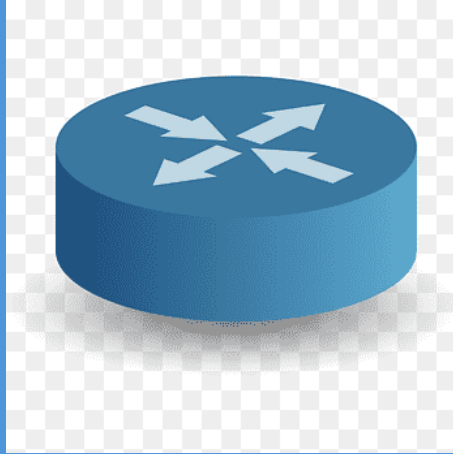


Documentation Routeur et Firewall

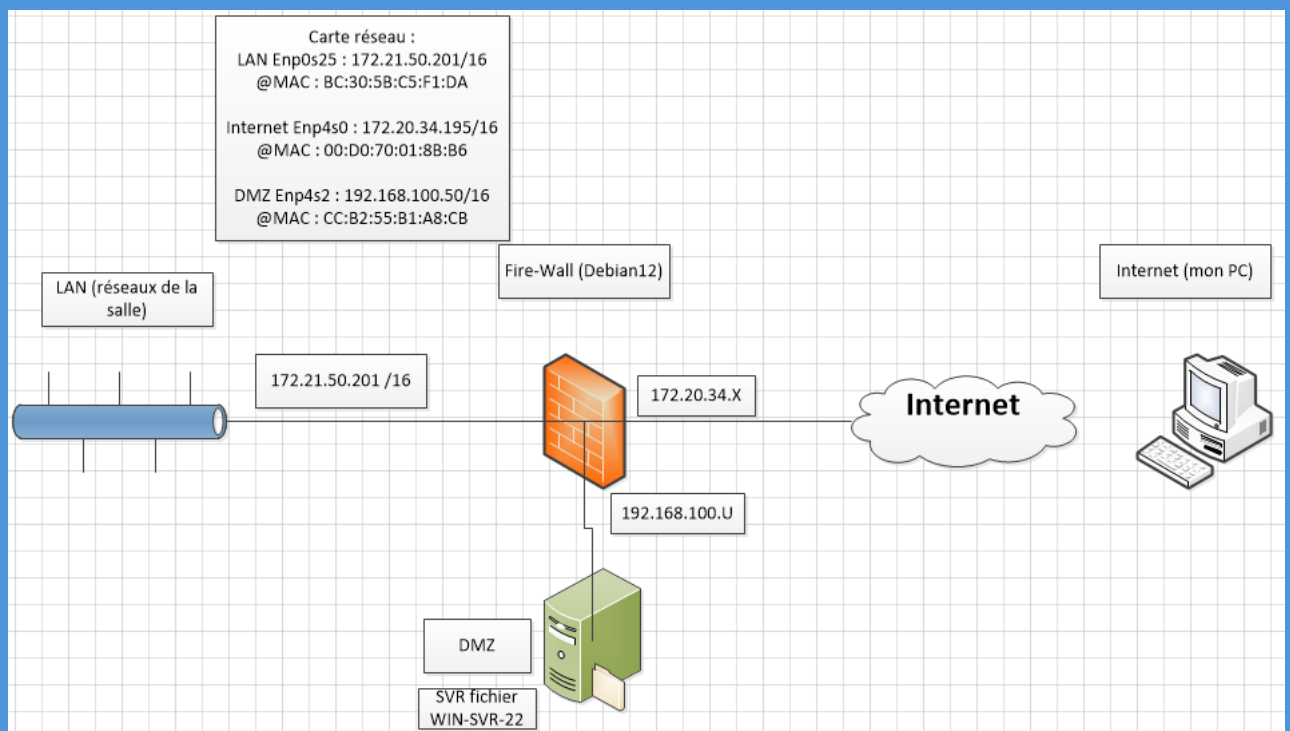


FIREWALL

Tables des matières :

Configuration du Firewall :	6
Activation du routage :	7
Configuration et installation du SVR WEB (IIS) :.....	9
Règles de nat et de filtrage pour pare-feu :.....	16
Configuration du FTPS :	18

Schéma réseau :



Configuration du Firewall :

I - LAN

Adresse MAC Interface enp0s25 :

BC:30:5B:C5:F1:DA

Adresse IP Interface enp0s25 :

172.21.50.201 /16

II – Internet

Adresse MAC Interface enp4s0 :

00:D0:70:01:8B:B6

Adresse IP Interface enp4s0 :

172.20.34.195 /16

III – DMZ

Adresse MAC Interface enp4s2 :

CC:B2:55:B1:A8:CB

Adresse IP Interface enp4s2 :

192.168.100.50 /24

Test :

```
root@Routeur-BEG-05:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:d0:70:01:8b:b6 brd ff:ff:ff:ff:ff:ff
    inet 172.20.34.195/16 brd 172.20.255.255 scope global enp4s0
        valid_lft forever preferred_lft forever
    inet6 fe80::ad5c:9327:e869:2157/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp4s2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether cc:b2:55:b1:a8:cb brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.50/24 brd 192.168.100.255 scope global enp4s2
        valid_lft forever preferred_lft forever
4: enp0s25: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether bc:30:5b:c5:f1:da brd ff:ff:ff:ff:ff:ff
    inet 172.21.50.201/16 brd 172.21.255.255 scope global enp0s25
        valid_lft forever preferred_lft forever
```

Activation du routage :

```
GNU nano 7.2 /etc/sysctl.conf *
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

```
GNU nano 7.2 /proc/sys/net/ipv4/ip_forward
1
```

Test :

```
C:\Users\HADJAB>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 172.21.34.88
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.21.50.201

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

C:\Users\HADJAB>ping 172.21.50.201

Envoi d'une requête 'Ping' 172.21.50.201 avec 32 octets de données :
Réponse de 172.21.50.201 : octets=32 temps<1ms TTL=64
Réponse de 172.21.50.201 : octets=32 temps<1ms TTL=64
Réponse de 172.21.50.201 : octets=32 temps<1ms TTL=64
Réponse de 172.21.50.201 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.21.50.201:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

