Compte Rendu GRP 4

AP Archi-Site

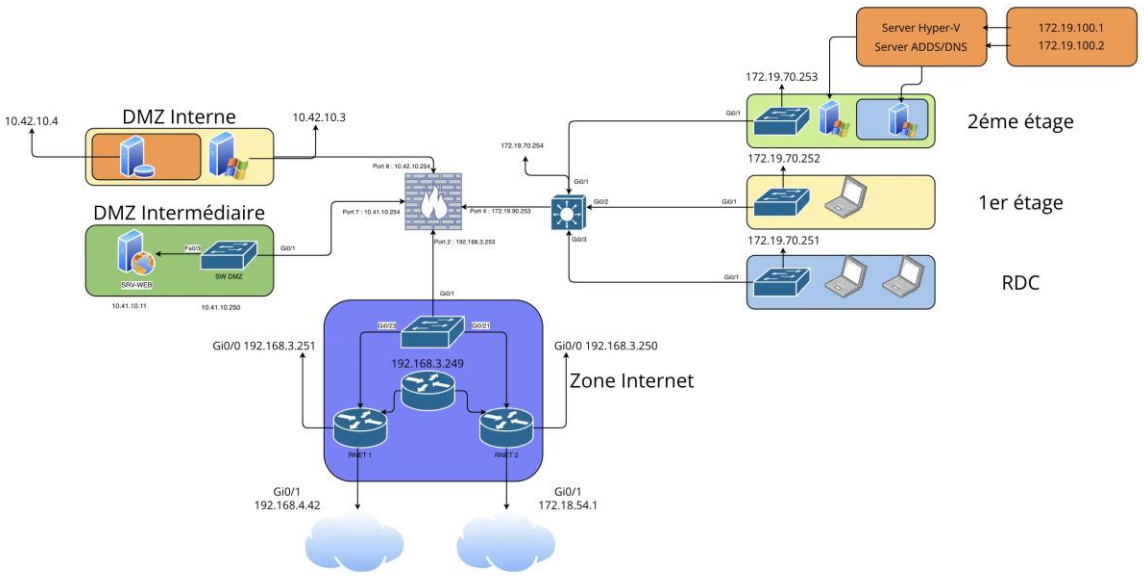
Antoine Girardey – Lucas Tardy

Sommaire

Planification du projet

Réalisation du schéma réseau

La première phase de ce projet mais néanmoins non négligeable est la planification du projet. Nous entendons par là le recensement de toutes les activités et étapes du projet. C'est également à cette étape que le Trello est créé et nous suivras tout du long de cette AP. Il faut également créer le GANTT et lui renseigner les premiers temps prévisionnels



Réalisation de la note technique sur l'utilisation des certificats

Comme demandé dans l'ordre de mission, une notre technique a été réalisée sur l'usage des certificats auto-signés ou certifiés par une autorité de confiance ainsi que les conséquences pour l'entreprise.

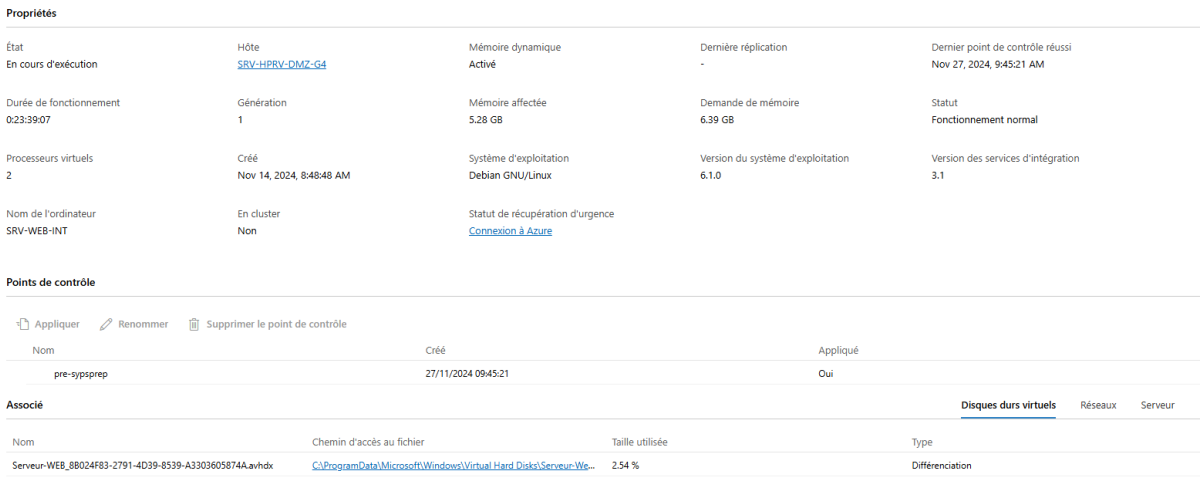
Les certificats numériques sont essentiels pour sécuriser les communications en ligne, mais leur choix a des implications techniques significatives. Le certificat auto-signé, généré par l'entreprise, est gratuit et rapide à mettre en place, mais déclenche des avertissements de sécurité et convient uniquement aux environnements de test internes. Le certificat signé par une autorité privée nécessite une infrastructure à clés publiques (PKI) et est adapté pour sécuriser les communications internes de l'entreprise. Le certificat signé par une autorité publique offre le plus haut niveau de confiance, est essentiel pour les services exposés sur internet, mais implique un coût plus élevé. Le choix dépend donc du contexte d'utilisation, des exigences de sécurité et de la nature des services à protéger, nécessitant une stratégie de gestion des certificats afin d'optimiser au mieux leurs gestions

