MSCYBER#04 - Sécurité des accès distants sur les architectures hybrides

En tant que administrateur Infrastructure Sécurisée, vous devez préparer un modèle de fichier de configuration pour sécuriser les connexions distantes sur les serveurs GNU/Linux de l'entreprise, qu'ils soient hébergés en propre par l'entreprise ou dans le cloud.

Authors

Roblot Jean-Philippe - jroblot.simplon@proton.me
Drula Kevin - k.drula.simplon@proton.me

Version

18/01/2024 - V1R0

Releases

PFsense 2.7.2 Ubuntu Server LTS 22.04 Apache 2.4.52 OpenVPN GUI 2.6.8

Powered by https://shields.io

1. PREPARATION

Installation d'une machine virtuelle Ubuntu Server via VirtualBox
Carte réseau en mode Pont
TCP/IP statique 10.0.5.10

Machine serveur

- GNU/Linux/UBUNTU Server LTS 22.04
- vCPU : 2 core
- vRAM 8Go
- vHDD : 40Go
- @ip : 10.0.5.1/24

Machine client

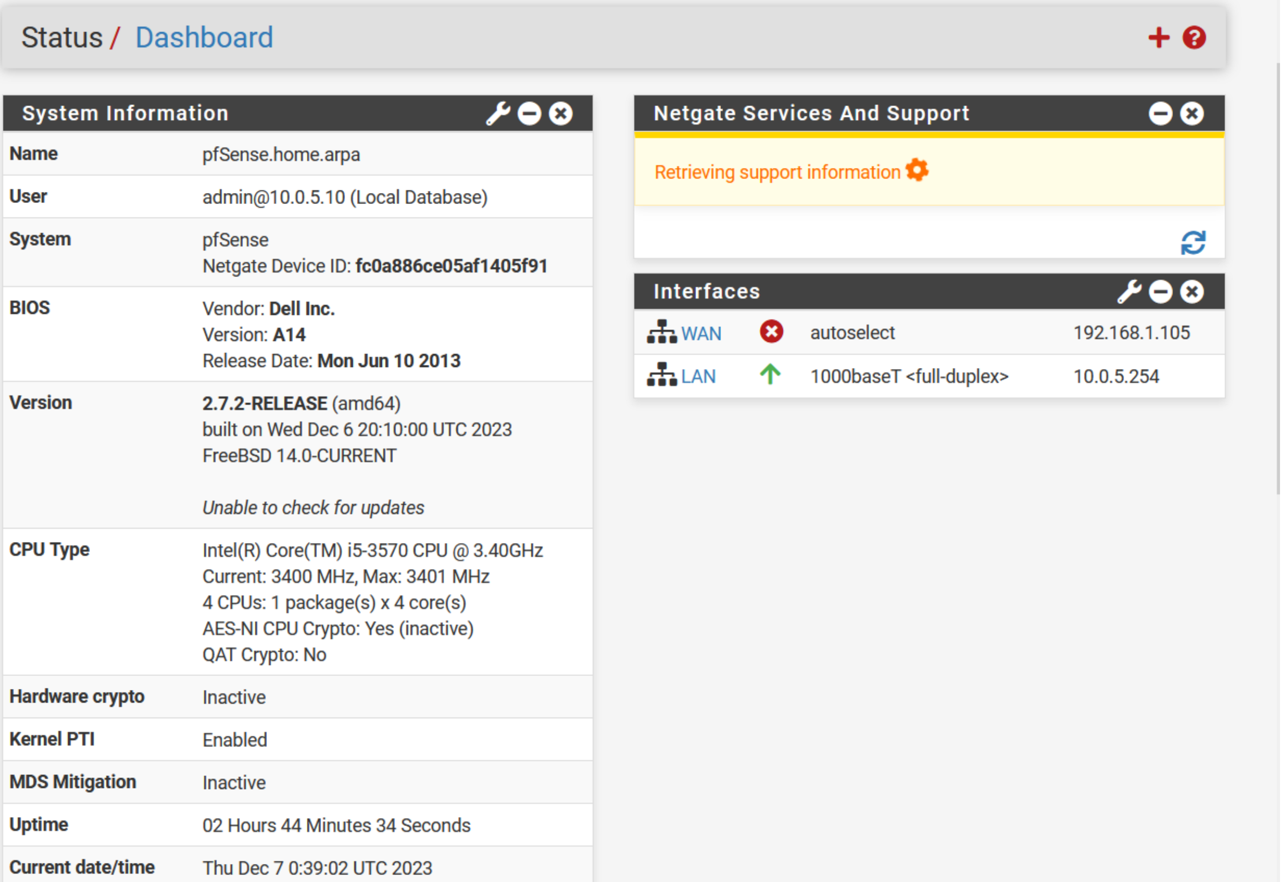
- Laptop Windows 10 Pro Version 22h2
- Nom : GDO-PC-PF1M1RXE
- CPU : 6 core
- RAM 32Go
- SSD : 512Go
- @ip : 10.0.5.10

Activités

- Installer PFsense sur une machine physique via l'ISO officielle v2.7.2 depuis une clé USB bootable. Format de fichiers ZFS.
- Paramétrer les deux interfaces de la machine en leur attribuant une IP

```
WAN -> em0 -> v4: 192.168.1.105/24
LAN -> bge0 -> v4: 10.0.5.254/24
```

- Connecter notre machine client en local via navigateur afin de bénéficier de la GUI



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@10.0.5.10 (Local Database)
System	pfSense Netgate Device ID: **fc0a886ce05af1405f91**
BIOS	Vendor: **Dell Inc.** Version: **A14** Release Date: **Mon Jun 10 2013**
Version	**2.7.2-RELEASE** (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT *Unable to check for updates*
CPU Type	Intel(R) Core(TM) i5-3570 CPU @ 3.40GHz Current: 3400 MHz, Max: 3401 MHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	02 Hours 44 Minutes 34 Seconds
Current date/time	Thu Dec 7 0:39:02 UTC 2023

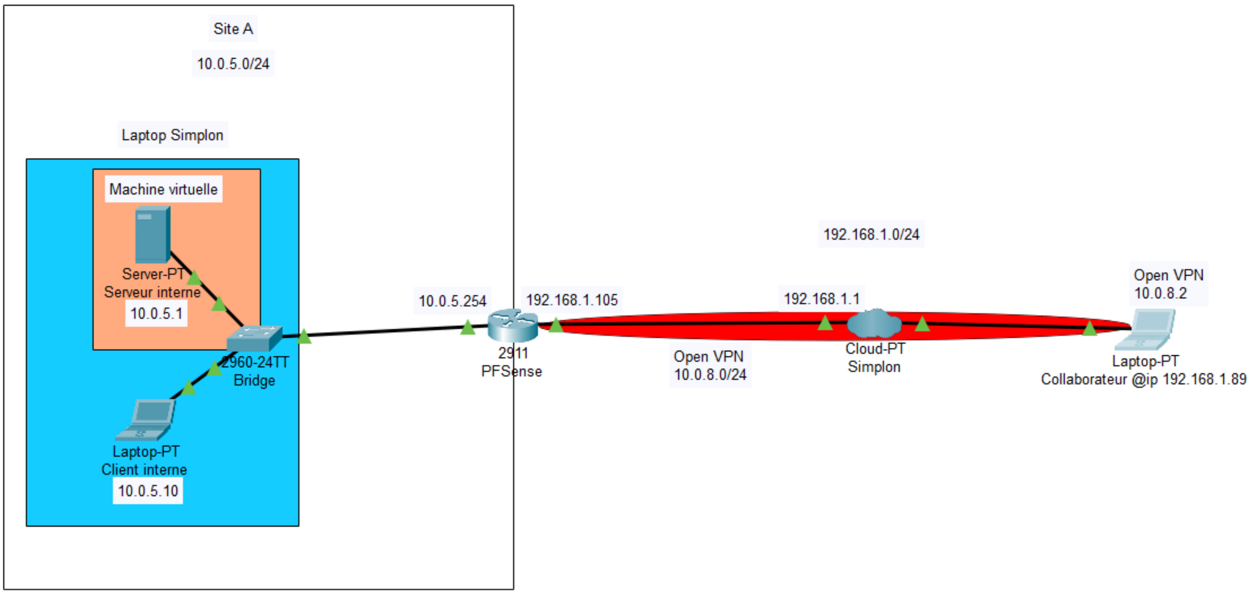
Netgate Services And Support

Retrieving support information

Interfaces

WAN	✗	autoselect	192.168.1.105
LAN	↑	1000baseT <full-duplex>	10.0.5.254

- Production d'un schéma logique du réseau sur Cisco Packet Tracer



- Paramétrer une machine virtuelle Ubuntu Server avec connexion par pont afin de déployer notre réseau local selon les contraintes
  - Le routeur pfsense
  - Un serveur Web
  - Une machine client W10 Pro
- Vérifier le fonctionnement du serveur web sur le réseau local
  - Ping du serveur depuis le client

