|  |  |
| --- | --- |
| formation-informatique-grenoble-cabare  http://[WWW.CABARE.NET](http://WWW.CABARE.NET) **©** | **Accès Réseaux Externes -  sys 32 – Cours & TP -** |
| **http(s)+webdav - vpn - rds**  **Michel Cabaré – Ver 1.1 – dec2017-** |

**Accès Réseaux externes**

**https + webdav – vpn - rds**

**Michel Cabaré – Ver 1.1 – Déc 2017**

[www.cabare.net](http://www.cabare.net) ©

**table des matiÈres**

protocoles Réseau 3

Protocoles lan – SMB – AFP- NFS: 3

Protocoles wan – http – https- webdav- ftp - ftps: 3

Protocoles vpn : 3

Gestion DNS (renvoi sur une adresse ip publique - GANDI) 4

partage Http 5

Pré-requis partage lien http : 5

Test depuis une machine Externe (réseau 4g) 5

Partage de lien http : 6

Webdav 8

Pré-requis webdav: 8

Activation webdav synology: 8

Test client Windows webdav http (5005-9105): 9

Test client Windows webdav https (5006-9106): 12

installation du certificat 12

Connexion depuis l'exterieur 12

Connexion depuis le réseau local - LANr 13

Bloccage 10 Accès infructueux dans les 10 mn: 13

VPN 14

Pré-requis VPN: 14

PPTP - Point to Point Tunnelling Protocol - (Microsoft) : 14

L2TP - Layer Two Tunnelling Protocol + IPSEC (IETF): 14

OPEN VPN (produit libre): 14

Activation VPN Server: 15

Paramétrage Serveur PPTP Synology (microsoft - TCP 1723) : 16

Paramètres Client PPTP windows: 16

Configurer la connexion vpn 17

Se connecter sur cette connexion vpn 20

Créer un lecteur réseau 21

Déconnecter la connexion vpn 21

Paramétrage Serveur L2TP sans IPSEC Synology (IETF – UDP 1701): 22

Paramètres Client L2TP - Windows 10: 22

Paramétrage Serveur OPENVPN (libre - UDP 1194) : 23

Paramètres Client OpenVpn - Windows 10: 24

Synology DS713+ 28

Maj DSM 6.x: 28

# protocoles Réseau

## Protocoles lan – SMB – AFP- NFS:

Pour nos réseaux locaux en entreprise (**LAN** - **Local Area Network**) ou particulier

* **SMB : (Server Message Block)** est un protocole de partage de ressources pour Windows. En 1998, **Microsoft** renomme **SMB** en **CIFS** (**Common Internet File System**). En 2006, **Microsoft** implémente une nouvelle version dans son OS et le nomme **SMB 2**. A noter, **Samba** est le nom de l’implémentation libre de **SMB**.
* **AFP : (Apple Filing Protocol)** est un protocole de partage de fichier utilisé pour **Mac sous OS X**. A noter, **Netatalk** est le nom de l’implémentation libre d’**AFP**
* **NFS : (Network File System)** est un protocole de partage de fichier utilisé pour **Unix** et **Linux**. Lui est déjà libre.

## Protocoles wan – http – https- webdav- ftp - ftps:

Notamment pour internet (**WAN** - **Wide Area Network**)

* **FTP : (File Transfer Protocol)** est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. Nécessite un client et un serveur.
* **FTPS : (File Transfer Protocol)** La variante de **FTP** protégée par les protocoles **SSL** ou **TLS** (**TLS** est le nouveau **SSL**) s'appelle **FTPS**.
* **http : (Hyper Text Transfer Protocol)** est un protocole standard de transport sur internet (en lecture seule)
* **https : (Hyper Text Transfer Protocol Secure)** le même protocole standard de transport sur internet avec de l'authentification basaée sur un certificat
* **Webdav :** (**Web-based Distributed Authoring and Versioning**)sur **http** ou **https :** est un protocole utilisant **http / http**s pour utiliser un partage distant (à travers internet) comme un partage local. **WebDAV** est un protocole (plus précisément, une extension du protocole **HTTP**) défini par le groupe de travail IETF du même nom. L'objectif principal de **WebDAV** est de rendre possible l'écriture à travers le web et pas seulement la lecture de données.

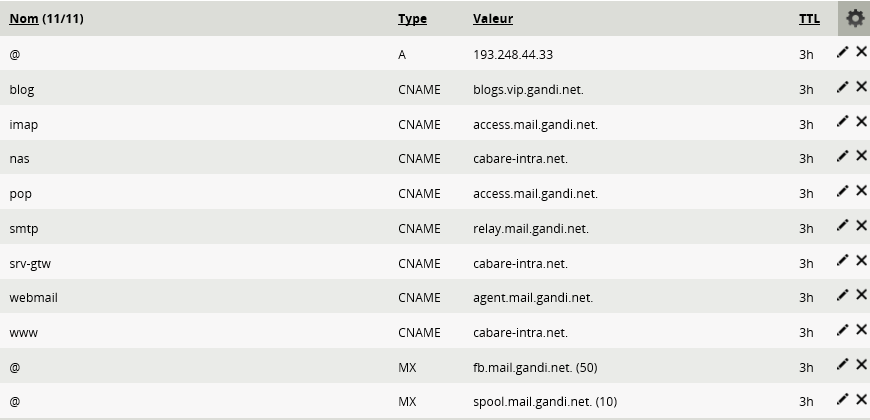
## Protocoles vpn :

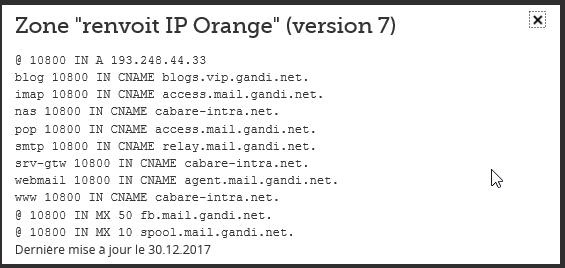
* **VPN : (Virtual Private Network)** ( en français, réseau privé virtuel), c'est une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel, privé, notamment via internet.

Un **réseau privé virtuel**, est donc un système permettant de créer un lien direct entre des ordinateurs distants. On accède à l'ordinateur distant comme s'il était local. Nécessite un client et un serveur.

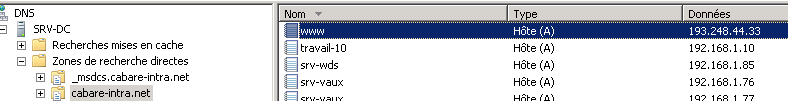
## Gestion DNS (renvoi sur une adresse ip publique - GANDI)

On associe à ce domaine un fichier de zone personnalisé dans lequel on aura effectué les changements, le **@** pour toutes les demandes et le **WWW** et le **srv-gtw**…et **nas**

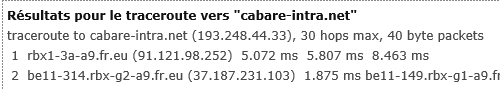




Un tracert interne depuis le domaine cabare-intra ne marche pas, sauf avec www car ajout d'un enregistrement DNS



Un tracert depuis la France via via <http://www.dnsfrog.com/fr>donne bien



# partage Http

## Pré-requis partage lien http :

Il faut : une ressource accessible et disponible via le **protocole http**

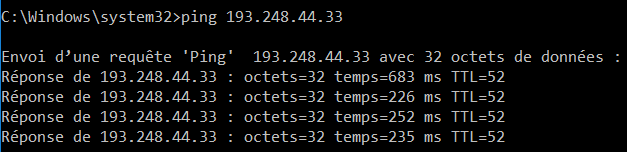
Dans notre exemple, une station **Synology**, partagée sur

* une **adresse ip publique** 82.66.116.111
* reliée à un **domaine DNS** [www.cabare-intra.net](http://www.cabare-intra.net)
* accessible sur le **port 9100** (redirigé via **NAT** en ***5000*** port natif **DSM synology**)

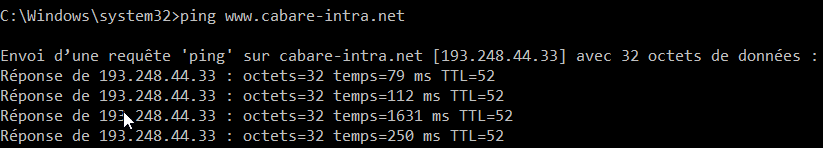
### Test depuis une machine Externe (réseau 4g)

on peut tester l'accessibilité via

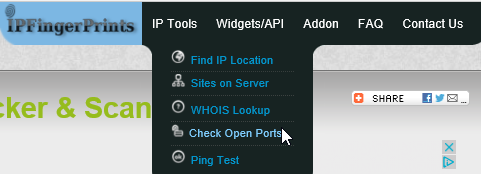
Accès **Ip** sur **@ IP publique** Orange



