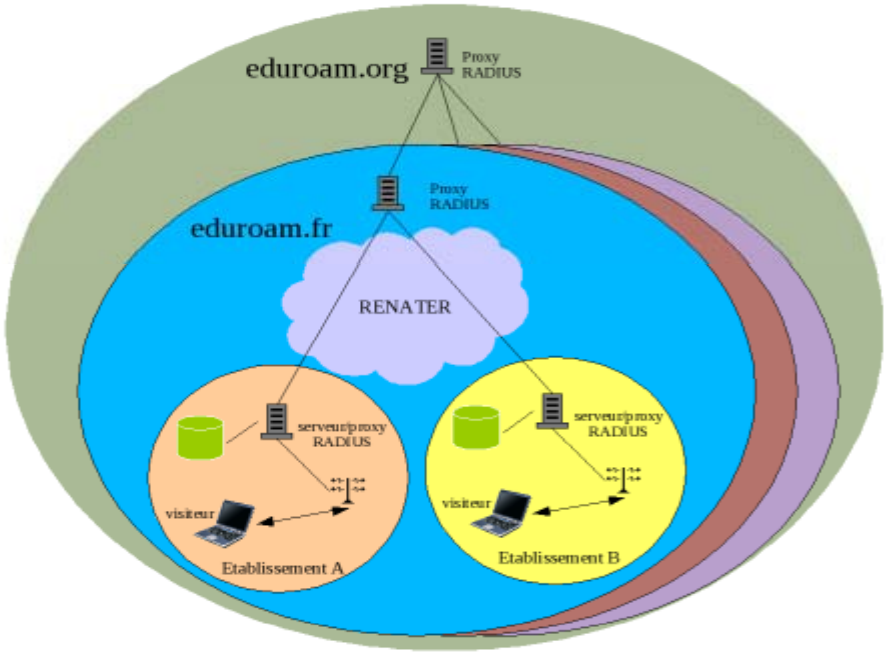
objectif du serveur Radius:

- Authentifier les équipements professionnels utilisant une connexion Wifi,
- Authentifier les équipements personnels (BYOD : tablettes et smartphones, .. à une époque …où on avait rien compris ;-)
- Déléguer l'authentification de nos visiteurs au serveur Radius de leur établissement d'origine via Eduroam.

Eduroam

Architecture

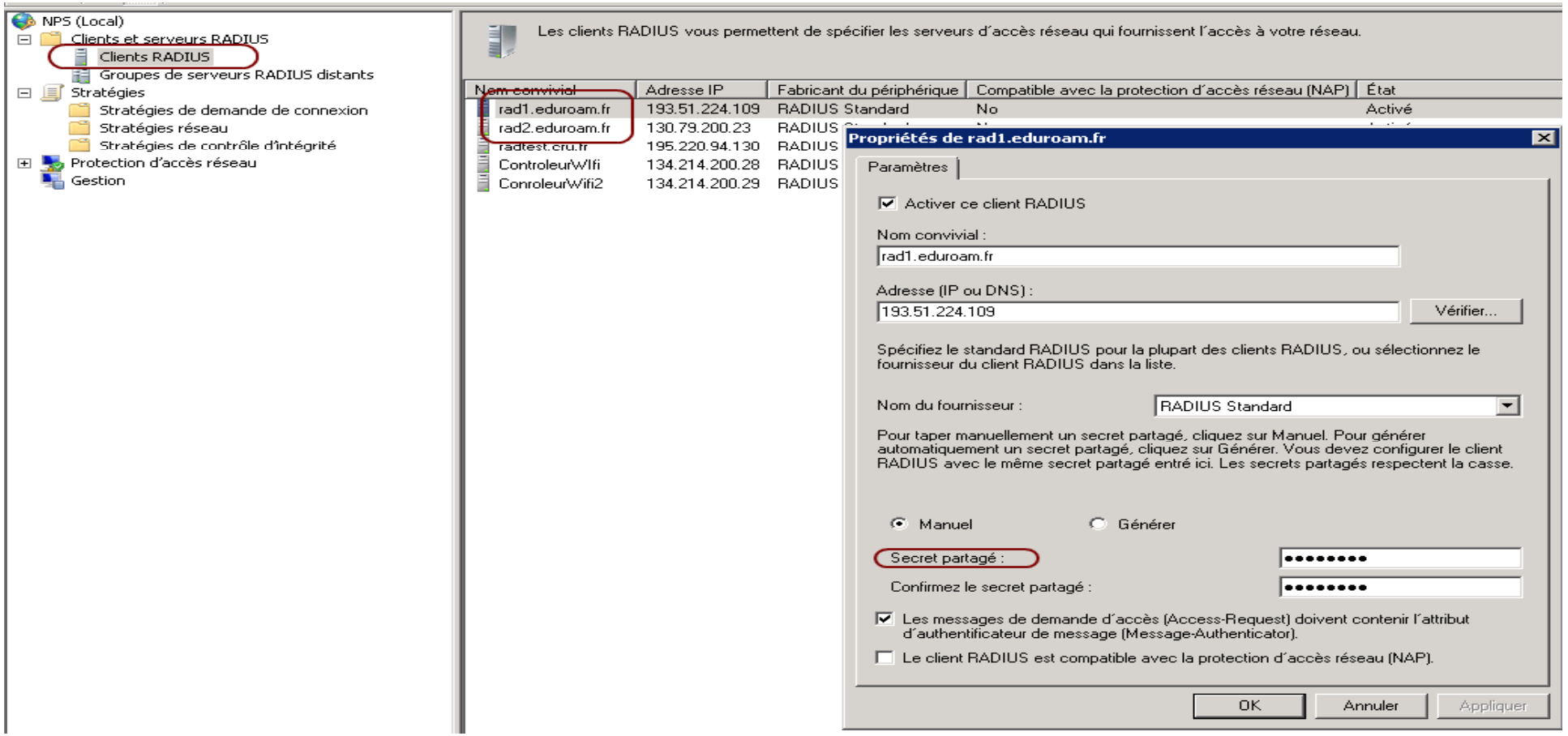
Chaque établissement raccorde son ou ses serveurs RADIUS au serveur proxy national (doublé) à qui il délègue toute demande d'authentification qui n'est pas de son ressort. Le serveur national remonte au serveur européen toutes les demandes ne concernant aucun des établissements français. Ces requêtes sont alors acheminées vers le bon pays puis l'établissement concerné. Les réponses suivent le chemin inverse.



