Le VPN

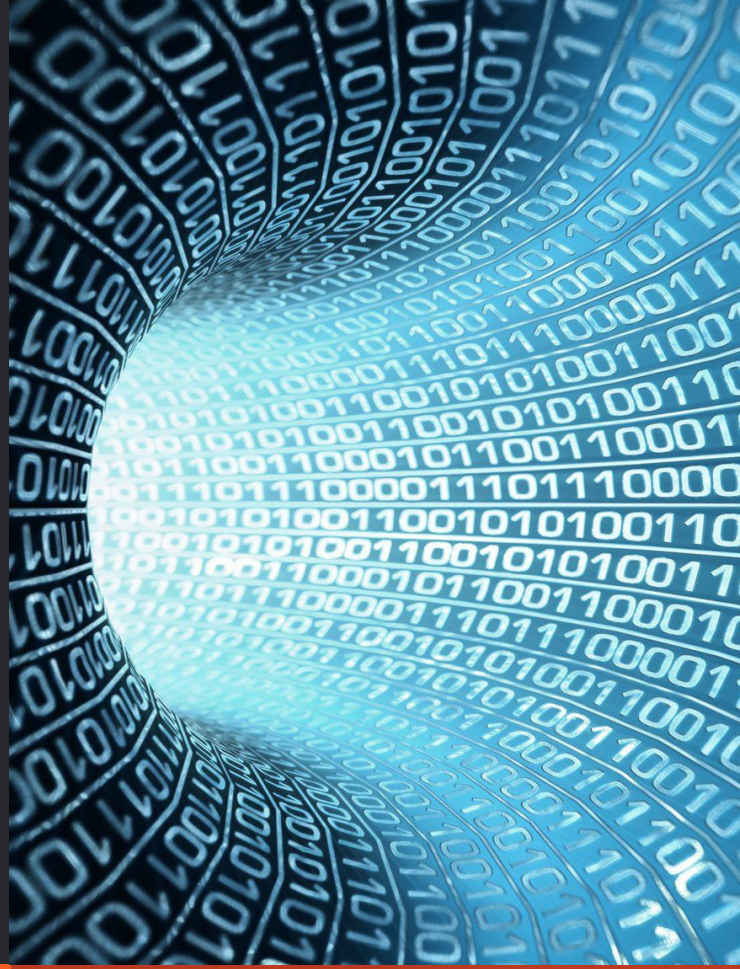
OPENVPN™

Yohan Fresneau

Structure du Plan:

- Présentation du VPN

- Observation du fonctionnement du VPN



1.
Qu’est ce que le VPN ?

Description et utilisation

Qu’est ce que le VPN ?

- VPN = Virtual Private Network, ou réseau Privé Virtuel
- Le VPN sert à créer des réseaux virtuels et sécurisés, permettant de se connecter peu importe l’endroit où l’on se trouve
- Les données passe dans un tunnel sécurisé
- Avec les mêmes fonctionnalitées qu’un réseau local

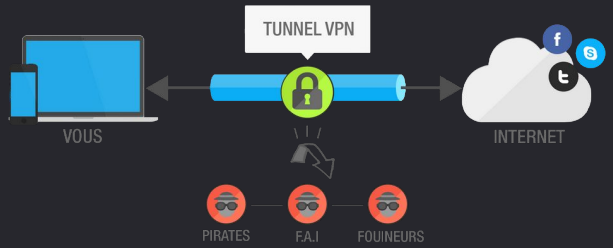
Les différentes utilisations du VPN :

En entreprise :

Permet de relier le personnel / les clients, de rester connectés au réseau de l'entreprise