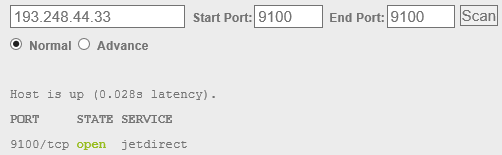
**DNS** Ok sur **Domaine** ***cabare-intra.net***



Depuis **ipfingerprints.com** / **IP Tools /** **Check Open Ports**



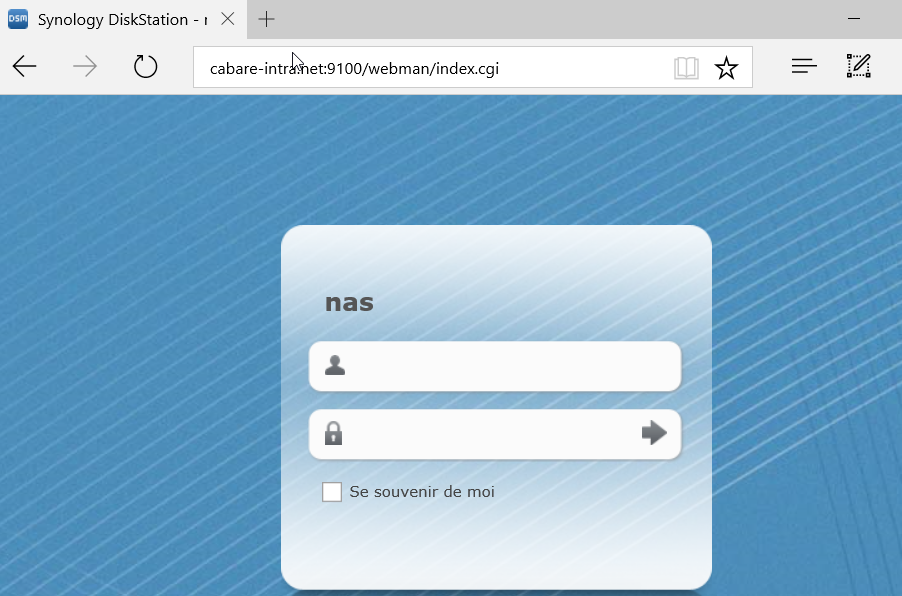
On peut tester si **le port 9100** est bien ouvert dans le **Pare-feu**



Du coup un accès en http devrait être possible

<http://www.cabare-intra.net:9100> ou <http://cabare-intra.net:9100>

donnant

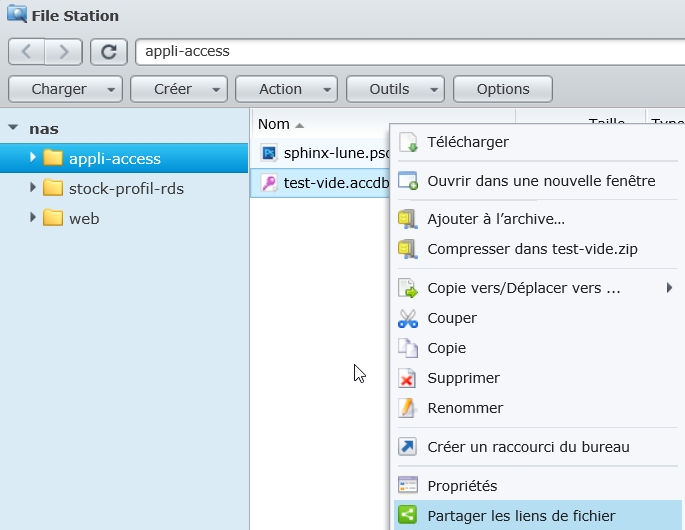


## Partage de lien http :

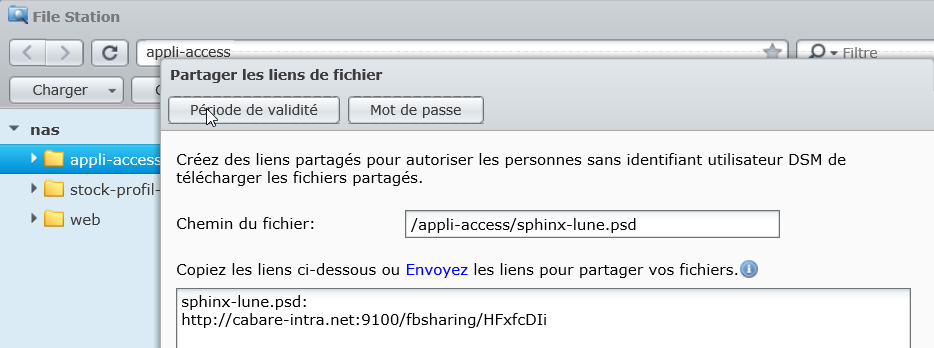
A partir du moment où la ressource est accessible à travers le réseau internet, on peut donc utiliser le **protocole http**

Coté **synology** l'application **File Station** propose une fonction classique de partage de lien sous forme d'un lien **hyper-texte http**

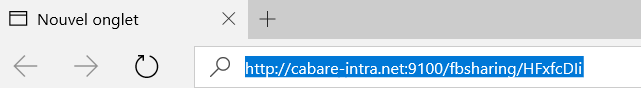
Une fois la ressource stockée dans le synology, et partagée, alors la fonction **partager les liens de fichier** devient accessible



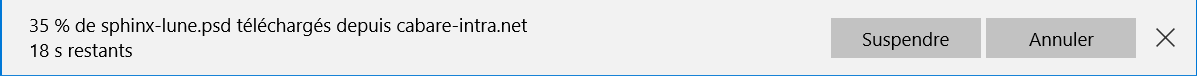
Et on obtient un **lien hyper-texte**



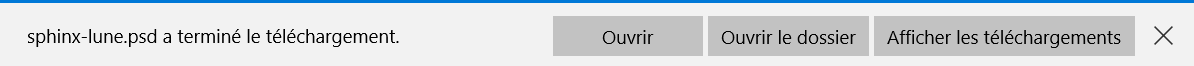
Qu'il suffit ensuite de coller dans la barre d'adresse d'un navigateur



Pour que le téléchargement commence…



Lorsqu’il sera terminé, on peut ouvrir le fichier, car il a été copié dans le dossier par défaut téléchargement



# Webdav

## Pré-requis webdav:

**WebDAV** est une extension du protocole **HTTP** conçue pour permettre aux utilisateurs de modifier et gérer les fichiers stockés sur des serveurs distants. Grâce au service **WebDAV de Synology DiskStation Manager**, les programmes clients qui prennent en charge **WebDAV**, tels que **Windows Explorer**, **Mac OS Finder**, **Linux File Browser**, sont capables d'accéder à distance comme pour un disque sur le réseau local.

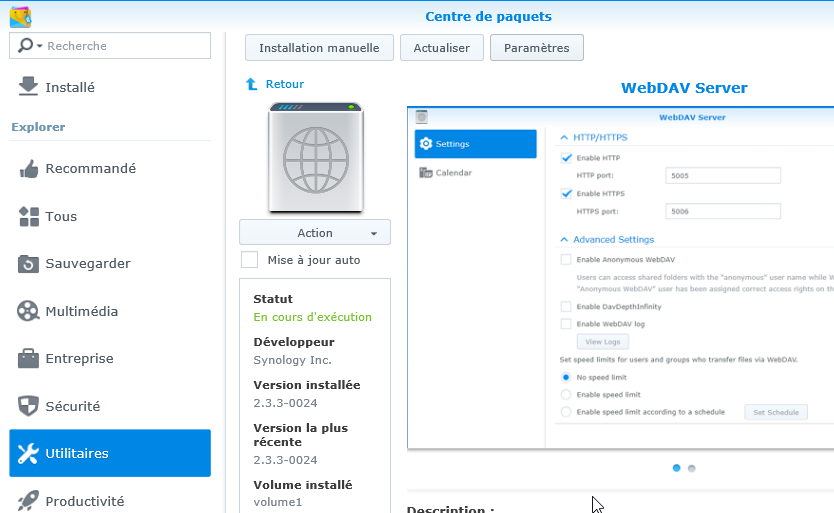
Dans notre exemple, une station **Synology**, partagée sur

* une **adresse ip publique** 193.248.44.33,
* reliée à un **domaine DNS** [www.cabare-intra.net](http://www.cabare-intra.net)
* accessible pour
  + webav sur http sur le **port 9105** (redirigé via **NAT** en ***5005*** port natif **DSM synology**)
  + webdav sur https sur le **port 9106** (redirigé via **NAT** en ***5006*** port natif **DSM synology**)