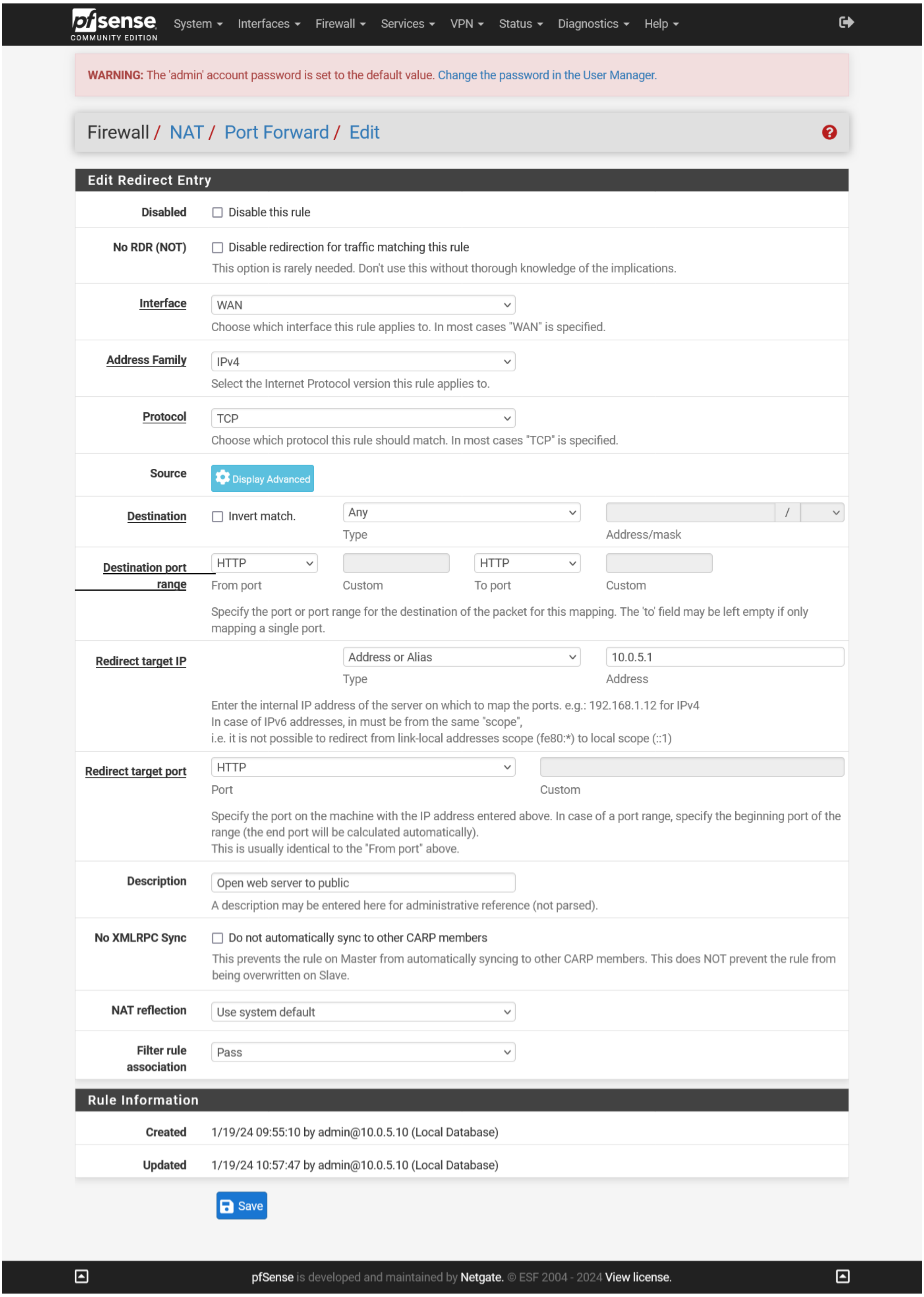
    ```
    C:\Users\Utilisateur>ping 10.0.5.1

    Envoi d’une requête 'Ping'  10.0.5.1 avec 32 octets de données :
    Réponse de 10.0.5.1 : octets=32 temps<1ms TTL=64
    Réponse de 10.0.5.1 : octets=32 temps=1 ms TTL=64
    Réponse de 10.0.5.1 : octets=32 temps=1 ms TTL=64
    Réponse de 10.0.5.1 : octets=32 temps=1 ms TTL=64

    Statistiques Ping pour 10.0.5.1:
      Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
      Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
    ```

  - Ping du routeur depuis le serveur ok
- A ce stade, nôtre serveur n'a pas la fonctionnalité serveur web, nous devons l'implémenter

  ```
  sudo apt install apache2

  sudo ufw app list # Affiche les profils d’application ufw disponibles
  ----------------------------------------------------------------------------
  --
  # Sortie
  Available applications:
  Apache
  Apache Full
  Apache Secure
  ----------------------------------------------------------------------------
  --
  sudo ufw allow 'Apache'
  # profil le plus restrictif qui permettra toujours le trafic que vous
  # avez configuré, en autorisant le trafic sur le port 80
  #(trafic web normal, non crypté)

  sudo ufw status # Vérifier notre config
  ----------------------------------------------------------------------------
  --
  #Sortie
  Status: active

  To                         Action      From
  --                         ------      ----
  ```

```
Apache                     ALLOW       Anywhere
Apache (v6)                ALLOW       Anywhere (v6)
----------------------------------------------------------------------------
--

sudo systemctl status apache2 # Vérifie que le service fonctionne

http://your_server_ip # Affiche la page d'accueil
```

- Rendre le serveur web accessible au public
  A ce stade, notre page d'acceuil est uniquement accessible dans le LAN
  - Paramétrer une redirection de port sur pfsense afin de permettre l'affichage de la page web depuis l'extérieur



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

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

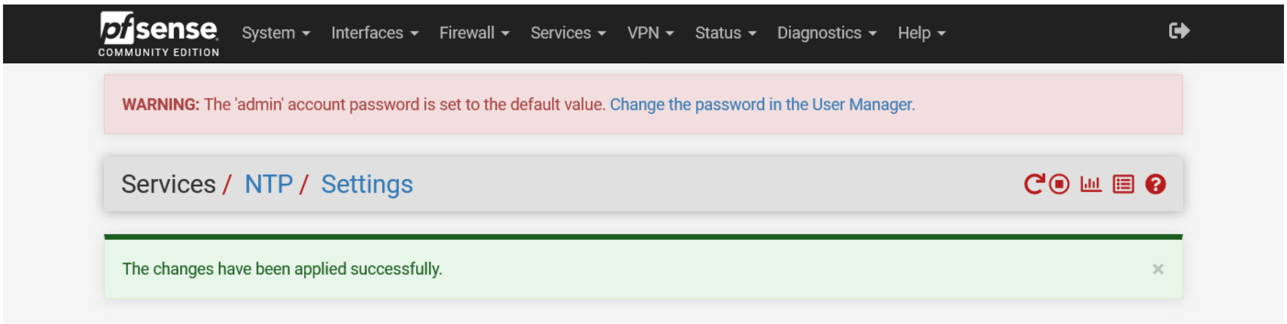
Disabled	□ Disable this rule
No RDR (NOT)	□ Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which protocol this rule should match. In most cases "TCP" is specified.
Source	Display Advanced
Destination	□ Invert match. Type: Any Address/mask: /
Destination port range	From port: HTTP Custom: To port: HTTP Custom: Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP	Type: Address or Alias Address: 10.0.5.1 Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, in must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)
Redirect target port	Port: HTTP Custom: Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.
Description	Open web server to public A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync	□ Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default
Filter rule association	Pass

Rule Information

Created	1/19/24 09:55:10 by admin@10.0.5.10 (Local Database)
Updated	1/19/24 10:57:47 by admin@10.0.5.10 (Local Database)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

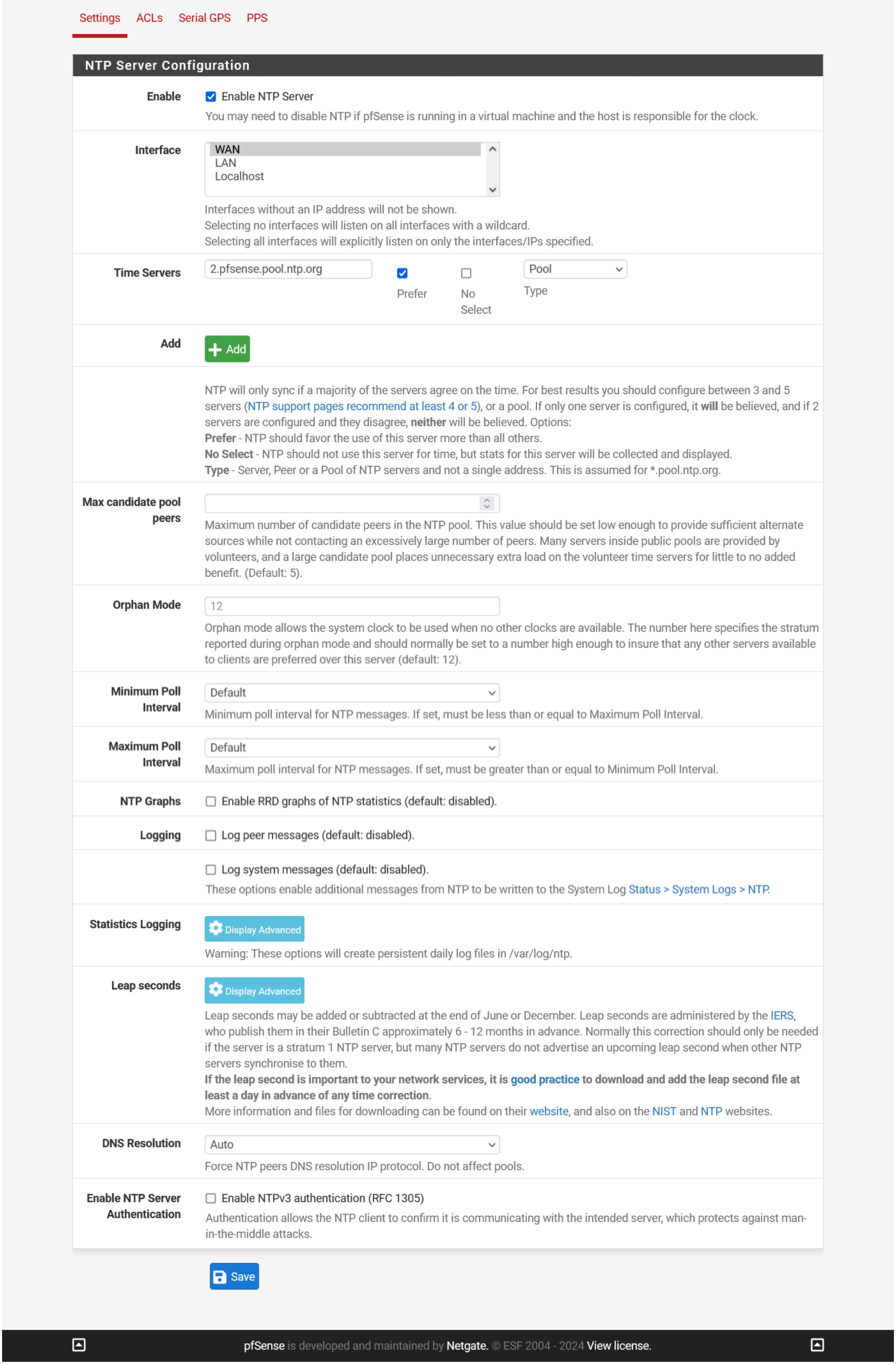
- Paramétrer le NTP



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

Services / NTP / Settings

The changes have been applied successfully.



NTP Server Configuration

Enable ☑ Enable NTP Server

You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.

Interface

WAN
LAN
Localhost

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers 2.pfsense.pool.ntp.org ☑ Prefer ☐ No Select Pool Type

Add + Add

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:
Prefer - NTP should favor the use of this server more than all others.
No Select - NTP should not use this server for time, but stats for this server will be collected and displayed.
Type - Server, Peer or a Pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.