Institut de recherches sur la catalyse et l'environnement de Lyon IRCELYON

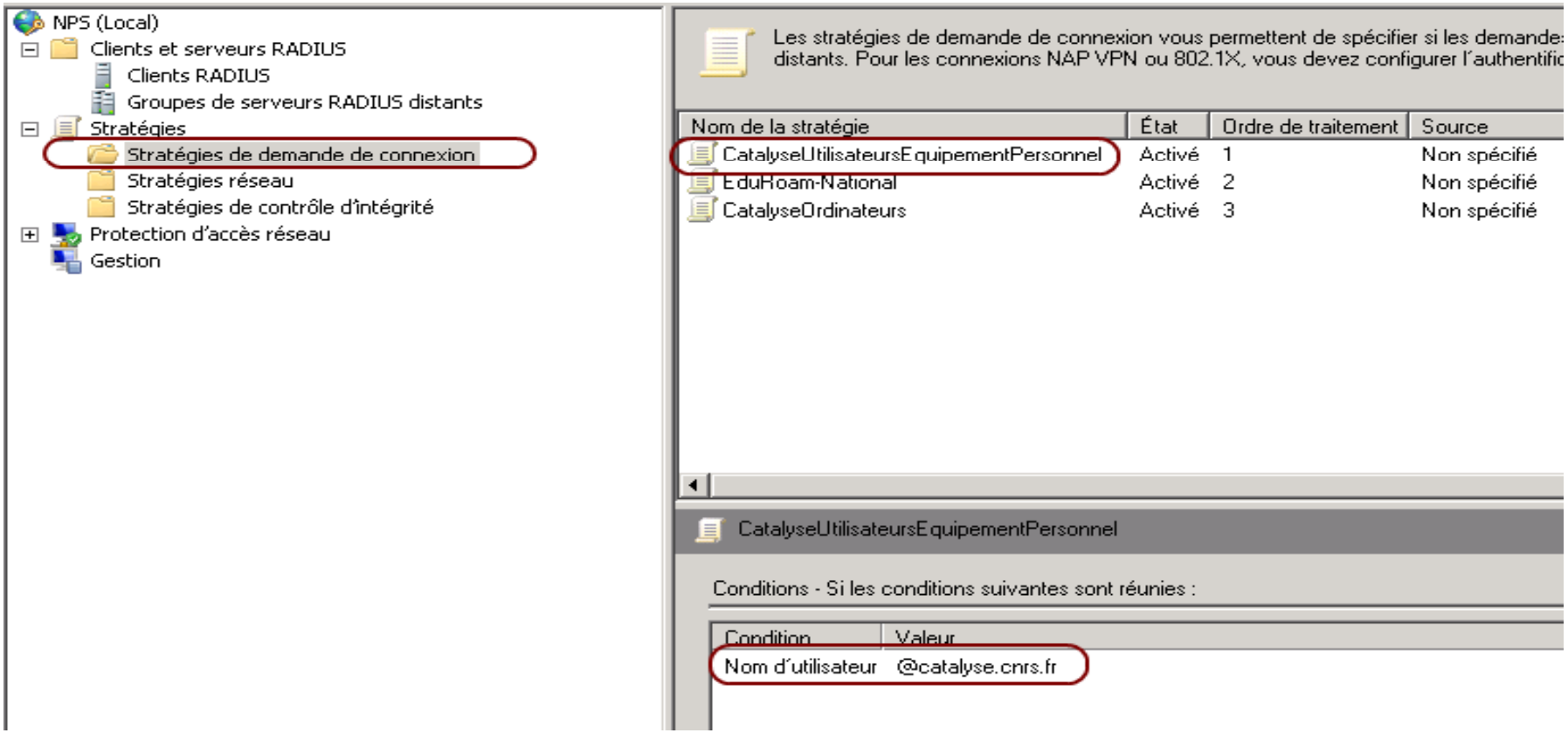
Configuration serveur Radius (NPS)