Installation des différents serveurs

Nous avons commencé par installer le serveur Web, pour ce faire nous avons installé un hyperviseur de type 2 sous un Windows serveur core, qui va ensuite héberger une machine virtuelle (VM) qui va servir de serveur Web.

```
PS C:\Users\Administrateur> Install-WindowsFeature -Name Hyper-V -IncludeAllSubFeature -Restart

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrateur>
>>
PS C:\Users\Administrateur> Get-WindowsFeature

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[ ] Accès à distance                                    RemoteAccess                   Available
    [ ] DirectAccess et VPN (accès à distance)          DirectAccess-VPN               Available
    [ ] Proxy d'application web                         Web-Application-Proxy          Available
    [ ] Routage                                         Routing                        Available
[ ] Attestation d'intégrité de l'appareil               DeviceHealthAttestat...        Available
[X] Hyper-V                                             Hyper-V                        Installed
[ ] Serveur DHCP                                        DHCP                           Available
[ ] Serveur DNS                                         DNS                            Available
[ ] Serveur Web (IIS)                                   Web-Server                     Available
    [ ] Serveur Web                                     Web-WebServer                  Available
        [ ] Fonctionnalités HTTP communes               Web-Common-Http                Available
            [ ] Contenu statique                        Web-Static-Content             Available
            [ ] Document par défaut                     Web-Default-Doc                Available
            [ ] Erreurs HTTP                            Web-Http-Errors                Available
            [ ] Exploration de répertoire               Web-Dir-Browsing               Available
            [ ] Publication WebDAV                      Web-DAV-Publishing             Available
```

Ensuite nous avons utilisé l'outil Windows Admin Center (WAC) pour installer une VM sur notre hyperviseur :



Nous avons installé l'OS Debian 12 pour notre serveur Web car il répondait parfaitement aux demandes en termes de performances et de besoin.

```
user@SRV-WEB-INT:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 12 (bookworm)
Release:        12
Codename:       bookworm
user@SRV-WEB-INT:~$
```

Après avoir installé l'OS nous avons installé les paquets pour préparer le site web, apache 2 et PHP pour que notre site web avec ses pages PHP puissent fonctionner :

```
root@SRV-WEB:/home/lucas# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 593 kB of archives.
After this operation, 1,905 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 apache2-data all 2.4.62-1
~deb12u2 [160 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 apache2-utils amd64 2.4.6
2-1~deb12u2 [210 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 apache2 amd64 2.4.62-1~de
b12u2 [223 kB]
Fetched 593 kB in 0s (9,282 kB/s)
Selecting previously unselected package apache2-data.
(Reading database ... 146220 files and directories currently installed.)
Preparing to unpack .../apache2-data_2.4.62-1~deb12u2_all.deb ...
```

