

- 1- Introduction
- 2- Infrastructure
- 3- Installation de pfsense
  - a- Téléchargement de pfsense
  - b- Vérification de l'intégrité du fichier téléchargé pfsense
  - c- Lancement de l'installation
- 4- Configuration post instalation
  - a- Déclaration des interfaces
  - b- Assignement des adresses aux interfaces wan, lan et opt1
    - L'interface Wan
    - L'interface lan
    - L'interface opt

1- Introduction

PfSense est un pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau d'entreprise.

Prérequis pour une machine PfSense

	Configuration minimale	Configuration recommandée
Processeur	600 MHz	1 GHz
Mémoire vive	512 Mo	1 Go
Stockage	> 6 Go	

2- Infrastructure Pour notre Labo :il faut 3 machines -Machine Pfsense FreeBSD dans le réseau Wan Nom du serveur : heimdall Adresse IP : 192.168.1.250 Net masque : 255.255.255.0 Passerelle : 192 .168.1.1 DNS : adresse de votre serveur DNS

-Une machine avec active directory et DNS (nom du domaine Dns et active directory est sitka.local) dans le réseau sitka\_lan -une machine Debian dans le réseau opt\_lan

-Machine AD dans le réseau sitka\_lan Nom du serveur : hermes Adresse IP : 172.20.0.14 Net masque : 255.255.255.0 Passerelle : 172.20.0.250 DNS : adresse de votre serveur DNS

-Une machine Debian ou Ubuntu et Windows dans le réseau opt\_lan Adresse IP : DHCP

3- Installation de pfsense

 a- Téléchargement de pfsense
 Pour installer pfSense il faut télécharger l'iso d'installation sur le site officiel à l'adresse : <u>https://www.pfsense.org/download/</u>
 Le lien de téléchargements est ci-dessous
 <u>https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.6.0-RELEASE-amd64.iso.gz</u>

Version:	260
Architecture:	AMD64 (64-bit) ~ 🚱
Installer:	DVD Image (ISO) Installer ~
	[and a second

b- Vérification de l'intégrité du fichier téléchargé pfsense

Une fois le fichier télécharger on va vérifier l'integrité du fichier telechargé avec la commande : **Get-FileHash** pfSense-CE-2.6.0-RELEASE-p1-amd64.iso.gz -Algorithm SHA256 | format-list

Å restΘ	neptun	e: -	Χ.	E W	/indows PowerShell	х.	+:	$\mathbf{X}_{\mathbf{x}}$			
PS C:\>	Get-F	fileHash	pfSens	e-CE-	2.5.2-RELEAS	E-pl-and6	4.is	o.gz	-Algorithm	SHA256	format-list
lgorith	n': <u>3</u>	SHA256		Ŧ		-					
llgorith: lash	n': <u>\$</u> :[(	SHA256	419C86	C665E	B8D908F584E1	06D54859AA	13F4	EEB17	75A60548C70	E228	

Comparer les deux empreintes 1 et 2 si les deux empreinte sont identique ceci implique que le fichier telechargé et intègre

c- Lancement de l'installation

il faut maintenant dézziper notre fichier pour avoir l'iso et lancer l'installation sur vmware



#### On choisit pfsense comme nom



On pointe vers le fichier iso de pfsense



#### On laisse 20 gb par défaut



#### Pour cette étape On mettra en place 3 cartes

Network Adapter en bridge $\rightarrow$ 192.168.1.0/24	
Network Adapter2 en Lan_1→172.20.0.0/24	
Network Adapter3 en Lan_2→192.168.2.0/24	
On mettra 1GB de mémoire	

WAN (wan)	-> ем0	-> v4: 192.168.1.250/24
LAN (lan)	-> ем1	-> v4: 172.20.0.250/24
OPT1 (opt1)	-> ем2	-> v4: 192.168.2.250/24



#### On clique sur finish et on commence l'installation



#### On accepte le contrat



#### On choisit le clavier français

keybbaru Map. Other keyMaps can be	chosen below.		
( ) Central European (QHERTY)			
( ) Colemak ergonomic alternative			
( ) Croatian			
( ) Czech (QHERT2, accent keys)			
( ) Banish			
( ) Danish (accent keys)			
( ) Banish (Macbook)			
( ) Butch (accent keys)			
() Estonian			
() Frank			
(x) French (accout kous)			
A Prench taccent keys/		278	
			_
(Select)	<cancel></cancel>		
EBroos arrests TO	P OF FHTEDI		

#### Puis on continue l'installation





#### On sélectionne Install puis ok



#### On test le clavier



On choisit le système UFS pour créer nos partitions



On nous demande si on veut aller sur le Shell pour d'autres manipulations on dit non



#### Puis on redémarre la machine



Une fois la machine a redemarrer on tombe sur l'interface menu

On remarque qu'il ya que deux interfaces qui sont reconnue **em0** et **em1** et que le clavier est en qwerty malgré notre choix pendant l'installation d'un clavier français



4- Configuration post instalation

Mannuellement on va mettre notre clavier en français mais temporairement car en redemarrant notre serveur le clavier redevient en querty ; on le configurera d'une façon permanente avec l'interface web: On choisit **l'option 8** pour demarrer le shell puis on tape la commande suivante

#kbdcontrol -l fr<mark>ou</mark>#kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd

a- Déclaration des interfaces Maintenant on va déclarer nos trois interfaces : Wan, lan et opt1 : C'est pour cela on choisit l'option 1

Enter an option: 1

Après il faut prendre les choix encadrés en rouge



A la fin on doit avoir le résultat suivant



Maintenant on va affecter les adresses IP à nos trois interfaces,

- b- Assignement des adresses aux interfaces wan, lan et opt1
  - L'interface Wan.

Le choix de des adresses qu'on va affecter à cette interface dépend de la configuration de notre box internet c'est pour cela il faut faire une ipconfig /all sur la machine physique pour déterminer la passerelle et l'ID réseau utilisé

Donc notre réseau est Id réseau 192.168.1.0/24 DNS/Passerelle 192.168.1.1

Carte Ethernet Ethernet :	
Suffixe DNS propre à la connexion : Description : Killer E2200 Gigabit Adresse physique : FC-AA-14-24-82-78 DHCP activé : Oui Configuration automatique activée : Oui Adresse IPv4 : 192.168.1.142(préfér Masque de sous-réseau : 255.255.255.0	Ethernet Controller :24c5%16(préféré) é)
Passerelle par défaut.         192.168.1.1           Serveur DHCP         : 192.168.1.1           IAID DHCP6         : 268216852           DUID de client DHCPv6.         : 00-01-00-01-27-51-18-51-FC-           Serveurs DNS.         : 192.168.1.1           Net&BIOS sur Topip.         : 212.128.1.1	AA-14-24-82-7B

On choisit l'option 2

Enter an option: 2

Et on fait les choix suivants







#### L'interface lan Et on fait les choix suivants

•

@ip:172.20.0.250 Masque de sous réseau 255.255.255.0 Passerelle : non DHCP IPv5 oui on crée un étendu de : 172.20.0.20--→172.20.0.30 Pas de IPv6 Pas de DHCP IPV6 Le web configurateur oui on le met sur l'interface Lan



#### L'interface opt ٠

@ip:192.168.2.250 Masque de sous réseau 255.255.255.0 Passerelle : non Pas de DHCP IPv5 Pas de IPv6 Pas de DHCP6

Enter the new OPT1 IPv4 address. Press <ENTER> for none: > 192.168.2.250

Enter the new OPT1 IPv4 subnet bit count (1 to 31): ≻24

Enter an option: 2

Available interfaces: WAN (em0 - static) LAN (em1 - static) OPT1 (em2)

Enter the new OPT1 IPv6 address. Press (ENTER) for none: Do you want to enable the DHCP server on OPT1? (y/n) n Please wait while the changes are saved to OPT1... Reloading filter... Reloading routing configuration... Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.8 = 24 2555.255.8.0 = 16 255.0.0.0 = 8 DHCPD... The IPv4 OPT1 address has been set to 192.168.2.250/24 Press <ENTER> to continue. For a WAN, enter <u>the new</u> OPT1 IPv4 upstreaм gateway address. For a LAN, press <mark><ЕНТЕК</mark> for none: > ∎



- 1- Teste de la connectivité
- 2- Exécution du Wizard de la configuration de base
- 3- La mise en place de la configuration du clavier en fr de façon permanente

1- Teste de la connectivité

Sur la machine active directory on va tester la liaison avec pfsense et tester la table de routage en allant sur internet



Maintenant on va accéder à l'interface web de PfSense en tapant l'adresse :

#### http://172.20.0.250



2- Exécution du Wizard de la configuration de base

Un Wizard à 9 étapes va s'exécuter par défaut Les premières étapes sont des informations d'ordre générales traitant le SAV Netgate



On rentre notre nom du serveur heimdall le nom de domaine sitka.local

On configure le serveur NTP sur **fr.pool.org** et le Timezone sur **Europe/Paris** 

5	- Manufacture Manual Processor AMM Matura Manualation Maka - 🍱
ense ayanan	<ul> <li>ивопасот + наточа + золчесть + ччи + акани + цифлозись + нор + це</li> </ul>
√izard / pfSens	e Setup / General Information 🛛 🕹
Step 2 of 9	
Seneral Information	n de la construcción de la constru
	On this screen the general pfSense parameters will be set.
Hostname	Heimdall
	DAMPLE rejenser
Domain	strka.jocal
	DCAMPLE ingeométicem
	The disfault behavior of the DNR Resident will ignore manually configured DNR servers for elect queries and query read DNR servers directly. To use the manually configured DNR servers below for client queries, viril Generale - DNR Resider and multir DNR Query Forwarding after completing the wiland.
Primary DNS Server	172 23.0.14
Secondary DNS Server	6.683
Override DNS	R.
	Allow DNS servers to be overridden by DHCP/PPP on WAN
	20 Reit

#### L'interface Wan est déjà configurée

< 🔿 🗖 http://17	 2.20.0.250/wizara ♀ ◆ ♥ ₱j pfSense.localdomain - Wizar ×	□ × }☆ ۞ 🙂
Wizard	/ pfSense Setup / Configure WAN Interface 0	^
	Step 4 of 9	
Configur	e WAN Interface	
	On this screen the Wide Area Network information will be configured.	
SelectedTy	pe Static 🗸	
General	configuration	
MAC Addre	This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with nome cable connections). Enter a MAC address in the following format: xccoccccccccc or leave blank.	
мт	TU Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.	
M	88	~

#### L'interface Lan est déjà configurée

		-		×
🗲 🛞 🗖 http://172.2	0.0.250/wizarc 🔎 👻 💆 pfSense.localdomain - Wizar ×	ĥ	121	\$ <del></del>
pf sense		Ξ		^
WARNING: The Manager.	'admin' account password is set to the default value. Change the password in the User			
Wizard /	pfSense Setup / Configure LAN Interface	Ø		
	Step 5 of 9			
Configure L	AN Interface			
	On this screen the Local Area Network information will be configured.			
LAN IP	172.20.0.250			
Address	Type dhcp if this interface uses DHCP to obtain its IP address.			
Subnet Mask	24	~		
	≫ Next			~

On change le mot de passe de l'admin Par défaut

On clique sur reload pour appliquer la configuration

<€⊜	http:// <b>172.20.0.2</b>	50/wizarc 🔎 👻 🗗 pfSense.localdomair	- Wizar ×	□ × ☆ ☆ ©	€0	http://192.168.1.250/wizard; /2 = C	- □ × 命☆藥 😌
	pf sense			A .		ofsense	
	Wizard / pfSe	nse Setup / Set Admin WebGUI Pas	sword O			Wizard / pfSense Setup / Reload configuration	0
	Set Admin WebGU On t SSH	UI Password his screen the admin password will be set, which is use I services if enabled.	d to access the WebGUI and also			Sig.7 d 9	
	Admin •• Password	***				Reload configuration	
	Admin Password AGAIN	•••	•			Click 'Reload' to reload pfSense with new changes.	
	»	Next		~		> Reload	



#### On peut relancer le Wizard en cas d'erreurs En allant dans **Système +Setup Wizard**

fisense	System - Interface			Dia		
Status / C	Advanced Cert. Manager			, je L	• • • • • • • • • • • • • • • • • • •	+ 0
System Info	High Avail, Sync	۵ و بر	Interface	es		F 0 0
Name	Logout (admin)		de WAN	•	1000baseT <full-duplex></full-duplex>	192.168.1.250
User	Package Manager	cal Database)	-LAN	•	1000baseT <full-duplex></full-duplex>	172.20.0.250
System	Routing Setup Wizard	ə b031131d2a39a410	A OPT1	*	1000baseT <full-duplex></full-duplex>	192.168.2.250
BIOS	Update User Manager	ologies LTD				
/ersion	2.4.5-RELEASE-p1 (a built on Tue Jun 02 1 FreeBSD 11 3-STABL	md64) 7:51:17 EDT 2020				

3- La mise en place de la configuration du clavier en fr de façon permanente En même temps on en profite pour installer VMware tools

Dans cette étape on installe les paquets shellcmd et VMWare tools



🗲 💮 👿 http://192.168.1.250/pkg.mgr.p. ρ + C 🛛 🖉 pf5ense.Bachelee.fr - Syste Χ		🔿 🖬 http	://192.168.1.25	i0/pkg_mgr.p ,0 + C 🚮 pfSense.	bachelor.fr - Syste ×		- □ × ଜ☆@@
D/Sense, System • interfaces • rirewaii • Services • vrvi • status • Diagnostics • help •		of sense	System	ı ▼ Interfaces ▼ Firewall ▼	Services - VPN - SI	tatus ▼ Diagnostics ≁ Help ▼	
System / Package Manager / Available Packages	0	System	/ Packa	age Manager / Avail	Auto Config Backup Captive Portal		0
Installed Packages Available Packages		Installed Pac	kages Aw	ailable Packages	DHCP Relay DHCP Server		
Search	0	Search			DHCPv6 Relay DHCPv6 Server & RA		. •
Search sem Vitiware tools Enter a search string or *nix regular expression to search package names and descriptions	Search Diear	Search terr	n	VMware tools	DNS Forwarder DNS Resolver	Both Q Search D G	Desr
Packages		Packages		Line a search song or more	Dynamic DNS IGMP Proxy	package names and descriptions.	
Name Version Description		Name	Version	Description	Load Balancer		
Open-VM- 10.1.0_4.1 VMware Tools is a suite of utilities that enhances the performance of the virtual machine's Tools system and improves management of the virtual machine.	s guest operating 3 + Install	Open-VM- Tools	10.1.0_4,1	VMware Tools is a suite of util system and improves manage	NTP PPPoE Server	ormance of the virtual machine's guest operati	ing 🕂 Install
Package Dependencies:				Package Dependencies:	Shellornd		

Tapez cette commande kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbddans le champcommande puis redémarrer votre machine pfsense et vérifiez que le clavier est en AZERTY

🔿 🚮 http://192.1	168.1.250/pkg.phj 🔎 👻 👩	🛿 pfSense.bachelor.fr - Packa 🛛	c .	-	□ ☆☆{
ofisense					≡
Package /	Services: Shellcr	md Settings			. 0.
Command	Shellcmd Type	Descriptio	n		
Command	Shellcmd Type	Descriptio	on 	+ Add	
Command	Shellcmd Type	Descriptio		+ Add	

🗇 ன http://192.168.1.250/pkg_ed 🔎 = 🖒 🚮 pfSense.bachelor.fr - Servic ×	
fsense	
Edit	0
Shellcmd Configuration	
ommand	
kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd	
inter the command to run.	
ihellcmd Type	
shellcmd	Ý
hoose the shelicmd type. Click Info for details.  ()	
escription	
mettre le clavier en fr	
nter a description for this command. (This is for your reference only.)	



- A- Sécurisez la console par mot de passe
- B- Sécurisez l'accès par ssh
- C- Sécurisez L'interface web par https
  - a- Créer une autorité de certification interne
  - b- Générer un certificat web
  - c- Injecter le certificat web dans mon serveur pfsense

#### A- Sécuriser la console Pfsense

n • Interfacee anced Manager anal Setup . Avail. Sync but (admin) cage Manager	s · Firewall · Services ·	VPN - Status	• Dia :es	ignostics + Help + 1000baseT «full-duplex»	€ + € € € € 192.168.1.250
enced Manager eral Setup . Avail. Sync out (admin) tage Manager	F O O	Interfac	es ↑	1000baseT <full-duplex></full-duplex>	+ 0 / 0 0 192.168.1.250
Avail. Sync Avail. Sync aut (admin) age Manager	cal Database)	Interfac	es	1000baseT <full-duplex></full-duplex>	<b>₽ 0 0</b>
out (admin) age Manager	cal Database)	# WAN	1	1000baseT <full-duplex></full-duplex>	192.168.1.250
age Manager	cal Database)	± 140			
		I LAN	•	1000baseT <full-duplex></full-duplex>	172.20.0.250
ing p Wizard	ə b031131d2a39a410	<b>DMZ</b>	•	1000baseT <full-duplex></full-duplex>	192.168.2.250
ate	ologies LTD				
Manager	2 2020				
RELEASE-p1.(ar n Tue Jun 02 17 SD 11.3-STABLE	md64) 7:51:17 EDT 2020 E				
	p Wizard ate Manager RELEASE-p1 (a n Tue Jun 02 1. SD 11.3-STABLi atem is on the	wizzed         stogies LTD           Manager         2 2020           RELEASE-p1 (amdd4)         n Tue Jun 02 17:51:17 EDT 2020           SD 113-5 TABLE         SD 113-5 TABLE	witzed         Jogies LTD           Manager         2 2020           RELEASE [1 (amd64)]         n Tue Jun 02 17:51:17 EDT 2020           SD 113-STABLE         SD 113-STABLE	witzed         Jogies LTD           Manager         12 2020           RELEASE (1 amd 6/)         n Tue Jun 02 17.51:17 EDT 2020           D0 113-STABLE         Image: 1 amd 6/2	witzer         Jogies LTD           Manager         2 2020           RELEASE / Lam640         n Tue Jun 02 17:51:17 EDT 2020           DS 11:3-STABLE

#### vous cochez la case console menu et vous Sauvegardez



On constate que ma console à un login



#### B- Sécurisez l'accès par ssh

On active ssh pour accéder à la console de manière sécurisée on change le port par défaut en (2121) en terme de sécurité il est toujours conseillé de changer les port par défaut; on peut aussi faire une authentification avec clé **privé/publique** au lieu d'une authentification par mot de passe



Maintenant il faut une **règle** autorisant **ssh** sur l'interface **Wan** on va dans le menu **interface** +**rule** + **ad** 

<i>pf</i> sen	ise <sup>Sys</sup>	stem 🛨 🗌	Interfaces 🚽	Firewall 🗸	Servi	ces 👻 VPI		Status 👻	Diagnost	ics 🗕 🛛 He			5	•
Firew	all / Rul	es / WA	Ν	Aliases NAT								≢⊌	ш 🔳	0
Floating Rules	WAN	LAN - hange Ord	OPT1 er)	Rules Schedules Traffic Shape Virtual IPs	er									
	States	Protocol	Source		Port	Destination	Port	Gateway	Queue	Schedule	Description		Action	ns
×	0 /40 KiB	*	RFC 1918 ne	tworks	*	* .	*	*	*		Block private networks	;	•	
× 1	0 /7 KiB	*	Reserved Not assigned	d by IANA	*	*	*	*	*		Block bogon networks		•	
														_

On rentre les choix ci-dessous après il ne faut pas oublier d'enregistrer et d'appliquer les changements comme indiqué dans ces captures d'écrans.

