Nicolas ERNST

Projet NovaResQ

## **BTS SIO 2025 Option SISR**

# Documentation Technique Situation Professionnelle 2

# Table des matières

1) Préparation des routeurs5
A) Initialisation de PfSense5
2) Configuration des PfSense 25
A) Première connexion + changement de mot de passe
B) CARP LAN + High Availability31
C) CARP WAN
3) OpenVPN RW
Documentation d'exploitation, L'utilisation et la gestion du Lot 1
Introduction :
Installation des rôles 109
Installation de l'Active Directory et DNS 117
2. Installation PRTG 126
3. Gestion Active Directory 132
Documentation d'installation Modoboa (Ubuntu)138
Introduction138
Installation
1) Installation d'Asterisk 144
A) Mise à jour du serveur + installations des dépendances requises 144
B) Téléchargement et pré-installation de Asterisk 146
C) Compilation et installation de Asterisk 153
C) Compilation et installation de Asterisk

B) Installation des dépendances requises	222
C) Téléchargement et déploiement de eBrigade	230

# Configuration des routeurs PfSense



09/04/2025

Nicolas ERNST

## 1) Préparation des routeurs

A) Initialisation de PfSense

Cliquer sur Accept.



Choisir Install puis valider.

Welcome         Welcome         Welcome         Install pfSense         Install pfSense         Launch a shell for rescue operations         Recover config.xml from a previous install	
Install Descue wellInstall pfSense Launch a shell for rescue operations Recover config.xml from a previous install	]
Cancel>	-

Choisir Auto (ZFS) puis valider.

pfSense Installer	
Partitioning         Ноw would you like to partition your disk?         Auto (2FS)       Buided Root-on-2FS         Guided UFS Disk Setup         Manual       Manual Disk Setup (experts)         Shell       Open a shell and partition by hand	
Cancel>	
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuid	le

Sélectionner Install

Configure Options:	
>>> Install	Proceed with Installation
I I I I I Per Disks:	stripe: 0 disks
- Rescan Devices	*
- Disk Info	*
N Pool Name	pfSense
4 Force 4K Sectors?	YES
E Encrypt Disks?	NU (DIGO)
P Partition Scheme	GPT (BIUS)
S Swap Size	1g
M Mirror Swap?	
м вногурт эмар?	
	<cancel> unctuation. TAB or ENTER]</cancel>

Choisir Stripe et valider.



Choisir le disque et valider.



Cliquer sur OK pour valider.



Attendre la fin du téléchargement.

pfSense Insta	ller
	Checksum Verification
	base.txz [ In Progress ]
	Verifying checksums of selected distributions.
	Overall Progress 0%

Cliquer sur Reboot pour redémarrer et finaliser l'installation. Attendre ensuite jusqu'à la prochaine étape.



Choisir le0 pour configurer le WAN.

```
Enter the WAN interface name or 'a' for auto-detection (le0 le1 or a): le0
```

Choisir ensuite le1 pour l'interface LAN.

Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (le1 a or nothing if finished): le1

Valider en tapant y. Attendre ensuite la fin de la configuration.

The interfaces will be assigned as follows: WAN -> le0 LAN -> le1 Do you want to proceed [y:n]? y

Nicolas ERNST

Voici le menu de PfSense. Choisir 2 pour modifier les adresses IP des interfaces.

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0) VMware Virtual Machine - Netgate Device ID: c285f019870b47b7fed9 \*\*\* Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense \*\*\* -> v4/DHCP4: 192.168.1.148/24 WAN (wan) -> le0 LAN (lan) -> le1 -> v4: 192.168.1.1/24 0) Logout (SSH only) 1) Assign Interfaces 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 7) Ping host 15) Restore recent configuration 16) Restart PHP-FPM 8) Shell Enter an option: 2

Sélectionner le LAN (2).

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6) 2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: 2

Choisir no.

Configure IPv4 address LAN interface via DHCP? (y/n) n

Documentation situation professionnelle 2

Nicolas ERNST

Entrer la nouvelle adresse LAN puis sélectionner le port 24.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:

> 192.168.50.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.

e.g. 255.255.255.0 = 24

255.255.0.0 = 16

255.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):

> 24
```

Appuyer sur la touche enter.



Choisir no et appuyer sur enter à la prochaine étape.

Configure IPv6 address LAN interface via DHCP6? (y/n) n Enter the new LAN IPv6 address. Press <ENTER> for none:

>

Choisir no aux 2 prochaines étapes.



## Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Appuyer sur enter pour valider tous les changements.

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 LAN address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.50.1/
Press <ENTER> to continue.
```

IL FAUT REALISER LE MEME PROCESSUS POUR <u>LE 2EME ROUTEUR</u> EN REMPLACANT L'ADRESSE LAN PAR UNE AUTRE (ex : 192.168.50.2).

2) Configuration des PfSense

### A) Première connexion + changement de mot de passe

Accéder maintenant à l'interface web du PfSense Master (192.168.50.1) via un navigateur sur un poste client.

Rentrer l'identifiant "admin" avec le mot de passe de base "pfsense" puis cliquer sur sign in.

v 🖸 přeme - Login X +	- ø ×
← → ♂ O Non sécurisé https://192.168.50.1/index.php	🗟 🌣 😩 :
<mark>pf</mark> sense	Login to pfSense
SIGN IN	
admin	
••••••	
pfSense is developed and maintained by Nelgate. © ESF 2004 - 2025 View license.	

Voici la page d'accueil de PfSense. Nous allons maintenant changer le mot de passe de base pour accéder à PfSense en tant qu'admin.



Aller dans System puis dans User Manager.

