Installation & Configuration d'un Serveur/Client OpenVPN

M.LEGRAND



Table des matières

Introduction :	3
Qu'est ce qu'est le VPN ?	3
Contexte :	3
Configuration du serveur OpenVPN	1
Installation et configuration d'OpenVPN	1
Test de la configuration	7
Installation OpenVpn sur client Windows :	>
Configuration du serveur Web Apache12	2
Pour les restrictions d'accès par adresse IP :13	3
Collecte et analyse des Logs sur le serveur OpenVPN :	5
Accès aux fichiers de log OpenVPN :1	5
Status OpenVpn.Service :	5
WireShark :	3
	3
Conclusion :	>
Annexe :)

Introduction :

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel. Son développement a commencé le 13 mai 2001 grâce à James Yonan.

Qu'est ce qu'est le VPN ?

Un VPN fonctionne en établissant un tunnel chiffré entre le dispositif de l'utilisateur (le client VPN) et un serveur VPN. Ce tunnel sert à encapsuler et à chiffrer les données échangées entre l'utilisateur et le serveur, assurant ainsi leur confidentialité et leur intégrité. Une fois que le client VPN envoie les données au serveur VPN, ce dernier les déchiffre et les transmet au serveur de destination, dans ce cas, un serveur web. De manière symétrique, les données envoyées depuis le serveur web sont reçues par le serveur VPN, qui les chiffre avant de les renvoyer au client VPN. Ce dernier déchiffre les données avant de les traiter. Ce processus garantit que les informations sensibles restent sécurisées même lorsqu'elles traversent des segments de réseau non sécurisés.

Contexte :

L'objectif de ce TP est de vous familiariser avec les principes de base des VPN, les protocoles de sécurisation comme IPSec et OpenVPN, et les meilleures pratiques pour la configuration et la gestion de la sécurité dans les communications réseau. Cette expérience pratique aidera les étudiants à comprendre comment les VPN contribuent à renforcer la sécurité des données et à maintenir la confidentialité des informations transmises sur Internet.



Configuration du serveur OpenVPN

Installation et configuration d'OpenVPN

On va commencer à mettre tous les paquets de Debian à jour et mettre la plus haute version de debian avec les commandes :

root@SRVVPN:~# apt update && apt upgrade

Ensuite, on va installer le service OpenVPN :

root@SRVVPN:~# apt install openvpn

proct@SRVVPN:~# apt installes.prove the answer of a non mis à jour. Il est nécessaire de prendre 2 499 ko dans les archives. Après cette opération, 7 628 ko d'espace disque supplémentaires seront utilisés. Souhaitez-vous continuer 7 [0/n] Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libccid amd64 1.5.2.1 [367 K8] Réception de :1 http://deb.debian.org/debian bookworm/main amd64 prescd amd64 1.9.9-2 [89,7 K8] Réception de :1 http://deb.debian.org/debian bookworm/main amd64 perscd amd64 1.9.9-2 [89,7 K8] Réception de :3 http://deb.debian.org/debian bookworm/main amd64 opensc_hotslin amd64 0.2.3.e-0.3-debi2ul [914 K8] Réception de :5 http://deb.debian.org/debian bookworm/main amd64 opensc_hotslin amd64 0.2.3.e-0.3-debi2ul [914 K8] Réception de :5 http://deb.debian.org/debian bookworm/main amd64 opensc_hotslin amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc_hotslin amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc_hotslin amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc_amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc_amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception de :6 http://deb.debian.org/debian bookworm/main amd64 opensc_amd64 0.2.3.e-0.3-debi2ul [917 K8] Réception du paquet libccid prizeddemment déselectionne. Préconfiguration de paquets page des.../Porscd_1.9.9-2_amd64.deb ... Pépaquetage de prized (1.5.2-1) Sélection du paquet pages de _.../?-Porscd_1.9.9-2_amd64.deb ... Pépaquetage de prized (1.9.9-2) Sélection du depaquetage de _.../?-Porscs_9.7.58.3.1.0e-1.1.deb Pépaquetage de opansc-pkcsli:amd64 (2.2.3.e-0.3-debi2ul_amd64.deb ... Pépa

