

# Mise en place d'un VPN sous Debian 8 avec OPENVPN



Objectif :

→ Mettre en place un serveur et client OpenVPN sous Debian 8 et Windows 7, nous voulons aussi que les clients est accès à un serveur Windows 2008 R2 en passant par le tunnel vpn.

# Table des matières

❖ CHAP.1 Configuration IP.

❖ CHAP.2 Schématisation.

❖ CHAP.3 Installation du service OPENVPN.

❖ CHAP.4 Création des certificats CA.

❖ CHAP.5 Générer la clé Diffie-Hellman.

❖ CHAP.6 Création des certificats serveur.

❖ CHAP.7 Configuration du d'OpenVPN Server.

❖ CHAP.8 Création des certificats client.

❖ CHAP.9 Configuration du d'openVPN client sous Windows.

❖ CHAP.9 **BIS** Configuration du d'openVPN client sous Debian 8.



CHAP.10 Partie Validation.



CHAP.11 Configuration d'un accès au serveur de fichier  
Windows.

❖ CHAP.1 Configuration IP.

⇒ Configuration IP du Serveur VPN Debian :

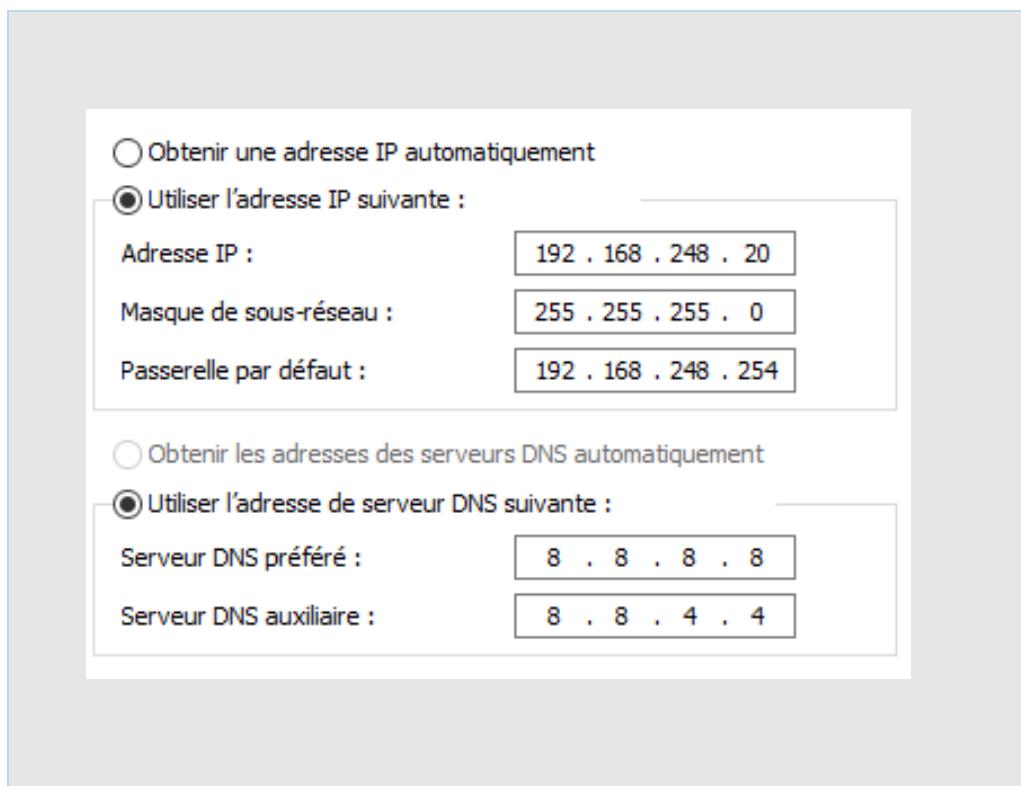
```
root@debianvpn:/home/mrnice# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:95:e6:ec
          inet adr:192.168.248.26 Bcast:192.168.248.255 Masque:255.255.255.0
            adr inet6: fe80::a00:27ff:fe95:e6ec/64 Scope:Lien
            adr inet6: 2a01:cb19:82c9:6f00:a00:27ff:fe95:e6ec/64 Scope:Global
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:648 errors:0 dropped:68 overruns:0 frame:0
              TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 lg file transmission:1000
              RX bytes:72604 (70.9 KiB) TX bytes:13737 (13.4 KiB)

eth1      Link encap:Ethernet HWaddr 08:00:27:b9:9e:44
          inet adr:172.16.20.10 Bcast:172.16.20.255 Masque:255.255.255.0
            adr inet6: fe80::a00:27ff:feb9:9e44/64 Scope:Lien
            adr inet6: 2a01:cb19:82c9:6f00:a00:27ff:feb9:9e44/64 Scope:Global
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:625 errors:0 dropped:70 overruns:0 frame:0
              TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 lg file transmission:1000
              RX bytes:63621 (62.1 KiB) TX bytes:12470 (12.1 KiB)
```

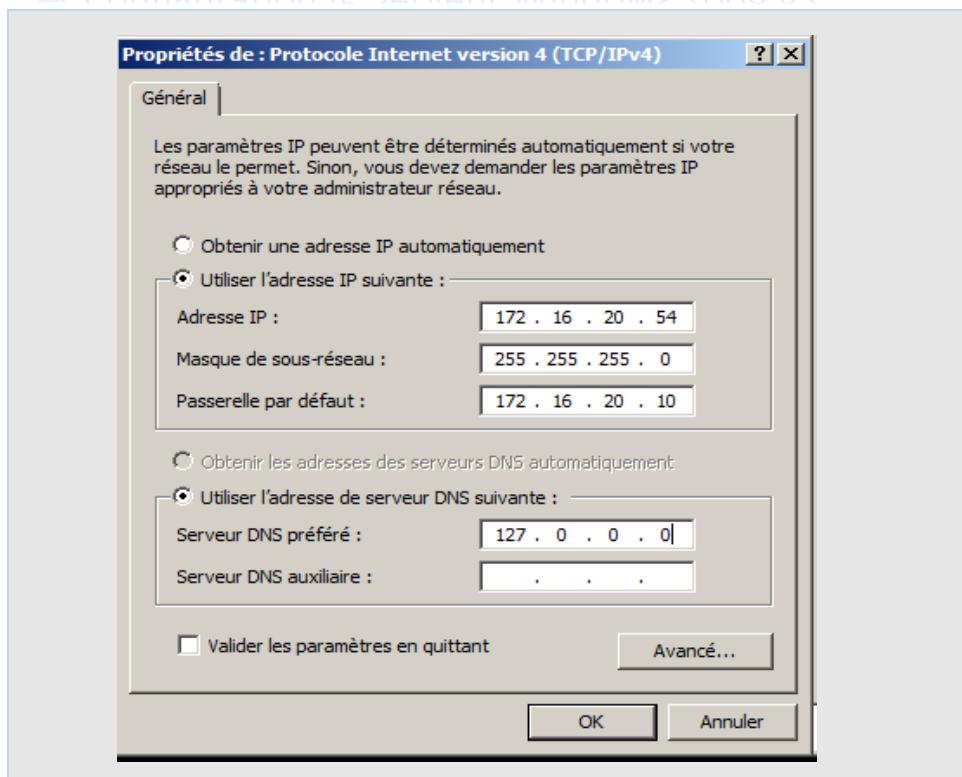
## ➤ Configuration IP client Debian 8 :

```
eth0      Link encap:Ethernet HWaddr 08:00:27:3d:a2:67
          inet adr:192.168.248.64 Bcast:192.168.248.255 Masque:255.255.255.0
            adr inet6: fe80::a00:27ff:fe3d:a267/64 Scope:Lien
            adr inet6: 2a01:cb19:82c9:6f00:a00:27ff:fe3d:a267/64 Scope:Global
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:13875 errors:0 dropped:1063 overruns:0 frame:0
              TX packets:7148 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 lg file transmission:1000
              RX bytes:2511769 (2.3 MiB) TX bytes:1019239 (995.3 KiB)
```

## ⇒ Configuration IP Windows Client :

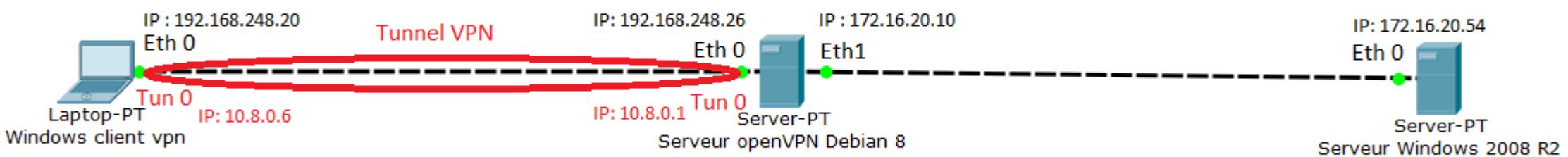


## ⇒ Configuration IP Serveur Windows 2008 R2 :





## CHAP.2 Schématisation.



- Ne pas oublier d'installer le mode sudo pour travailler en toutes sécurité, comme nous travaillons en local nous n'utiliserons pas le mode sudo :

```
root@debianvpn:/home/mrnice# apt-get install sudo
```

- Installation d'openVPN :

```
root@debianvpn:/home/mrnice# apt-get install openvpn
```

- Mise à jour :

```
root@debianvpn:/home/mrnice# apt-get update
```

- Copier le dossier easy-rsa qui se trouve dans /usr/share/ dans /etc/openvpn :

```
root@debianvpn:/home/mrnice# cp -a /usr/share/easy-rsa /etc/openvpn/
```

- Aller dans le dossier /etc/openvpn/easy-rsa

```
root@debianvpn:/home/mrnice# cd /etc/openvpn/easy-rsa
```

```
root@debianvpn:/etc/openvpn/easy-rsa# |
```

➤ Taper ls -l pour regarder les fichiers :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -l
total 112
-rwxr-xr-x 1 root root    119 janv.  7 2014 build-ca
-rwxr-xr-x 1 root root   352 janv.  7 2014 build-dh
-rwxr-xr-x 1 root root   188 janv.  7 2014 build-inter
-rwxr-xr-x 1 root root   163 janv.  7 2014 build-key
-rwxr-xr-x 1 root root   157 janv.  7 2014 build-key-pass
-rwxr-xr-x 1 root root   249 janv.  7 2014 build-key-pkcs12
-rwxr-xr-x 1 root root   268 janv.  7 2014 build-key-server
-rwxr-xr-x 1 root root   213 janv.  7 2014 build-req
-rwxr-xr-x 1 root root   158 janv.  7 2014 build-req-pass
-rwxr-xr-x 1 root root   449 janv.  7 2014 clean-all
-rwxr-xr-x 1 root root  1471 janv.  7 2014 inherit-inter
-rwxr-xr-x 1 root root   302 janv.  7 2014 list-crl
-rw-r--r-- 1 root root  7859 janv.  7 2014 openssl-0.9.6.cnf
-rw-r--r-- 1 root root  8416 janv.  7 2014 openssl-0.9.8.cnf
-rw-r--r-- 1 root root  8313 janv.  7 2014 openssl-1.0.0.cnf
-rwxr-xr-x 1 root root 13246 janv.  7 2014 pkictool
-rwxr-xr-x 1 root root  1035 janv.  7 2014 revoke-full
-rwxr-xr-x 1 root root   178 janv.  7 2014 sign-req
-rw-r--r-- 1 root root  2077 janv.  7 2014 vars
```

➤ Supprimer toutes les clés du fichier vars :