		System -	Interfa	ces 🔻	Firewall 🗸	s
Sta Sys Name User Syste	atus / C stem Info s	Advanced Certificates General Setu High Availab Package Mai Register Routing Setup Wizard Update	p ility nager	) (Local D ine Scfdde2dd	atabase) c1537e67992 ; LTD	
Versi	on	User Manage Logout (adm built on We FreeBSD 14	in) d Jun 28 (	ov <b>12 202</b> 64) 03:53:34 U NT	<b>0</b> JTC 2023	

Cliquer sur l'icône du petit crayon pour accéder aux paramètres du compte admin de PfSense.



Entrer un nouveau mot de passe et confirmer le.

c		🔹 Interfaces 🕶 Firewall 👻 Services 👻 VPN 👻 Status 👻 Diagnostics 👻 Help 👻 🕒	
	System / User Ma	anager / Users / Edit 🛛 😧	
	Users Groups S	Settings Authentication Servers	
	User Properties		
	Defined by	SYSTEM	
	Disabled	This user cannot login	
	Username	admin	
	Password	Password Confirm Password	
	Full name	System Administrator User's full name, for administrative information only	
	Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
	Custom Settings	Use individual customized GUI options and dashboard layout for this user.	
	Group membership	admine	

Descendre tout en bas de la page et cliquer sur Save.

<b>+</b> Ac
Enter authorized SSH keys for this user
C Keep shell command history between login sessions If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.

Une fois cette opération ayant été effectué, votre mot de passe a été changé.

**!** Cette opération est aussi à réaliser sur le deuxième PfSense en inscrivant <u>le</u> <u>même</u> mot de passe que sur le PfSense Master. **!** 

B) CARP LAN + High Availability

Avant de commencer cette étape, voici un rappel de la configuration des deux cartes LAN sur les 2 pfsense. On peut regarder ça en allant dans Interfaces, puis Assignements. Ensuite il faut cliquer sur em1 (LAN).

Voici la carte LAN sur le PfSense Master :

<i>∎/</i> isense	vstem • Interfaces • Firewall • Services	• VPN • Status • Dispositics •	Help + G4		
COMMUNITY ESITION					
Interfaces /	LAN (em1)		₩ 0		
General Config	uration			1	
	sable 👩 Enable interface				
Descr	ption LAN				
	Enter a description (name) for the interface her	0.			
IPv4 Configuration	Type Static IPe4	¥			
IPv6 Configuration	Type None				
MAC Ad	fress (xexecutioned)				
	This field can be used to modify ("spoof") the N Enter a MAC address in the following format: x	MAC address of this interface. concorcococcor or leave blank			
	MTU				
	If this field is blank, the adapter's default MTU	will be used. This is typically 1500 bytes but can vary in	some circumstances.		
	MSS				
	If a value is entered in this field, then MSS clarr minus 60 for IPv6 (TCP/IPv6 header size) will b	iping for TCP connections to the value entered above n in effect.	tinus 40 for IPv4 (TCP/IPv4 header size) and		
Speed and D	uplex Default (no preference, typically autoselect)	*			
	Explicitly set speed and duplex mode for this in WARNING: MUST be set to autoselect (automa	iterface. tically negotiate speed) unless the port this interface o	onnects to has its speed and duplex forced.		
Static IPv4 Co	figuration			1	

Voici la carte LAN sur le PfSense Backup :

pfSense.home.arpa - Interface: X     pfSense.home.arpa - Interface:     A     O     Non securitie     Neters//192.168.50.2/interfaces.php?ifsla	•	- 0 20 0 + 1
community Cartons System	n - Interfaces - Firewall - Services - VPN - Status - Disproptics - Help - 😝	
Interfaces / LA	i (em1) ≡ ≅ Ø	
General Configurat	on	
Enable	C Enable interface	
Description	LAN Tomar a description (nume) for the interface here.	
IPv4 Configuration Type	Static IPv4 ¥	
IPv6 Configuration Type	None	
MAC Address	INTERCEPTION	
мть	If this field is blank, the adapter's default MTU will be used. This is typically 1800 bytes but can vary in some circumstances.	
MS	If a value is entered in this field, then MSG clamping for TOP connections to the value entered above minus 40 for IPH4 (TOP/IPH4 header size) and minute 40 for IPH4 (TOP/IPH4 header size) will be in effect.	
Speed and Dupley	Default (no preference, typically autoreliency Diputoly are speed and deplane mode for this interface. WWMMMM. MMLT are to autorelated (autoreliandy regoldrate speed) unless the port this interface convects to has its speed and duplex forced.	
tatic IPv4 Config	ration	
IPv4 Address	192.168.50.2 / 24 🗸	
IPv4 Upstream gateway	None * + Add a new gateway	
	If this interface is an internet connection, select an existing Gateway from the list or add a new one using the "Add" button.	

Ici, on peut voir que les deux cartes LAN sont sur la même plage d'adresse.

Pour créer notre CARP LAN, il faut d'abord configurer une IP virtuelle sur notre plage d'adresse.

Pour ce faire, aller dans Firewall puis Virtual IPs sur le PfSense Master.



Cliquer sur le bouton ADD.

:

Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du LAN).

Une fois les paramètres remplis, cliquer sur Save.

Cette opération est aussi à effectuer sur le PfSense Backup <u>en remplaçant seulement</u> <u>Skew par 100 à la place de 0</u>.

Firewall / Virtual	IPs/ Edit		0
Edit Virtual IP			
Туре	O IP Alias       CARP		○ Other
Interface	LAN	*	
Address type	Single address	*	
Address(es)	192.168.50.254 The mask must be the network's subnet mask. It doe	s not specify a CIDR range.	/ 24 🗸
Virtual IP Password	Enter the VHID group password.	Cor	
VHID Group	1 Enter the VHID group that the machines will share.	~	
Advertising frequency	1       Base       The frequency that this machine will advertise. 0 mea       master.	O     Ske ans usually master. Otherwise	w e the lowest combination of both values in the cluster determines the
Description	CARP LAN A description may be entered here for administrative	reference (not parsed).	
	B Save		

Cliquer ensuite sur Apply Changes pour appliquer les changements.