Définition des clients radius nationaux (et locaux : contrôleur de bornes WiFI)



Configuration serveur Radius (NPS)

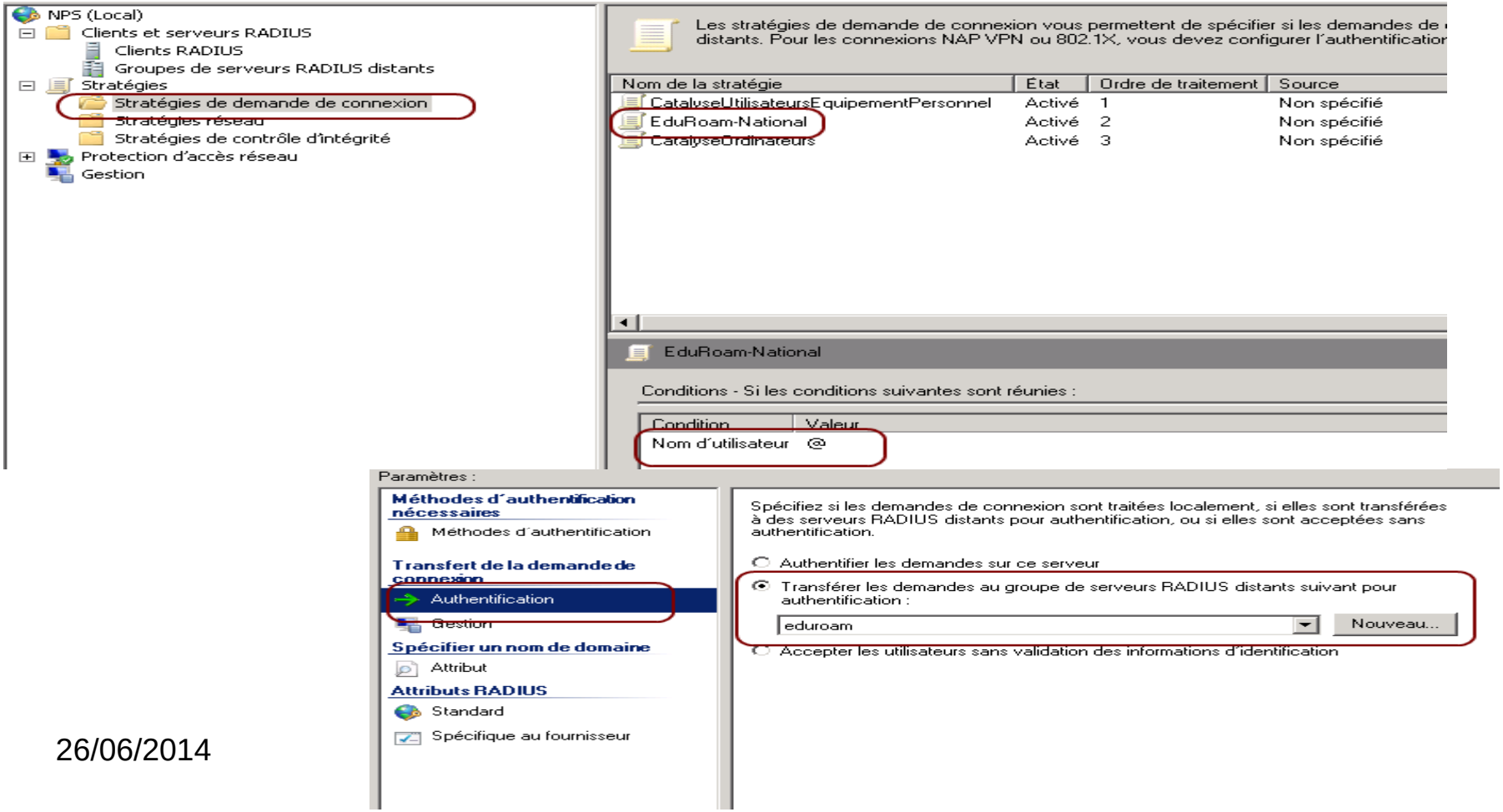
Stratégies de demande de connexion: nos utilisateurs avec leur **équipement personnel** (Smartphone, Tablette)