Max candidate pool peers

Maximum number of candidate peers in the NTP pool. This value should be set low enough to provide sufficient alternate sources while not contacting an excessively large number of peers. Many servers inside public pools are provided by volunteers, and a large candidate pool places unnecessary extra load on the volunteer time servers for little to no added benefit. (Default: 5).

Orphan Mode 12

Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server (default: 12).

Minimum Poll Interval Default

Minimum poll interval for NTP messages. If set, must be less than or equal to Maximum Poll Interval.

Maximum Poll Interval Default

Maximum poll interval for NTP messages. If set, must be greater than or equal to Minimum Poll Interval.

NTP Graphs ☐ Enable RRD graphs of NTP statistics (default: disabled).

Logging ☐ Log peer messages (default: disabled).

☐ Log system messages (default: disabled).

These options enable additional messages from NTP to be written to the System Log Status > System Logs > NTP.

Statistics Logging Display Advanced

Warning: These options will create persistent daily log files in /var/log/ntp.

Leap seconds Display Advanced

Leap seconds may be added or subtracted at the end of June or December. Leap seconds are administered by the IERS, who publish them in their Bulletin C approximately 6 - 12 months in advance. Normally this correction should only be needed if the server is a stratum 1 NTP server, but many NTP servers do not advertise an upcoming leap second when other NTP servers synchronise to them.
If the leap second is important to your network services, it is good practice to download and add the leap second file at least a day in advance of any time correction.
More information and files for downloading can be found on their website, and also on the NIST and NTP websites.

DNS Resolution Auto

Force NTP peers DNS resolution IP protocol. Do not affect pools.

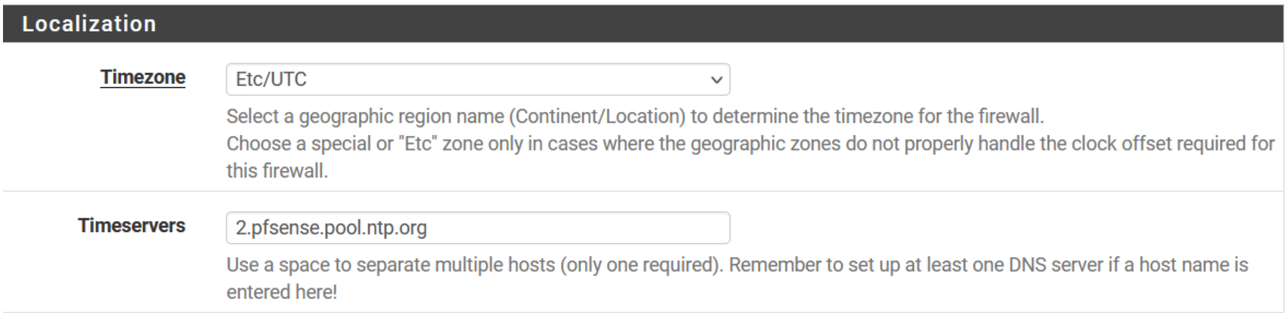
Enable NTP Server Authentication ☐ Enable NTPv3 authentication (RFC 1305)

Authentication allows the NTP client to confirm it is communicating with the intended server, which protects against man-in-the-middle attacks.

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

- Régler le fuseau horaire du routeur (System => General setup)

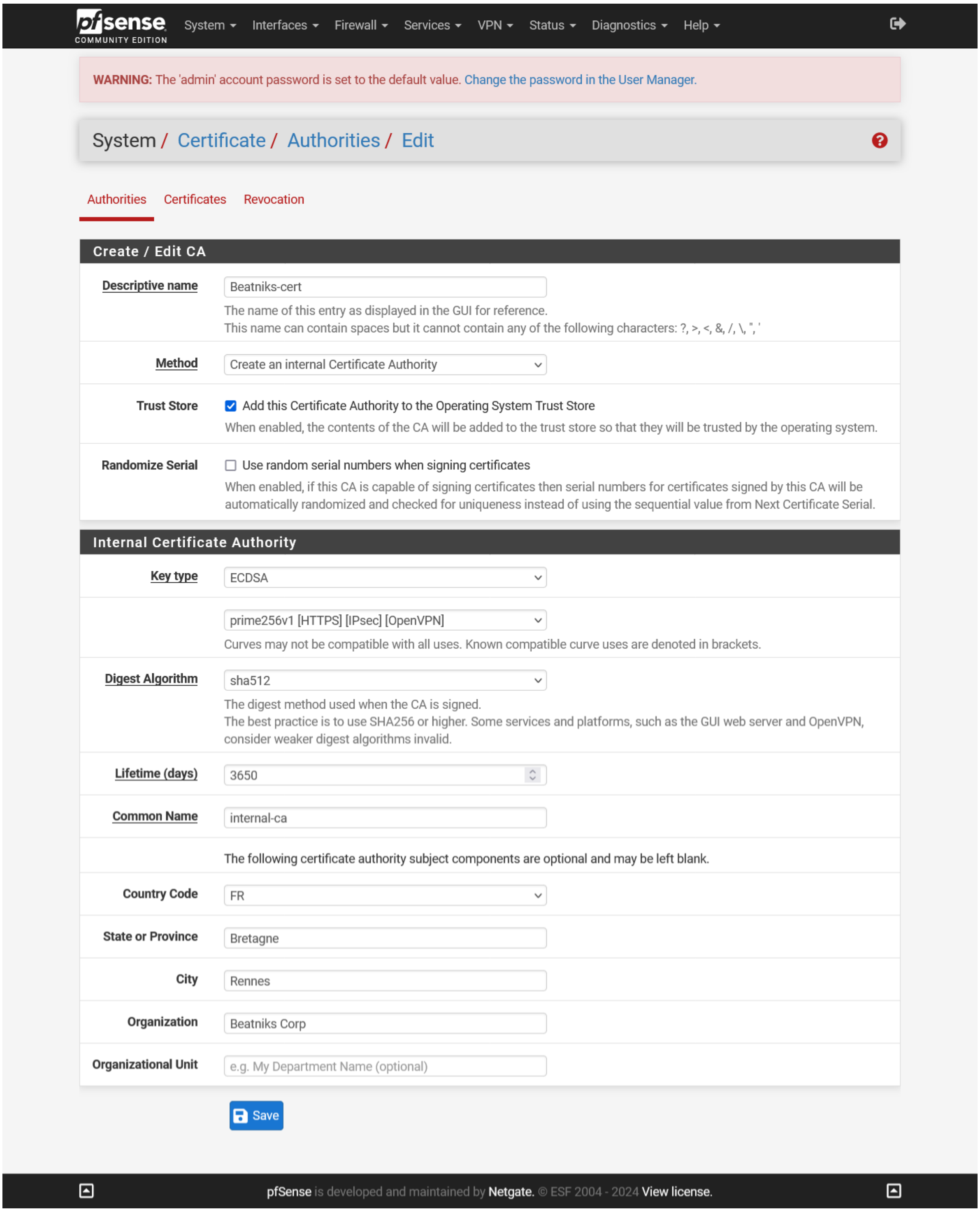


Localization

Timezone: Etc/UTC
Select a geographic region name (Continent/Location) to determine the timezone for the firewall.
Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

Timeservers: 2.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

- Dans l'optique de configurer un VPN afin de permettre aux collaborateurs de travailler à distance, nous devons effectuer plusieurs actions. Nous nous appuirons ici sur les recommandations de l'ANSSI pour les différentes configurations.
    - Créer une CA et son certificat



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

System / Certificate / Authorities / Edit

Create / Edit CA

Descriptive name: Beatniks-cert
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: ?, >, <, &, /, \, ", '

Method: Create an internal Certificate Authority

Trust Store: ☑ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: ☐ Use random serial numbers when signing certificates
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.

Internal Certificate Authority

Key type: ECDSA

prime256v1 [HTTPS] [IPsec] [OpenVPN]
Curves may not be compatible with all uses. Known compatible curve uses are denoted in brackets.

Digest Algorithm: sha512
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days): 3650