The VIP configuration has been changed.		Apply Change				
The changes must be applied for them to take effect.						
Virtual IP Address						
/irtual IP address	Interface	Туре	Description	Actions		
192.168.50.254/24 (vhid: 1)	LAN	CARP	CARP	e 🖉 🛅		
192.168.1.140/24 (vhid: 10)	WAN1	CARP	CARP WAN1	e 🖉 🖬		
192.168.1.141/24 (vhid: 20)	WAN2	CARP	CARP WAN2	e 🖉 🖬		

Aller ensuite dans Status puis CARP (failover).
Sense System - Interfaces - Firewall - Services - VPN -	Status - Diagnostics - Help -
Firewall / Rules / DMZ	Captive Portal CARP (failover) 🔁 🔟 🗐 🕜
The changes have been applied successfully. The firewall rules are now reloading in the bac Monitor the filter reload progress.	based a bhog bases
Floating WAN1 LAN WAN2 OVPN_INTERFACE DMZ Ope	DNS Resolver Filter Reload Gateways
Rules (Drag to Change Order)	Interfaces
States Protocol Source Port Destination Port	G hedule Description Actions
O/46.40 MiB IPv4 * DMZ net * * *	NTP

Si tout est normal, voici ce qui devrait s'afficher sur les deux PfSense.

• PfSense Master :

**Nicolas ERNST** 

← → C Non securité https://192.168.50.1/status_carp.php		r 😩
COMMANT 19 nos		
Status / CARP 🚔 🖬 😧		
CARP Maintenance           Temporarily Disable CARP		
CARP Status         Virtual IP Address         Status           Interface and VHID         Virtual IP Address         Status           LAN©1         192:168.50.254/24         MASTER		
PfSense Backup :		- 0
3 O Non sécurisé https://192.168.50.2/status_carp.php	ା ସ୍ଥାଇ	\$
System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -		
Status / CARP 🚔 🖬 😧		
CARP Maintenance           Temporarily Disable CARP              // Enter Persistent CARP Maintenance Mode		
CARP Status         Interface and VHID         Virtual IP Address         Status           LAN©1         192.168.50.254/24         O BACKUP		

-> Explication : le routeur master (192.168.50.1) est pour l'instant actif. Si ce dernier tombe en panne, le routeur backup (192.168.50.2) prendra le relais en passant de backup à master.

Voici un exemple quand le routeur master est éteint.

•



Passons maintenant à la configuration de la High Availability afin que les paramètres effectués sur le PfSense Master soit aussi appliqués sur le Backup.

Aller dans System puis High Availability.

Nicolas ERNST



Voici les paramètres à rentrer dans le PfSense Master.

System / High A	vailability	<u>Lut</u> 😮
State Synchronizatio	on Settings (pfsync)	
Synchronize states	pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). If interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)	also listens on that
Synchronize Interface	LAN If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.	
Filter Host ID	37e67992 Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.	
pfsync Synchronize Peer IP	192.168.50.2         Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.         nization. Settings. (XML RPC: Sync.)	
nchronize Config to IP	192.168.50.2 Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!	remote system's port an
Remote System Username	admin Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!	
Synchronize admin	synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System	n Username account.
Select opt	ions to sync 4 User manager users and groups 4 Authentication servers (e.g. LDAP; RADIUS) C Certificate Authorities, Certificate Revocation Lists 5 Firewall also 6 Firewall also 7 Firewall alsoes 9 NAT configuration 1 Pisec configuration 9 OperVPN configuration 10 DerOrVN configuration 10 DerOrVN configuration 10 DerOrVN extra settings 10 DEOrVN faily settings 10 DEOrVN faily settings 10 State Route configuration 11 Yintal IPS 11 Yintal IPS 12 Traffic Shaper Lonfiguration 13 Traffic Shaper Lonfiguration 14 Traffic Shaper Lonfiguration 15 DNS Forwarder and DNS Resolver configurations 16 Captive Portal 17 Togreen	

Voici les paramètres à rentrer dans le PfSense Backup.

State Synchronization	n Settings (pfsync)	
Synchronize states	pfsync transfers state insertion, update, and deletion messages betwee Each firewall sends these messages out via multicast on a specified inter interface for similar messages from other firewalls, and imports them init This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configu	een firewalls. :face, using the PFSYNC protocol (IP Protocol 240). It also listens on that o the local state table. uration Synchronization Settings below)
Synchronize Interface	LAN V If Synchronize States is enabled this interface will be used for communic It is recommended to set this to an interface other than LANI A dedicated An IP must be defined on each machine participating in this failover group	ation. interface works the best. 2.
Filter Host ID	An IP must be assigned to the interface on any participating sync nodes. d1702440 Custom pf host identifier carried in state data to uniquely identify which h Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01 Each node nardicipating in state synchronization must have a different ID.	ost created a firewall state. , abcdef01).
pfsync Synchronize Peer IP	192.168.50.1       Setting this option will force pfsync to synchronize its state table to this IF	P address. The default is directed multicast.
Synchronize Config to IP	TIP Address Enter the IP address of the file of the the device comparation section XMLRPC sync is currently only supported over connections using the same pro protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup clust	III NE PAS REMPLIR III     s should be synchronized.  otocol and port as this system - make sure the remote system's port and er members!
Remote System Username	admin Enter the webConfigurator username of the system entered above for synchro Do not use the Synchronize Config to IP and username option on backup clust	nizing the configuration. er members!
Remote System Password	Enter the webConfigurator password of the option unless debut for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!	III ENTRER LE MEME MOT DE PASSE QUE
Synchronize admin	synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have This option automatically updates XMLRPC Remote System Password when t	a different admin password. he password is changed on the Remote System Username account.
Select options to sync	User manager users and groups     Authentication servers (e.g. LDAP, RADIUS)     Certificate Authorities, Certificates, and Certificate Revocation Lists     Firewall rules     Firewall rules     Firewall aliases     NAT configuration     PoperVPN configuration     OperVPN configuration     OperVPN configuration (Implies CA/Cert/CRL Sync)     DHCP Server settings     DHCP Relay settings     OHCP Kelay settings     Static Route configuration     Virtual IPs     Traffic Shaper configuration     Traffic Shaper configuration     DNS Forwarder and DNS Resolver configurations     DNS Forwarder     DNS Forwarder	

Cliquer sur Save pour valider les paramètres sur les deux PfSense. Une fois cela fait, les deux PfSense seront synchronisés.