```
root@debianvpn:/home/mrnice# cd /etc/openvpn/easy-rsa
root@debianvpn:/etc/openvpn/easy-rsa# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
root@debianvpn:/etc/openvpn/easy-rsa# ./clean-all
root@debianvpn:/etc/openvpn/easy-rsa# █
```



## CHAP.4 Création des certificats CA.

➤ Création des certificats de l'autorité de certification racine CA :

```
root@debianvpn:/etc/openvpn/easy-rsa# ./build-ca
```

- Personnalisation des paramètres des certificats CA, laissez-les par défauts :

```
Generating a 2048 bit RSA private key
.+++
.....
.....++++
writing new private key to 'ca.key'
-----
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) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:
```

- Après la création vérifier que les certificats soient bien créés et qu'ils soient lisibles que par l'utilisateur root, taper la commande suivante :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/
```

```
drwx----- 2 root root 4096 nov. 12 18:51 .
drwxr-xr-x 3 root root 4096 nov. 12 17:19 ..
-rw-r--r-- 1 root root 5736 nov. 12 18:51 01.pem
-rw-r--r-- 1 root root 1818 nov. 12 18:05 ca.crt
-rw----- 1 root root 1704 nov. 12 18:05 ca.key
-rw-r--r-- 1 root root 424 nov. 12 18:37 dh2048.pem
-rw-r--r-- 1 root root 152 nov. 12 18:51 index.txt
-rw-r--r-- 1 root root 21 nov. 12 18:51 index.txt.attr
-rw-r--r-- 1 root root 0 nov. 12 17:19 index.txt.old
-rw-r--r-- 1 root root 3 nov. 12 18:51 serial
-rw-r--r-- 1 root root 3 nov. 12 17:19 serial.old
-rw-r--r-- 1 root root 5736 nov. 12 18:51 srvcert.crt
-rw-r--r-- 1 root root 1102 nov. 12 18:51 srvcert.csr
-rw----- 1 root root 1704 nov. 12 18:51 srvcert.key
```

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/
total 20
drwx----- 2 root root 4096 nov. 12 18:05 .
drwxr-xr-x 3 root root 4096 nov. 12 17:19 ..
-rw-r--r-- 1 root root 1818 nov. 12 18:05 ca.crt
-rw----- 1 root root 1704 nov. 12 18:05 ca.key
-rw-r--r-- 1 root root 0 nov. 12 17:19 index.txt
-rw-r--r-- 1 root root 3 nov. 12 17:19 serial
```



## CHAP.5 Générer la clé Diffie-Hellman.

- On génère la clé Diffie-Hellman, clé de cryptage qui sert à sécuriser les échanges,  
[https://fr.wikipedia.org/wiki/%C3%89change\\_de\\_cl%C3%A9\\_Diffie-Hellman](https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9_Diffie-Hellman) :

```
root@debianvpn:/etc/openvpn/easy-rsa# ./build-dh
```

```
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....+.....
+.....+.....
.....+.....
.....+.....
.....+.....
```

- Après la création vérifier que la clé de cryptage soit bien créée et qu'elle soit lisible que par l'utilisateur root, taper la commande suivante :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/
total 92
drwx----- 2 root root 4096 déc.  3 14:18 .
drwxr-xr-x 3 root root 4096 nov. 12 17:19 ..
-rw-r--r-- 1 root root 5736 nov. 12 18:51 01.pem
-rw-r--r-- 1 root root 5641 déc.  3 14:18 02.pem
-rw-r--r-- 1 root root 1818 nov. 12 18:05 ca.crt
-rw----- 1 root root 1704 nov. 12 18:05 ca.key
-rw-r--r-- 1 root root  424 nov. 12 18:37 dh2048.pem
```



## CHAP.6 Crédit des certificats serveur.

- Crédit des certificats serveur :

```
root@debianvpn:/etc/openvpn/easy-rsa# ./build-key-server srvcert
```

- Personnalisation des paramètres des certificats serveur, laisser les paramètres par défauts sauf le paramètre du nom de votre serveur :

```
Country Name (2 letter code) [US]:  
State or Province Name (full name) [CA]:  
Locality Name (eg, city) [SanFrancisco]:  
Organization Name (eg, company) [Fort-Funston]:  
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:  
Common Name (eg, your name or your server's hostname) [srvcert]:debianvpn  
Name [EasyRSA]:  
Email Address [me@myhost.mydomain]:  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:  
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf  
Check that the request matches the signature  
Signature ok  
The Subject's Distinguished Name is as follows  
countryName :PRINTABLE:'US'  
stateOrProvinceName :PRINTABLE:'CA'  
localityName :PRINTABLE:'SanFrancisco'  
organizationName :PRINTABLE:'Fort-Funston'  
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'  
commonName :PRINTABLE:'debianvpn'  
name :PRINTABLE:'EasyRSA'  
emailAddress :IA5STRING:'me@myhost.mydomain'  
Certificate is to be certified until Nov 10 17:51:32 2027 GMT (3650 days)  
Sign the certificate? [y/n]:y  
  
1 out of 1 certificate requests certified, commit? [y/n]y  
Write out database with 1 new entries  
Data Base Updated
```

- Après la création vérifier que les certificats soient bien créés et qu'ils soient lisibles que par l'utilisateur root, taper la commande suivante :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/
```



## CHAP.7 Configuration du d'openVPN.

- Vérifier quelle est l'adresse du serveur DNS du VPN et vous en rappeler :

```
# Generated by NetworkManager
search home home.
nameserver 8.8.8.8
```

- Décompresser le fichier server.conf.gz qui est dans /usr/share/doc/openvpn/examples/sample-config-files/ dans le fichier /etc/openvpn/server.conf :

```
root@debianvpn:/etc/openvpn# gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf
```

- Edition du fichier server.conf ayant d'éditer le fichier faire une copie et enlever les lignes commenté par un # pour y voir plus claire:

```
root@debianvpn:/etc# cp /etc/openvpn/server.conf /etc/openvpn/server.conf.old
```

```
root@debianvpn:/etc/openvpn# nano /etc/openvpn/server.conf root@debianvpn:/etc/openvpn# grep -E -v '^(#|$)' /etc/openvpn/server.conf.old > /etc/openvpn/server.conf
```

➤ Modifier, ou dés commenter les lignes suivante :

```
root@debianvpn:/etc/openvpn# nano /etc/openvpn/server.conf
```

```
;local a.b.c.d
port 1194
proto tcp
;proto udp
;dev tap
dev tun
;dev-node MyTap
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/srvcert.crt
key /etc/openvpn/easy-rsa/keys/srvcert.key
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
```

```
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
;log          openvpn.log
;log-append  openvpn.log
verb 3
```

➤ Chemin des certificats :

```
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/srvcert.crt
key /etc/openvpn/easy-rsa/keys/srvcert.key  # This file should be kept secret
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
```

- Redirection du flux de donnée, OpenVPN serra la passerelle par défaut, dés commenter la ligne :

```
push "redirect-gateway def1 bypass-dhcp"
```

- Utilisation du DNS alternatif, ajouter l'adresse du DNS récupéré dans les étapes précédentes :

```
push "dhcp-option DNS 8.8.8.8"
```

- Lancer OpenVPN :

```
root@debianvpn:/home/mrnice# openvpn /etc/openvpn/server.conf
```

```
Sun Nov 26 11:49:23 2017 OpenVPN 2.3.4 i586-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Jun 26 2017
Sun Nov 26 11:49:23 2017 library versions: OpenSSL 1.0.1t  3 May 2016, LZO 2.08
Sun Nov 26 11:49:23 2017 Diffie-Hellman initialized with 2048 bit key
Sun Nov 26 11:49:23 2017 Socket Buffers: R=[163840->131072] S=[163840->131072]
Sun Nov 26 11:49:23 2017 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:95:e6:ec
Sun Nov 26 11:49:23 2017 TUN/TAP device tun0 opened
Sun Nov 26 11:49:23 2017 TUN/TAP TX queue length set to 100
Sun Nov 26 11:49:23 2017 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Sun Nov 26 11:49:23 2017 /sbin/ip link set dev tun0 up mtu 1500
Sun Nov 26 11:49:23 2017 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Sun Nov 26 11:49:23 2017 /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Sun Nov 26 11:49:23 2017 GID set to nogroup
Sun Nov 26 11:49:23 2017 UID set to nobody
Sun Nov 26 11:49:23 2017 UDPv4 link local (bound): [undef]
Sun Nov 26 11:49:23 2017 UDPv4 link remote: [undef]
Sun Nov 26 11:49:23 2017 MULTI: multi_init called, r=256 v=256
Sun Nov 26 11:49:23 2017 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Sun Nov 26 11:49:23 2017 IFCONFIG POOL LIST
Sun Nov 26 11:49:23 2017 Initialization Sequence Completed
```

- Puis vérifier qu'il ouvre bien un point d'accès vers son tunnel tun0 avec un autre terminal :

```
root@debianvpn:/home/mrnice# ifconfig tun0
bash: ifconfig : commande introuvable
root@debianvpn:/home/mrnice# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:10.8.0.1  P-t-P:10.8.0.2  Masque:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 lg file transmission:100
                  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

- L'adresse IP du tunnel tun0 est 10.8.0.1.
- Activation de l'IP forwarding pour la redirection des paquets (le serveur doit router le trafic vers d'autres machines), éditez le fichier /etc/sysctl.conf :

```
root@debianvpn:/home/mrnice# nano /etc/sysctl.conf
```

- Dés commenté la ligne suivante :

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

➤ Vérifier la configuration :

```
root@debianvpn:/home/mrnice# sysctl -p /etc/sysctl.conf  
net.ipv4.ip_forward = 1
```

➤ Configuration du Pare feu, activation du NAT, désinstaller le service ipmitool si il est installé :

```
root@debianvpn:/home/mrnice# apt remove ipmitool  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances  
Lecture des informations d'état... Fait  
Le paquet « ipmitool » n'est pas installé, et ne peut donc être supprimé  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

➤ Installation du service IPtables persistant au cours de l'installation répondre yes pour l'enregistrement des tables ipv4 et ipv6 actuelle :

```
root@debianvpn:/home/mrnice# apt install iptables-persistent
```

### Configuration de iptables-persistent

Les règles actuelles peuvent être enregistrées dans le fichier de configuration « /etc/iptables/rules.v4 ». Ces règles seront chargées au prochain redémarrage de la machine.

Les règles ne sont enregistrées automatiquement que lors de l'installation du paquet. Veuillez consulter la page de manuel de iptables-save(8) pour connaître la manière de garder à jour le fichier des règles.

Faut-il enregistrer les règles IPv4 actuelles ?

<Oui>

<Non>

### Configuration de iptables-persistent

Les règles actuelles peuvent être enregistrées dans le fichier de configuration « /etc/iptables/rules.v6 ». Ces règles seront chargées au prochain redémarrage de la machine.

Les règles ne sont enregistrées automatiquement que lors de l'installation du paquet. Veuillez consulter la page de manuel de ip6tables-save(8) pour connaître la manière de garder à jour le fichier des règles.

Faut-il enregistrer les règles IPv6 actuelles ?

<Oui>

<Non>

➤ Ajout des règles IPtables suivantes et sauvegarde pour le prochain redémarrage :

```
root@debianvpn:/home/mrnice# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@debianvpn:/home/mrnice# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

```
root@debianvpn:/home/mrnice# /etc/init.d/netfilter-persistent save
[....] Saving netfilter rules...run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
done.
```