## Activation webdav synology:

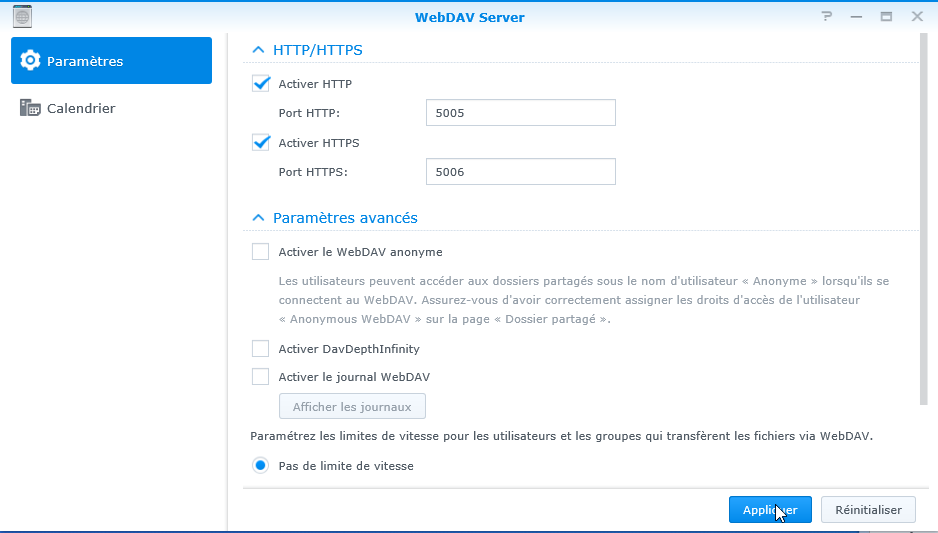
Depuis DSM 6 il faut installer un paquet spécifique. Il suffit d'aller dans le **centre de paquets**, et demander **utilitaires / Webdav Server**

Et installer le paquet



On active

* le **port 5005** pour **http**
* et le **port 5006** pour **https** (proposés par défaut par synology)

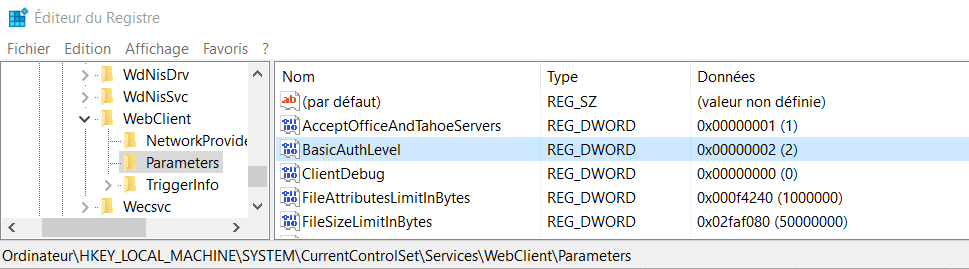


## Test client Windows webdav http (5005-9105):

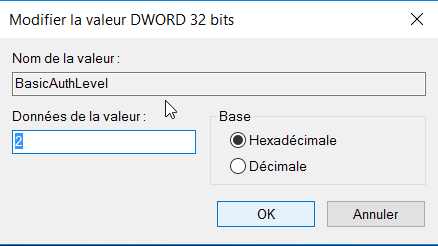
**N.B**: normalement, pour un poste Windows 10 cela n'est pas possible, car les connexions doivent obligatoirement être sécurisées, donc, au format **https.** Il est possible cependant de contourner cette obligation en modifiant une clé de ma base de registre de la machine

Marche avec utilitaire gratuit vieille version 

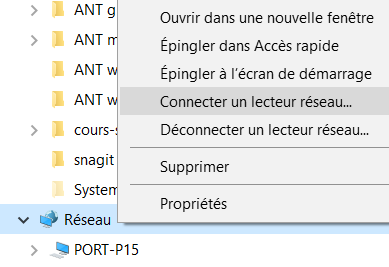
Donc **regedit**, dans la ruche : **HKLM\SYSTEM\CurrentcontrolSet\Services\WebClient\parameters**



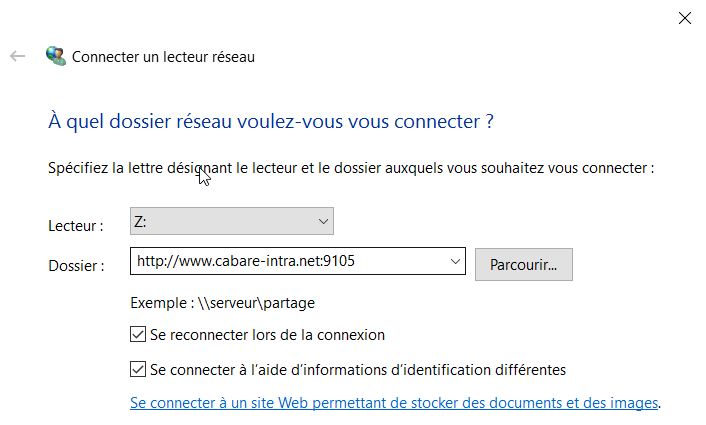
puis mettre à **2** la clé **basicAuthLevel**



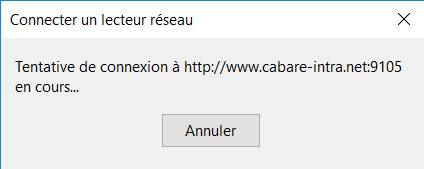
Ensuite on demande de **connecter un lecteur réseau**

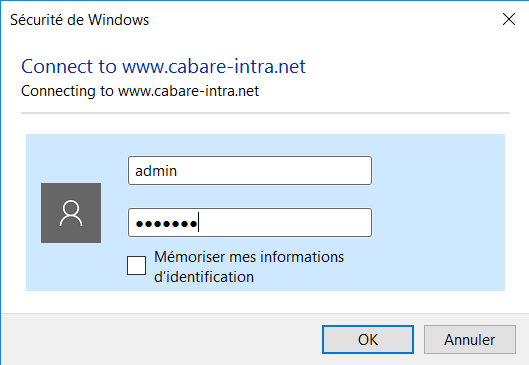


Dans l'assistant on rentrer l'adresse [**http://www.cabare-intra.net:9105**](http://www.cabare-intra.net:9105) **et cocher les 2 options**



On doit avoir

 avec

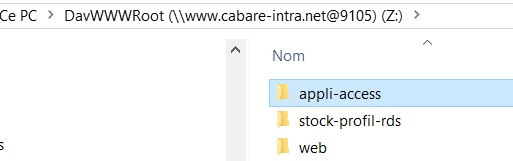


admin

naszk28

Et le tour est joué

On a un lecteur **Z:** (dans l'exemple) que l'on peut utiliser normalement (le renommer, le déconnecter…)



## Test client Windows webdav https (5006-9106):

Un poste Windows 10 nécessite des connexions sécurisées, donc, au format **https.** Il faut donc installer 1 **certificat** sur le **NAS Synology**

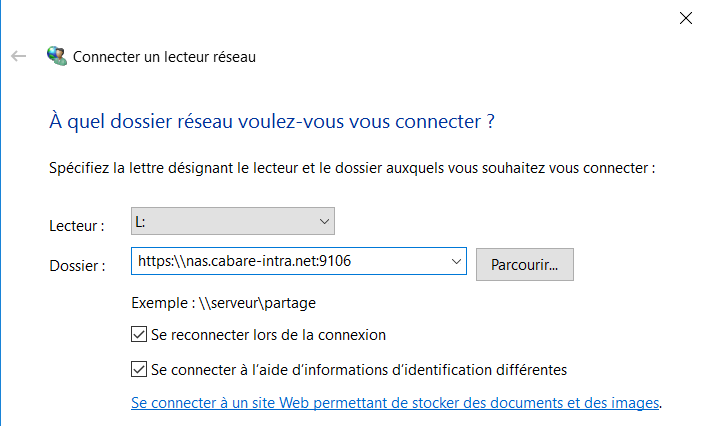
### installation du certificat

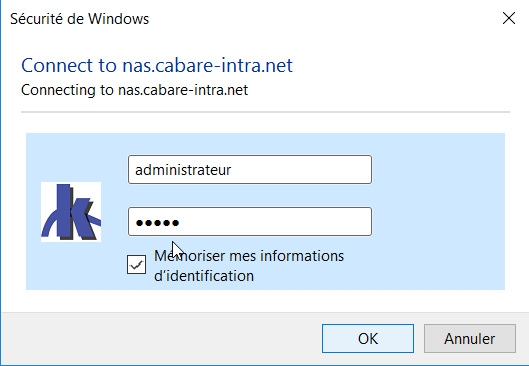
on a installé un certificat correspondant à ***nas-cabare-intra.net***

