Contrôle d’accès au réseau

Emmanuel REUTER

26 Juin 2014

IFSTTAR

I. Glossaire

- **NAC :** *Network Access Control*
- ***NAS** : Network Access Server*
- ***GVRP** : Generic Vlan Registration Protocol*
- **Radius** : Remote Authentication Dial-In User Service
- **Attribute value pairs :** Attributs renvoyés par le radius
- **LDAP** : Lightweight Directory Access Protocol

I. IFSTTAR : Etat des lieux

- Architecture réseau complexe distribuée sur le territoire Français
- 7 sites IFSTTAR
- Plus de 250 switches
- Plus de 1700 machines
- Environ 120 portables
- Environ 90 tablettes
- +… BYOD

I. Problématique du contrôle d'accès au réseau

- **Enjeu : Faire en sorte que chacun des réseaux informatiques restent protégés et que les utilisateurs aient accès aux ressources**
  - **Personnels de l'IFSTTAR**
  - **Thésards, personnes de passage**
  - **Prestataires**
  - **Machines pilotées depuis l'extérieur**
  - **Les filiales**

I. Problématique du contrôle d'accès au réseau

- **Chaque personnel de l'IFSTTAR doit pouvoir se déplacer sur tous les sites**
  - Portables via le Wifi
  - Portables connectés sur le réseau filaire
  - Pieuvre IP de conférence
- **Eviter la multiplication des adresses MAC des machines dans les différents DHCP**
- **Dans tous les cas, il faut diminuer l'intervention humaine pour ce type d'urgence**

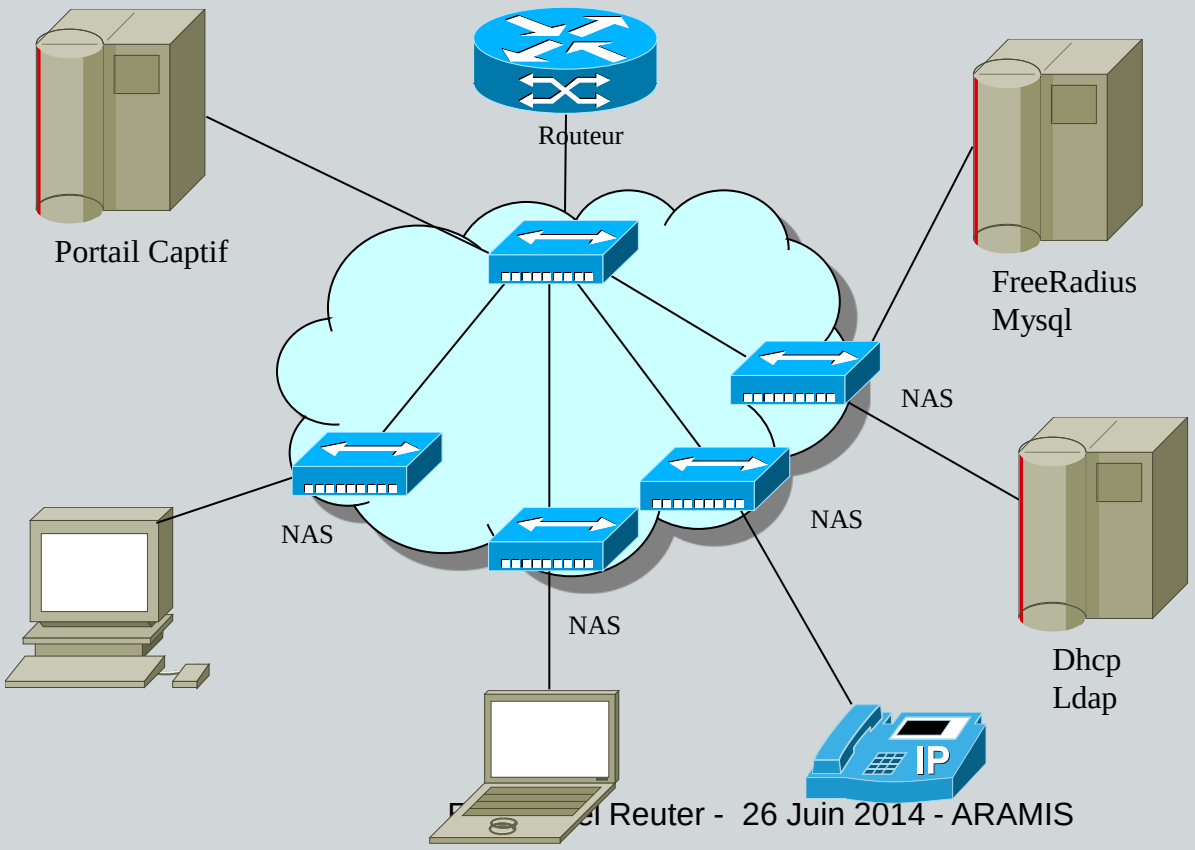
II. Solution

- Basée sur un LDAP central
  - Un serveur DHCP par site qui récupère ses données dans le LDAP IFSTTAR
    - Objectclass dhcpHost
    - Attribut dhcpHWAddress
    - Attribut dhcpVlan
    - Attribut ieee802
  - Une base de données Mysql pour conserver les logs des connexions
  - Tout le réseau est configuré de la même manière : fixe ou migrant
    - Une seule déclaration des adresses MAC dans le LDAP, quelque soit le site
    - Une machine peut se connecter n'importe où

