

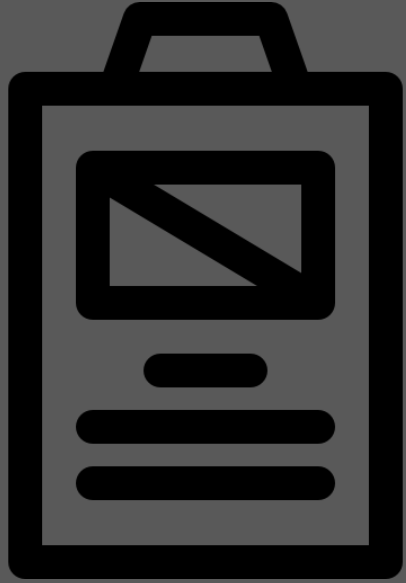
TP



KALETA Maxime

BTS SIO

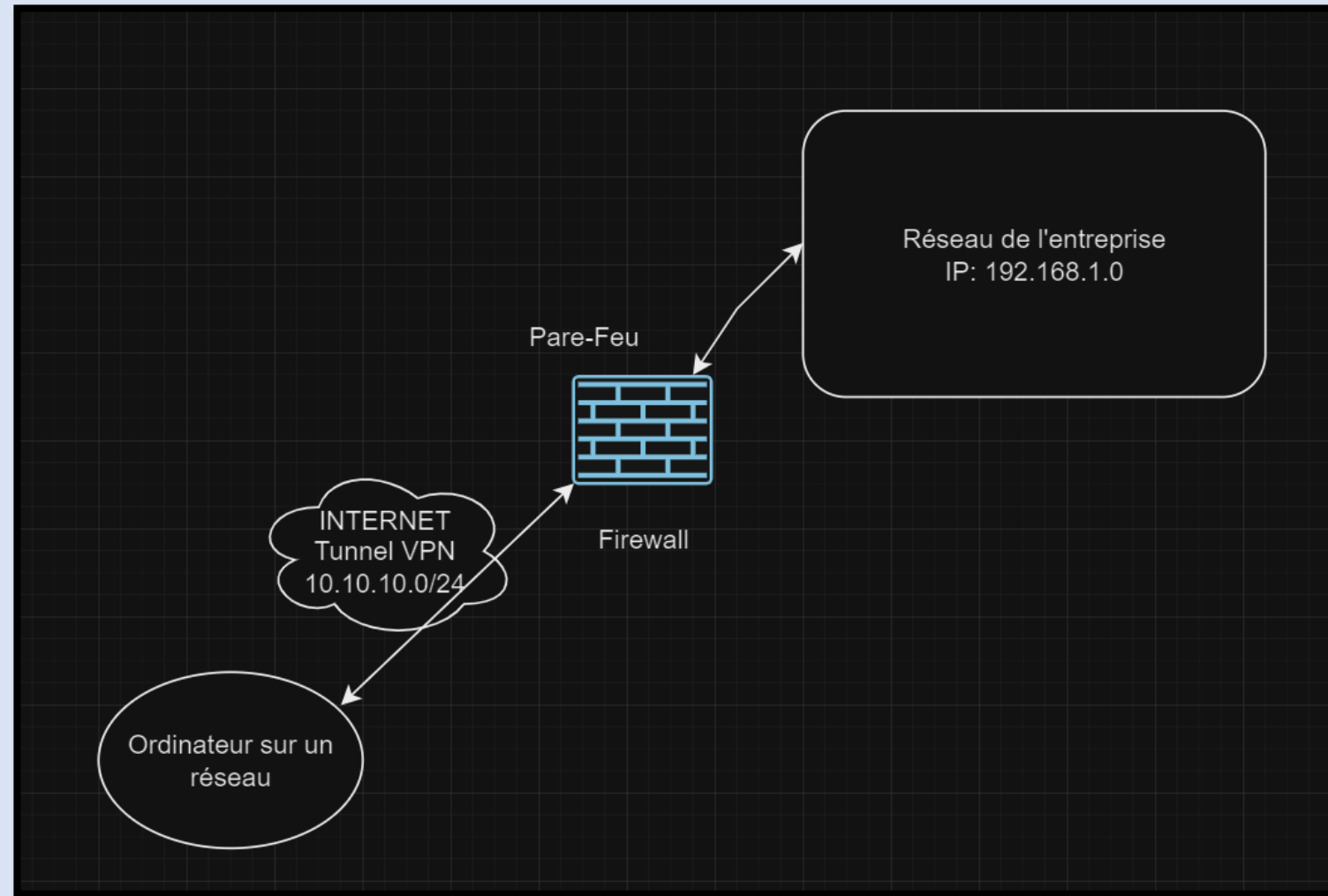




Sommaire

- Création autorité de certification
- Création du certificat Server
- Création des utilisateurs locaux
- Configuration du server OpenVPN
- Paramètres client
- Client d'exportation de la configuration
- Règles
- Mise en place et connection du VPN

Infrastructure



Création autorité de certification

- Ajouter un Name
- sélectionner la bonne Méthod
- donner un NAME Common Name

The screenshot shows the pfSense web interface for creating a Certificate Authority. The breadcrumb trail is System / Certificate / Authorities / Edit. The 'Create / Edit CA' form has the following fields and values:

- Descriptive name:** openVPN (indicated by a red arrow)
- Method:** Create an internal Certificate Authority (indicated by a red arrow)
- Trust Store:** ☐ Add this Certificate Authority to the Operating System Trust Store
- Randomize Serial:** ☐ Use random serial numbers when signing certificates
- Internal Certificate Authority section:**
 - Key type:** RSA
 - Key length:** 2048
 - Digest Algorithm:** sha256
 - Lifetime (days):** 3650
 - Common Name:** VPN-max (indicated by a red arrow)

At the bottom right, there is a watermark: "Activer Windows 10 - Accédez aux paramètres".

Création des utilisateurs locaux



Dans l'onglet System> User manager> Users> Edit

- Saisir un nom et mot de passe

System / User Manager / Users / Edit

Users Groups Settings **Authentication Servers**

User Properties

Defined by	USER		
Disabled	☐ This user cannot login		
Username	max		
Password	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	admins		
	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.		