➤ Vérifier les tables de routage :

```
root@debianvpn:/etc/openvpn/easy-rsa# route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0          192.168.248.254 0.0.0.0         UG        0      0        0 eth0
10.8.0.0          10.8.0.2       255.255.255.0   UG        0      0        0 tun0
10.8.0.2          0.0.0.0       255.255.255.255 UH        0      0        0 tun0
172.16.20.0       0.0.0.0       255.255.255.0   U        0      0        0 eth1
192.168.248.0     0.0.0.0       255.255.255.0   U        0      0        0 eth0
```



## CHAP.8 Création des certificats client.

➤ Créez des certificats client sur le serveur openVPN. Allez dans le dossier suivant :

```
root@debianvpn:/home/mrnice# cd /etc/openvpn/easy-rsa/
```

➤ Tapez les commandes suivantes pour générer les certificats et clés client :

```
root@debianvpn:/etc/openvpn/easy-rsa# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/
keys
root@debianvpn:/etc/openvpn/easy-rsa# ./build-key monlaptopcert
```

## ➤ Personnalisation des paramètres des certificats client, laissez-les par défauts :

```
Country Name (2 letter code) [US]: 
State or Province Name (full name) [CA]: 
Locality Name (eg, city) [SanFrancisco]: 
Organization Name (eg, company) [Fort-Funston]: 
Organizational Unit Name (eg, section) [MyOrganizationalUnit]: 
Common Name (eg, your name or your server's hostname) [monlaptopcert]: 
Name [EasyRSA]: 
Email Address [me@myhost.mydomain]: 

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'CA'
localityName         :PRINTABLE:'SanFrancisco'
organizationName    :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName           :PRINTABLE:'monlaptopcert'
name                 :PRINTABLE:'EasyRSA'
```

```
emailAddress      :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Dec 1 13:18:24 2027 GMT (3650 days)
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

➤ Après la création vérifier que les certificats soient bien créés et qu'ils soient lisibles que par l'utilisateur root, taper la commande suivante :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/
```

```
-rw-r--r-- 1 root root 5641 déc. 3 14:18 monlaptopcert.crt  
-rw-r--r-- 1 root root 1110 déc. 3 14:18 monlaptopcert.csr  
-rw----- 1 root root 1704 déc. 3 14:18 monlaptopcert.key
```

➤ Liste final :

```
root@debianvpn:/etc/openvpn/easy-rsa# ls -la keys/  
total 92  
drwx----- 2 root root 4096 déc. 3 14:18 .  
drwxr-xr-x 3 root root 4096 nov. 12 17:19 ..  
-rw-r--r-- 1 root root 5736 nov. 12 18:51 01.pem  
-rw-r--r-- 1 root root 5641 déc. 3 14:18 02.pem  
-rw-r--r-- 1 root root 1818 nov. 12 18:05 ca.crt  
-rw----- 1 root root 1704 nov. 12 18:05 ca.key  
-rw-r--r-- 1 root root 424 nov. 12 18:37 dh2048.pem  
-rw-r--r-- 1 root root 308 déc. 3 14:18 index.txt  
-rw-r--r-- 1 root root 21 déc. 3 14:18 index.txt.attr  
-rw-r--r-- 1 root root 21 nov. 12 18:51 index.txt.attr.old  
-rw-r--r-- 1 root root 152 nov. 12 18:51 index.txt.old  
-rw-r--r-- 1 root root 5641 déc. 3 14:18 monlaptopcert.crt  
-rw-r--r-- 1 root root 1110 déc. 3 14:18 monlaptopcert.csr  
-rw----- 1 root root 1704 déc. 3 14:18 monlaptopcert.key  
-rw-r--r-- 1 root root 3 déc. 3 14:18 serial  
-rw-r--r-- 1 root root 3 nov. 12 18:51 serial.old  
-rw-r--r-- 1 root root 5736 nov. 12 18:51 srvcert.crt  
-rw-r--r-- 1 root root 1102 nov. 12 18:51 srvcert.csr  
-rw----- 1 root root 1704 nov. 12 18:51 srvcert.key
```

➤ Pour la suite installer PROFTPD sur votre serveur :

```
root@debian:/home/mrnice# apt-get install proftpd
```

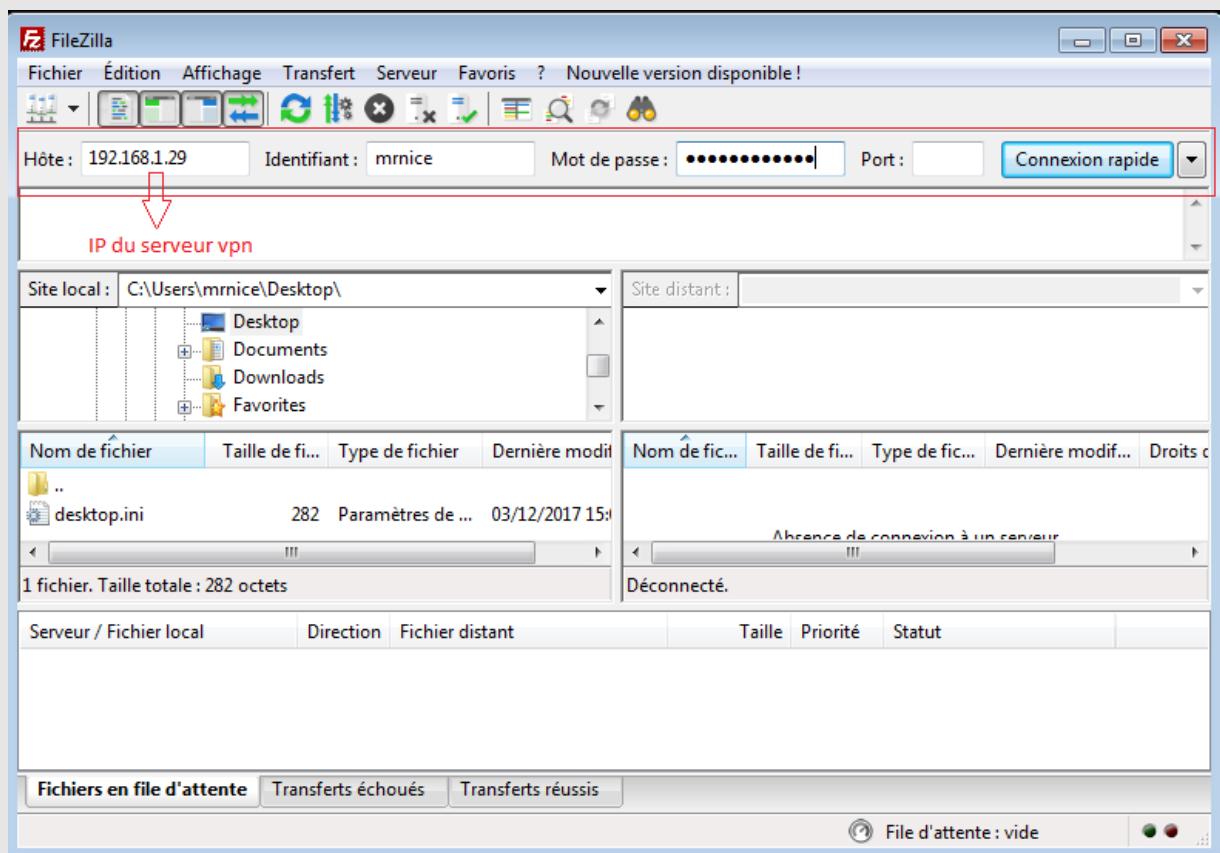


## CHAP.9 Configuration d'openVPN client sous Windows.

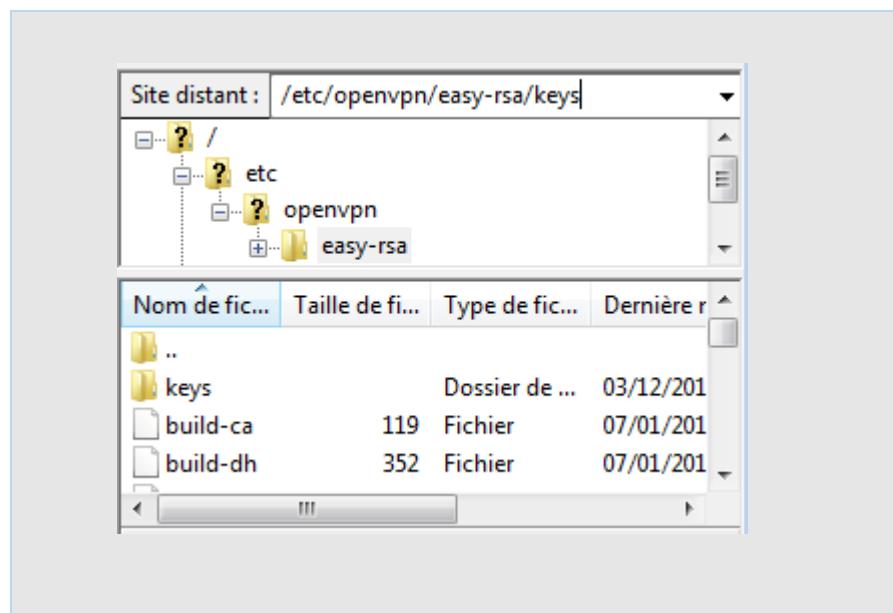
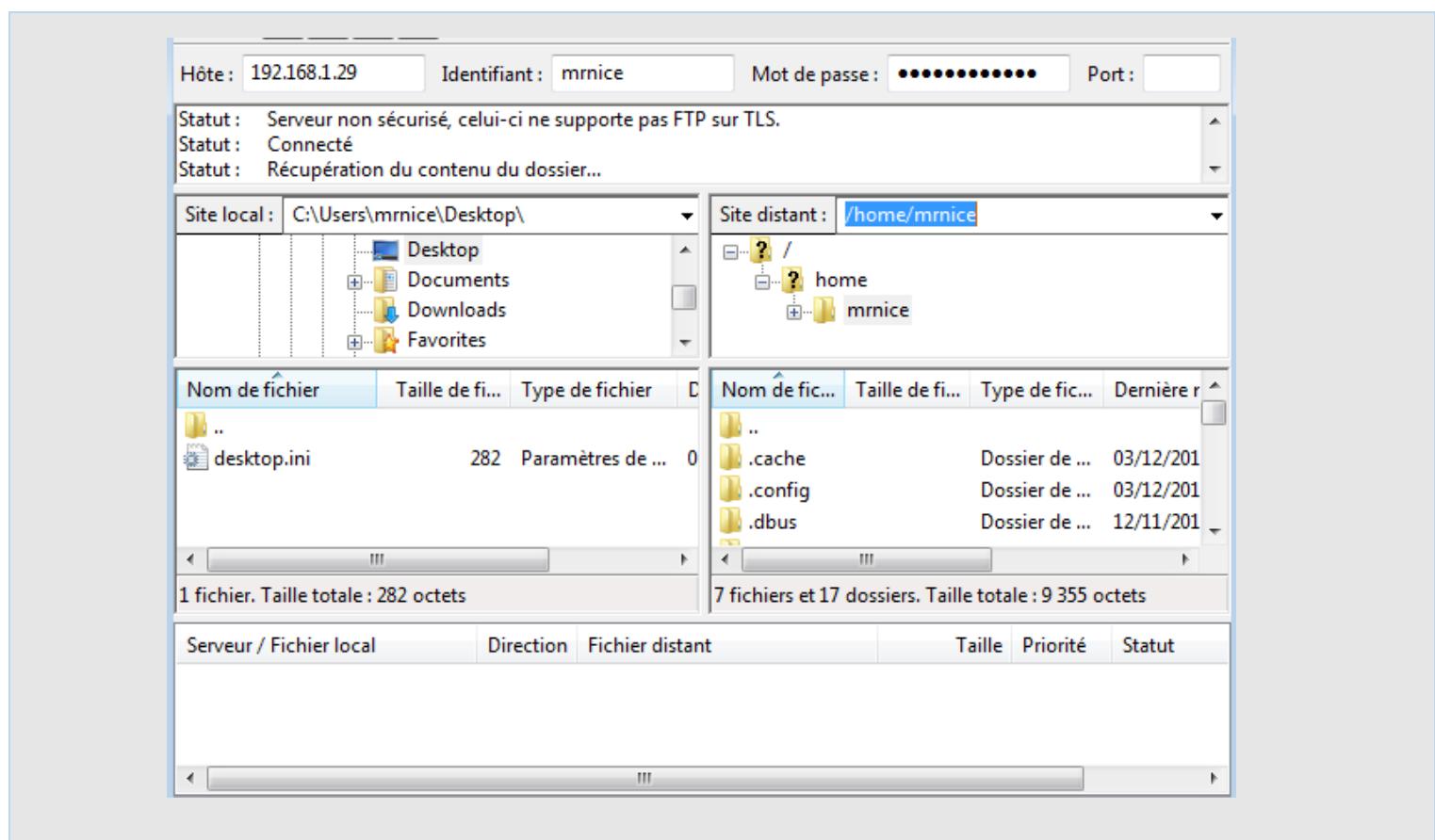
- Installer Filezilla sur le client :