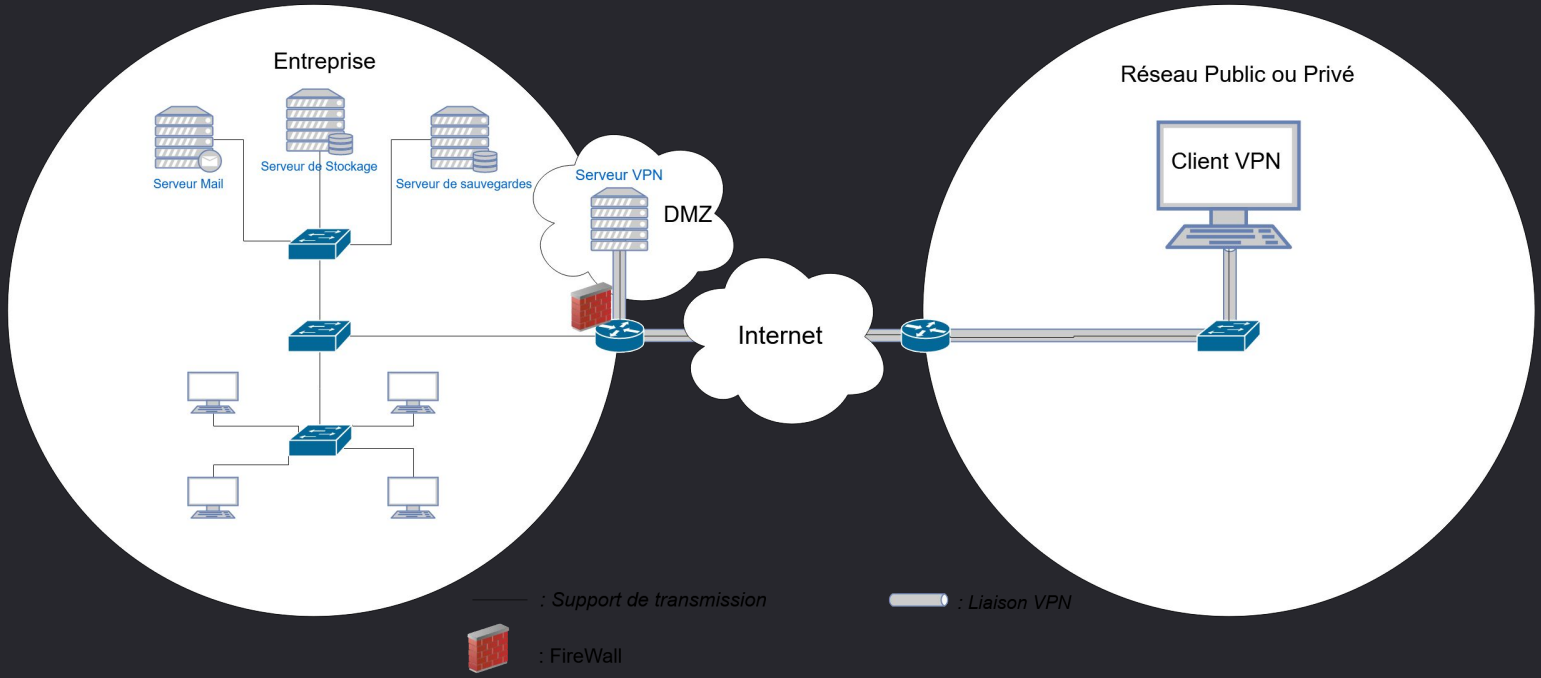
En grand public :