	250/firewall_rules_edit.php?if=w	an&after=- 🎗 🕶 🖒	🗾 pfSense.bachelor.fr - Firewa	×		1.1.1		
pf	sense System	Interfaces -	- Firewall - Servic	es ▼ VPN ▼	Status -	Diagnostics -	Help 👻	e
F	Firewall / Rules /	Edit						÷ ⊡ ≡ 0
	dit Firewall Rule							
	Action	Pass Choose what to o Hint: the differen whereas with blc	do with packets that match th ice between block and reject ock the packet is dropped sile	e criteria specified b s that with reject, a p ntly. In either case, th	pelow. backet (TCP RST of the original packet	r ICMP port unreac	hable for UDP) is retu	irned to the sender,
	Disabled	Disable this re Set this option to	ule o disable this rule without rem	oving it from the list				
	Interface	WAN Choose the inter	face from which packets mu	t come to match this	<b>v</b>			
	Address Family	IPv4	ot Protocol version this sub-s	aplice to				
	Protocol		et Protocol version this rule a	ppiles to.	>			
s	Source	Choose which IP	protocol this rule should ma	ich.				and a second s
	Source	Invert match	any			▼ Source /	ddress	
		Display Advance The Source Port its default value,	Range for a connection is typ any.	ically random and al	most never equa	to the destination p	ort. In most cases th	is setting must remain at
Destination								
Destinatio	on 🗆 Invert match	C	WAN address		~	Destination A	ddress	/ ~
Destination Port Rang	ge (other) From	<b>→</b>	2121 ] ustom	(other) To	~	2121 Custom		
	Specify the desti	nation port or po	ort range for this rule. The	"To" field may be l	left empty if on	y filtering a single	e port.	
Extra Options								
Lo	Dog Cog packets to Hint: the firewall the Status: Syste	hat are handled has limited loca m Logs: Setting	by this rule Il log space. Don't turn on Is page).	logging for everyth	hing. If doing a	ot of logging, cor	nsider using a rem	ote syslog server (see
Descriptio	A description ma log.	y be entered her	re for administrative refere	ence. A maximum	of 52 characte	s will be used in	the ruleset and dis	played in the firewall
Advanced Option	ns Display Advance	ed						
Rule Information								
Tracking	ID 1640165746							
Create	ed 12/22/21 10:35:4	6 by admin@17	72.20.0.14 (Local Databas	e)				
Update	ed 12/22/2110:39:	i3 by admin@17	72.20.0.14 (Local Databas	e)				
	Save							
Après avoire e	enregistrer	Save	applique les c	nangemer	nts 🔽	ply Changes		

< 🔊 🗹 http://192.1	68.1.250/firewall	_rules.php?if=wan		,○ - Ċ 🗾 pfSense.bacheld	or.fr - Fire	wa×						
	<i>pf</i> isens	e System					/PN - 9	Status 👻	Diagno	stics 👻	Help 👻	( <del>)</del>
	Firewal	II / Rules	/ WAN									≢ Lui 📼 Ø
	The firewal The change	Il rule configura es must be app	ition has bee lied for them	n changed. to take effect.								✓ Apply Changes
	Floating	WAN	LAN D	MZ								
	Rules (D	rag to Chan	ge Order)		:	et a t						
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	Ó /0 B	* : : :	RFC 1918 networks	*	*	*	*	*		Block private networks	•
	*	0 /247 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	•
		0 /0 B	IPv4 TCP	*	*	WAN net	22 (SSH)	*	none		Laisser passé ssh	₺₡₪₡₶
										bbA 🕇	🕽 Add 🛍 Delete	🖞 Save 🕂 Separator

Attention sur Windows 2016 ssh n'est pas installé nativement contrairement à Windows 2019 ou Windows 10 sur ces deux dernière version ssh est parmi les fonctionnalités qu'on peut installer. Donc pour Windows 2016 suivre la procédure du fichier ssh\_2016.docs pour installer ssh

On teste la connexion à l'intérieure de notre périmètre j'utilise une des machines dans un Lan : Je prends la machine AD je démarre le PowerShell et je me connecte sur une des interfaces de pfsense :

Le serveur pfsense m'envoie l'empreinte numérique de sa clé publique :



On peut vérifier si l'empreinte numérique sur le serveur ssh est la même que celle envoyée par le serveur j'affiche le contenu détaillé du répertoire /etc/ssh après je génère l'empreinte numérique de la clé publique ssh\_host\_ed25519\_key.pub

en suivant les étapes 1+2+3+4

En fin je compare les deux empreintes on constate qu'elles sont identiques



Maintenant on va tester la connexion en dehors de notre périmètre **Wan, sitka\_Lan et opt\_lan** On va essayer une connexion de notre machine physique qui est en dehors de ce périmètre

Vindows PowerShell ×	+ ~		
PS C:\> ssh admin@192.168	1.250		
<pre>ssh: connect to host 192.; PS C:\&gt;</pre>	168.1.250 port 22:	Connection timed	out

On remarque qu'il y'a **échec de connexion** ; on essaye de faire un **ping** sur cette interface, même constat

2 Windows PowerShell × + ∨
PS C:\> ping 192.168.1.250
Envoi d'une requête 'Ping' 192.168.1.250 avec 32 octets de données : Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Statistiques Ping pour 192.168.1.250: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), PS C:\>

Cet échec est normal car PfSense bloque toutes requêtes venant d'une adresse privée en dehors de son périmètre **Wan, sitka\_lan et opt\_lan,** on peut vérifier ceci aisément en allant dans le menu **Interface + Wan** tout en bas de la page on trouve deux cases cochées ce qui explique ce blocage

A ttp://192	.168.1.250/interfaces.php?if=wan	P - ¢ <u>⊅</u>	pfSense.bachelor.	fr - Interfa ×		
	pf sense System	- Interfaces -	Firewall 👻	Services -	VPN -	Status 👻
	Interfaces / WAN	Assignments				
		WAN				
	General Configuratio			.:		
	Description	WAN				
		Enter a description (n	ame) for the int	erface here.		
	IPv4 Configuration Type	Static IPv4				$\checkmark$
	IPv6 Configuration Type	None				~
Reserved Networks						
Block private networks and loopback addresses	Decks traffic from IP addresses that are RFC 4193 (fc00::/7) as well as loopback private address space, too.	reserved for private networks j addresses (127/8). This option	per RFC 1918 (10/8, 1 should generally be t	72.16/12, 192.168/10 aurned on, unless this	5) and unique loca network interface	al addresses per e resides in such a
Block bogon networks	Description: Blocks traffic from reserved IP addresse routing table, and so should not appear a Note: The update frequency can be chan	s (but not RFC 1918) or not yet is the source address in any pa ged under System > Advanced,	assigned by IANA. Bo ckets received. Firewall & NAT settir	ogons are prefixes tha gs.	t should never ap	opear in the Internet
	P Save					

On trouve la même chose dans les règles par défaut de l'interface wan

<i>pf</i> se	nse <sup>Sys</sup>	tem <del>+</del> li	nterfaces <del>-</del>	Firewall -	s	ervices -	VPN -	Status -	Diagn	ostics -	Help 👻	
	annaithe an			Aliases	u <sup>7</sup> e		1					
Fire	wall / Rule	es / WAI	N	NAT								
				Rules								
Floati	ng WAN	LAN	DMZ	Schedules	5					3 6		
		•		Traffic Sh	aper					les dei	ux regles qui nous bloq	ues
Rule	s (Drag to Cl	nange Orde	er)	Virtual IPs	3	1977 1977 - 1977		11:	ā a	* =		÷
Rule	s (Drag to Ch States	nange Orde Protocol	er) Source	Virtual IPs	Port	Destination	Port	Gateway	Queue	Schedule	Description V	Actions
Rule	s (Drag to Ch States 0 /0 B	Protocol	er) Source RFC 1918 ne	Virtual IPs etworks	Port *	Destination	Port *	Gateway *	Queue *	Schedule	Description Block private network	Actions s 🔅
Rule	s (Drag to Ch States 0 /0 B 0 /138 KiB	Protocol * *	er) Source RFC 1918 ne Reserved	Virtual IPs etworks	Port * *	Destination * *	Port * *	Gateway *	Queue * *	Schedule	Description Block private network Block bogon networks	Actions s O
Rule:	s (Drag to Ch States 0 /0 B 0 /138 KiB	nange Orde Protocol * *	er) Source RFC 1918 ne Reserved Not assigne	Virtual IPs etworks d by IANA	Port * *	Destination * *	Port *	Gateway *	Queue *	Schedule	Description Block private network Block bogon networks	Actions S O Actions

Maintenant on va essayer d'accéder à notre serveur PfSense à partir de l'extérieur en utilisant notre adresse publique. Tout d'abord :

1- Il faut accéder à la boxe internet et ouvrir le port 22 en créant une redirection de port

÷ .	Service	Adresse IP du serveur	Protocole	Ports externes	Ports internes	Activer la règle
^	Utilisateur					
E	SSH	192.168.1.250	TCP/UDP	22 • 22	22 • 22	on

- 2- Ensuite il faut déterminer notre adresse publique soit à partir de la boxe ou un site internet http://www.whatismyip.com
- 3- Après sur notre smartphone on télécharge un client ssh sur Soogle Play google store Juicessh



JuiceSSH - SSH Client

- 4- Sur notre smartphone il faut qu'on se mette en 4G et non en wifi car il na faut pas oublier que PfSense bloque les connexions provenant d'adresse IP en dehors de son périmètre.
- 5- On ouvre l'application et on commence à établir notre connexion ssh

On sélectionne connexion rapide



ssh adm	nin@ ac	lresse	publiq	ue
---------	---------	--------	--------	----

:05 🐜 <b>နေ ဂတ</b> ရာ လာ	(t) 🕸 🗗	99
Connexion rapide Connect to a new host		4
Connexions fréquentes Vos connexions les plus utilisées		*
Connexion rapide		
Type: SSH Votre	adresse pu	ıblique
admin@		
Enregistrer la connexior	1	
	ANNULER	ок
Paramètres Personnaliser vos sessions		00
Aide Voir notre FAQ		?
Modules		ċ.

Le serveur nous envoie l'empreinte de sa clé publique On constate que c'est la même que celle qu'on a calculé Sur le serveur

EM/HtKbrYNKa5kIX9gpC/txmQri9GrM2UmCoX7Lf3TE rentre le mot de passe admin



Après on tombe sur notre console PfSense

21:52 VMwarc Virte	Me 🕹 💷 📢 Wal Machino — Nof to pfSense 2.4.5	tgato Device ID: e 5-RFLFASE-pl (amd6	a366031131d2a1 4) on pfSense	194410 ***	2 🛛 🖉 7	1 % 🖬
LAN (lan) DHZ (opt1)	→ cm0 → cm1 → em2	→ v4: 192.168 → v4: 172.20. → v1: 192.168	0.250/24 .2.250/24 .2.250/24			
<ul> <li>e) Logout</li> <li>1) Assign</li> <li>2) Set inti</li> <li>3) Reset w</li> <li>4) Reset t</li> <li>5) Reboot</li> <li>6) Hall sys</li> <li>7) Ping has</li> <li>8) Shell</li> <li>Enter an op</li> </ul>	(33H onLy) Interfaces mrface(s) TP add bhConfigurator p b factory default system st tion:	9) per. 10) Fil ress 11) Res assword 12) PHP ts 13) Upd 14) Dis 15) Res 16) Res	op ter Logs tart webConfig shall + pfSer ate from consc able Secure Sf lore recent co tart PHP-FPH	gurator ise tools ble mfiguratic		
ESC	/ 1	- HOME		END	PGPRÉ C	FN
ТАВ	CTRL A	LT 🔶	Ļ	→ F	osuiv	

- D- Sécurisez L'interface web par https
   1- Créer une autorité de certification interne

On va dans le menu système + CertManager

	anced_admin.php 🔎		
<i>pf</i> sense	System - Interfa	ces + Firewall + Services + VPN + Status + Diagnostics + Help +	•
System /	Advanced Cert. Manager	nin Access	0
Admin Acces	General Setup High Avail. Sync Logout (admin)	Networking Miscellaneous System Tunables Notifications	
webConfig	Package Manager		
	Setup Wizard	O HTTPS (SSL/TLS)	
	Update User Manager	om port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect imm	nediately

On commence à créer une autorité de certification interne

🗇 🛃 http://192.168.1.250/system_camanager.php	,오 ▾ ở 🚮 pfSense.bache	elor.fr - Syste ×			
pfsense System	<ul> <li>Interfaces → Firewall →</li> </ul>	Services - VPN -	Status - Diagnostics -	Help +	C)
System / Certific	ate Manager / CAs				0
CAs Certificates	Certificate Revocation				
Search					•
Search term	1		Both	Q Search 🕽 Clear	
	Enter a search string or *nix regu	ular expression to search certific	cate names and distinguished nam	nes.	
Certificate Authoritie	?S				
Name Internal	Issuer	Certificates D	istinguished Name	In Use Actio	ons
					+ Add

On remplit les champs suivants

	- Interfaces - Firewall -	Services - VPN -	Status 🗸	Diagnostics -	Help 🗸	<b>4</b> 5 G
System / Certific	ate Manager / CAs / Ed	it				0
	, <u>.</u>					_
CAs Certificates	Certificate Revocation					
Create / Edit CA						
Descriptive name	Autorité de certification Sitka					
Method	Create an internal Certificate Auth	ority	~			
Trust Store	Add this Certificate Authority to t When enabled, the contents of the C	the Operating System Trust St CA will be added to the trust st	ore tore so that the	ey will be trusted by th	ne operating syste	em.
Randomize Serial	Use random serial numbers whe When enabled, if this CA is capable checked for uniqueness instead of u	n signing certifices of signing certificates then se using the sequential value fro	erial numbers f m Next Certific	or certificates signed ate Serial.	by this CA will be	e automatically randomized and
Internal Certificate A	uthority					
Key type	RSA		~			
	2048		~			
	The length to use when generating a The Key Length should not be lower	a new RSA key, in bits. than 2048 or some platforms	may consider	the certificate invalid	I.	
Digest Algorithm	sha256		~			
	The digest method used when the C The best practice is to use an algori	A is signed. thm stronger than SHA1. Som	ne platforms m	ay consider weaker d	ligest algorithms	invalid
Lifetime (days)	3650					
Common Name	internal-ca-sitka					
	The following certificate authority se	ubject components are option	al and may be	left blank.		
Country Code	FR		~			
State or Province	IDF					
City	Paris					
Organization	sitka					
Organizational Unit	SK					
	Save					

Une fois qu'on enregistre nos paramètre notre autorité de certification apparait, on appuie sur le crayon pour éditer notre CA

System - System -	Interfaces	✓ Firewa	ll <del>-</del> Servio	ces 👻 VPN	- Status	- Diagnos	tics <del>-</del>	Help 🗸		<b>4</b> 5	(
System / Certificat	te Manage	er / CAs									0
CAs Certificates	Certificate Revo	cation									
Search											e
Search term						Both	$\sim$	Q Search	D Clear		
	Enter a search	string or *nix	regular express	sion to search c	ertificate names	and distinguish	ned names				
<b>Certificate Authorities</b>											
Name	Internal	Issuer	Certificates	Distinguis	ed Name				In Use	Actions	
Autorité de certification Sitka	~	self-signed	0	ST=IDF, OL	I=SK, O=sitka, L=	Paris, CN=inter	nal-ca-sitk	a, C=FR 🚺			Ci
				Valid From: \$ Valid Until: T	Sat, 27 Nov 2021 2 ue, 25 Nov 2031 2	1:31:04 +0100 1:31:04 +0100				•	
											- 4

On affiche notre certificat et la clé publique qui lui est associé

System / Certific	ate Manager / CAs / Edit
CAs Certificates	Certificate Revocation
reate / Edit CA	
Descriptive name	Autorité de certification Sitka
Method	Import an existing 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 certifices When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized checked for uniqueness instead of using the sequential value from Next Certificate Serial.
xisting Certificate A	uthority
Certificate data	BEGIN CERTIFICATE MIIEIDCCAwigAwIBAgIIPmg7cGMSa8swDQYJKoZIhvcNAQELBQAwZD EaMBgGA1UE Axt/NRah/50ZXJuYNwtY2Etc210a2ExCzAJBgN/BAYTAkZSMQwwCgYDVQ QIEwNJREYx Paste a certificate in X.509 PEM format here.
Certificate Private Key (optional)	BEGIN PRIVATE KEY MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC70e kV1xgQcd/7 FiH4jAa0qAii45sMXSP9Ts6INa7J2Qd88szCh2CUBvggG9V9VX2T8r hlebXA+BWH Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (C

2- Générer un certificat web

Maintenant on va créer notre certificat web délivrer par la CA **autorité de certification sitka** qu'on a mis en place dans l'étape précédente il suffit de cliquer sur add et remplir les champs nécessaires

sense, System -	Interfaces 🕶	Firewall 👻	Services -	VPN -	Status 🗸	Diagnostics -	Help 🛨		C
System / Certifica	te Manager /	Certificate	es						Ø
CAs Certificates	Certificate Revocation	n							
Search Search term					В	oth	♥ Q Search	Clear	Θ
Certificates	Enter a search strin	g or *nix regular	expression to e	search certifica	te names and	i distinguished nan			
lame	lssuer	Distinguish	ed Name				In Use	Actions	
vebConfigurator default 6001f6f281597) Server Certificate 2A: <b>No</b> Server: <b>Yes</b>	self- signed	O=pfSense i Valid From: F Valid Until: Th	webĊonfigurat iri, 15 Jan 2021 21 hu, 17 Feb 2022 2	or Self-Signed ( 1:11:30 +0100 1:11:30 +0100	Certificate, CN	N=pfSense-6001f6f	281597	<b>₩</b> Q, <b>1</b> û	
									+ Add/Sig

ci-dessous les champs remplie pour créer notre certificat

COMMUNITY EDITION	v Interfaces  ▼ Firewall  ▼ Services  ▼ VP	N <del>•</del> Status <del>•</del>	Diagnostics <del>-</del>	Help +	<b>\$</b> 5	•
System / Certific	ate Manager / Certificates / Edit					0
CAs Certificates	Certificate Revocation					
Add/Sign a New Cert	ficate					
Method	Create an internal Certificate	~				
Descriptive name	Certificat SSL pour le serveur web Heimdall					
Internal Certificate						
Certificate authority	Autorité de certification Sitka	~				
Key type	RSA	~				
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some plat	✔ tforms may consider t	he certificate invalid	L		
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA*	I. Some platforms ma	y consider weaker d	igest algorithms invalid		
Lifetime (days)	3650 The length of time the signed certificate will be valid, in day Server certificates should not have a lifetime over 398 days	s. or some platforms m	ay consider the certi	ficate invalid.		
Common Name	heimdall.sitka.local					
	The following certificate subject components are optional a	and may be left blank.				
Country Code	FR	~				
State or Province	IDF					
City	Paris					
Organization	sitka					
Organizational Unit	SK					

Certificate Attributes								
Attribute Notes	The following attributes are added to certific selected mode.	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	v						
	Add type-specific usage attributes to the sig	ned certificate: used for placing usage restrictions on, or granting abilities to, the signed certificate.						
Alternative Names	FQDN or Hostname 🗸	heimdall.sitka.local						
	FQDN or Hostname	pfsense.sitka.local						
•	IP address 🗸	172.20.0.250						
	IP address	192.168.1.250						
	IP address 🗸	192.168.2.250						
		www.heimdall.local						
	Туре	Value '						
	Enter additional identifiers for the certificate signing CA may ignore or change these value	in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The es.						
Add	+ Add							
	Save							