<https://filezilla-project.org/>

- Lancer Filezilla et connectez-vous au serveur openVPN :



- Une fois connecté aller dans le dossier /etc/openvpn/easy-rsa/keys :



➤ Le message d'erreur suivant doit apparaître car il faut modifier les droits du dossier Keys sur le serveur openVPN :

Erreurs : Impossible de récupérer le contenu du dossier

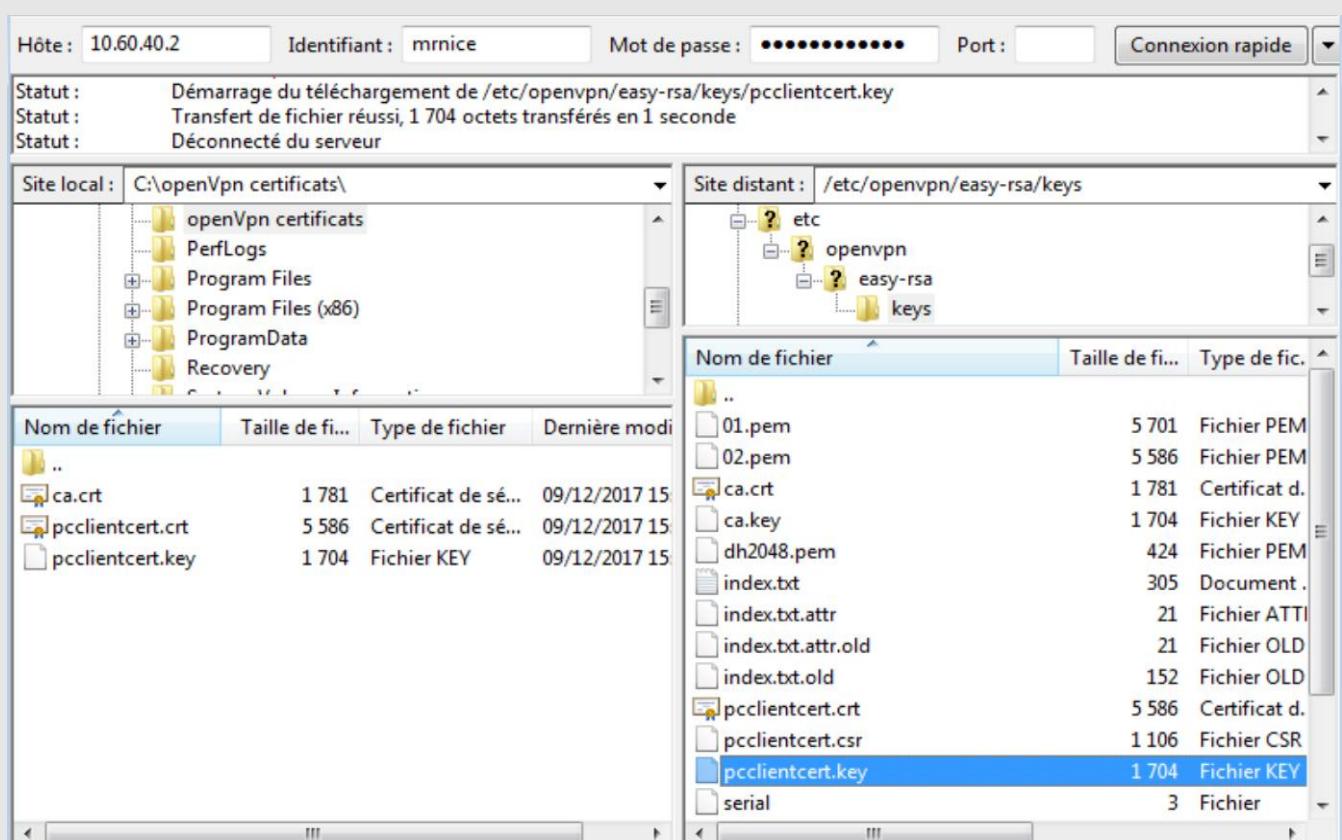
➤ Sur le serveur open VPN aller dans le dossier suivant :

```
root@debianvpn:/home/mrnice# cd /etc/openvpn/easy-rsa
```

➤ Ajouter le droit en exécution du dossier et sous-dossiers keys :

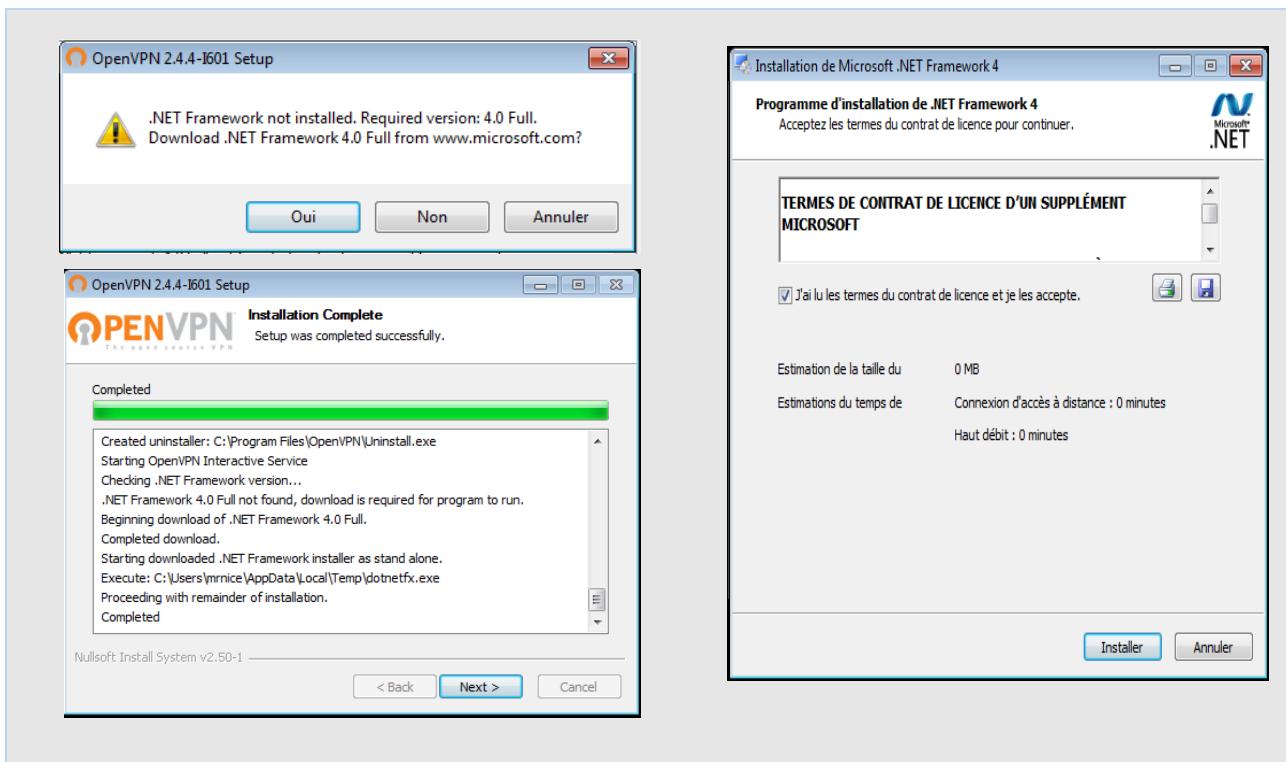
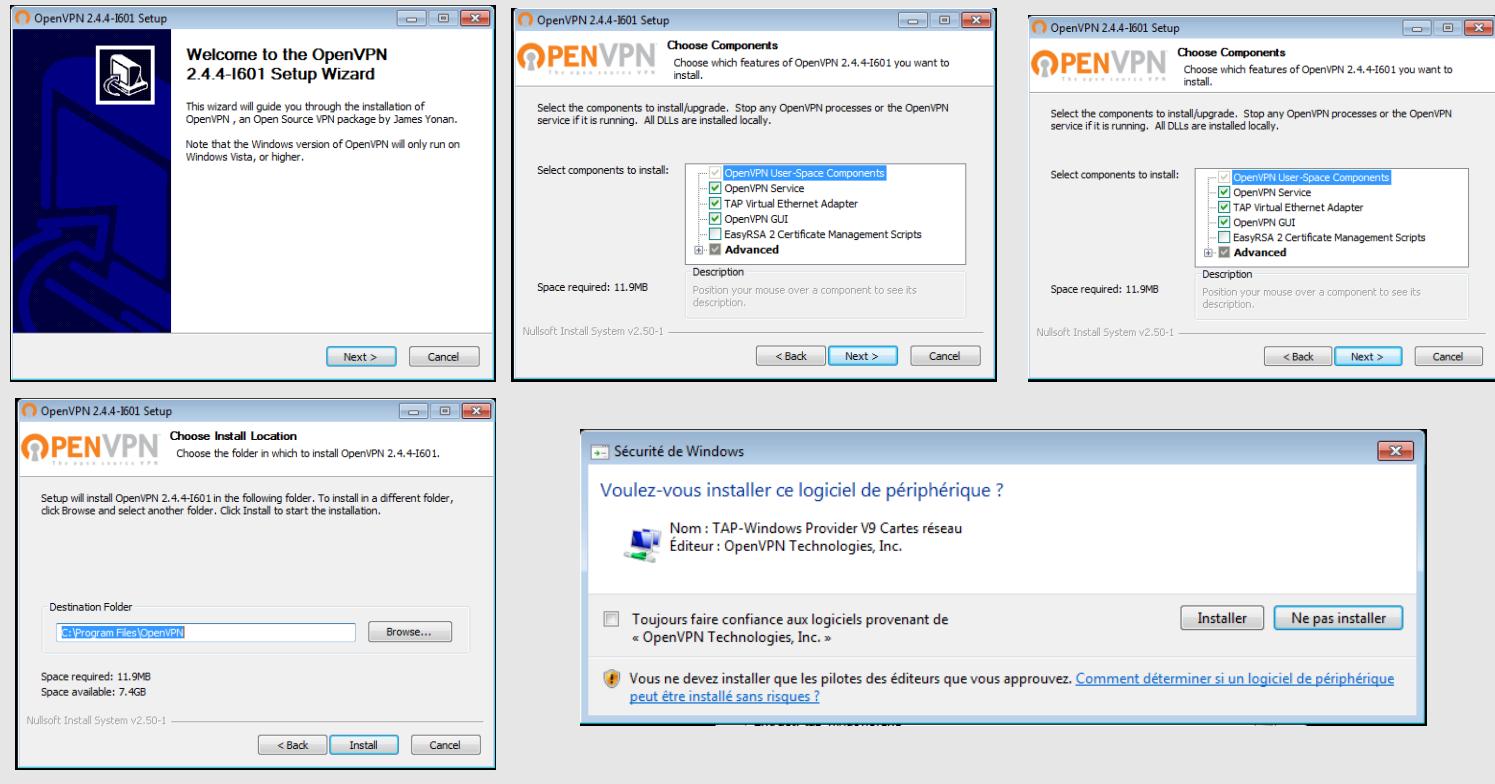
```
root@debianvpn:/home/mrnice# chmod -R 775 /etc/openvpn/easy-rsa/keys/
```