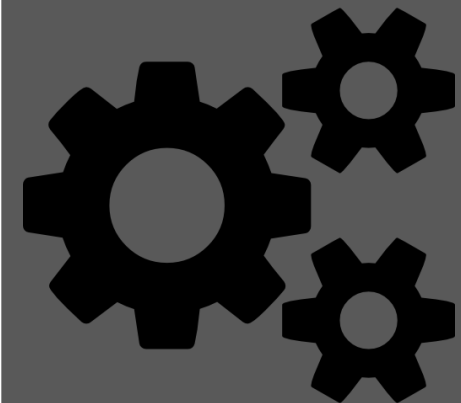
Create Certificate for User

Descriptive name	VPN-USER
Certificate authority	openVPN
Key type	RSA
	2048
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256
	The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.
Lifetime	3650

Activ

KALETA Maxime

Configuration du server OpenVPN



Dans l'onglet VPN> OpenVPN il faut ajouter une configuration

- Changer le Server mode pour mettre celui afin d'avoir une authentification à la connexion.

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards

General Information

Description
A description of this VPN for administrative reference.

Disabled ☐ Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode Remote Access (SSL/TLS + User Auth)

Sélectionner le certificat d'authentification ainsi le certificat server

Cryptographic Settings

TLS Configuration ☒ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

☒ Automatically generate a TLS Key.

Peer Certificate Authority openVPN

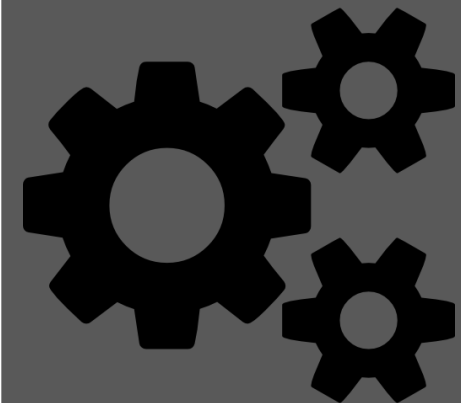
Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check ☐ Check client certificates with OCSP

Server certificate CA-max-VPN (Server: Yes, CA: openVPN)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

Configuration du server OpenVPN



Configuration de l'IP tunnel ainsi que celle du réseau local :

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.0.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway ☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway ☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Paramètres du client :

Client Settings

Dynamic IP ☒ Allow connected clients to retain their connections if their IP address changes.