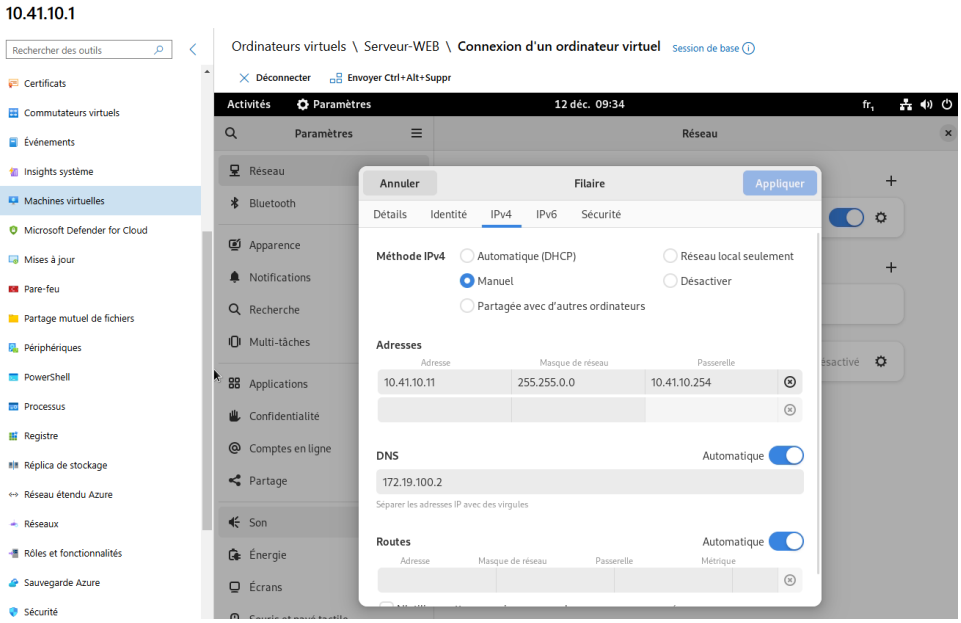
```
root@SRV-WEB:/home/lucas# apt install php libapache2-mod-php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.2 php-common php8.2 php8.2-cli php8.2-common
  php8.2-opcache php8.2-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php8.2 php php-common php8.2 php8.2-cli
  php8.2-common php8.2-opcache php8.2-readline
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,520 kB of archives.
After this operation, 21.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 php-common all 2:93 [13.1 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 php8.2-common amd64 8.2.24-1~deb12u1 [684 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 php8.2-opcache amd64 8.2.24-1~deb12u1 [345 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 php8.2-readline amd64 8.2.24-1~deb12u1 [12.4 kB]
Get:5 http://deb.debian.org/debian bookworm/main amd64 php8.2-cli amd64 8.2.24-1~deb12u1 [1,737 kB]
Get:6 http://deb.debian.org/debian bookworm/main amd64 libapache2-mod-php8.2 amd64 8.2.24-1~deb12u1 [1,678 kB]
Get:7 http://deb.debian.org/debian bookworm/main amd64 libapache2-mod-php all 2:8.2+93 [3,764 B]
Get:8 http://deb.debian.org/debian bookworm/main amd64 php8.2 all 8.2.24-1~deb12u1 [42.3 kB]
Get:9 http://deb.debian.org/debian bookworm/main amd64 php all 2:8.2+93 [3,628 B]
Fetched 4,520 kB in 3s (1,701 kB/s)
Selecting previously unselected package php-common.
(Reading database ... 146756 files and directories currently installed.)
Preparing to unpack .../0-php-common_2%3a93_all.deb ...
Unpacking php-common (2:93) ...
Selecting previously unselected package php8.2-common.
Preparing to unpack .../1-php8.2-common_8.2.24-1~deb12u1_amd64.deb ...
```

Paramétrage IP global:

