Authentification Forte

Fouad YAHIA
Service Informatique
Institut de Physique Nucléaire d'Orsay
yahia@ipno.in2p3.fr

Le Plan

1. L’origine du projet
2. L’évolution du projet
3. Choix de la technologie
4. Pré-requis
5. Infrastructure de clés publiques
6. Le serveur RADIUS
7. Le serveur VPN
8. Configuration du client
9. Bilan

L'origine du projet

- L'accès au réseau IPN n'est autorisé qu'aux machines configurées et administrées par le service informatique de l'IPN

- **Origine**
  - Accès sûr des machines au réseau Wifi du laboratoire

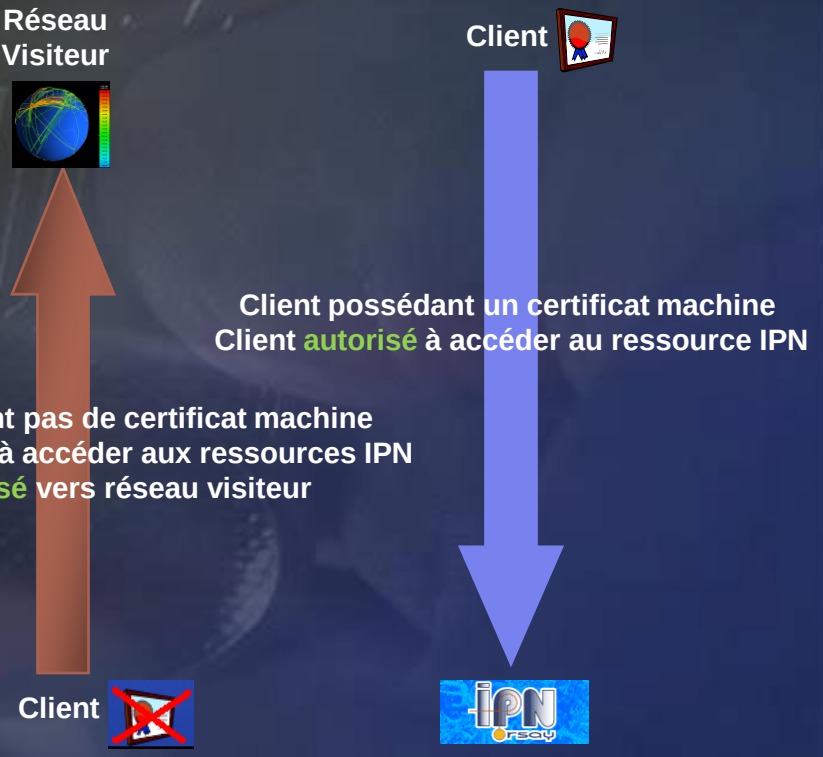
- **L'existant**
  - Le réseau wifi de l'institut est sécurisé par clé WEP
    - ✓ La durée de vie d'une clé WEP est très réduite
    - ✓ Accès autorisé seulement sur le réseau visiteur (uniquement le web)
  - Le réseau filaire de l'institut est sécurisé de la manière suivante
    - ✓ Chaque machine s'authentifie par son adresse MAC sur un port particulier du commutateur

L’évolution du projet

- Sécuriser le réseau WIFI
- Mise en place d’une plate forme VPN
- Sécuriser le réseau filaire avec l’authentification 802.1X

Contraintes :

- Administration légère
- Gestion automatisée
- Authentifier les machines
- Authentification sûre
- Possibilité d’évolution
- Clients hétérogènes



Client = client wifi ou client Filaire (Linux, Windows)

Choix de la technologie

La méthode d'authentification ?

- **La méthode la plus robuste est EAP-TLS (Transport Layer Security)**

EAP-TLS = Une authentification mutuelle entre le client et le serveur par certificat

Utiliser quel Certificat ?

- **Choix du certificat**

  CNRS-xxx ? ---> ça ne correspond pas au cahier des charges !

  - **Certificat CNRS-xxx est juste destiné à authentifier le client**
    - **Signer le courrier électronique**
    - **Recevoir des courriers électroniques chiffrés**
    - **Accéder à des services Internet nécessitant une authentification par certificat**
  - **Déploiement automatique de certificat par GPO (Group Policy Object)**

Solution ?