Voici un test : Création d'une règle de pare-feu sur le PfSense Master qui va se répliquer sur le Backup.

- Ini	terfaces +	Firewall +	Servic	es +	VPN +	Status +	Diagnostics -
/ DMZ		Aliases NAT Rules					
oplied service ogress.	essfully. The	Schedules Traffic Shape	er	bading in	the backgro	ound.	
LAN	WAN2	OVPN_INTER	ACE	DMZ	OpenVP	'N	

Dans le <u>PfSense Master</u>, aller dans Firewall puis Rules.

Cliquer sur Add pour ajouter une nouvelle règle (pour l'exemple, création d'une règle dans le LAN ici).

Floating	WAN1	LAN	WAN2	OVPI	INTERFACE	DMZ	OpenVPN			
Rules (I	Drag to Ch	ange Ord	er)							
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
~	18/639 KiB	*	*	*	LAN Address	443 80	*	*	Anti-Lockout Rule	٥
- 🗸	2/44 KiB	IPv4 UDP	192.168.50.3	*	*	161 (SNMP)	*	none	PRTG	҄ ∜
□ ✓	3/270 KiB	IPv4 *	*	*	*	*	*	none	PETIT POIX	∜ ∕ ि © 面 ×
• 🟅	0/0 B	IPv4 *	LAN net	*	*	*	WAN_FAILOVER	none	Default allow LAN to any rule	∜ ∕ ⊄ © © 面 ×
	0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	҄ ∜
0								dd Add 🛅	Delete 🚫 Toggle 🔲 Copy 🛛	Save + Separato

Descendre tout en bas, ajouter une description (Test dans l'exemple) et cliquer sur Save.

Extra Options	
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Legen Setting a page)
Description	Test A description may be entered here for administrative reference. A performant of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Cisplay Advanced
	B Save

Cliquer sur Apply Changes.

Nicolas ERNST

Firewall / Rules / LAN									≢ ਘ 🗏 9
The firewall The change	rule configu s must be ap	ration has b oplied for th	een change em to take e	d. ffect.					<ul> <li>Apply Changes</li> </ul>
Floating	WAN1	LAN	WAN2	OVPN_INTERFACE	DMZ	OpenVPN			

La nouvelle règle "Test" apparaît dans la liste des règles sur le LAN.



Si tout fonctionne, la règle apparaît aussi sur le PfSense Backup.

👻 🗾 pfSense.home.arpa - Firewall: R 🗙 💆 pfSense.home.arpa - Fire	ewall: R × +				- 0
← → C O Non sécurisé https://192.168.50.2/firet II_rule	es.php?if=lan				🌆 Q 🕁 💄
<i>pf</i> sense	System - Interfaces -	Firewall • Services •	VPN • Status • Diagnostics •	Help - 🕒	
COMMUNITY EDITION					
Firewall /	Rules / LAN			≢ Ш 🗏 🕅	
Floating		OVPN INTERFACE DM7	OpenVPN		
· recently					
Rules (Drag	g to Change Order)				
U Sta	ates Protocol Source	Port Destination Port	Gateway Queue Schedule	Description Actions	
✓ 20	0/4.11 * *	* LAN 443	* *	Anti-Lockout Rule	
		Address 80		1.1007	
	/10 KiB IPv4 * *	* * *	* none	Test UOD X	
□ ✔ 0/	/417 KiB IPv4 192.16	.50.3 * 101	none	PRIG 🕹 🖉 💭 🕥 💼	
	UDP	(SNMP	)	×	
□ ✔ 0/	/271 KiB IPv4 * *	* * *	* none	PETIT POIX 🕹 🖉 🗋 🗙	
□ <mark>↓</mark> º/	/0 B IPv4 * LAN ne	* * *	WAN_FAILOVER none	Default allow LAN to any rule 🕹 🖋 🗔 🛇 💼 🗙	
□ ✔ 0/	/0 B IPv6 * LAN ne	* * *	* none	Default allow LAN IPv6 to any 🕹 🖋 🖵 🛇 🛅 rule 🗙	
			1 Add 1 Add	elete 🚫 Toggle 🔲 Copy 🔒 Save 🕂 Separator	
0					

Vous pouvez ensuite supprimer la règle créée, c'était juste un exemple (elle va aussi se supprimer sur le PfSense Backup).

**!** Les règles appliquées sur le PfSense Master s'appliqueront aussi sur le Backup, mais cela <u>ne marche pas inversement</u> ! Seul le Pfsense Master peut influer sur le Backup. **!** 

C) CARP WAN

Pour cette partie, chaque PfSense devra disposer chacun de deux cartes WAN distinctes sur la même plage d'adresse. Dans mon cas, cette plage sera en 192.168.1.0.

Aller dans Interfaces puis Assignements.

System +	Interfaces -	Firewall 🗸	Services +	VPN +	Status 🗸	Dia
 	Assignments	>+	_			

Ici, en ayant ajouté une troisième carte réseau sur le PfSense Master avec les mêmes propriétés que celle déjà existante en WAN, nous pouvons voir que em2 est disponible à la configuration (il reste un assignement réseau à ajouter grâce à l'ajout de notre nouvelle carte réseau). Cet assignement sera le 2ème WAN.

Cliquer sur Add.