➤ Transférer les certificats suivant sur le client Windows :

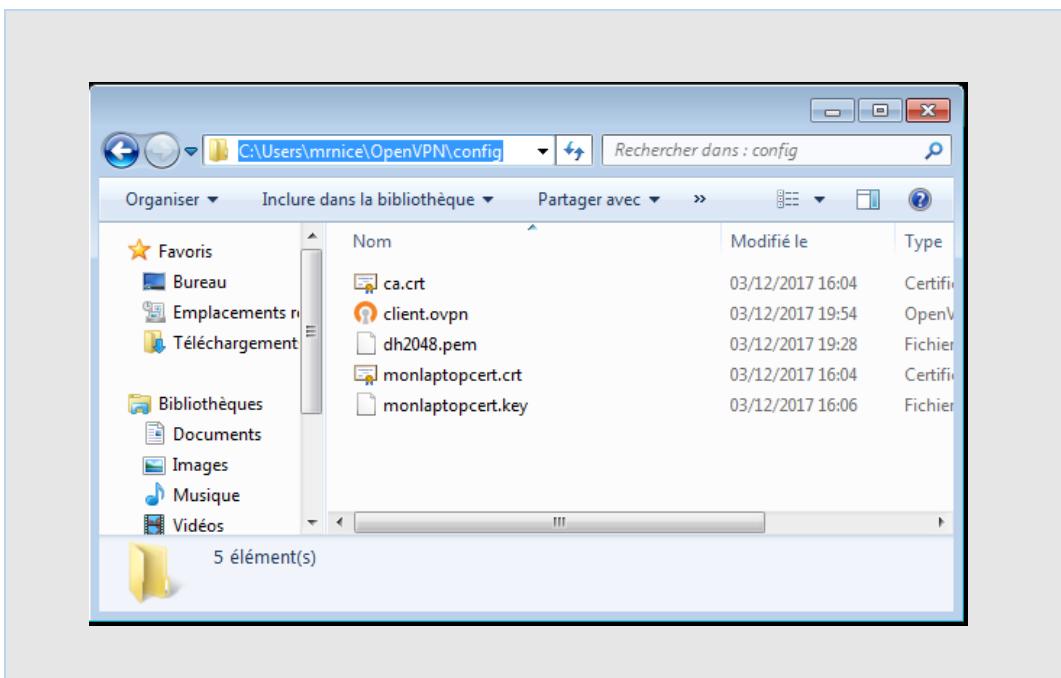


## ➤ Installer par default openVPN sur le client Windows :

<https://openvpn.net/index.php/open-source/downloads.html>



- Configurer openVPN, une fois installé ajouter les certificats et clés récupéré dans les étapes précédentes les ajouter dans le dossier suivant C:\Utilisateur\nom-de-l'utilisateur\openvpn\config :



- Télécharger et installer Notepad ++ par default :

<https://notepad-plus-plus.org/fr/>

**Installer Language**

Please select a language.

French

OK Cancel

**Installation de Notepad++ v7.5.2**

Bienvenue dans le programme d'installation de Notepad++ v7.5.2

Vous êtes sur le point d'installer Notepad++ v7.5.2 sur votre ordinateur.

Avant de démarrer l'installation, il est recommandé de fermer toutes les autres applications. Cela permettra la mise à jour de certains fichiers système sans redémarrer votre ordinateur.

Cliquez sur Suivant pour continuer.

Suivant > Annuler

**Installation de Notepad++ v7.5.2**

Licence utilisateur

Veuillez examiner les termes de la licence avant d'installer Notepad++ v7.5.2.

Appuyez sur Page Suivante pour lire le reste de la licence utilisateur.

COPYING -- Describes the terms under which Notepad++ is distributed. A copy of the GNU GPL is appended to this file.

IMPORTANT NOTEPAD++ LICENSE TERMS

Copyright (C)2016 Don HO <don.h@free.fr>. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2 with the clarifications and exceptions described below. This guarantees your right to use, modify, and redistribute this software under certain conditions.

Si vous acceptez les conditions de la licence utilisateur, cliquez sur J'accepte pour continuer. Vous devez accepter la licence utilisateur afin d'installer Notepad++ v7.5.2.

Je code donc je suis —

< Précédent J'accepte Annuler

**Choisissez le dossier d'installation**

Choisissez le dossier dans lequel installer Notepad++ v7.5.2.

Ceci installera Notepad++ v7.5.2 dans le dossier suivant. Pour installer dans un autre dossier, cliquez sur Parcourir et choisissez un autre dossier. Cliquez sur Suivant pour continuer.

Dossier d'installation

C:\Program Files (x86)\Notepad++ Parcourir...

Espace requis : 11.0Mo Espace disponible : 6.8Go

Je code donc je suis —

< Précédent Suivant > Annuler

**Installation de Notepad++ v7.5.2**

Choisissez les composants

Choisissez les composants de Notepad++ v7.5.2 que vous souhaitez installer.

Cochez les composants que vous désirez installer et décochez ceux que vous ne désirez pas installer. Cliquez sur Suivant pour continuer.

Type d'installation :

Ou, sélectionnez les composants optionnels que vous voulez installer :

Personnalisée

- Localization
- Auto-completion Files
- Themes
- Context Menu Entry
- Plugins
- Auto-Updater

Description

Passez le curseur de votre souris sur un composant pour en voir la description.

Espace requis : 6.6Mo

Je code donc je suis —

< Précédent Suivant > Annuler

**Choisissez les composants**

Choisissez les composants de Notepad++ v7.5.2 que vous souhaitez installer.

Don't use %APPDATA%  
Enable this option to make Notepad++ load/write the configuration files from/to its install directory. Check it if you use Notepad++ in a USB device.

Allow plugins to be loaded from %APPDATA%\notepad++\plugins  
It could cause a security issue. Turn it on if you know what you are doing.

Create Shortcut on Desktop

Je code donc je suis —

< Précédent Installer Annuler

**Fin de l'installation de Notepad++ v7.5.2**

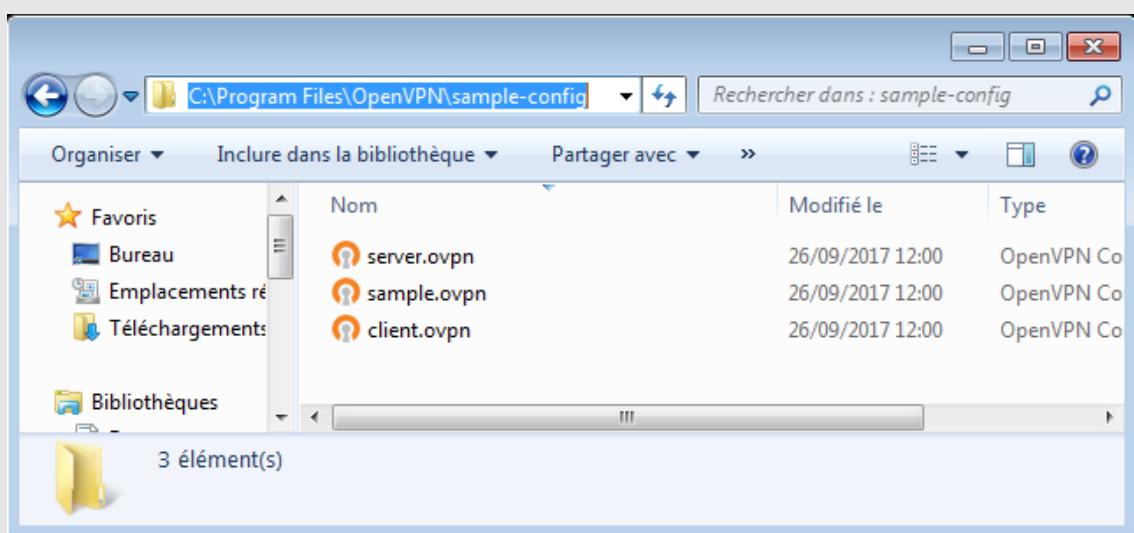
Notepad++ v7.5.2 a été installé sur votre ordinateur.

Cliquez sur Fermer pour quitter le programme d'installation.

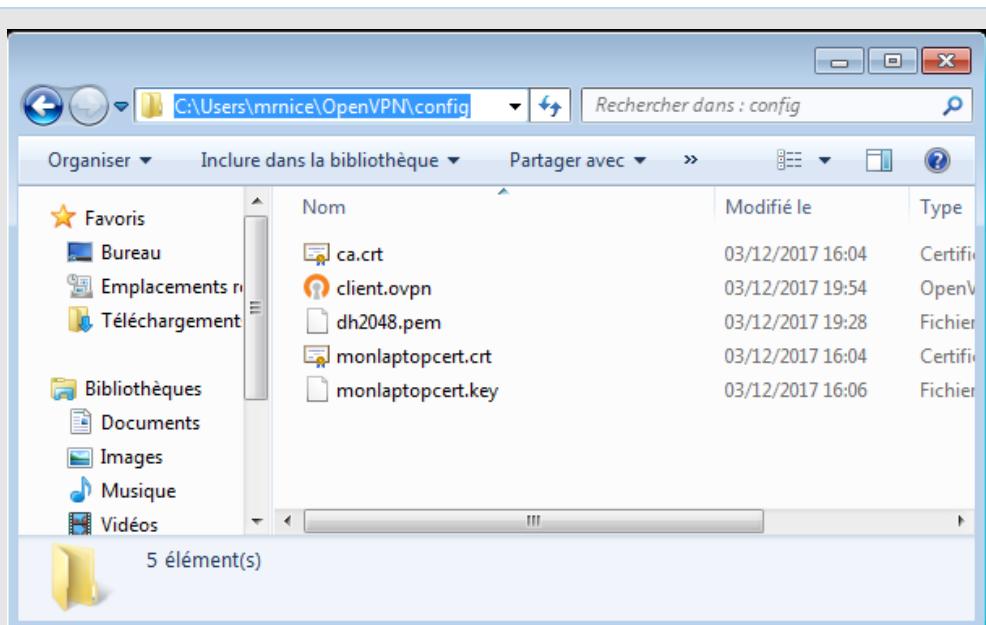
Lancer Notepad++ v7.5.2

< Précédent Fermer Annuler

- Une fois installée, allez dans le dossier C:\Program Files\OpenVPN\sample-config, copiez le fichier client.ovpn :



