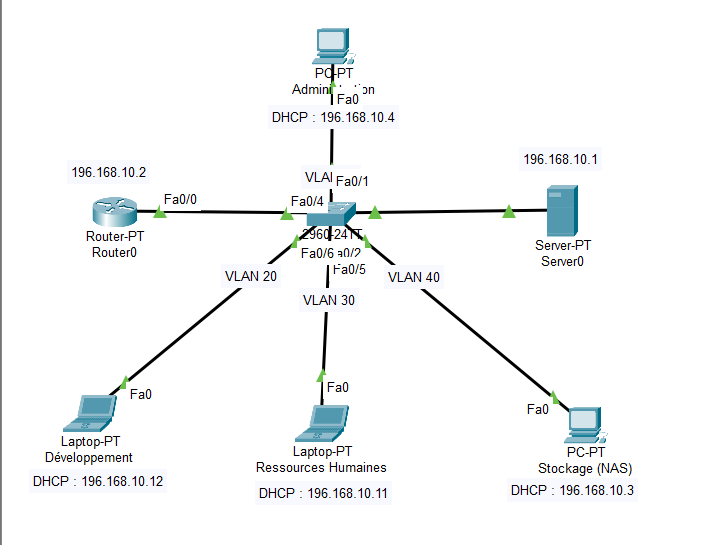
Documentation Projet PiedPiper

*Groupe : Ilan Heas, Vladimir Vitrou, Lucas Molendi, Thomas Braud, Nino Caillaud*

Schéma de notre réseaux sur Packet Tracer :

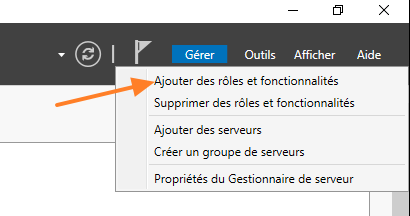


Windows Server : Active Directory, GPO et DHCP

Mise en place de l’active directory (AD), d’une Groupe Policy Object (GPO) et du Dynamic Host configuration Protocol (DHCP) :

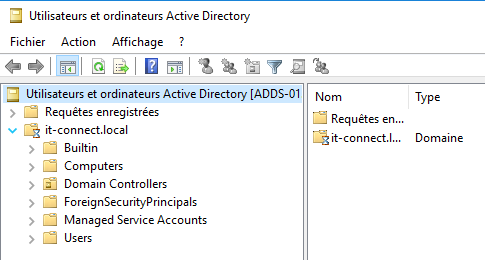
Faire un AD

Une fois que windows fut mit en place sur le serveur grâce à l’image ISO, nous avons entrepris le fait de télécharger des rôles et des fonctionnalités dans le Gestionnaire de serveur.



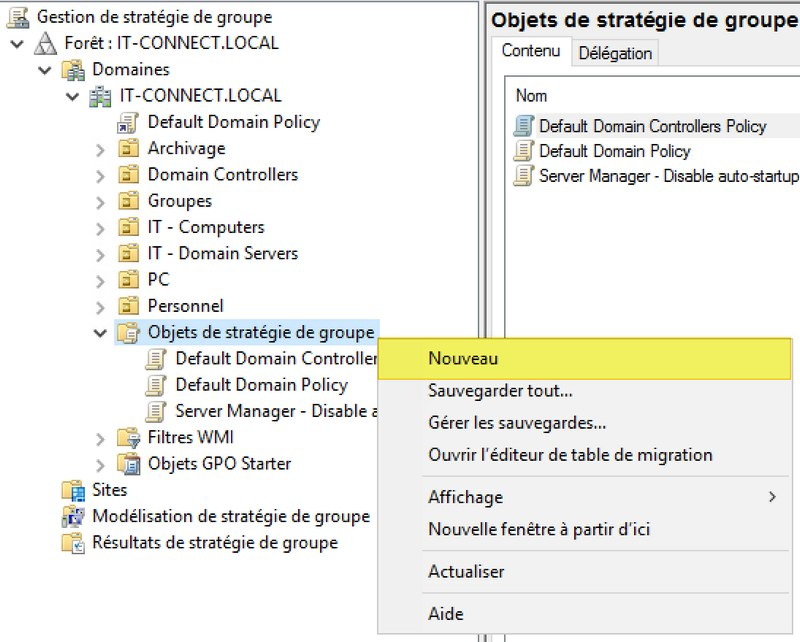
Parmis ces rôles : l’AD, le DHCP et le GPO