### Connexion depuis l'exterieur

On demande de se connecter sur

***https://nas.cabare-intra.net:9106***

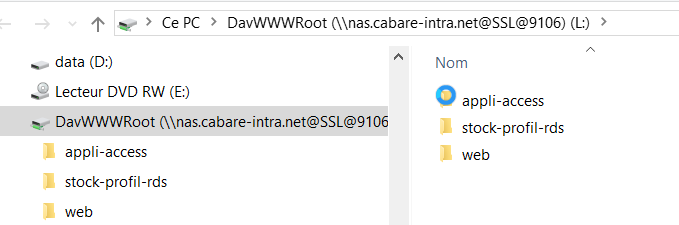




administrateur

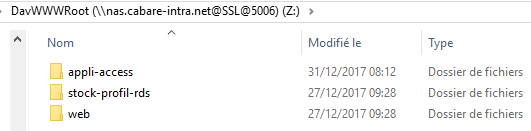
local

On obtient



### Connexion depuis le réseau local - LANr

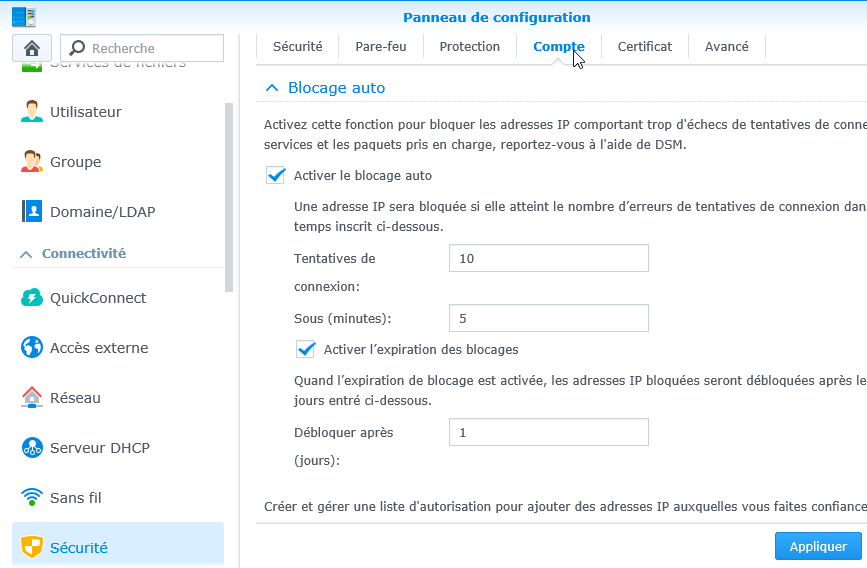
Idem mais avec le port 5006 (direct)



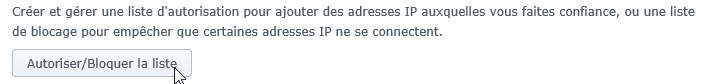
## Bloccage 10 Accès infructueux dans les 10 mn:

Le NAS Synology s'auto-protège sur des tentatives répétées en échec

Dans **panneau de Configuration**, **Sécurité**, Onglet **Compte**



Et on peut ajouter une adresse IP dans la liste des adresses non blocables !





# VPN

## Pré-requis VPN:

Un **réseau privé virtuel (VPN)** est un réseau privé qui utilise une infrastructure de réseau public telle qu'Internet, pour fournir des connexions sécurisées et chiffrées pour la transmission de données.

Avec le package **Serveur VPN** de Synology, il est possible d'accéder à distance et en toute sécurité aux ressources partagées dans le réseau local du DiskStation. En intégrant des protocoles **VPN** communs tels que **PPTP**, et **L2TP / IPSec**, et le protocole libre open source **OpenVPN**

Il existe plusieurs protocoles standards :

• **PPTP - Microsoft** : Authentification/Transport + Cryptage

• **L2TP de l’IETF** : Authentification/Transport

• **IPSEC de l'IETF** : Cryptage

Il existe plusieurs solutions logicielles complètes (client – serveur) :

• **OPEN VPN** : Produit open source

### PPTP - Point to Point Tunnelling Protocol - (Microsoft) :

C’est un protocole qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur un réseau IP. PPTP permet aussi le cryptage des données PPP encapsulées mais aussi leur compression. L’intérêt de PPTP est de ne nécessiter aucun matériel supplémentaire car les deux logiciels d’extrémité (le client et le serveur) sont intégrés depuis NT4. Il est assez ancien !!!

### L2TP - Layer Two Tunnelling Protocol + IPSEC (IETF):

Microsoft et Cisco, reconnaissant les mérites des deux protocoles L2F et PPTP, se sont associés pour créer le protocole L2TP. Ce protocole réunit quelques avantages de PPTP et L2F. Il est couplé à IPSEC.

### OPEN VPN (produit libre):

Dans notre exemple, une station **Synology**, partagée sur

* une **adresse ip publique** 193.248.44.33,
* reliée à un **domaine DNS** [www.cabare-intra.net](http://www.cabare-intra.net)
* accessible pour
  + **PPTP** – port **TCP 1723**
  + **OPEN VPN** **port UPD 1194**
  + **L2TP + I~~PSEC~~** – port **UDP 1701** (L2TP)

~~port UDP 500 (IPSEC protocoIe IKE)~~

~~port UDP 4500 (IPSEC NAT traversal)~~

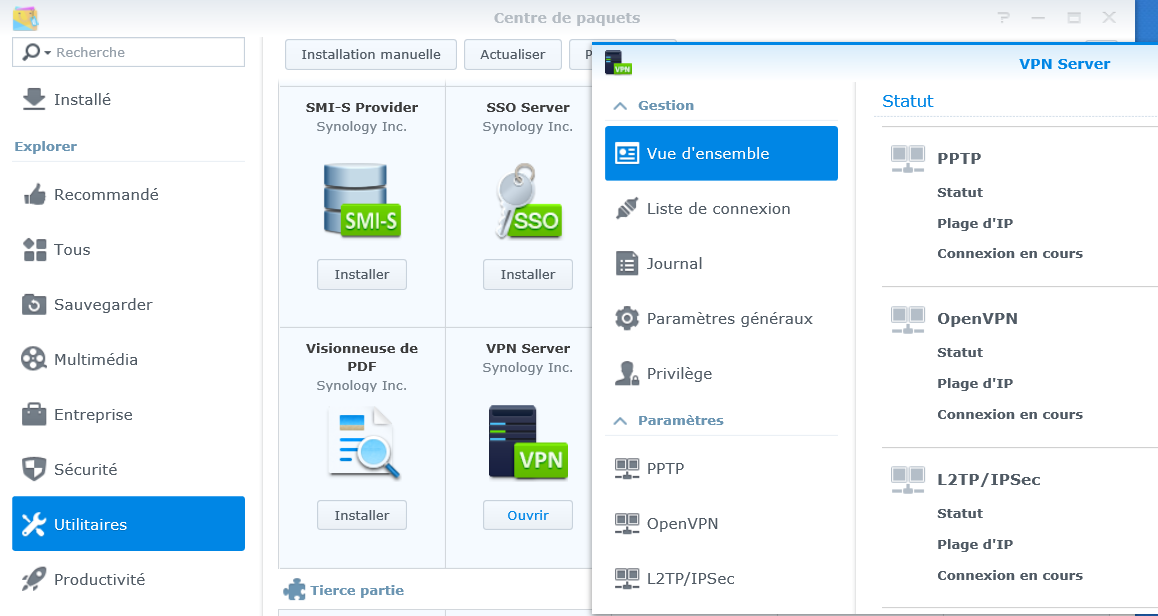
~~protocole 50 (IPSEC ESP encapsulating Security Payload)~~

## Activation VPN Server:

Dans DSM 6 il faut installer un paquet spécifique. Il suffit d'aller dans le **centre de paquets**, et demander **utilitaires / VPN Server**