Common Name: internal-ca

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

Country Code: FR

State or Province: Bretagne

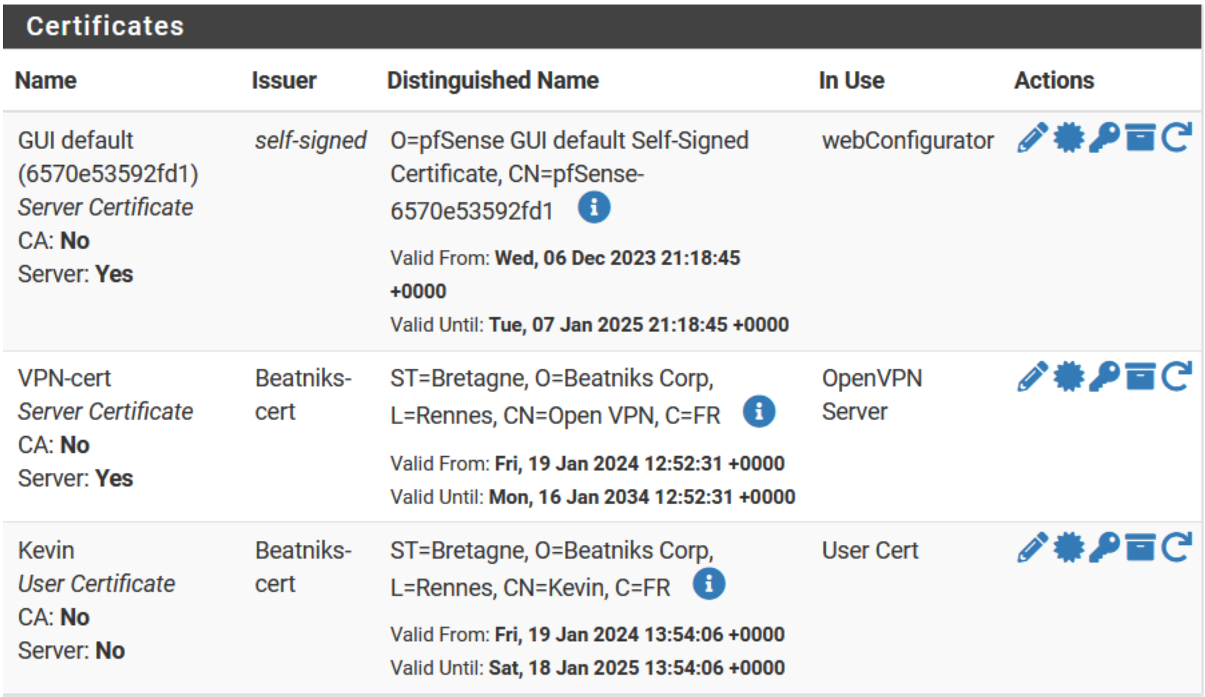
City: Rennes

Organization: Beatniks Corp

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

Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

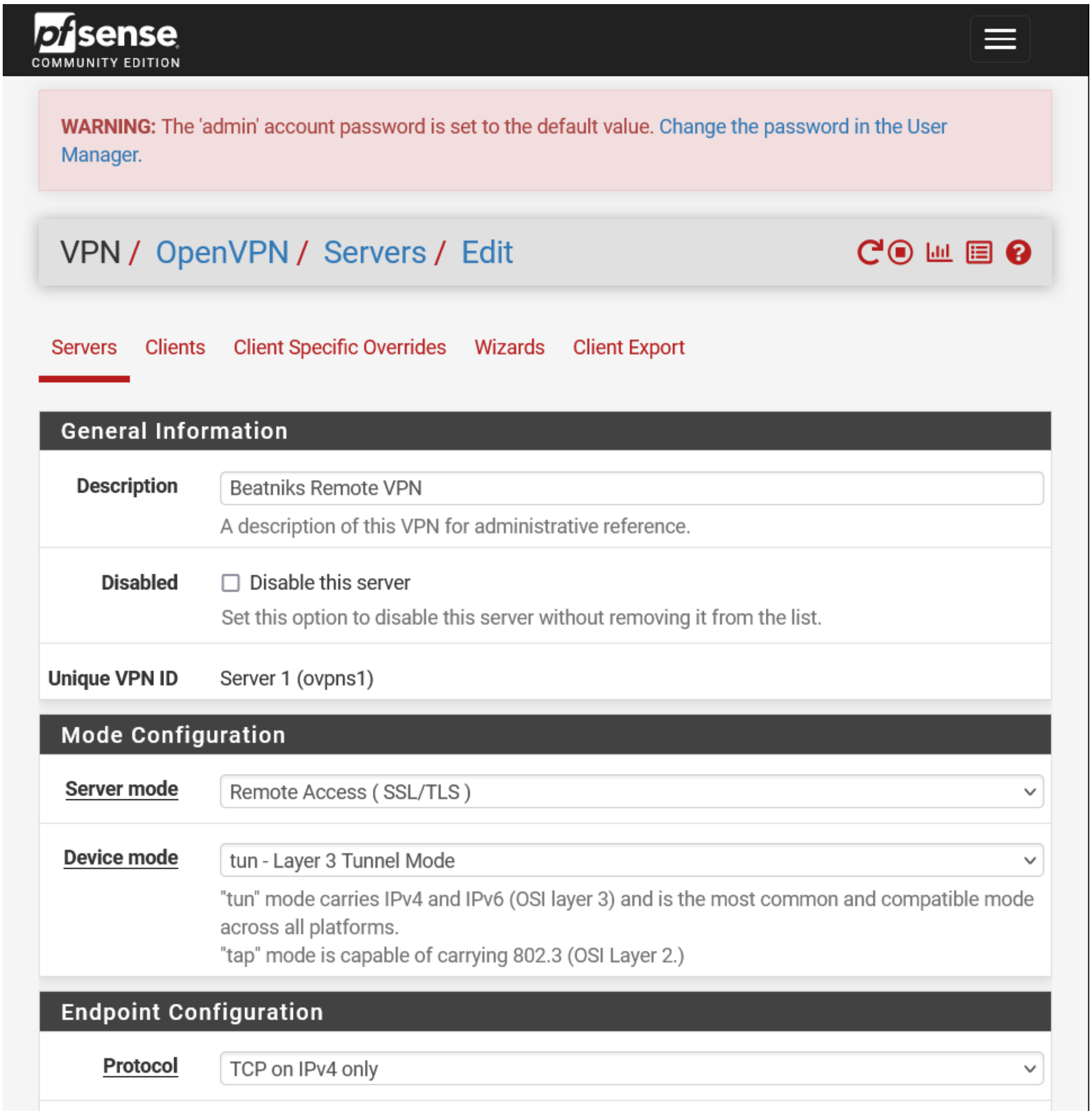
- Générer un certificat pour le serveur VPN
- Créer un utilisateur et son certificat



Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6570e53592fd1) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6570e53592fd1 Valid From: **Wed, 06 Dec 2023 21:18:45 +0000** Valid Until: **Tue, 07 Jan 2025 21:18:45 +0000**	webConfigurator	
VPN-cert *Server Certificate* CA: **No** Server: **Yes**	Beatniks-cert	ST=Bretagne, O=Beatniks Corp, L=Rennes, CN=Open VPN, C=FR Valid From: **Fri, 19 Jan 2024 12:52:31 +0000** Valid Until: **Mon, 16 Jan 2034 12:52:31 +0000**	OpenVPN Server	
Kevin *User Certificate* CA: **No** Server: **No**	Beatniks-cert	ST=Bretagne, O=Beatniks Corp, L=Rennes, CN=Kevin, C=FR Valid From: **Fri, 19 Jan 2024 13:54:06 +0000** Valid Until: **Sat, 18 Jan 2025 13:54:06 +0000**	User Cert	

- Créer notre serveur OpenVPN



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

VPN / OpenVPN / Servers / Edit

General Information

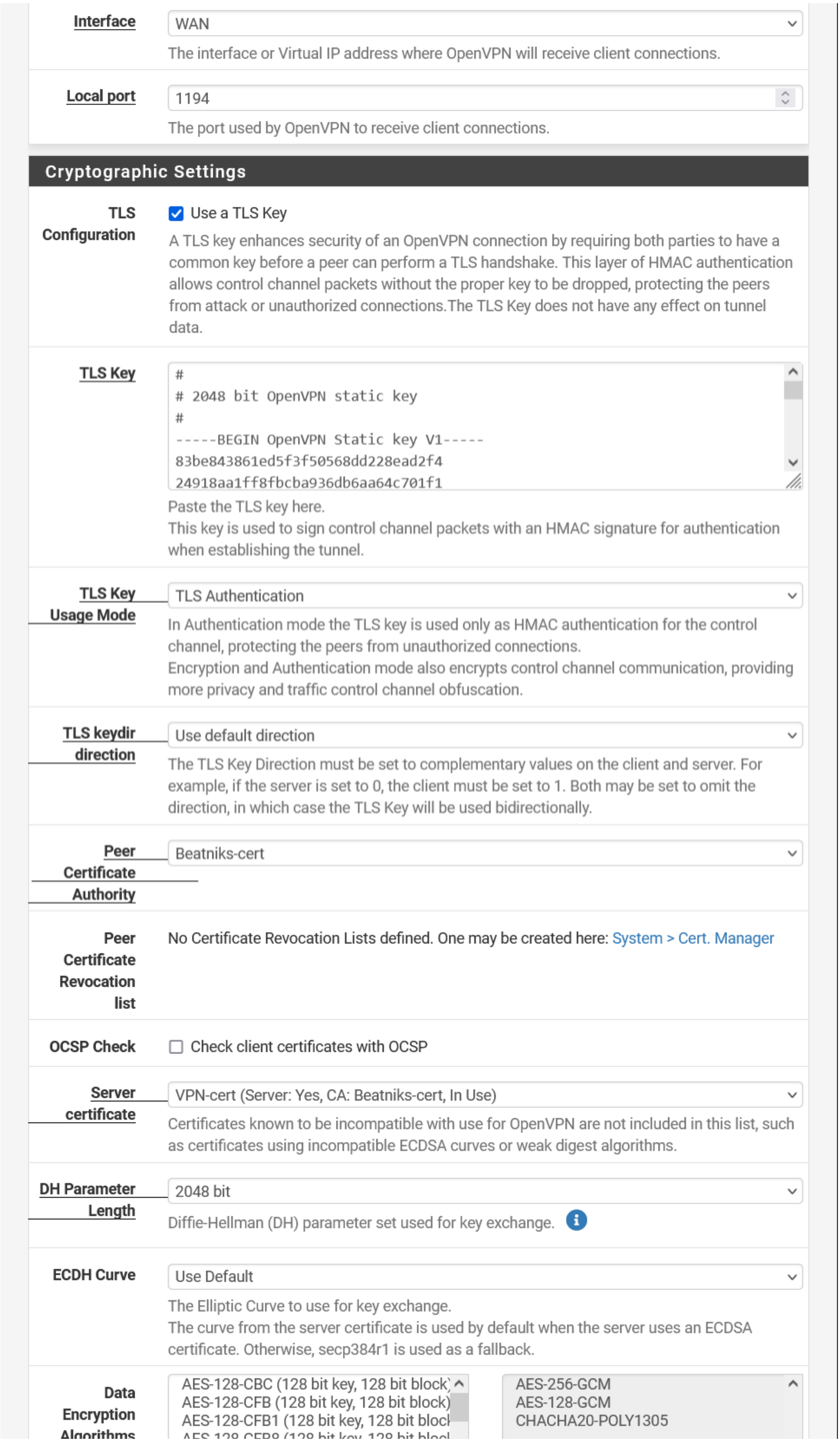
Description	Beatniks Remote VPN A description of this VPN for administrative reference.
Disabled	☐ Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 1 (ovpns1)

Mode Configuration

Server mode	Remote Access (SSL/TLS)
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	TCP on IPv4 only



Interface: WAN

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

Local port: 1194

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.

