

TP4 : OpenVPN

Pfsense

Fait par DEPRADE ELIOTT

SOMMAIRE

But du TP	2
Configuration dans Pfsense	3
Création certificat serveur	3
Création d'un utilisateur	5
Configuration du VPN	7
Export de la configuration	9
Configuration du client VPN (machine physique)	10
Derniers tests	11
Vérification de l'interface	12

But du TP

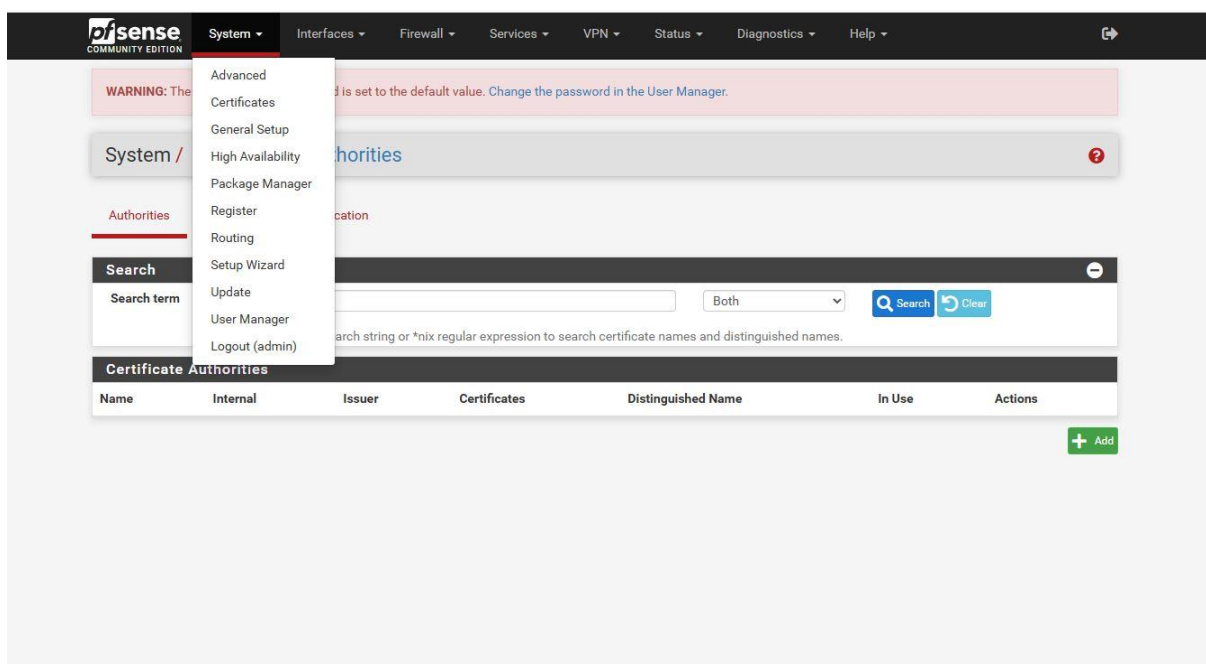
Un client nomade (ordinateur personnel) doit pouvoir se connecter à distance au réseau local derrière pfSense, comme s'il y était physiquement connecté.

La connexion doit être chiffrée en UDP.

Configuration dans Pfsense

Création certificat serveur

Dans un premier temps on va créer le certificat du serveur en allant dans System > Certificates > Authorities :



Cliquons sur “Add”.

The screenshot shows the pfSense web interface. At the top, there's a 'Create / Edit CA' form. The 'Descriptive name' field contains 'OpenVPN'. Below it, a note states: 'The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ', ' '. The 'Method' dropdown is set to 'Import an existing Certificate Authority'. Under 'Trust Store', the checkbox 'Add this Certificate Authority to the Operating System Trust Store' is checked, with a note: 'When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.' Under 'Randomize Serial', the checkbox 'Use random serial numbers when signing certificates' is checked, with a note: 'When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.'

Below the form is a section titled 'Existing Certificate Authority'. It shows a breadcrumb 'System / Certificate / Authorities' with a help icon. There are three tabs: 'Authorities' (selected), 'Certificates', and 'Revocation'. A search bar is present with a 'Search term' field, a 'Both' dropdown, and 'Search' and 'Clear' buttons. Below the search bar, a note says: 'Enter a search string or *nix regular expression to search certificate names and distinguished names.'

The 'Certificate Authorities' table is displayed with the following data:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN	✓	self-signed	0	CN=pfsense.cs.cr Valid From: Sat, 06 Dec 2025 23:16:46 +0000 Valid Until: Tue, 04 Dec 2035 23:16:46 +0000		

A green '+ Add' button is located at the bottom right of the table.