Et installer le paquet

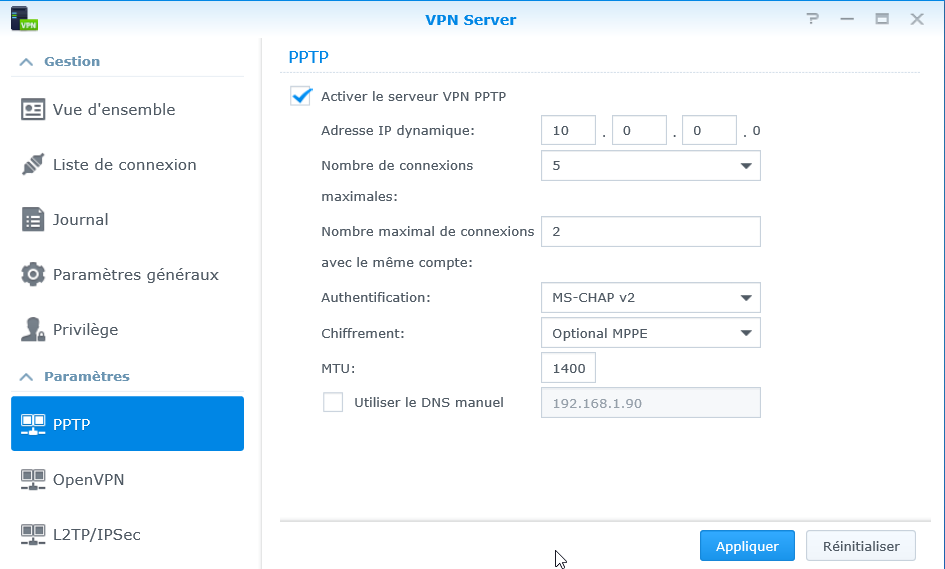
Que l'on peut ouvrir



On peut utiliser 3 types différentes de VPN …

## Paramétrage Serveur PPTP Synology (microsoft - TCP 1723) :

Il faut demander dans **VPN Server** / **paramètres / Server PPTP**,



**Adresse IP dynamique**: Le serveur VPN attribue des adresses IP virtuelles aux clients VPN. Par exemple, avec "10.0.0.0", l'adresse IP virtuelle attribuée aux clients VPN va de "10.0.0.1" à "10.0.0x"

**Nombre maximal de connexions**: Nombre maximal de connexions VPN simultanées autorisés.

**Authentification**: si possible mieux MS-CHAP v2:

* **PAP**: pas de cryptage des mots de passe des clients VPN lors de l'authentification.
* **MS-CHAP v2**: cryptage possible des mots de passe des clients VPN au cours de l'authentification via Microsoft CHAP v2

**Chiffrement**: Si on a choisit MS-CHAP v2, options de cryptage possible:

* **No MPPE**: Les connexions VPN ne seront pas protégées par un mécanisme de cryptage.
* **Optionnal MPPE**: les connexions VPN seront protégées ou non par un cryptage de 40 ou 128 bits, selon la configuration du client
* **Require MPPE:** les connexions VPN seront protégées par un mécanisme de cryptage de 40 à 128 bits, selon la configuration du client

**MTU**: si besoin taille d''unité de transmission maximale pour limiter la taille des paquets de données transmis via le VPN.

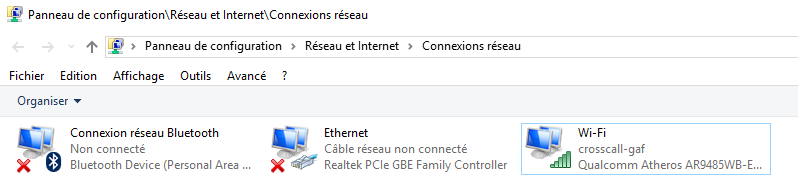
## Paramètres Client PPTP windows:

Il va falloir demander de :

* Configurer une nouvelle connexion VPN
* Se Connecter sur cette connexion VPN
* Créer un lecteur réseau (une seule fois)
* Déconnecter la connexion VPN

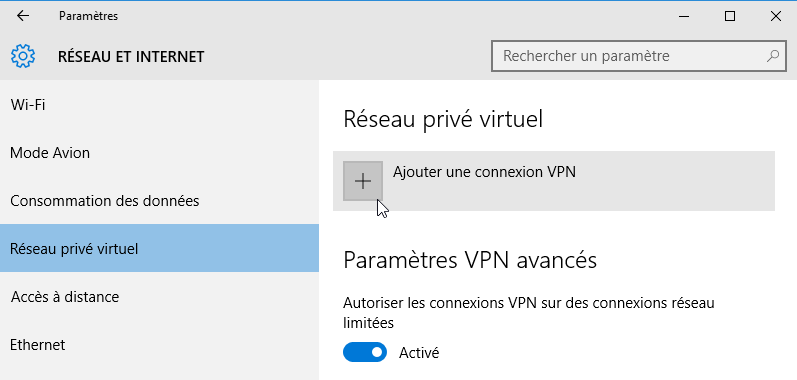
### Configurer la connexion vpn

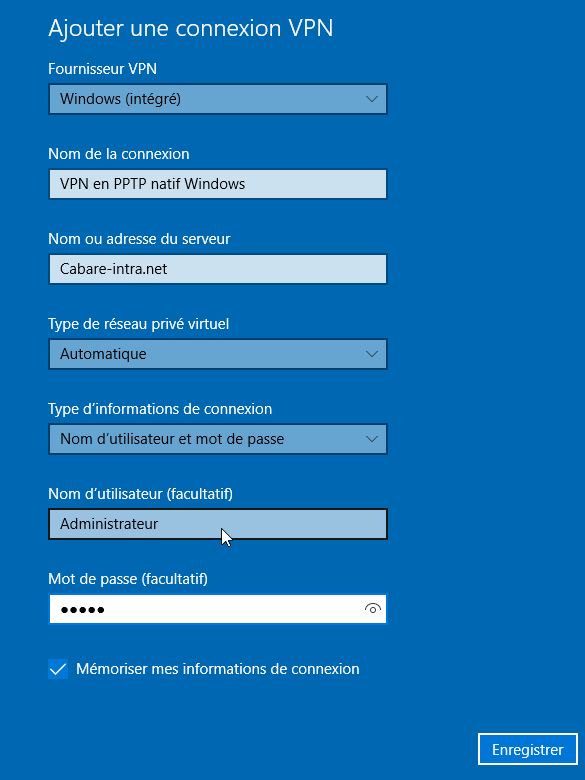
Soit une machine avec une connexion internet, ici ***Wifi – crosscall-gaf***



Pour **Windows 10**, on va dans **Paramètres** 

puis **Réseau privé virtuel / Ajouter une connexion VPN**





Apparait une boite de dialogue, on remplit

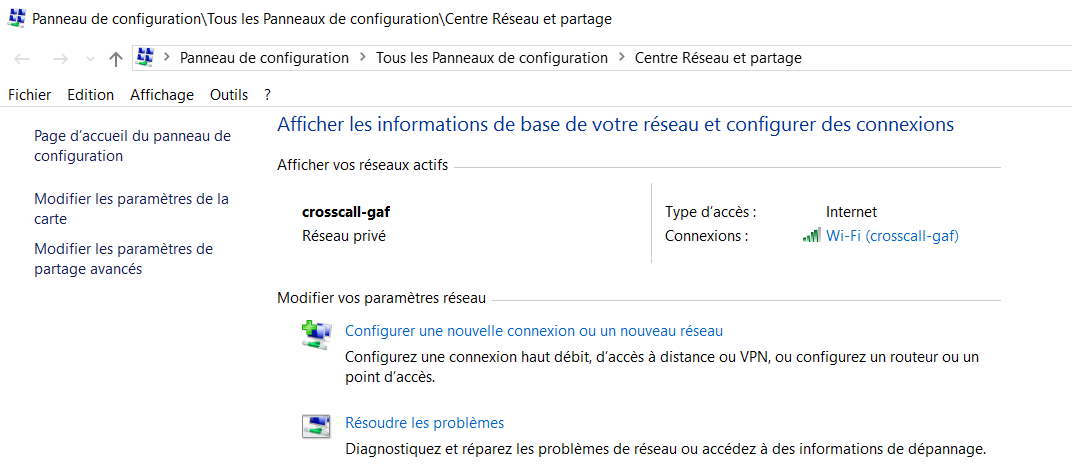
c’est monté !

