

VPN OPEN SSL

BTS – SIO 1 / SISR



Clément Paccard

29/01/2024

TABLE DES MATIERES

| | |
|---|----------|
| FIREWALL PFSENSE..... | 1 |
| Introduction | 1 |
| 1- Créer l'autorité de certification | 2 |
| 2- Créer le certificat serveur | 4 |
| 3- Configurer le serveur Open VPN | 5 |
| Conclusion | 11 |

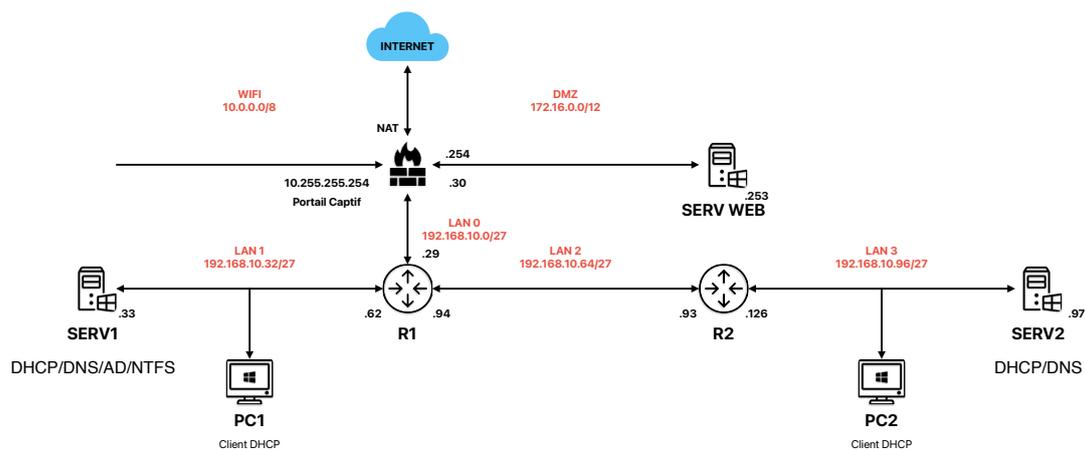
FIREWALL

PFSENSE

INTRODUCTION

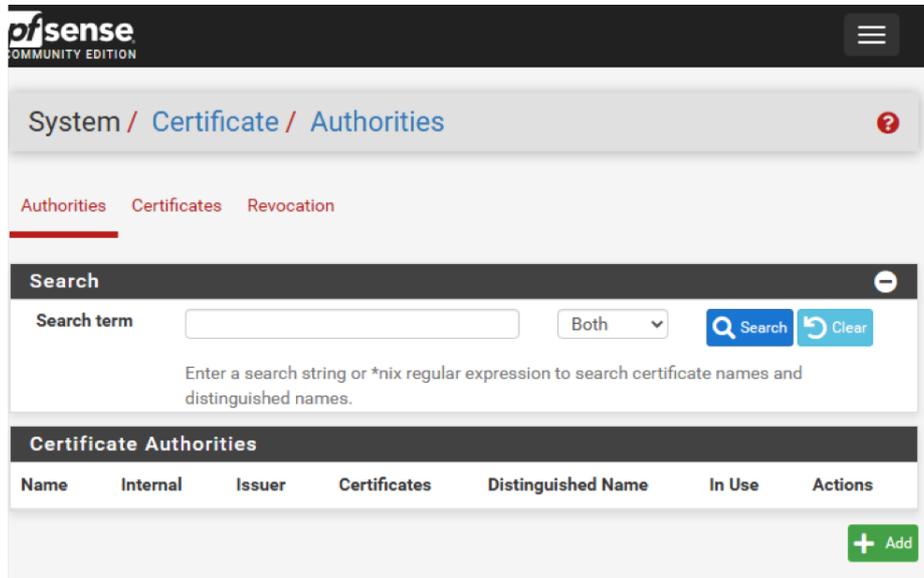
Cette procédure montre comment installer et paramétrer un VPN OPEN SSL sur un Pare-feu PFSense.

Un VPN SSL est un réseau privé virtuel créé à l'aide du protocole SSL (Secure Sockets Layer) pour établir une connexion sécurisée et chiffrée entre deux réseaux.