Nous avons dû réviser les adresses IP de plusieurs parties de notre réseau pour pouvoir nous conformer aux attentes de ce nouveaux projet.
Premièrement j'ai modifié l'adresse IP du serveur HYPERV-Windows Core qui était dans l'ancienne DMZ en 10.4.10.1 en 10.41.10.1:

```
PS C:\Users\Administrateur> Remove-NetIpAddress -InterfaceAlias Ethernet -confirm:$False
PS C:\Users\Administrateur> New-NetIpAddress -InterfaceAlias Ethernet -IpAddress 10.41.10.1 -PrefixLength 16 -DefaultGateway 10.41.10.254


IPAddress         : 10.41.10.1
InterfaceIndex    : 3
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 16
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 10.41.10.1
InterfaceIndex    : 3
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 16
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

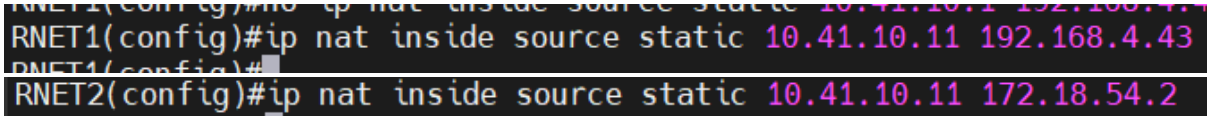
ensuite j'ai mis une adresse IP cohérente pour le serveur Web en lui rajoutant juste un "1" derrière l'adresse IP du serveur Hyper V.



La modification de l'adresse IP de ce serveur Hyper V est faite pour avoir deux parties dans le DMZ, une en "10.41.... " accessible de l'extérieur puisqu'elle contient uniquement le serveur web et le service SFTP, et une en "10.42...." inaccessible

depuis l’extérieure dans laquelle il y a le serveur BDD.

La DMZ intermédiaire est nommée ”dmz-SRV-WEB" pour bien la distinguer malgré le nombre de caractères limité.
Ensuite j’ai modifié le NAT que nous avions effectué sur nos deux routeur RNET pour permettre l’accès d’utilisateur connecter via le WAN ou sur le réseau de notre Campus sur le serveur web.



Sécurisation du serveur web

En premier lieu la sécurisation du serveur web passe par la mise en place de SFTP afin de pouvoir récupérer sereinement le site web et pouvoir dialoguer sans que les échanges passent en clairs. Car le SFTP intègre une gestion des certificats afin de chiffrer le tout.

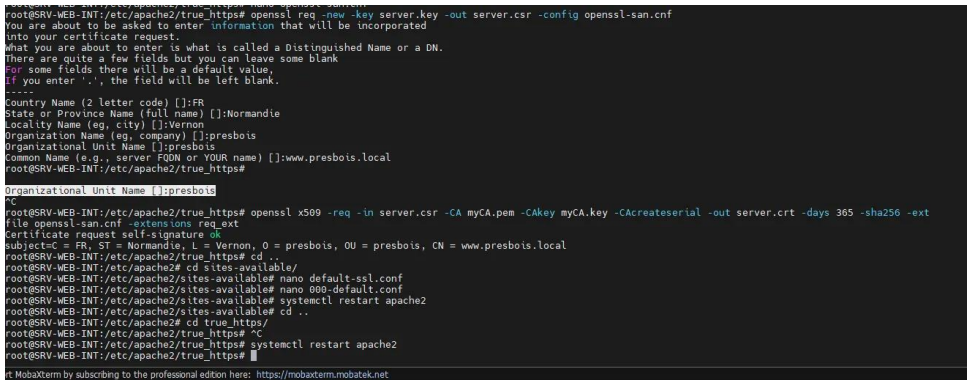
Par la suite afin de gerer les certificats du site web, j'ai créé une clé chiffrée, j'ai rentré les informations nécessaires de notre entreprise dans la clé, puis j'ai modifié le fichier de configuration openssl et pouf finir j'ai créé une clé pour le serveur

```
root@SRV-WEB-INT:/# cd /etc/apache2
root@SRV-WEB-INT:/etc/apache2# mkdir true_https
root@SRV-WEB-INT:/etc/apache2# cd true_https/
root@SRV-WEB-INT:/etc/apache2/true_https# openssl genrsa -out myCA.key 2048
root@SRV-WEB-INT:/etc/apache2/true_https# openssl req -x509 -new -nodes -key myCA.key -sha256 -days 3650 -out myCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Normandie
Locality Name (eg, city) []:Vernon
Organization Name (eg, company) [Internet Widgits Pty Ltd]:presbois
Organizational Unit Name (eg, section) []:presbois
Common Name (e.g. server FQDN or YOUR name) []:www.presbois.local
Email Address []:
root@SRV-WEB-INT:/etc/apache2/true_https# nano openssl-san.cnf
root@SRV-WEB-INT:/etc/apache2/true_https# openssl genrsa -out server.key 2048
```

Voici à quoi ressemble le fichier de configuration :

```
  GNU nano 7.2                                                    openssl-san.cnf
[req]
default_bits       = 2048
default_md         = sha256
distinguished_name = req_distinguished_name
req_extensions     = req_ext

[req_distinguished_name]
countryName                = Country Name (2 letter code)
stateOrProvinceName        = State or Province Name (full name)
localityName               = Locality Name (eg, city)
organizationName           = Organization Name (eg, company)
organizationalUnitName     = Organizational Unit Name
commonName                 = Common Name (e.g., server FQDN or YOUR name)