- Puis ajouter le dans le dossier C:\Utilisateur\nom-de-l'utilisateur\openvpn\config l'en renomment conf.ovpn :



- Edition du fichier conf.ovpn, l'ouvrir avec Textpad :

C:\Program Files\OpenVPN\config\conf.ovpn - Notepad++

Fichier Édition Recherche Affichage Encodage Langage Paramétrage  
Outils Macro Exécution Compléments Documents ? X

conf.ovpn x

```
1 #####  
2 # Sample client-side OpenVPN 2.0 config file #  
3 # for connecting to multi-client server. #  
4 #  
5 # This configuration can be used by multiple #  
6 # clients, however each client should have #  
7 # its own cert and key files. #  
8 #  
9 # On Windows, you might want to rename this #  
10 # file so it has a .ovpn extension #  
11 #####  
12  
13 # Specify that we are a client and that we  
14 # will be pulling certain config file directives  
15 # from the server.  
16 client  
17  
18 # Use the same setting as you are using on  
19 # the server.  
20 # On most systems, the VPN will not function  
21 # unless you partially or fully disable  
22 # the firewall for the TUN/TAP interface.  
23 ;dev tap  
24 dev tun  
25
```

Ln:1 Col:1 Sel:0|0 Unix (LF) UTF-8 INS

➤ Modifier ou dés commenter les lignes suivante :

```
client
;dev tap
dev tun
;dev-node MyTap
proto tcp
;proto udp
remote 192.168.248.26 1194
;remote my-server-2 1194
;remote-random
resolv-retry infinite
nobind
user nobody
group nobody
persist-key
persist-tun
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
ca ca.crt
cert monlaptopcert.crt
key monlaptopcert.key
remote-cert-tls server
auth-nocache
;cipher AES-256-CBC
comp-lzo
verb 3
;mute 20
```



CHAP.9 BIS Configuration du d'openVPN client sous Debian

8.

➤ Installer OpenVPN :

```
root@debian:/home/mrnice# apt-get install openvpn
```

➤ Installer FileZilla :

```
root@debian:/etc/openvpn# apt-get install filezilla
```

- Copier le fichier de configuration dans /etc/openvpn :

```
root@debian:/home/mrnice# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

- Créer un dossier Keys dans /etc/openvpn :

```
root@debian:/home/mrnice# cd /etc/openvpn/  
root@debian:/etc/openvpn#  
root@debian:/etc/openvpn# mkdir -p Keys
```

- Créer de nouveaux certificats clients sur le serveur OpenVPN comme dans les étapes précédentes sauf nommer les bernardcert.

- Récupérer les certificats et clés avec FileZilla comme dans les étapes de configuration du client Windows et les ajouter dans le dossier /etc/openvpn/Keys :

```
root@debian:/etc/openvpn# cd keys/  
root@debian:/etc/openvpn/keys# ls -l  
total 16  
-rw-r--r-- 1 root root 5628 déc. 14 10:37 bernardcert.crt  
-rw-r--r-- 1 root root 1708 déc. 14 10:37 bernardcert.key  
-rw-r--r-- 1 root root 1818 déc. 14 10:37 ca.crt
```

- Editer le fichier client.conf ayant de le modifier en faire un copie et un grep :

```
root@debian:/etc/openvpn# cp client.conf client.conf.old
```

```
root@debian:/etc/openvpn# grep '^(#|$)' -E -v client.conf.old > client.conf
```

```
client
;dev tap
dev tun
;dev-node MyTap
proto tcp
;proto udp
remote 192.168.248.26 1194
;remote my-server-2 1194
;remote-random
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/bernardcert.crt
key /etc/openvpn/keys/bernardcert.key
;ns-cert-type server
;tls-auth ta.key 1
;cipher x
comp-lzo
verb 3
;mute 20
```



## CHAP.10 Partie Validation.

### Client Windows

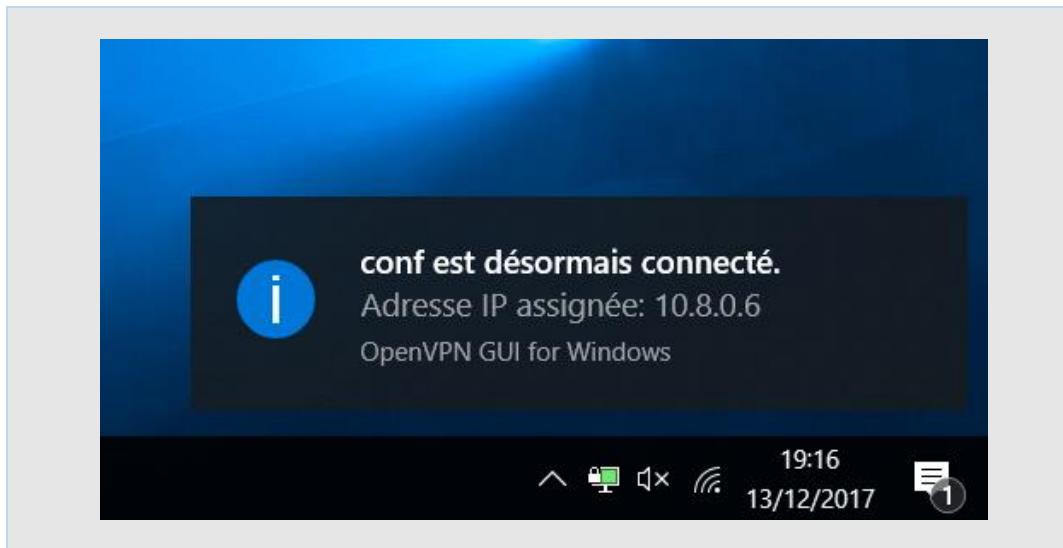
➤ Lancer openVPN et vérifier que le tunnel soit bien établi :



Connexion OpenVPN (conf)

Etat actuel: Connecté

```
Wed Dec 13 19:23:12 2017 TAP-WIN32 device [Ethernet 2] opened: \\.\Global\{30CB7E07-4251-4EDB-9764-8D19CEC9ECA8}.tap
Wed Dec 13 19:23:12 2017 TAP-Windows Driver Version 9.21
Wed Dec 13 19:23:12 2017 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.6/255.255.255.252 on interface {30CB7E07-4251-4EDB-9764-8D19CEC9ECA8}
Wed Dec 13 19:23:12 2017 Successful ARP Flush on interface [6] {30CB7E07-4251-4EDB-9764-8D19CEC9ECA8}
Wed Dec 13 19:23:12 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Dec 13 19:23:12 2017 MANAGEMENT: >STATE:1513189392,ASSIGN_IP,,10.8.0.6,,
Wed Dec 13 19:23:17 2017 TEST ROUTES: 2/2 succeeded len=1 ret=1 a=0 u/d=up
Wed Dec 13 19:23:17 2017 C:\WINDOWS\system32\route.exe ADD 192.168.1.26 MASK 255.255.255.255 192.168.1.1 IF 7
Wed Dec 13 19:23:17 2017 Route addition via service succeeded
Wed Dec 13 19:23:17 2017 C:\WINDOWS\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.8.0.5
Wed Dec 13 19:23:17 2017 Route addition via service succeeded
Wed Dec 13 19:23:17 2017 C:\WINDOWS\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.8.0.5
Wed Dec 13 19:23:17 2017 Route addition via service succeeded
Wed Dec 13 19:23:17 2017 MANAGEMENT: >STATE:1513189397,ADD_ROUTES,....
Wed Dec 13 19:23:17 2017 C:\WINDOWS\system32\route.exe ADD 10.8.0.1 MASK 255.255.255.255 10.8.0.5
Wed Dec 13 19:23:17 2017 Route addition via service succeeded
Wed Dec 13 19:23:17 2017 Initialization Sequence Completed
Wed Dec 13 19:23:17 2017 MANAGEMENT: >STATE:1513189397,CONNECTED,SUCCESS,10.8.0.6,192.168.1.26,1194,192.168.1.17,49757
```



- Une fois le tunnel établi faites un ping du client vers le serveur :

```
Envoi d'une requête 'Ping' 10.8.0.1 avec 32 octets de données :  
Réponse de 10.8.0.1 : octets=32 temps<1ms TTL=64  
Réponse de 10.8.0.1 : octets=32 temps<1ms TTL=64  
Réponse de 10.8.0.1 : octets=32 temps<1ms TTL=64  
Réponse de 10.8.0.1 : octets=32 temps<1ms TTL=64
```

- Puis faites un ping du serveur vers le client :

```
root@debianvpn:/home/mrnice# ping 10.8.0.6  
PING 10.8.0.6 (10.8.0.6) 56(84) bytes of data.  
64 bytes from 10.8.0.6: icmp_seq=1 ttl=128 time=0.474 ms  
64 bytes from 10.8.0.6: icmp_seq=2 ttl=128 time=0.450 ms  
64 bytes from 10.8.0.6: icmp_seq=3 ttl=128 time=0.519 ms  
...
```

## Client Debian 8

➤ Lancer OpenVPN :

```
root@debian:/etc/openvpn/keys# openvpn /etc/openvpn/client.conf
```

```
Fri Dec 15 00:22:50 2017 /sbin/ip route add 172.16.20.0/24 via 10.8.0.9
RTNETLINK answers: File exists
Fri Dec 15 00:22:50 2017 ERROR: Linux route add command failed: external program exited with error status: 2
Fri Dec 15 00:22:50 2017 /sbin/ip route add 10.8.0.1/32 via 10.8.0.9
RTNETLINK answers: File exists
Fri Dec 15 00:22:50 2017 ERROR: Linux route add command failed: external program exited with error status: 2
Fri Dec 15 00:22:50 2017 GID set to nogroup
Fri Dec 15 00:22:50 2017 UID set to nobody
Fri Dec 15 00:22:50 2017 Initialization Sequence Completed
```

➤ Une fois le tunnel établi faites un ping du client vers le serveur :

```
root@debian:/etc/openvpn/keys# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.431 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.367 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=0.388 ms
```

➤ Puis faites un ping du serveur vers le client :

```
root@debianvpn:/home/mrnice# ping 10.8.0.10
PING 10.8.0.10 (10.8.0.10) 56(84) bytes of data.
64 bytes from 10.8.0.10: icmp_seq=1 ttl=64 time=0.405 ms
64 bytes from 10.8.0.10: icmp_seq=2 ttl=64 time=0.396 ms
64 bytes from 10.8.0.10: icmp_seq=3 ttl=64 time=0.411 ms
```

## ❖ CHAP.11 Configuration d'un accès au serveur Windows 2008 R2.

- Vérifier que la route pour accéder au serveur Windows 2008 R2 depuis le serveur OpenVPN soit créée :

```
root@debianvpn:/etc/openvpn/easy-rsa# route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask        Indic Metric Ref    Use Iface
0.0.0.0         192.168.248.254 0.0.0.0        UG    0      0        0 eth0
10.8.0.0        10.8.0.2       255.255.255.0   UG    0      0        0 tun0
10.8.0.2        0.0.0.0       255.255.255.255 UH    0      0        0 tun0
172.16.20.0     0.0.0.0       255.255.255.0   U     0      0        0 eth1
192.168.248.0   0.0.0.0       255.255.255.0   U     0      0        0 eth0
```

- Ajouter dans le fichier server.conf la ligne suivante pour que le client Windows accède au serveur Windows 2008 R2 :