Nicolas ERNST

Documentation situation professionnelle 2

Une fois après avoir créé une nouvelle interface, celle-ci s'est automatiquement renommée en "OPT1".

Cliquer dessus pour modifier ses paramètres.

h	nterface	Network port	
١	WAN1	em0 (00:0c:29:43:e4:bb)	•
l	AN	em1 (00:0c:29:43:e4:c5)	Delete
	OPT1	em2 (00:0c:29:43:e4:cf)	Delete

Documentation situation professionnelle 2 50 sur 247

Cocher "Enable Interface", renommer l'interface en "WAN2", et changer la configuration IPv4 en DHCP (ou statique, même si l'adresse fourni en DHCP via PfSense ne changera jamais).

eneral Configuratio	n
Enable	Enable interface
Description	WAN2
	Ептена иссоприон (нолье) но чистиченое пого.
/4 Configuration Type	DHCP
v6 Configuration Type	None
MAC Address	XXXXXXXXXXXX
	This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxxxxx or leave blank.
мти	
	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	
	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect)
	Explicitly set speed and duplex mode for this interface.

Descendre tout en bas et cliquer sur Save pour appliquer les changements sur l'interface.

**Nicolas ERNST** 

	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).
Alias IPv4 address	✓ 24 ✓ The value in this field is used as a fixed alias IPv4 address by the DHCP client.
Reject leases from	To have the DHCP client reject offers from specific DHCP servers, enter their IP addresses here (separate multiple entries with a comma). This is useful for rejecting leases from cable moderns that offer private IP addresses when they lose upstream sync.
Reserved Networks	
Block private networks and loopback addresses	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	

#### Cliquer sur Apply Changes.



Documentation situation professionnelle 2

Voici la configuration qui apparaît sur le menu du routeur PfSense Master.

- WAN1: 192.168.1.143
- WAN2:192.168.1.145



Répéter le même processus sur le routeur Backup.

Voici la configuration qui apparaît sur le menu du routeur PfSense Backup.

- WAN1:192.168.1.144
- WAN2:192.168.1.146



Nous allons maintenant créer 2 nouvelles IP virtuelles pour nos 2 CARP WAN.

Sur le PfSense Master, aller dans Firewall puis Virtual IPs.



Cliquer sur le bouton Add.

Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du WAN).

<u>Il ne faut pas</u> remettre le même VHID Group sur l'IP virtuelle LAN (j'ai mis 10 ici).

it Virtual IP						
Туре	O IP Alias	CARP	O Proxy AF	RP Oth	er	
Interface	WAN1		~			
Address type	Single address		~			
Address(es)	192.168.1.140 The mask must be the	network's subnet mask. It does	not specify a CIDR ran	ge.	/ 24 🗸	
Virtual IP Password	Enter the VHID group p	assword.		Confirm		
VHID Group	10 Enter the VHID group t	nat the machines will share.	~			
Advertising frequency	1 Base The frequency that this master.	machine will advertise. 0 mea	✓ ns usually master. Othe	0 Skew rwise the lowest combinat	ion of both values in the cluster of	✓ determines the
Description	CARP WAN1 A description may be e	ntered here for administrative (	reference (not parsed).			

Une fois les paramètres remplis, cliquer sur Save.

Refaire la manipulation en créant une nouvelle IP virtuelle pour les 2ème WAN, tout en inscrivant un autre VHID Group comme pour le première IP virtuelle WAN (j'ai mis 20 ici).

Voici, dans mon cas, les paramètres à entrer.

Une fois les paramètres remplis, cliquer sur Save.

#### Nicolas ERNST

Type					○ Other	
<u>-112-</u>		- CAN	U 1 10xy	-444	Outer	
Interface	WAN2		~			
Address type	Single address		~			
Address(es)	192.168.1.141				/ 24	*
	The mask must be the net	work's subnet mask. It does	not specify a CIDR ra	inge.		
Virtual IP Password	•••••			•••••		
	Enter the VHID group pass	word.		Confirm		
VHID Group	20		~			
	Enter the VHID group that t	the machines will share.				
dvertising frequency	1		~	0		~
<u> </u>	Base			Skew		
	The frequency that this ma master.	ichine will advertise. O mear	ns usually master. Oth	nerwise the lowes	t combination of both values in th	ne cluster determines the
Description	CARP WAN2					
	A description may be enter	ed here for administrative re	eference (not parsed	L.		

Cette opération n'est pas a effectué sur le Backup, grâce au High Availability, les paramètres se sont déjà répliqués.

Sur le PfSense Master, retourner ensuite dans Status puis CARP (failover).

Nicolas ERNST

Sense System - Interfaces - Firewall - Services - VPN -	Status - Diagnostics - Help -
Firewall / Rules / DMZ	Captive Portal CARP (failover) Dashboard
The changes have been applied successfully. The firewall rules are now reloading in the backg Monitor the filter reload progress.	DHCP Leases × DHCPv6 Leases
Floating WAN1 LAN WAN2 OVPN_INTERFACE DMZ OpenV	DNS Resolver Filter Reload Gateways
Rules (Drag to Change Order)	Interfaces
□         States         Protocol         Source         Port         Destination         Port         C           ↓         0/46.40 MiB         IPv4 *         DMZ net         *	IPsec thedule Description Actions Monitoring DMZ Internet $3 - 2 - 2 = 0$ for $\times$

Les 2 CARP WAN sont bien présents en MASTER sur le PfSense Master.

👻 🗹 pfSense.home.arpa - Status: CA 🗙 💆 pfS	Sense.home.arpa - Interfaces ×   +			- 0
← → C O Non sécurisé https://192.16	8.50.1/status_carp.php			\$z Q ☆ 😩
	COMMUNITY EDITION System - Interfaces - Firewall	Services - VPN - Status - Diagno	ostics - Help - 🕞	
	Status / CARP		幸 🗷 🕑	
	CARP Maintenance			
	🚫 Temporarily Disable CARP 🖋 Enter Persistent CARP M	faintenance Mode		
	CARP Status			
	Interface and VHID	Virtual IP Address	Status	
	LAN@1	192.168.50.254/24	MASTER	
	WAN1@10	192.168.1.140/24	MASTER	
	► WAN2@20	192.168.1.141/24	MASTER	

Sur le PfSense Backup, les CARP WAN sont aussi présents mais en Backup.