[req_ext]
subjectAltName = @alt_names

[alt_names]
IP.1   = 10.41.10.11       # Replace with your server's IP
DNS.1  = www.presbois.local        # Replace with your server's hostname (e.g., myserver.local)
```

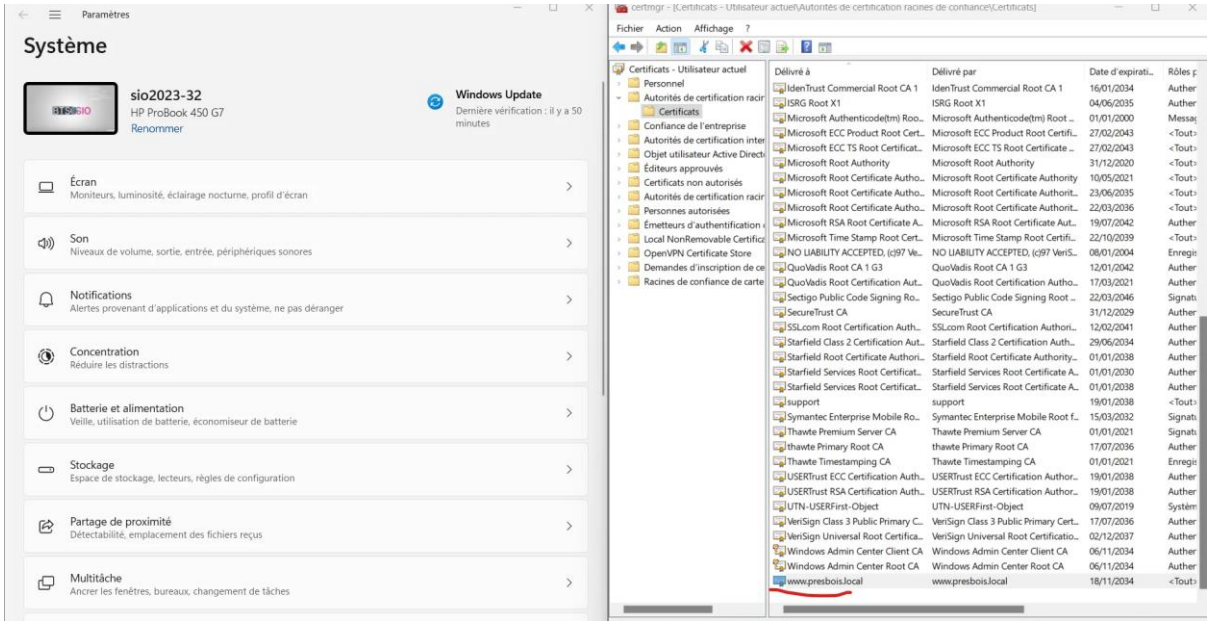
Ensuite j'ai rentré les informations de notre entreprise dans la clé du serveur. Pour finir j'ai auto-signé mon certificat et mis les paramètres du site dans le fichier de configuration apache2 (default-ssl.conf), ensuite plus qu'à redémarrer le service apache et importer le site web



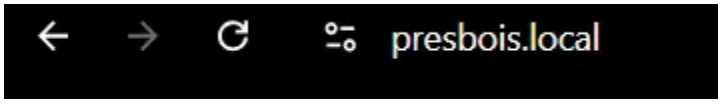
Fichier de conf apache:

```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on

        #   A self-signed (snakeoil) certificate can be created by installing
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2/README.Debian.gz for more info.
        #   If both key and certificate are stored in the same file, only the
        #   SSLCertificateFile directive is needed.
        SSLCertificateFile      /etc/apache2/true_https/server.crt
        SSLCertificateKeyFile   /etc/apache2/true_https/server.key

        #   Server Certificate Chain:
        #   Point SSLCertificateChainFile at a file containing the
        #   concatenation of PEM encoded CA certificates which form the
        #   certificate chain for the server certificate. Alternatively
        #   the referenced file can be the same as SSLCertificateFile
        #   when the CA certificates are directly appended to the server
        #   certificate for convinience.