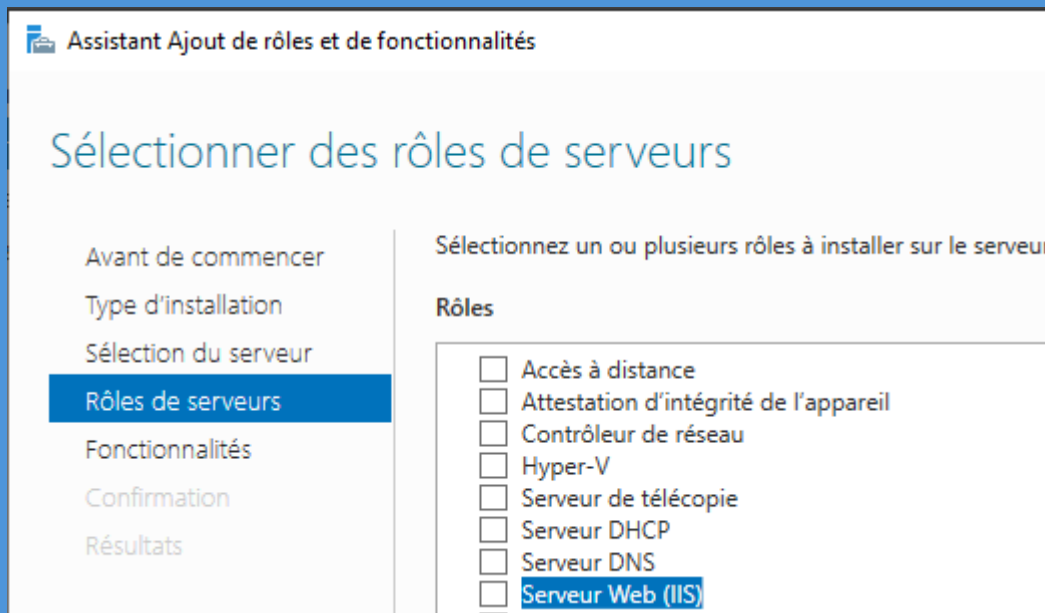
C:\Users\HADJAB>ping 192.168.100.50

Envoi d'une requête 'Ping' 192.168.100.50 avec 32 octets de données :
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.100.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```


Configuration et installation du SVR WEB (IIS) :

Installation de la VM SVR-WIN-22, pour installer le service IIS, il faut aller dans “Ajout de rôles et de fonctionnalités” --> “rôles des serveurs” et sélectionner “Serveur Web (IIS)” comme l’image si dessous.



Cliquer sur “suivant”, jusqu’à l’installation.

Création de la page web :

Cliquer sur << outils>> et <<gestionnaire de services (IIS)>>

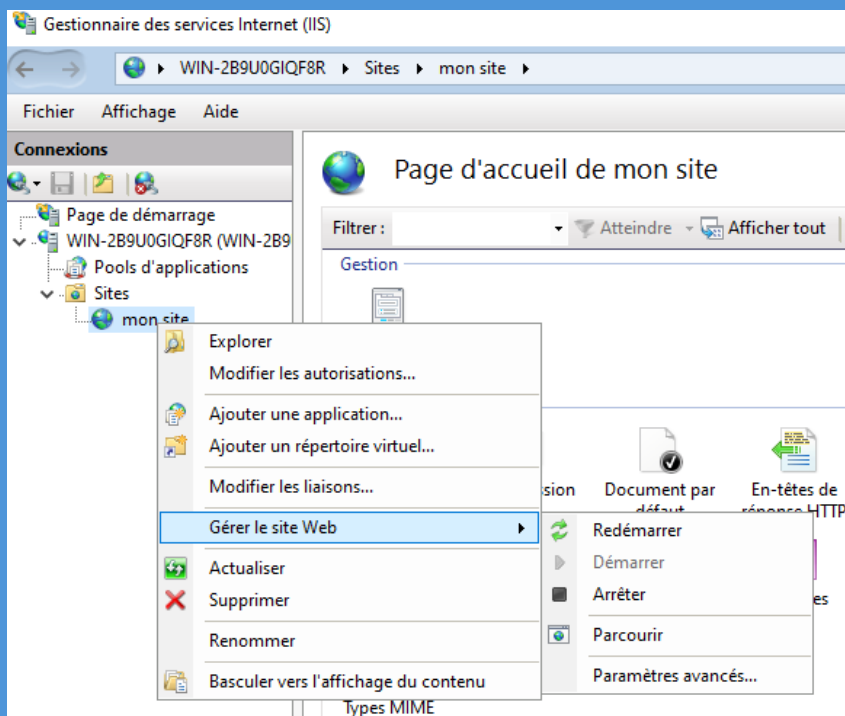
Puis cliquer sur votre nom de machine --> 'sites'.

Aller dans le disque "C:." créer un dossier nommé "WWW", créer un fichier txt dedans.

Écrire quelque chose dedans comme "bonjour, bienvenue chez nous", enregistrer.

Aller dans les propriétés du fichier pour changer le "txt" en "html".

Faite un clic droit dessus, aller dans << Gérer le site web>> et << paramètres avancés>>.

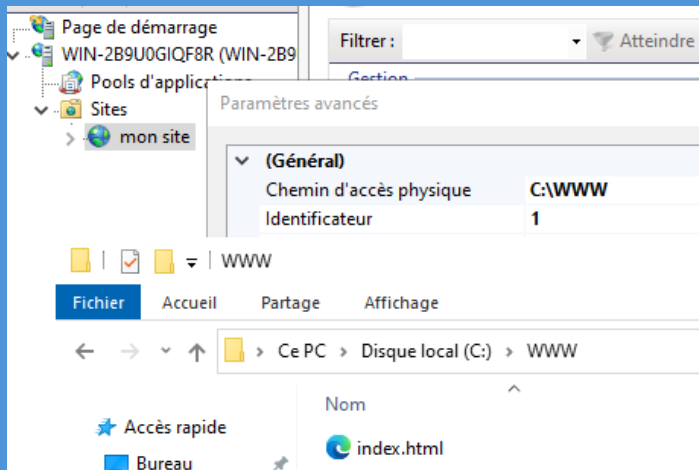


On remplace le chemin d'accès physique par défaut, par le chemin qui va à notre dossier qui contient la page web.

