

**BTS SIO** 





Sommaire

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

### Infrastructure



## Création autorité de certification

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



## Création du certificat Server

#### - Cliquer sur « Add/sign »



- Ajouter un Name

- Séléctionner la bonne « Méthod » -
- Sélectionner le nom de votre certficat d'authorité -
- Ne pas oublier d'y ajouter le « common name » -

		System / Certific	ates / Certificates / Edit	
		Authorities Certificat	es Certificate Revocation	
		Add/Sign a New Cert	ificate	
		Method	Create an internal Certificate	~
		Descriptive name	CA-max-VPN	
			The name of this entry as displayed in the GUI for re This name can contain spaces but it cannot contain	eference. n any of the following cha
		Internal Certificate		
	-	Certificate authority	openVPN	~
	Certificate Attributes	3		
Sélectionner	Attribute Notes	The following attributes are added to certificates and requests when the selected mode.	hey are created or signed. These attributes behave differently depending on the	
	Considerate Trees	For Internal Certificates, these attributes are added directly to the certi	ficate as shown.	
le type de –	Certificate 1908	Add type-specific usage attributes to the signed certificate. Used for pl	<ul> <li>lacing usage restrictions on, or granting abilities to, the signed certificate.</li> </ul>	
/ 1	Alternative Names	FQDN or Hostname  Value Value		
certificat		Enter additional identifiers for the certificate in this list. The Common N signing CA may ignore or change these values.	Name field is automatically added to the certificate as an Alternative Name. The	
	Add SAN Row	+ Add SAN Row		KAI FTA Maxime
		Save	Activer Wi	

## Création des utilisateurs locaux



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

- Saisir un nom et mot de passe

System / User Ma	anager / Users / Edit	
Users Groups S	lettings Unthentication Servers	
User Properties	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 di	ate as MM/DD/YYYY
Custom Settings	<ul> <li>Use individual customized GUI options and dashboard layout for this use</li> </ul>	er.
Group membership	admins	
	Not member of	Member of
	>> Move to 'Member of' list	K 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 v	
Key type	RSA	0
	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 o	onsider 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 platf	orms may consider weaker digest algorithms invalid
Lifetime	3650	) Activ
		/ tett

## Configuration du server OpenVPN

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

Servers

VPN / OpenVPN / Servers / Edit

Clients

Description

Disabled

**General Information** 

Client Specific Overrides

Disable this server

Wizards

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

A description of this VPN for administrative reference.

Remote Access ( SSL/TLS + User Auth

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

Sélectionner	le certificat	d'authentification	ainsi le	certificat serv	P
Delectionner	ie certincat	u autrientintation		CELLILLAL SELV	C

Server mode

Mode Configuration



**KALETA Maxime** 

V

## Configuration du server OpenVPN

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

Tunnel	Settings	
IPv4 *	Tunnel Network	10.10.10.0/24 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. te80:::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirec	ct IPv4 Gateway	Force all client-generated IPv4 traffic through the tunnel.
Redirec	ct IPv6 Gateway	Force all client-generated IPv6 traffic through the tunnel.
IPv4 L	ocal network(s)	192.168.1.0/24 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 L	ocal 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.
Concurre	ent connections	10 Specify the maximum number of clients allowed to concurrently connect to this server.

#### Paramètres du client :

refusant la mise en cache



Advanced Configuration

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

	0.000						
				Custom options	auth-	nocache	-
OpenVP	N Servers	Tunnel Network	Mode / Crunto		Description	Actions	
WAN	UDP4 / 1194	10.10.10.0/24	Mode: Remote Access ( SSL/TLS + User A	uth )	VPN		
	(TUN)		Data Ciphers: AES-256-GCM, AES-128-GCM Digest: SHA256 D-H Params: 2048 bits	и, CHACHA20-POLY1305, AES-256-CBC		,	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

options

Server Client C	ient specific overrides - wizards - client export			
DpenVPN Server				
Remote Access Server	VPN UDP4:1194	~	G	
Client Connection Be	havior			
Host Name Resolution	Interface IP Address	~		
Verify Server CN	Automatic - Use verify-x509-name where possible	~		
	Optionally verify the server certificate Common Name (C	CN) when the client connect	S.	
Block Outside DNS	<ul> <li>Block access to DNS servers except across OpenVPI Requires Windows 10 and OpenVPN 2.3.9 or later. Only not affected.</li> </ul>	N while connected, forcing Windows 10 is prone to DN	clients to use only VPN DNS servers. S leakage in this way, other clients will ignore the	option as
Legacy Client	Do not include OpenVPN 2.5 and later settings in the When using an older client (OpenVPN 2.4.x), check this configuration.	client configuration. option to prevent the export	er from placing known-incompatible settings int	o the clien
Silent Installer	Create Windows installer for unattended deploy.			
	Create a silent Windows installer for unattended deploy; need special software to deploy it correctly.	installer must be run with e	elevated permissions. Since this installer is not si	igned, you
Bind Mode	Do not bind to the local port	~		
	If OpenVPN client binds to the default OpenVPN port (11	194), two clients may not ru	n concurrently.	