👻 🙍 pfSense.home.arpa - Status: CAL 🗙 💆 pfSen	ise.home.arpa - Status: CAI 🗙 🕂			-
← → C ONon sécurisé htt; €//192.168.5	50.2/staus_carp.php			ba ⊂,
	COMMUNITY EDITION System - Interfaces -	Firewall - Services - VPN - Status -	Diagnostics - Help -	G
	Status / CARP		幸 画	. 0
	CARP Maintenance			
	S Temporarily Disable CARP	t CARP Maintenance Mode		
	CARP Status			
	Interface and VHID	Virtual IP Address	Status	
	LAN@1	192.168.50.254/24	0 BACKUP	
	WAN1@10	192.168.1.140/24	D BACKUP	
	WAN2@20	192.168.1.141/24	D BACKUP	

Si le routeur Master est en panne, le routeur Backup prend bien le relais.

👻 🗹 pfSense.home.arpa - Status: CAI 🗙 💆 pfSens	se.home.arpa - Status: CAI × +				
← → C S Non sécurisé http://192.168.5	0.2/staus_carp.php				
	Sense System - Interface	s + Firewall + Services +	VPN - Status -	Diagnostics - Help -	¢
	Status / CARP				≢ ⊎ 0
	CARP Maintenance				
	🚫 Temporarily Disable CARP 🗲 Enter P	Persistent CARP Maintenance Mode			
	CARP Status				
	Interface and VHID	Virtual IP	Address		Status
	LAN@1	192.168.	50.254/24		MASTER
	WAN1@10	192.168.	1.140/24	(	MASTER
	WAN2@20	192.168.	1.141/24		MASTER

De même si l'on désactive une interface sur le PfSente Master (WAN1 ici), dans CARP (failover) WAN1 sera bien évidemment inactif sur le PfSense Master, et le WAN1 sur le PfSense Backup passera en MASTER. • PfSense Master :

Y of pfSense.home.arpa - Status: CA × of pfSens	se.home.arpa - Status: CAI 🗙   🕂						
← → C S Non sécurisé https://192.168.5	50.1/status_carp.php						
	COMMUNITY EDITION	Interfaces - Firewall -	Services - VPI	N • Status •	Diagnostics +	Help +	G
	Status / CARP						≢ ਘ 8
	CARP Maintenance						
	S Temporarily Disable CARP	🎾 Enter Persistent CARP Main	tenance Mode				
	CARP Status						
	Interface and VHID		Virtual IP Address			Status	
	LAN@1		192.168.50.254/2	24		MASTER	
	WAN1@10		192.168.1.140/24	4		$\bigcirc$	
-	WAN2@20		192.168.1.141/24	4		MASTER	

• PfSense Backup :

Y 🗹 pfSense.home.arpa - Status: CAL X 💆 pfSens	se.home.arpa - Status: CA × +		
← → C ON Non sécurisé https://192.168.5	0.2/status_carp.php		
	System - Interfaces - Firewall -	Services - VPN - Status - Diagnostics -	Help - 🕞
	Status / CARP		幸 🔟 😧
	CARP Maintenance		
	Temporarily Disable CARP	nance Mode	
	CARP Status		
	Interface and VHID	Virtual IP Address	Status
	LAN@1	192.168.50.254/24	0 BACKUP
	• WAN1@10	192.168.1.140/24	MASTER
	WAN2@20	192.168.1.141/24	D BACKUP

# 3) OpenVPN RW

# !Cette partie est à réaliser seulement après avoir configurer ADDS sur leserveur Windows (voir doc associé)!

Il reste à configurer le VPN OpenVPN RW pour les clients distants. Premièrement, aller dans System puis Certificates.

yfSense.hor	me.arpa - Status: Da	as <b>X</b>	+				
← → C	8 Non sécurisé	https:/	/192.168.50.1	1			
CPU Type	System   Inter  Advanced  Certificates  General Setup  High Availability  Package Manager  Register  Routing  Setup Wizard  Update  User Manager  Logout (admin)  built on Wed Jun 2  FreeBSD 14.0-CUR  The system is on t Version informatio  2 CPUs: 2 package  AES-NI CPU Crypto  QAT Crypto: No	faces - 3 (Local hine 3 cfdde2 hnologi pv 12 20 164) 28 03:53:34 RENT the latest v on updated Core(TM) i e(s) x 1 colo p: Yes (inac	Firewall - Database) dc1537e67992 es LTD D20 4 UTC 2023 errsion. I at Tue Apr 22 18 5-12450H re(s) ctive)	Services -	VPN -	Status - D Netgate Service Contract t NETGATE If you purchased yo Community Suppor hardware, you have the NETGATE RES You also may upgra Support subscription committed to deliven more than competiti . Upgrade Your S . Netgate Global S . Netgate Profess	iagnostics - es And Suppor ype Community Community AND pfSense gatewa rt at the point of sa access to various OURCE LIBRARY de to a Netgate Gli n. We're always on ring enterprise-clas ve when compared upport  Support FAQ  sional Services
Hardware crypto	Inactive						

Dans la partie Authorities, cliquer sur Add pour rajouter un certificat d'autorité.

Search						
Search term	L			Both	✓ Q Sea	rch 🖸 Clear
	En	ter a search string o	r *nix regular expressi	on to search certificate names and distinguished nar	nes.	
Certificate A	uthorities					
Name	Internal	Issuer	Certificates	Distinguished Name	In Us	e Actions
Openvpn_CA	<b>~</b>	self-signed	1	CN=Openvpn_CA 🚺		<i>₽</i> ₩₽C```
				Valid From: Tue, 15 Apr 2025 07:10:05 +0000 Valid Until: Fri 13 Apr 2035 07:10:05 +0000		

Rentrer les mêmes paramètres et cliquer sur Save.