On va copier le répertoire easy-rsa qui permet de générer les certificats :

root@SRVVPN:~# cp -pr /usr/share/easy-rsa /etc/openvpn/server/ && cd /etc/openvpn/server/easy-rsa

On va renommer et éditer le fichier vars :

root@SRVVPN:~# cp vars.example vars && nano vars





Puis on décommente et modifie selon nos informations :



5

On va maintenant crée l'autorité de certification :

root@SRVVPN: ~# ./easyrsa init-pki



Common Name : Mettre FR ou laisser par défaut

On génère désormais le certificat du serveur :

root@SRVVPN:~#./easyrsa build-server-full server

Puis le certificat du client :

root@SRVVPN:~#./easyrsa build-client-full client

Ensuite, générer le fichier dh.pem :

Ce fichier va être utilisé pour la première connexion en chiffrement symétrique.

root@SRVVPN:~#./easyrsa gen-dh

Tout dépend de votre machine mais, l'opération peut-être plus au moins de temps.

On génère le fichier clé :

root@SRVVPN:~# openvpn -genkey tls-auth ta.key

6

On renomme le fichier dh.pem :

root@SRVVPN:~# mv /etc/openvpn/dh.pem /etc/openvpn/dh2048.pem

Test de la configuration

On tape: root@SRVVPN:~# systemctl status openvpn.service

```
root@SRVVPN:~# systemctl status openvpn.service

• openvpn.service - OpenVPN service

Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; preset: enabled)

Active: active (exited) since Tue 2024-05-14 19:08:28 CEST; 1h 50min ago

Process: 919 ExecStart=/bin/true (code=exited, status=0/SUCCESS)

Main PID: 919 (code=exited, status=0/SUCCESS)

CPU: 2ms

mai 14 19:08:28 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...

mai 14 19:08:28 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.

root@SRVVPN:~#
```

On redémarre openvpn :

root@SRVVPN:~# systemctl restart openvpn.service

On va copier le dossier client1.ovpn :

root@SRVVPN:~# cp client1.ovpn /home

Puis :

root@SRVVPN:~# nano /home/client1.ovpn

7



On copie l'entité du fichier et on le collera plus tard.

Installation OpenVpn sur client Windows :

🌬 🏠 🙂 🗄 ← → C = openvpn.net/client/client-ci nect-vpn-for-windows/ NEW Forbes: OpenVPN CEO Talks Private SaaS Q Community Support Log In Request a Demo Get Started for Free OPENVPN' Products Solutions Apps Pricing Resources Partners **OpenVPN Connect for Windows** This is the official OpenVPN Connect client software for Windows developed and maintained by OpenVPN Inc. This is the recommended client program for the OpenVPN Access Server. The latest version of For Windows 7, 8, 10, and 11. r Windows is available here. Note: Windows 7 and 8 are not officially supported anymore an OpenVPN Access Server, it is recommended to the OpenVPN Connect client software directly from your A 32 bits version is also available: Download OpenVPN Connect v3 for 32 bits sha256 signature: fb4efcca3894b13aa7e786e8206c0e1e26c25c338b Try Access Server s Server, as it will then come preconfigured for use. The ailable here does not come preconfigured, but you can Get started with two free VPN connections. onnection configuration into it. It can also be used to update installation and retain settings. Previous generation OpenVPN Connect V2 is available here: Learn More Download OpenVPN Connect v2.7.1 For Windows 7, 8, and 10.

Ouvrir Edge et taper https://openvpn.net/client/client-connect-vpn-for-windows/ :

Ouvrer OpenVPN :

OpenVPN Cor	nnect		- ×
≡	Import	Profile	Þ
VI	A URL	UPLOAD I	FILE
Drag a You ca	and drop to up n import only	oload .OVPN proof one profile at a	ofile. a time.
	<i>`</i> _ `		
	BRO	WSE	

On va créer le fichier client1.ovpn dans bloc-notes et on colle ce qu'on a copié précédemment sur le serveur, enregistrer sous le fichier en « nomdufichier.ovpn » puis glisser le dans « upload file »

Et vous voilà connecter ! :



Configuration du serveur Web Apache

Pour installer apache :

root@SRVWEB : ~# apt install apache2

Pour activer la sécurisation https/tls d'apache :

root@SRVWEB : ~# a2enmod ssl && a2ensite

Puis modifier le fichier « index.html » situer dans /var/www/html :