# Une fois qu'on enregistre notre certificat apparait

Sense System - I	Interfaces - Firewall -	Services - VF	PN <del>-</del> Status -	<ul> <li>Diagnostics</li> </ul>	▪ Help ▪ .	<b>4</b> 5	
System / Certificate M	Aanager / Certifica	tes					0
Created internal certificate Certific	at SSL pour le serveur web He	eimdall					8
CAs Certificates Certif	icate Revocation						
Search Search term Ent	er a search string or *nix regu	lar expression to search	certificate names	Both and distinguished n	Q Search ames.	DClear	9
Certificates Name	Issuer	Distinguished Name	• •		In Use	Actions	
webConfigurator default (61a2591ac0fff) Server Certificate CA: <b>No</b> Server: <b>Yes</b>	self-signed	O=pfSense webConfig 61a2591acOfff () Valid From: Sat, 27 Nov 24 Valid Until: Fri, 30 Dec 202	ourator Self-Signed 021 17:13:14 +0100 22 17:13:14 +0100	Certificate, CN=pfS	ense-	<b>∥₩₽</b> ₽₿₿	
Certificat SSL pour le serveur web Heimdall Server Certificate CA: No Server: Yes	Autorité de certification Sitka	ST=IDF, OU=SK, O=sit Valid From: Sat, 27 Nov 20 Valid Until: Tue, 25 Nov 20	ka, L=Paris, CN=he 021 22:21:01 +0100 031 22:21:01 +0100	imdall.sitka.local, C	=FR <b>③</b>	<b>∥₩₽</b> ∎C`@	•
						+	Add/Sig

3- Injecter le certificat web dans mon serveur PfSense

Maintenant on va injecter notre certificat dans notre serveur web PfSense, donc on va dans **système** + **Avanced** 

- On sélectionne notre certificat crée
- On laisse le port par défaut
- On laisse 2 en nombre de connexion simultané c'est-à-dire 2 personne max peuvent se connecter sur l'interface web PfSense

Notifications

- On refuse la connexion en http
- On refuse que le navigateur enregistre les données de connexion

Admin Access Firewall & NAT Networking Miscellaneous System Tunables

webConfigurator	
Protocol	O HTTP
SSL/TLS Certificate	Certificat SSL pour le serveur web Heimdall
TCP port	Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Max Processes	2 Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
WebGUI redirect	Disable webConfigurator redirect rule When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.
HSTS	Disable HTTP Strict Transport Security When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)
OCSP Must-Staple	Force OCSP Stapling in nginx When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.
WebGUI Login Autocomplete	Enable webConfigurator login autocomplete When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

### Après on sauvegarde notre navigateur va démarrer automatiquement On se connecte sur l'interface https://172.20.0.250

🗾 Heimdall.sitka.local - Sta	tus: Dash 🗙 🕂		✓ - □ ×
	sécurisé https://172.20.0.250		
COMMUNITY EDITION	System - Interfaces - Firewall - Services - V	/PN → Status → Diagnostics → Help →	<b>4</b> 6 C+
Status /	Dashboard		+ 0
System Inf	formation 🖉 🗩 👄 😣	Netgate Services And Support	$\bigcirc \otimes$
Name	Heimdall.sitka.local	Contract type Community Support	
User	admin@172.20.0.14 (Local Database)	Community Support Or	yly
System	VMware Virtual Machine Netgate Device ID: <b>74a1573f04e3a4d71064</b>	NETGATE AND pfSense COMMUNITY SUPPO	RTRESOURCES
BIOS	Vendor: <b>Phoenix Technologies LTD</b> Version: <b>6.00</b> Release Date: <b>Thu Nov 12 2020</b>	If you purchased your pfSense gateway firewall a Netgate and elected <b>Community Support</b> at the	ppliance from point of sale or
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE	installed pfSense on your own hardware, you hav various community support resources. This includ RESOURCE LIBRARY.	e access to les the NETGATE

Le certificat représente des erreurs car notre autorité de certification n'est pas de confiance donc il faut l'intégrer dans le magasin des autorités de certification de confiance en installant le certificat de l'autorité racine

		×
	👻 😵 Erreur d	le certificat 🖒 Rechercher 🔎 🗸 🛱 😃
💋 pfSense - Login 🛛 🗙 📑		
<b>pf</b> sense		Général Détails Chemin d'accès de certification
		Informations sur le certificat Impossible de vérifier ce certificat auprès d'une Autorité de certification de confiance.
	SIGN	Délivré à : heimdall.sitka.local Délivré par : internal-ca-sitka
	Password	Valide du 27/11/2021 au 25/11/2031
	SIGN I	Installer un certificat Déclaration de l'émetteur
		ОК

### Protection de la connexion

Login Protection	on	
Thre	eshold	8
		Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.
Bloc	cktime	180
		Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.
Detection	n time	259200 ×
		Remember potential attackers for up to detection_time seconds before resetting their score.
Wh	nitelist	Address / 128
		Addresses added to the whitelist will bypass login protection.
Add ad	dress	+ Add address



# A- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur le serveur active directory hermes

- 1- Connectivité LDAP
- 2- Connectivité LDAPS (LDAP sur SSL)
  - a- Création d'une autorité de certification sur le contrôleur de domaine hermes
    - i- Ajouter le rôle certificat sur hermes
    - ii- Configuration du rôle certificat sur hermes
- B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)
- C- Création des comptes utilisateurs sur le contrôleur de domaine
- D- Création des authentifications LDAP et LDAPS sur le serveur pfsense

# E- Création de l'authentifications LDAP

- 1- Création de l'authentifications LDAP
- 2- Création de l'authentifications LDAPS
  - a- Création du formulaire de l'authentification LDAPS
  - b- Analyse avec Wire Shark du trafic pfsense active directory
  - c- Exportation du certificat de l'autorité de certification hermes
  - d- Importation du certificat de l'autorité de certification racine
  - e- Test de la connexion ssl entre pfsense et le contrôleur de domaine
- 3- Utilisation des authentifications LDAP et LDAPS sur le serveur pfsense
  - a- Vérification de l'authentification LDAP et LDAPS
  - b- Création et configuration d'un groupes sur pfsense
  - c- Test de connexion sur l'interface web avec un compte ldap

## A- Test de la connectivité LDAP et LDAPS sur le serveur active directory hermes

#### 1- Connectivité LDAP

Sur le contrôleur de domaine on test la connectivité LDAP standard, donc clique droit sur le menu démarrer + exécuter puis on tape **ldp.exe** pour ouvrir l'explorateur LDAP

	Paramètres	I Exécuter X
	Explorateur de fichiers	Entrez le nom d'un programme, dossier, document ou
	Rechercher	ressource interiet, et vintuows rouvina pour vous.
	Exécuter 2	Ouvrir : Idp.exe   Cette tâche sera créée avec les autorisations d'administrateur.
	Arrêter ou se déconnecter >	
	Bureau Clique droit	OK Annuler Parcourir
-	Tapez ici pour effectuer une recherche	

Un fois l'explorateur LDAP est ouvert l'explorateur on choisit le menu Se connecter et on rentre le nom du serveur **hermes.sitka.local** ainsi que le port de connexion **389** 

Connecion Parcourir Affichage Options Outils ?	× Se connecter	$\times$
Lier Ctri+8 Se déconnecter	Serveur : hermes	
Nouveau Ctrl+N Enregistrer Enregistrer sous	Port : 389 Non connecté	
Quitter	OK Annuler	

La connexion à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire



2- Connectivité LDAPS (LDAP sur SSL)

On fait la même chose que la procédure établissant une connexion standard on change juste le numéro de port et on coche ssl

Paramètres	🖾 Exécuter 🛛 🗙
Explorateur de fichiers	Entrez le nom d'un programme, dossier, document ou
Rechercher	ressource Internet, et Windows l'ouvrira pour vous.
Exécuter 2	Ouvrir : Idp.exe ~
Arrêter ou se déconnecter >	Cette tâche sera créée avec les autorisations d'administrateur.
Bureau Clique droit	OK Annuler Parcourir
Talez ici pour effectuer une recherche	

On tombe sur un message d'erreur, le contrôleur de domaine ne supporte pas LDAPS car il n'est pas associé à un certificat.

Connexion Parcourir	Affichage	Options Outils ?	- 🗆 X	Se connecter	×
Se connecter Lier Se déconnecter	Ctrl+B			Serveur : hermes.	sitka.local
Nouveau Enregistrer Enregistrer sous	Ctrl+N			Port : 636	Non connecté
Quitter				ОК	Annuler
1		Ldp onnexion Parcourir	Affichage Options Outils ? Id = Idag_selinit("hermes.sika.local", 636, 1) Error 0 = Idag_set_option(RLdap, LDAP_OP Error 3 = Idag_connect(hLdap, NULL); Server error: «empty» Error «0x51»: Fail to connect to hermes.sikk Ldp Impossible d'ouvrir la connect C	); r_PROTOCOL_VERSION, 3) ;a.local. x exion.	

Il existe deux méthodes pour activer LDAPS (LDAP sur SSL) sur un contrôleur de domaine :

- Mettre un Certificat Racine sur le contrôleur de domaine en installant une autorité de certification racine sur hermes
- Utiliser un certificat tiers sur le contrôleur de domaine. (Hermes)

Pour notre procédure on choisira la première méthode, Donc il faut installer une autorité de certification afin de tirer parti de LDAPS

a- Création d'une autorité de certification sur le contrôleur de domaine hermes

Il est nécessaire d'installer le service autorité de certification. Pour fournir au contrôleur de domaine un certificat qui permettra au service LDAPS d'opérer sur le port 636.

i- Ajouter le rôle certificat sur hermes

Accédez au menu Gérer et cliquez sur Ajouter des rôles et des fonctionnalités.



On vérifie le nom et l'adresse IP de notre serveur on clique après sur suivant

🌇 Assistant Ajout de rôles et de f	onctionnalités	- 0	×	Assistant Aiout de rôles et de fonctionnalités		_	п×
Avant de comme	Encer services de rôle ou des fonctionnalités	EUR DE DESTINATIO hermes.sitka.loc	N al	Sélectionner le serveur de	destination	SERVEUR (	DE DESTINATION bermes.sitka.local
Avail de confinence Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Cet Assistant permet d'installer des roles, des services de role ou des fonctionnalités. Yous devez détermine relardies, services de role ou fonctionnalités à installer en fonction des becions informatiqu de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web. Pour supprimer des rôles, des services de rôle ou des fonctionnalités Demarrer l'Assistant de Suppression de rôles et de fonctionnalités Avant de continuer, vérifier que les travaux suivants ont été effectués : • Le compte d'administrateur possède un mot de passe fort • Les paramètes réseau, comme les adresses IP statiques, sont configurés Les dennières mise à jour des écurité de Window: Update sont installées Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.	Jes	Avant de commencer Type d'installation Sélection du serveur Roles de serveurs Fonctionnalités Confirmation Résultats Nom Dermes srika	Sélectionner le serveur ou le disque dur virtuel sur lequel installer des rôles et des fon         Sélectionner un serveur du pool de serveurs         Sélectionner un disque dur virtuel         Pool de serveurs         Filtre :         Nom       Adresse IP         Système d'exploitation         Jærmes situalocal       172200.14         Microsoft Windows Server 2022 Data		onctionnalités.	
	Ignorer cette page par défaut  Précédent  Suivant >  Installe	er Annuler		1 ordinateur(s Cette page pr ont été ajouts serveurs hors incomplète ne	) trouvé(s) Esente les serveurs qui exécutent Windo a Taide de la commande Ajouter des s connexion et les serveurs nouvellement sont pas répertoriés. < Précédent	ows Server 2012 ou une version ulté serveurs dans le Gestionnaire de ser ajoutés dont la collecte de donnée Suivant > Installer	trieure et qui rveur. Les s est toujours

On coche Services de Certificats Active Directory et on rejoute les fonctionnalités

🚡 Assistant Ajout de rôles et de fonctionnalités	- 🗆 X	🔁 Assistant Ajout de rôles et de fonctionnalités 🛛 🗙
Sélectionner des rôles de serveurs Avant de commencer Type d'installation Sélection du serveur Rotel de serveurs Rotcionnalités Confirmation Résultats Confirmation	SERVEUR DE DESTINATION hermes.sitialocal a installer sur le serveur sélectionné. appareil Construités de centificats Active Directory (AD CS) servent à créer des associés pour de troites de servicités de centification et les services de role associés pour duitisés dans diverses applications.	Ajouter les fonctionnalités requises pour Services de certificats Active Directory ? Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur. • Outils d'administration de serveur distant • Outils d'administration de roles • Outils de services de certificats Active Directory [Outils] Outils de gestion de l'autorité de certification vertification de roles vertification de roles
	< Précédent Suivant > Installer Annuler	

#### Sur les deux Boites de dialogues ci-dessous on laisse tout par défaut en faisant suivant.



#### On sélectionne que l'option Autorité de certification

ᡖ Assistant Ajout de rôles et de f	fonctionnalités	- 🗆 ×	🔁 Assistant Ajout de rôles et de fonctionnalités	- 🗆 ×
Sélectionner des	services de rôle	SERVEUR DE DESTINATION hermes.sitica.local	Confirmer les sélections d'installation	SERVEUR DE DESTINATION hermes.sitka.local
Avant de commencer Type d'installation Sélection du serveur Roles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Sélectionner les services de rôle à installer pour Services o Services de rôle    Autorité de certification   rascription de l'autorité de certification via le Wel  Bepolardure ni ligne  Service d'inscription de périphérique réseau  Service Web Inscription de certificats  Service Web Stratégie d'inscription de certificats	de certificats Active Directory Description L'inscription de l'autorité de certification via le Vérb fournit une interface Vérb Simple permettant aux utilisateurs d'effectuer des täches tielles que la demande et la recouvellement de certificats, la recouvellement de certificats, la recouvellement de certificats, la recouvellement de certificats, la recouvellement de certificats et l'inscription à des certificats de carte à puce.	Avant de commencer "ybe d'installation Bélication du serveurs Fonctionnalités Ab CS Berlos Confirmation Résultats Résultats AD CS Berlos Confirmation Résultats Rés	cionnalités suivants sur le serveur sélectionné, cliquez sur de destination, si nécessaire (comme des outils d'administration) soient affichées sur omstuguement, Si vous ne voulez pas intaller ces ent pour désactiver leurs cases à cocher. tive Directory de certification
	< Précédent	Suivant > Installer Annuler		

Dernière étape on clique sur le lien Configurer les services Active Directory sur le serveur de destination



ii- Configuration du rôle certificat sur hermes

Une fois le rôle certificat est installé il faut maintenant le configurer, on vérifie les informations d'identification, il est obligatoire d'être connecté avec le compte de l'administrateur de l'entreprise (domaine\administrateur).

On coche après Autorité de certification, toutes les autres options on peut les installer après au besoin



On sélectionne Autorité de certification d'entreprise afin que l'autorité de certification puisse utiliser l'annuaire LDAP



On sélectionne autorité de certification racine

Ce type d'autorité de certification couplé avec un Active Directory est utile pour un intranet mais est déconseillée pour un accès public. Puisque notre autorité n'est pas listée parmi les autorités de certification de confiance, les personnes utilisant des certificats émis par notre autorité de certification auront un avertissement mentionnant que nos certificats ne sont pas de confiance.



# On choisit de créer une clé privée



On choisit nos clés de chiffrage, plus les clés sont longues plus la sécurité est renforcée mais malheureusement les performances vont être impactées.

🔁 Configuration des services de cer	-	- c		$\times$	
Chiffrement pour l	SERVEUR DE DESTINATION hermes.sitka.local			oN	
Informations d'identificati Services de rôle	Spécifier les options de chiffrement				
Type d'installation	Sélectionnez un fournisseur de chiffrement :	Longueur d	e la clé :		
Type d'AC	RSA#Microsoft Software Key Storage Provider	4096			~
Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	Sélectionnez l'algorithme de hachage pour signer les certificats émis SHA256 SHA384 SHA512 SHA1 Autorisez l'interaction de l'administrateur lorsque l'autorité de ce privée.	par cette AC	: cède à la	clé	
	En savoir plus sur le chiffrement				
	< Précédent Suivant >	Configure	r A	nnuler	

On peut modifier les valeurs par défaut ; je choisis hermes-CA comme nom commun de ACR

🏊 Configuration des services de ce	rtificats Active Directory				$\times$
Nom de l'autorité	de certification	SERVEUR	DE DE	STINATI s.sitka.lo	ON Ical
Informations d'identificati Services de rôle Type d'installation Type d'AC Clé privée Chiffrement <u>Nom de l'AC</u> Période de validité Base de données de certi	Spécifier le nom de l'AC Tapez un nom commun pour identifier cette autorité de certification. Le certificats émis par l'autorité de certification. Les valeurs des suffixes o automatiquement, mais elles sont modifiables. Nom commun de cette AC : HERMES-CA Suffixe du nom unique : DC=sitka DC=local	Ce nom est du nom uniq	ajouté jue sor	à tous le at génére	es ées
Confirmation Progression Résultats	Aperçu du nom unique : CN=HERMES-CA,DC=sitka,DC=local En savoir plus sur le nom de l'autorité de certification				
	< Précédent Suivant >	Configure	er 🗌	Annule	r

On rentre le période de validité pour le certificat de l'ACR., la période de validité du certificat de l'autorité de certification doit dépasser la période de validité des certificats émis.

comganation act sections ac et	anneats mente bite					-	
					SERVEUR D	E DESTINA	TION
Periode de validite	0				h	ermes.sitka	local
Informations d'identificati	Spécifier la	période	de validité				
Services de rôle							
Type d'installation	Sélectionnez la	période de va	idité du certifie	at généré pour cette	autorité de certi	fication :	
Type d'AC	(15) Ar	nées	~				
Clé privée	Date d'expiratio	n de l'AC : 09	01/2025 09:45	:00			
Chiffrement	La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la						
Nom de l'AC	période de valid	lité pour les c	ertificats qu'elle	e émettra.			
Période de validité							
Base de données de certi							
Confirmation							
	En savoir plus si	ur la période d	le validité				
	chi suvon pius si	at in periode c	ie vonche				

On laisse les dossiers des bases de données et des logs, par défaut.

