

Procédure de configuration des équipements

Auteur: Bagassien Stephen

Référence : Assurmer

Date : 04/2024



SOMMAIRE

Table des matières

Installation de l'agent checkMK **Erreur ! Signet non défini.**

Procédure de configuration des équipements

OpenVPN

Prérequis :

- Un pare-Feu Netgate sg-3100
- Un accès Internet

Étapes pour l'installation :

- a. Génération des certificats d'autorité et de serveur.

The screenshot shows the Mikrotik WinBox interface for the Certificate Manager. The breadcrumb navigation is "System / Certificate Manager / Certificates / Edit". The "Certificates" tab is active. The main section is "Add/Sign a New Certificate".

Add/Sign a New Certificate

Method: Create an Internal Certificate

Descriptive name: [Empty field]

Internal Certificate

Certificate authority: ASM-CERTIF

Key type: RSA

Key Length: 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 (Days): 3650
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.

Common Name: ASM-VPN-CERTIF

The following certificate subject components are optional and may be left blank.

Country Code: FR

State or Province: e.g. Texas

City: e.g. Austin

Organization: e.g. My Company Inc

Organizational Unit: e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes: The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type: Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names: FQDN or Hostname [Empty field]
Type: [Empty field] Value: [Empty field]

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Search

Search term Both

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
ASM-CERTIF	<input checked="" type="checkbox"/>	self-signed	2	CN=internal-ca, C=FR Valid from: Fri, 17 Feb 2023 22:23:54 +0100 Valid until: Mon, 14 Feb 2033 22:23:54 +0100	OpenVPN Server	

b. Création d'un utilisateur avec son certificat associé.

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username:

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:
Member of

Not member of

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

Certificate: Click to create a user certificate

c. Mise en place d'un serveur OpenVPN

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

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)

Backend for authentication Local Database

Device mode tun - Layer 3 Tunnel 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 UDP on IPv4 only

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

Local port 1195

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 ASM-CERTIF

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 ASM-VPN (Server: Yes, CA: ASM-CERTIF, in Use)

DH Parameter Length 2048 bit
Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

ECDH Curve Use Default
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 Negotiation Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data Encryption Algorithms

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

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.

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 first 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.

Allow Compression

Allow compression to be used with this VPN instance.

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".

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".

Ping settings

Inactive

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

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

Timeout

Advanced Client Settings

DNS Default Domain

 Provide a default domain name to clients

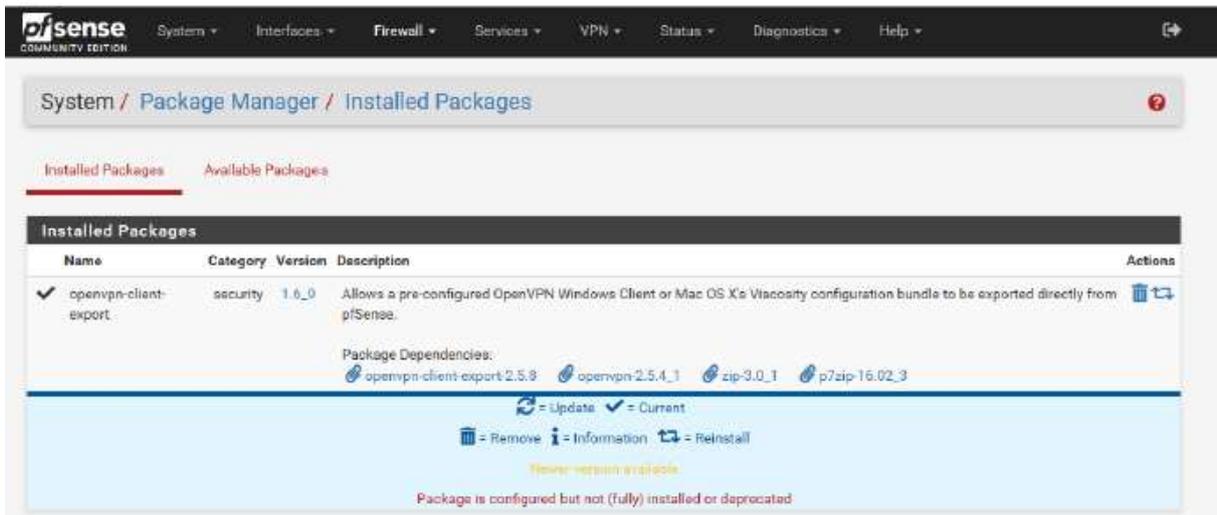
DNS Default Domain

DNS Server enable

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

DNS Server 1

d. Installation du package « openvpn-client-export »



e. Configuration des règles de pare-feu pour permettre l'accès à la DMZ depuis le VPN



Exportation et déploiement du client sur l'utilisateur distant