Topology

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Dans la zone "Custom options", indiquez : auth-nocache. Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache

Advanced Configuration

Custom options

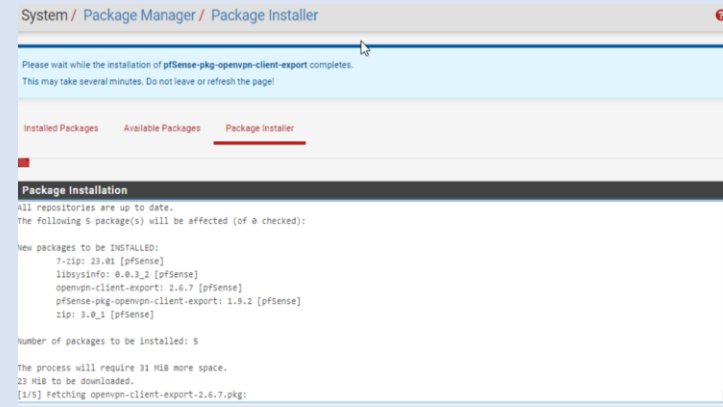
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN	  

KALETA Maxime

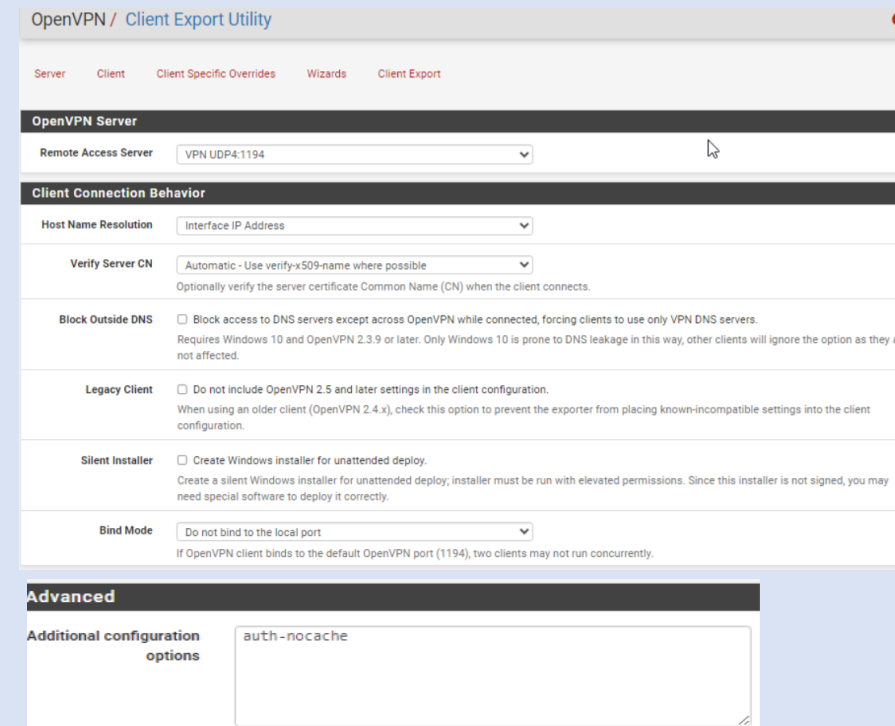
Client d'exportation de la configuration



Pour exporter les fichiers il est nécessaire d'installer un plugin :
Recherchez « openvpn » et installez le premier paquet :



Configuration pour l'exportation du client



Règles

Wan :

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol UDP
Choose which IP protocol this rule should match.

