Lucas Tardy – Antoine Girardey

Fiche technique RADIUS

1)

La configuration pour le radius utilisateur sur un switch est la suivante

La partie « Radius-server host » permet de dire quel est le serveur RADIUS qui va être utiliser.

```
SWRDC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWRDC(config)#aaa new-model
SWRDC(config)#aaa authentication dot1x default group RADIUS
SWRDC(config)#aaa authorization network default group RADIUS
SWRDC(config)#dot1x system-auth-control
SWRDC(config)#Radius-server host 172.19.100.2 auth-port 1812 acct-port 1813 key PwdClientRADIUS
SWRDC(config)#Radius-server host 172.19.100.2 auth-port 1812 acct-port 1813 key @password25
SWRDC(config)#
```

Switch radius utilisateur + SSH

La partie « aaa authentication login » permet d'activer l'authentification avec un utilisateur d'un domaine, la partie « aaa authorization exec » permet d'être directement en mode « enable ».

La partie écrite dans le « int range fa0/1-24 » permet d'activer l'authentification via radius avec spanning-tree sur des ports spécifiques pour les utilisateurs qui se connectent avec un compte du domaine.

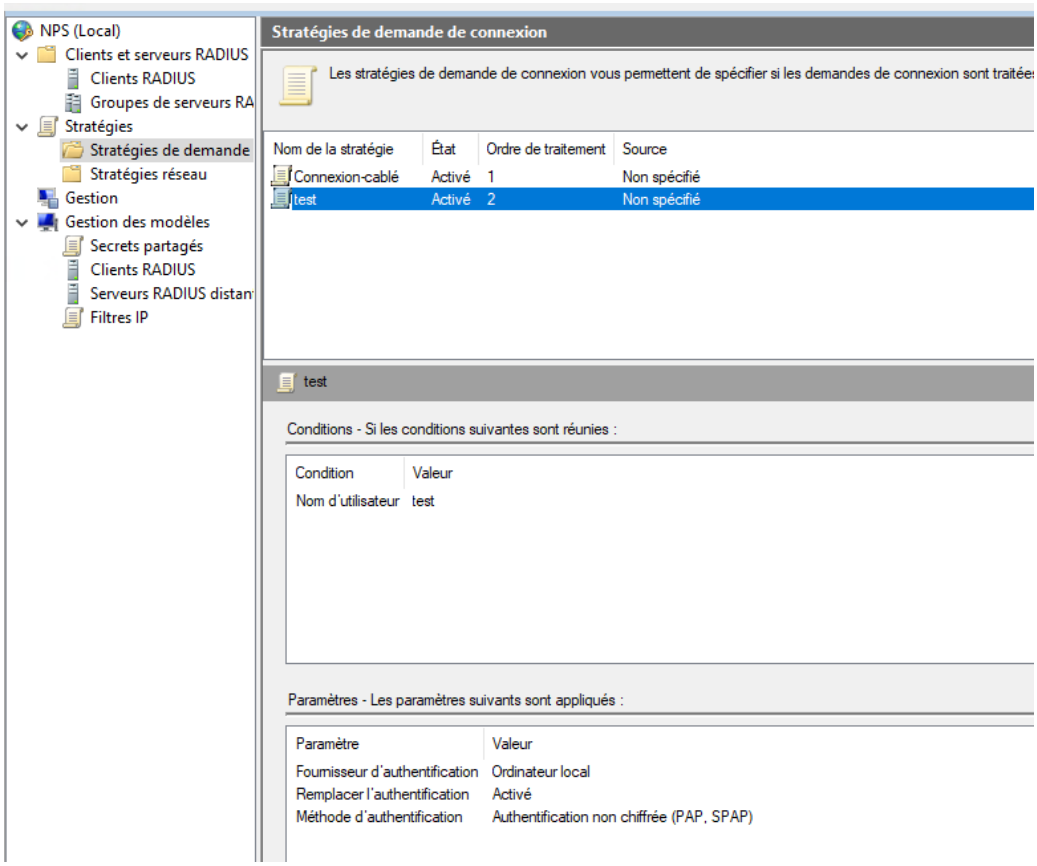
```
SW1ER>
SW1ER>
SW1ER>en
Password:
SW1ER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1ER(config)#aaa new-model
SW1ER(config)#aaa authentication login default group radius
SW1ER(config)#aaa authorization exec default group radius
SW1ER(config)#aaa authentication dot1x default group radius
SW1ER(config)#aaa authorization network default group radius
SW1ER(config)#
SW1ER(config)#radius-server host 172.19.100.2 auth-port 1812 acct-port 1813 key 7 13250713181F132539207A66
 Warning: The CLI will be deprecated soon
 'radius-server host 172.19.100.2 auth-port 1812 acct-port 1813 key 7 13250713181F132539207A66'
 Please move to 'radius server <name>' CLI.
SW1ER(config)#int range fa0/1-24
SW1ER(config-if-range)#switchport mode access
SW1ER(config-if-range)#authentication host-mode multi-host
SW1ER(config-if-range)#authentication port-control auto
SW1ER(config-if-range)#dot1x pae authenticator
SW1ER(config-if-range)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

SW1ER(config-if-range)#exit
SW1ER(config)#dot1x system
SW1ER(config)#dot1x system-auth-control
```