Configuration serveur Radius (NPS)

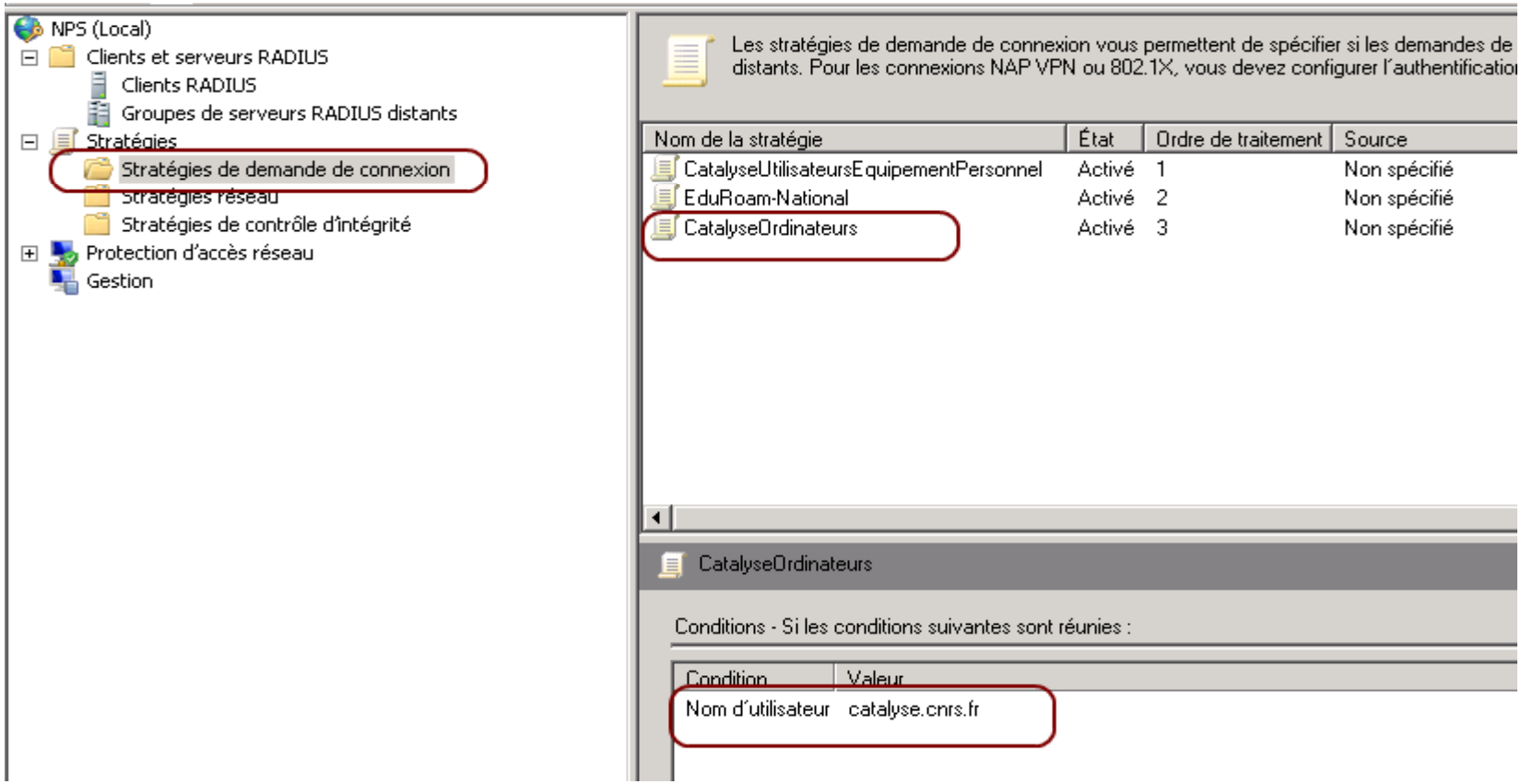
Stratégies de demande de connexion: **Les visiteurs « membre d'eduroam »,**

