	0
VPN SOUS	
- PFSENSE	
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	

••••

TOPOLOGIE



0-

٢

 \bigcirc

Premièrement je met en place sur mon proxmox un pfsense avec dans notre contexte, ajouter une carte réseau pour le LAN et garder

celle de base pour le wan. (ici la 3ème est pour la DMZ mais c'est optionnel)

× •	Virtual Machine 225 (pfsenseB2) on node 'proxmox1'	ap 🖊
	Summary	Add ~ Remove Edit	
	>_ Console	🚥 Memory	2.00 GiB
	Hardware	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]
	Cloud-Init	BIOS	Default (SeaBIOS)
	Options	🖵 Display	Default
	Task History	📽 Machine	Default (i440fx)
		SCSI Controller	VirtIO SCSI single
WAN	Monitor	O CD/DVD Drive (ide2)	local.iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media
	🛱 Backup	🖨 Hard Disk (scsi0)	local-lvm:vm-225-disk-0,iothread=1,size=32G
	✿ Replication		e1000=BC:24:11:AE:DB:E0,bridge=vmbr0,firewall=1
LAN ———	2 Snapshots		virtio=BC:24:11:1D:63:2A,bridge=vmbr100,firewall=1
	♥ Firewall ▶		virtio=BC:24:11:1E:ED:9C,bridge=vmbr101,firewall=1

Configuration du pfsense

Ο

Ensuite guand on lance le pfsense, on assigne les interfaces en appuyant 2

et on attribue une ip aux interfaces wan et lan

otarting LRUN done. ofSense 2.7.2-RELEASE amd64 20240304-1953 Bootup complete	
reeBSD/amd64 (pfSense.home.arpa) (ttyv0)	
KVM Guest - Netgate Device ID: 087a611f1adf	d52c8b41
*** Welcome to pfSense 2.7.2-RELEASE (amd64	I) on pfSense ***
NAN (wan) -> em0 -> v4/DHCP4: LAN (lan) -> vtnet0 -> v4: 192.1 DMZ (opt1) -> vtnet1 -> v4: 192.1	192.168.20.62/24 68.55.1/24 68.65.1/24
0) Logout (SSH only) 9) p 1) Rssign Interfaces 10) F 2) Set interface(S) IP address 11) R 3) Reset webConfigurator password 12) P 4) Reset to factory defaults 13) N 5) Reboot system 14) E 6) Halt system 15) R 7) Ping host 16) R	ofTop ilter Logs testart webConfigurator MP shell + pfSense tools pdate from console nable Secure Shell (sshd testore recent configurat testart PHP-FPM

Mise en place d'une debian

Dans un premier temps, je vais simplement cloner ma VM modèle, et je vais lui modifier sa carte réseau pour la pointer sur vmbr100 qui permettra d'être sur le LAN du réseau



 \mathbf{O}

0

Configuration du VPN

Une fois toutes les étapes précédentes réalisées, je dispose à présent d'un PFsense vierge . Il ne nous reste plus qu'à configurer le VPN, appliquer des règles firewalll, et tester.

Autorité de certification.

Le client et le serveur VPN sont authentifiés à l'aide de certificats. Pour cela, ces certificats doivent être émis par une autorité de certification reconnue comme sûre aussi bien par le serveur que par le client. Dans notre cas, c'est avec notre PFsense que nous créerons une autorité de certification, pour ce faire, je vais dans System>Certificate > Authorities.

	System 🗸	Interfaces 🕶	Firewall 🗸	Services +	VPN +	Status 🗸
WARNING: The	'admin' account	password is set to	o the default valu	ie. Change the p	assword in th	e User Mateg
System /	Certificate	/ Authoriti	es / Edit			
Authorities	Certificates	Revocation				
Create / Edi	t CA					
Descript	tive name					

Je vais par la suite, remplir les informations suivantes :

Descriptive name: MorellePFSenseVPN

Method : Create a internal CA

Common-name: Morelle

N	Certificate Authori	ties				
	Name	Internal	Issuer 🖕	Certificates	Distinguished Name	
	MorellePFSenseVPN	~	self-signed	0	CN=Morelle	
					Valid From: Wed, 20 Nov 2024 08:36:19 +0000	
					Valid Until: Sat, 18 Nov 2034 08:36:19 +0000	•

Créer un certificat serveur.

Ensuite, pour créer un certificat de type serveur, je me rends dans System>Certificates>Certificates.

Dans cette page, je renseigne les informations suivantes :

Descriptivename: Certificat Serveur pour VPN

Common Name : vpn.morelle.local

Certificat Type : Server Certificate

Alternative Names: vpn.morelle.local

COMMUNITY EDITION	 Interfaces 	Firewall 👻		VPN
WARNING: The 'admin' ac	count password is set	to the default val	<mark>ue</mark> . Change the p	assword
System / Certific	cates / Certific	cates		
Authorities Certifica	ates Certificate R	evocation		
Edit an Existing Cer	tificate			
Method	Edit an existing c	ertificate		
Descriptive name	Certificat serveur	pour vpn		
	The name of this e This name can cor	ntry as displayed Itain spaces but i	in the GUI for ref t cannot contain	erence. any of t
Subject	CN=vpn.morelle.lo	cal		
Edit Certificate				_

Créer un user et son certificat.

Dans cette étape, je vais créer un utilisateur ainsi que son certificat, celui-ci nous permettra de nous connecter au VPN. Pour créer un utilisateur, je me rends dans System> UserManager.