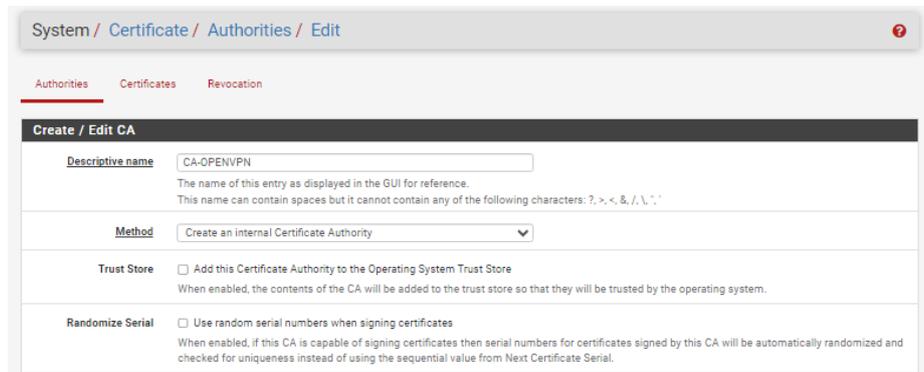


1-CRÉER L'AUTORITÉ DE CERTIFICATION

Pour ce faire allez dans System -> Certificate -> Authorities puis cliquez sur Add.



Ensuite on va nommer l'autorité (CA-OPENVPN)



Ensuite remplissez les informations pour votre entreprise :

| Internal Certificate Authority | |
|--------------------------------|--|
| Key type | RSA |
| | 2048 |
| | <small>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.</small> |
| Digest Algorithm | sha256 |
| | <small>The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid</small> |
| Lifetime (days) | 3650 |
| Common Name | paccard-vpn |
| | <small>The following certificate authority subject components are optional and may be left blank.</small> |
| Country Code | FR |
| State or Province | Haute Savoie |
| City | Annecy |
| Organization | ECORIS |
| Organizational Unit | e.g. My Department Name (optional) |

Activer Windows
Accédez aux paramètres
pour activer Windows.

2-CREER LE CERTIFICAT SERVEUR

Maintenant nous allons créer le certificat du serveur.

System -> Certificate -> Certificates et cliquez sur le bouton Add/Sign

Choisissez ensuite Create an internal Certificate, on peut lui ajouter une description.

Ensuite choisissez l'autorité de certification (on choisit celle créé précédemment)

Ajoutez un nom puis remplissez les informations pour votre entreprise.

The screenshot shows a web interface for creating a new certificate. The breadcrumb navigation is 'System / Certificates / Certificates / Edit'. There are three tabs: 'Authorities', 'Certificates', and 'Certificate Revocation', with 'Certificates' being the active tab. The main heading is 'Add/Sign a New Certificate'. The form is divided into two sections: 'Add/Sign a New Certificate' and 'Internal Certificate'. The 'Add/Sign a New Certificate' section includes a 'Method' dropdown set to 'Create an internal Certificate', a 'Descriptive name' text input with 'VPN-SSL-PACCARD' and a note about character restrictions. The 'Internal Certificate' section includes a 'Certificate authority' dropdown set to 'CA-OPENVPN', a 'Key type' dropdown set to 'RSA', a key length dropdown set to '2048' with a note about key length requirements, a 'Digest Algorithm' dropdown set to 'sha256' with a note about digest methods, a 'Lifetime (days)' text input with '3650' and a note about lifetime limits, a 'Common Name' text input with 'vpn.paccard.acy' and a note about optional subject components, a 'Country Code' dropdown set to 'FR', a 'State or Province' text input with 'Haute Savoie', a 'City' text input with 'Annecy', an 'Organization' text input with 'ECORIS', and an 'Organizational Unit' text input with 'e.g. My Department Name (optional)'. A 'Activer Windows' watermark is visible in the bottom right corner.

| Add/Sign a New Certificate | |
|----------------------------|---|
| Method | Create an internal Certificate |
| Descriptive name | VPN-SSL-PACCARD <small>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: ?, >, <, &, /, \, ", '.</small> |
| Internal Certificate | |
| Certificate authority | CA-OPENVPN |
| Key type | RSA |
| | 2048 <small>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.</small> |
| Digest Algorithm | sha256 <small>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.</small> |
| Lifetime (days) | 3650 <small>The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.</small> |
| Common Name | vpn.paccard.acy <small>The following certificate subject components are optional and may be left blank.</small> |
| Country Code | FR |
| State or Province | Haute Savoie |
| City | Annecy |
| Organization | ECORIS |
| Organizational Unit | e.g. My Department Name (optional) |

Enfin, sélectionnez Server Certificate pour le type de certificat.