Notre chemin d'accès de notre sera le disque "C:" puis le dossier WWW.

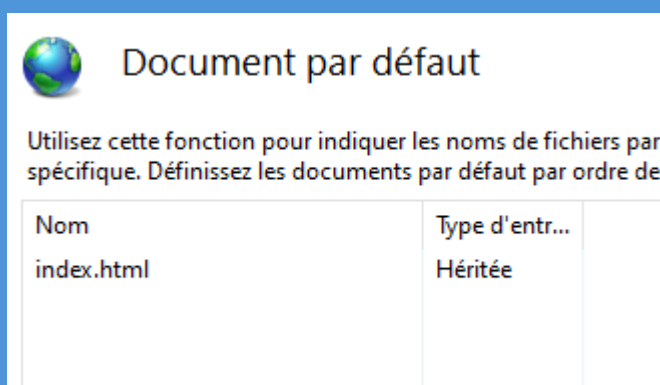
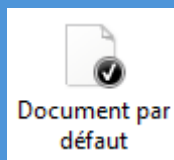
Cliquer le dossier WWW, pour affecter le nouveau chemin.

Votre fichier contenant la page web devra s'appeler "index.html".



Renommer le site web par défaut par le nom du site que vous voulez, "mon site".

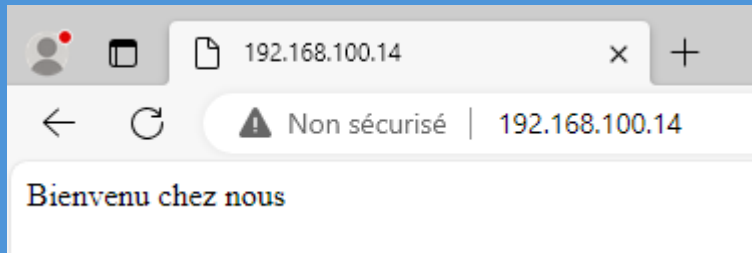
Penser à supprimer dans "documents par défaut", toutes les pages ou autres, il faut qu'il reste juste votre page web nommé "index.html".



Sur notre page web, on a mis "Bienvenu chez nous".

Voici le test réaliser :

On met notre @IP dans un navigateur web pour afficher notre page créée.



Pour le faire apparaitre sur un autre PC comme celui de Zinédine, il faut changer la conf IP du PC qui gère la machine virtuelle et changer l'@MAC de la machine virtuelle.

Voici une liste de ping réaliser depuis le SVR IIS

```
C:\Users\Administrateur>ping 192.168.100.50

Envoi d'une requête 'Ping' 192.168.100.50 avec 32 octets de données :
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.100.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>ping 172.20.34.88

Envoi d'une requête 'Ping' 172.20.34.88 avec 32 octets de données :
Réponse de 172.20.34.88 : octets=32 temps=1 ms TTL=127
Réponse de 172.20.34.88 : octets=32 temps=1 ms TTL=127
Réponse de 172.20.34.88 : octets=32 temps=1 ms TTL=127
Réponse de 172.20.34.88 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.20.34.88:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Le premier ping explique que je ping la DMZ depuis le serveur IIS.

Le deuxième ping explique que je ping le serveur IIS au PC de Zineddine.

Voici une liste de ping réaliser depuis le PC de zineddine :

```
C:\Users\HADJAB>ping 172.20.34.195

Envoi d'une requête 'Ping' 172.20.34.195 avec 32 octets de données :
Réponse de 172.20.34.195 : octets=32 temps<1ms TTL=64
Réponse de 172.20.34.195 : octets=32 temps<1ms TTL=64
Réponse de 172.20.34.195 : octets=32 temps<1ms TTL=64
Réponse de 172.20.34.195 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.20.34.195:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\HADJAB>ping 192.168.100.50

Envoi d'une requête 'Ping' 192.168.100.50 avec 32 octets de données :
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.50 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.100.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\HADJAB>ping 192.168.100.14

Envoi d'une requête 'Ping' 192.168.100.14 avec 32 octets de données :
Réponse de 192.168.100.14 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.14 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.14 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.14 : octets=32 temps=1 ms TTL=127

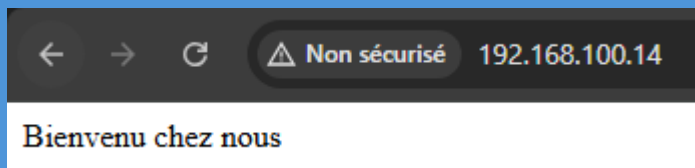
Statistiques Ping pour 192.168.100.14:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Le ping 172.20.34.195, du PC de zino vers internet

Le ping 192.168.100.50, de internet au routeur de la DMZ

Le ping 192.168.100.14, de internet au SVR IIS

On peut apercevoir depuis internet notre page web créée.



Connexion SSH de mon PC vers le FW :

Commande : `ssh admin-rbeg@Routeur-BEG-05`

MDP : rbeg5

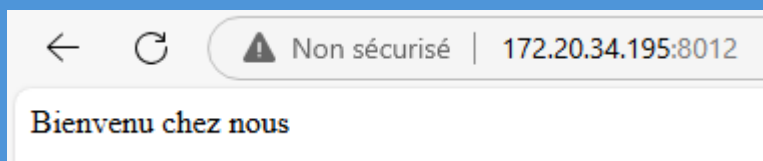
Règles de nat et de filtrage pour pare-feu :

Règles de NAT :

```
iptables -t nat -A PREROUTING -p tcp --dport 8012 -i enp4s0 -j DNAT --to-destination 192.168.100.14:80
```

```
iptables -t nat -A POSTROUTING -o enp4s0 -j MASQUERADE
```

Test :



Règles de filtrage :

De base à mettre :

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

1 input:

```
iptables -A INPUT -p tcp --dport 22 -s 172.20.5.38 (ip de l'admin) -j ACCEPT
```

1 output:

```
iptables -A OUTPUT -p tcp --sport 22 -d 172.20.5.38 (ip de l'admin) -m state --state ESTABLISHED,RELATED -j ACCEPT
```