Ici, nous allons créer notre user, je précise les informations nécessaires, à savoir:

Username: lorenzo.vpn Password: sio\$2024

Fullname: lorenzomorelle Et je veille bien à cocher "Click to create à user certificate"

et pour Descriptive name je met Certificat-VPN

Config OpenVPN Serveur.

Place à la configuration d'OPEN VPN, je me rends dans l'onglet VPN > OPENVPN > Server Voici les informations renseignées :

 Dans général Information :Description : VPNMORELLE

 Dans mode configuration Server mode : Remote Access (SSL/TLS + User Auth)

 Backend for auth. : Local Database

 Device mode : tun – Layer 3 Tunnel Mode

 Dans endpoint Configuration :Protocol: UDP on IPv4 only

 Interface: WAN

 Local port : 1194

 Dans Cryptographic Settings : Server certificate: Certificat Serveur pour VPN (celui créer précédemment)

 Ensuite on laisse par défaut pour cette partie

User	s		•
	Username	Full name	
	 admin 	System Administrator	
	Lorenzo.vpn	lorenzomorelle	

Config OpenVPN Serveur.

La configuration maintenant à moitié faites, il ne nous reste plus qu'à faire la configuration liée au tunnel VPN.

Dans tunel Settings Je renseigne dans IPv4 Tunnel Network, l'adresse réseau que nous assignons au tunnel vpn je met : 192.168.54.0/24

Dans IPv4 Local Network, j'entre la / les adresse réseau que je désire mettre à disposition de mes clients VPN ici 192.168.55.0/24

Puis, dans Concurrent Connections, j'entre la valeur 10, cette variable correspond au nombre d'user simultanés

Dans client settings on va opter pour la topology net30 (attention, avec cette option 1user = 4 ip)

Dans Advanced Client settings on coche DNS Default Domain, et on met comme nom ici vpn.morelle.local de DNS.

Puis dans **Advanced Configuration**, je vais saisir l'option customisé "auth-nocache" qui va apporter une couche de protection en plus, pour empêcher la mise en cache de logins.

Exporter le certificat.

Pour exporter la configuration, on va aller dans System > Packet manager. Je vais chercher OpenVPN Client export dans available package, et je vais le télécharger. On devrait le retrouver dans l'onglet "installed packages".

Par la suite, je me rends sur "OPENVPN", puis dans "client export". Ici, on prend connaissance des configurations mises par défaut, dans mon cas je ne change rien sauf dans Advanced > "additionnal configuration options" où je vais écrire "auth-nocache".

0

Exporter le certificat.

Puis je fais "Save as Default". Ensuite, en bas de cette page, on distingue une section "OPENVPN Clients". Ici, je vais cliquer sur "Archive" dans Bundled Config. Et j'irais prendre plus tard l'installateur pour Windows10 pour mon client).

penVPN Clients		
r	Certificate Name	Export
ŧ	Certificica: VPN	- Inter Configuration: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configurations: Control Configuration: Control Configuration: Configura

Ac	(Pass (
	Hint: the difference between block and reject is that with reject, a packet (1 whereas with block the packet is dropped silently. In either case, the origin	ILEEN	es Firewall oben ven
Disa	eled Disable this rule		
	Set this option to disable this rule without removing it from the list.		
Inter	WAN V Choose the interface from which packets must come to match this rule.	Voici la règle	mise en place dans l'interface WAN. Allez dans firewall>rules>WAN et mettez comme sur les screen
Address Fa	nily IPv4		
	Select the Internet Protocol version this rule applies to.	Action · Pass	Interface WAN Address Family : Inv4 Protocol : IIDP
Prot	CODP v Choose which IP protocol this rule should match.		
Source			
Source	Invert match Any	Source Address	Source : any
	🕸 Display Advanced		
	The Source Port Range for a connection is typically random and almost ne its default value, any.	ever equal to the destination port. In most c	
Destination			
Destination	Invert match WAN address	Destination Address	
Destination Port Range	(other) v 1194 (other)	v 1194	Destination : WAN Address
	From Custom To	Custom	
Extra Ontions	opecity the destination port or port range for this rule. The "To" field may b	ae ien empty ii only intering a single port.	Port Range : (notre nort de von, nar défaut : 1194)
Extra Options	I on packets that are bandled by this rule		rort hange . (notre port de vpn, par delade. 1197)
	Hint: the firewall has limited local log space. Don't turn on logging for even	rything. If doing a lot of logging, consider us	
	ure status, system Logs, setungs page).		Description: Accès distant pfsense
Description	A description may be entered here for administrative reference. A maximu	um of 52 characters will be used in the rules	
	log.		

Ο

Vérifications du fonctionnement du VPN.

On clique sur le .exe	🗣 i 🖸 🗖 🖛 i		Gérer	Te	éléchargements			×
	Fichier Accueil Partage	Affichage	Outils d'application					~ 🕐
	← → × ↑ 🕹 > Ce PC	> Téléchargem	ients 🗸 🗸	ō	,○ Rechercher dans	: Téléchargements		
	🖈 Accès rapide	Nom Aujourd'hui (1)		Modifié le 💙	Туре	Taille	
et on fais install now	↓ Téléchargement: ★	openvpn-pfS	ense-UDP4-1194-mais-	insta	. 24/11/2024 12:23	Application		861 Ko

on fait clique droit se connecter dans la barre des tache sur l'icône de notre

logiciel et on met le user et le mdp

On clique sur

Utilisateur:	test	
Mot de passe:	Ì	
Enregistrer r	not de passe	
✓] Enregistrer r	not de passe	





[😵 Install Now
	Customize

R

... X

Choose setup type

Ο

Ο