GNU nano 7.2 <h1>HELLO WORLD</h1>	! BY MK				/var/www/html/index	.html				
	_	_	_	_	[Lecture de 1 ligne	1	_	_	_	_
^G Aide	∧O Écrire AB Lire fich	AW Chercher	^K Couper	AT Exécuter	AC Emplacement M-	U Annuler Rofaire	M-A Marquer	M-] -> Crochet	M-Q Précédent	AB En arrière

Pour les restrictions d'accès par adresse IP :

root@SRVWEB:~#nano /etc/apache2/sites-available/000-default.conf

Insérer cela :

<Directory /var/www/html> Order allow,deny Deny from all Allow from 10.0.231.109 </Directory>

GNU nano 7.2				000-default	.conf				
<virtualhost *:80=""></virtualhost>									
# The ServerName directive set	s the reques	st scheme, hostr	name and port that						
# the server uses to identify	itself. This	s is used when d	creating						
# redirection URLs. In the con	text of virt	tual hosts, the	ServerName						
<pre># specifies what hostname must</pre>	appear in t	the request's Ho	ost: header to						
# match this virtual host. For	the default	t virtual host ((this file) this						
<pre># value is not decisive as it</pre>	is used as a	a last resort ho	ost regardless.						
# However, you must set it for	any further	r virtual host e	explicitly.						
#ServerName www.example.com									
ServerAdmin webmaster@localhos	t								
DocumentRoot /var/www/html									
<directory html="" var="" www=""></directory>									
Order allow, deny									
Deny from all									
Allow from 10.0.231.0									
<pre># Available loglevels: trace8.</pre>	, tracel	L. debug, info,	notice, warn,						
# error, crit, alert, emerg.									
# It is also possible to confi	qure the loc	plevel for parti	icular						
# modules, e.g.									
#LogLevel info ssl:warn									
ErrorLog \${APACHE LOG DIR}/err	or.log								
CustomLog \${APACHE_LOG_DIR}/ad	cess.log com	nbined							
# For most configuration files	from conf-a	available/. whic	ch are						
# enabled or disabled at a glo	bal level, i	it is possible t	to						
<pre># include a line for only one</pre>	particular v	/irtual host. Fo	or example the						
# following line enables the G	, GI configura	ation for this h	host only						
<pre># after it has been globally d</pre>	lisabled with	n "a2disconf".							
No Aide A Écrire A (hercher	AK Couper	Exécuter	AC Emplacement	M=U Appuler	M-A Marquer	M=1 -> Crochet	N=0 Précédent	A En arrière
AN Ouitter AB Lire fich	emplacer	All Coller	Allustifier	Aller ligne	M-E Refaire	M-6 Conjer	A Retrouver	M-M Suivant	AE En avant
				tr ingite		topici			

Ce qui nous donnera ceci :

2 D OpenVPN Connect - VPN For You 🗙 🔓 www.bing.com	× QRecherche	× 🎦 403 Forbidden	× +			-	Ø	×
← C ▲ Non sécurisé 10.0.231.109				A* ☆ Φ	ర్≡	÷		0
Forbidden								Q
You don't have permission to access this resource.								
Apache/2.4.59 (Debian) Server at 10.0.231.109 Port 80								
								<u></u>
								•
								0
								-
								-
								+
								ŝ



Désormais on a accès que par https depuis les clients VPN :

Collecte et analyse des Logs sur le serveur OpenVPN :

Accès au fichier « server.conf » qui correspond aux meilleures pratiques de sécurité et aux exigences du système.