🚘 Configuration des services de certificats Active Directory					$\times$
Base de données d	de l'autorité de certification	SERVEUR	DE DE	STINATI s.sitka.lo	ON ocal
Informations d'identificati Services de rôle	Spécifier les emplacements des bases de donné	ées			
Type d'installation	Emplacement de la base de données de certificats :				
Type d'AC	C:\Windows\system32\CertLog				
Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	Emplacement du journal de la base de données de certificats : C:\Windows\system32\CertLog				
	En savoir plus sur la base de données de l'autorité de certification				
	< Précédent Suivant >	Configure	er	Annule	r

L'assistant nous affiche un résumé de la configuration choisit, on lance ensuite le processus de Configuration

On doit obtenir le message configuration réussie

Configuration des services de ce	rtificats Active Directory	_		$\times$
Résultats	SERVEU	R DE DI	ESTINAT es.sitka.l	ION
Informations d'identificati	Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :			
	Services de certificats Active Directory			
Type d'AC	En savoir plus sur la configuration de l'autorité de certification			
Chiffrement				
Nom de l'AC				
Période de validité				
Base de données de certi				
Confirmation				
Progression				
Résultats				
	< Précédent Suivant > Ferme	er	Annul	er

On reteste maintenant notre connexion LDAPS à partir de l'explorateur LDAP La connexion sécurisée utilisant le **ssl** sur le port **636** à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire

Commenter X	daps://hermes.sitka.local/DC=sitka,DC=local – D 🗙
se connecter X	Connexion Parcourir Affichage Options Outils ?
Serveur : hermes.sitka.local Port : 636 Non connecté SSL OK Annuler	Id = kdap_sslinit("hermes sitka.locaf", 636, 1);         Error 0 = iddap_set_option(hLdap,         LDAP_OPT_PROTOCOL_VERSION, 3);         Error 0 = iddap_connect(hLdap,NULL);         Error 0 = iddap_get_option(hLdap,LDAP_OFT_SSL_(void*)&Iv);         Host supports SSL_SSL cipher strength = 256 bits         Established connection to hermes.sitka.local.         Retrieving base DSA information         Getting 1 entries:         Dr: (RootDSE)         configuration,DC=sitka,DC=local;         currentTime: 09/01/2022 10:1/48 Paris, Madrid;         defaultNamingContext:         CH=Configuration,DC=sitka,DC=local;         domainControllerFunctionality: 7 = (VIN2016 );         domainControllerFunctionality: 7 = (VIN2016 );         domainServiceName: CN=NTDS         Settings, CN=HERMES,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=sitka,DC=local;         forestFunctionality: 7 = (VIN2016 );         horestFunctionality: 7 = (VIN2016 );         homainControllerFunctionality: 7 = (VIN
	Prét

# B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)

Sur pfsense on test la connexion de pfsense à la base d'annuaire du controleur de domaine en tapant la commande suivante soit en ssh ou derectement sur pfsense:

#### # openssl s\_client -showcerts -connect 172.20.0.14:636 ¦less

On peut faire la meme chose sur l'interface web de pfsense pour tester la connexion de

pfsense à la base d'annuaire du controleur de domaine, donc on va sur Diagnostics



On tape la commande suivante :

openssl s\_client -showcerts -connect hermes.sitka.local:636
Diagnostics / Command Prompt	0
Advanced Users Only The capabilities offered here can be dangerous. No support is available. Use them at your own risk!	
Execute Shell Command	
openssl s_client -showcerts -connect 172.20.0.14:636 ×	
≪ <sup>4</sup> €xecute ≫ ⊃ Clear	

# Le contrôleur de domaine nous envoie le certificat qu'il utilise pour appliquer le ssl

<pre>depth=0 CW = hermes.sitka.local verify error:mum=20unble to get local issuer certificate verify return:1 depth=0 CW = hermes.sitka.local verify return:1 CONNCTDD(00000003) Content of s:CM = hermes.sitka.local verify return:1 CONNCTDD(00000000000000000000000000000000000</pre>	Shell Output - openssl s_client -showcerts -connect hermes.sitka.local:636					
<pre>LiDL =</pre>	<pre>depth=0 CN = hermes.sitka.local verify error:num=20:unable to get local issuer certificate verify return:1 depth=0 CN = hermes.sitka.local verify error:num=21:unable to verify the first certificate verify return:1 depth=0 CN = hermes.sitka.local verify return:1 CONNECTED(00000003)  Certificate chain 0 s:CN = hermes.sitka.local is:CN = hermes.sitka.local</pre>					
	<pre>i:DC = local, DC = sitka, CN = HERMES-CA BEGIN CERTIFICATE HIG02CCBLugAWIBAgITEgAAAAJXCyfPesdnYgAAAAAAAjANBgkqhkiG9w08AQ0F ADBCKMLWEWYKCZImiZPyLGQBGYFbG9jYWwxFTATBgoJkiaJk/IsZAEZFgVzaXRr YTESMBAGAIUEAXMJSEVSTUUTLUNBMBAXDTIYMDEwOTA4NDIZOFOXDTIZMDEwOTA4 NDIZOFowHTEbMBKGAIUEAXMSaGVybWVZLnNpdGthLmxvY2FSMIIBIJANBgkqhkiG 9w08AQEFAAOCAQ&amp;AMIIBCgKCAQEAvHhsSUeELmjovxUSP48XHqDa9gIsfF7R10M 421sBUP67Nya73IUDqYQ8QsQmzaqkgNDqaQXd08Bdqq8prbZxa6QIGPHURHr8du ANZxtntbMic0rCp3RnQS1PDq4mNJ3XvL+IU820R4nBZ34minC6rQa20N/kNw+UwW 42EDHMgQplVc7NvE7JUSYSCMpioz1x+MQDexH11/EW1K64S0PaPj2CUFzTxTB/r ba0pNhI+A6d4fMWRsetDimC6xEhIKy82sZg/+1K2fJzHIFYeTTIBV2jw6qTXqLCA DTf1adu2EJiXwUmxG2uM6Gbfd0wH6kSQQRrKNxdDQgJDSeuLFQIDAQABo4ICSTCC AuEwLwYJKwYBBAGCNxQCBCIEIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbWBSAGAA 2QByMB0GAIUdJQQMMBQGCCSGAQUFBwMCBggrBgEFBQcDATA0BgNVHQ8BAF8EBAMA 2QByMB0GAIUdJQQMBQGCCSGAQUFBwMCBggrBgEFBQcDATA0BgNVHQ8BAF8EBAMA 2QByMB0GAIUdJQQMBQGCCSGAQUFBwMCBggrBgEFBQcDATA0BgNVHQ4EFgQUg6yhqFRdi131 c8ttwCd0/ZineRNwHwYDVR0jBBgwFoAUBV88Xf2IRChIBMqLFpBDLHNF/QwgCYG AUUHwSBvjCBuzCBuKCBtaCBsoaBr2xKYXA6Ly8VQ049SEVSTUVTLUNBLENOPWh1 cm11cyxDTj1DRFAsQ049UHVibGjJTIWSZV5JTIWUZVydMjjZXN8Q049U2Vydm1j ZXMSQ049Q29uZmIndXJhdGiVbixEQz1zaRrYSxEQz1sbNDbJjZXJ0aWZ2PY2F0 ZVJIdm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGIzdHJpYNV0aW9U UG9pbnQwgbsGCCSGAQUFBwEBBIGUMIGrMIG08ggrBgEFBQcwAoaBm2xkYXA6Ly8v Q049SEVSTUVTLUNBLENOPUFJQSXDTJV3VBDABGKAALBYP2F0 ZVJIdm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGIzdHJpYNV0aW9U UG9pbnQwgbsGCCSGAQUFBwEBBIGUMIGrMIG08BJEEBKHZD9EAy1G10BTFWocF2C Emhlcm11cySzzRrYS5sb2NhbDANBgkqhkiG9w0BAQ0FAAOCAgEAF39BzYd7S5hP uWp5C80+YbDONHXcVee1AB3gp2jhMj3itAHa37TKDXKXMbXjNtguBTIIIUzuwh jwfTIwS0yj1Z+WUH03fujuWINVTJHFmgoUH6U77BwC7KTz+iiwH30HPXVKKiVR 701xSy2ITSSVZIFEWDbuNWe4gA+y20F4+dgN+1+RrQH/Hxc12VE7UXArVF1m/Y 48QEE84fCWJyLrVXsiPG6BsRKtBLFSyPjiOJJPH/KND/KXWbZ3ISM2F2IH0MIEcqc6e QVnbBMmLcwcqLVgFyEssyb15NLqI8RSYDJBAUARWYJKWBAGCNXKBSIEFKHDPHVMKXVR 702ZZMAHFVMKberhHdQt4cE77kFGOGJUmD0JDDJUGKW3ISKS5Irr/tU/KGve6B1G9 BWP0UZEb21+1</pre>					

# C- Création des comptes utilisateurs sur le contrôleur de domaine

Sur le contrôleur de domaine je crée :

- Un groupe **pfsense**
- Un utilisateur kaiser faisant partie du groupe pfsense
- Un utilisateur cesar faisant partie du groupe pfsense
- Un utilisateur **pfsensead** faisant partie du groupe **pfsense** et qui va servir de faire la liaison entre pfsense et le contrôleur de domaine



#### D- Création des authentifications LDAP et LDAPS sur le serveur pfsense

Sur pfsense il existe déjà une base locale permettant l'authentification des utilisateurs. On va utiliser deux autres méthodes qui permettrons l'authentification en utilisant LDAP et LDAPS

#### 1- Création de l'authentifications LDAP

Maintenant on va créer une authentification LDAP sur pfsense à partir l'interface web on va sur System/User Manager/Authentication Servers

Et on clique sur 🕂 📶 pour rajouter une authentification Servers

<mark>pf</mark> sense <sub>.</sub> System → Interfa	aces	s • VPN • Status •	Diagnostics	<b>4</b> 0 G
System / User Manager /	Authentication Servers	5		0
Users Groups Settings	Authentication Servers			
Authentication Servers	•	· · ·		
Server Name	Туре	Host Name	Actions	
Local Database		pfsense		
				🕂 Add

On remplit Les champs comme indiqué ci-dessous, les étapes 1,2 et 3 il faut les exécuter à la fin de notre procédure les faires : on tape cn dans le champ **Authentification containers** puis on clique sur **select a container** 

Authentication containers	cn1	1	Q Select a container	2

Users Groups	Settings Authentication Servers
Server Settings	
Descriptive name	authentification Idap
Туре	
I DAP Server Setting	
Hostname or IP address	barmas sitka local
	NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.
Port value	389
Transport	Standard TCP
Peer Certificate Authority	Global Root CA List
	This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.
Protocol version	3 Select LDAP containers for authentication
Server Timeout	25 Containers Z OU=Asgard_DC=sitka_DC=local
	Timeout for LDAP operations (sec OU=Domain Controllers,DC=sitka,DC=local OU=Microsoft Exchange Security Groups DC=sitka,DC=local
Search scope	Level CN=Users,DC=sitka,DC=local
	Entire Subtree
	Base DN 13
	DC=sitka,DC=local
Authentication containers	OU=Asgard,DC=sitka,DC=local Q Select a container
	Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc=
	component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers
Extended query	Enable extended query
Bind anonymous	Use anonymous binds to resolve distinguished names
Bind credentials	CN=pfsensead,OU=Asgard,DC=sitka,DC=local
User naming attribute	samAccountName
Group naming attribute	Cn
Group member attribute	memberOf
850 0007 0	
RFC 2307 Groups	LDAP Server uses RFC 2307 style group membership     RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active
	Directory style group membership (RFC 2307bis).
Group Object Class	posixGroup
	Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
Shell Authentication Group DN	If I DAD equarie used for shall authentication user must be a member of this group and have a valid posis/Account attributes to be able to login
	Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com
UTF8 Encode	UTF8 encode LDAP parameters before sending them to the server.
	Required to support international characters, but may not be supported by every LDAP server.
Username Alterations	Do not strip away parts of the username after the @ symbol
	ב.y. שפו שחוטיג שבעחורב' שצפו שחורח שחורחפלגובש.
Allow unauthenticated bind	Allow unauthenticated bind Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.
	B Save

# 2- Création de l'authentifications LDAPS

a- Création du formulaire de l'authentification LDAPS

Users	Groups	Settings	Authentication Servers
Server S	Settings		
De	scriptive name	auther	tification Idaps
	Туре	LDAP	♥
LDAP S	erver Settin	igs	
<u>Hostnam</u>	e or IP address	NOTE: V server S	s. sitka.local When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP ISL/TLS Certificate.
	Port value	636	
	Transport	SSL/T	LS Encrypted V

Même procédure que l'authentification LDAP sauf pour les champs encadrés en **vert** on fait le choix de **SSL/TLS** et en utilise le port **636** 

Dans authentification containers on tape cn puis on clique sur

Authentiation containers	cn1		2
Authentication containers		Select a container	2

La boite de dialogue qui nous permet de choisir l'OU qui héberge nos utilisateurs ne s'ouvre pas en plus on a un message d'erreur qui apparait en bas de la page

Could not connect to the LDAP server. Please check the LDAP configuration.

b- Analyse avec Wire Shark du trafic pfsense active directory

Donc l'authentification LDAPS ne fonctionne pas, on va essayer de faire un diagnostic en faisant une capture de trames avec Wire Shark pour identifier le problème.

On installe Wire Shark sur notre contrôleur de domaine, puis on déclenche une capture de trame en même temps on exécute la manipulation précédente

On fait un filtre ssl/tls dans notre capture de trame

Les trames qui représentent l'échange entre pfsense et le contrôleur de domaine sont encadrée en vert :

- Le dialogue commence par **client hello** la source est pfsense destination le hermes
- Hermes répond par server hello et présente son certificat à pfsense
- Pefsense répond par une alerte il ne reconnait pas le certificat

-	*Etherr	net0						—		$\times$
Fi	chier E	diter Vue Al	ler Capture Analyser	Statistiques Telephonie	Wireless 0	Outils Aide				
		🛞 📙 📑 🕻	🗙 😂   🍳 👄 👄 🕾 👔	5 🕹 📃 📃 🔍 Q (	R. 🎹					
	ssl							A		- +
No		Time	Source	Destination	Protocol	Length Info				^
	10	0.869552	172.20.0.250	172.20.0.14	TLSv1.2	106 Application Data	1			
	19	0.918263	172.20.0.250	172.20.0.14	TLSv1.2	361 Client Hello				
	20	0.930438	172.20.0.14	172.20.0.250	TLSv1.2	2322 Server Hello, Ce	ertificate, Server Key Exchange,	Certificate Rec	uest, …	
	23	0.932646	172.20.0.250	172.20.0.14	TLSv1.2	73 Alert (Level: Fa	tal, Description: Unknown CA)			
	27	0.935831	172.20.0.250	172.20.0.14	TLSv1.2	531 Application Data	1			
	28	0.937566	104.26.10.240	172.20.0.14	TLSv1.2	576 Application Data	, Application Data			
										~
> > > >	Ethern Intern Transm Transp	et II, Src: ) et Protocol ) ission Contro port Layer Sec	VMware_cb:74:c4 (00:0c Version 4, Src: 172.20 ol Protocol, Src Port: curity	::29:cb:74:c4), Dst: 1 0.0.250, Dst: 172.20.0 38899, Dst Port: 630	/Mware_23: 0.14 5, Seq: 29	11:5f (00:0c:29:23:11: 6, Ack: 2257, Len: 7	5f)			
0	000 <b>00</b>	Øc 29 23 11	5f 00 0c 29 cb 74 c4	08 00 45 00 ···)#·_	).t	E-				
0	010 00	35 00 00 40	00 40 06 e1 8c ac 14	00 ta ac 14 ;@	@· · · · · · ·					
0	020 <b>00</b>	0e 97 T3 02	7C 02 26 50 06 98 4a	e3 T0 80 18	-& PJ					
0	030 <b>02</b> 040 <b>d0</b>	02 01 41 00	00 01 01 08 08 00 50	10 49 62 13	0					
					-					
	2 1	wireshark_Etherne	t0QQOEF1.pcapng				Paquets: 46 · Affichés: 9 (19.6%) · Perdu	s: 0 (0.0%)	Profile: Det	fault

Donc le souci vient du fait que le certificat présenté par Hermes n'est pas reconnu par pfsense pour contourner ce problème on va importer le certificat de l'autorité de certification racine installée sur hermes sur notre serveur pfsense.

- c- Exportation du certificat de l'autorité de certification hermes
  - On ouvre une console mmc et on rajou<sup>1</sup> Ajouter/Supprimer un composant logiciel enfichable... le composant certificat pour ordinateur
  - On exporter le certificat de l'autorité de certification racine au format '.cer' on l'enregistre avec le nom qu'on choisit

📮 hermes-ca
-------------

09/01/2022 21:33

Console1 - [Racine de la console\Certificats (ordina	ateur local)\Perso	nnel\Certificats]			_		×
Eichier Action Affichage Eavoris Fenêtre	?						- x
		~	-				
Accine de la console	Delivre a		Delivre	e par	Actions		
	hermes.sitka.	local	HERM	ES-CA	Certificats		-
Contificate	HERMES-CA		HERM	ES-CA	Autres actions		•
Autorités de certification racines de con	0.	uvrir					
Certificato			_		HERMES-CA	-	-
Confignce de l'entrenrise	То	utes les tâches	>	Ouvrir			•
Autorités de certification intermédiaires	Co	ouper		Demander	un certificat avec une nouvelle clé		
Éditeurs approuvés	6	nior		Popouvolo	r la cartificat avec una nouvella clé		
Certificats non autorisés		, .		Kenouvere	The certificat avec une nouvelle cle		
Autorités de certification racine tierce ni	Su	pprimer		Gérer les c	lés privées		
Personnes autorisées	Pr	opriétés		Opération	avancées	>	
Émetteurs d'authentification de client							
Racines de version d'évaluation	Ai	de		Exporter			
Racines de test							
> Cocal NonRemovable Certificates							
> 🧮 Bureau à distance							
> Demandes d'inscription de certificat							
> 📫 Racines de confiance de carte à puce							
> 📫 Autorités d'installation d'applications er							
> Périphériques approuvés							
< >	<			>			
Contient les opérations pouvant être effectuées sur l'élé	ment.				,		

On choisit de ne pas exporter la clé privée

<ul> <li>Assistant Exportation du certificat</li> </ul>	
Bienvenue dans l'Assistant Exportation du certificat	Exporter la clé privée Vous pouvez choisir d'exporter la dé privée avec le certificat.
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un magasin de certificats vers votre disque. Un certificat, émis par une autorité de certification, canfirme votre identité et content des informations permettant de protéger des données ou d'étaile des convexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés. Pour continuer, cliquez sur Suivant.	Les dés privées sont protégées par mot de passe. Si vous voulez exporter la dé privée avec le certificat, vous devez taper un mot de passe dans une prochaine page. Voulez-vous exporter la dé privée avec le certificat ? Oui, exporter la dé privée
Suivant Annuler	Suivant Annuler

On choisit le format X.509 encodé DER (\*.cer) et en l'enregistre avec le nom hermed-ca.cer



- J'ouvre mon fichier hermes-ca.cer avec le bloc note pour afficher le certificat de l'autorité de certification après on le copie pour l'insérer dans pfsense



d- Importation du certificat de l'autorité de certification racine

On va sur **cerificate manager + Cas** on clique sur ad pour rajouter une autorité de certification

	System	n <del>-</del> Interface	s + Firewall +	Services +	VPN 👻	Status 🚽	Diagnostics 👻	Help -		C
Systen	n / Certifi	cate Manag	er / CAs							Ø
CAs	Certificates	Certificate Rev	ocation							
Search										e
Search te	erm						Both	~ (	Clear	
		Enter a sear	ch string or *nix reg	ular expression to :	search certific	ate names an	d distinguished na	mes.		
Certifica	ate Authorit	ies								
Name	Internal	Issuer	Certificates	Distinguished	Name				In Use	Actions
CA-Sitka	~	self-signed	1	ST=IDF, OU=S	K, O=sitka, L=	Paris, CN=Ca-	sitka, C=GB 🕕		OpenVPN Server	## <b>#</b> C
				Valid From: Wee Valid Until: Sat,	d, 22 Dec 2021 1 21 Dec 2024 10	0:15:57 +0100 :15:57 +0100				
										+ Ad

On donne un nom à notre autorité de certification et on choisit comme méthode **import an** existing Certificate Autority

Apres il suffit de coller le certificat de l'autorité de certification racine hermes dans le champ certificate data

System / Certific	ate Manager / CAs / Edit
CAs Certificates	Certificate Revocation
Create / Edit CA	
Descriptive name	hermes-ca
Method	Import an existing Certificate Authority
Trust Store	CAdd 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 certifices 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.
Existing Certificate A	Authority
<u>Certificate data</u>	HITFX2CCA0egAWIEAGIQNIJXTd1fepNC4G9VJL19MZANBgkqhkiG9W         HITFX2CCA0egAWIEAGIQNIJXTd1fepNC4G9VJL19MZANBgkqhkiG9W         BAQ0FADBC         HRUWEWYKCZIEMIZPyLGQBGRYFDG9JYWwXFTATBgoJkiaJk/ISZAEZFg         YZXXRYYTES         Paste a certificate in X.509 PEM format here.
Certificate Private Key (optional)	Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).
Next Certificate Serial	Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.
	Save

e- Test de la connexion ssl entre pfsense et le contrôleur de domaine

On constate qu'il n'y'a plus de messages d'erreurs que le message handshake (poignée de main) est établie et crypté on peut maintenant revenir pour terminer de remplir notre formulaire authentification LDAPS