Create / Edit CA	
Descriptive name	Openvpn_CA The name of this entry as displayed in the GIII for reference. This name can contain spaces but it cannot contain any of the following characters: $2, >, <, & /, \backslash_{*}^{*}$ .
Method	Create an internal Certificate Authority
Trust Store	Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Internal Certificate A	uthority
Key type	RSA
	1024         The length to use when generating a new RSA key, in bits.         The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256  The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)	
Common Name	Openvpn_CA
	The following certificate authority subject components are optional and may be left blank.
Country Code	None
State or Province	e.g. Texas
City	e.g. Austin
Organization	e.g. My Company Inc
Organizational Unit	e.g. My Department Name (optional)
	Save

Aller ensuite dans Certificates puis cliquer sur Add/Sign pour ajouter un certificat.

System / Certificat	tes / Certificate	S		G
Authoritus Certificates	e Ortificate Revoca	tion		
Search				e
Search term		Both	V Q Search	Clear
	Enter a search string o	*nix regular expression to search certificate names and distinguished n	ames.	
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67d58186ab106) Server Certificate CA: <b>No</b> Server: <b>Yes</b>	self-signed	0=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 67d58186ab106 Valid From: Sat, 15 Mar 2025 13:32:54 +0000 Valid Until: Fri, 17 Apr 2026 13:32:54 +0000	webConfigurator	<b>∕*₽</b> ∎C'
Cert Server Certificate CA: <b>No</b> Server: <b>Yes</b>	self-signed	CN=Cert  Valid From: Sat, 15 Mar 2025 14:06:10 +0000 Valid Until: Fri, 17 Apr 2026 14:06:10 +0000		<b>∥*₽</b> ∎C```
OpenVPN_Server Server Certificate CA: <b>No</b> Server: <b>Yes</b>	external	CN=OpenVPN_Server Valid From: Mon, 17 Mar 2025 07:56:59 +0000 Valid Until: Thu, 15 Mar 2035 07:56:59 +0000		<b>/*₽</b> ≡ڨ
test User Certificate CA: <b>No</b> Server: <b>No</b>	external	CN=Internal-CA 0 Valid From: Thu, 20 Mar 2025 10:21:12 +0000 Valid Until: Sun, 18 Mar 2035 10:21:12 +0000	User Cert	/* <b>/</b> =
Dpenvpn_Cert Server Certificate CA: <b>No</b> Server: <b>Yes</b>	Openvpn_CA	CN=Openvpn_Cert Valid From: Tue, 15 Apr 2025 07:14:19 +0000 Valid Until: Wed, 15 Apr 2026 07:14:19 +0000	OpenVPN Server	<b>∕*₽</b> ≣Ċ

Rentrer ensuite ces paramètres.

Dans Certificate Authorities, sélectionner l'autorité de certificat créée avant (OpenVPN\_CA).

tern/ ceruiic	ates/ ceruncates/ con		U.
orties Certificati	es Cartificate Revocation		
/Sign a New Cert	ificate		
Method	Greate an internal Certificate	*	
Descriptive name	Openingst, Cert The name of this entry as displayed in the GDI for reference. This name can contain space but it cannot contain any of the f	illusing characters 2.5.5.6.7.121	
ernal Certificate			
Certificate authority	Openspo, GA		
Keytype	ASA		
	2048	*	
	The length to use when generating a new RSA key, in bits. The Key Length should nut be lower than 2048 or some platform	a may consider the certificate invalid.	
Digest Algorithm	(sha258	*	
	The digest method used when the certificate is signed. The later practice is to use SHA255 or higher. Some services an algorithms invalid.	I platforms, such as the GUI web server and O	ser/VPN, sonsider washer digest
Lifetime (days)	3650		
	The length of time the signed certificate will be valid, in days. Server certificates should not have a Meterie over 398 days or a	ma platforms may consider the cartificate inv	det.
Common Name	(a.g. monotompletum		
real Cartificate			
Settles to actually			
Certificate administry	openipo_Ca		
Key type	RSA	*	
	2548	(e)	
	The larights use when generating a new RSA key, in bit The Kay Length should not be lower than 2048 or some	t platforms may consider the certificate in-	ble
Digest Algorithm	sha256	<i></i>	
	The digest risthed used when the certificate is argoed. The least practice is to use \$HA256 or higher. Some set algorithms invalid	ices and platforms, such as the QUI web	accor and Oper/PNL consider weaker digest
Lifetime (days)	345	1	
	The length of time the sogned certificate will be valid, in Server certificates should not have a lifetime over 200 d	lays. ays or some platforms may consider the i	arth Smald
Common Name	a gravina example ports		×0
	The following certificate subject components are option	al and may be left blank.	
Country Code	None	*	
State or Province	+# Texes		
City	(e.g. Jump)		
Organization	ang My Company Inc.		
Organizational Unit	(e.g. My Department Name (optional)		

Veiller à bien choisir Server Certificate et cliquer sur Save.

Attribute Notes	The fullpointy attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the aelected mode.				
	For internal Cartificates these attributes are added decetly to the pertificate as shown.				
Cartificata Type	Server Certificate				
	procing usage restrictions on, or granting abilities to, the agreed certificate.				
Alternative Names	FQDN or Hostname *				
	Type Volue				
	Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. To signing CA may sprote or change these values.				
Add SAN Row	+ AddSAN Have and T				
	+ Ald SW Roe				

Aller ensuite dans System puis User Manager.