Permet de sécuriser les échanges entre les différents utilisateurs



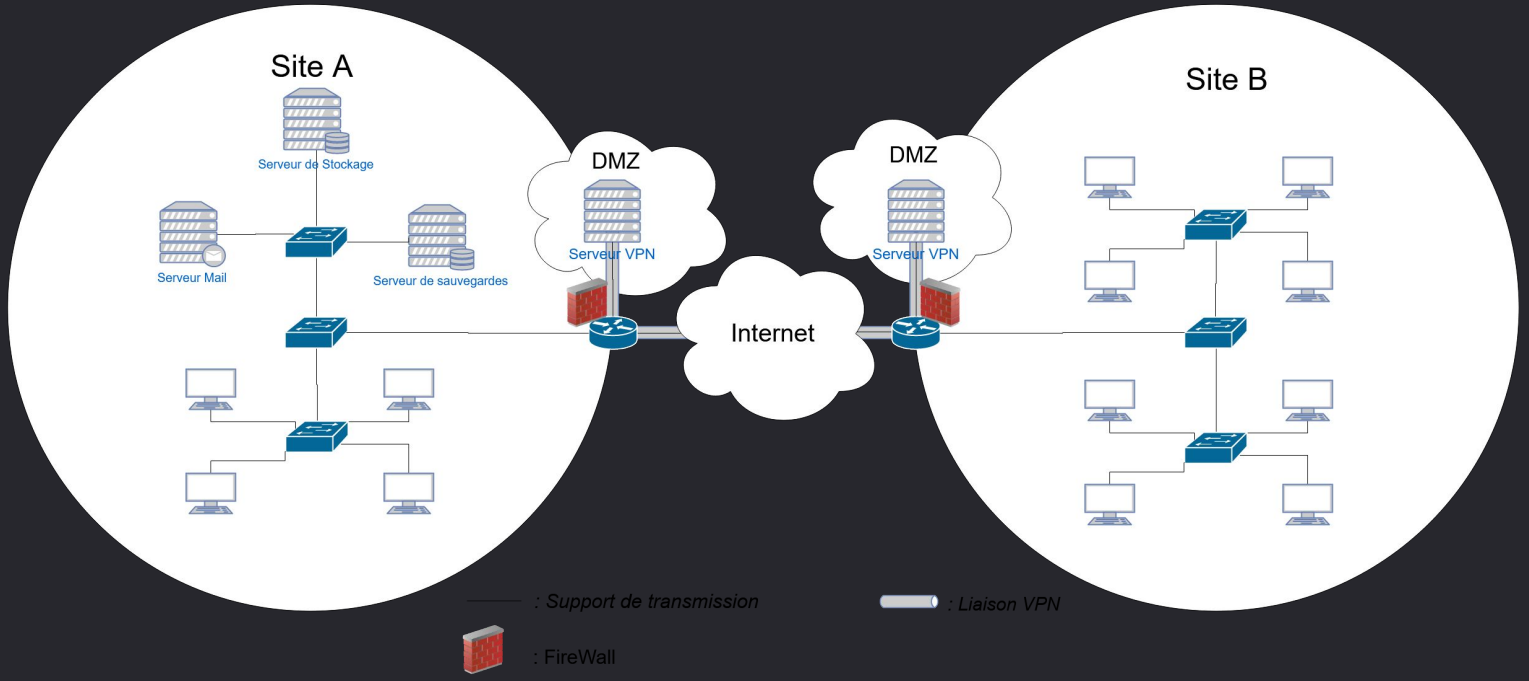
Les deux manières d'utiliser un VPN

Connexion entre un client et un serveur VPN



Les deux manières d'utiliser un VPN

Connexion inter-sites avec 1 serveur VPN par site



Pourquoi utiliser un VPN au lieu d'un autre protocole ?

- Le VPN permet de relier des hôtes à différents lieux géographiques à travers un tunnel chiffré.

- Le VPN permet de faire passer tous les flux à travers ce tunnel chiffré, tandis que le SSH permet de faire passer seulement certains flux.

- Cette différence est dûe à l'intervention du VPN sur la couche 2 du modèle OSI, qui encapsule les données et chiffre le contenu, alors que le SSH intervient sur la couche 3 du modèle OSI.

Quels sont les protocoles utilisés pour les VPN ?

VPN SSL :

VPN SSL est clientless, ne requiert pas de logiciel client, un navigateur internet peut suffire avec des sessions HTTPS SSL/TLS.

VPN IPsec :

Nécessite l'installation d'un agent, pour établir un tunnel vers un serveur VPN, où plusieurs protocoles pourront y être véhiculé (Telnet, SMTP ...).

OpenVPN :

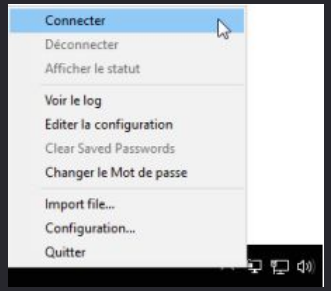
Protocole VPN en open source, qui utilise le protocole SSL pour créer une authentification pour une connexion cryptée.