Test (un avec l'IP de l'administrateur en 172.20.5.38 puis test avec l'IP d'un client autre que l'administrateur en 172.20.5.36) :

```
C:\Windows\system32>ssh admin-rbeg@Routeur-BEG-05
admin-rbeg@routeur-beg-05's password:
Linux Routeur-BEG-05 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 13 18:16:27 2024 from 172.20.5.38
admin-rbeg@Routeur-BEG-05:~$ client_loop: send disconnect: Connection reset

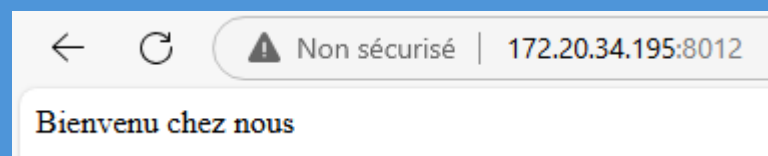
C:\Windows\system32>ssh admin-rbeg@Routeur-BEG-05
C:\Windows\system32>
```

Sauvegarde règle filtrage : netfilter-persistent save

2 forward : **iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT**

Iptables -A FORWARD -d 192.168.100.14/24 -p tcp --dport 80 -m state --state NEW -j ACCEPT

Test :



Configuration du FTPS :

Installation du service FTP anonyme (sur le serveur de fichiers) :

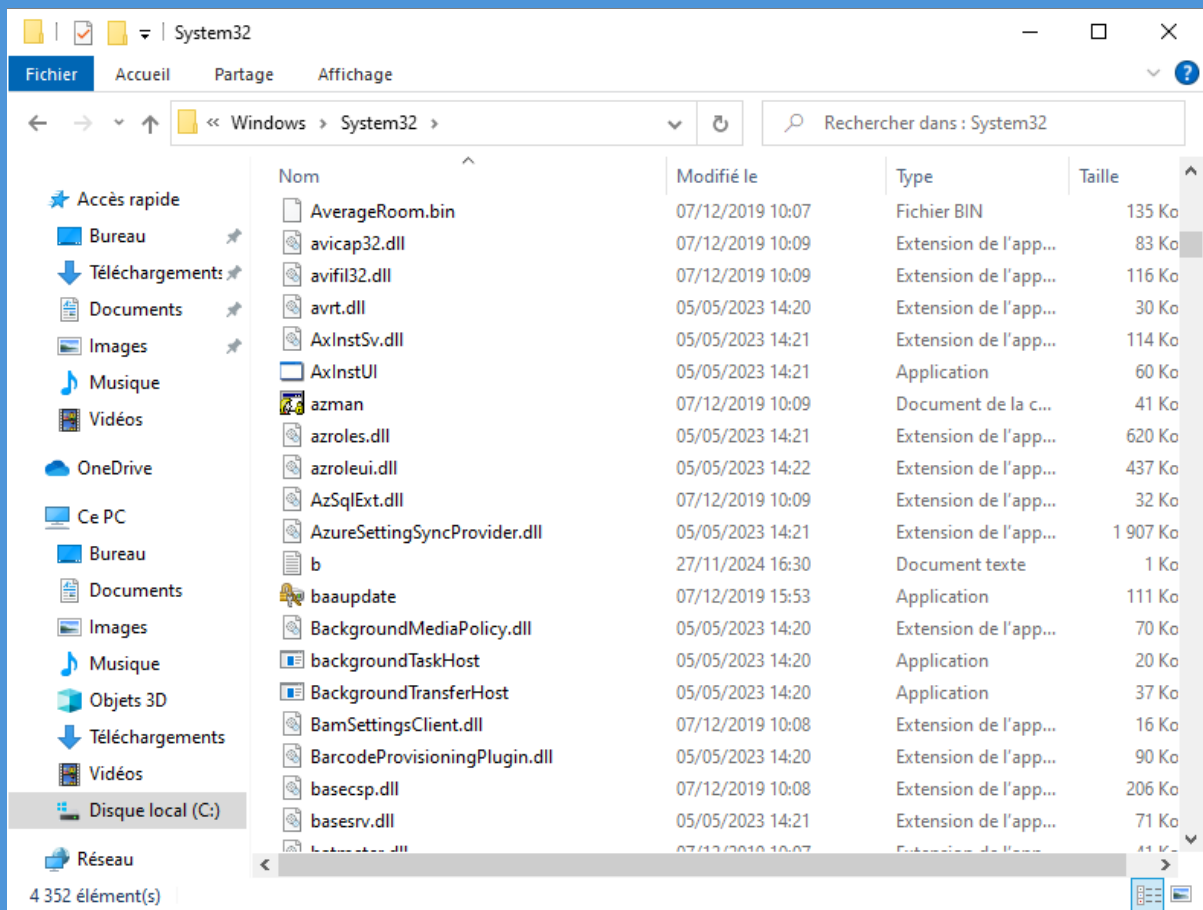
Voir [DOC](#)

Paramétrer en mode anonyme

Test :