La demande est transférée …



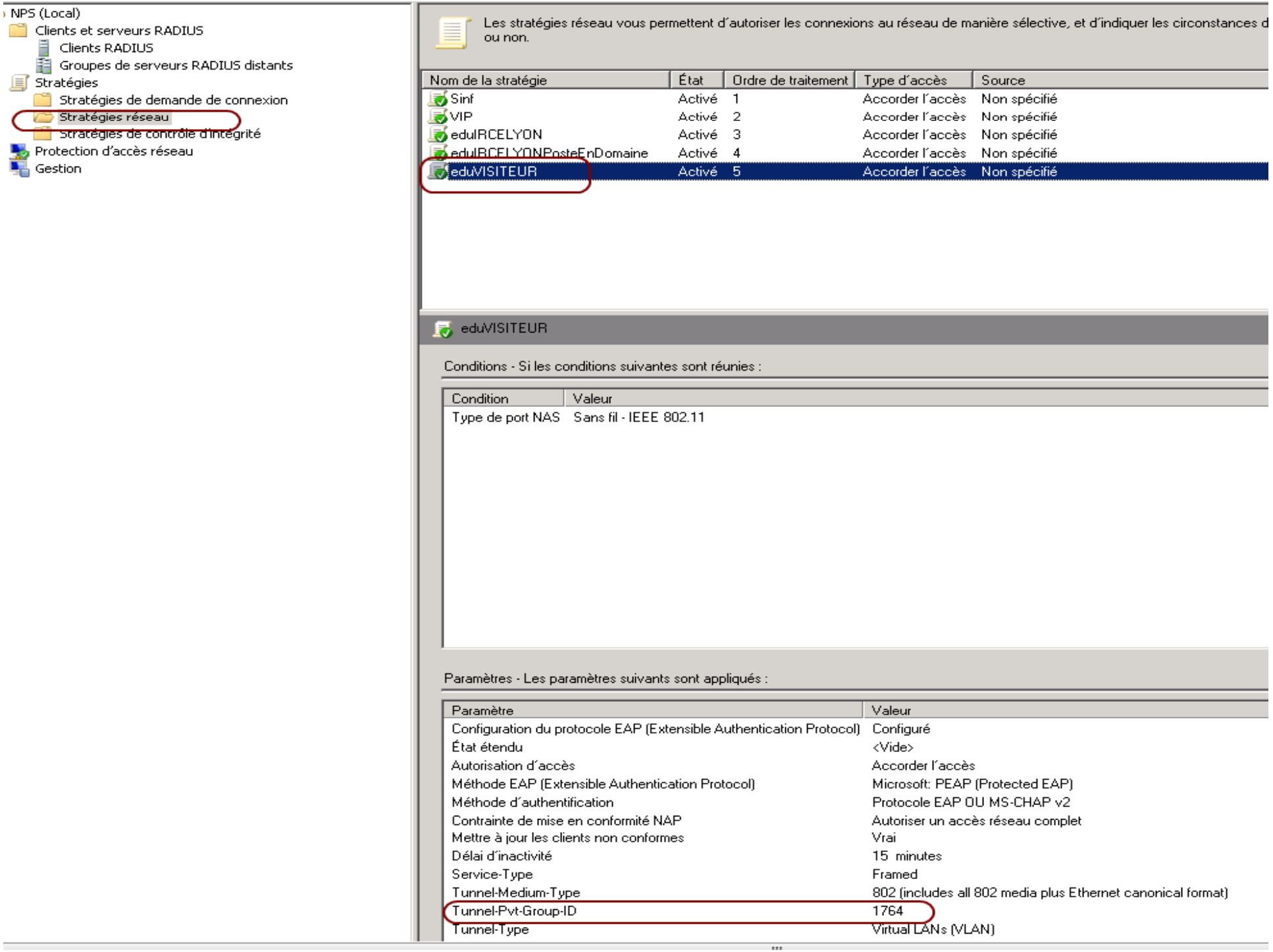
Configuration serveur Radius (NPS)