Une fois l’AD téléchargé, comme il s'agit d'un tout nouveau domaine dans une nouvelle forêt, nous avons créé une nouvelle forêt que nous avons définit comme le serveur DNS

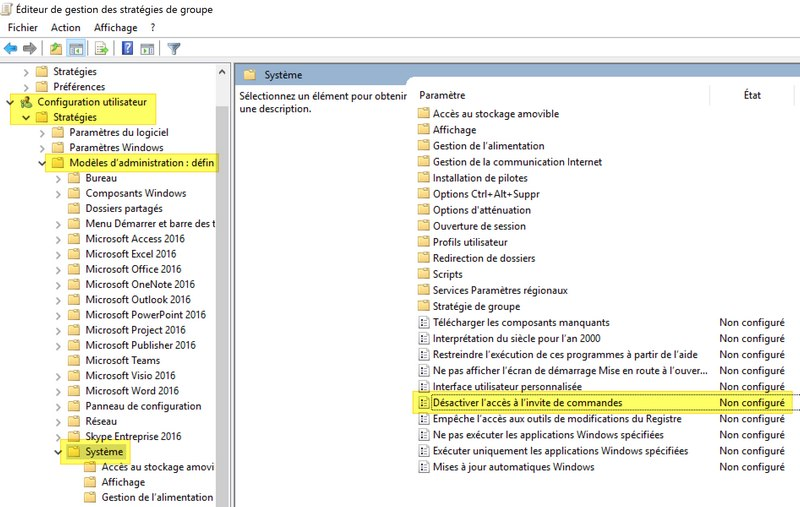


Sur l’image, notre forêt est “it-connect.local”

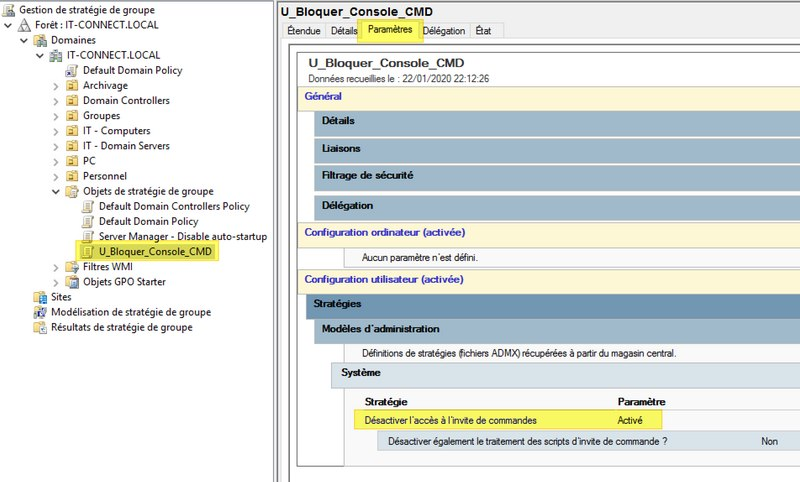
Faire un GPO

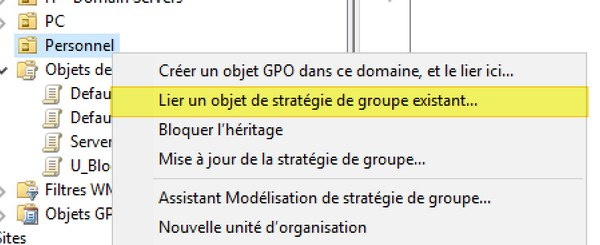


Première chose à faire : ajouter un nouvel objet de stratégie de groupe.



Dans cet exemple, le GPO désactivera l’accès à l’invite de commande pour les utilisateurs