#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

        #   Certificate Authority (CA):
        #   Set the CA certificate verification path where to find CA
        #   certificates for client authentication or alternatively one
```

Pour finir j'importe le certificat sur l'ordinateur via lequel je veux me connecter sur le serveur web:



Le certificat fonctionne bien une fois l'importation du site faite.



Adaptation des règles de pare-feu

Afin de répondre au mieux au besoin il a fallu configurer différentes règles de filtrage sur le pare-feu :

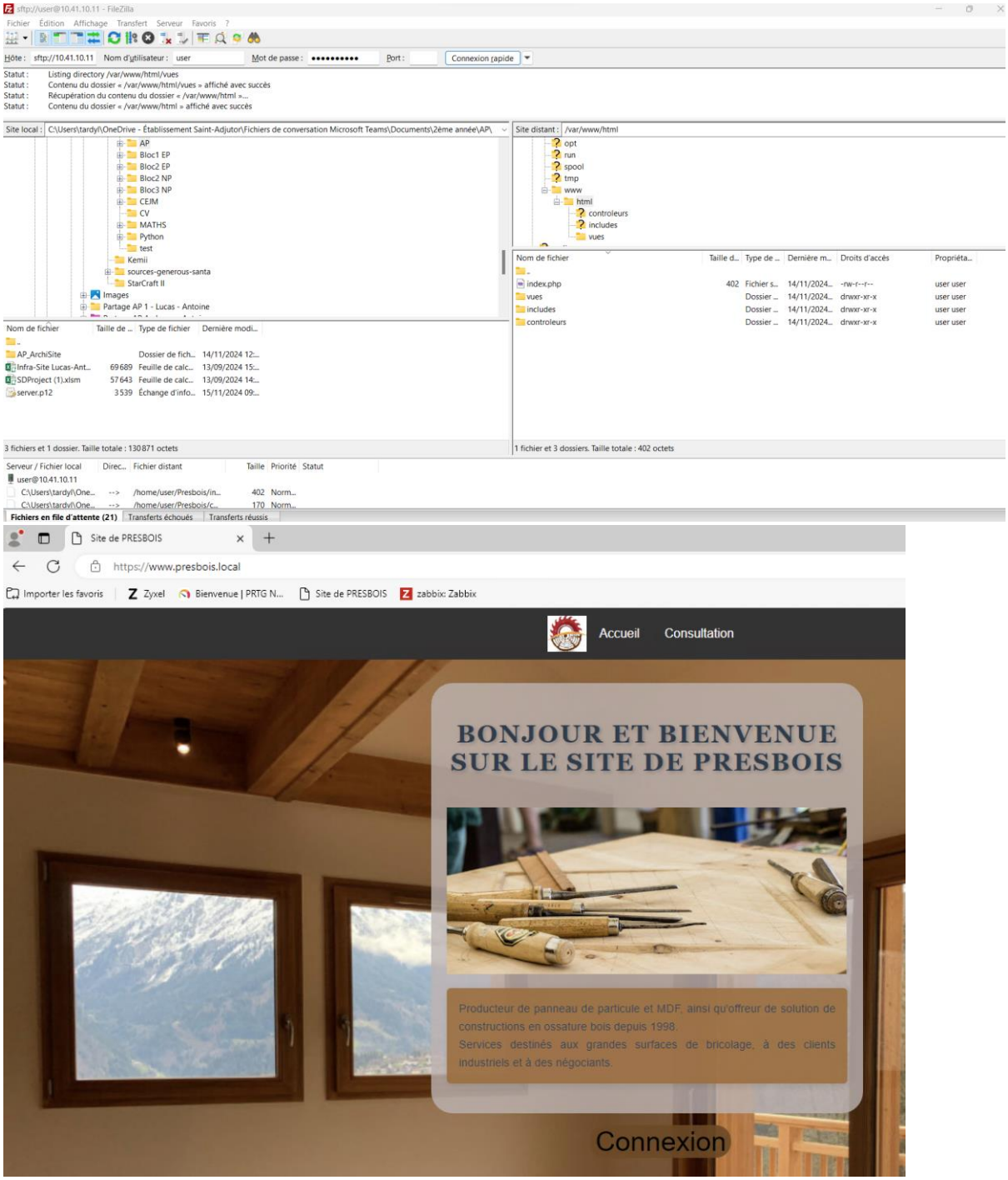
3		WEB	any	DMZ	any	srv-web	HTTPS	any	none	allow	no
4		BDD-WEB	OPT	DMZ	BDD	srv-web	any	any	none	allow	no

Grâce à ces règles tout le monde peut accéder au serveur web via HTTP.

Cependant la base de données de reste accessible uniquement pour le serveur web afin d’éviter tout risque de sécurité.

Mise en place finale du site