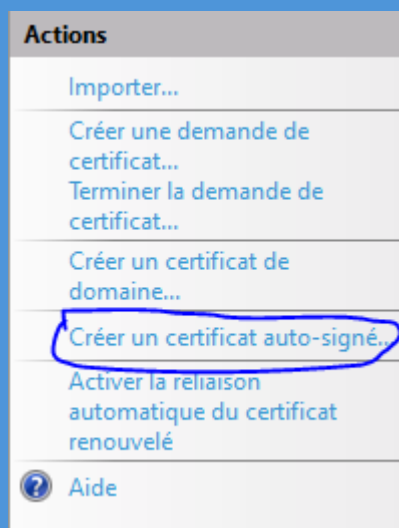
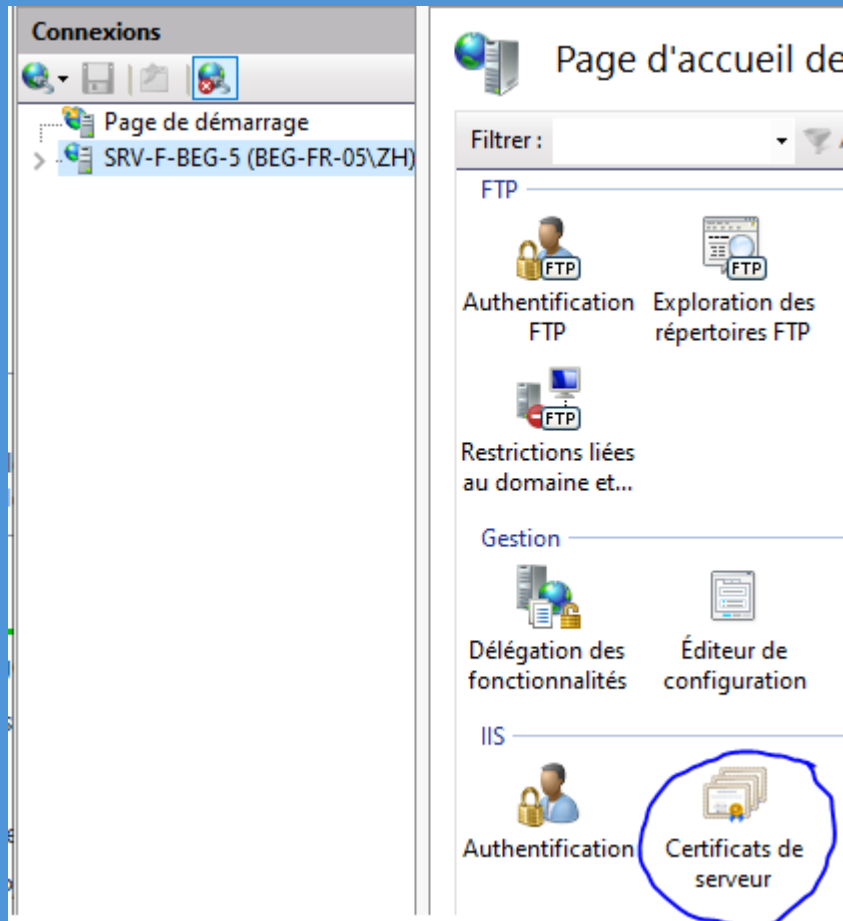
```
C:\Windows\system32>ftp 172.20.15.100
Connecté à 172.20.15.100.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Utilisateur (172.20.15.100:(none)) : anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Mot de passe :
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-27-24 04:29PM <DIR> a.dion
09-20-24 01:10PM <DIR> a.dossantosjesus
09-20-24 01:10PM <DIR> a.dufour
11-22-24 04:21PM <DIR> test
226 Transfer complete.
ftp : 201 octets reçus en 0.00 secondes à 201000.00 Ko/s.
ftp> cd a.dion
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-27-24 04:28PM 9 b.txt
226 Transfer complete.
ftp : 49 octets reçus en 0.00 secondes à 49000.00 Ko/s.
ftp> mget b.txt
200 Type set to A.
mget b.txt?
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp : 9 octets reçus en 0.04 secondes à 0.23 Ko/s.
ftp> _
```

Le fichier se retrouve là :




Mise en place du service FTPS :

Création du certificat autosigné :



Créer un certificat auto-signé ? X

 **Indiquer un nom convivial**

Indiquez un nom de fichier pour la demande de certificat. Ces informations peuvent être envoyées à une autorité de certification en vue de la signature :

Indiquer un nom convivial pour le certificat :

Sélectionnez un magasin de certificats pour le nouveau certificat :

▼

OK Annuler

Création du site FTP :

Connexions

- Page de démarrage
- SRV-F-BEG-5 (BEG-FR-05\ZH)
- Pools d'applications
- Sites
 - Default Web Site


Sites

Filtrer : Atteindre Afficher tout Regrouper par : Aucun regroupement

Nom	Identificate...	État	Liaison	Chemin d'accès
Default Web Site	1	Arrêté (http)	*:80 (http)	%SystemDrive%\inetpub\wwwroot

Ajouter un site Web...
Définir les valeurs par défaut des sites Web...
Ajouter un site FTP...

Ajouter un site FTP ? X

 **Informations sur le site**

Nom du site FTP :

BEG-FTP


Répertoire de contenu

Chemin d'accès physique :

C:\Private\$...

Précédent Suivant Terminer Annuler

Ajouter un site FTP ? X

 **Liaison et paramètres SSL**

Liaison

Adresse IP : Port :
Toutes non attribuées 990

☐ Activer les noms des hôtes virtuels :
Hôte virtuel (exemple : ftp.contoso.com) :

☒ Démarrer automatiquement le site FTP


SSL

☐ Pas de SSL
☐ Autoriser SSL
☒ Exiger SSL

Certificat SSL :
FTPS-BEG Sélectionner... Afficher...