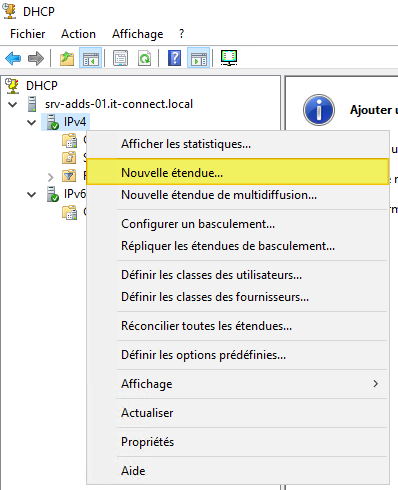


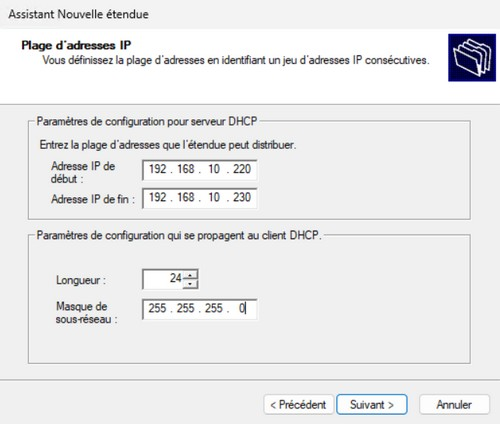


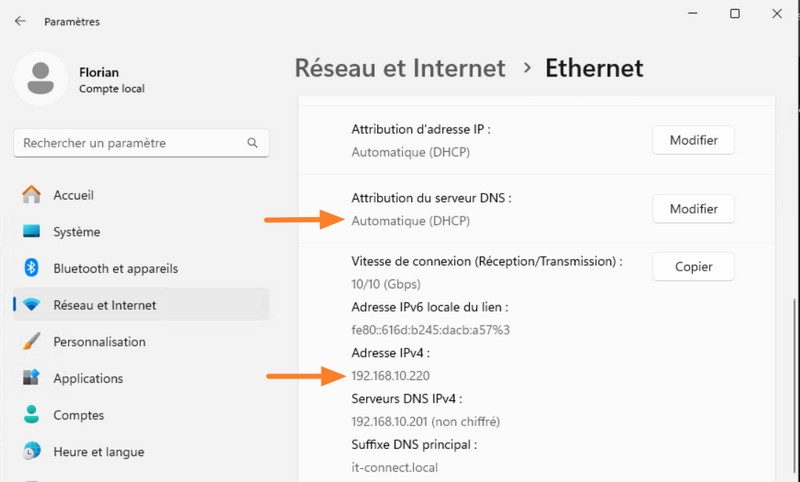
Attention à ne pas oublier de lier l’objet GPO à l’utilisateur (dans l’exemple : “personnel”)

Faire le DHCP :

Pour mettre en place le DHCP, comme pour l’AD, nous avons ajouté une fonctionnalité dans le gestionnaire du serveur, puis, nous avons renseigné notre adresse réseau (sans oublier d’exclure quelques adresses à destinations du routeur, du serveur, etc)







(image du DHCP réussi)

Il y a deux commandes à connaître sous Windows pour gérer un bail DHCP. La première commande va permettre de libérer le bail DHCP au niveau du serveur DHCP, ce qui implique que le PC va perdre son adresse IP :

ipconfig /release

Ensuite, nous pouvons émettre une nouvelle demande d'adresse IP auprès du serveur DHCP grâce à cette seconde commande :

ipconfig /renew

Quelques secondes plus tard, l'ordinateur obtiendra une adresse IP

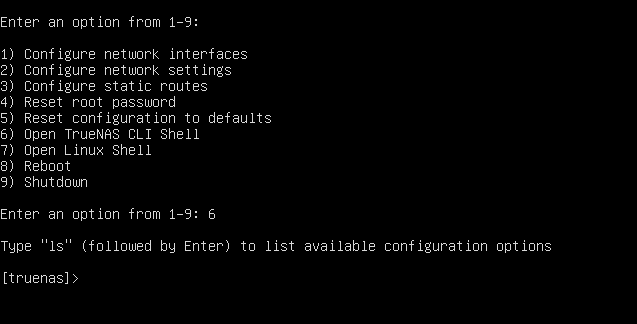
Faire un Pare-Feu :

Le pare-feu est un dispositif qui protège un réseau des tentatives d’intrusions.