2.
Resultats attendus des flux VPN

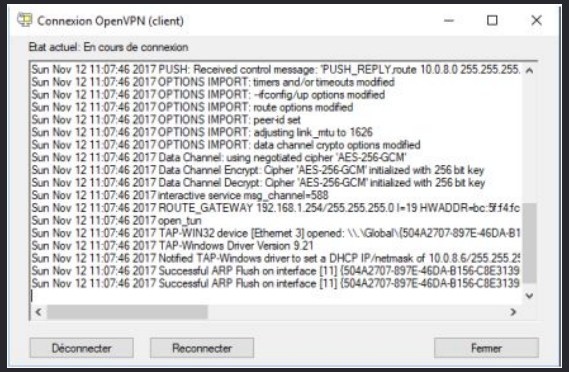
Les attentes du service VPN

Connexion au VPN :

Pour se connecter au VPN, il faut faire clic droit sur l'icône "OpenVPN Gui" dans la barre des tâches, puis cliquez sur "connecter"



Une fenêtre de log va apparaître, avec les informations du client et de la connexion



Connexion au VPN :

Une fois connecté, un message va apparaître et nous informer de votre adresse IP, dans le réseau VPN en 10.0.8.0 /24

Cette icône  signifie que l'on est connecté au VPN

Si cette icône  apparaît, le client essaye de joindre le serveur VPN

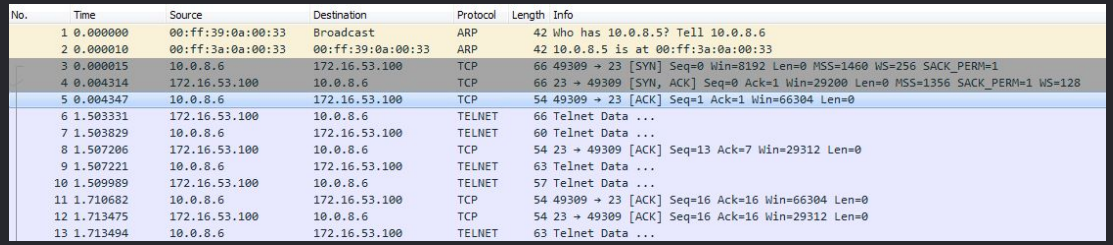
Cette icône  signifie que l'on est pas connecté au serveur VPN

Conclusion :

Si nous pouvons ping les serveurs et les autres clients du réseau de l'entreprise, cela signifie que le VPN est fonctionnel.

Connexion au VPN :

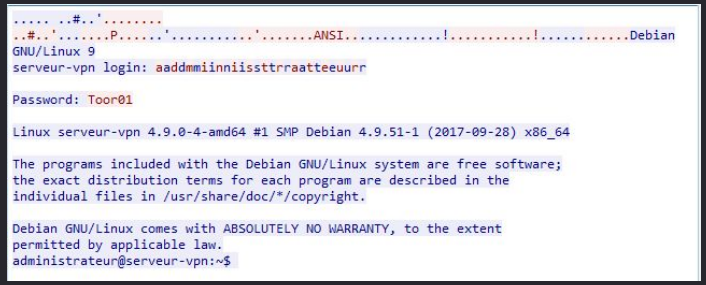
Connectez-vous à votre serveur VPN en telnet et sniffer les cartes réseaux de vos serveurs, voilà ce que nous obtiendront :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:ff:39:0a:00:33	Broadcast	ARP	42	Who has 10.0.8.5? Tell 10.0.8.6
2	0.000010	00:ff:3a:0a:00:33	00:ff:39:0a:00:33	ARP	42	10.0.8.5 is at 00:ff:3a:0a:00:33
3	0.000015	10.0.8.6	172.16.53.100	TCP	66	49309 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.004314	172.16.53.100	10.0.8.6	TCP	66	23 → 49309 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1356 SACK_PERM=1 WS=128
5	0.004347	10.0.8.6	172.16.53.100	TCP	54	49309 → 23 [ACK] Seq=1 Ack=1 Win=66304 Len=0
6	1.503331	172.16.53.100	10.0.8.6	TELNET	66	Telnet Data ...
7	1.503829	10.0.8.6	172.16.53.100	TELNET	60	Telnet Data ...
8	1.507206	172.16.53.100	10.0.8.6	TCP	54	23 → 49309 [ACK] Seq=13 Ack=7 Win=29312 Len=0
9	1.507221	10.0.8.6	172.16.53.100	TELNET	63	Telnet Data ...
10	1.509989	172.16.53.100	10.0.8.6	TELNET	57	Telnet Data ...
11	1.710682	10.0.8.6	172.16.53.100	TCP	54	49309 → 23 [ACK] Seq=16 Ack=16 Win=66304 Len=0
12	1.713475	172.16.53.100	10.0.8.6	TCP	54	23 → 49309 [ACK] Seq=16 Ack=16 Win=29312 Len=0
13	1.713494	10.0.8.6	172.16.53.100	TELNET	63	Telnet Data ...