Précédent Suivant Terminer Annuler

Ajouter un site FTP ? X

 **Informations sur les autorisations et l'authentification**

Authentification

☐ Anonyme
☒ De base

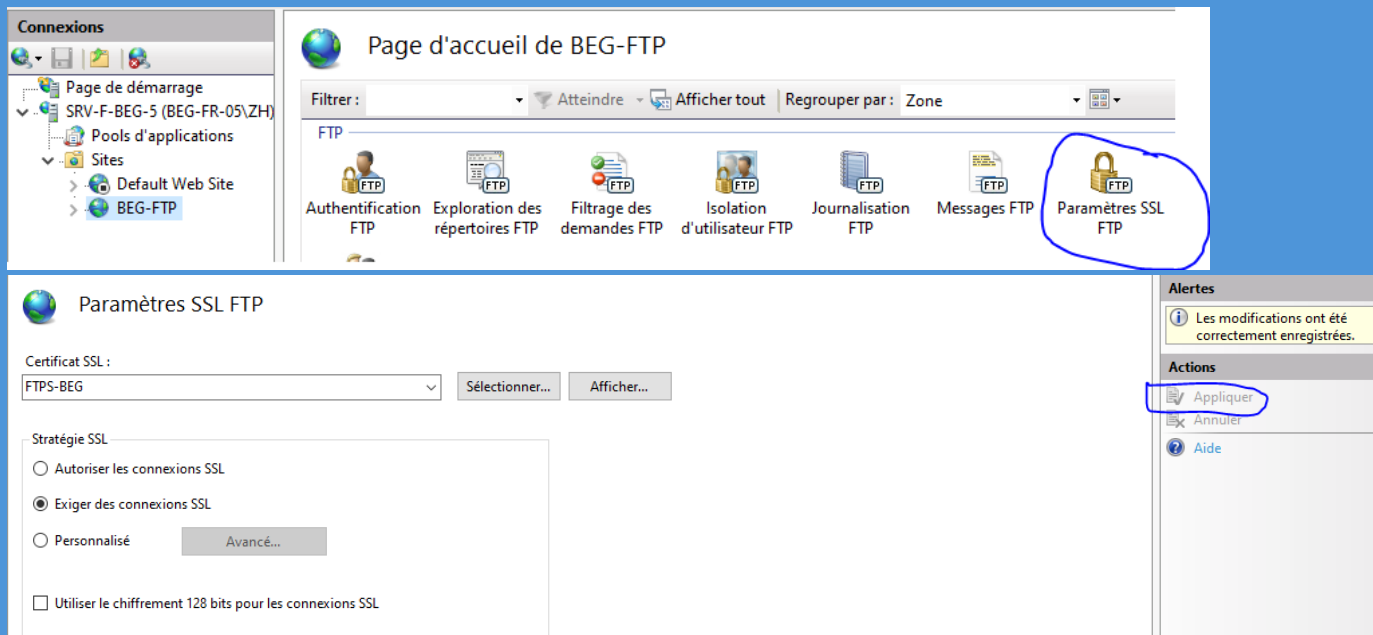
Autorisation

Autoriser l'accès à :
Tous les utilisateurs

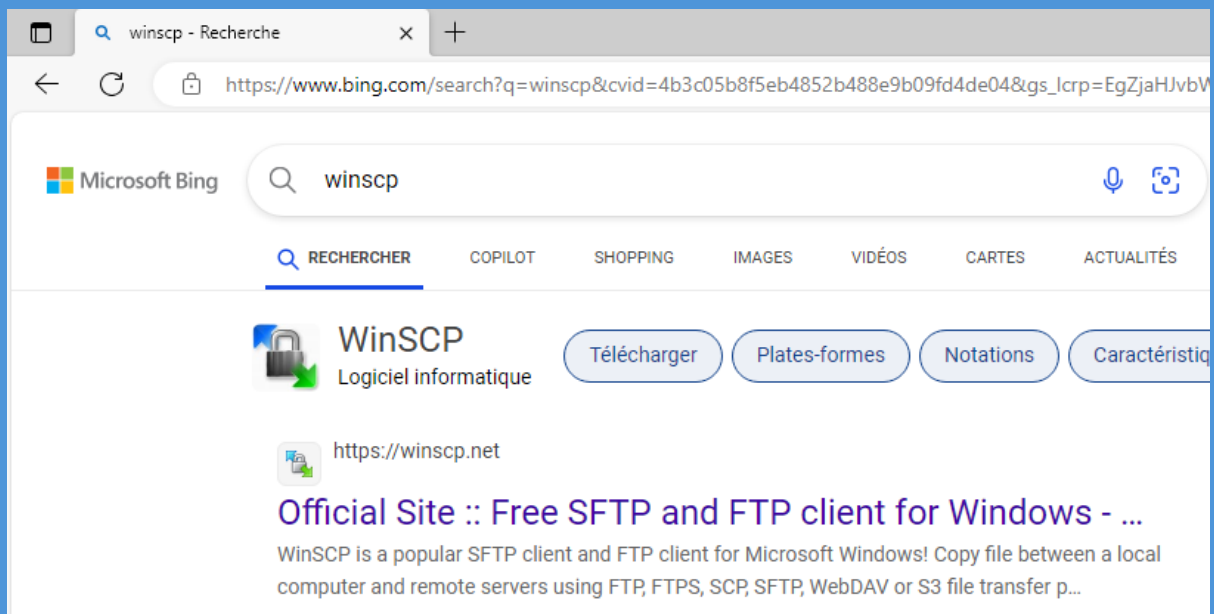
Autorisations

☒ Lecture
☒ Écriture

Précédent Suivant Terminer Annuler



Test (avec un client possédant WinSCP) :





WinSCP

Free SFTP, SCP, S3 and FTP client for Windows

Search

[Home](#)[News](#)[Introduction](#)[Download](#)[Install](#)[Documentat](#)

Free Award-Winning File Manager

WinSCP is a popular SFTP client and FTP client for Microsoft Windows!

Copy file between a local computer and remote servers using

FTP, FTPS, SCP, SFTP, WebDAV or S3 file transfer protocols.

[DOWNLOAD NOW](#)[ABOUT WINSCP](#)

227 million downloads to date

THE CLOCK IS TICKING...
ON INTERNET
EXPLORER



June 15th 2022, Internet Explorer
goes out of support
Is Your Organization
Ready?

The End of Internet Explorer



Flynet Ltd

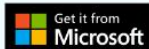
[Download](#)

WinSCP 6.3 is a major application update. New features and enhancements include:

- Single large file can be downloaded using multiple SFTP connections.
- Support for OpenSSH certificates for host verification.
- File hash can be used as criterion for synchronization.
- Improved behavior when duplicating and moving remote files.
- Support for HMAC-SHA-512.
- TLS/SSL core upgraded to OpenSSL 3.
- [List of all changes.](#)

[DOWNLOAD WINSCP 6.3.6 \(11 MB\)](#)