Destination

Destination ☐ Invert match WAN address Destination Address

Destination Port Range OpenVPN (1194) OpenVPN (1194)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗ 0/35 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
☐	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			📌✎🔄🗑

Règles

OpenVPN : Règle pour le contrôle à distance

Firewall / Rules / Edit

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Destination

Destination ☐ Invert match /

Destination Port Range (other) (other)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

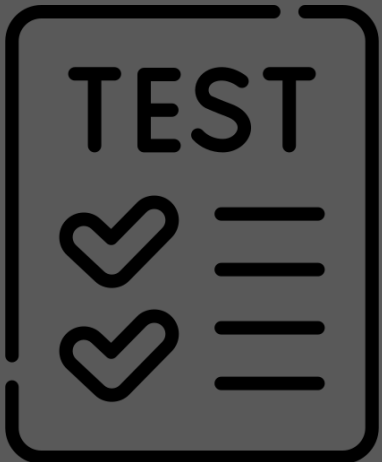
Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

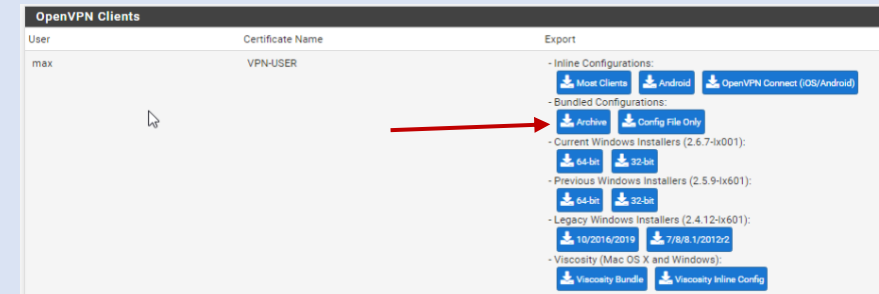
Advanced Options

Mise en place et connexion du VPN

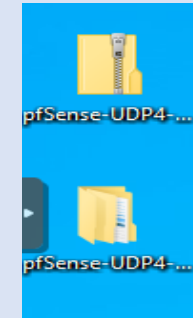


- Obtention du client

Pour obtenir le client il faut se rendre dans l'onglet OpenVPN puis dans client export :

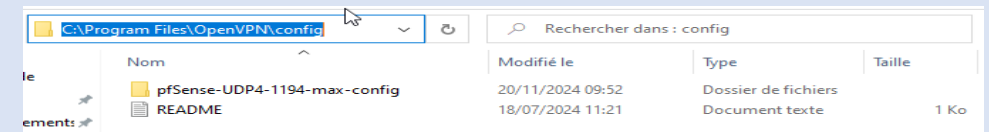


Transfert du Fichier .zip vers la machine hors du réseau via un partage :

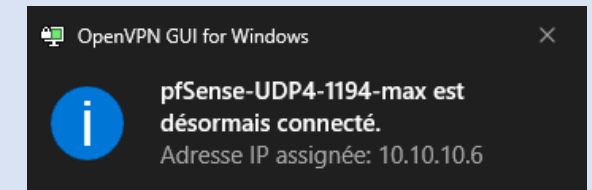
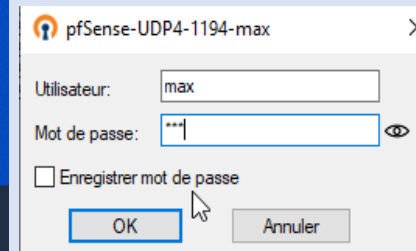
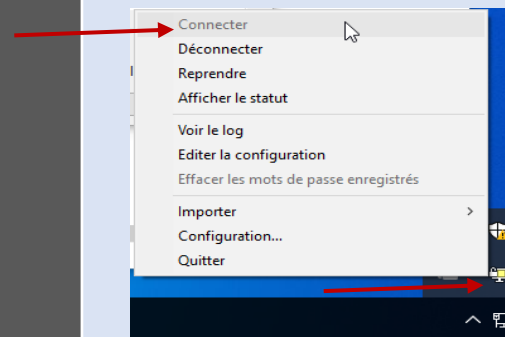


- Installation du client OPENVPN

Mettre le fichier de config du vpn dans le chemin ci-dessous :



Je me rends sur l'icone openvpn puis connecter



KALETA Maxime