Et on obtient

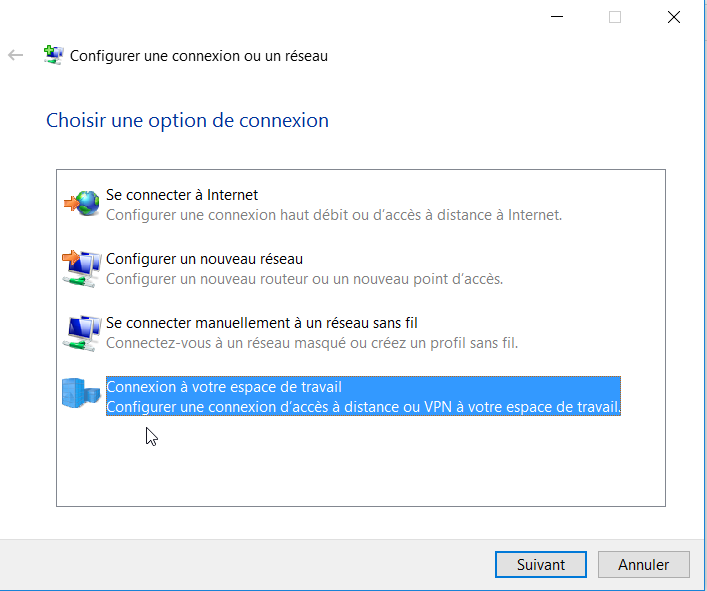


Pour Windows 7 et suivant, Il faut dans le **centre de réseaux et partage**,

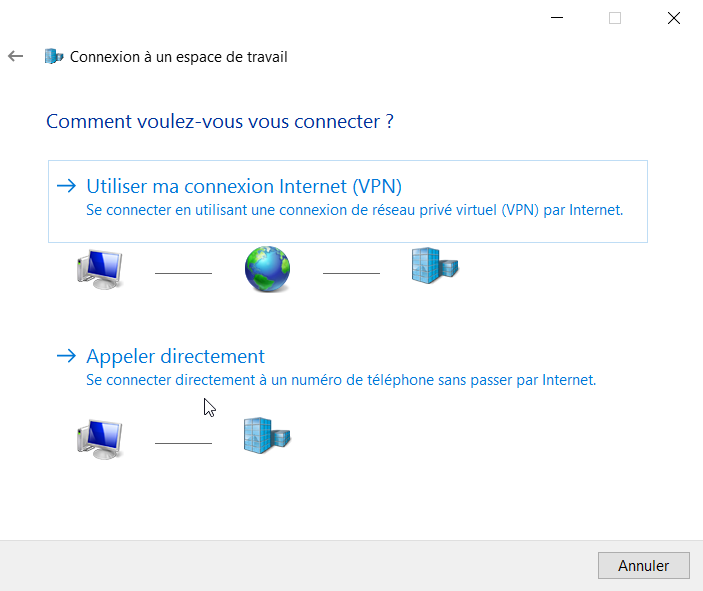
demander de **configurer une nouvelle connexion réseau ou un nouveau réseau**



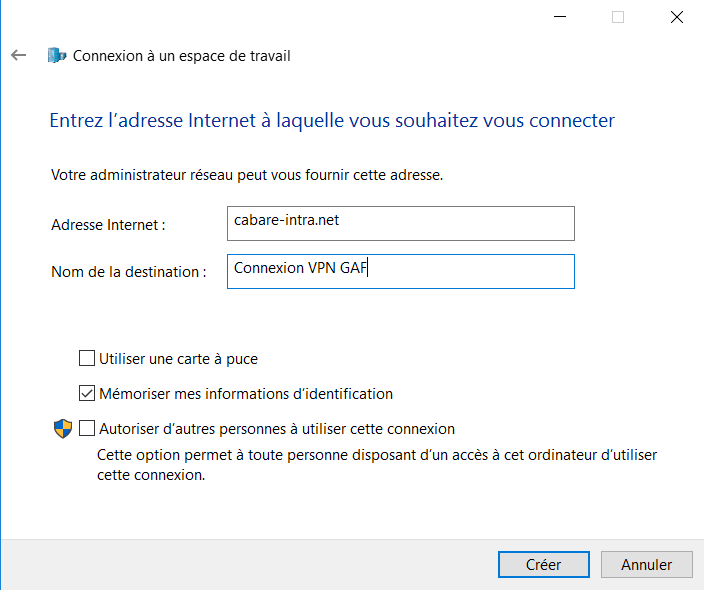
ensuite **Connexion a votre espace de travail**



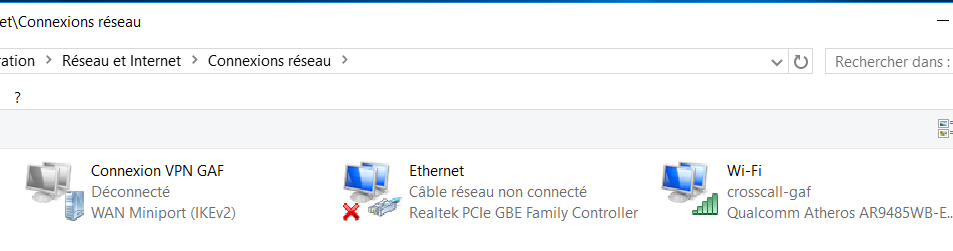
Ensuite **Utiliser ma connection internet VPN**



Il faut ensuite saisir l’adresse de destination, et **Créer**



Lorsque c’est terminé une nouvelle « connexion réseau » apparait disponible sur la machine



### Se connecter sur cette connexion vpn

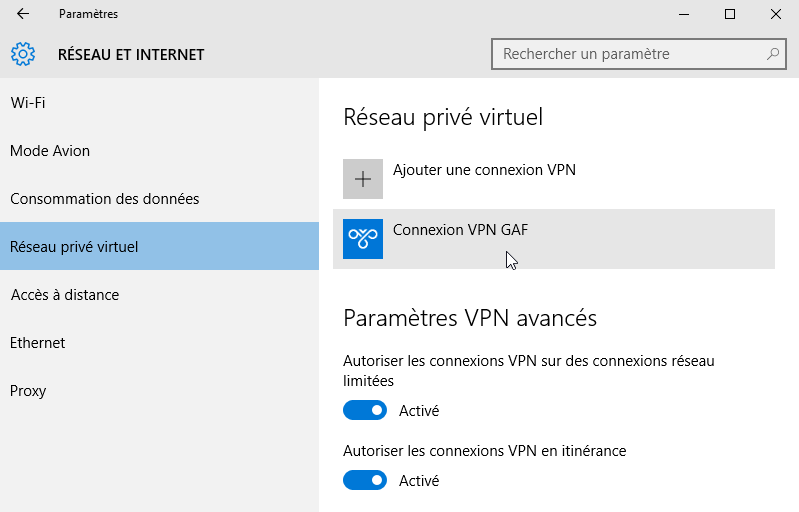
Cette connexion VPN va apparaitre

comme une connexion wifi.

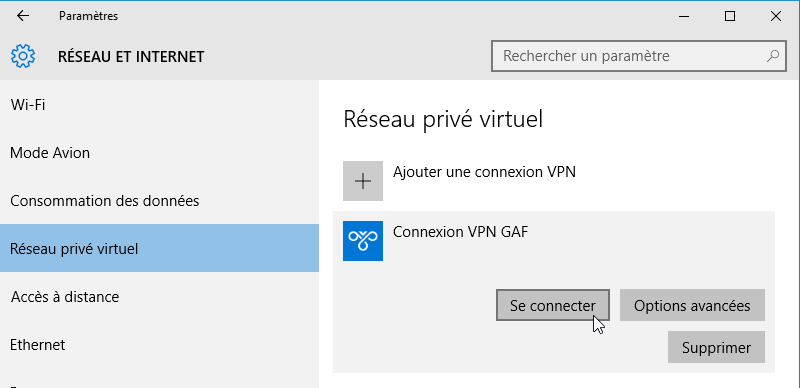
Pour s’en servir il faut l’activer / la paramétrer

On clique dessus

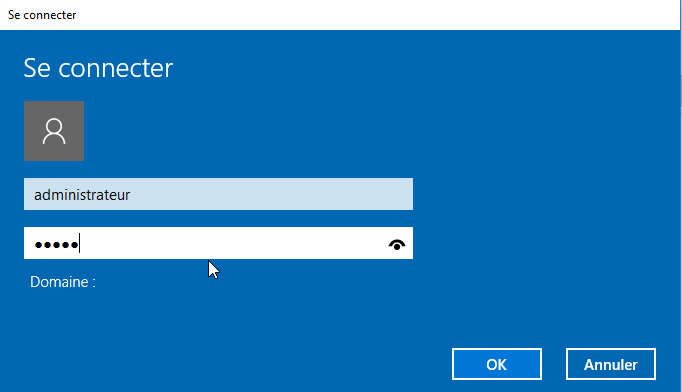
La boite de dialogue suivante apparaît



Et on demande simplement **Se connecter**



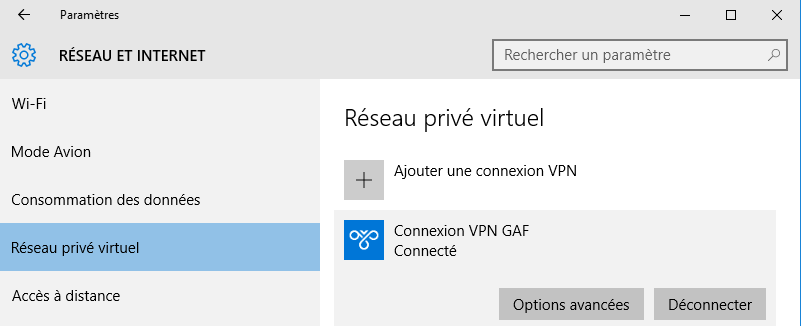
On s'identifie (si besoin)



administrateur

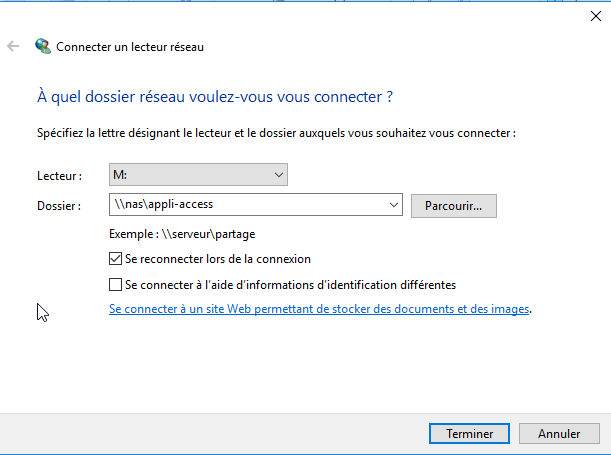
local

Et on est Connecté !