_									
🛋 *E	thernet0						-		$\times$
Fichie	r Editer Vue	Aller Capture Analyse	r Statistiques Telephoni	e Wireless Outils	Aide				
<b>A</b>	1 🖉 💿 📘 🚮	🔀 🖾 🍳 👄 👄 🖻	i 🕧 😃 🥃 📃 🔍 e	Q III					
l est							~		<b>→</b> ] +
Ne	Time	Sev.mee	Destination	Destagel Length	Tafa				
110.	24 3 180984	172 20 0 14	172 20 0 250	TLSv1 2 381	Application Data				
	27 3.181661	172.20.0.250	172.20.0.14	TLSv1.2 89	Application Date				
	35 3,188387	172.20.0.250	172.20.0.14	TLSv1.2 361	Client Hello	-			
	36 3.190890	172.20.0.14	172.20.0.250	TLSv1.2 2322	Server Hello, Ce	ertificate, Server Key Exchange,	Certificate Requ	uest,	
1	40 3.194817	172.20.0.250	172.20.0.14	TLSv1.2 236	Certificate, Cli	ient Key Exchange, Change Cipher	Spec, Encrypted	Hands	
	41 3.196216	172.20.0.14	172.20.0.250	TLSv1.2 117	Change Cipher Sp	pec, Encrypted Handshake Message			
	43 3.196628	172.20.0.250	172.20.0.14	TLSv1.2 158	Application Data	a			~
> En	ame 41: 117 byt	es on wire (936 bits:	), 117 bytes captured	(936 bits) on in	terface \Device\N	IPF_{CD7E2F95-314F-4B15-B68B-1106	SA9E5CCE}, id 0		
> Et	hernet II, Src:	VMware_23:11:5f (00	:0c:29:23:11:5f), Dst	: VMware_cb:74:c4	(00:0c:29:cb:74:	c4)			
> In	ternet Protocol	Version 4, Src: 172	.20.0.14, Dst: 172.20	.0.250					
> Tr	ansmission Cont	rol Protocol, Src Po	rt: 636, Dst Port: 42	252, Seq: 2257, A	ck: 466, Len: 51				
2 16	ansport Layer S	ecurity							
0000	00 0c 29 cb 7	4 c4 00 0c 29 23 11	5f 08 00 45 00 😶	•t••••)#•_••E•					
0010	00 67 e0 d8 4	0 00 80 06 00 00 ac	14 00 0e ac 14 ·g·	@					
0020	00 Ta 02 /c a	5 0C 95 6C 8T 69 93	7d 1f f7 po 06	1					
0040	c7 46 14 03 0	3 00 01 01 16 03 03	00 28 00 00 00 ·F·						
0050	00 00 00 00 0	0 55 42 75 a7 1e b6	de af 60 26 fa ····	••UBu ••••••					
0060	c5 13 d1 75 d	2 73 83 0d a7 a7 d4	8b ba 64 d4 6b · · ·	u·s·· ····d·k					
0070	5f 38 7f d5 1	d	_8 ·						
0	wireshark_Ether	net0W30DF1.pcapng				Paquets: 63 · Affichés: 20 (31.7%) · Perdu	is: 0 (0.0%)	Profile: De	fault
-									

# 3- Utilisation des authentifications LDAP et LDAPS sur le serveur pfsense

Je vérifie l'authentification Active directory de mon compte **kaiser** à partir de l'interface web de pfsense, on va sur diagnostic + authentification



- a- Vérification de l'authentification LDAP et LDAPS
- L'authentification Active directory en utilisant LDAP a réussit

Diagnostics / Aut	Diagnostics / Authentication			
User kaiser authenticated successfully. This user is a member of groups:				
Authentication Test				
Authentication Server	authentification Idap  Select the authentication server to test against.			
Username	kaiser			
Password				
	<b>≁</b> Test			

#### - L'authentification Active directory en utilisant LDAPS a réussit

Diagnostics / Aut	Diagnostics / Authentication				
User kaiser authenticated successfully. This user is a member of groups:					
Authentication Test					
Authentication Server	authentification Idaps				
Username	kaiser				
Password					
	<b>≁</b> Test				

b- Configuration des groupes et des utilisateurs sur pfsense

On crée un groupe de même nom que celui crée sur active directory le groupe **pfsense** on clique sur **add** pour rajouter un groupe

System / User	System / User Manager / Groups				
Users Groups	Settings Authentication Servers				
Groups	Description	Member Count	Actions		
all	All Users	1			
admins	System Administrators	1	ø		
			+ Add		

On remplit les champs comme indiqué ci-dessous puis on sauvegarde

Users Groups Set	tings Authentication Servers	
Group Properties	5	
Group name	pfsense	
Scope	Remote V Warning: Changing this setting may affect the local groups t take effect.	file, in which case a reboot may be required for the changes to
Description	Group description, for administrative information only	
Group membership	admin *	
	Not members	Members
	>> Move to "Members"	K Move to "Not members
	Hold down CTRL (PC)/COMMAND (Mac) key to select multi	ple items.
	E Save	

Dès que le groupe est créé je l'édite pour lui donner les droits admin

pfsense compte active directory 0		
-----------------------------------	--	--

Dans assigned Privilèges je clique sur add

Assigned Privileges				
	Name	Description	Action	
				+ Add
	🖺 Save			

Je sélectionne WebCfg – All pages comme droit

roup Privileges		
Group	pfsense	
Assigned privileges	System - HA node sync User - Config: Deny Config Write User - Notices: View and Clear User - Struices: Captive Portal login User - System: Copy files (ocp) User - System: Shell account access User - System: Shell account access User - System: Shell account access User - VPN: IPSec xauth Dialin User - VPN: IPSec Xauth Dialin User - VPN: IPSec Xauth Dialin User - VPN: Constant WebCfg - AJAX: Get Service Providers WebCfg - AJAX: Get Stats WebCfg - Crash reporter WebCfg - Dashboard (all) WebCfg - Dashboard (all)	
	WebCfg - All pages WebCfg - Crash reporter WebCfg - Dashboard (all) WebCfg - Dashboard widgets (direct access). WebCfg - Diagnostics: ARP Table	

On remarque le groupe pfsense aura tous les droits

🖺 Save 🝸 Filter 🗶 Clear			
Allow access to all pages (This privileg	je effectively gives administrator-lev	vel access to users in the group)	

On enregistre notre configuration

Assigned Privileges			
	Name	Description	Action
	WebCfg - All pages	Allow access to all pages (admin privilege)	<b>m</b>
	Security notice: Users in this group	p effectively have administrator-level access	
			- <b>+</b> Ad
	🖹 Save		

On fait un test de connexion avec la base LDAP

System	+ Interfaces +	Firewall 🗸 🗧	Services <del>-</del>	VPN 🗸	Status 🗸	Diagnostics 🚽	Help 🗸	¢
System / User M	anager / Settir	ngs						Ø
Users Groups	Settings Authentic	cation Servers						
Settings Session timeout	30 Time in minutes to e risk!	xpire idle managem	nent sessions. Ti	he default is	4 hours (240 r	minutes). Enter 0 to r	never expire sessions. 1	NOTE: This is a security
Authentication Server	authentification Ida	ар			~			
Shell Authentication	Use Authentication If RADIUS or LDAP s To allow logins with To allow logins with	on Server for Shell A erver is selected it i RADIUS credentials LDAP credentials, S	Authentication is used for conso s, equivalent loca Shell Authenticat	ole and SSH al users with tion Group D	authentication the expected p N must be spe	n. Otherwise, the Loc privileges must be cr ccified on the LDAP s	al Database is used. eated first. erver configuration pag	je.
Auth Refresh Time	Time in seconds to o to authentication ser	cache authenticatio vers.	n results. The de	efault is 30 s	econds, maxin	num 3600 (one hour	). Shorter times result i	n more frequent queries
	🖬 Save 🎤 Save	e & Test						

#### La connexion a réussi

LDAP settings

reactesuits	Attempting connection to	hermes.sitka.local	
	Attempting bind to	hermes.sitka.local	
	Attempting to fetch Organizational Units from	hermes.sitka.local	
	Organization units found		
	OU=Asgard,DC=sitka,DC=local		
	OU=Domain Controllers,DC=sitka,DC=local		
	OU=Microsoft Exchange Security Groups.DC=sitka.DC=local		
	CN=Users.DC=sitka.DC=local		

# On fait un test de connexion avec la base LDAPS

	em – Interfac	ces + Firewall +	Services -	VPN -	Status 🚽	Diagnostics 👻	Help 👻	G
System / User	Manager /	Settings						Ø
Users Groups	Settings	Authentication Servers						
Settings								
Session timeo	ut 30 Time in min risk!	utes to expire idle man	agement sessions	. The default	is 4 hours (240	minutes). Enter 0 to	never expire sess	sions. NOTE: This is a security
Authentication Serve	er authentific	cation Idaps			~			
Shell Authenticatio	If RADIUS o To allow log To allow log	nentication Server for S r LDAP server is select jins with RADIUS crede jins with LDAP credenti	hell Authentication ed it is used for co ntials, equivalent i als, Shell Authenti	n Insole and SS Iocal users with Iocation Group	H authentication th the expected DN must be sp	on. Otherwise, the Lo I privileges must be o ecified on the LDAP	cal Database is us created first. server configurati	sed.
Auth Refresh Tim	Time in sec to authentic	onds to cache authenti ation servers.	cation results. The	e default is 30	seconds, max	imum 3600 (one hou	r). Shorter times r	result in more frequent queries
	Save	🗲 Save & Test						

#### La connexion a réussi

### LDAP settings

Test results	Attempting connection to	hermes.sitka.local	OK
	Attempting bind to	hermes.sitka.local	ок
	Attempting to fetch Organizational Units from	hermes.sitka.local	ок
	Organization units found OU=Asgard,DC=sitka,DC=local OU=Domain Controllers,DC=sitka,DC=local OU=Microsoft Exchange Security Groups,DC=sitka,DC=local CN=Users,DC=sitka,DC=local		

# On teste notre configuration en se connectant avec notre compte kaiser

🗖 🗾 pfSense - Login 🗙	+			—		$\times$
$\leftarrow$ $\rightarrow$ $C$ $rightarrow$ https://heimda	II.sitka.local	🖉 as ★	£°≡	Ē	۲	
<u>pf</u> sense			Logir	n to pf	Sense	÷
	SIGN IN					
	kaiser					
	·					
	SIGN IN	E 000 ( 0000 )				
prsense is developed a	ind maintained by Netgate. 🗢 ES	F 2004 - 2022 V	iew license			

On verifie bien qu'on est connecter avec un compte issue de la base LDAP

🗖 🗾 heimdall.sit	tka.local - Status: Dash 🗙 🕂					—		3
$\leftarrow \rightarrow $ C	🕆 https://heimdall.sitka.local	Ð	ക	20	£°≡	Ð		
ofsense						[		
Status / D	ashboard						+ 0	1
Status, D							• •	
System Infor	mation		_	_	_	J.	- 8	ī.
System Infor Name	heimdall.sitka.local		_			، عر	• •	1
System Infor Name User	heimdall.sitka.local kaiser@172.20.0.14 (LDAP/authentifi	cation Idaps)		-	-	، عو	08	1
System Infor Name User System	heimdall.sitka.local kaiser@172.20.0.14 (LDAP/authentifi VMware Virtual Machine	cation Idaps)				¥	0 8	1
System Infor Name User System	Mation heimdall.sitka.local kaiser@172.20.0.14 (LDAP/authentifi VMware Virtual Machine Netgate Device ID: <b>7c7777e1ee8ed9</b> 1	cation Idaps)				بر	• •	
System Infor Name User System BIOS	Mation heimdall.sitka.local kaiser@172.20.0.14 (LDAP/authentifi VMware Virtual Machine Netgate Device ID: 7677771ee8ed91 Vendor: Phoenix Technologies LTD	oation Idaps) 11e66				1	00	

~



- 1- Introduction
- 2- Activation du portail captive
- 3- Configuration du DHCP
- 4- Création des règles sur le firewall
- 5- Test de notre portail captive

### 1- Introduction

Le portail captif est un moyen qui force les clients d'un réseau de passer par une page Web d'authentification pour pouvoir se connecter à Internet.

Il est utilisé dans des réseaux assurant un accès public comme certain espace de la SNCF, les hôtels, les établissement scolaires ...

# 2- Activation du portail captive

On se connecte sur l'interface de web de pfsense, après on va sur Services + Captive Portal

	System 🗸 Interfaces 🗸 Firewall	✓ Services ✓ VPN ·	+ Status +	Dia	gnostics - Help -	<b>4</b> 2 🗘
Status /	Dashboard	Auto Config Backup Captive Portal DHCP Relay				+ 0
System Inf	ormation	DHCP Server	Interfaces			ی 🖨 ۴
Name	heimdall.sitka.local	DHCPv6 Relay	🕂 WAN	1	1000baseT <full-duplex></full-duplex>	192.168.1.250
User	admin@172.20.0.14 (Local Database)	DHCPv6 Server & RA	📥 LAN	1	1000baseT <full-duplex></full-duplex>	172.20.0.250
System	VMware Virtual Machine	DNS Forwarder	- OPT1	1	1000baseT <full-duplex></full-duplex>	192.168.2.250

# On clique sur **Add**

	System 👻	Interfaces 🗸	Firewall 🗕	Services +	VPN 🗸	Status 🗸	Diagnostics 🗸	Help 🗸		<b>¢</b> 2	•	•
Services	/ Captive F	Portal								601	•	•
Captive Po Zone	rtal Zones	ces	Numt	per of users			Description	A	ctions			
											+ /	٩dd

On renseigner le Nom du Portail Captif et sa description :

Sitka\_portal pour le nom de la zone

Portail captive sitka pour la description de la zone

COMMUNITY EDITION	m 👻 Interfaces 👻	Firewall - Services -	VPN <del>-</del> St	atus <del>-</del> Diagnostics	<b>≜</b> 2 G•
Services / Cap	tive Portal / Add	Zone			₩ 🗏 🕄
Add Captive Porta	Zone				
Zone nam	e sitka_portail Zone name. Can only	contain letters, digits, and un	derscores (_) and m	ay not start with a digit.	
Zone descriptio	A description may be	entered here for administrativ	ve reference (not pa	rsed).	
	Save & Continue	2			

# On active le portail et on enregistre

COMMUNITY EDITION	🔸 Interfaces 🗸 Firewall 🗸 Services 🗣 VPN 🗣 Status 🖌 Diagnostics 🗸 Help 🗸 🦺 🕑 🕩
Services / Captin	ve Portal / sitka_portail / Configuration 😤 🖼 🗐 😧
Configuration MAC:	s Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager
Captive Portal Conf	iguration
Enable	Enable Captive Portal
Description	portail captif de sitka A description may be entered here for administrative reference (not parsed).
	B Save
Don't forget to enable the Also, the DNS Forwarder o	DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Ir Resolver must be enabled for DNS lookups by unauthenticated clients to work.
Don't forget to enable the Also, the DNS Forwarder o	DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. r Resolver must be enabled for DNS lookups by unauthenticated clients to work.

- On active Enable Captive Portal
- On sélectionne l'interface **Opt1**
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)
- Idle timeout (Minutes) on choisit **15**:(Les clients seront déconnectés après cette période d'inactivité)

COMMUNITY EDITION	🔹 Interfaces 🗸 Firewall 🗸 Services 🖌 VPN 🖌 Status 🖌 Diagnostics 🖌 Help 🗸 🦺 🕑 🕩
Services / Captiv	e Portal / sitka_portail / Configuration C® 幸 Ш 🗉 😢
Configuration MACs	Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager
Captive Portal Config	juration
Enable	Enable Captive Portal
Description	portail captif de sitka A description may be entered here for administrative reference (not parsed).
Interfaces	WAN LAN OPT1 Select the interface(s) to enable for captive portal.
Maximum concurrent connections	(1) Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)	Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

- Définir **After authentication Redirection URL (URL HTTP** de redirection Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont tenté d'accéder après s'être authentifiés)
- Activer **Disable Concurrent user logins** (seule la connexion la plus récente par nom d'utilisateur sera active)
- Activer **Disable MAC filtering** (lorsque l'adresse MAC du client ne peut pas être déterminée)

Logout popup window	Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	https://www.bing.com/ Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	https://www.bing.com/ Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	Last login Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

On peut choisir un logo et une image d'arrière-plan ainsi qu'un charte de connexion

Captive Portal Login	l Page
Display custom logo image	enable to use a custom uploaded logo
Logo Image	Choisir un fichier Aucun fichier choisi Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, It can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.
Display custom background image	enable to use a custom uploaded background image
Background Image	Choisir un fichier Aucun fichier choisi Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.
Terms and Conditions	Charte d'utilisation du wifi Charte d'utilisation Charte d'utilisation du réseau Wifi DE SITKA La présente charte a pour objet de définir les règles d'utilisation de la connexion Wifi du Gite auberge les Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

- On sélectionne Use an Authentication backend
- On sélectionne Authentification LDAPS comme méthode d'authentication

Authentication	
Authentication Method	Use an Authentication backend  Select an Authentication Method to use for this zone. One method must be selected "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server	authentification Idaps         authentification Idaps         Local Database         You can add a remote authentication server in the User Manager.         Vouchers could also be used, please go to the Vouchers Page to enable them.
Secondary authentication Server	authentification Idap authentification Idaps Local Database You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.
Reauthenticate Users	Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

# On active ssl pour notre portail active

HTTPS Options	
Login	Denable HTTPS login When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.
HTTPS server name	heimdall.sitka.local This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.
SSL/TLS Certificate	sitka_certificates Certificates known to be incompatible with use for HTTPS are not included in this list. If no certificates are defined, one may be defined here: System > Cert. Manager
HTTPS Forwards	Disable HTTPS Forwards If this option is set, attempts to connect to HTTPS (SSL/TLS on port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.
	B Save
Don't forget to enable the Also, the DNS Forwarder o	× DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

Les clients ont besoin d'une résolution DNS donc on va autoriser cette résolution en autorisant l'adresse IP du DNS 172.20.0.14

	System -	Interfaces -	Firewall +	Services -	VPN - St	atus <del>-</del> Diag	nostics 🚽	Help 🗸	<b>¢</b> 2 🔂
Services /	Captive	Portal / sitka	_portail /	Allowed IF	Addresses				℃● 幸 🗉 🛙
Configuration	MACs	Allowed IP Addres	sses Allov	ved Hostnames	Vouchers	High Availabi	lity File I	Manager	
IP Addresses				Description				Actions	
									+ Add
0									

COMMUNITY EDITION	✓ Interfaces ✓ Firewall ✓	Services - VPN -	Status 🗕 Diag	gnostics 🗸 Help 🗸	<b>4</b> 2 🗘
Services / Captiv	ve Portal / sitka_portail	/ Allowed IP Addre	sses / Edit		C® ≕ Ш 🗏 🛛
Edit Captive Portal I	P Rule				
IP Address	172.20.0.14			/ 24	~
Description	serveur dns Enter a description here for refere	nce only. (Not parsed)			
Direction	Both Use "From" to always allow acces non-authenticated ones) behind ti	is to an address through the cap he portal to this IP.	▶ ptive portal (without aut	thentication). Use "To" to allow acce	ss from all clients (even
Bandwidth up	Enter an upload limit to be enforc	ed on this address in Kbit/s			
Bandwidth down	Enter a download limit to be enfo	rced on this address in Kbit/s			
	B Save				