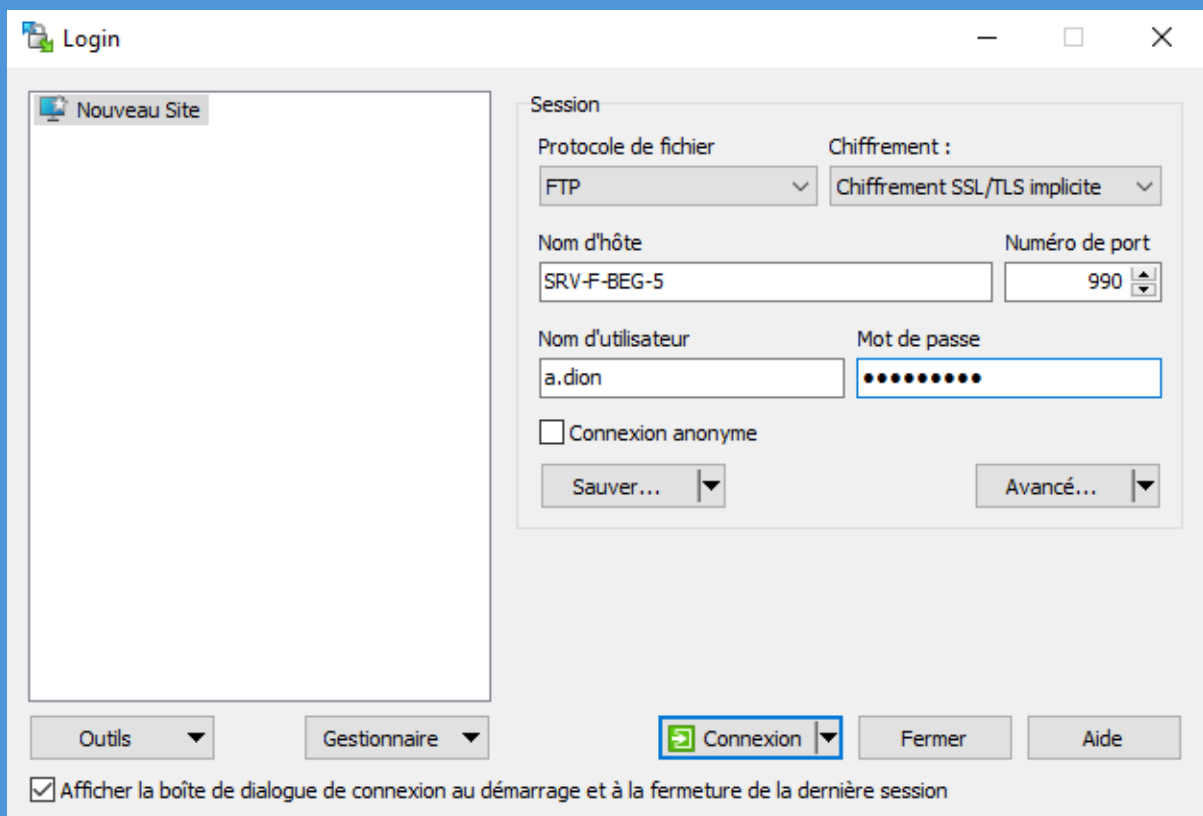
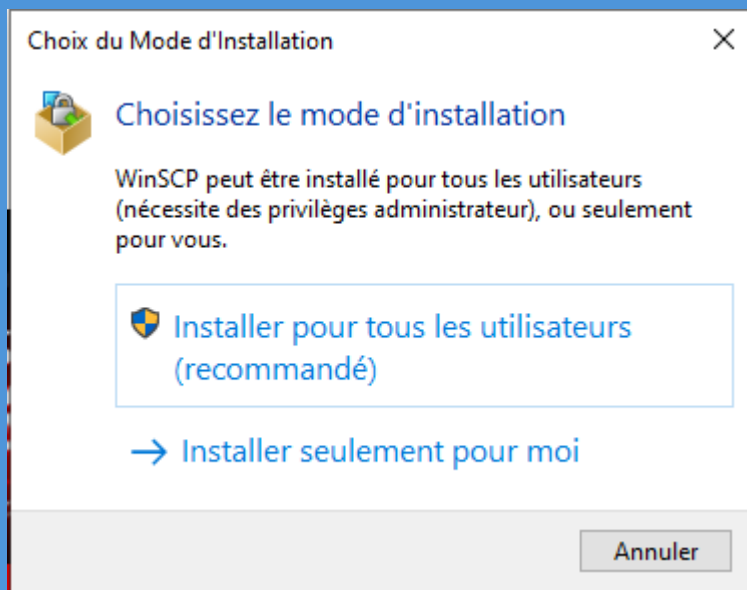
610,398 downloads since 2024-11-25