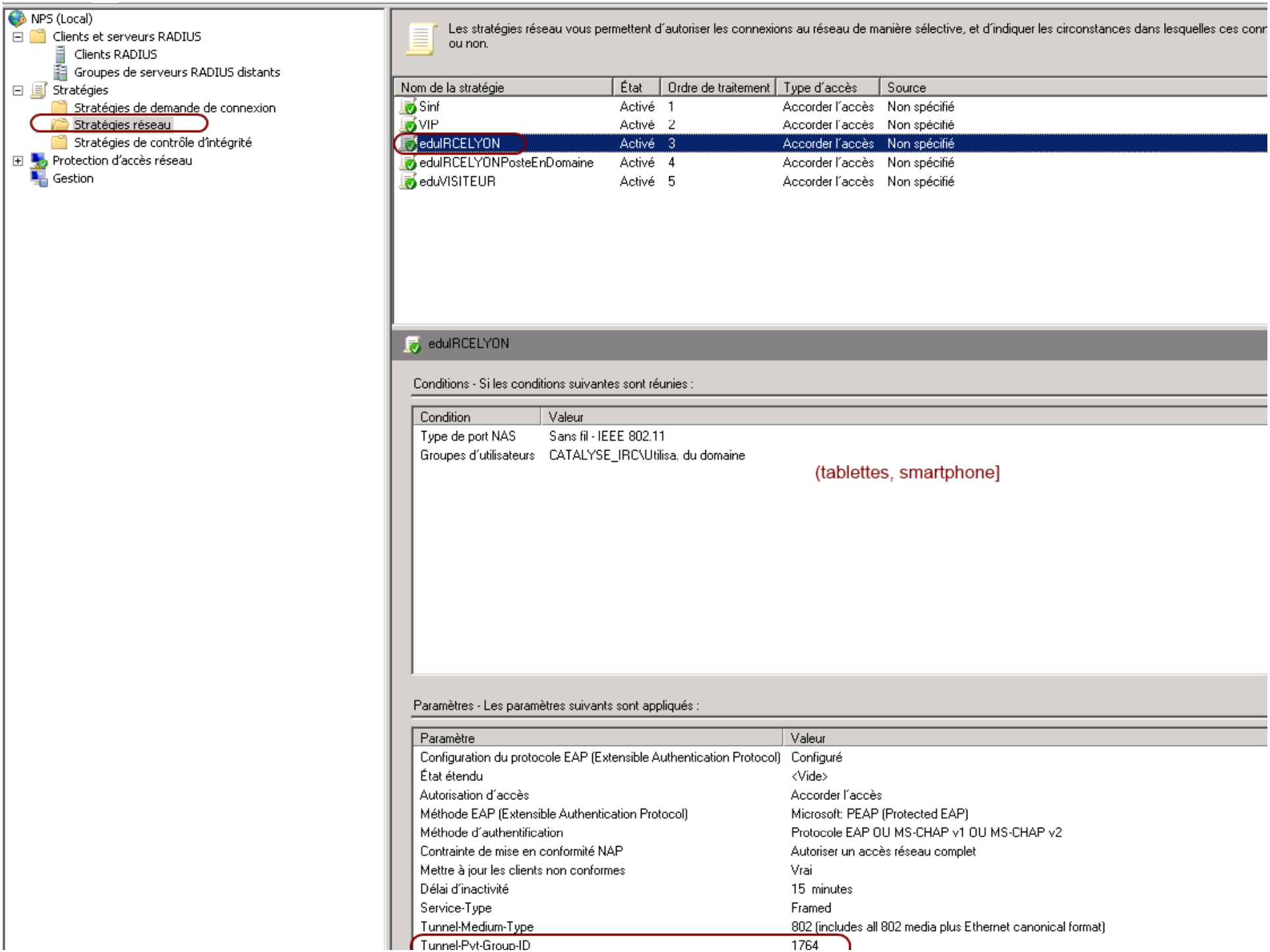
Stratégies de demande de connexion: **les équipements propriétés de l'institut**