	System 🗸	Interfaces +	Firewall 🗕	Services 🗸	VPN 🗸	Status 🚽	Diagnostics		lp <del>-</del>	<b>4</b> 2 G
Services /	Captive	e Portal / sitka	a_portail /	Allowed IF	P Address	es				C® ≢ Ш 🗏 🛛
Configuration	MACs	Allowed IP Addre	sses Allo	wed Hostnames	Vouchers	High A	wailability	File Mana	ger	
IP Addresses				Descript	ion			1	ctions	
≓ 172.20.0.14 /24				serveur	dns				e 🖉	
→ = All connections	to the add	ress are allowed, $\leftarrow$ =	All connections	from the addres	s are allowed, <del>,</del>	2 = All conne	ctions <u>to or fro</u>	<u>m</u> are allow	ed	
0										+ Add

# 3- Configuration du DHCP

Maintenant On va activer le DHCP sur l'interface opt1

	System 👻 Interfaces 👻	Firewall +	Services - V	/PN -	Status 🗸	Dia	gnostics <del>-</del>	Help 🗸		<b>¢</b> 2	6
Status /	Dashboard		Auto Config Backu Captive Portal DHCP Relav	up						+	0
System Inf	ormation		DHCP Server	1	Interfaces					۶0	8
Name	heimdall.sitka.local		DHCPv6 Relay	-	WAN	↑	1000baseT <	<full-duplex></full-duplex>	192.168.	.1.250	
User	admin@172.20.0.14 (Local Da	atabase)	DHCPv6 Server &	RA 🖥	LAN	↑	1000baseT «	<full-duplex></full-duplex>	172.20.0	.250	
System	VMware Virtual Machine		DNS Forwarder	-	OPT1	1	1000baseT <	full-duplex>	192.168.	.2.250	

# On déclare notre étendue

	<ul> <li>Interfaces -</li> </ul>	Firewall 🗕	Services 🗸	VPN -	Status 🗸	Diagnostics 🗸	Help 🗸		<b>\$</b> 2	•
Services / DHCP	Server / OPT1							≢	<u>iii</u> 📰	0
WAN LAN OPT	1									
General Options Enable	Enable DHCP ser	ver on OPT1 inte	erface							
воотр	Ignore BOOTP qu	ieries								
Deny unknown clients	Allow all clients When set to Allow al interface, any DHCP interface, only MAC	II <b>clients</b> , any DH client with a MA addresses listed	ICP client will get AC address listed d below (i.e. for th	t an IP addres I on <b>any</b> scop his interface)	s within this see(s)/interface( will get an IP a	cope/range on this s) will get an IP add ddress within this s	interface. If set to ress. If set to Alle cope/range.	o Allow known clien ow known clients fr	its from a om only t	any this
Ignore denied clients	Denied clients wi This option is not co	II be ignored rati Impatible with fa	her than rejected ailover and canno	ot be enabled	when a Failove	r Peer IP address is	s configured.			
Ignore client identifiers	If a client include This option may be a server behavior viola	es a unique ident useful when a cl ates the official [	ifier in its DHCP i ient can dual boo DHCP specificatio	request, that I ot using differ on.	UID will not be ent client ident	recorded in its leas ifiers but the same	e. hardware (MAC)	address. Note that	the result	ting
Subnet	192.168.2.0									
Subnet mask	255.255.255.0									
Available range	192.168.2.1 - 192.16	8.2.254								
Range	192.168.2.20 From				1 To	92.168.2.50				

# On rentre l'adresse de notre DNS

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	172.20.0.14
	8.8.8.8
	DNS Server 3
	DNS Server 4
	Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

On rentre l'adresse de la passerelle et du nom de domaine

Other Options	
Gateway	192.168.2.250 The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.
Domain name	sitka.local The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

# 4- Création des règles sur le firewall

On Cree deux règles autorisant le DNS et le https

	System	<ul> <li>Interfaces -</li> </ul>	Firewall 🗸	Se	ervices <del>-</del>	VPN 🗸	Status 👻	Diagnostics			<b>\$</b> 2	•
Firewa	II / Rules /	OPT1									≢ ⊡ ≣	9
The chang Monitor th	es have been ap e filter reload pro	plied successfully. T ogress.	he firewall rules	are now	reloading in	the backgroun	d.					×
Floating	WAN	LAN OPT1										
Rules (D	rag to Chan	ge Order)										
0 :	States	Protocol	Source	Port	Destination	Port	Gate	way Queue	Schedule	Description	Actions	
0 🗸	4 /30 KiB	IPv4 TCP/UDP	OPT1 net	*	*	53 (DNS)	*	none			₺∥□0	Ē
• 🗸	9 /13.89 MiB	IPv4 TCP/UDP	OPT1 net	*	*	443 (HTTF	PS) *	none			₺∥□♡	<u>۵</u>
								t	Add 🕽 Ad	d 间 Delete	🕞 Save 🕂 S	eparator

# 5- Test de notre portail captive

On fait notre test de connexion

Captive Portal Login Page	× +	—	×
$\leftarrow$ $ ightarrow$ C $finite https://h$	eimdall.sitka.local:8003/index.php? 🗔 🎛 🖉 🏠	€ @	
	pfsense		
	kaiser		
	Login		
	Made with ♥ by Netgate		

Sur pfsense on peut vérifier les connexions

	System +	Interfaces 🛨	Firewall +	Services +	VPN 🗸	Status 🚽	Diagnostics 🚽	Help <del>+</del>		<b>¢</b> 2	•
Services /	Captive P	ortal								Lut 📰	0
Captive Porta	I Zones										
Zone	Inte	rfaces	Numbe	er of users		Des	scription		Actions		
sitka_portail	0P	т1				ро	rtail captif de sitka		1		
										-	Add

	System 🗸	Interfaces 🗸	Firewall 🗸	Services 🗸	VPN 🗸	Status 🗸	Diagnostics 👻	Help 👻		2	•
Status / C	Captive Por	tal / sitka_	portail						C® ≢ (	.11 🖽	0
Users Logge	ed In (1)										
IP address		Usernan	ne		Session sta	rt		Actions			
192.168.2.20		kaiser			01/16/2023	2 22:06:04			â		
								Show Las	t Activity 🔟 Disconr	nect All U	lsers

- On chercher **You are connected** et remplacer par **Vous êtes connecté** 

- On chercher Disconnecting... et You have been disconnected et on remplacer par Déconnexion... et Vous êtes déconnecté
- On cherche **Invalid credentials specified** et on remplace **par Les informations saisies sont invalides,** il y a 2 lignes à modifier
- Après on enregistre les modifications

C:\heimdall\	/usr/local/captiveportal/
Nom	Nom
<b>★</b>	<ul> <li></li> <li>captiveportal-backgroundjpeg</li> <li>captiveportal-default-logo.png</li> <li>captiveportal-logopng</li> <li>indexphp</li> </ul>
< >>	< >>
0 B de 0 B dans 0 de 0	10,2 KB de 5,48 MB dans 1 de 4
	G SFTP-3 🗐 0:03:29

Maintenant on va sur /etc/inc puis et on ouvre captiveportal.inc

- On chercher Captive Portal login Page et on remplacer par : Portail Captif de sitka
- On chercher Login et Made with ... by ... Netgate et on remplacer par Connexion et Connectez-vous avec votre compte LDAPS
- On chercher User et Password et on Remplace par Utilisateur et Mot de Passe
- On rechercher Logout et Click the button below to disconnect on remplace par Déconnexion et Cliquez sur le bouton ci-dessous pour vous déconnecter
- On enregistre les modifications

C:\heimdall\	/etc/inc/
Nom	Nom
<u>t</u>	🔁
captiveportal.inc	📙 priv
index.php	acb.inc
	auth.inc
	auth_check.inc
	auth_func.inc
	authgui.inc
	Captiveportal.inc
	⊂ certs.inc ✓
< >>	< >
102 KB de 112 KB dans 1 de 2	0 B de 2,24 MB dans 0 de 62
	G SFTP-3 🗐 0:18:57 🤮





- 1- Introduction
- 2- Création d'un compte dans Snort
- 3- Installation de Snort
- 4- Configuration de Snort
- 5- Test d'intrusion

# 1- Introduction

Dans cette partie consacrée à Pfsense on va voir comment installer le package Snort sur PfSense, et ainsi un IDS voir même un IPS !

On va d'abord voire un peu ce qu'est un IDS et un IPS et la différence entre eux.

Les IDS (Intrusion Detection Systems) n'a pas comme rôle de bloquer les attaques, IDS utilisent une base de données d'attaques afin de :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque.
- Détecter les violations de la politique de sécurité,
- Détecter les malwares et les scanners de port.

Les IPS (Intrusion Prevention Systems): Les IPS bloquent et rejettent les paquets réseau en utilisant un profil de sécurité en cas de menaces .

# 2- Création d'un compte dans Snort

Il faut créer un compte sur le site officiel de Snort

### (https://www.snort.org/users/sign\_up)

, car Snort va nous fournir une clé (**Snort Oinkmaster Code)** qui nous servira à la mise à jour des règle Snort.

Une fois le formulaire d'inscription est rempli il faut se rendre sur la messagerie qu'on a renseigné dans notre formulaire d'inscription pour confirmer notre inscription à partir du mail envoyé par Snort.



Une fois L'inscription confirmé on se rend sur le site de Snort <u>https://www.snort.org/</u>et on se connecte avec nos identifiants



Une fois connecté on va dans le menu Oincode pour récupérer le code de téléchargement et de mise à jour des règles Snort



#### 3- Installation de Snort

On accède au menu System et sélectionnez l'option de Package Manager.

	System - Int	erfaces 🕶	Firewall -	Services -	VPN -	Status 👻	Diagnostics	- Help -	G
	Advanced								
Status / C	Cert. Manager								+ 0
	General Setup								
System Info	High Avail. Sync			6 6 عر	3	nterfaces			ی 🔿 کر
Name	Logout (admin)	cal			-	WAN	1	1000baseT <full-duplex></full-duplex>	192.168.1.250
User	Package Manager	0.14 (Loca	I Database Fall	back)	4	SITKA_LAN	1	1000baseT <full-duplex></full-duplex>	172.20.0.250
System	Routing	Machine				SITKA_CLIEN	rts 🛧	1000baseT <full-duplex></full-duplex>	192.168.2.250

Sur l'écran de Package Manager, accédez à l'onglet Available Paquages.

Sur le moteur de recherche, on cherche Snort et on installe le paquet Snort.

Syst	tem / F	Package Manager / Available Packages	0
Instal	led Packaç	Available Packages	
Sear	ch		Θ
Searc	ch term	snort Both  Q Search  Clear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Pack	ages		
Name	Version	Description	
snort	4.1.5	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly- based inspection.	🕂 Install
		Package Dependencies: Ø snort-2.9.19	

Accédez au menu Pfsense Services et sélectionnez l'option Snort.

COMMUNITY EDITION System - Interfaces -	Firewall - Services -	VPN -	Status -	Diagnostics -	Help -
System / Package Manager / Package	Auto Conf Captive Po DHCP Reli	g Backup rtal			
pfSense-pkg-snort installation successfully complet	DHCP Ser DHCPv6 R	erelay			
Installed Packages Available Packages	Package Insta DNS Forw DNS Reso DNS reso	erver & RA arder ver			
Package Installation	ICMP Prov				
Please note that, by default, snort will tri default snaplen of 15158 bytes. Additional Stream5 target-based reassembly. It is reco your card supports it.	uncate pack ly, LRO may commended to PPPoE Se Shellcmd	ver			
This can be done by appending '-lro' to your	if config_ SNMP				
Message from pfSense-pkg-snort-4.1.5:	Snort UPnP & N	T-PMP			
Please visit Services - Snort - Interfaces	tab first t Wake-on-L	AN er	n select your	desired rules p	ackages a

# 4- Configuration de Snort

On va dans l'onglet Global Settings, dans cette étape on va activer le téléchargement de règles gratuites, en cochant la case Enable Snort VRT.

Et ensuite nous pouvons cocher les cases :

- Enable Snort GPLv2,
- Enable ET Open,
- Enable OpenAppID, On ne coche pas car il faut une licence

Services / Snort	/ Global Settir	ngs								0	
Snort Interfaces Glo	bal Settings Upd	ates Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync		
Snort Subscriber Ru	les										
Enable Snort VRT	Collick to enable o	download of Snort f	ree Registered	User or paid Sub	scriber rules						
	Sign Up for a free R Sign Up for paid Sn	legistered User Rule ort Subscriber Rule	s Account Set (by Talos)								
Snort Oinkmaster Code	bbedc54fdevgehu Obtain a snort.org (	bedc54fdevgehuhg543a7767898460jhnsdrevxtr tain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URLI)									
Snort GPLv2 Commu	inity Rules										
Enable Snort GPLv2	Click to enable of	download of Snort G	PLv2 Commun	nity rules							
	The Snort Commun ruleset is updated o	nity Ruleset is a GPL daily and is a subset	v2 Talos certifi of the subscri	ed ruleset that is ber ruleset.	distributed free	of charge with	iout any Snort Si	ubscriber License	restriction	is. This	
Emerging Threats (E	T) Rules										
Enable ET Open	Click to enable o	download of Emergi	ng Threats Ope	en rules							
	ETOpen is an open	source set of Snort	rules whose co	overage is more l	imited than ETP	ro.					
Enable ET Pro	Click to enable of	download of Emergi	ng Threats Pro	rules							
	Sign Up for an ETP ETPro for Snort off	ro Account ers daily updates an	d extensive co	verage of current	malware threat	s.					

Dans la zone Rules Update Settings on effectue la configuration suivante :

Update Interval :1 DAY

Update Start Time : 00 :01

Hide Deprecated Rules Categories : On coche

Remove Blocked Hosts Interval : 1 HOUR

Keep Snort Settings After Deinstall : Si on désinstalle Snort on laisse les paramètres de configuration On coche

#### Startup/Shutdown Logging : pour avoir les log On coche



Services / S	nort / Update	es									0
Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	

Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

COMMUNITY EDITION System - Interfaces - Firewall -	Services - VPN - Status -	Diagnostics - Help -			
Services / Sport / Updates	Rules Update Task ×				
Services / Short / Opdates			•		
Snort Interfaces Global Settings Updates Alerts	Updating rule sets may take a while please wait for the process to complete.	IP Lists SID Mgmt Log Mgmt Sync			
Installed Rule Set MD5 Signature	This dialog will auto-close when the update is finished.				
Rule Set Name/Publisher		MD5 Signature Date			
Snort Subscriber Ruleset	1.2	Not Enabled			
Snort GPLv2 Community Rules		Not Downloaded			
Emerging Threats Open Rules	Close	Not Downloaded			
Snort OpenAppID Detectors	Not Enabled	Not Enabled			
Snort AppID Open Text Rules	Not Enabled	Not Enabled			
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled	Not Enabled		
Update Your Rule Set					
Last Update Unknown Result: Unknown	NID				
Update Rules Vpdate Rules		Force Update			
Click UPDATE RULES to check for an the MDS hashes and force the down	d automatically apply any new posted updates oad and application of the latest versions of th	for selected rules packages. Clicking FORCE UPDATE will a e enabled rules packages.	cero out		
Manage Rule Set Log					
View Log		lear Log			
The log file is limited to 1024K in size	and is automatically cleared when that limit is	exceeded.			
Logfile Size Log file is empty					

### A la fin de la mise à jours on voit qu'on a le message Result :Success

Oct Hoces, One	opulate									•		
Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync		
Installed Rule Set	MD5 Signatu	re										
Rule Set Name/Publish	her		MD5 Signat	ture Hash			MD5	Signature Date				
Snort Subscriber Rules	set		73370d55	59b00f2a1001	decf9167c5b5		Sun	day, 30-Jan-22 1	7:30:26 CET			
Snort GPLv2 Community Rules			5a1e3be23	3ee59e10d78c	164a156ddac7a		Sun	day, 30-Jan-22 1	7:30:26 CET			
Emerging Threats Ope	en Rules		fecb4fd2ct	6c161041efb2	695a3c57b27		Sun	iday, 30-Jan-22 1	7:30:27 CET			
Snort OpenAppID Detectors			Not Enable	t Enabled Not Enabled								
Snort AppID Open Tex	Snort AppID Open Text Rules			ed be			Not	Not Enabled				
Feodo Tracker Botnet	C2 IP Rules		Not Enabled				Not	Not Enabled				
Update Your Rule	Set											
Last Upda	te Jan-30 202	2 17:30	Result:	Success								
Update Rule	es 🗸 Update	Rules				📥 Ford	e Update					
	Click UPDA the MD5 ha	TE RULES to che ashes and force t	ck for and a the downloa	automatically and applicat	apply any new po tion of the latest	sted updates for versions of the e	r selected rules mabled rules p	s packages. Click ackages.	king FORCE UPD	ATE will zero out		
Manage Rule Set	Log											
	View Lo	eg 🛛				Clea	r Log					
	The log file	is limited to 102	4K in size a	nd is automat	ically cleared who	en that limit is ex	ceeded.					
Logfile Siz	ze 12 KiB											

En affichant les logs on a un message qui précise que Snort n'est configuré sur aucune interface

Manage Rule Set Log		
	View Log	
	The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.	
Logfile Size	7 KIB	
Rules Update	Log	×
	Installation of Snort Subscriber rules completed. Extracting and installing Snort GPLv2 Community Rules Installation of Snort GPLv2 Community Rules completed. Extracting and installing Emerging Threats Open rules Installation of Emerging Threats Open rules completed. Conving new config and map files Warning: No Interfaces configured for Snort were found The works sponte has instance. The for Snort were found	

Close

Maintenant on va sur **Snort interfaces** pour choisir l'interface ou les interfaces sur laquelle Snort va analyser et écouter le trafic réseau **on clique sur add pour rajouter notre interface :**  **Snap Length** est la longueur maximale des paquets capturés par Snort. Il permet de limiter la quantité de données qui sont stockées en mémoire pour chaque paquet, et donc de réduire la charge sur le système.

Services / Snort / Interfaces											•
nort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
terrace Setti	ngs Overview										

Dans la zone General Setting on activer l'interface wan qui est l'interface à surveiller

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings	
General Settings	
Enable	@Enable interface
Interface	WAN (em0)  Choose the Interface where this Snort Instance will inspect traffic.
Description	WAN Enter a meaningful description here for your reference.
Snap Length	1518 Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Localiser la zone Alerts Settings et effectuer la configuration suivante : Send Alerts to System Log on active cette option pour avoir les alertes de snort

Alert Settings	
Send Alerts to System Log	Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	LOG_AUTH Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	LOG_ALERT  Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures	Drhecking this option will automatically capture packets that generate a Snort alert into a topdump compatible file
Packet Capture File Size	128 Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em060059 is rotated and a new file opened.
Enable Unified2 Logging	Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Dans la zone Block Settings on active le mode IPS en appliquant la configuration ci-dessous Ceci permettra de bloquer les hôtes qui génère l'alerte

Block Settings	
Block Offenders	Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode
	Select blocking mode operation. Legacy Mode inspects copies of packets while inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.
	Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Sont can determine if the traffic matches a rule and should be blocked. Inline mode instead instrects part of inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States	Ochecking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.

Après on laisse tout par défaut et clique sur le bouton Save.

Maintenant on accède à l'onglet Wan Catégories et on effectue la configuration suivante :

**Resolve Flowbits** (les "flowbits" sont une fonctionnalité de Snort qui permet de maintenir l'état de traitement des connexions réseau et d'ajouter des conditions supplémentaires à des règles en fonction de l'état de traitement de ces connexions) :

On active cette option Snort activera automatiquement les règles requises pour les flowbits et il examinera les règles activées dans les catégories de règles qu'on a choisies pour les **Resolve Flowbits**. Toutes les règles qui définissent ces flowbits dépendants seront automatiquement activées et ajoutées à la liste des fichiers dans le répertoire des règles de l'interface.