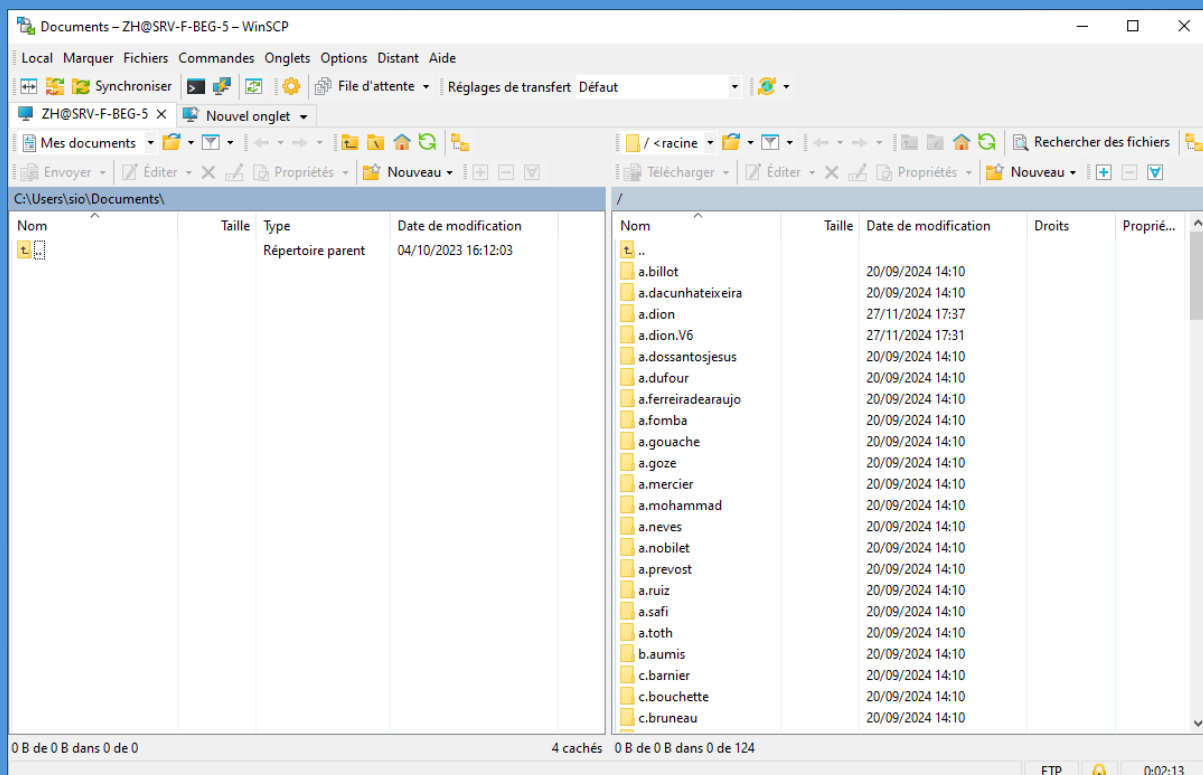
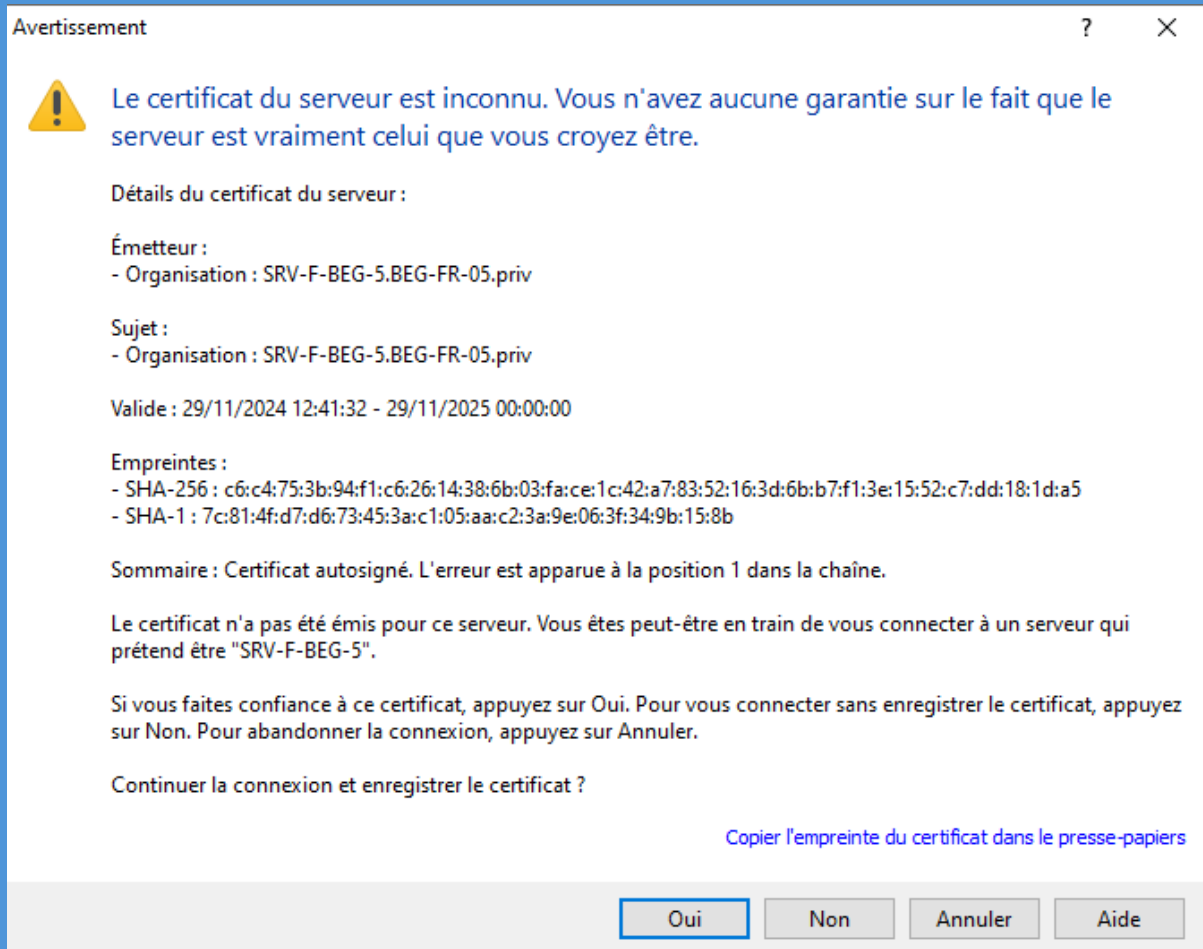


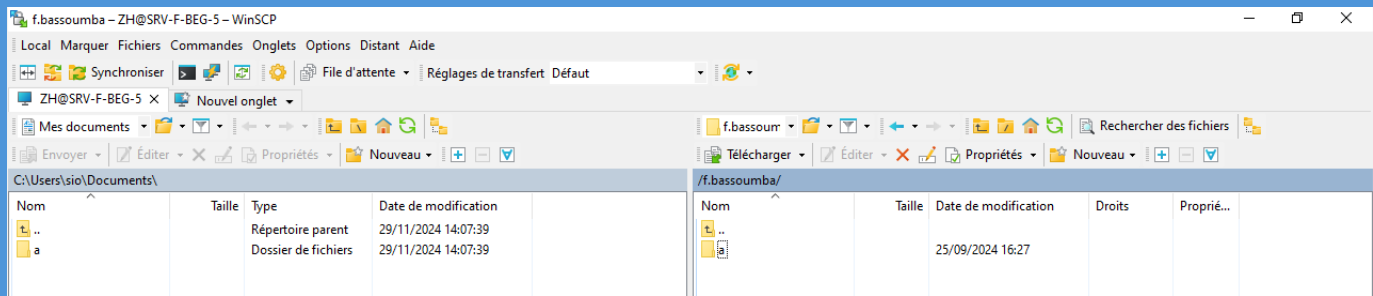
50% OFF

[OTHER DOWNLOADS](#)

[What is this?](#)







WebDav :

1-Teste SFTP :

2-Teste webDav :

Connexion via le port 80 en html

L'utilisateur doit se connecter à son espace de fichier depuis une page web

Il modifier dans le dns, que le svr de fichier == www (le serveur de fichier doit remplacé le www)

Lien utilisable :

<https://helpcenter.onlyoffice.com/fr/installation/groups-connect-webdav-windows.aspx>

<https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/cloud/azure/syncroazure/webdav>

- SVR de domaine et fichier allumé
-