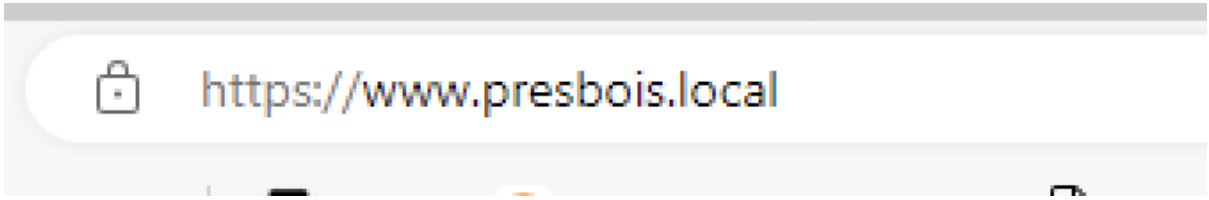
J’ai importé les fichiers du serveur Web via filezila en SFTP



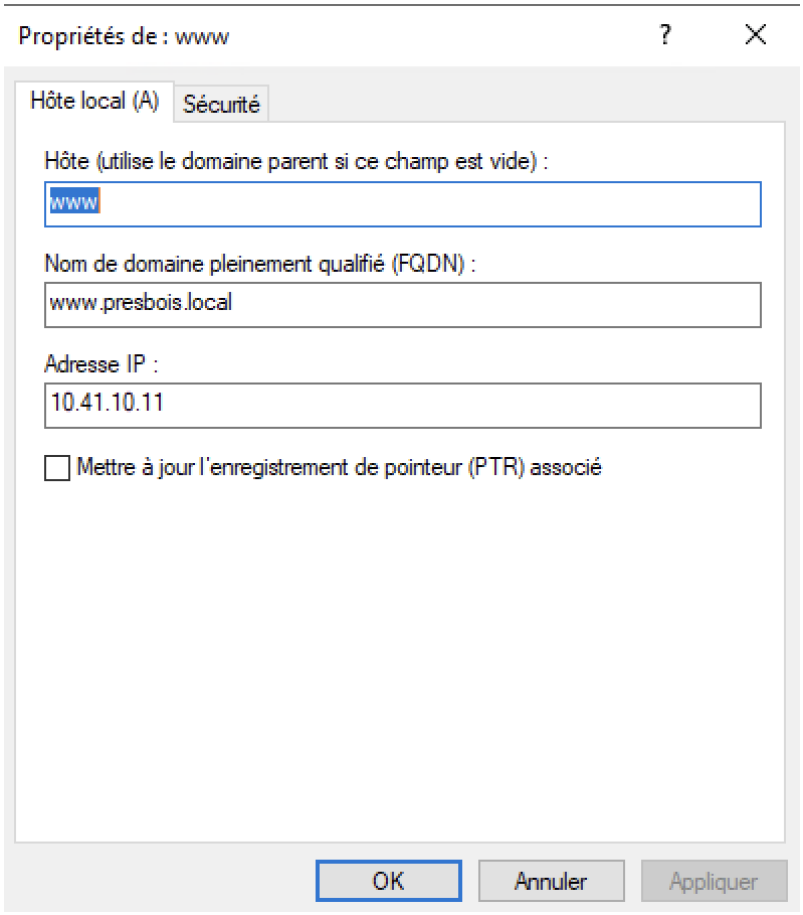
Mise en place DNS & tests finaux

Afin de mener de finir cette AP une des dernières tâches à effectuer étais la mise en place de DNS sur la maquette afin de pouvoir trouver le site web uniquement avec son nom de domaine dans notre barre de recherche. En local cela se fait via le fichier host cependant ce n'est ici pas nécessaire étant donné que nous avons notre propre serveur DNS sur notre Active Directory.

Objectif attendu :



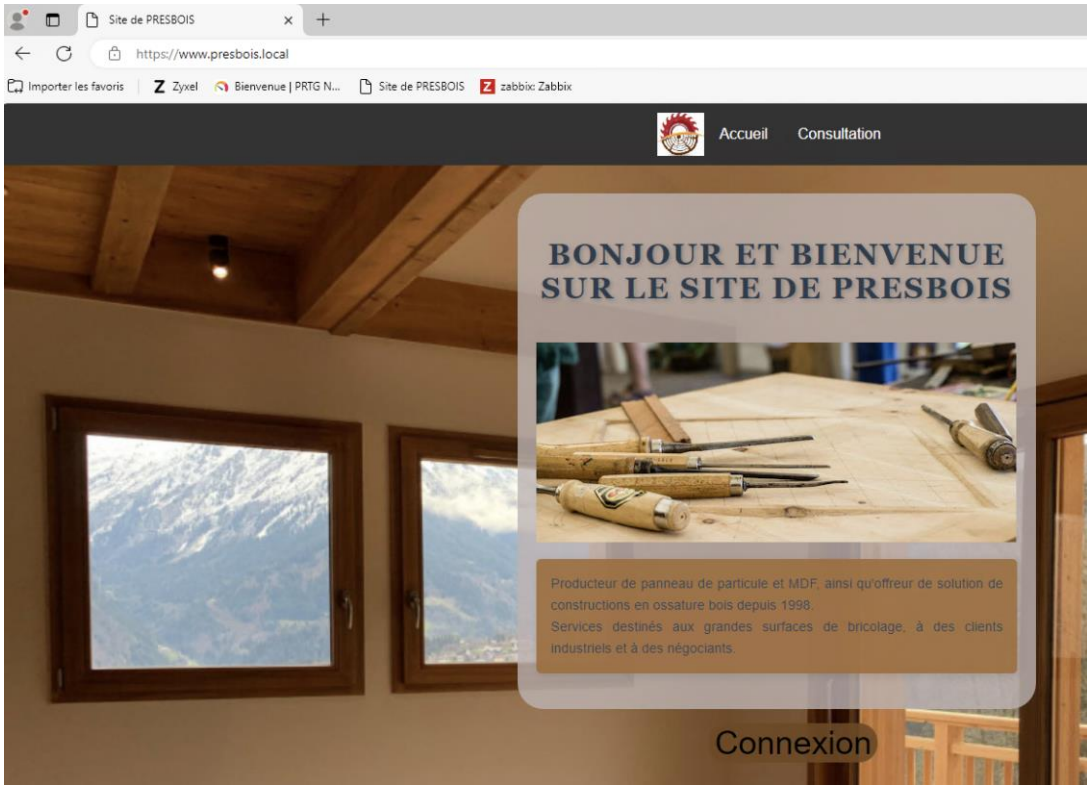
Ainsi, dans notre serveur DNS il faut rajouter un nouvel enregistrement de type (A) qui correspond à un enregistrement d'hôte ipv4, et y associer un nom de domaine voulu :



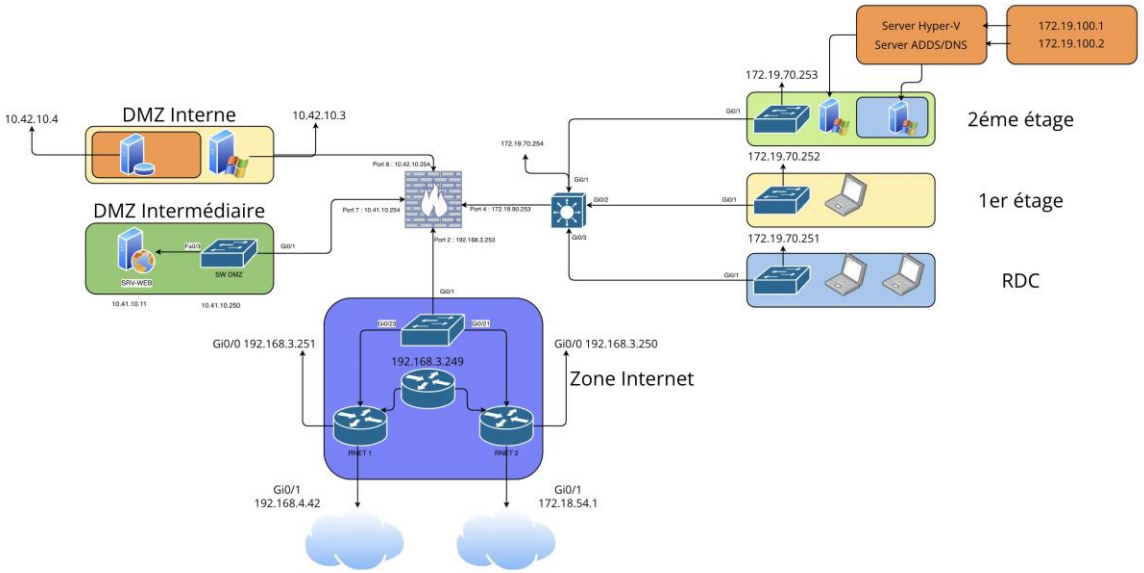
Une fois cette étape effectuée il faut s’assurer que tous nos postes ont bien comme DNS notre serveur DNS comme ceci :