Flux telnet à destination du serveur OpenVPN

Contenue de l'échange Telnet

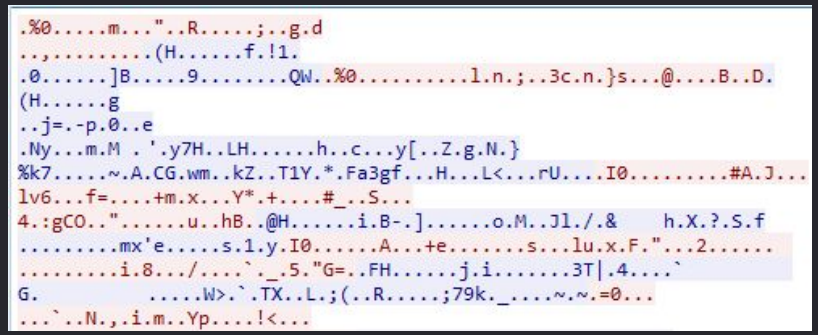


```
..... ..#..'........
..#..'.......P......'...........'.......ANSI.............!...........!............Debian
GNU/Linux 9
serveur-vpn login: aaddmmiinniissttrraatteeuurr

Password: Toor01

Linux serveur-vpn 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) 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.
administrateur@serveur-vpn:~$
```

Analyse des flux :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.65.89.62	192.168.1.1	OpenVPN	93	MessageType: P_DATA_V1
2	0.208485	192.168.1.1	200.65.89.62	TCP	54	49304 → 1194 [ACK] Seq=1 Ack=40 Win=16144 Len=0
3	5.009390	Vmware_45:50:d1	Vmware_51:6e:63	ARP	60	Who has 192.168.1.1? Tell 192.168.1.254
4	5.009410	Vmware_51:6e:63	Vmware_45:50:d1	ARP	42	192.168.1.1 is at 00:0c:29:51:6e:63
5	7.243758	192.168.1.1	200.65.89.62	OpenVPN	96	MessageType: P_DATA_V2
6	7.246929	200.65.89.62	192.168.1.1	TCP	60	1194 → 49304 [ACK] Seq=40 Ack=43 Win=511 Len=0
7	10.436423	200.65.89.62	192.168.1.1	OpenVPN	93	MessageType: P_DATA_V1
8	10.644351	192.168.1.1	200.65.89.62	TCP	54	49304 → 1194 [ACK] Seq=43 Ack=79 Win=16134 Len=0
9	12.033619	Vmware_51:6e:63	Vmware_45:50:d1	ARP	42	Who has 192.168.1.254? Tell 192.168.1.1
10	12.034874	Vmware_45:50:d1	Vmware_51:6e:63	ARP	60	192.168.1.254 is at 00:0c:29:45:50:d1
11	16.853870	192.168.1.1	200.65.89.62	OpenVPN	96	MessageType: P_DATA_V2
12	16.856478	200.65.89.62	192.168.1.1	TCP	60	1194 → 49304 [ACK] Seq=79 Ack=85 Win=511 Len=0
13	19.479770	192.168.1.1	200.65.89.62	OpenVPN	132	MessageType: P_DATA_V2

Flux VPN envoyés sur le réseau



Les échanges telnet dans le tunnel VPN

Merci de votre attention

Si vous avez davantage de questions, n’hésitez pas à les poser