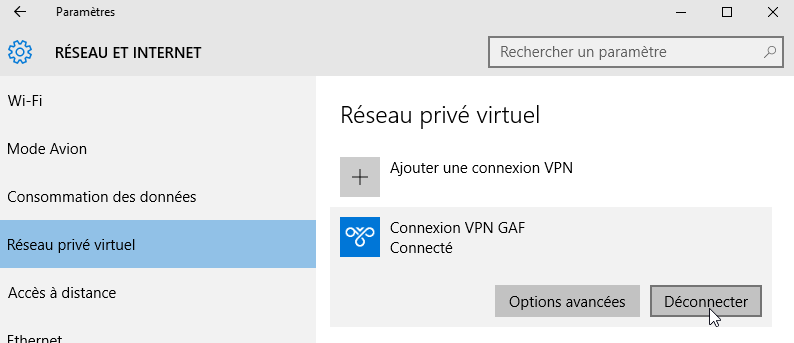
### Créer un lecteur réseau

Il n’y a plus qu’à créer le lecteur réseau (avec un chemin réseau local) comme ***\\nas\appli-access***



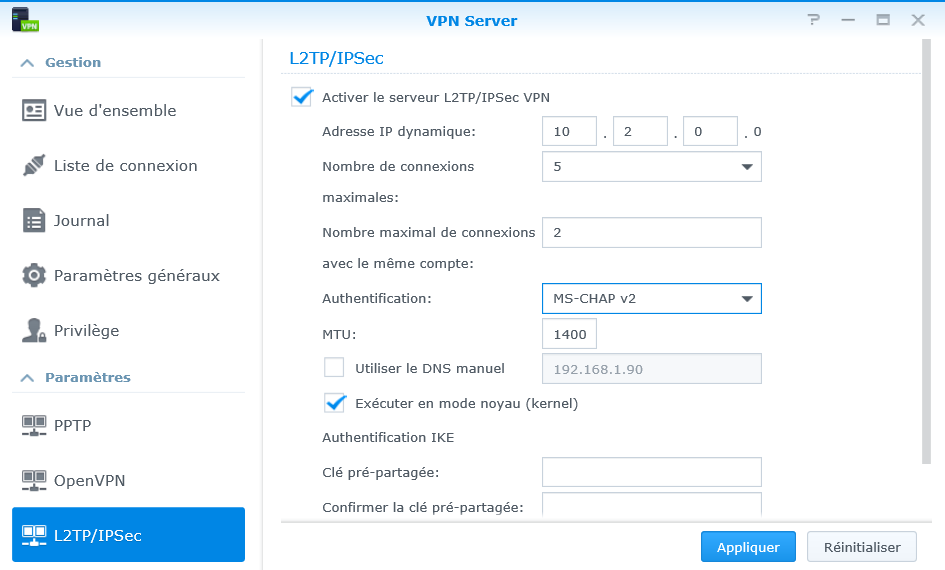
### Déconnecter la connexion vpn

Lorsque l’on a fini de travailler, on se deconnecte



## Paramétrage Serveur L2TP sans IPSEC Synology (IETF – UDP 1701):

Il faut demander dans **VPN Server** / **paramètres / ServerL2TP**,



**Adresse IP dynamique**: Le serveur VPN attribue des adresses IP virtuelles aux clients VPN. Par exemple, avec "10.0.0.0", l'adresse IP virtuelle attribuée aux clients VPN va de "10.0.0.1" à "10.0.0x"

**Nombre maximal de connexions**: Nombre maximal de connexions VPN simultanées autorisés.

**Authentification IKE** : non obligatoire:

* **Clé pré-partagée**: pour augmenter la sécurité. VPN-zk28
* **Compatible SHA**-2 : pour compatibilité anciens systèmes (il faut redeammer le synology)

**MTU**: si besoin taille d''unité de transmission maximale pour limiter la taille des paquets de données transmis via le VPN.

## Paramètres Client L2TP - Windows 10:

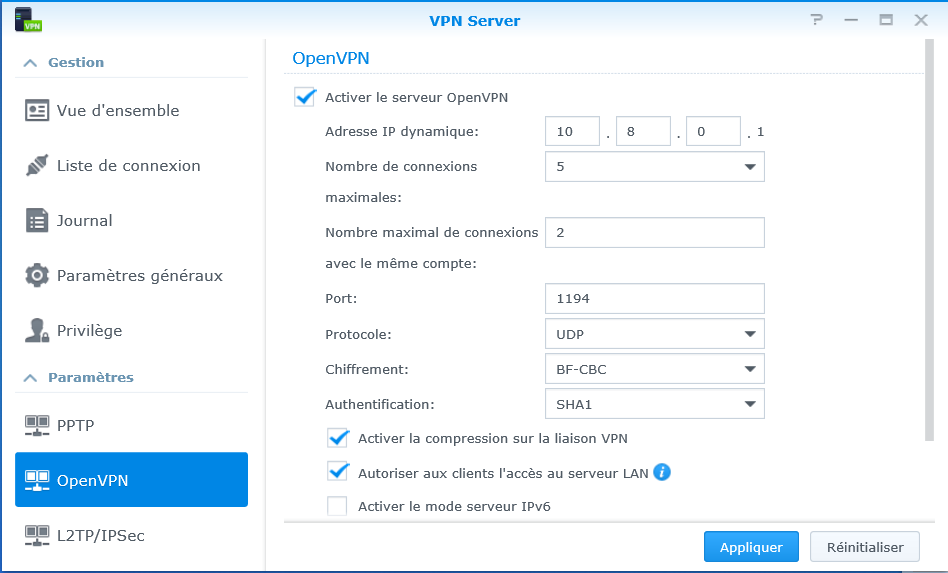
Il va falloir demander de :

* Configurer une nouvelle connexion VPN
* Se Connecter sur cette connexion VPN
* Créer un lecteur réseau (une seule fois)
* Déconnecter la connexion VPN

C'est la même manipulation que pour le cleint PPTP

## Paramétrage Serveur OPENVPN (libre - UDP 1194) :

Il faut demander dans **VPN Server** / **paramètres / Server OpenVPN**



Avec comme chiffrement le rapport qualité suivant :



Et eventuellement



* Si on ne coche pas, on ne pourra accéder que au NAS
* Si on cochen on peut accéder aux autres ressourcs locales du réseau, mais on passera par le VPN pour la connection internet ….