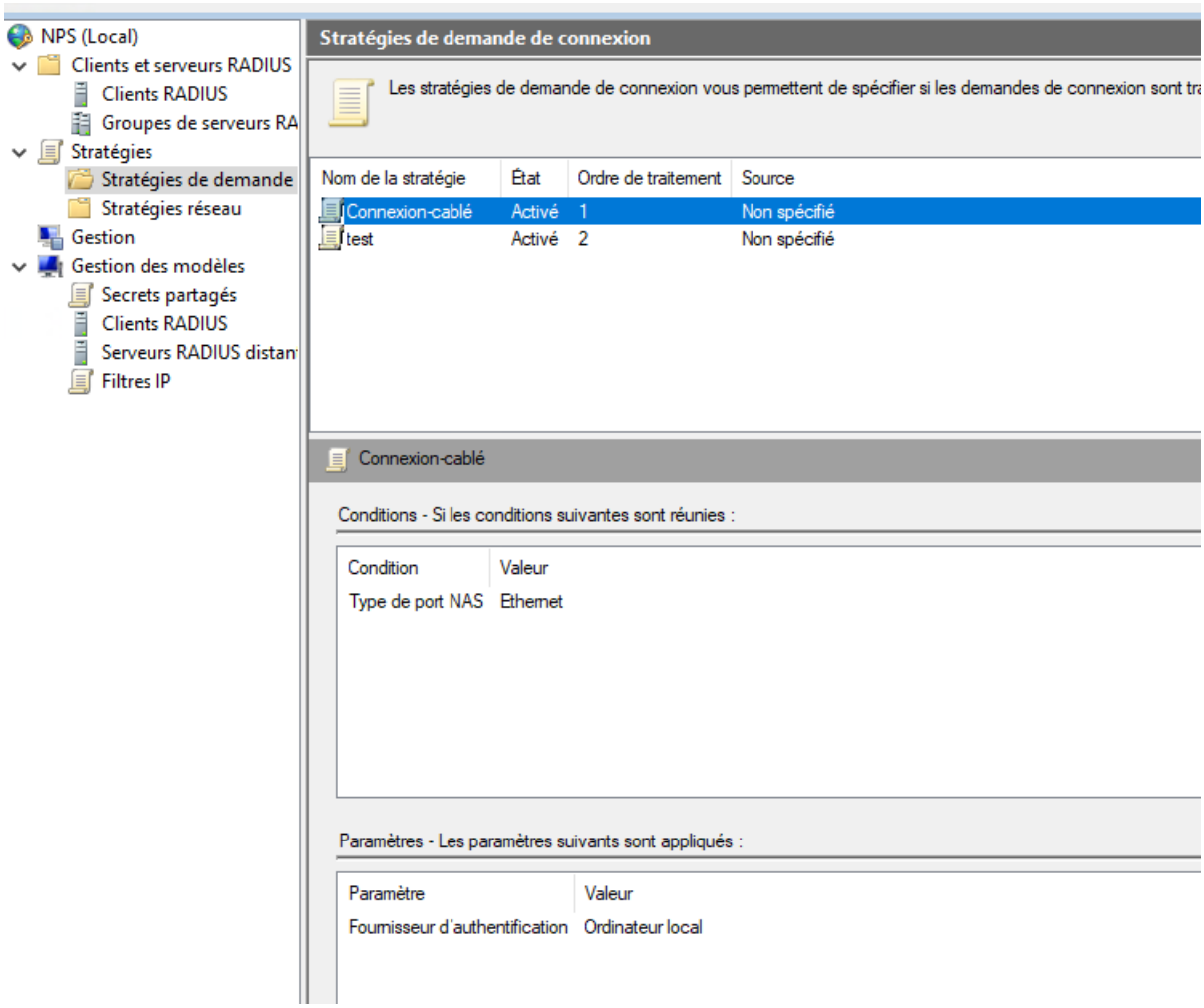
La configuration du switch cœur (switch de niveau 3) et des routeurs est la même pour l'administration à distance sécurisée via Radius :

```
RNET2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RNET2(config)#aaa n
RNET2(config)#aaa new-model
RNET2(config)#aaa authentication login default group radius
RNET2(config)#aaa authorization exec default group radius
RNET2(config)#
RNET2(config)#
RNET2(config)#radius server 172.19.100.2
RNET2(config-radius-server)# address ipv4 172.19.100.2 auth-port 1645 acct-port 1646
RNET2(config-radius-server)# key 7 072F314D5D1A0E0A05165959
RNET2(config-radius-server)#
```

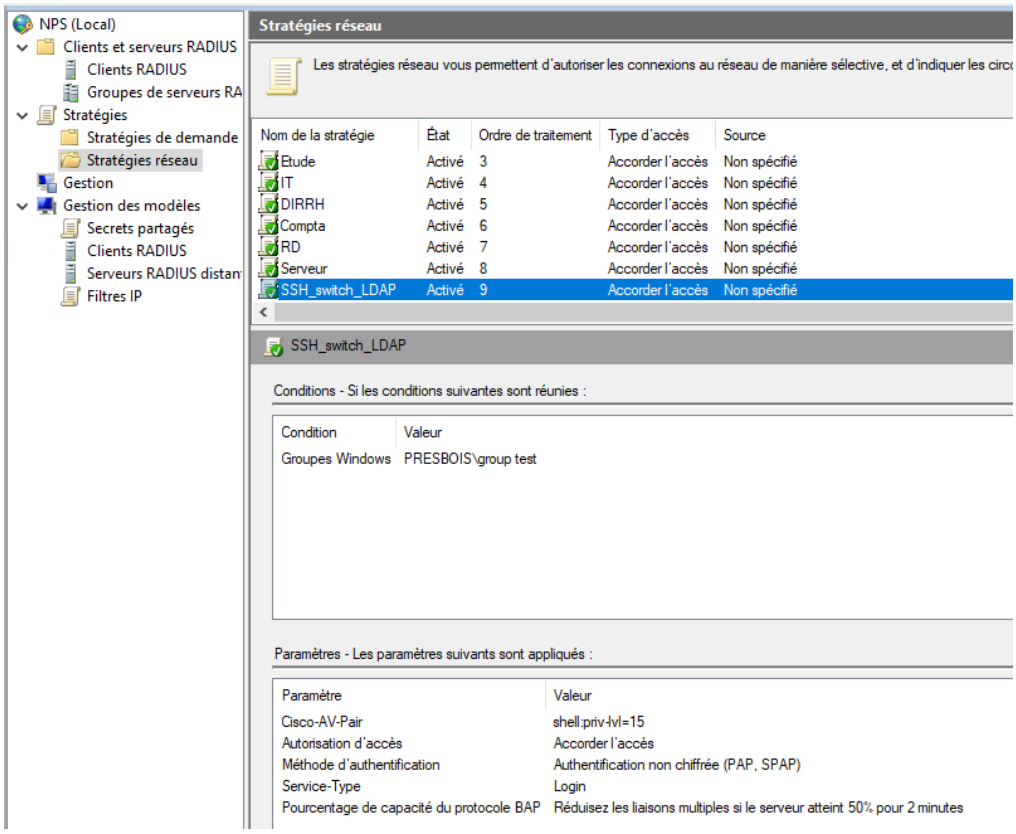
Pour la configuration sur le serveur NPS, il faut créer une stratégie de demande où l'on autorise que l'utilisateur souhaiter peut se connecter via SSH sur les commutateurs:



Voici la stratégie de demande de base qu'il ne faut pas changer :



Voici les stratégie réseau pour se connecter en SSH avec un groupe de sécurité.



Il faut aussi créer les clients RADIUS sur le serveur NPS, chaque client étant un commutateur qui se connecte