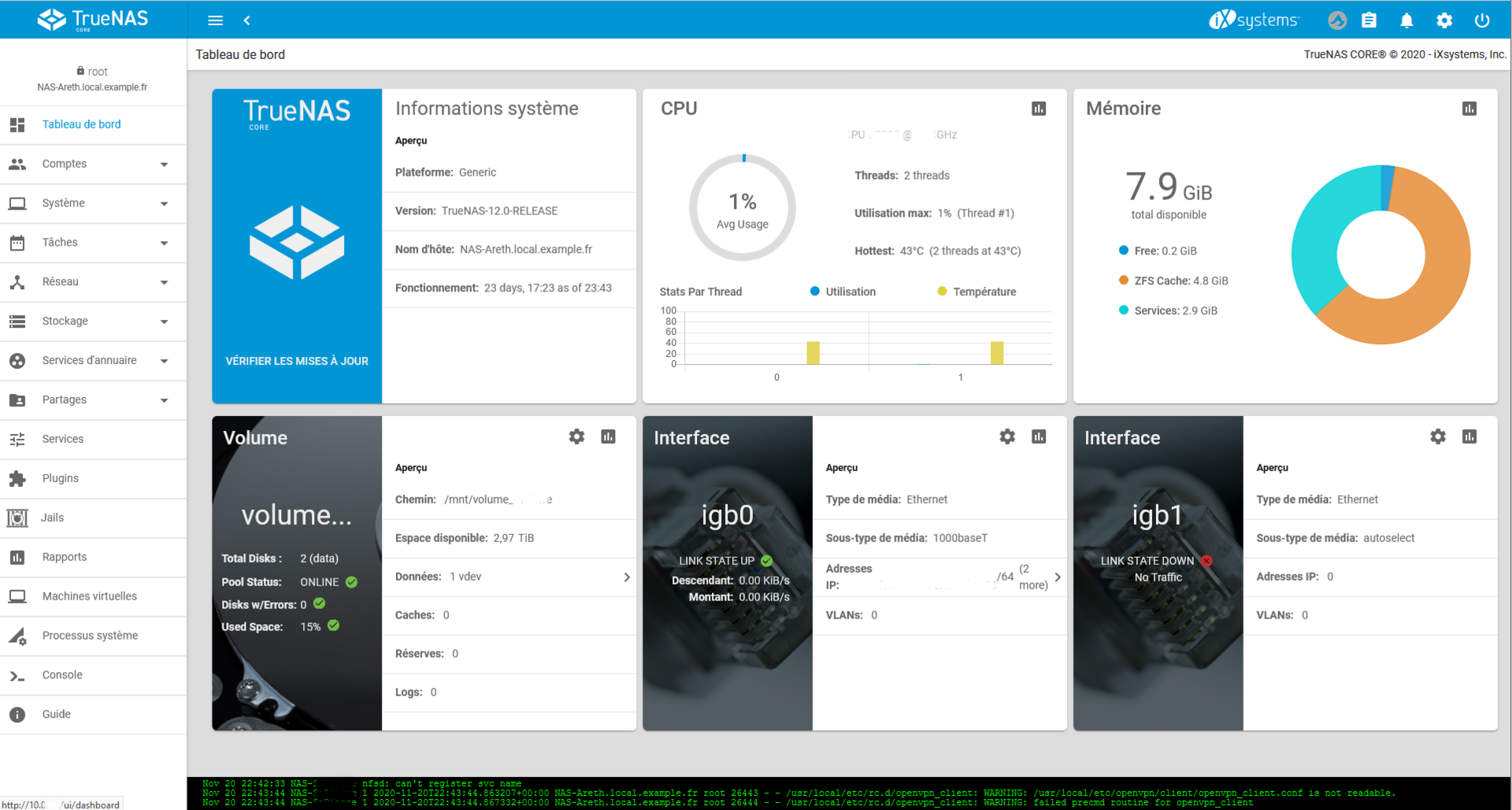
On a mis le fichier ISO de Pfsense sur une clé pour pouvoir l’installer sur un PC. L’installation s’est bien exécutée et s’est terminée. Le problème c’est que le PC qu’on a eu avait juste une entrée réseau, pas de sortie, donc on a pas pu configurer le pare-feu.

NAS  
Le NAS est un serveur de stockage centralisée en réseau qui intègre l’AD

Pour le NAS : on a choisi TrueNAS. Après plusieurs essais, pour l’installer sur des VM, on l’a finalement installé sur un PC directement. Avant de l’installer on a ajouté un disque dur supplémentaire dans le PC. Pour l’installer,on l’a boot a partir d’une clé. L’installation a réussi mais on a pas eu le temps de faire toute la configuration. On a stopper la configuration sur :



Au final le NAS aurait dû être comme ça :



Supervision du réseau

Le but de la supervision du réseau est de vérifier l’état des équipements critiques (PFSENSE, routeur CISCO, switch,serveur Windows, NAS).

Les performances du réseau (bande passante, utilisation CPU/mémoire des équipements)

L'Etat de stockage du NAS.

Pour la supervision du réseau, on voulait passer par Observium, pour cela on a boot un linux sur un pc.

Pour installer Observium, on passe par le Terminal, mais pendant son installation on a rencontré plusieurs erreurs, qui nous ont empêché de l’installer. On a essayé de passer par Zabbix et Nagios, et rencontrer d’autres erreurs, rendant impossible l’installation.

Impossible donc de configurer des alertes pour alerter les administrateurs en cas de panne ou

d’anomalie.

Au final on aurait dû avoir : Avec notre serveur Windows, le DHCP, le NAS,