#### Export configuration OpenVpn pour le client

Dans la partie basse de la boite de dialogue, il faut demander **Exporter la configuration**,

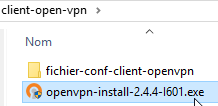


pour récupérer dans un fichier ***openvpn.zip*** la configuration du client et le certificat



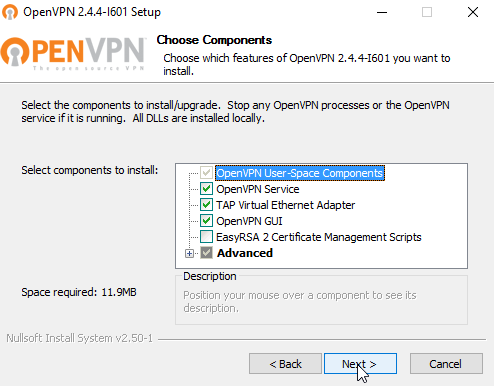
## Paramètres Client OpenVpn - Windows 10:

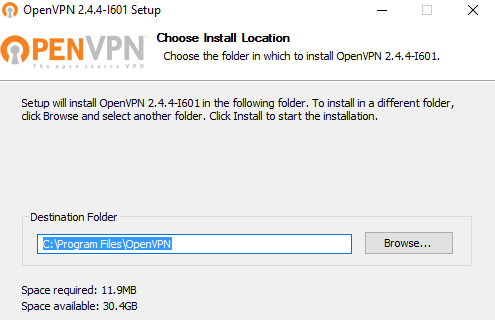
Il va falloir demander de :



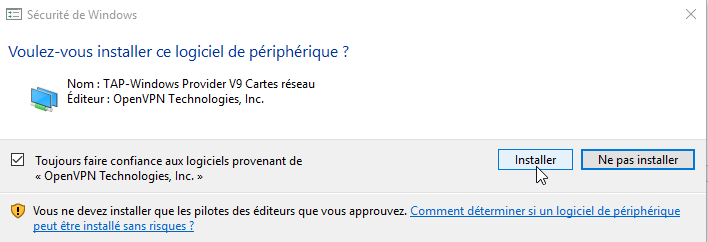


On laisse tout par défaut

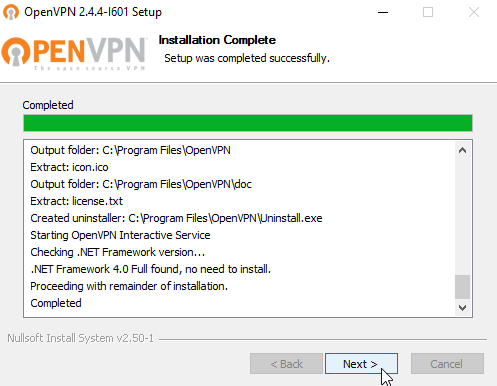




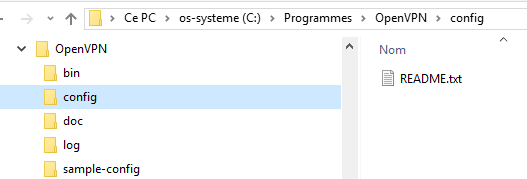
On valide



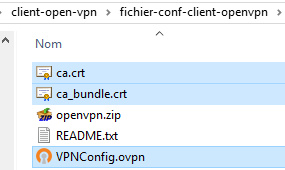
Et c’est fini



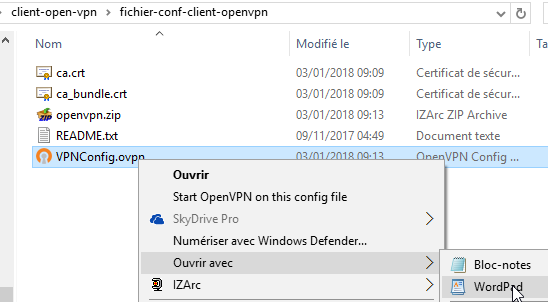
Cela crée la structure suivante



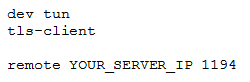
On prend les fichiers exportés précédemment et on les copie dans le dossier config



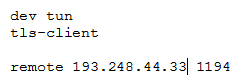
On édite le fichier **VPNConfig.ovpn**



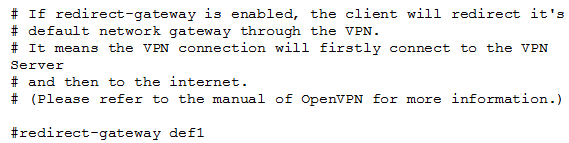
On remplace son adresse IP publique



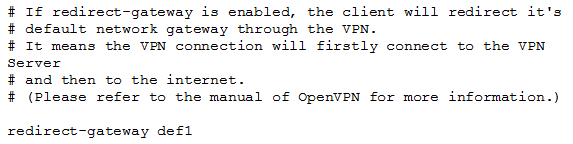
Par



Si on veut laisser un accès complet au réseau via le VPN (et pas que le NAS) on enlève le commentaire, donc on remplace



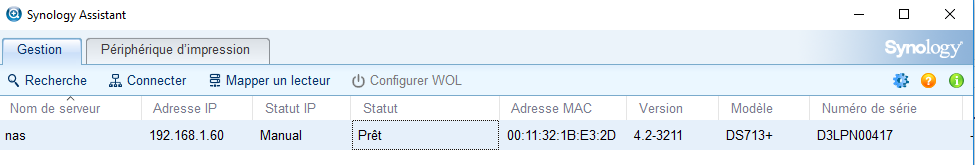
Par



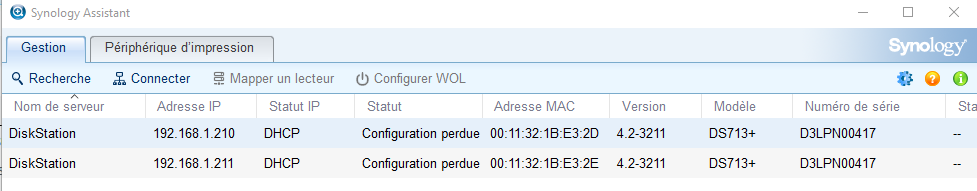
Import de la configuration en copiant le fichier au bon endroit

# Synology DS713+

## Maj DSM 6.x:



Double reset

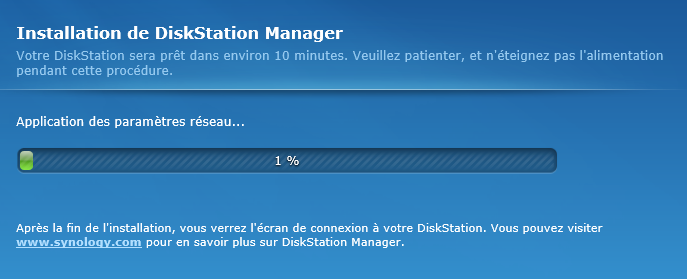


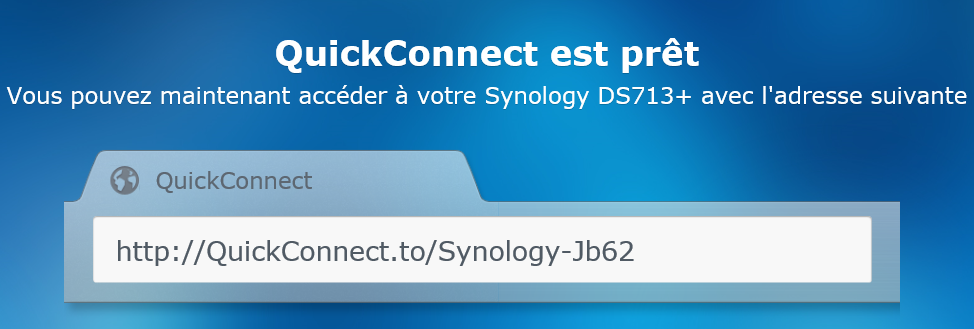
Assistant de reinstall

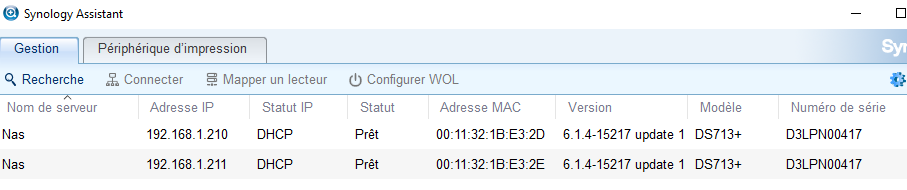




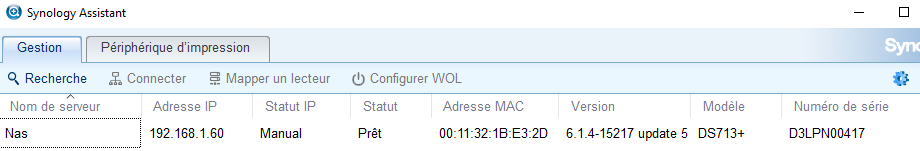


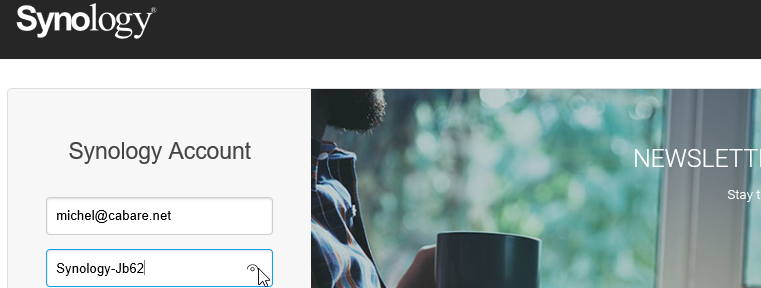






On agrègera dans le synology (BOND) les deux cartes réseau en 192.168.1.60





# Synology DS713+

## Maj DSM 6.x: