Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Justice and Police FDJP

Post and Telecommunications Surveillance Service PTSS

IP-based Delivery Network via OpenVPN - Provider Handbook

Date: 23 July 2018

Version 1.9

Address and contact:

Post and Telecommunications Surveillance Service PTSS
Fellerstrasse 15
3003 Bern, Switzerland

Contact: https://www.li.admin.ch/

Table of contents

1. Scope of the Document

This handbook provides information regarding the setup and the correct operation of the IP-based Delivery Network via OpenVPN according to VD-ÜPF Anhang 02 [2], section 8.2.1

Its intended audience is any CSP implementing this delivery method.

2. Abbreviations

CA	Certificate Authority
CSP	Communications Service Provider
FDJP	Federal Department of Justice and Police
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC-FDJP	IT Service Centre, Federal Department of Justice and Police
ISS	Interception System Schweiz
LEMF	Law Enforcement Monitoring Facility
MF	Mediation Function
NAT	Network Address Translation
PTSS	Post and Telecommunications Surveillance Service
VPN	Virtual Private Network

3. Terminology

Law Enforcement Monitoring Facility (LEMF)
Designates the transmission destination for the results of interception relating to a particular interception subject. PTSS operates the LEMF in Switzerland.

Mediation Function (MF)
Mechanism which passes information between a CSP and a Handover Interface, and information between the Internal Network Interface and the Handover Interface.

VPN client
The VPN client is part of the CSP’s infrastructure and it connects to the VPN endpoint.

VPN endpoint
The VPN endpoint is part of the IP-based Delivery Network via OpenVPN and it acts as a server for the VPN connections of the CSP. It is operated by PTSS.

4. References

[1]	VD-ÜPF Anhang 01	Technical requirements for the delivery networks for the conduct of the Surveillance of Telecommunications, Annex 1, Version 1, 1 March 2018
[2]	VD-ÜPF Anhang 02	Technical requirements for the delivery networks for the conduct of the Surveillance of Telecommunication, Annex 2, Version 1, 1 March 2018
[3]	RFC1918	Address Allocation for Private Internets, February 1996

5. OpenVPN Concept

The OpenVPN based delivery network is one of the proposed variants for IP based delivery of interception results from the CSP to the LEMF described in [2] (section 8.2.1, variant A).

IP based delivery of interception results is generally used to transmit

- HI1 information via FTP transfer;
- HI2 information via FTP transfer;
- HI2 and HI3 information via TCP stream.

5.1. PTSS (Server) Side

5.1.1. VPN Nodes

For redundancy and maintenance reasons, PTSS operates two OpenVPN server nodes, which are designated:

- “node1” and
- “node2”.

Each node can be reached at its own dedicated public IP address (using the same UDP port number).

5.1.2. VPN Instances

OpenVPN is used in tunnelling mode, which implies using IP addresses inside the VPN tunnel. In order to avoid conflicts with the CSP’s own network, PTSS allows the CSP to choose from four distinct instances; each instance is configured with a different private (RFC1918 [3]) network. The instances are designated:

- “instanceA”,
- “instanceB”,
- “instanceC”,
- “instanceD”.

Each instance is available on both nodes, thus allowing failover from one node to the other (see Table 1: VPN instances and corresponding IP ranges). Each instance is reached over a distinct destination port.

5.2. CSP (Client) Side

5.2.1. Failover

OpenVPN clients must automatically try reconnecting to both nodes whenever needed.

OpenVPN clients must be configured to always connect to the same predefined VPN instance (port number). In case of a failure to connect to one node, then a failover must be executed towards the same instance of the other node.

The OpenVPN client has a basic form of load balancing and failover built in, making failover configuration simple for the CSP. If the CSP ensures that both nodes are configured in the OpenVPN config file (two “remote” entries, one for each node, with different IP addresses and the same port numbers) then the OpenVPN client, under normal operation, will randomly choose one node or the other, and in the case of a failure of one node, the OpenVPN client will automatically fallback to the available node.

5.2.2. Instance and Client IP Range Selection

Each OpenVPN client certificate is tied to one instance only.

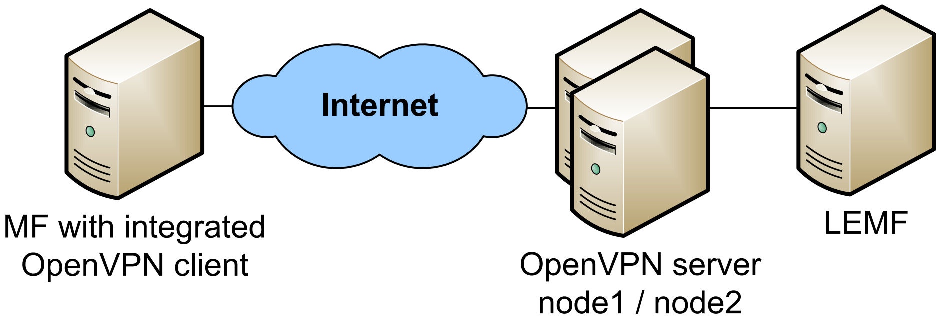
The CSP must communicate to PTSS which instance they intend to use prior to the certificate being issued. PTSS will deliver the certificate once the proper reservation has been made on that instance.

5.2.3. Installation Architecture

There are two proposed installation alternatives: the OpenVPN client can either be installed on the same machine as the MF, or on a dedicated machine.

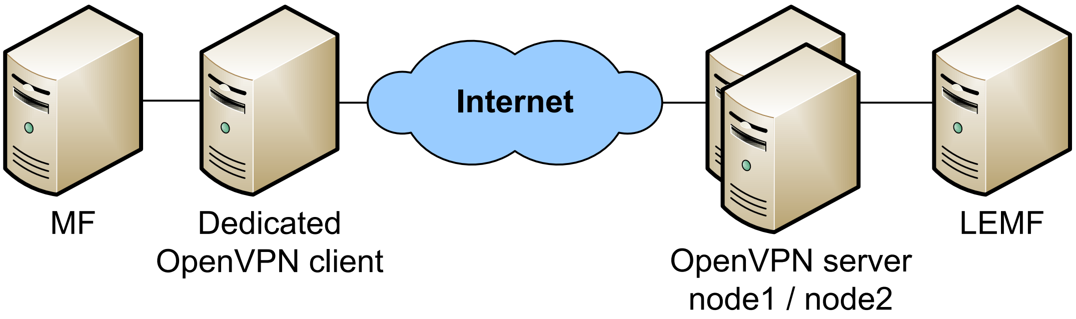
5.2.3.1. OpenVPN Client on MF

In this configuration, the OpenVPN client is installed on the same machine as – typically – the mediation function. This alternative requires the least effort.


Internet
MF with integrated OpenVPN client
OpenVPN server node1 / node2
LEMF

5.2.3.2. Dedicated OpenVPN Client

In this configuration, the OpenVPN client is installed on a dedicated machine. This alternative requires more effort as care must be taken to configure the correct routing; NAT (masquerading) may be required.



5.3. Destinations

All systems at PTSS receiving data on the standard ETSI Handover Interfaces can be reached via one unique tunnel. If required, additional tunnels can be setup by the CSP subject to the approval of PTSS. A separate client certificate and key is required for each client instance.

6. IP Addressing and Security Features

6.1. Addressing

6.1.1. VPN endpoints

The IP addresses for both nodes as well as the UDP ports for each instance will be provided by PTSS to the CSP together with the client certificates and keys.

In order to ensure a high quality of service (QoS), the CSP has to provide PTSS with a list of source IP addresses used for the VPN client.

6.1.2. IP addresses within the VPN tunnel

The CSP's IP address within the VPN tunnel is allocated automatically during the handshake when establishing the connection. The VPN client uses the IP address assigned by the VPN endpoint (OpenVPN Server).

The addresses used within the VPN are allocated according to RFC1918 [3]. Each VPN client receives such an address for its virtual network interface towards the VPN tunnel. The CSP can choose from 4 different VPN instances which use different RFC1918 ranges (see also 5.2.2).

VPN instance	RFC1918 Range
instanceA	10.1.141.0/24
instanceB	10.3.141.0/24
instanceC	10.198.57.0/24
instanceD	192.168.152.64/26

Table 1: VPN instances and corresponding IP ranges

The purpose of the 4 different ranges is to prevent conflicts with the internal addressing of the CSP. Each CSP can decide which VPN instance to use. The ranges within the VPN will not change in the foreseeable future.

The VPN tunnel IP addresses do not change, even in the event of a VPN node failover. In the event that the VPN connection fails, the CSP shall periodically (approximately every 5 seconds) try to re-establish the connection. This failover mechanism is an automatic function of the OpenVPN client if it is set up with multiple remote hosts. The CSP may also use redundant VPN clients at its own discretion.

The allocation of an IP address to a CSP is defined statically on the VPN endpoint but PTSS can modify this allocation. When setting up the VPN connection, a CSP must therefore not assume that it will receive the same IP address every time, and take this into account in its configuration (see also 8.2).

6.1.3. IPv6

Currently only IPv4 is supported.

6.2. Security Features

Using OpenVPN ensures that the data transmitted over the Internet is encrypted. The encryption is done with the AES algorithm with at least 256 bit key length. Additionally, an integrity check of the transmitted data is performed in order to detect manipulations.

In order for the client to authenticate at the VPN endpoint, each CSP receives:

- One «TLS Auth Key» (tlsauth.pem) which is used for the authentication of the TLS handshake
- A copy of the root CA certificate (ca.crt), plus a client certificate (client.crt) and the corresponding private key (client.key)

These files must be placed in the appropriate location on the client (according to the paths set in the OpenVPN client configuration file) in order for the client to successfully authenticate at the VPN endpoint. The client keys are considered secret, therefore the CSP is obliged to appropriately protect the keys from misuse and to make sure that they are not accessible to third parties.

After a VPN client has successfully authenticated itself to the VPN endpoint, individual encryption session keys are periodically negotiated. The method for generating the session key complies with the Perfect Forward Secrecy principle.

7. Setup process

The different steps for setting up the OpenVPN based delivery network are as follows:

1. A prerequisite is that a secure communication channel has been established between the CSP and PTSS, using OpenPGP encrypted e-mail according to [1], section 4.3.

2. The CSP contacts PTSS and requests a client certificate. The request must include the VPN instance chosen by the CSP (see 5.2.2 and 6.1.2) as well as the list of source IP addresses that will be used by the VPN client (see 6.1.1).

3. PTSS issues the client certificate and provides it to the CSP along with

- the security elements listed in 6.2;
- the IP addresses for both nodes as well as the UDP port for the instance;
- a sample configuration file.

4. The CSP configures the VPN endpoint.

8. OpenVPN Configuration

8.1. Configuration File for the OpenVPN Client

A sample OpenVPN configuration file is shown below for reference. A CSP must adapt this configuration to its installation of the OpenVPN client.

```
# Define OpenVPN as a client, “tun” device as virtual tunnel interface and
# UDP as the transport protocol
client
dev tun0
proto udp

# Configure the IP addresses and port of the VPN endpoints (remote)
# see VPN endpoints list and IP ranges table
remote-random
remote xxx.xxx.xxx.xxx pppp
remote yyy.yyy.yyy.yyy pppp

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.
resolv-retry infinite

# Do not bind to local address and port
nobind

# Define the username and group of the OpenVPN client
user nobody
group nogroup

# Re-use the key and the "tun" device each time the connection is
# re-established
persist-key
persist-tun

# Limit the size of the UDP packets to max. 1300 bytes (MTU) within the tunnel
fragment 1300

# Path to the CA certificate
ca /path/to/ca.crt

# Path to the client certificate
cert /path/to/client.crt

# Path to the Client-Private-Key
key /path/to/client.key

# Path to the TLS-Auth Key
tls-auth /path/to/tlsauth.pem 1
```

```
# Ensure that the client only connects to a host which is a designated
# server. This is an important security precaution to protect against a
# man-in-the-middle attack where an authorized client attempts to connect
# to another client by impersonating the server.
ns-cert-type server

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-CBC
auth SHA512

#Set the client to use tls and set it to a client role in the TLS negotiation
tls-client

# Use fast LZO compression - mandatory
comp-lzo

# Set log output verbosity level to 3. Level 3 is recommended if
# you want a good summary of what's happening without being swamped by
# output. (see OpenVPN manual for details)
verb 3
```

Table 2: Configuration file of a VPN client

8.2. Client configuration considerations

In general, it makes sense to run the VPN client under a dedicated user account. This way, the Least Privilege Principle is applied. It is wise not to grant administrator or other special rights to the VPN client.

All keys which the CSP receives from PTSS must be stored as clear text on the system with the VPN client in order to establish the VPN connection. Care must be taken to prevent the theft of the keys. This can be achieved by granting limited access rights on the file system (for example exclusive read access for the dedicated user account of the OpenVPN client).

The CSP can implement the VPN client according to its own security policy. The two proposals above are recommendations. However, PTSS requires the CSP to adequately protect the VPN keys from theft. In the event that a key has been compromised, the CSP must inform PTSS immediately so that the certificate can be revoked.

Particular care must be taken when the IP address assigned to the VPN virtual interface changes. On some operating systems, re-configuring the VPN tunnel with another IP address causes a connection loss: the client could stop when it gets a new address from the server. Therefore, the CSP must prepare its VPN system for such events by implementing appropriate monitoring and ensuring prompt automatic re-establishment of the VPN connection.