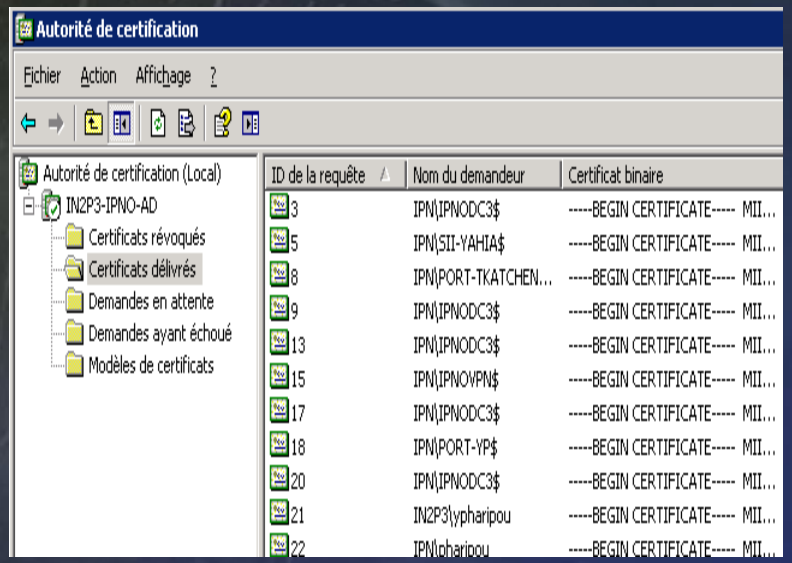
- **Adopter une Infrastructure de clés publiques propre à nous « ipno.in2p3.fr » qui génère des certificats X509**

Pré-requis

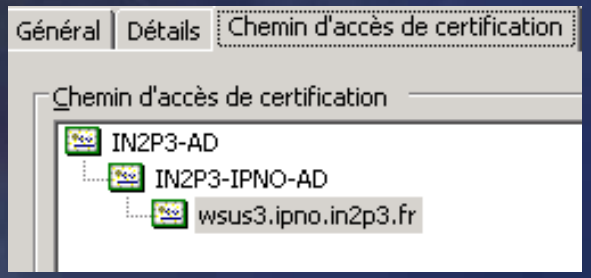
- Windows server 2003
  - Active Directory pour centralisation des comptes
  - IIS (Internet Information Service) 6.0 installé, ASP (Active Server Pages) installé et autorisé
  - Déploiement automatiquement de certificats par GPO
- Deux autorités de certifications d'entreprise
  - Une autorité de certification Racine d'entreprise « IN2P3-AD » (IIS n'est pas installé)
  - Une autorité de certification Secondaire d'entreprise « IN2P3-IPNO-AD »
- Deux serveurs Radius IAS (Internet Authentication Service) redondant
  - Paramétrage des deux serveurs IAS installés sur les deux contrôleurs de l'IPNO
- Un serveur VPN (L2TP/IPSEC) Layer 2 Tunneling Protocol
  - Membre du domaine IPNO
  - Paramétrage du protocole L2TP/IPSEC

Infrastructure de clés publiques PKI

Un système permettant une authentification et une certification de l'identité de l'utilisateur par une tierce partie (Associer des clés publiques à des utilisateurs)



- **Les fonctionnalités**
  - **Serveur autorité de certification**
  - **Intégration Active Directory**
  - **Enrôlement automatique**
  - **Modèles de certificats modifiables**
  - **Séparation des rôles d'administration**
  - **Application web d'enregistrement**
  - **Audit/journalisation**



Le serveur RADIUS

- Une serveur RADIUS est un service AAA
  AAA= Authentification, Autorisation, Accounting

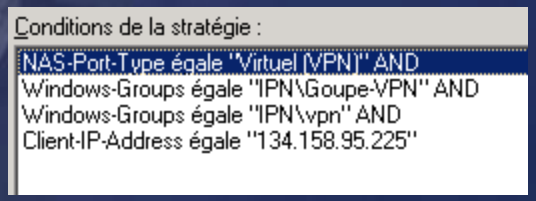
Le service IAS peut effectuer une authentification, une autorisation et une gestion des comptes centralisées pour différentes connexions réseau

- Paramétrage du serveur IAS
  - Un client radius (Borne Wifi, Switch ou serveur VPN…)
  - Les méthodes d'authentification
  - Une stratégie d'accès dépend du client Radius

  - Exemple de paramétrage d'une stratégie 802.1x (Réseau Filaire)

Service-Type	RADIUS Standard	Framed
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	2
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

  - Autre exemple pour une stratégie VPN
    - Client Radius (serveur VPN)
    - Les conditions de la stratégie VPN