TLS Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
83be843861ed5f3f50568dd228ead2f4
24918aa1ff8fbcba936db6aa64c701f1
```

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode: TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections.
Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction: Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority: Beatniks-cert

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: VPN-cert (Server: Yes, CA: Beatniks-cert, In Use)

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.

DH Parameter Length: 2048 bit

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

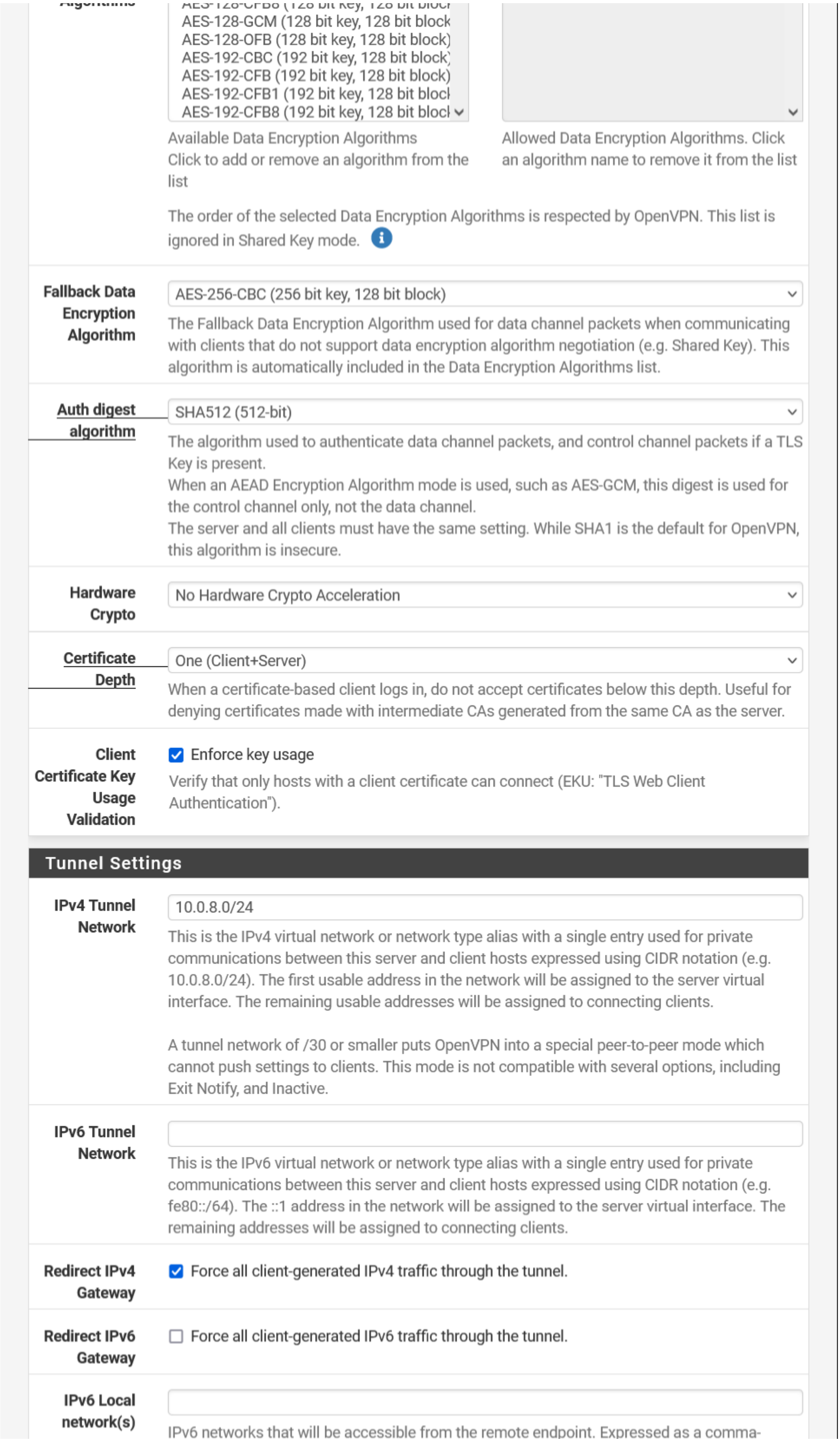
ECDH Curve: Use Default

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



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-192-CFB8 (192 bit key, 128 bit block

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

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: AES-256-CBC (256 bit key, 128 bit block)

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: SHA512 (512-bit)

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: No Hardware Crypto Acceleration

Certificate Depth: 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.

Client Certificate Key Usage Validation: ☑ Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network: 10.0.8.0/24

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:

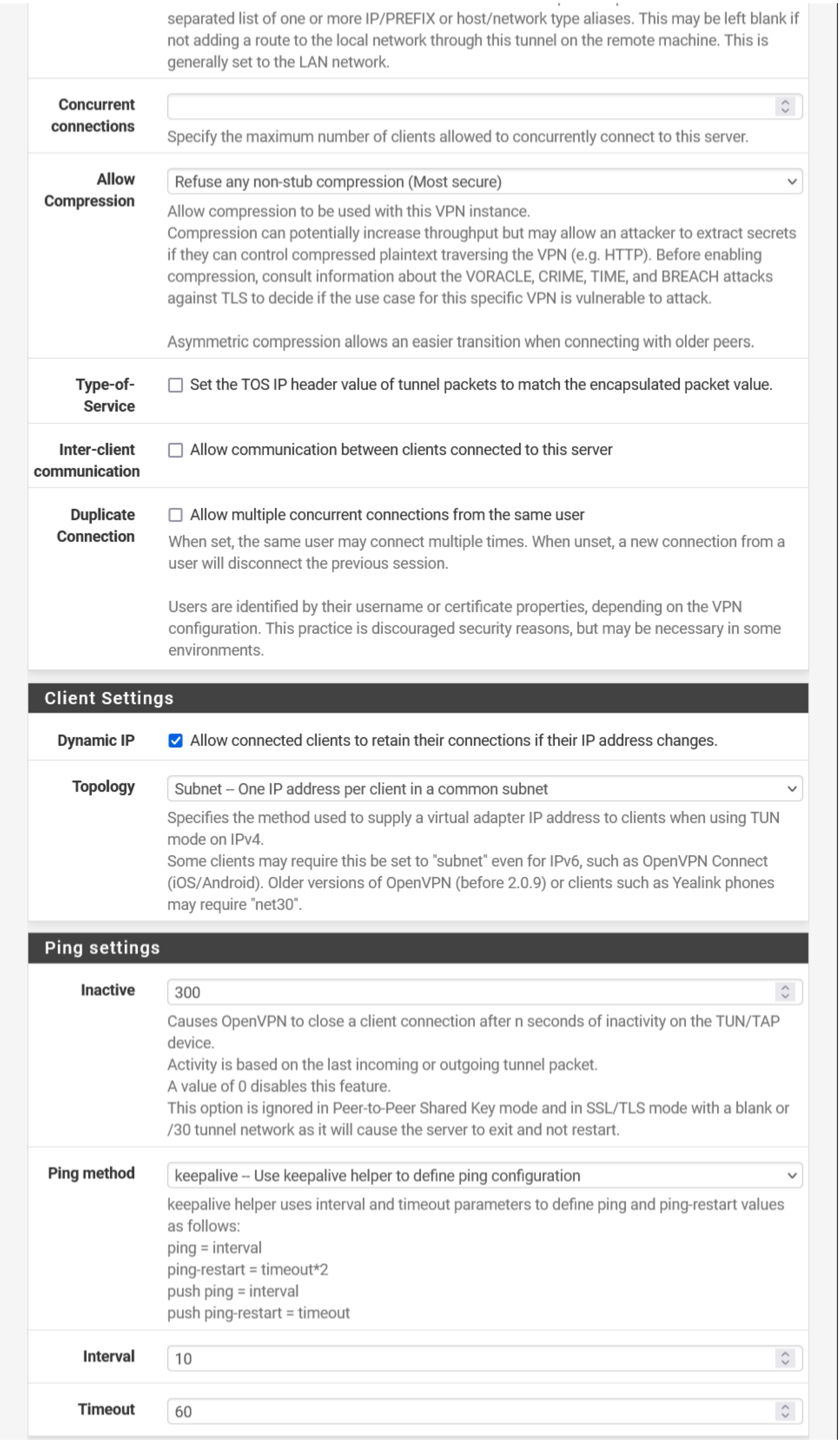
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will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

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: 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 traversing the 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.

Asymmetric compression allows an easier transition when connecting with older peers.

Type-of-Service: □ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication: □ Allow communication between clients connected to this server

Duplicate Connection: □ Allow multiple concurrent connections from the same user

When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

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

Topology: Subnet -- One IP address per client in a common subnet

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: 300

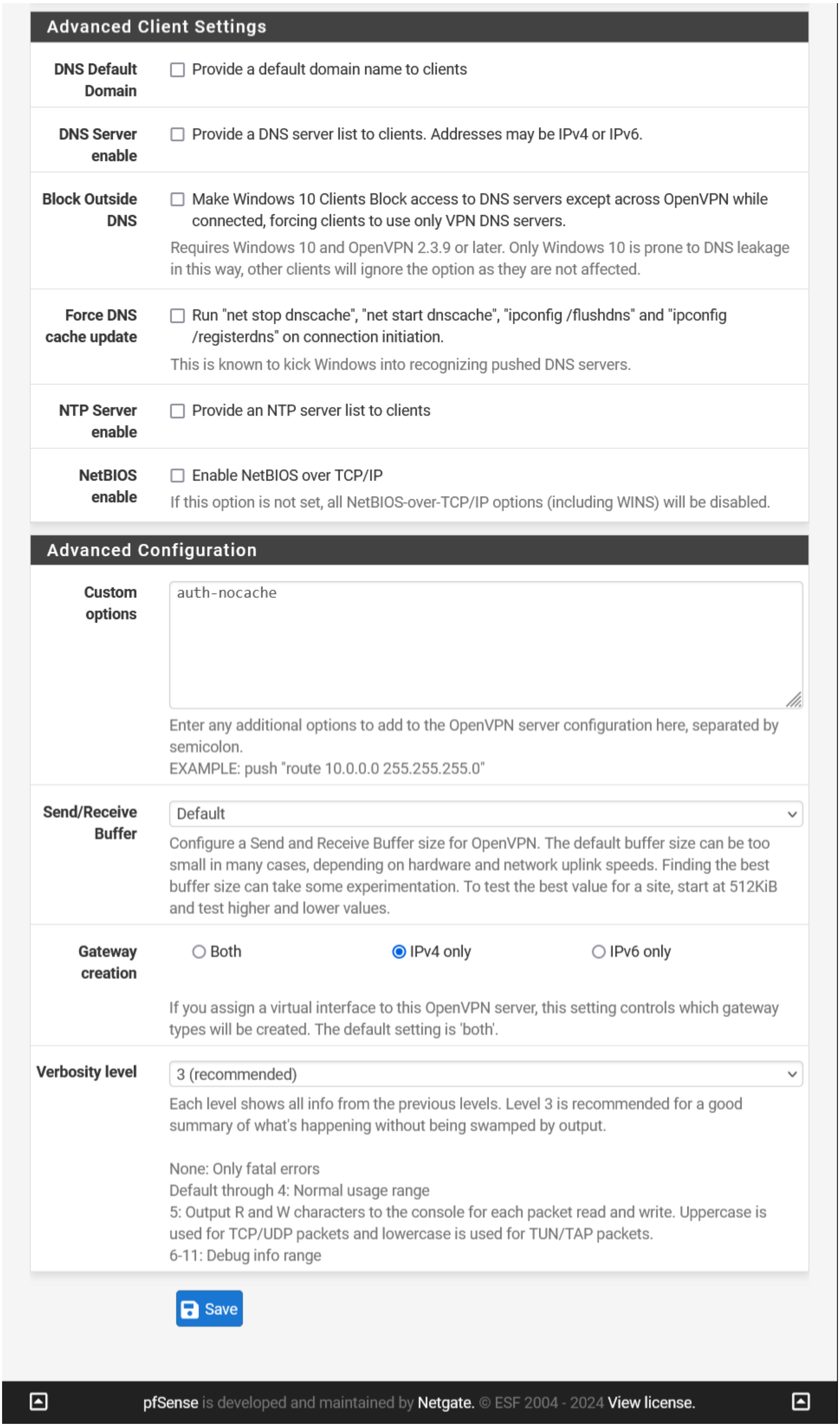
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method: 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: 10

Timeout: 60



Advanced Client Settings

DNS Default Domain □ Provide a default domain name to clients

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

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