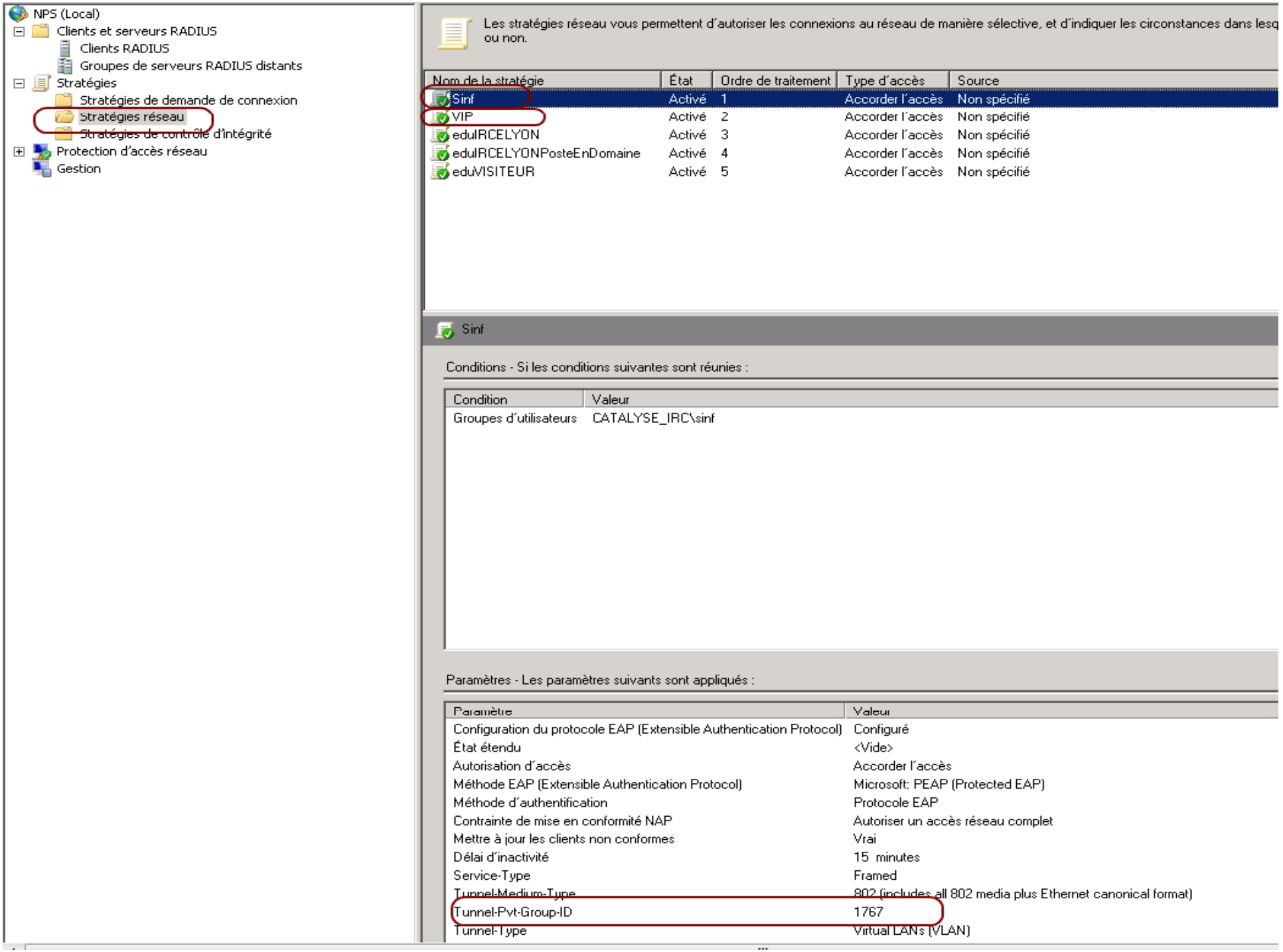


Configuration serveur Radius (NPS)

Stratégies Réseau .. On peut affiner


NPS (Local)
Clients et serveurs RADIUS
Clients RADIUS
Groupes de serveurs RADIUS distants
Stratégies
Stratégies de demande de connexion
Stratégies réseau
Stratégies de contrôle d'intégrité
Protection d'accès réseau
Gestion
Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances d
ou non.
Nom de la stratégie | État | Ordre de traitement | Type d'accès | Source
Sinf | Activé | 1 | Accorder l'accès | Non spécifié
VIP | Activé | 2 | Accorder l'accès | Non spécifié
eduIRCELYON | Activé | 3 | Accorder l'accès | Non spécifié
eduIRCELYONPosteEnDomaine | Activé | 4 | Accorder l'accès | Non spécifié
eduVISITEUR | Activé | 5 | Accorder l'accès | Non spécifié
eduVISITEUR
Conditions - Si les conditions suivantes sont réunies :
Condition | Valeur
Type de port NAS | Sans fil - IEEE 802.11
Paramètres - Les paramètres suivants sont appliqués :
Paramètre | Valeur
Configuration du protocole EAP (Extensible Authentication Protocol) | Configuré
État étendu | <Vide>
Autorisation d'accès | Accorder l'accès
Méthode EAP (Extensible Authentication Protocol) | Microsoft: PEAP (Protected EAP)
Méthode d'authentification | Protocole EAP OU MS-CHAP v2
Contrainte de mise en conformité NAP | Autoriser un accès réseau complet
Mettre à jour les clients non conformes | Vrai
Délai d'inactivité | 15 minutes
Service-Type | Framed
Tunnel-Medium-Type | 802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID | 1764
Tunnel-Type | Virtual LANs (VLAN)