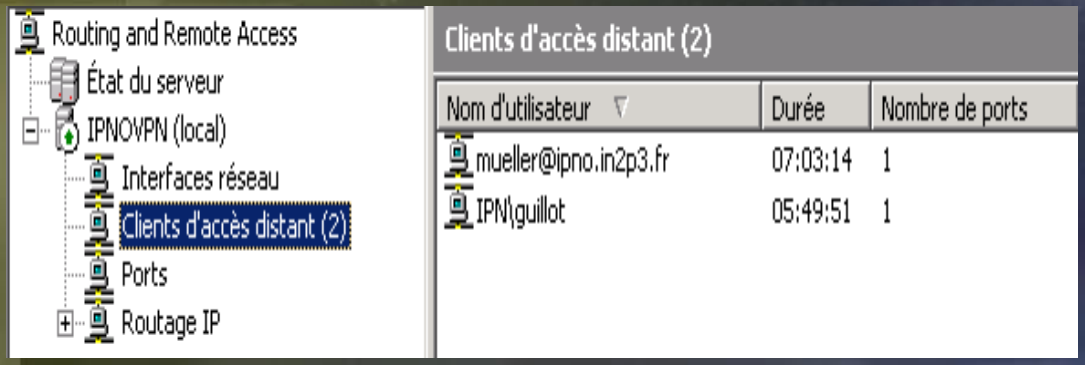


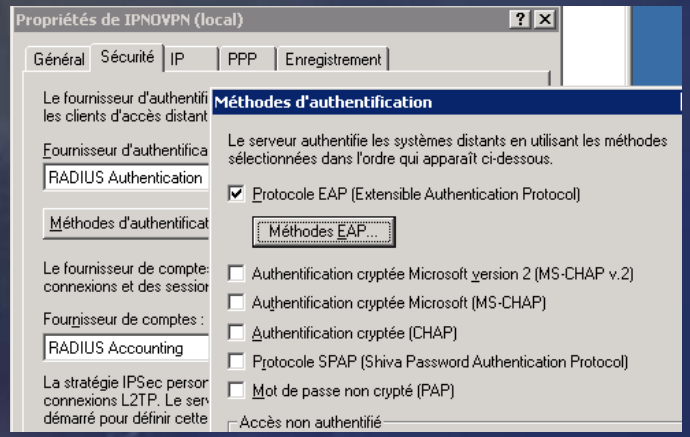
Le serveur VPN-L2TP/IPSEC

Rôle initial d'un VPN ?

Avantages :

- **Assurer des échanges sécurisés et une qualité de service**
- **Répondent aux besoins fondamentaux**
  - ✓ **Cryptage des données IPSEC (Internet Protocol Security)**
  - ✓ **Authentification des hôtes avec EAP-TLS (MS-CHAP v2 ou cas !)**
  - ✓ **Contrôle d'intégrité des données**
  - ✓ **Assurer la confidentialité aux données**





Configuration du client
« Réseau filaire »

Pour Windows

Windows offre un support natif d'EAP-TLS dans le système d'exploitation

Pour Linux « Ubuntu 8.04 LTS »

Il faut installer un ***Supplicant***, puis le configurer

Paramétrage du client Linux

- Exportation du certificat de notre autorité de certification
- Exportation certificat (clé publique et clé privée) de l'utilisateur
- Conversions des certificats
  - openssl x509 -inform DER -in in2p3-ad.cer -out RootA.pem
  - openssl pkcs12 –in testlinux.pfx –out testlinux.pem -nodes
- Configuration du fichier Xsupplicant.conf

Xsupplicant.conf

```
network_list = all
default_netname = default
logfile = /var/log/xsupplicant.log
default_interface = eth0
default
{
    type = wired
    allow_types=eap_tls
    identity="testlinux"

eap_tls
                {
     user_cert = testlinux.pem          « Certificat de l'utilisateur »
     user_key = testlinux.pem           « Clé privée de l'utilisateur »
     user_key_pass = "Test$802"         « Mot de passe de la clé privée »
    root_cert = RootA.pem               « Certificat de l'autorité racine »
    root_dir = /etc/xsupplicant/cert/
     chunk_size = 1398
     random_file = /dev/urandom
     session_resume=yes
                }
}
```

Lancer le démon : xsupplicant -c /etc/xsupplicant/xsupplicant.conf -i eth0 -d 1 -f

Bilan

Pour le WIFI (Pas en production)

- Authentification EAP-TLS fonctionne
- Projet Portail Captif en cours..

Pour le VPN (en production)

- La plate forme VPN(L2TP/IPSEC) est en production (~35 physiciens)
- fonctionne avec EAP-TLS et MS-CHAP v2 (en cas de problème)

Pour le Réseau Filaire (Pas encore en production)

- Authentification EAP-TLS fonctionne (mais avec certif user)
- Pas encore en production (on voulait combiner deux méthodes d'authentification EAP-TLS et l'authentification par adresse MAC


Questions ?

Schéma conceptuel du réseau