The screenshot shows the 'Certificate Attributes' configuration page. It includes the following sections:

- Attribute Notes:** Explains that attributes are added to certificates and requests, and that for internal certificates, they are added directly to the certificate.
- Certificate Type:** A dropdown menu set to 'Server Certificate'. Below it, a note states: 'Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.'
- Alternative Names:** A section with a dropdown for 'Type' set to 'FQDN or Hostname' and a text input for 'Value' containing 'vpn.paccard.acy'. A note below says: 'Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.'
- Add SAN Row:** A green button with a plus sign and the text 'Add SAN Row'.
- Save:** A blue button with a floppy disk icon and the text 'Save'.

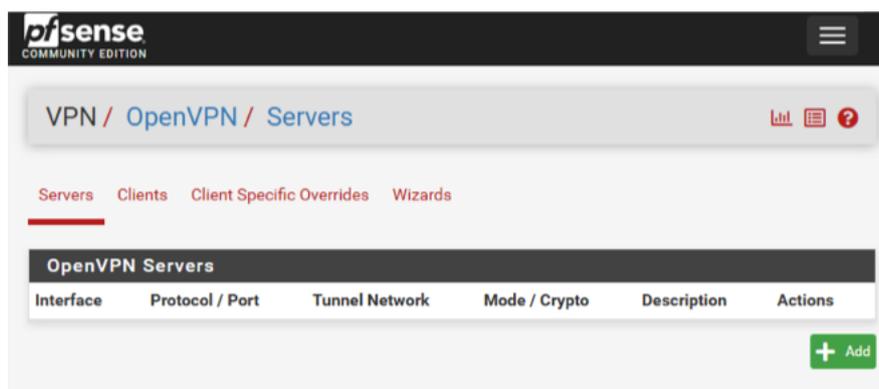
At the bottom right, there is a watermark for 'Activer Windows' and 'Accédez aux paramètres po'.

Validez avec Save, voilà le certificat apparaît maintenant dans la liste des certificats du Pare-Feu.

3- CONFIGURER LE SERVEUR OPEN VPN

On va maintenant configurer le VPN en lui-même. Pour ce faire allez dans le menu VPN -> OpenVPN

Dans l'onglet Server cliquez sur Add.



Ensuite il faut sélectionner le "Server Mode" suivant : Remote Access (SSL/TLS + User Auth).

On laisse bien l'interface WAN sélectionné et les paramètres suivants :

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

Backend for authentication
Local Database

Device mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

Interface

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

The port used by OpenVPN to receive client connections.

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

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

DH Parameter Length

Diffie-Hellman (DH) parameter set used for key exchange. 

ECDH Curve

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

- AES-128-CBC (128 bit key, 128 bit block)
- AES-128-CFB (128 bit key, 128 bit block)
- AES-128-CFB1 (128 bit key, 128 bit block)
- AES-128-CFB8 (128 bit key, 128 bit block)
- AES-128-GCM (128 bit key, 128 bit block)
- AES-128-OFB (128 bit key, 128 bit block)
- AES-192-CBC (192 bit key, 128 bit block)
- AES-192-CFB (192 bit key, 128 bit block)
- AES-192-CFB1 (192 bit key, 128 bit block)
- AES-192-CFB8 (192 bit key, 128 bit block)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. 

Fallback Data Encryption Algorithm

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.

When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

| | |
|--|--|
| Hardware Crypto | <input type="text" value="No Hardware Crypto Acceleration"/> |
| Certificate Depth | <input type="text" value="One (Client+Server)"/> When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server. |
| Strict User-CN Matching | <input type="checkbox"/> Enforce match When authenticating users, enforce a match between the common name of the client certificate and the username given at login. |
| Client Certificate Key Usage Validation | <input checked="" type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: 'TLS Web Client Authentication'). |