Accès aux fichiers de log OpenVPN :



Status OpenVpn.Service :

```
:oot@SRVVPN:/var/log/openvpn# systemctl status openvpn.service
    openvpn.service - OpenVPN service
    Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; preset: enabled)
    Active: active (exited) since Tue 2024-05-14 21:01:11 CEST; 1h 24min ago
    Process: 4372 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 4372 (code=exited, status=0/SUCCESS)
    CPU: 2ms
nai 14 21:01:10 SRVVPN systemd[1]: Stopping openvpn.service - OpenVPN service...
nai 14 21:01:11 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...
nai 14 21:01:11 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
```

Pour voir le journal d'openvpn (Utile en cas d'erreur !) :

root@SRVVPN:~#journalctl -xeu openvpn.service

17

```
L'unité (unit) openvpn.service a commencé à démarrer.
iai 14 19:08:28 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
  Subject: L'unité (unit) openvpn.service a terminé son démarrage
  Defined-By: systemd
  Support: https://www.debian.org/support
 L'unité (unit) openvpn.service a terminé son démarrage, avec le résultat done.
iai 14 21:01:10 SRVVPN systemd[1]: openvpn.service: Deactivated successfully.
  Subject: Unit succeeded
  Defined-By: systemd
  Support: https://www.debian.org/support
 The unit openvpn.service has successfully entered the 'dead' state.
iai 14 21:01:10 SRVVPN systemd[1]: Stopped openvpn.service - OpenVPN service.
  Subject: L'unité (unit) openvpn.service a terminé son arrêt
  Defined-By: systemd
  Support: https://www.debian.org/support
 L'unité (unit) openvpn.service a terminé son arrêt.
iai 14 21:01:10 SRVVPN systemd[1]: Stopping openvpn.service - OpenVPN service...
  Subject: L'unité (unit) openvpn.service a commencé à s'arrêter
  Defined-By: systemd
  Support: https://www.debian.org/support
  L'unité (unit) openvpn.service a commencé à s'arrêter.
iai 14 21:01:11 SRVVPN systemd[1]: Starting openvpn.service - OpenVPN service...
  Subject: L'unité (unit) openvpn.service a commencé à démarrer
  Defined-By: systemd
  Support: https://www.debian.org/support
  L'unité (unit) openvpn.service a commencé à démarrer.
iai 14 21:01:11 SRVVPN systemd[1]: Finished openvpn.service - OpenVPN service.
  Subject: L'unité (unit) openvpn.service a terminé son démarrage
  Defined-By: systemd
  Support: https://www.debian.org/support
  L'unité (unit) openvpn.service a terminé son démarrage, avec le résultat done.
```

WireShark :

Depuis client Windows :



Depuis Serveur :