```
push "route 172.16.20.0 255.255.255.0"
```

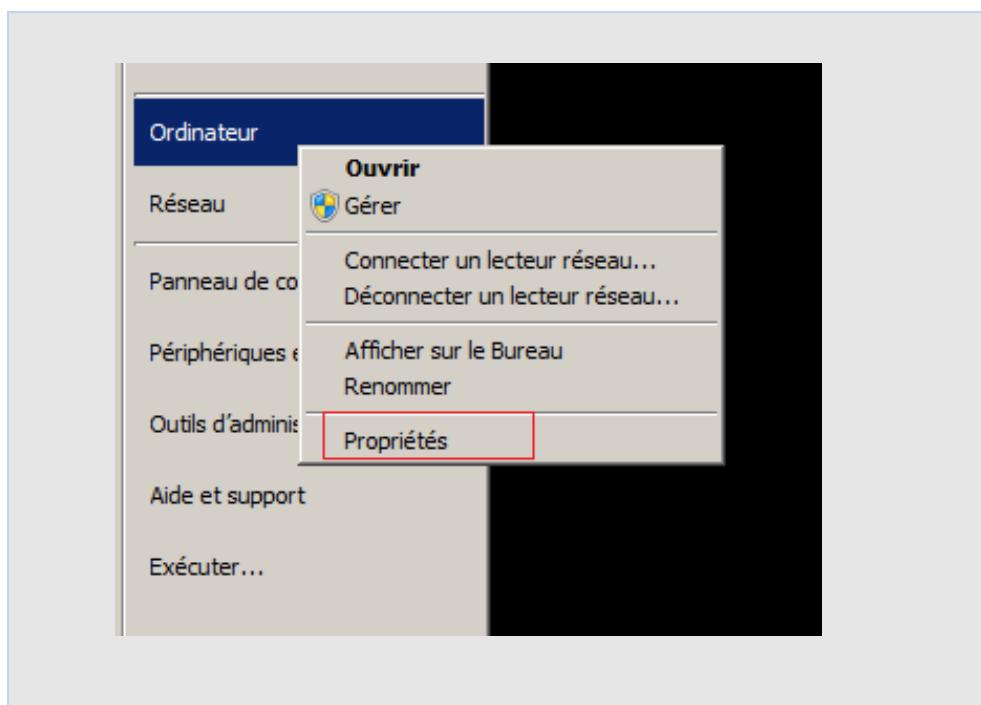
- Faites un ping du client Windows vers le serveur Windows 2008 R2 et faire pareille pour le client Debian 8:

```
C:\Users\Mr Nice Adrar>ping 172.16.20.54
```

```
Envoi d'une requête 'Ping' 172.16.20.54 avec 32 octets de données :  
Réponse de 172.16.20.54 : octets=32 temps=347 ms TTL=127  
Réponse de 172.16.20.54 : octets=32 temps=43 ms TTL=127  
Réponse de 172.16.20.54 : octets=32 temps=12 ms TTL=127
```