On choisi la méthode **Method: Create an Internal Certificate Authority**

Et dans le **Common Name** on renseigne **le nom de domaine**, exemple pour ici : pfsense.cs.cr

Ensuite, passez à l'onglet **Certificates** et créez un nouveau certificat de serveur en cliquant sur Add/Sign. Choisissez Create an internal certificate, nommez-le (p.ex. OpenVPN-remote-access), sélectionnez la CA créée précédemment et entrez comme Common Name le nom du serveur (par ex. pfSense.cs.sr). Dans Certificate Type, sélectionnez Server Certificate. Cliquez sur Save.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / Certificates / Certificates



Created internal certificate OpenVPN-remote-access



Authorities Certificates Certificate Revocation

Search



Search term

Both ▾



Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6922fac4d31d4) Server Certificate	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6922fac4d31d4 Valid From: Sun, 23 Nov 2025 12:15:01 +0000 Valid Until: Sat, 26 Dec 2026 12:15:01 +0000		
OpenVPN-remote-access Server Certificate	OpenVPN	CN=pfSense.cs.cr Valid From: Sat, 06 Dec 2025 23:22:48 +0000 Valid Until: Tue, 04 Dec 2035 23:22:48 +0000		

[+ Add/Sign](#)

Création d'un utilisateur

Allez ensuite dans System>User Manager>Users>Edit.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username:

Password: Confirm Password:

Full name:
User's full name, for administrative information only

Expiration date:
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership:

Not member of: Member of:

[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate: ☐ Click to create a user certificate

Activ
Accès

Créer votre utilisateur et cochez la case “Create User Certificate”.

Effective Privileges

Inherited from	Name	Description	Action
			+ Add

User Certificates

Name	CA
alice	OpenVPN

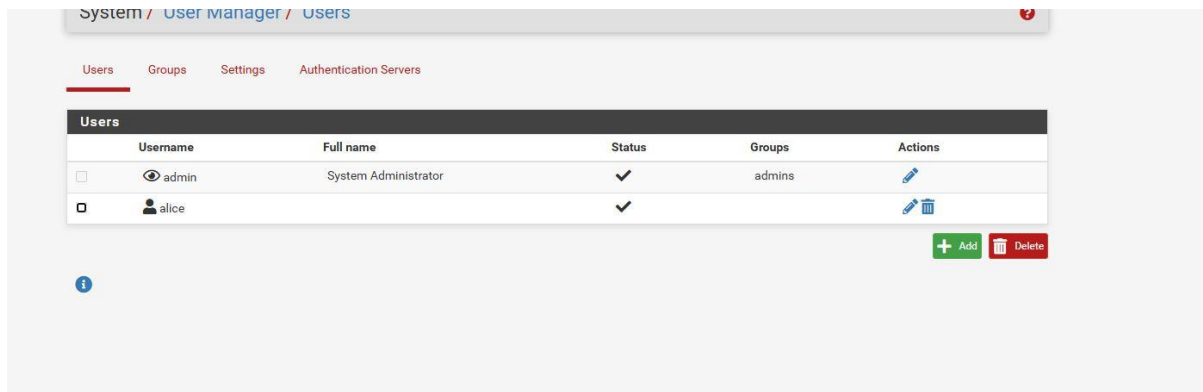
[+ Add](#)

Keys

Authorized SSH Keys

Utilisez le CA que vous venez de créer.