```
auth-nocache
```

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"

Send/Receive Buffer Default

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'.

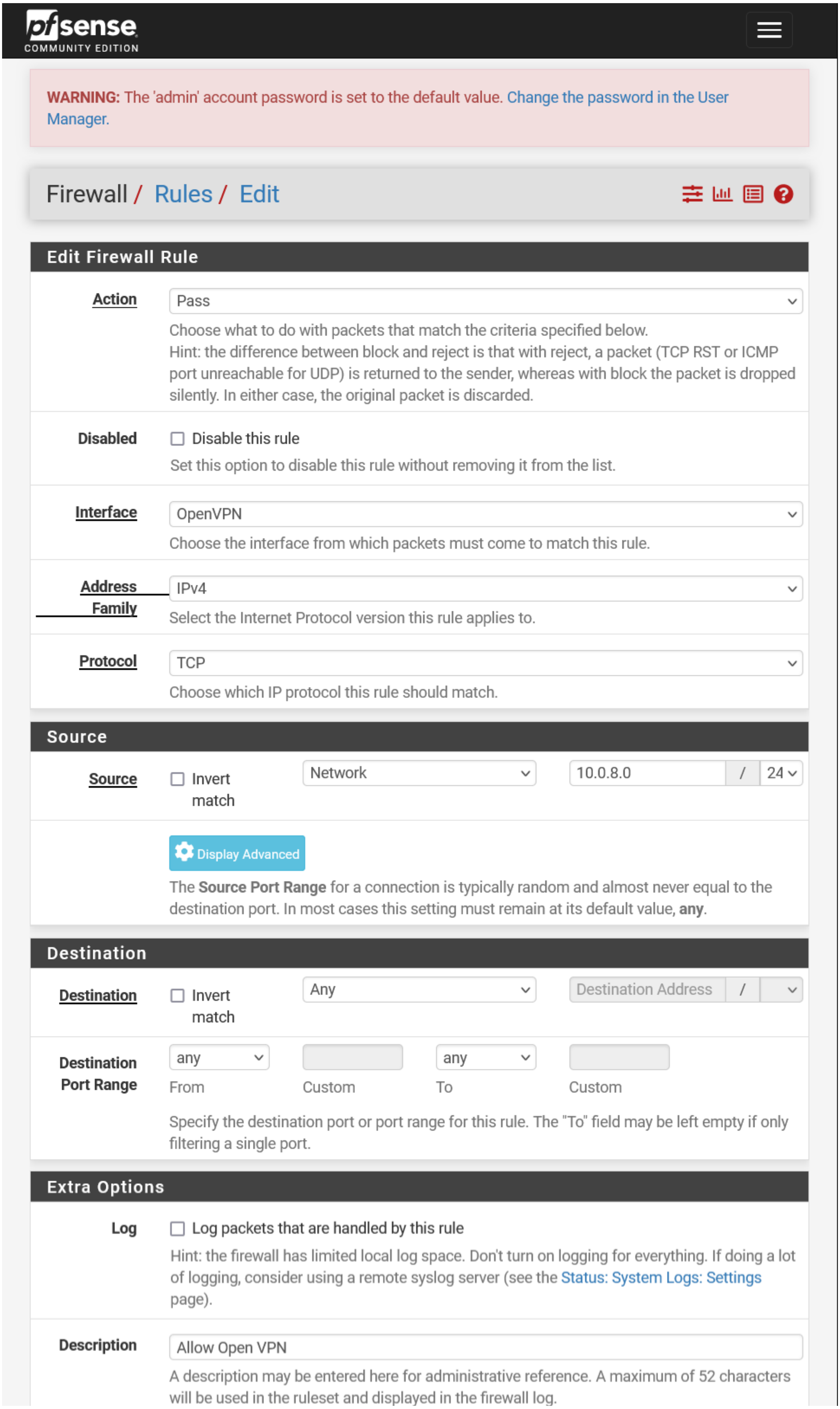
Verbosity level 3 (recommended)

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

- Autoriser le traffic depuis le serveur VPN avec une règle de pare-feu



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

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: OpenVPN

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: TCP

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Network | 10.0.8.0 / 24

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Any | Destination Address /

Destination Port Range: any (From) | (Custom) | any (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.

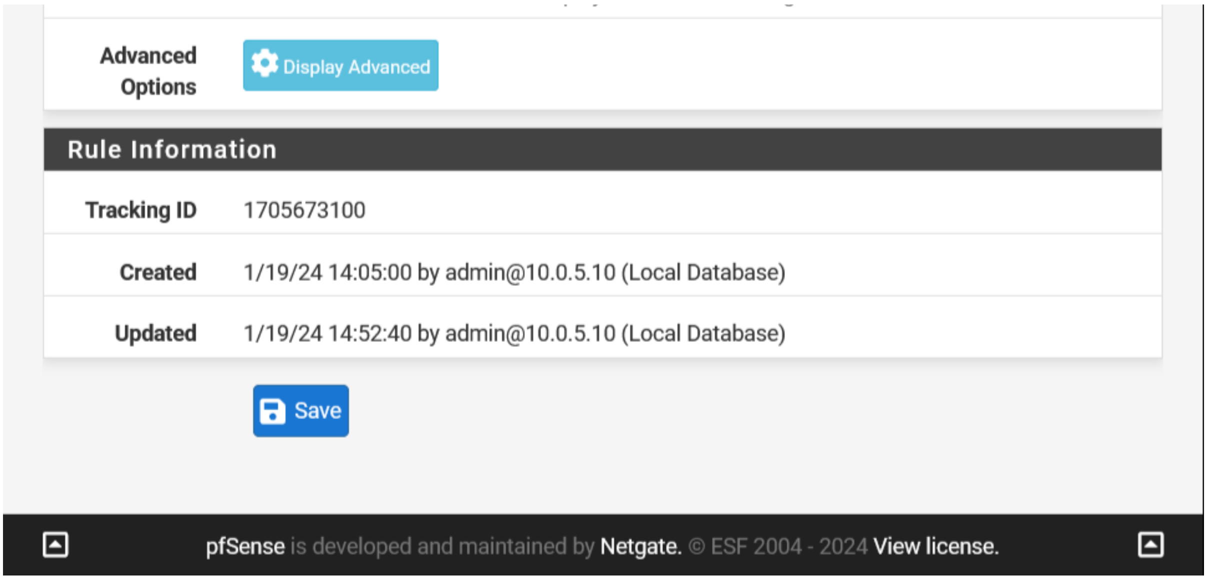
Extra Options

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: Allow Open VPN

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.



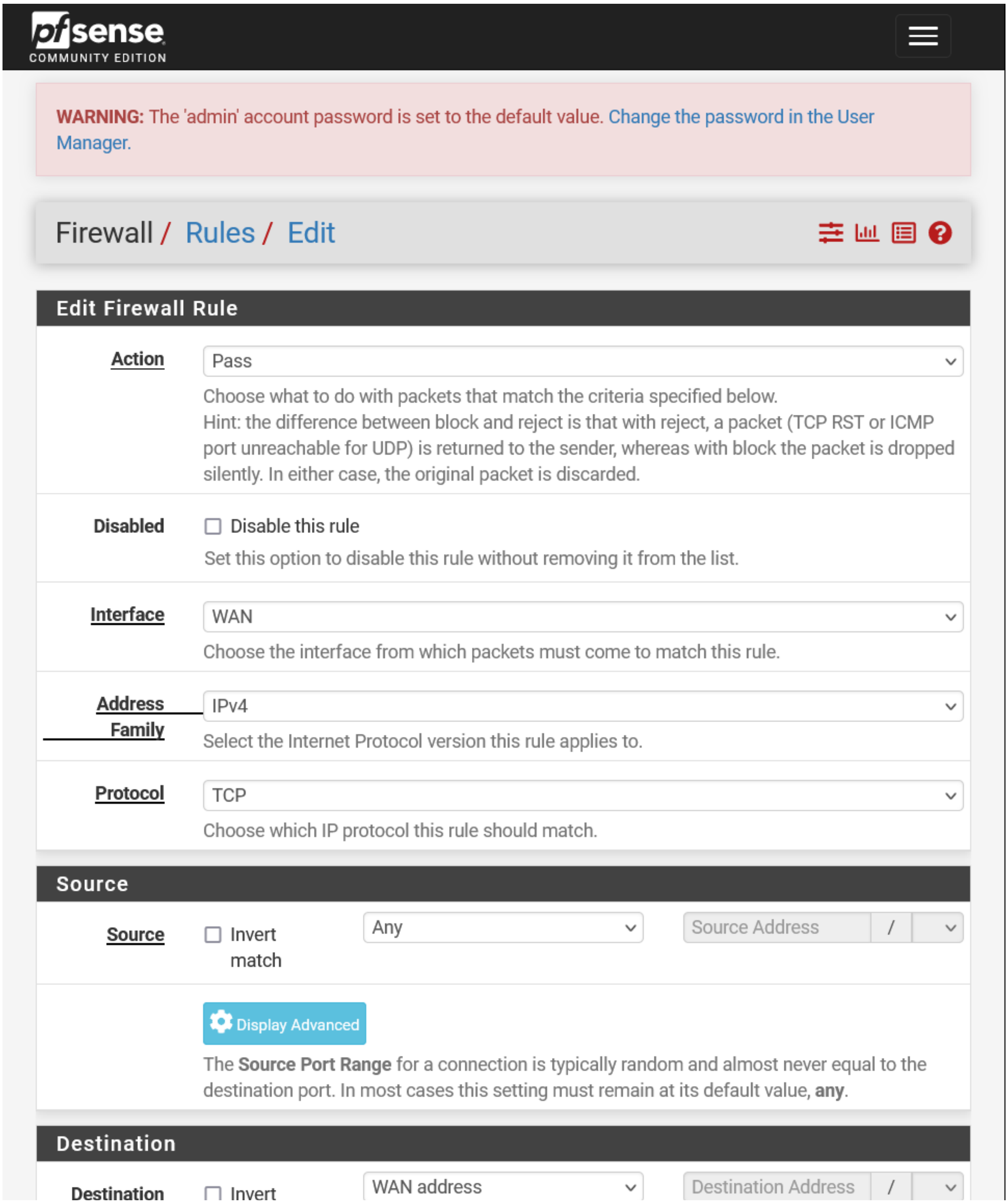
Advanced Options

Rule Information

Tracking ID	1705673100
Created	1/19/24 14:05:00 by admin@10.0.5.10 (Local Database)
Updated	1/19/24 14:52:40 by admin@10.0.5.10 (Local Database)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

- Créer une règle pour ouvrir le port de notre VPN sur notre interface WAN



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

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: TCP
Choose which IP protocol this rule should match.