	Capture en cours de ens33	- a x
Fichier Editer Vue Alter Capture Analyser Statistiques Telephonie Wi	eless Outils Aide	
Appliquer un filtre d'affichage <ctrl-></ctrl->		
No. Time Source Destination 37674 5022.5768334.10.02.231.101 10.0.231.101 10.0.231.109 37674 5022.5768324.10.0.231.101 10.0.231.109 133.5.198.50 37676 5022.5768324.10.0.231.109 13.35.198.50 139.109 37676 5022.5768324.10.0.231.109 13.35.198.50 139.769 37676 5022.5769328.10.0.231.109 13.262.244.33 10.0.231.109 37680 5022.5080021.2.32.26.244.33 10.0.231.109 13.262.244.33 37680 5022.5806022.3.10.75.73.229 10.0.231.109 13.6762.502.511.461.146.75.73.229 37680 5022.5807138.14.04.07.57.3.229 10.0.231.109 136.73.109 37680 5022.583958.10.0.231.101 10.0.231.101 10.3.131.09 37685 5022.583958.10.0.231.101 10.0.231.101 10.3.31.101 37686 5022.584233.0.0.231.101 10.0.231.101 10.0.231.101 37686 5022.6343709.10.231.101 10.0.231.101 10.0.231.101 37686 5022.6134799.10.0.231.101 10.0.231.101 10.0.231.101 37686 5022.6134799.10.0.231.101 10.0.231.101 10.0.231.101 37686 5022.6134799.10.0.231.101 10.0.231.101 10.0.231.101 </td <td>Protocol Length Info OpenVPM 166 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 55 Protected Payload (KP0), DCID=2c28918316740d6cf947421cee7e69b5f63e8dfd OpenVPM 178 MessageType: P_DATA_V2 TLSV1.3 118 Change Cipher Spec, Application Data TCP 60 443 - 60675 [AcK] Seg=235 Ack=2038 Win=64240 Len=0 OpenVPM 160 MessageType: P_DATA_V2 TLSV1.3 50 Server Hello, Change Cipher Spec, Application Data, Application Data OpenVPM 118 Change Cipher Spec, Application Data OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 180 MessageType: P_DATA_V2 OpenVPM 138 MessageType: P_DA</td> <td></td>	Protocol Length Info OpenVPM 166 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 137 MessageType: P_DATA_V2 OpenVPM 55 Protected Payload (KP0), DCID=2c28918316740d6cf947421cee7e69b5f63e8dfd OpenVPM 178 MessageType: P_DATA_V2 TLSV1.3 118 Change Cipher Spec, Application Data TCP 60 443 - 60675 [AcK] Seg=235 Ack=2038 Win=64240 Len=0 OpenVPM 160 MessageType: P_DATA_V2 TLSV1.3 50 Server Hello, Change Cipher Spec, Application Data, Application Data OpenVPM 118 Change Cipher Spec, Application Data OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 170 MessageType: P_DATA_V2 OpenVPM 180 MessageType: P_DATA_V2 OpenVPM 138 MessageType: P_DA	
<pre>states docc.dob/sdbs_let.et.alilet.gst_let.g</pre>	upperind 100 mossage:spc: r_204A_V2 ed(1376b bits) 0n interface ens33 DVPdmcast_ff:ff:fa (01:00:5e:7f) 0010 0010 00 cb 20 ec 00 00 0111 0020 01 00 5c 7f ff fa 64 07 6c 00 b7 b0 2b 42 d3 25 44 152 0020 04 00 20 ec 00 00 0111 0020 04 00 20 22 a2 04 55 45 56 5c 2f 31 2c 31 00 00 a5 45 45 52 0020 04 48 02 3a 20 46 54 56 5c 2f 31 2c 31 00 00 a5 46 45 20 0020 04 48 02 3a 20 46 54 56 5c 2f 31 2c 31 00 00 a5 46 00 7f 11 1.5 1.5 100 00 a5 100 00 a4 14 43 20 0020 04 48 02 3a 20 10 00 a5 54 54 25 77 26 60 a 0020 22 73 73 64 70 3a 64 69 73 63 57 72 62 6a 0020 20 6f 72 67 73 76 69 73 65 72 62 6a 0020 04 65 83 21 2c 67 36 67 66 72 22 46 67 65 27 0020 04 72 67 33 73 75 72 76 69 33 65 44 66 10orgrser vicedia 0020 20 67 26 73 73 76 57 26 75 26 64 30 66 10 - orgrser vicedia 0020 04 25 32 72 67 73 66 73 26 57 36 44 76 35 27 0020 04 20 72 77 36 76 67 3 20 57 69 120 20 20 37 30 57 72 67 30 10 - orgrser vicedia 0020 03 13 23 34 2e 39 26 22 34 37 38 2e 39 37 20 57 69 124.0,24 78.97 Wi 0020 31 32 34 2e 39 22 32 34 37 38 2e 39 37 20 57 69 124.0,24 78.97 Wi<	~
ens33: live capture in progress>	Paquets : 68896 · Affichés : 68896 (100.0%)	Profil : Default

Conclusion :

J'en tire de ce TP qui est très intéressant pour une entreprise d'adopter la technologie VPN, il sécurise les échanges envers les différents services. Grâce au chiffrement, personne ne peut avoir accès aux informations qui sont envoyées sur Internet. C'est un gage de sécurité qui permet d'éviter, par exemple, des attaques par déni de service sur le réseau de l'entreprise. De plus, le VPN permet de chiffrer la connexion internet des collaborateurs, ce qui permet de se protéger contre l'attaque de l'homme au milieu. Cette attaque est très fréquente lorsque l'on se connecte depuis des réseaux publics, il est donc indispensable pour vous et vos collaborateurs d'utiliser un VPN lors de déplacements.

Annexe :

Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)

7000	fileserver
7001	Cache Manager callback service
7002	ptserver
7003	vlserver (VLDB)
7004	kaserver
7005	volserver (volume management)
7007	bosserver
7008	upserver
7009	AFS/NFS Translator
7020	AFS backup coordinator
7021	AFS backup buserver
7025-7032	AFS backup tape controllers
7101	xstat
2106	fs monitor port
next available port	pts, kas, fs, klog, etc.

 $/\!\!/$