NPS (Local)
Clients et serveurs RADIUS
Clients RADIUS
Groupes de serveurs RADIUS distants
Stratégies
Stratégies de demande de connexion
Stratégies réseau
Stratégies de contrôle d'intégrité
Protection d'accès réseau
Gestion
Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces conn
ou non.
Nom de la stratégie | État | Ordre de traitement | Type d'accès | Source
Sinf | Activé | 1 | Accorder l'accès | Non spécifié
VIP | Activé | 2 | Accorder l'accès | Non spécifié
eduIRCELYON | Activé | 3 | Accorder l'accès | Non spécifié
eduIRCELYONPosteEnDomaine | Activé | 4 | Accorder l'accès | Non spécifié
eduVISITEUR | Activé | 5 | Accorder l'accès | Non spécifié
eduIRCELYON
Conditions - Si les conditions suivantes sont réunies :
Condition | Valeur
Type de port NAS | Sans fil - IEEE 802.11
Groupes d'utilisateurs | CATALYSE_IRC\Utilisa. du domaine
(tablettes, smartphone]
Paramètres - Les paramètres suivants sont appliqués :
Paramètre | Valeur
Configuration du protocole EAP (Extensible Authentication Protocol) | Configuré
État étendu | <Vide>
Autorisation d'accès | Accorder l'accès
Méthode EAP (Extensible Authentication Protocol) | Microsoft: PEAP (Protected EAP)
Méthode d'authentification | Protocole EAP OU MS-CHAP v1 OU MS-CHAP v2
Contrainte de mise en conformité NAP | Autoriser un accès réseau complet
Mettre à jour les clients non conformes | Vrai
Délai d'inactivité | 15 minutes
Service-Type | Framed
Tunnel-Medium-Type | 802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID | 1764


NPS (Local)
Clients et serveurs RADIUS
Clients RADIUS
Groupes de serveurs RADIUS distants
Stratégies
Stratégies de demande de connexion
Stratégies réseau
Stratégies de contrôle d'intégrité
Protection d'accès réseau
Gestion
Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesq
ou non.
Nom de la stratégie
État
Ordre de traitement
Type d'accès
Source
Sinf
Activé
1
Accorder l'accès
Non spécifié
VIP
Activé
2
Accorder l'accès
Non spécifié
eduIRCELYON
Activé
3
Accorder l'accès
Non spécifié
eduIRCELYONPosteEnDomaine
Activé
4
Accorder l'accès
Non spécifié
eduVISITEUR
Activé
5
Accorder l'accès
Non spécifié
Sinf
Conditions - Si les conditions suivantes sont réunies :
Condition
Valeur
Groupes d'utilisateurs
CATALYSE_IRC\sinf
Paramètres - Les paramètres suivants sont appliqués :
Paramètre
Valeur
Configuration du protocole EAP (Extensible Authentication Protocol)
Configuré
État étendu
<Vide>
Autorisation d'accès
Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)
Microsoft: PEAP (Protected EAP)
Méthode d'authentification
Protocole EAP
Contrainte de mise en conformité NAP
Autoriser un accès réseau complet
Mettre à jour les clients non conformes
Vrai
Délai d'inactivité
15 minutes
Service-Type
Framed
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID
1767
Tunnel-Type
Virtual LANs (VLAN)

Log

Événement 6278, Microsoft Windows security auditing.

Général | Détails

Le serveur NPS a accordé l'accès total à un utilisateur car l'hôte répond aux critères définis par la stratégie d'intégrité.

Utilisateur :
- ID de sécurité : CATALYSE_IRC\PEGASE$
- Nom de compte : host/pegase.catalyse.cnrs.fr
- Domaine du compte : CATALYSE_IRC
- Nom de compte complet : catalyse.cnrs.fr/Supports/Sinf/PEGASE

Ordinateur client :
- ID de sécurité : NULL SID
- Nom de compte : -
- Nom de complet complet : -
- Version du système d'exploitation : -
- Identificateur de la station appelée : 000B860C9C00
- Identificateur de la station appelante : C0CB38780E30

Serveur NAS :
- Adresse IPv4 du serveur NAS : 134.214.200.28
- Adresse IPv6 du serveur NAS : -
- Identificateur du serveur NAS : 134.214.200.28
- Type de port du serveur NAS : Sans fil - IEEE 802.11
- Port du serveur NAS : 0

Client RADIUS :
- Nom convivial du client : ControleurWifi
- Adresse IP du client : 134.214.200.28

Informations détaillées de l'authentification :
- Nom de la stratégie proxy: CatalyseOrdinateurs
- Nom de la stratégie réseau : eduIRCELYONPosteEnDomaine
- Fournisseur d'authentification : Windows
- Serveur d'authentification : ares.catalyse.cnrs.fr
- Type d'authentification : PEAP
- Type EAP : Microsoft: Carte à puce ou autre certificat
- Identificateur de la session du compte : -