```
root@debian:/etc/openvpn/keys# ping 172.16.20.54  
PING 172.16.20.54 (172.16.20.54) 56(84) bytes of data.  
64 bytes from 172.16.20.54: icmp_seq=1 ttl=127 time=0.967 ms  
64 bytes from 172.16.20.54: icmp_seq=2 ttl=127 time=0.687 ms  
64 bytes from 172.16.20.54: icmp_seq=3 ttl=127 time=0.617 ms  
^C
```

➤ Autoriser les connexions au Bureau à distance sur le serveur Windows 2008 R2 :

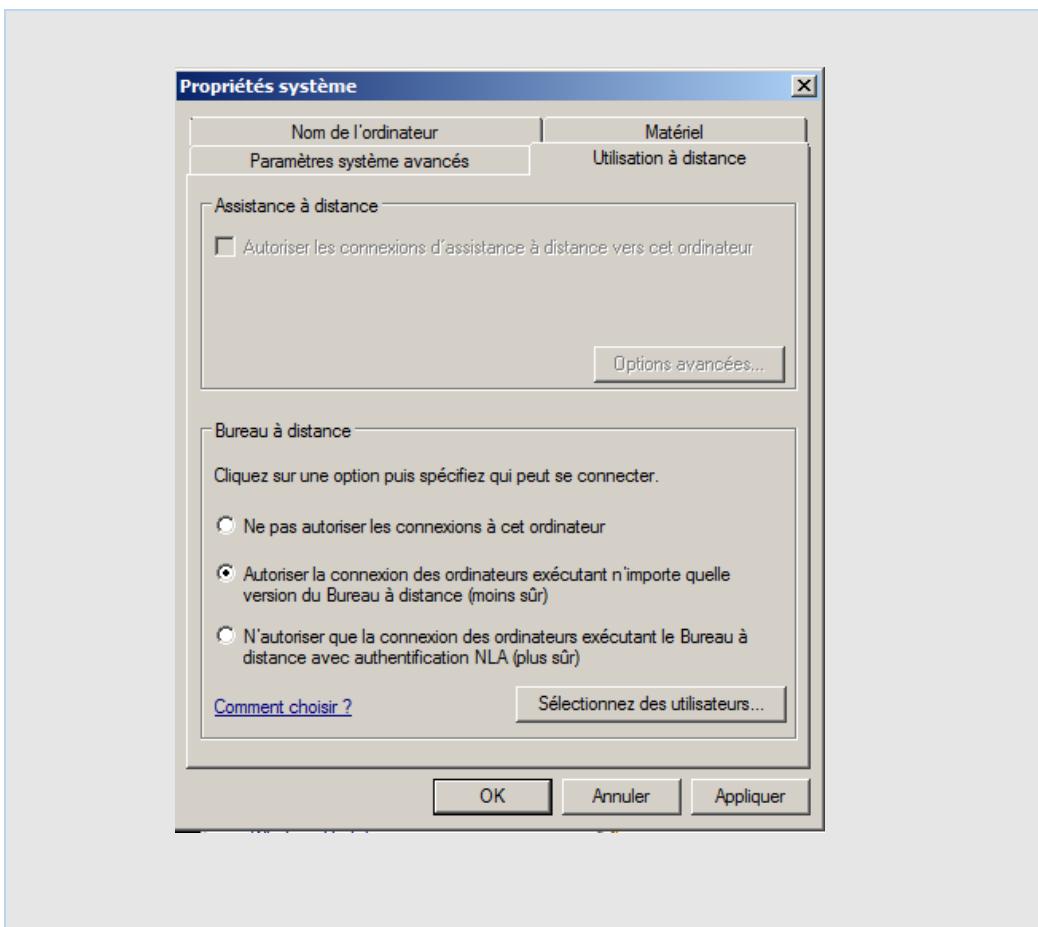


Édition Windows

Windows Server 2008 R2 Entreprise

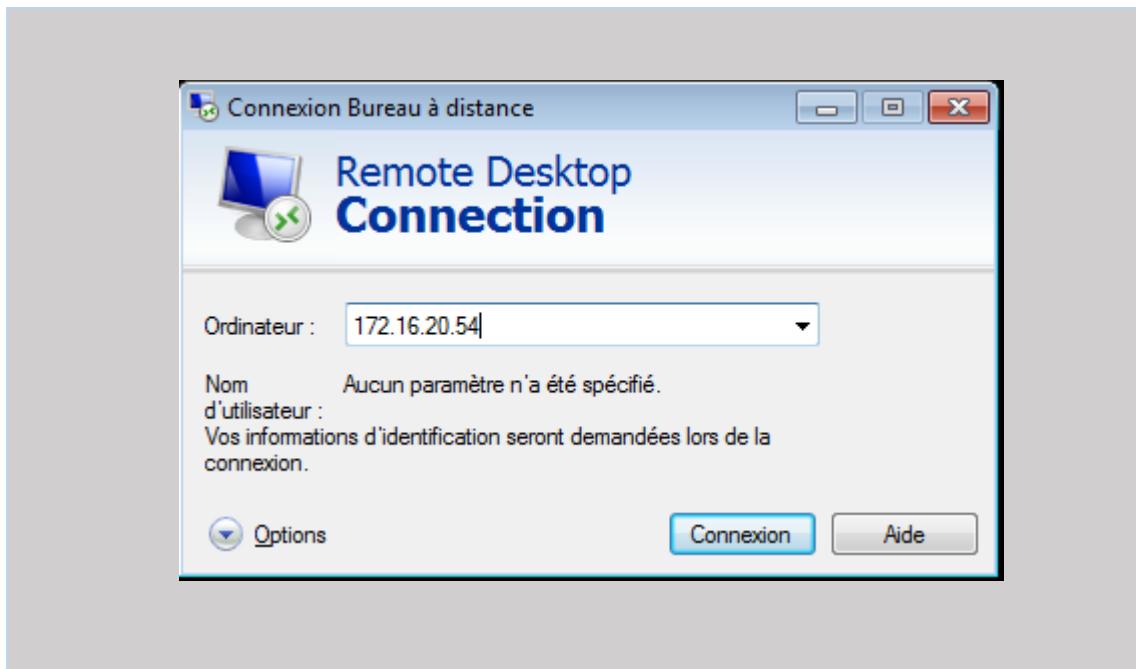
Copyright © 2009 Microsoft Corporation. Tous droits réservés.

Service Pack 1

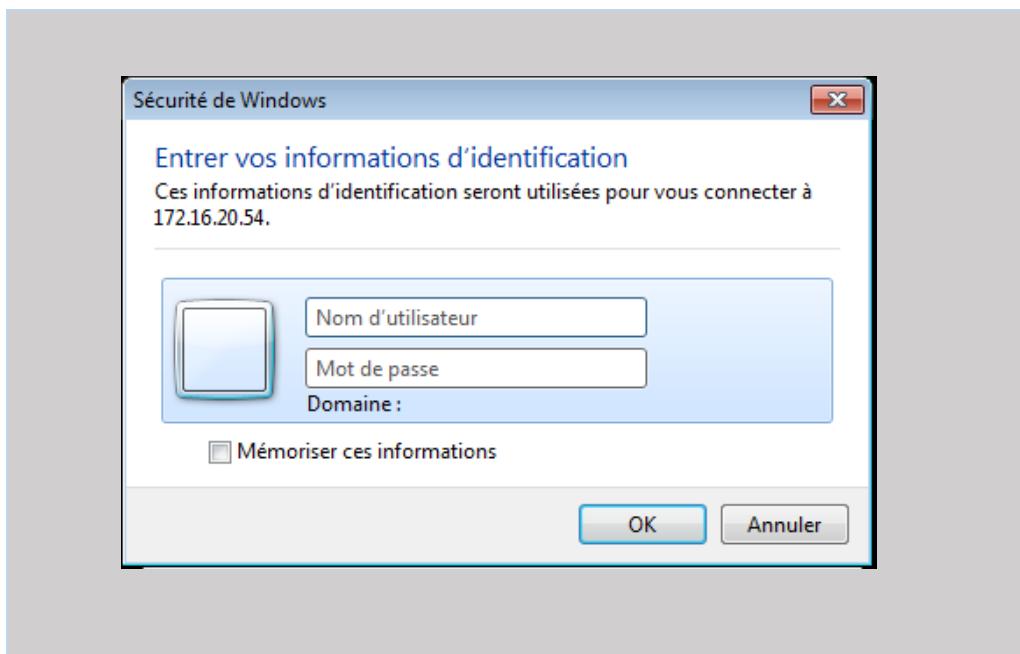


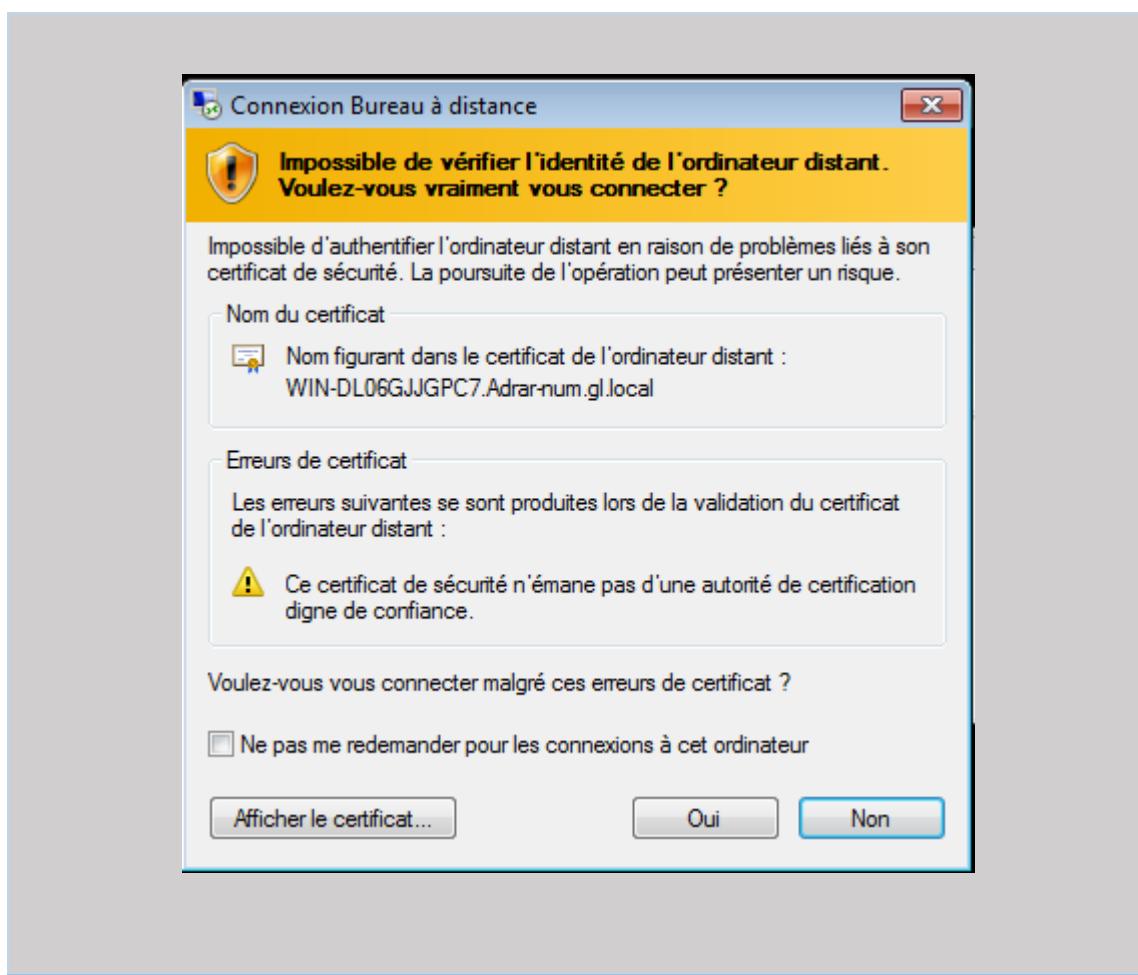
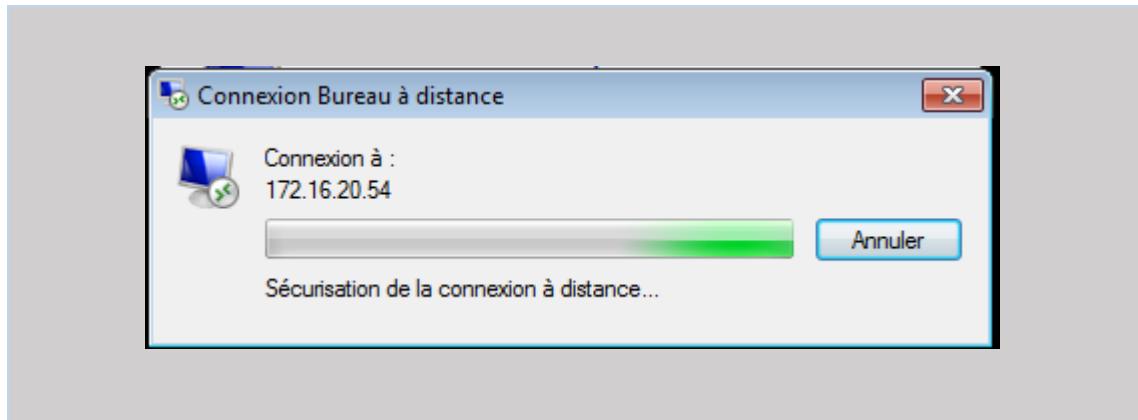
## RDP Client Windows

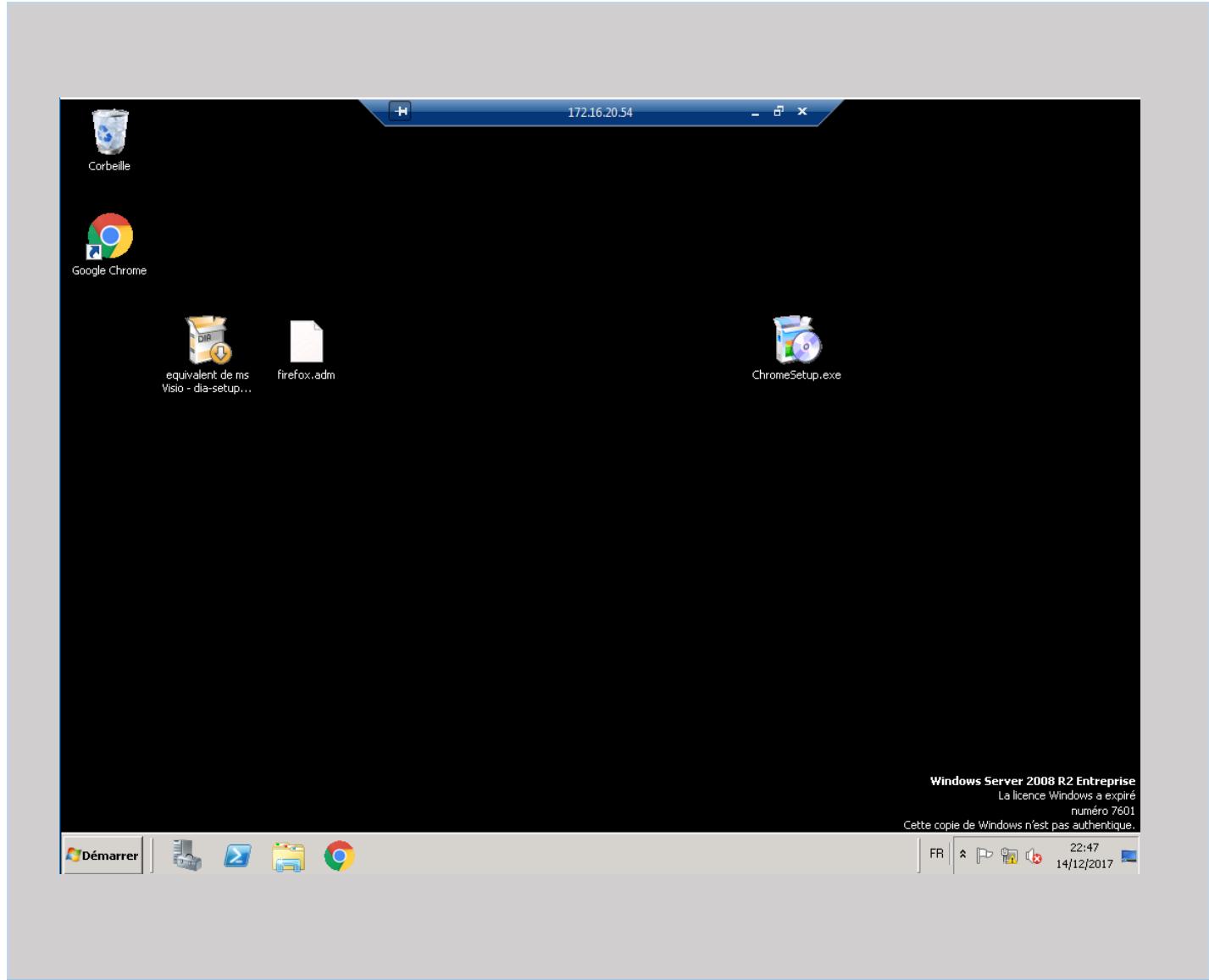
- Depuis le client Windows lancer une connexion bureau à distance sur le serveur 2008 R2 :



- Authentifier vous :

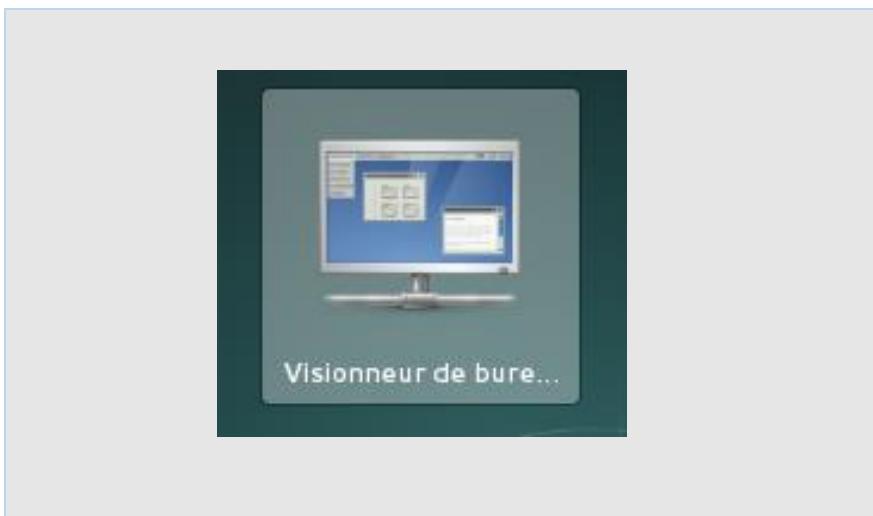






## RDP Debian 8

- Depuis le client Debian 8 lancer une connexion bureau à distance sur le serveur 2008 R2 :



**Se connecter**

**Choisissez un bureau distant auquel se connecter**

Protocole : RDP ▼ Accéder à des bureaux distants MS Windows

Hôte : 172.16.20.54 ▼ Rechercher

**Options de connexion**

Plein écran

**Options RDP**

Nom d'utilisateur : mrnice

Largeur : 800 - +

Hauteur : 600 - +

Aide Annuler Se connecter

This screenshot shows the "Se connecter" (Connect) dialog box for an RDP connection. It includes fields for selecting the protocol (RDP), entering the host IP address (172.16.20.54), and setting connection options like full screen mode and resolution (800x600). At the bottom, there are "Aide" (Help), "Annuler" (Cancel), and "Se connecter" (Connect) buttons.

## ➤ Authentification :