```
Serveurs DNS. . .  . . . . . . . . . . . : 172.19.100.2
```

Puis il ne reste plus qu’à tester :



Annexes :



PROJET : Archi-Site
Groupe : 4
Chef de projet : Breggion
Durée prévisionnelle du projet : 22 h 00
Durée réelle du projet : 21 h 10

N°	Activité	Etudiant	Planning	Temps
1	Installation Hyper-V & srv web	Lucas	Prévisionnel	2:30
			Réel	3:10
2	Installation HyperV & BDD	Antoine	Prévisionnel	1:30
			Réel	1:30
3	Note technique	Groupe	Prévisionnel	0:30
			Réel	0:30
4	Installation FTPS & paramétrage	Antoine	Prévisionnel	1:30
			Réel	1:30
5	Paramétrage IP	Lucas	Prévisionnel	1:00
			Réel	0:45
6	paramétrage accès BDD et FTPS	Antoine	Prévisionnel	1:00
			Réel	0:30
7	Paramétrage srv web	Lucas	Prévisionnel	3:00
			Réel	0:30
8	Mise en place certificats	Lucas	Prévisionnel	2:00
			Réel	6:30
9	Règles parefeu WEB & FTP	Antoine	Prévisionnel	2:00
			Réel	1:30
10	Importation site web	Lucas	Prévisionnel	0:30
			Réel	0:30
11	Importation BDD	Antoine	Prévisionnel	2:00
			Réel	1:45
12	Mise en place MAriaDB	Antoine	Prévisionnel	2:00
			Réel	2:00
13	paramétrage DNS	Antoine	Prévisionnel	2:30
			Réel	0:30

Récapitulatif temps prévu et passé par étudiant		
Etudiant	Temps prévu	Temps réel
Lucas	09:00	11:25
Antoine	12:30	09:15