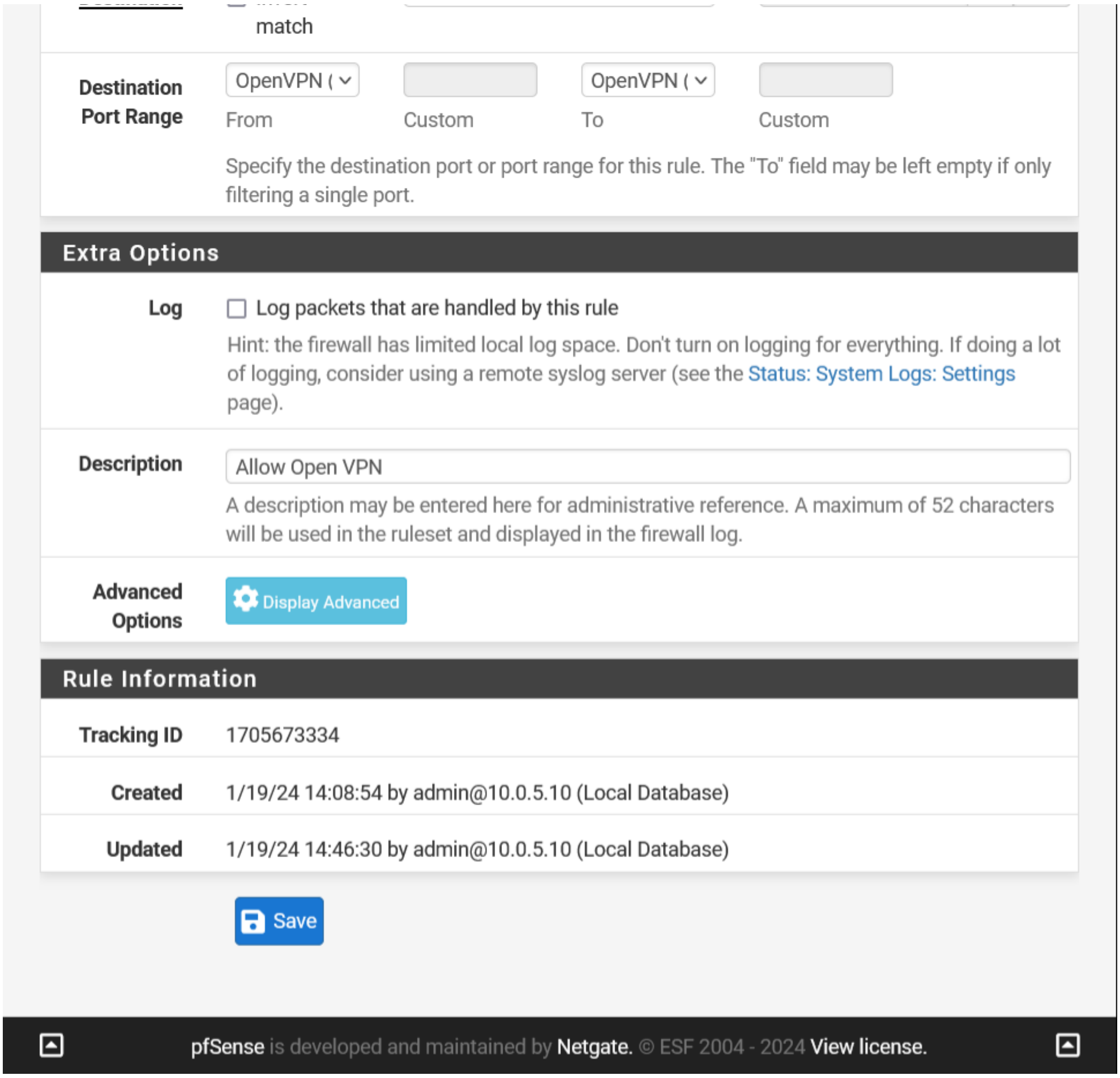
Source

Source: □ Invert match | Any | Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert | WAN address | Destination Address /



match

Destination Port Range

OpenVPN (		OpenVPN (	
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 Allow Open VPN

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 Display Advanced

Rule Information

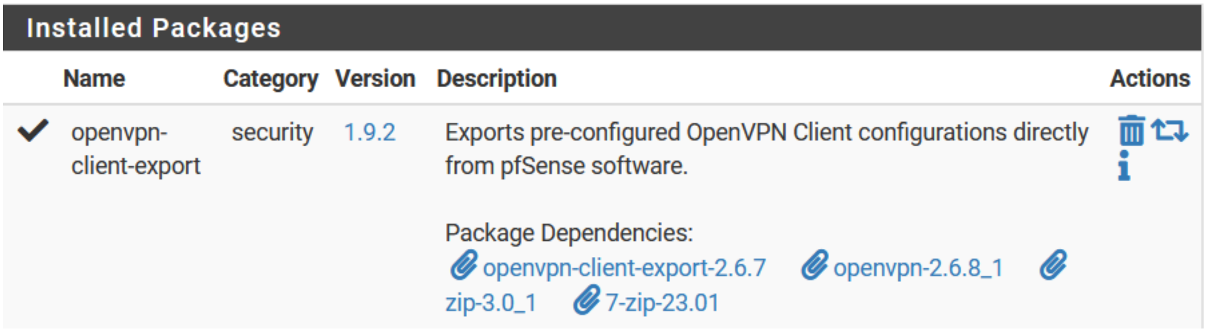
Tracking ID	1705673334
Created	1/19/24 14:08:54 by admin@10.0.5.10 (Local Database)
Updated	1/19/24 14:46:30 by admin@10.0.5.10 (Local Database)

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

- Exporter la configuration serveur afin de renseigner le client OpenVPN

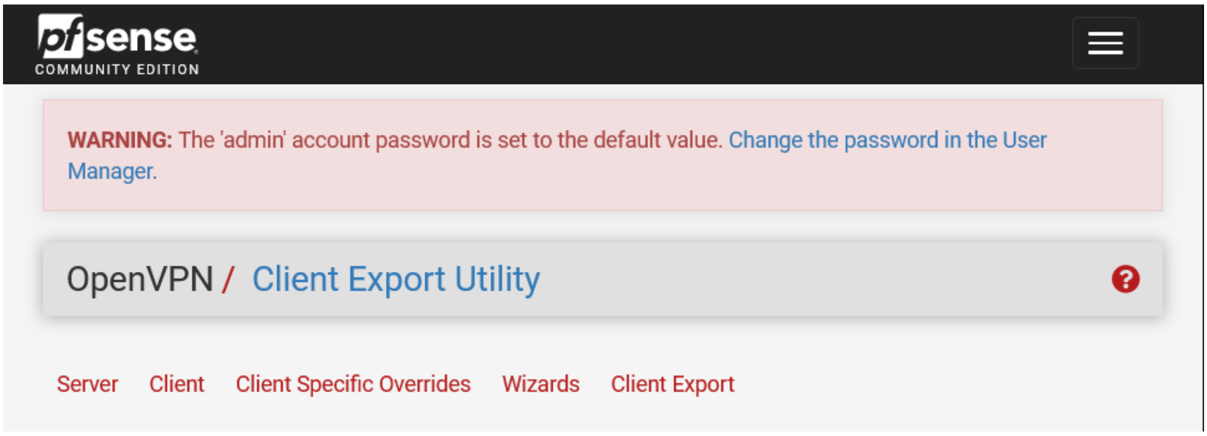
  1 - Installer OpenVPN Client Export via Package Manager sur pfsense



Installed Packages

	Name	Category	Version	Description	Actions
✓	openvpn-client-export	security	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	

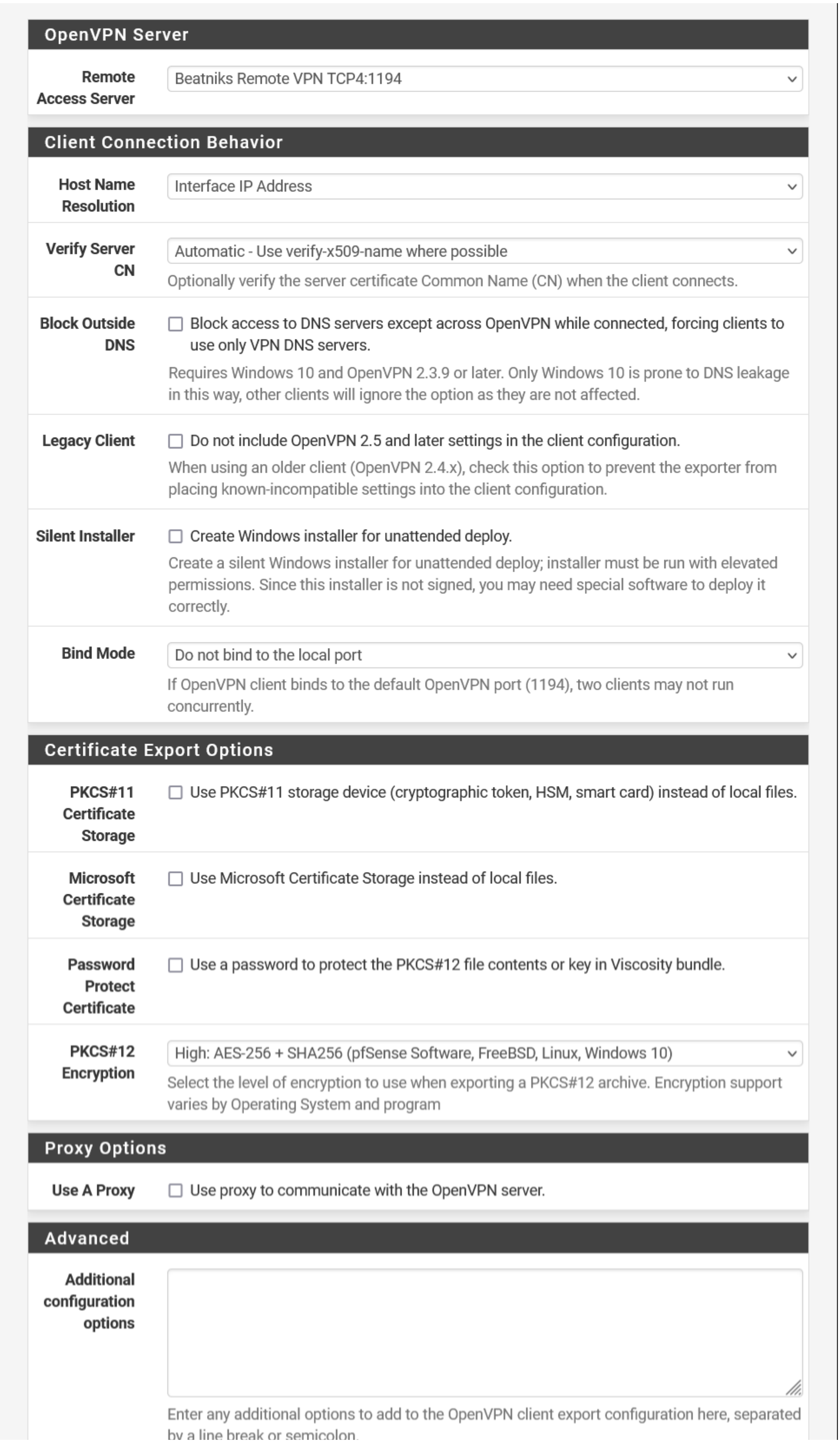
  2 - Exporter la configuration



pfsense COMMUNITY EDITION

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

OpenVPN / Client Export Utility



OpenVPN Server

Remote Access Server: Beatniks Remote VPN TCP4:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

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, Windows 10)

Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

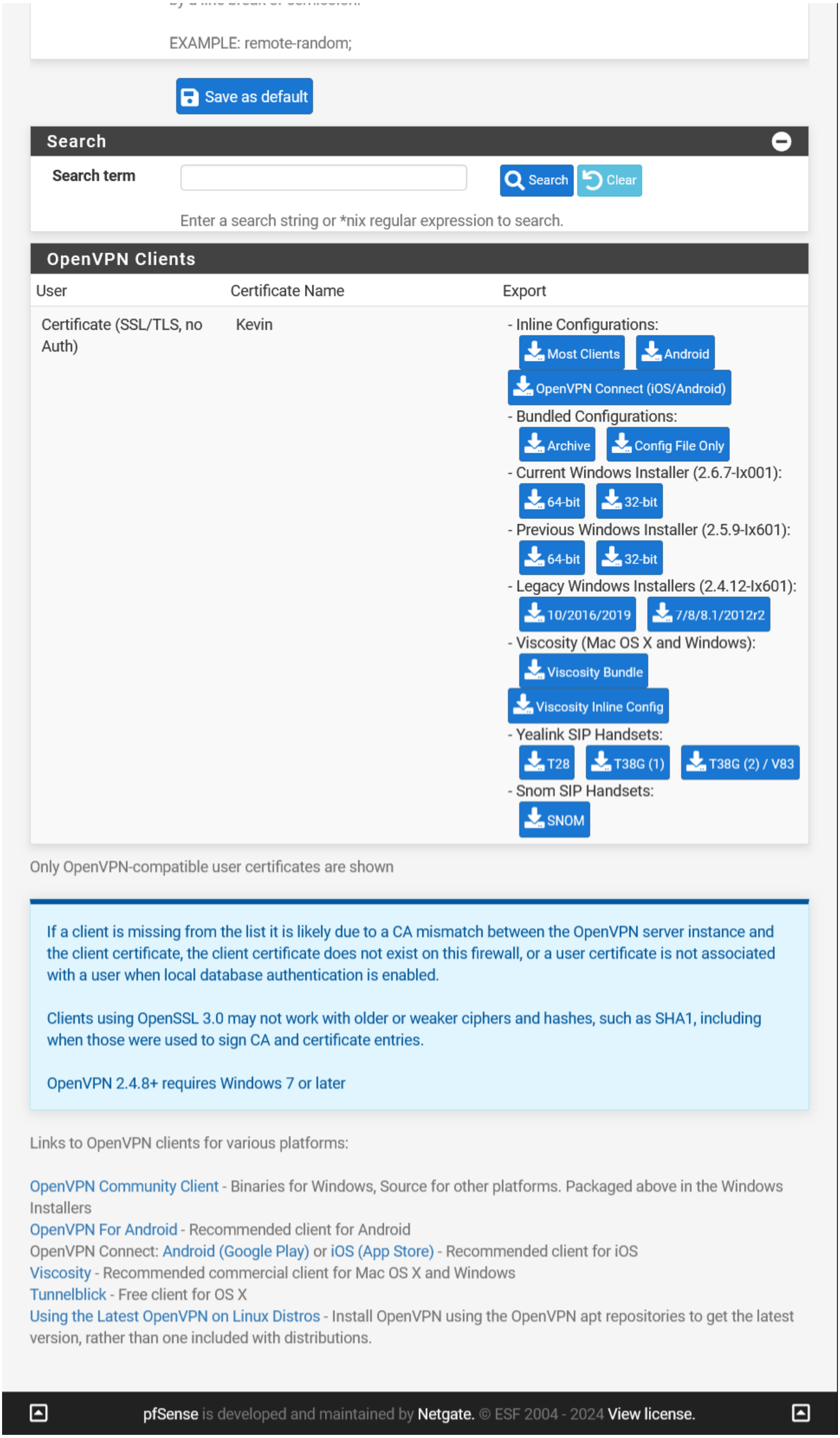
Proxy Options

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