- IPS Policy Selection : On active cette option et on sélectionne comme politique IPS Balanced.
 L'activation de cette option désactive le choix manuel des règles Snort Snort Text Rules, Snort
 SO Rules par-contre les règles ET Open Rules reste manuelle



Select the rulesets	(Categories) Snort wi	ll load at star	tup						
Category is auto-ena	bled by SID Mgmt conf files								
A - Category is auto-disa	abled by SID Mgmt conf files							Select All Un	select All Save
Services / Snort	/ Interface Settin	gs / WAN -	Categories						0
Snort Interfaces Glo	obal Settings Updates	Alerts	Blocked Pas	ss Lists S	uppress	IP Lists	SID Mgmt	Log Mgmt	Sync
WAN Settings WAN	N Categories WAN Rul	es WAN Var	riables WAN	Preprocs	WAN IP Rep	WAN	Logs		
Automatic Flowbit F	Resolution								
Resolve Flowbits	f checked, Snort will Snort will examine the e automatically enabled a	auto-enable rules nabled rules in yo nd added to the li	required for check ur chosen rule cate st of files in the inte	ked flowbits. De egories for chee erface rules dir	efault is Checl cked flowbits. ectory.	ked. . Any rules th	at set these dep	pendent flowbit:	s will be
Snort Subscriber IP	S Policy Selection								
Use IPS Policy	Selecting this option dis selected if enabled on the selected of the selected if enabled on the selected if enabled if enabl	use rules from or ables manual sele ne Global Settings	ne of three pre-definection of Snort Sub tab. These will be	ned IPS policies oscriber catego added to the p	s in the Snort ries in the list re-defined Sno	Subscriber n below, althou ort IPS policy	ules. Default is I ugh Emerging T rules from the	Not Checked. hreats categoric Snort VRT.	es may still be
IPS Policy Selection	Balanced Snort IPS policies are: C Connectivity blocks mos covers most threats of t rules such as a Flash ot with caution on product	onnectivity, Balan st major threats w he day. It includes ject in an Excel fil on systems!	ced, Security or Ma ith few or no false ; all rules in Connec e. Max-Detect is a p	<ul> <li>Ax-Detect.</li> <li>positives. Balar</li> <li>ctivity. Security</li> <li>policy created for the security</li> </ul>	nced is a goo is a stringent for testing net	d starter poli policy. It cor twork traffic 1	cy. It is speedy, ntains everything through your de	has good base g in the first two vice. This policy	coverage level, and plus policy-type should be used
Select the rulesets	(Categories) Snort wi bled by SID Mgmt conf files bled by SID Mgmt conf files	ll load at stari	tup					Select All Un	select All

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer (save)

Enable	Ruleset: Snort GF	PLv	2 Com	munity Rules			
	Snort GPLv2 Cor						
Enable	Ruleset: ET Open Rules		Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
	emerging-activex.rules			snort_app-detect.rules		snort_browser-chrome.so.rules	
	emerging-attack_response.rules			snort_blacklist.rules		snort_browser-ie.so.rules	
	emerging-botcc.portgrouped.rules			snort_browser-chrome.rules		snort_browser-other.so.rules	
0	emerging-botcc.rules			snort_browser-firefox.rules		snort_browser-webkit.so.rules	

### Maintenant on va démarrer notre Interface Snort

Snort	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Inter	face Setting	js Overview									
	Interface	Snort	Status	Patt	ern Match	Blo	cking Mode		Description	Action	าร
0	WAN (em0)	8(	0	AC-	BNFA	LE	GACY MODE		WAN	Ø 🕻	) 🗇
0										•	Add 🔟 Delete
Snort	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Inter	face Setting	js Overview									
	Interface	Snort	Status	Patt	ern Match	Blo	cking Mode		Description	Actio	ns
0	WAN (em0)	$\odot$	Co	AC-	BNFA	LE	GACY MODE		WAN	Ø 🕻	
8											Add 🛅 Delete

### Test d'intrusion

Sur Notre machine physique on installe un utilitaire nmap qui servira de scanner les ports de pfsense



Sur Pfsense dans l'onglet Alerte on relève des notifications d'attaques d'une machine dont l'adresse IP est 192.168.1.128 c'est l'adresse de notre machine physique, l'attaque détectée n'est que la requête nmap

Snort Inter	rfaces	Global	Settings	Updates	Alerts	Blocked	Pas	s Lists S	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Alert Log	g View S	etting	s											
Interf	ace to Insp	pect	WAN (em Choose inte	0) 🗸	Auto-	refresh viev	v	250 Alert lines to	o display.	Save				
Aler	rt Log Acti	ons	🛃 Downloa	d 🔟 Clear										
Alert Log	g View F	ilter												÷
15 Entrie	es in Act	tive Lo	g											
Date	Action	Pri	Proto	Class	Source	e IP	SPort	Destination	IP DPort	GID:SID	Description	1		
2022-01-30 21:35:58	Δ	2	UDP	Attempted Information L	192. eak <b>Q</b> [	168.1.128 <b>± ×</b>	48917	192.168.1.2 <b>Q 🛨</b>	250 3823	7 1:201848 <b>• ×</b>	9 ET SCAN N	MAP OS Detection	n Probe	
2022-01-30 21:35:58	Δ	2	UDP	Attempted Information L	192. eak <b>Q</b> [	168.1.128 <b>± ×</b>	48917	192.168.1.2 <b>Q                                    </b>	250 3823	7 1:201848	9 ET SCAN M	MAP OS Detection	n Probe	
2022-01-30 21:35:57	Δ	2	UDP	Attempted Information L	192. eak <b>Q</b>	168.1.128 + ×	48917	192.168.1.2 <b>Q</b> 🛨	250 3823	7 1:201848	9 ET SCAN N	MAP OS Detection	Probe	

Dans l'onglet Bloked on voit que la machine dont l'adresse IP est 192.168.1.128 est bloqué car elle est identifié comme hoste hostile

Snort	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Block	ked Hosts a	nd Log View Se	ttings								
	Blocked Ho	osts 🛃 Downloa	d booto will be source	d			Clea	r Ind boots will l	a removed		
Ref	resh and Log Vi	iew Save Save auto-re	fresh and view se	ettings	Default	resh t is ON	All block	500 Numb Defaul	er of blocked ent t is 500	ries to view.	
Last #	500 Hosts E IP	Blocked by Snor Alert Descri	t (only applica ptions and Event 1	able to L Times	egacy Blo	cking Mode i	nterfaces)				Remove
1	141.98.10.82 <b>Q</b>	ET COMPRO	OMISED Known Co	ompromise	ed or Hostile H	lost Traffic TCP	group 9 2022-0	01-30 21:22:52	1		×
2	192.168.1.128         ET SCAN Suspicious inbound to mySQL port 3306 – 2022-01-30 21:35:35           Q         ET SCAN Potential VNG Scan 5900 5920         2022 01 30 21:35:37           ET SCAN Suspicious Inbound to MSSQL port 1437 – 2022-01-30 21:35:40         ET SCAN Potential VNG Scan 5800-5820 – 2022-01-30 21:35:40           ET SCAN Suspicious Inbound to PostgreSQL port 1521 – 2022-01-30 21:35:46         ET SCAN Suspicious Inbound to PostgreSQL port 5432 – 2022-01-30 21:35:54           ET SCAN Number OS DEtection Probe – 2022-01-30 21:36:00         ET SCAN Suspicious Inbound to PostgreSQL port 5432 – 0222-01-30 21:35:54										×
			2 host IP address	ses are cur	rently being b	locked by Snort	on Legacy Mode	Blocking inte	rfaces.		





- 1- Introduction
- 2- Création d'un compte dans Snort
- 3- Installation de Snort
- 4- Configuration de Snort
- 5- Création des règles sur le firewall
- 6- Test de notre portail captive

# 1- Introduction

Dans cette partie consacrée à Pfsense on va voir comment installer le package Snort sur PfSense, et ainsi un IDS voir même un IPS !

On va d'abord voire un peu ce qu'est un IDS et un IPS et la différence entre eux.

Les IDS (Intrusion Detection Systems) n'a pas comme rôle de bloquer les attaques, IDS utilisent une base de données d'attaques afin de :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque.
- Détecter les violations de la politique de sécurité,
- Détecter les malwares et les scanners de port.

Les IPS (Intrusion Prevention Systems): Les IPS bloquent et rejettent les paquets réseau en utilisant un profil de sécurité en cas de menaces .

# 2- Création d'un compte dans Snort

Il faut créer un compte sur le site officiel de Snort

### (https://www.snort.org/users/sign\_up)

, car Snort va nous fournir une clé (**Snort Oinkmaster Code)** qui nous servira à la mise à jour des règle Snort.

Une fois le formulaire d'inscription est rempli il faut se rendre sur la messagerie qu'on a renseigné dans notre formulaire d'inscription pour confirmer notre inscription à partir du mail envoyé par Snort.



Une fois L'inscription confirmé on se rend sur le site de Snort <u>https://www.snort.org/</u>et on se connecte avec nos identifiants



Une fois connecté on va dans le menu Oincode pour récupérer le code de téléchargement et de mise à jour des règles Snort



#### 3- Installation de Snort

On accède au menu System et sélectionnez l'option de Package Manager.

	System - Int	erfaces 🕶	Firewall -	Services -	VPN -	Status 👻	Diagnostics	- Help -	G
	Advanced								
Status / C	Cert. Manager								+ 0
	General Setup								
System Info	High Avail. Sync			6 6 عر	3	nterfaces			ی 🔿 کر
Name	Logout (admin)	cal			-	WAN	1	1000baseT <full-duplex></full-duplex>	192.168.1.250
User	Package Manager	0.14 (Loca	I Database Fall	back)	4	SITKA_LAN	1	1000baseT <full-duplex></full-duplex>	172.20.0.250
System	Routing	Machine				SITKA_CLIEN	rts 🛧	1000baseT <full-duplex></full-duplex>	192.168.2.250

Sur l'écran de Package Manager, accédez à l'onglet Available Paquages.

Sur le moteur de recherche, on cherche Snort et on installe le paquet Snort.

Syst	tem / F	Package Manager / Available Packages	0
Instal	led Packaç	Available Packages	
Sear	ch		Θ
Searc	ch term	snort Both  Q Search  Clear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Pack	ages		
Name	Version	Description	
snort	4.1.5	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly- based inspection.	🕂 Install
		Package Dependencies: Ø snort-2.9.19	

Accédez au menu Pfsense Services et sélectionnez l'option Snort.

COMMUNITY EDITION System - Interfaces -	Firewall - Services -	VPN -	Status -	Diagnostics -	Help -
System / Package Manager / Package	Auto Conf Captive Po DHCP Reli	g Backup rtal			
pfSense-pkg-snort installation successfully complet	DHCP Ser DHCPv6 R	elay			
Installed Packages Available Packages	Package Insta DNS Forw DNS Reso DNS reso	erver & RA arder ver			
Package Installation	ICMP Prov				
Please note that, by default, snort will tri default snaplen of 15158 bytes. Additional Stream5 target-based reassembly. It is reco your card supports it.	uncate pack ly, LRO may commended to PPPoE Se Shellcmd	ver			
This can be done by appending '-lro' to your	if config_ SNMP				
Message from pfSense-pkg-snort-4.1.5:	Snort UPnP & N	T-PMP			
Please visit Services - Snort - Interfaces	tab first t Wake-on-L	AN er	n select your	desired rules p	ackages a

# 4- Configuration de Snort

On va dans l'onglet Global Settings, dans cette étape on va activer le téléchargement de règles gratuites, en cochant la case Enable Snort VRT.

Et ensuite nous pouvons cocher les cases :

- Enable Snort GPLv2,
- Enable ET Open,
- Enable OpenAppID, On ne coche pas car il faut une licence

Services / Snort	/ Global Sett	ings								0
Snort Interfaces Glo	bal Settings Up	odates Ale	ts Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Snort Subscriber Ru	les									
Enable Snort VRT	Click to enable	e download of S	nort free Registered	d User or paid Sub	scriber rules					
	Sign Up for a free Sign Up for paid S	Registered Use Snort Subscriber	Rules Account Rule Set (by Talos)							
Snort Oinkmaster Code	bbedc54fdevger Obtain a snort.org	uhg543a77678 g Oinkmaster co	98460jhnsdrevxtr de and paste it here	e. (Paste the code	only and not the	URL!)				
Snort GPLv2 Commu	nity Rules									
Enable Snort GPLv2	Click to enable	e download of S	nort GPLv2 Commu	inity rules						
	The Snort Comm ruleset is updated	unity Ruleset is a I daily and is a s	GPLv2 Talos certi ubset of the subsci	fied ruleset that is riber ruleset.	distributed free	of charge with	iout any Snort Si	ubscriber License	restriction	ıs. This
Emerging Threats (E	T) Rules									
Enable ET Open	Click to enable	e download of E	merging Threats Op	en rules						
	ETOpen is an ope	n source set of	Snort rules whose o	coverage is more l	imited than ETP	ro.				
Enable ET Pro	Click to enable	e download of E	merging Threats Pr	o rules						
	Sign Up for an ET ETPro for Snort o	Pro Account ffers daily updat	es and extensive c	overage of current	t malware threat	s.				

Dans la zone Rules Update Settings on effectue la configuration suivante :

Update Interval :1 DAY

Update Start Time : 00 :01

Hide Deprecated Rules Categories : On coche

Remove Blocked Hosts Interval : 1 HOUR

Keep Snort Settings After Deinstall : Si on désinstalle Snort on laisse les paramètres de configuration On coche

#### Startup/Shutdown Logging : pour avoir les log On coche



Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

COMMUNITY EDITION System - Interfaces - Firewall -	Services - VPN - Status - Diagnosti	
Services / Snort / Updates	Rules Update Task ×	Ø
Snort Interfaces Global Settings Updates Alerta	Updating rule sets may take a while please wait for the IP L process to complete.	liste SID Mgmt Log Mgmt Sync
Installed Rule Set MD5 Signature	This dialog will auto-close when the update is finished.	
Rule Set Name/Publisher		MD5 Signature Date
Snort Subscriber Ruleset	4.2	Not Enabled
Snort GPLv2 Community Rules		Not Downloaded
Emerging Threats Open Rules	Close	Not Downloaded
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
Undate Your Rule Set		
Last Update Unknown Result: Unknow	<u>vn</u>	
Update Rules Vpdate Rules	📩 Force Update	
Click UPDATE RULES to check for an the MDS hashes and force the downl	d automatically apply any new posted updates for select oad and application of the latest versions of the enabled	ed rules packages. Clicking FORCE UPDATE will zero out rules packages.
Manage Rule Set Log		
View Log	Clear Log	
The log file is limited to 1024K in size	and is automatically cleared when that limit is exceeded	d.
Logfile Size Log file is empty		

A la fin de la mise à jours on voit qu'on a le message **Result :Success** 

Services / Snort	/ Update	s									0	
Snort Interfaces Glo	bal Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync		
Installed Rule Set M Rule Set Name/Publisher	D5 Signatur	e	MD5 Signat	ure Hash			MD	5 Signature Date				
Snort Subscriber Ruleset			73370d555	59b00f2a1001	decf9167c5b5		Sur	nday, 30-Jan-22 1	7:30:26 CET			
Snort GPLv2 Community F	Rules		5a1e3be23	ee59e10d78d	d64a156ddac7a		Sur	nday, 30-Jan-22 1	17:30:26 CET			
Emerging Threats Open R	ules		fecb4fd2c6	5c161041efb2	2695a3c57b27		Sur	Sunday, 30-Jan-22 17:30:27 CET				
Snort OpenAppID Detecto	rs		Not Enabled					Not Enabled				
Snort AppID Open Text Ru	iles		Not Enable	d			Not	t Enabled				
Feodo Tracker Botnet C2	IP Rules		Not Enabled					Not Enabled				
Update Your Rule Se	t											
Last Update	Jan-30 2023	2 17:30	Result:	Success								
Update Rules	🛹 Update F	Rules				📥 Ford	e Update					
	Click UPDA the MD5 has	TE RULES to ch shes and force	eck for and a the download	utomatically d and applica	apply any new po tion of the latest	sted updates for versions of the e	r selected rule mabled rules p	s packages. Clic packages.	king FORCE UPD	ATE will zer	ro out	
Manage Rule Set Log												
	View Log	2				Clea	r Log					
	The log file	is limited to 10	24K in size ar	nd is automat	ically cleared who	en that limit is ex	ceeded.					
Logfile Size	12 KiB											

En affichant les log on un message qui précise que Snort n'est configuré sur aucune interface

Manage Rule Set Log		
	🕒 View Log	
	The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.	
Logfile Size	7 KiB	
Rules Update	e Log	×
	Installation of Snort Subscriber rules completed. Extracting and installing Snort GPLv2 Community Rules Installation of SnotalGPLv2 Community Rules completed. Installation of SnotalGPLv2 Community Rules completed. Installation of Energing Threats Open rules completed. Conving new config and map files Warning: No Interfaces configured for Snort were found The Rules Opeate may interfaces configured for Snort were found	

Close

Maintenant on va sur **Snort interfaces** pour choisir l'interface ou les interfaces sur laquelle Snort va analyser et écouter le trafic réseau **on clique sur add pour rajouter notre interface :** 

Services / Sr	nort / Interfac	es									0
Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Interface Settin	igs Overview										
Interface	Snort Status		Pattern N	Match	Block	ing Mode		Description	Act	ions	
										6	+ Add

Dans la zone **General Setting** on activer l'interface wan qui est l'interface à surveiller

Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
WAN Settings										
General Settings										
Ena	ble 🕜 Enable ir	nterface								
Interfa	WAN (em) Choose the	)) interface where	e this Snort i	instance will in	spect traffic.	~				
Descript	ion WAN Enter a mea	ningful descrip	tion here for	your reference	е.					
Snap Len	gth 1518 Enter the de	sired interface	snaplen valu	ue in bytes. De	fault is 1518 and	is suitable for n	nost applicatio	ns.		

Localiser la zone Alerts Settings et effectuer la configuration suivante : Send Alerts to System Log on active cette option pour avoir les alertes de snort



Dans la zone Block Settings on active le mode IPS en appliquant la configuration ci-dessous Ceci permettra de bloquer les hôtes qui génère l'alerte

Block Offenders	Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode 🗸
	Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network s between the NIC and the OS. Default is Legacy Mode.
	Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will or before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they a handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (foroped) and not passed to the network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netma Supported drivers: bruxt, cc, cxgbe, cxl, em, em, ena, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch t Legacy Mode Instead.
Kill States	Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH
	Select which IP extracted from the packet you wish to block. Default is POTH

Après on laisse tout par défaut et clique sur le bouton Enregistrer.

Maintenant on accéde à l'onglet **Wan Catégories** et effectuez la configuration suivante : Résoudre les débits - Oui - Utiliser la politique IPS - Oui Sélection des politiques IPS – Connectivité

Dans notre exemple, nous avons activé la fonctionnalité IPS et sélectionné la stratégie nommée **Connectivité**.

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer et démarrez le service Snort sur


## Introduction

- 1- Gestion des certificats
  - Création de l'autorité de certification
  - Création du certificat Server
- 2- Configurer le serveur OpenVPN
- 3- Créer les règles de firewall pour OpenVPN
  - a. A. Autoriser le flux OpenVPN
  - b. B. Autoriser les flux vers les ressources
- 4- Exportation de la configuration OpenVPN clientes
- 5- Test de la connexion VPN
  - a. Test depuis un client Windows
  - b. Test depuis un client Android

### Introduction

**OpenVPN** est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Son développement a commencé le 13 mai 2001 grâce à James Yonan.

OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. Il utilise de manière intensive la **bibliothèque** d'authentification OpenSSL ainsi que le multitude protocole SSLv3/TLSv1. Disponible avec une d'environnements tel que Solaris, OpenBSD, FreeBSD, NetBSD, Linux (Debian, Redhat, Ubuntu, etc.), Mac OS X, Windows 2000, XP, Vista, 7, 8 et 10, il offre de nombreuses fonctions de sécurité et de contrôle.

OpenVPN n'est pas compatible avec IPsec ou d'autres logiciels VPN. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie.

### 1- Gestion des certificats

- Création de l'autorité de certification
- Création du certificat Server

### 2- Configurer le serveur OpenVPN

Pour configurer notre VPN on va cliquer sur le menu "VPN" puis "OpenVPN"

	System - Interfaces -	Firewall 👻	Services 🗸	VPN <del>-</del>	Status 🗸	Diagnos	stics <del>-</del>	Help <del>-</del>		•
Status /	Dashboard			IPsec L2TP						+ 0
System Inf	ormation		) 0 عر	OpenVPN	vetgate Sér	vices An	d Suppo	ort		⊖ ⊗
Name	heimdall.sitka.local				Contr	act type	Communi	ty Support		
User	admin@172.20.0.14 (Local	Database)			Cont	astipe	Community Support Only			
System	VMware Virtual Machine			_						

Dans l'onglet **Servers** on clique sur **Add afin de** créer une nouvelle configuration.

	System 🗸	Interfaces 🗸	Firewall <del>-</del>	Services 🗸	VPN -	Status 🗸	Diagnostics 🗸	Help 🗸	€
VPN/ Op	oenVPN/S	Servers							···· 🗉 😧
Servers	Clients Clie	ent Specific Overrid	es Wizards						
OpenVPN S	Servers								
Interface	Protoco	ol / Port	Tunnel N	letwork		Mode / Crypto		Description	Actions
									+ Add

Dans "Server Mode" on choisit : Remote Access (User Auth).

Le VPN utilise UDP, avec **le port 1194** par défaut on choisira **le port 1919 pour des raisons de securité.** 

L'interface, utilisée est la WAN c'est l'interface qui sera utilisé pour notre connexion à distance.

General Information	
Disabled	Disable this server Set this option to disable this server without removing it from the list.
Server mode	Remote Access (User Auth )
Backend for authentication	authentification Idaps Local Database
Protocol	UDP on IPv4 only
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.)
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.
Description	OPENVPN SITKA A description may be entered here for administrative reference (not parsed).

## Dans le champ **Peer Certificate Authority** on sélectionne notre autorité de certification Dans le champ **Server certificate** on sélectionne notre certificat

oryprographic octim	190	
TLS Configuration	A TLS Key A TLS key enhances security of an OpenVPN connection by requirin This layer of HMAC authentication allows control channel packets unauthorized connections. The TLS Key does not have any effect of	iring both parties to have a common key before a peer can perform a TLS handshake. Its without the proper key to be dropped, protecting the peers from attack or t on tunnel data.
	Utomatically generate a TLS Key.	
Peer Certificate Authority	CA-Sitka	~
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here:	e: System > Cert. Manager
OCSP Check	Check client certificates with OCSP	
Server certificate	https_sitka (Server: Yes, CA: CA-Sitka, In Use)	<b>~</b>
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 s	✓ ✓ server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Negotiation	Enable Data Encryption Negotiation This option allows Open/VPN clients and servers to negotiate a con selected in the Data Encryption Algorithms list below. Disabling th	compatible set of acceptable cryptographic data encryption algorithms from those this feature is deprecated.
Data Encryption Algorithms	AES-192-CPB (192 bit Key, 128 bit block) AES-192-CPB (192 bit Key, 128 bit block) AES-192-CPB (192 bit Key, 128 bit block) AES-192-CPB (192 bit Key, 128 bit block) AES-192-OFB (192 bit Key, 128 bit block) AES-256-CPB (256 bit Key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305 AES-256-CBC
	Available Data Encryption Algorithms Click to add or remove an algorithm from the list The order of the selected Data Encryption Algorithms is respected	Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list ed by OpenVPN.
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) The Fallback Data Encryption Algorithm used for data channel pac negotiation. This algorithm is automatically included in the Data Er	ackets when communicating with clients that do not support data encryption algorithm     Encryption Algorithms list.
Auth digest algorithm	SHA256 (256-bit) The algorithm used to authenticate data channel packets, and con When an AEAD Encryption Algorithm mode is used, such as AES-G The server and all clients must have the same setting. While SHA1	ontrol channel packets if a TLS Key is present. FGCM, this digest is used for the control channel only, not the data channel. A1 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 b generated from the same CA as the server.	> selow this depth. Useful for denying certificates made with intermediate CAs

Maintenant on va configurer le tunnel VPN.

- IPv4 Tunnel Network : En se connectant en VPN le client obtiendra une adresse IP dans ce réseau

- IPv4 Local network : les LAN qu'on veut rendre accessibles via le tunnel VPN. Dans notre cas, on va rendre accessible les réseaux 192.168.1.0/24, 192.168.2.0/24, 172.20.0.0/24

- Concurrent connections : le nombre de connexions VPN simultanés autorisés.

Tunnel Settings	
IPv4 Tunnel Network	192.168.1.0/24         This is the IPv4 virtual network 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.
IPv6 Tunnel Network	This is the IPv6 virtual network 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.
IPv4 Local network(s)	172.20.0.0/24,192.168.1.0/24,192.168.2.0/24         IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. 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. 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	3月     €       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.
Push Compression	Push the selected Compression setting to connecting clients.
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	<ul> <li>Allow multiple concurrent connections from the same user</li> <li>When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.</li> <li>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.</li> </ul>

Pour les paramètres des clients, on coche **Dynamic IP** : Ceci aux client de garder leur connexion si l'adresse IP publique d'un client change, en se connectant via une connexion 4G. Au niveau de la **Topology**, : pour des raisons de sécurité, il vaut mieux utiliser la topologie **net30 - isolated /30 network per client** pour que chaque client soit isolé dans un sous-réseau de la plage réseau VPN afin que les clients ne puissent pas communiquer entre eux

Inconvénient de cette méthode la connexion VPN, va consommer 4 adresses IP : une adresse IP pour le PC, une adresse IP pour le pare-feu et les adresses de réseau et broadcast du sousréseau en /30.



On coche l'option **Provide a DNS server list to clients.** 

On indique le nom de domaine

On coche l'option "**Provive a default domain name to clients**" pour indiquer le nom de domaine local.

On indique les adresses IP de nos serveurs DNS

Aussi en force la mise à jour du cache dns

Advanced Client Set	tings
DNS Default Domain	Provide a default domain name to clients
DNS Default Domain	sitka.local
DNS Server enable	Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.1.1
DNS Server 2	172 20.0.14
DNS Server 3	
DNS Server 4	
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	Drun "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.

Dans la zone "**Custom options**", on tape : **auth-nocache**. Cette option refuse la mise en cache des identifiants

Advanced Configurat	tion							
Custom options	auth-nocache Enter any additional options to a EXAMPLE: push 'route 10.0.0.0	dd to the OpenVPN server configuration here, 255.255.255.0*	separated by semicolon.					
Username as Common Name	Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purpose such as determining Client Specific Overrides.							
UDP Fast I/O	<ul> <li>Use fast I/O operations with I Optimizes the packet write event bandwidth limiting.</li> </ul>	JDP writes to tun/tap. Experimental. Loop, improving CPU efficiency by 5% to 10%	. Not compatible with all platforms, and not compatible with OpenVPN					
Exit Notify	Reconnect to this server / Retry Send an explicit exit notification for a timeout. In SSL/TLS Server Network, this value controls how	y once to connected clients/peers when restarting o modes, clients may be directed to reconnect many times this instance will attempt to sen	r shutting down, so they may immediately disconnect rather than waiting or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel d the exit notification.					
Send/Receive Buffer	Default Configure a Send and Receive Bu uplink speeds. Finding the best b values.	v Iffer size for OpenVPN. The default buffer siz putfer size can take some experimentation. To	e can be too small in many cases, depending on hardware and network test the best value for a site, start at S12KiB and test higher and lower					
Gateway creation	Both     If you assign a virtual interface to	O IPv4 only othis OpenVPN server, this setting controls w	IPv6 only hich gateway types will be created. The default setting is 'both'.					
Verbosity level	3 (recommended) Each level shows all info from the output. None: Only fatal errors Default through 4: Normal usage 5: Output R and W characters to 1 TUN/TAP packets. 6-11: Debug info range	e previous levels. Level 3 is recommended for range the console for each packet read and write. U	a good summary of what's happening without being swamped by ppercase is used for TCP/UDP packets and lowercase is used for					
	Save							

Maintenant on enregistre pour valider la configuration.de notre VPN

VPN /	OpenVPN / S	Servers					iiii 🗐 🔞
Servers	Clients Clier	nt Specific Overrides	Wizards	Client Export	Shared Key Export		
OpenVP	N Servers						
Interface	Protocol / Port	Tunnel Network	Mode / Cryp	to		Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.1.0/24	Mode: Remo Data Cipher Digest: SHA D-H Params	ote Access ( User A s: AES-256-GCM, A 256 : 2048 bits	uuth ) ES-128-GCM, CHACHA20-POLY1305, AES-256-CBC	OPENVPN SITKA	a 🗋 🖉
							+ Add

# 3- Création les règles de firewall pour OpenVPNa. Autoriser OpenVPN sur l'interface Wan

Il ne faut pas oublier de créer une règle autorisant le VPN sur notre interface wan

~	0 /80 B	IPv4 TCP/UDP	*	*	WAN address	1919	*	none	authoriser VPN	ݨ∥□◯面
								1	Add 🕽 Add 🛅 Delete	Save + Separator

## b. Autoriser l'accès aux ressources

Maintenant on va ajouter une règle, sur l'interface OpenVPN.

La règle va autoriser l'accès en RDP à l'hôte 172.20.0.14 au travers du tunnel VPN. On doit créer une ou plusieurs règles en fonction des ressources auxquelles nous voulons y accéder via le VPN.

Firewall / Rules / OpenVPN =												
Floating	WAN	N SITKA_L	AN SI	TKA_CLI	ENTS OpenVF	PN						
Rules (	Drag to	Change Orde	er)									
Rules (	Drag to States	Change Orde Protocol	er) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
Rules (	Drag to States 0 /0 B	Change Orde Protocol IPv4 TCP	er) Source *	Port *	Destination 172.20.0.14	Port 3389 (MS RDP)	Gateway	Queue	Schedule	Description	Actions	

## 4- Exportation de la configuration OpenVPN

Pour exporter la configuration de notre openvpn pour les clients on va installer un paquet dont le nom est **openvpn-client-export** sur pfsense..

On va dans le menu suivant : System > Package Manager > Available Packages.

Recherchez "openvpn" et installez le	paquet : <b>openvpn-client-export</b> .
--------------------------------------	---

System	/ Pack	kage Manager / Available Packages	0
Installed Pa	ckages	Available Packages	
Search			-
Search term	n	openvpn Both V Q Search D Clear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Packages			
Name	Version	Description	
openvpn- client-export	1.6_2	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	+ Install
chieft export		Package Dependencies: Ø openvpn-client-export-2.5.2 Ø openvpn-2.5.2_2 Ø zip-3.0_1 Ø p7zip-16.02_3	

Une fois l'installation est faite, on retourne dans le menu **OpenVPN** puis dans l'onglet **Client Export**.

Dans host name on rentre notre adresse IP publique pour nous connecter

OpenVPN / Clien	t Export Utility 0
Server Client C	tient Specific Overrides Wizards Client Export Shared Key Export
OpenVPN Server	
Remote Access Server	OPENVPN SITKA UDP4:1919
Client Connection Be	havior
Host Name Resolution	Other 🗸
Host Name	93.124.120.13 Enter the hostname or IP address the client will use to connect to this server.
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	<ul> <li>Do not include OpenVPN 2.5 settings in the client configuration.</li> <li>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.</li> </ul>
Silent Installer	Create Windows installer for unattended deploy. Create a silent Windows Installer for unattended deploy. Since this installer is not signed, you may need special software to deploy it correctly.
Use Random Local Port	Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

On tous les autres options par défaut, on rajoute seulement l'option **auth-nocache** ; après en enregistre

-
auth-nocache
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;
Save as default

- 5- Test de la connexion VPN depuis un poste client
- a- Téléchargement du client openvpn

Selon le client on télécharge le programme adéquate

OpenVPN Clients		
User	Certificate Name	Export
Authentication Only (No Cert)	none	Inline Configurations: Most Clients ▲ Android) ▲ OpenVPN Connect (/0S/Android) Bundled Configurations: ▲ Archive ▲ Config File Only Current Windows Installer (2.5.2-Ix01): ▲ of-bit ▲ 3:2-bit Legacy Windows Installers (2.4.11-Ix01): ▲ 10/2016/2019 ▲ 7/8/8.1/2012/2 Viscosity Bundle ▲ Viscosity Inline Config
Only OpenVPN-compatible user certificates ar	re shown	

On teste l'accès distant depuis un poste client Windows, Android ou Apple . Pour apple on choisit Viscosity gratuit un mois après c'est payant ou Tunneblick qui est gratuit

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. 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
FEAT VPN For Android - For older versions of 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.

#### b- Test de connexion sur un client Windows

Sur un PC client, on installe le client **OpenVPN** <sup>35</sup> openvpn-heimdall-UDP4-1919-install-2.5.2-I601-amd64

Setup OpenVPN 2.5.2-I601		×	🕼 Setup OpenVPN 2.5.2-I601	$\times$
Choose setup type.		<b>P</b>	Installing OpenVPN	n
	Install Now		_	
	Customize		Deleting TUN/TAP adapters	



Une fois l'agent VPN est installé un icone dans la barre des taches apparait qui va ne permettre de se connecter à notre serveur VPN ainsi que les interfaces réseaux propre au VPN comme c'est illustré ci-dessous

🕜 OpenVPN Configuration Setup – 🗆 🗙	
Setup was completed successfully.	
Completed	
Completed OpenVPN installation. Installing configuration files Installing certificate and key files Completed	Ŧ
	^ ∉ ⊄⊗ 2
Nullsoft Install System v2.50-1 < Back Close Cancel	
🕎 Connexions réseau	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ 🔄 > Panneau de configuration > Réseau et Internet > Connexions réseau >	
Organiser 🝷	
Ethernet0 sitka.local Intel(R) 82574L Gigabit Network C	OpenVPN Wintun Câble réseau non connecté Wintun Userspace Tunnel

### c- Test de connexion sur un client Android

Sur google store on télécharge l'application openvpn

÷		Q	:
<b>?</b>	OpenVPN Fast & Sa Client <sub>OpenVPN</sub>	l Connect – fe SSL VPN	
Dés	installer	Ouvrir	

Sur l'interface web de pfsense on télécharge le client androïde pour smartphone en cliquant

Android

.

Sur

Une fois Le fichier que le fichier téléchargé on l'envoi par mail et on le récupère sur notre messagerie sur le smartphone, Ce fichier on va l'enregistrer et on va l'injecter dans notre application openvpn Android, après on rentre notre identifiant utilisateur et notre mot de passe

22:19 • • • ▲ ▲ @ >. • • • • • • • • • • • • • • • • • •	22:24 🐱 🋦 🧿 >_ 🔕 👘 🕸 🖹 🗊 1
URL FILE 1	← Imported Profile
Please, select .ovpn profile to import Location: /storage/emulated/0/Download	
e Back	Profile successfully imported
heimdall-UDP4-1194-android-config.ovpn	Profile Name
heimdall1919-config.ovpn	3.4.200.74 [heimdall-UDP4-1194-android-com
	Username
	kaiser
2	Save password
3	Connect offer import
┝━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━	
Dueflee	
Profiles 😭	
Profiles 🖻	
ONNECTED	DISCONNECTED
OpenVPN Profile	DISCONNECTED OpenVPN Profile 93.4.200.74 Ineimdall-UDP4-1194-a
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a	DISCONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a Profile]
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a	DISCONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a Profile] Enter password
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a ndroid-config]	
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a  Android-config]	Profiles      OpenVPN Profile     93.4.200.74 [heimdall-UDP4-1194-a      Indroid-config]      Enter password      Profile: 93.4.200.74     Iheimdall-UDP4-1194-android-config]     Password
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a	DISCONNECTED OpenVPN Profile 93.4.200,74 Ineimdall-UDP4-1194-a Profile: 93.4.200,74 Ineimdall-UDP4-1194-android-configI Password Azerty123
ONNECTED OpenVPN Profile 93.4.200.74 [heimdall-UDP4-1194-a ndroid-config]	Profiles     OpenVPN Profile     93.4.200.74 [heimdall-UDP4-1194-a      ndroid-config]     Enter password     Profile: 93.4.200.74 [heimdall-UDP4-1194-android-config]     Password     Azerty123

Voila la connexion est établie de mon smartphone connecté en 4G sur mon serveur Pfsense connecté sur la box Internet de mon fournisseur d'accès ; je peux vérifier mon accès à hermes avec un ping depuis mon smartphone

22:42 🗯	🛚 📼 🖪 ቆ 🗛 🚱 • 🗇 Ժ 🕸 📓	15 % 📋	07:26	10 C	8 4	s s	- 🔿		1		- 🗳 🛛 8	37 % 🗖
— Рг	ofiles	10	64 by 127 t	/tes :ime=	from 86.0	172 ms	.20.0	0.14:	icm	ıp_se	q=2	ttl=
			64 by 127 t	/tes :ime=	trom 67.8	172 ms	.20.0	0.14:	10	ip_se	q=3	tt1=
CONNEC	TED		64 by 127 t	tes ime=	from 64.3	172 ms	.20.0	0.14:	icm	p_se	q=4	ttl=
	OpenVPN Profile		64 by	tes	from	172	.20.0	0.14:	icm	ip_se	q=5	ttl=
	93.4.200.74 [heimdall-UDP4-1194	4-a	64 by	tes	from	172	.20.0	0.14:	icm	ıp_se	q=6	ttl=
	ndroid-config]		64 by	tes	from	172	.20.0	0.14	icm	ip_se	q=7	ttl=
			64 by	tes	from	ms 172	.20.0	0.14:	icm	p_se	q=8	ttl=
CONNEC	CTION STATS		127 t 64 by	tes	from	ms 172	.20.0	0.14:	icm	ip_se	q=9	ttl=
5.3KB/s			127 t 64 by	:ime= /tes	78.3 from	ms 172	.20.0	0.14:	icm	p_se	q=10	ttl
			=127 ping:	time ser	e=79. ndmsg	2 ms : Ne	tworl	k is	unre	acha	ble	
			ESC		-	CTRL	AI	LT	—	Ļ		t
			1	2	3	4	5	6	7	8	9	0
OB/S		CTER OUT	а	z	е	r	t	v	u	i	0	p
4 B/S	🔶 🕇 🕯	B/S						-				•
			q	S	d	f	g	h	j	k	1	m
DURATION 00:05:04	PACKET RECEIVED		$\sim$	14				, r				
	-	•	°.	~	~ ~		- `	/ L	, ,			
kaiser		Ð	?123	з,		Ð	F	rançai	5			4
Renser												

De même Sur l'interface web (Status+Openvpn] la connexion vpn du client Android est enregistré

Status / OpenVPN 幸 📖 🗉								
OPENVPN SITKA UDP4:1194 Client Connections: 1								
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher		
UNDEF kaiser	77.130.124.130:46214	192.168.1.13	2022-01-24 22:56:12	5 KiB	2 KiB	AES-256-GCM	×	
Status: 🖉 Actions: C 💿								
Show Routing Table     Display OpenVPN's internal routing table for this server.								