Tunnel Settings

| | |
|-------------------------------|--|
| IPv4 Tunnel Network | <input type="text" value="10.10.10.0/29"/> 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. 10.0.8.0/24). 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 | <input type="text"/> 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 | <input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel. |
| Redirect IPv6 Gateway | <input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel. |
| IPv4 Local network(s) | <input type="text" value="192.168.10.0/24"/> 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) | <input type="text"/> 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 | <input type="text"/> Specify the maximum number of clients allowed to concurrently connect to this server. |
| Allow Compression | <input type="text" value="Refuse any non-stub compression (Most secure)"/> Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traffic (e.g. VPN (e.g. HTTP)). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack. |

Client Settings

| | |
|-------------------|--|
| Dynamic IP | <input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes. |
| Topology | <input type="text" value="net30 -- Isolated /30 network per client"/> 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". |

Ping settings

| | |
|--------------------|---|
| Inactive | <input type="text" value="300"/> Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart. |
| Ping method | <input type="text" value="keepalive -- Use keepalive helper to define ping configuration"/> keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval ping-restart = timeout*2 push ping = interval push ping-restart = timeout |
| Interval | <input type="text" value="10"/> |
| Timeout | <input type="text" value="60"/> |

Advanced Client Settings

DNS Default Domain Provide a default domain name to clients

DNS Default Domain

DNS Server enable Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

DNS Server 2

DNS Server 3

DNS Server 4

Block Outside DNS Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable Provide an NTP server list to clients

NetBIOS enable Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Advanced Configuration

Custom options

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 certificate common name for purposes 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 platforms, and not compatible with OpenVPN bandwidth limiting.

Exit Notify

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Send/Receive Buffer

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation Both IPv4 only IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Activer Wind
Accédez aux para
activer Windows

Il ne reste qu'à valider avec Save et voilà.

Pour télécharger la configuration au format .ovpn, il est nécessaire d'installer un paquet supplémentaire sur le pare-feu.

Rendez-vous dans le menu suivant :

System -> Package Manager -> Available Packages.

Recherchez "openvpn" et installez le paquet : openvpn-client-export.
Lorsque c'est fait, retournez dans le menu OpenVPN puis dans l'onglet "Client Export".

Si vous souhaitez utiliser l'adresse IP publique pour vous connecter, utilisez l'option "Interface IP Address" pour l'option "Host Name Resolution". Il y a d'autres options possibles, notamment par nom de domaine.

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server: VPN-OPENVPN UDP4:1194

Client Connection Behavior

Host Name Resolution: Other

Host Name: 192.168.170.135
Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN: Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS: Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client: Do not include OpenVPN 2.5 and later settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer: Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode: Do not bind to the local port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage: Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage: Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate: Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption: High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windi...
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program.

Activer Windows
Accédez aux paramètres
activer Windows.

Les autres options peuvent être laissées par défaut... Il y a seulement notre option "auth-nocache" à reporter dans la section des options additionnelles.

Proxy Options

Use A Proxy Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options

`auth-nocache`

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.

EXAMPLE: remote-random;

[Save as default](#)

Search

Search term [Search](#) [Clear](#)

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

OpenVPN Clients

| User | Certificate Name | Export |
|------------------|------------------|---|
| itconnect.vpn.fb | VPN-SSL-RA-FB | <p>- Inline Configurations:</p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installer (2.4.9-1x01):</p> <p>7/8.1/2012/2 10/2016/2019</p> <p>- Old Windows Installers (2.3.18-1x02):</p> <p>x86-xp x64-xp x86-win6 x64-win6</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle Viscosity Inline Config</p> |

Enfin dans les packages ont peu du coup télécharger le client pour les postes distants.

Search

Search term [Search](#) [Clear](#)

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

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, TLS Encryption+Authentication, ECDH, LZ4 Compression and other non-legacy compression choices, IPv6 DNS servers, and more.

OpenVPN Clients

| User | Certificate Name | Export |
|------------------|------------------|---|
| itconnect.vpn.fb | VPN-SSL-RA-FB | <p>- Inline Configurations:</p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installer (2.4.9-1x01):</p> <p>7/8.1/2012/2 10/2016/2019</p> <p>- Old Windows Installers (2.3.18-1x02):</p> <p>x86-xp x64-xp x86-win6 x64-win6</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle Viscosity Inline Config</p> |

CONCLUSION

Voilà les utilisateurs peuvent maintenant se connecter avec leur compte Active Directory au VPN via une connexion internet et ainsi accéder aux ressources de l'entreprise.

Voici donc maintenant le schéma de l'infrastructure :