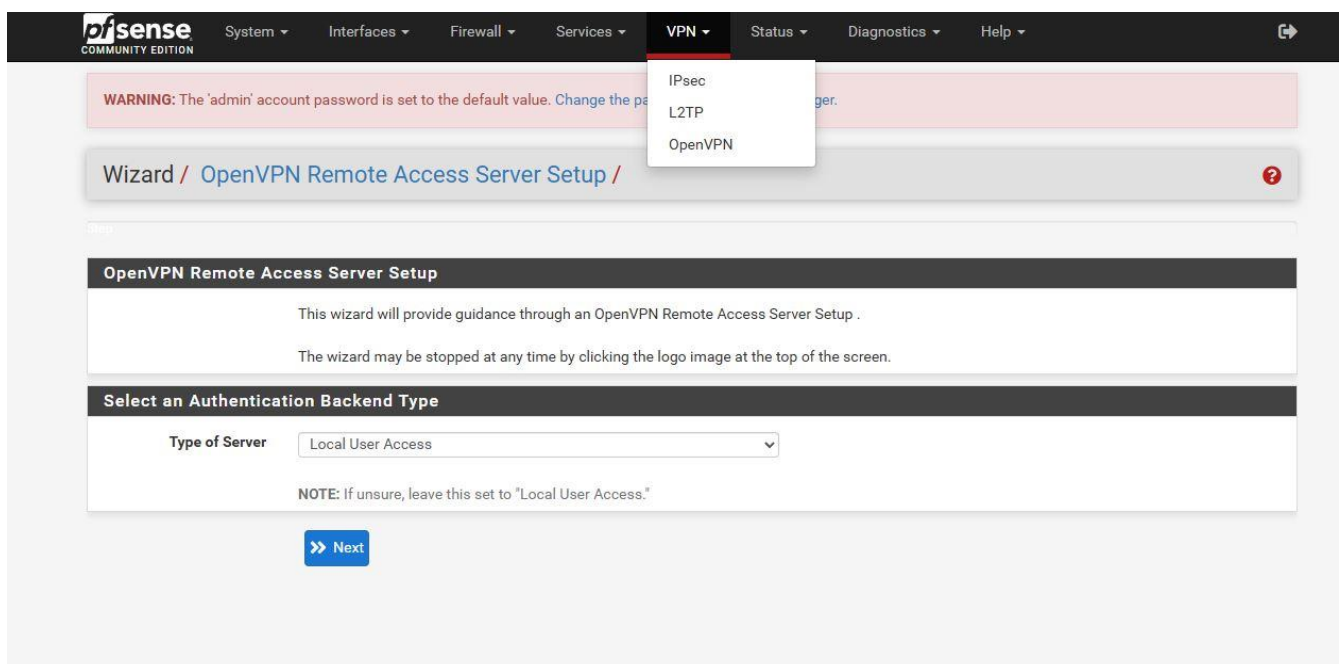
Parfait, votre utilisateur devrait être maintenant visible dans vos Users.



Passons à la configuration du VPN

Configuration du VPN

Allez dans VPN > OpenVPN > Wizard



Type of serveur = Local User Access

Autorité CA et certificat serveur = choisissez la CA interne créée et le certificat serveur (OpenVPNremote-access) déjà générés.

Adresse WAN du serveur = indiquez l'IP WAN actuelle du pfSense (ici 192.168.1.130)

Choisissez une adresse différente de votre Wan ou Lan pour votre **Tunnel**

Local Network = spécifiez le réseau LAN local à rendre accessible par le VPN

Advanced Client Settings = entrez DNS Default Domain = votre domaine, DNS Server 1 = (IP LAN) et DNS Server 2 = (IP WAN/pfSense)

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="192.168.200.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation. The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to clients.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	<input type="text" value="10.10.10.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not desired. If set, the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/> <small>Allow compression to be used with this VPN instance, which is potentially insecure.</small>
Compression	<input type="text" value="Disable Compression [Omit Preference]"/> <small>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This option is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that compression is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. <small>NOTE: This is not generally recommended, but may be needed for some scenarios.</small>
Duplicate Connection Limit	<input type="text"/> <small>Limit the number of concurrent connections from the same user.</small>

Advanced Client Settings	
DNS Default Domain	<input type="text" value="cs.cr"/> <small>Provide a default domain name to clients.</small>
DNS Server 1	<input type="text" value="10.10.10.1/24"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 2	<input type="text" value="8.8.8.8"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 3	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 4	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>
NTP Server	<input type="text"/> <small>Network Time Protocol server to provide to connecting clients.</small>
NTP Server 2	<input type="text"/> <small>Network Time Protocol server to provide to connecting clients.</small>
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP. <small>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</small>
NetBIOS Node Type	<input type="text" value="none"/> <small>Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).</small>
NetBIOS Scope ID	<input type="text"/>

Le Wizard propose ensuite d'ajouter automatiquement des règles de pare-feu. Validez les options Add a firewall rule et Add an OpenVPN rule pour autoriser le trafic VPN entrant. Terminez le Wizard. Un serveur OpenVPN est alors créé, mais nous devons affiner certains réglages.

Dans **“advanced configuration”** ajoutez la ligne push **“route LAN MASK”** dans Custom Option

Advanced Configuration

Custom options

push "route 10.10.10.0 255.255.255.0"

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Username as Common Name

☒ Use the authenticated client username instead of the certificate common name (CN).
When a user authenticates, if this option is enabled then the username of the client will be used in place of the such as determining Client Specific Overrides.

UDP Fast I/O

☐ Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platform bandwidth limiting.

Votre VPN est normalement fin prêt :

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.200.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		

[+ Add](#)

Export de la configuration

Installez le paquet **openvpn-client-export** via **System > Packages**. Ensuite, retournez dans VPN > OpenVPN, onglet Client Export. Sélectionnez l'utilisateur alicé et cliquez sur **Most Clients** pour générer un fichier .ovpn (il contient automatiquement le certificat utilisateur et la CA) . Téléchargez ce profil sur le poste client.