# Règles

#### Wan :

Edit Fire	wall Rule											
	Action	Pass			~							
		Choose w Hint: the whereas	what to do with packets that matc difference between block and rejo with block the packet is dropped	ch the criteria speci ect is that with reje- silently. In either ca	fied below. ct, a packet (1 ase, the origin	CP RST or ICMP port u al packet is discarded.	inreachable for	UDP) is ret	urned to the se	ender,		
	Disabled	Disab	le this rule									
		Set this o	option to disable this rule without	removing it from th	ne list.					and the second s		
	Interface	WAN			~							
		Choose t	he interface from whi <mark>ch packets</mark> i	must come to mate	ch this rule.							
A	ddress Family	IPv4			~							
		Select the	e Internet Protocol version this ru	le applies to.								
	Protocol	UDP			~							
		Choose v	which IP protocol this rule should	match.								
Destin	MUNIFUL R	ange				oper						
Destin     Firewa	all / Rul	es / W	From Specify the destination po VAN	Custom ort or port range	e for this ru	To To field n	nay be left e	mpty if o	Custom	a single port.		Ŀ
Firewa	all / Rul	es / W en applied ad progres	From Specify the destination po VAN d successfully. The firewal ss.	Custom ort or port range	e for this ru reloading	ile. The "To" field n	nay be left e	mpty if o	Custom	a single port.		Ŀ
Destin	all / Rul	es / W en appliec ad progres	From Specify the destination po VAN d successfully. The firewal ss. OpenVPN	Custom ort or port range	e for this ru reloading	in the background	nay be left e	mpty if o	Custom nly filtering	a single port.		Ŀ
Destin Firewa The chan Monitor t Floating Rules (	all / Rul nges have be the filter relo WAN (Drag to C	es / W en applied ad progres LAN hange (	From Specify the destination po VAN d successfully. The firewal ss. OpenVPN Drder)	Custom ort or port range	e for this ru	in the background	nay be left e	mpty if o	Custom nly filtering	a single port.		Ľ
Destin	all / Rul nges have be the filter relo WAN (Drag to C States F	es / W en applied ad progres LAN hange C Protocol	From Specify the destination po VAN d successfully. The firewal ss. OpenVPN Drder) Source	Custom ort or port range	e for this ru reloading ation	ile. The "To" field n	nay be left e	mpty if o	Custom nly filtering Schedule	a single port.		Actions
Destin	all / Rul nges have be the filter relo WAN (Drag to C States F 0/35 KiB	es / W en applied ad progres LAN hange ( Protocol	From Specify the destination po VAN d successfully. The firewal ss. OpenVPN Drder) Source Reserved Not assigned by IANA	Custom Custom int or port range I rules are now Port Destine * *	e for this ru reloading ation	in the background	Gateway	Queue	Custom nly filtering Schedule	a single port. Description Block bogon ne	tworks	Actions

## Règles

#### OpenVPN : Règle pour le contrôle à distance

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 s
	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 V
	Choose the interface from which packets must come to match this rule.
Address Family	IPv4 V
	Select the Internet Protocol version this rule applies to.
Protocol	TCP
	Choose which IP protocol this rule should match
Destination	
Destination Destination	Invert match     Address or Alias     Invert match
Destination Destination Destination Port Range	□         Invert match         Address or Allas         ✓         192.168.1.2         /           (other)         ✓         3389         (other)         ✓         3389
Destination Destination Destination Port Range	Invert match       Address or Alias       Imatch       Imatch       Imatch       Imatch         (other)       Imatch       Imatch       Imatch       Imatch       Imatch       Imatch         From       Custom       To       Custom       Imatch       Imatch       Imatch
Destination Destination Destination Port Range	Invert match       Address or Alias       192.168.1.2       /         (other)       3389       (other)       3389         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.       Image: Custom
Destination Destination Destination Port Range Extra Options	Invert match       Address or Alias       192.168.1.2       /         (other)       3389       (other)       3389         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.
Destination Destination Destination Port Range Extra Options Log	Invert match       Address or Alias       192.168.1.2       /         (other)       3389       (other)       3389         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.         Log packets that are handled by this rule
Destination Destination Port Range Extra Options Log	Address or Alias     Invert match     Invert matc
Destination Destination Destination Port Range Extra Options Log Description	Invert match     Address or Alias     Ig2.168.1.2     //     (other)     3389     (other)     3389     (other)     3389     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.      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 s     the Status: System Logs: Settings page).      Autoriser RDP vers PC Windows 10
Destination Destination Port Range Extra Options Log Description	Address or Alias     Invert match     Invert match     Invert match     Address or Alias     Invert match     Invert match     Invert match     Address or Alias     Invert match     Invert match     Invert match     Invert match     Invert match     Address or Alias     Invert match
Destination Destination Destination Port Range Extra Options Log Description Advanced Options	Address or Alias     192.168.1.2     (     (other)     3389     (other)     3389     (other)     3389     (other)     3389     (other)     3389     (other)     3389     (other)     Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.      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 systog s     the Status: System Logs: Settings page).      Autoriser RDP vers PC Windows 10     A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in th     log.      Outplay Advanced

## Mise en place et connection 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 :



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

README

pfSense-UDP4-1194-max-config

le me	rends	sur l'icone	openyon	puis	connecter
	LIIUS .			puis	CONNECTED

Connecter Déconnecter Reprendre	
Afficher le statut Voir le log Editer la configuration Effacer les mots de passe enregistrés	Utilisateur: max Mot de passe: ***1 @
Importer > Configuration Quitter	CK Annuler
^	



Type

Dossier de fichiers

Document texts

Taille

**KALETA Maxime** 

1 Ko

# pfSense-UDP4-...

5

Modifié le

20/11/2024 09:52

18/07/2024 11:21



Rechercher dans : config