II. Solution

- dhcpStatements: fixed-address 137.121.xx.193
- dhcpVlan: xx
- objectClass: dhcpHost
- objectClass: dhcpOptions
- objectClass: ieee802Device
- objectClass: radiusprofile
- dhcpOption: host-name aruba-ap03
- dhcpOption: broadcast-address 137.121.xx.255
- dhcpOption: routers 137.121.xx.201
- dhcpOption: subnet-mask 255.255.255.0
- dhcpHWAddress: ethernet 00:0b:86:ca:d3:88
- macAddress: 00:0b:86:ca:d3:88
- uid: 000b86cad388
- radiusTunnelAssignmentId: xx
- radiusTunnelPrivateGroupId: xx
- radiusTunnelType: VLAN
- radiusTunnelMediumType: IEEE-802

III. Architecture de la solution



III. Architecture de la solution

- Un replicat LDAP par site
- Un DHCP local qui interroge le LDAP local
  - Dans la même base LDAP que le radius
  - Intérêt de mettre de la redondance
- Le backup est assuré, par la configuration des :
  - Switches vers le radius de Marne pour l'accès au réseau
  - Cœurs de réseaux pour le secours DHCP vers Marne

IV. Solution de mobilité

- Comment rendre les machines toute mobile
- Sans aucune intervention d'un administrateur réseau
  - Utilisation du radius
  - Programmation et utilisation de ulang

- Une machine qui se connecte hors site
  - Machine IFSTTAR donc accès autorisé
  - Problématique : Dans quel VLAN

IV. Solution de mobilité

- Gestion du VLAN
  - On re-écrit le numéro de Vlan en fonction du site
  - On utilise le ulang de radius
  - /etc/freeradius/sites-enabled/default

IV. Solution de mobilité

```
Auth-Type CHAP {
# on réécrit les adresses MAC
if (request:User-Name =~ /^00085d/i) { # ce test permet de savoir si un ToIP veut s'authentifier…
        update control {
            Cleartext-Password := "%{User-Name}"
        }
        ok
        }
        if (control:Cleartext-Password =~ /ethernet (..):(..):(..):(..):(..):(..)/i ) {
        update control {
        Cleartext-Password := "%{1}%{2}%{3}%{4}%{5}%{6}"
        }
        ok
        }
```

– # l'attribut LDAP qui est récupéré est uid= adresse MAC

IV. Solution de mobilité

```
# Mobilite inter-sites. Si la machine est authentifiee  et hors site, alors Vlan de mobilite
#
if (ok) { # Donc authentification OK
# On vérifie le UserDN LDAP :
# Si c'est le site, alors aucun changement
                if ( control:Ldap-UserDn=~/satory/) {
                        ok
                }
                else {
# Sinon machine IFSTTAR donc redirection vers un VLAN de Mobilité
# Simple, non !
                        update reply {
                                Tunnel-Private-Group-Id := 1010
                        }
                }
                ok
            }
        }
# L'accès de la machine est garantie, et cette dernière est redirigée vers le Vlan de mobilité!
# Fallait y penser ;-)
```

IV. Solution de mobilité

- Pour l'authentification sur du matériel H3C/HP Networking
- Auth-Type PAP {

```
if (request:User-Name =~ /^00809f/i) {
update control {
        Cleartext-Password := "%{User-Name}"
}
ok
}
if (control:Cleartext-Password =~ /ethernet (..):(..):(..):(..):(..):(..)/i ) {
update control {
Cleartext-Password := "%{1}%{2}%{3}%{4}%{5}%{6}"
}
ok
}
```

Etc..

IV. Solution de mobilité

- En résumé
  - On vérifie que la machine est déclarée dans le LDAP
  - On lisse l'adresse Ethernet pour avoir une pseudo standardisation
    - Par exemple, différence entre HP Procurve et les H3C (xx:yy et XX-YY….)
  - On vérifie la provenance de l'adresse Ethernet
    - Si site local, alors VLAN LDAP renvoyé au switch
    - Sinon, VLAN de mobilité renvoyé au switch

V. Les nomades

- Pour contrôler les nomades
- /etc/freeradius/module/perl
  - perl {
  - #
  - # The Perl script to execute on authorize, authenticate,
  - # accounting, xlat, etc. This is very similar to using
  - # 'rlm_exec' module, but it is persistent, and therefore
  - # faster.
  - #
  - # Créer son propre module PERL
  - module = ${confdir}/recordMac.pl

V. Les nomades

- Pour contrôler les nomades
- /etc/freeradius/radiusd.conf
- Dans la partie module
- **********
- $INCLUDE ${confdir}/modules/perl
-
- Dans la partie authorize
- **********
- # Adding module perl
- perl

- Ainsi à chaque demande d'accès, il est possible de faire exécuter le script PERL
  - Vérification, par exemple, lors de la validité d'un certificat
  - Enregistrement des adresses Wifi Ethernet

V. Les nomades

- http://wiki.freeradius.org/modules/Rlm_perl
- Ma fonction

```
sub recordMAC {
 # Loads some external perl and evaluate it
 my ($filename,$username,$calling_station_id,$nas_address) = @_;
 #my $filename="/var/tmp/recordMAC.lst";


 local *FH;
 open FH, ">>$filename " or die "open '$filename' $!";
 print FH "$username\t$calling_station_id,\t$nas_address \n";
 local($/) = undef;
 my $sub = <FH>;
 close FH;
}
```

Questions ?