The image shows two screenshots from the pfSense web interface. The top screenshot is the 'System / Package Manager / Available Packages' page. It features a search bar with 'openvpn-client-export' entered. Below the search bar, a table lists available packages. The 'openvpn-client-export' package is highlighted, showing its version (1.9.2) and description: 'Exports pre-configured OpenVPN Client configurations directly from pfSense software.' A green '+ Install' button is visible next to the package name. Below the package name, there are links for package dependencies: 'openvpn-client-export-2.6.7', 'openvpn-2.6.8_1', 'zip-3.0_1', and '7-zip-23.01'. The bottom screenshot is the 'OpenVPN Clients' page. It shows a table with columns 'User', 'Certificate Name', and 'Export'. The user 'alice' is listed. Under the 'Export' column for 'alice', there are several download links categorized under 'Inline Configurations', 'Bundled Configurations', 'Current Windows Installers', 'Previous Windows Installers', 'Legacy Windows Installers', and 'Viscosity'. The 'Most Clients' link under 'Inline Configurations' is highlighted.

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: openvpn-client-export Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01

Enter a search string or *nix regular expression to search.

OpenVPN Clients

User	Certificate Name	Export
alice	alice	<ul style="list-style-type: none">- Inline Configurations:<ul style="list-style-type: none">Most Clients Android OpenVPN Connect (iOS/Android)- Bundled Configurations:<ul style="list-style-type: none">Archive Config File Only- Current Windows Installers (2.6.7-ix001):<ul style="list-style-type: none">64-bit 32-bit- Previous Windows Installers (2.5.9-ix601):<ul style="list-style-type: none">64-bit 32-bit- Legacy Windows Installers (2.4.12-ix601):<ul style="list-style-type: none">10/2016/2019 7/8/8.1/2012/2- Viscosity (Mac OS X and Windows):<ul style="list-style-type: none">Viscosity Bundle Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown

Configuration du client VPN (machine physique)

Sur la machine physique (située sur le réseau WAN), installez un client OpenVPN adapté à l'OS

Sous Windows, installez OpenVPN Connect puis importez le fichier .ovpn :



Vous serez ensuite connecté à votre pfSense grâce aux identifiants de l'utilisateur créé précédemment.

Derniers tests

Essayez de pinguer votre LAN depuis votre machine en WAN :

```
Microsoft Windows [version 10.0.19045.6575]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\depra>ping 10.10.10.10

Envoi d'une requête 'Ping' 10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps<1ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\depra>
```

Si ce test ne fonctionne pas, vérifiez votre pare-feu psSense voir s'il n'y a pas de règles trop strictes.

En faisant ipconfig/all votre pc devrait avoir une interface dans la plage de l'IP choisie plus tôt :

Vérification de l'interface

130 215.404181	fe80::7188:e82b:b58a:55c3	ff02::1b	NDNS	102 Standard query 0x0000 PTR _g
137 215.405430	192.168.200.2	224.0.0.251	NDNS	82 Standard query 0x0000 PTR _g
138 215.405844	fe80::7188:e82b:b58a:55c3	ff02::1b	NDNS	102 Standard query 0x0000 PTR _g
139 218.962569	00:ff:4f:97:78:42	Broadcast	ARP	42 Who has 192.168.200.1? Tell
140 218.962579	00:ff:50:97:78:42	00:ff:4f:97:78:42	ARP	60 192.168.200.1 is at 00:ff:50
141 219.418510	fe80::7188:e82b:b58a:55c3	ff02::1:2	DHCPv6	147 Solicit XID: 0xbd2570 CID: 0
142 224.280377	192.168.200.2	192.168.200.255	STEANDISCOVER	280 Client Status from THOOR[Hal
143 224.699103	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
144 224.699994	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
145 225.701332	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
146 225.702304	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
147 226.703242	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
148 226.704277	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
149 227.706576	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
150 227.707607	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
151 235.419577	fe80::7188:e82b:b58a:55c3	ff02::1:2	DHCPv6	147 Solicit XID: 0xbd2570 CID: 0

On peut voir que j'utilise bien l'interface 192.168.200.2 (le tunnel)

Et sur l'interface wan cela se traduit par du trafic en UDP chiffré :

81 3.532875	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=657, data
82 3.532837	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=657, data
83 3.533880	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=658, data
84 3.533354	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=659, data
85 3.533367	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=660, data
86 3.533070	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=661, data
87 3.535471	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=662, data
88 3.535471	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=663, data
89 3.535687	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=664, data
90 3.535645	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=665, data
91 3.535890	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=666, data
92 3.536220	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=667, data
93 3.536489	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=8a40dfc7c4, counter=668, data