Advanced

Additional configuration options:

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



EXAMPLE: remote-random;

Search

Search term

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

OpenVPN Clients

User	Certificate Name	Export
Certificate (SSL/TLS, no Auth)	Kevin	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.6.7-Ix001): 64-bit 32-bit - Previous Windows Installer (2.5.9-Ix601): 64-bit 32-bit - Legacy Windows Installers (2.4.12-Ix601): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config - Yealink SIP Handsets: T28 T38G (1) T38G (2) / V83 - Snom SIP Handsets: SNOM

Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

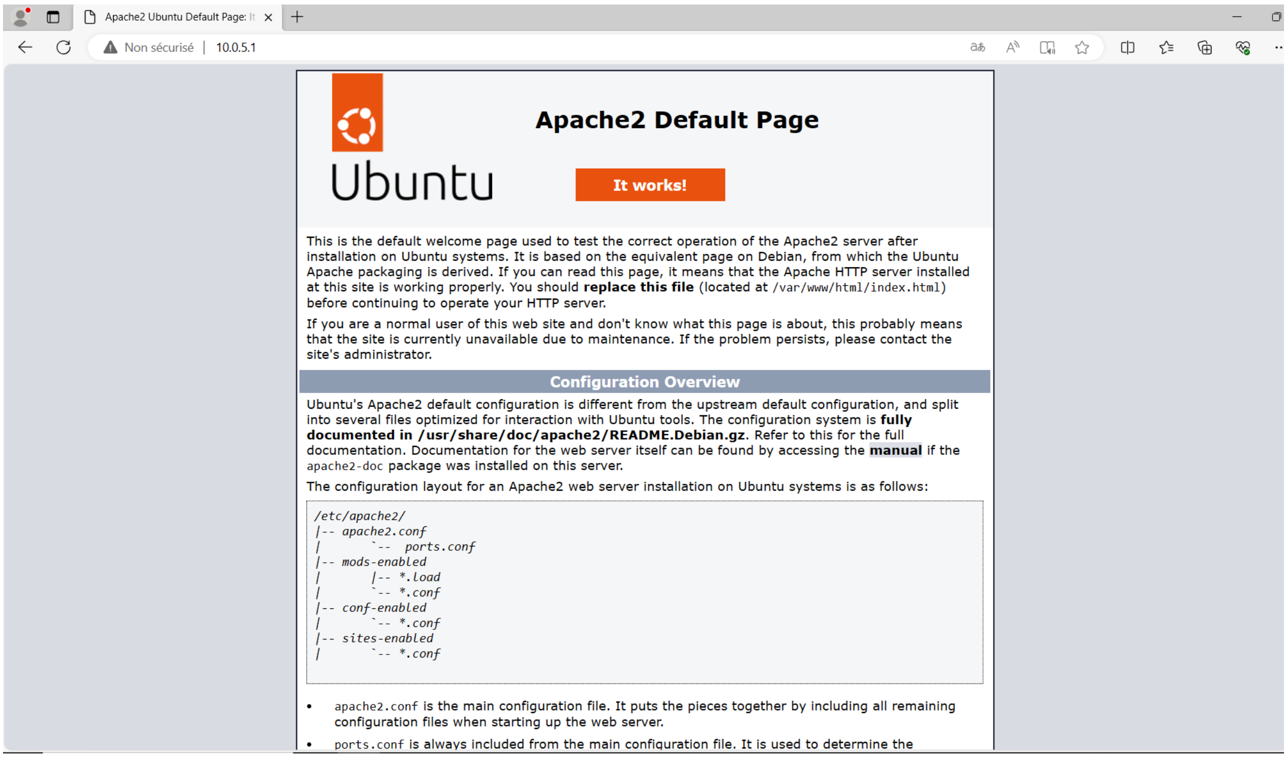
OpenVPN 2.4.8+ requires Windows 7 or later

Links to OpenVPN clients for various platforms:

OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
OpenVPN For Android - Recommended client for Android
OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS
Viscosity - Recommended commercial client for Mac OS X and Windows
Tunnelblick - Free client for OS X
Using the Latest OpenVPN on Linux Distros - Install OpenVPN using the OpenVPN apt repositories to get the latest version, rather than one included with distributions.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

- Côté client distant, lancer le client OpenVPN et importer la configuration serveur
- Une fois la connexion établie, accéder à notre serveur web 10.0.5.1 via le navigateur



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the