Nicolas ERNST

•	of pfSense.he	ome.arpa - System:	Ce X	+					
←	$\rightarrow$ G	8 Non sécurisé	https:/	/192.168.50.	1/system_cert	tmanager.	php?act=e	dit&id=67fe074	lb8e4
		System - Inte	erfaces +	Firewall -	Services +	VPN <del>-</del>	Status 🗸	Diagnostics 🗸	He
	System /	Advanced Certificates General Setup	ertifi	cates					
	Authorities	High Availability Package Manager	ficate F	levocation					
	Edit an Exis	Register Routing Setup Wizard	isting	certificate			~		
	Descrip	Update User Manager Logout (admin) Subject CN=Opd	Cert If the calculation envpn_Cert	ntry as displayed	in the GUI for ref t cannot contain	erence. any of the fol	lowing charact	ers: ?, >, <, &, /,  ", "	
	Edit Certific	ate							
	Certifi	cate Type 🔹 🗴	.509 (PEM)	)				OPKCS #12 (PFX)	
	Certif	cate data	BEGIN CER	TIFICATE					

Aller dans Authentification Servers et cliquer sur Add.
System / User Manager / Authentication Servers			8	
Users Groups Setting	s Authentication Servers			
Authentication Servers	Type	Host Name	Actions	
Active Directory	LDAP	192.168.50.3		
Local Database		pfSense		

Entrer ces paramètres.

System / User Ma	anager / Authentication Servers / Edit	≣ 0
Users Groups S	Settings Authentication Servers	
Server Settings		
Descriptive name	Active Directory	
Туре	LDAP	
LDAP Server Settings	Adresse IP du Serveur Windows	,
lostname or IP address	192.168.50.3 NOTE: Uffice weing SSL/TLS or STATTTLS deite to the control of a Subject Alternative Name (SAN) or the Common Name (CN) of the LDA server SSL/TLS Certificate.	ĄΡ
Port value	389	
Transport	Standard TCP 🗸	
er Certificate Authority	Openvpn_CA	tch the
Protocol version	3	
Server Timeout	25 Timeout for LDAP operations (seconds)	
Search scope	Level Centire Subtree	
	Base UN DC=securitecivile,DC=local	
uthentication containers	OU=Utilisateurs,DC=securitecivile,DC=local  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.	

Une fois les paramètres rentrés, cliquer sur Save.

Extended query	Enable extended query		
Bind anonymous	Use anonymous binds to resolve distinguished names		
Bind credentials	CN=Administrateur,CN=Users,DC=securitecivile,DC=local	[	
User naming attribute	samAccountName		
Group naming attribute	Cn	Mot de passe de	
Group member attribute	memberOf	l'Administrateur du	
RFC 2307 Groups	<ul> <li>LDAP Server uses RFC 2307 style group membership</li> <li>RFC 2307 style group membership has members listed on the group object</li> <li>Directory style group membership (RFC 2307bis).</li> </ul>	domaine rather than using groups listed on user object. Leave unchecked for Active	
Group Object Class	posixGroup Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".		
Shell Authentication Group DN	If LDAP server is used for shell authentication, user must be a member of th Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com	is group and have a valid posixAccount attributes to be able to login.	
UTF8 Encode	UTF8 encode LDAP parameters before sending them to the server. Required to support international characters, but may not be supported by encoded and the support of the	very LDAP server.	
Username Alterations	<ul> <li>Do not strip away parts of the username after the @ symbol</li> <li>e.g. user@host becomes user when unchecked.</li> </ul>		
Allow unauthenticated bind	Allow unauthenticated bind Unauthenticated binds are bind with an existing login but with an empty pas any possibility to disable it.	sword. Some LDAP servers (Microsoft AD) allow this type of bind without	
	Save		

Pour tester si la connexion d'un utilisateur du domaine au PfSense fonctionne, aller dans Diagnostics puis Authentification.

Nicolas ERNST



Sélectionner le serveur Active Directory, rentrer les identifiants d'un utilisateur du domaine et cliquer sur Test.

Diagnostics / Aut	hentication $\Xi$ $\Theta$
Authentication Test	
Authentication Server	Active Directory  Select the authentication server to test against.
Username	arthur.fix
Password	[······
Debug	<ul> <li>Set debug flag</li> <li>Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).</li> </ul>
	✓ Test

Si ce message s'affiche, alors la configuration est correcte.

agnostics / Au	hentication 후
er arthur.fix authenticate	d successfully. This user is a member of groups:
uthentication Test	
Authentication Server	Active Directory
	Select the authentication server to test against.
Username	arthur.fix
Password	
Debug	Set debug flag

Aller dans VPN puis OpenVPN.



Dans la section Servers, cliquer sur Add.

Servers tlients	Client Specific Over	rides Wizards	Client Export		
OpenVPN Servers	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
192.168.1.140 (CARP WAN1)	TCP4 / 11940 (TUN)	10.10.30.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256- CBC Digest: SHA256 D-H Params: 2048 bits	Corp_VPN	#D1

Voici la configuration à rentrer.

VPN / OpenVPN	/ Servers / Edit	С⊚ 幸 ш 🗏 🕄
Servers Clients	Client Specific Overrides Wizards Client Export	
General Information		
Description	Corp_VPN	
	A description of this VPN for administrative reference.	
Disabled	<ul> <li>Disable this server</li> </ul>	
	Set this option to disable this server without removing it from the list.	
Unique VPN ID	Server 1 (ovpns1)	
Mode Configuration		
Server mode	Remote Access ( User Auth )	
Backend for authentication	Active Directory Active Directory	
Device mode	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common an "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	d compatible mode across all platforms.
Endpoint Configurati	on	
Protocol	TCP on IPv4 only	
Interface	192.168.1.140 (CARP WAN1)	nections.
Local port	11940 The port used by OpenVPN to receive client connections.	

## Nicolas ERNST

Cryptographic Settin	gs
TLS Configuration	Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
<u>TLS Key</u>	#       2048 bit OpenVPN static key         #       2048 bit OpenVPN static key         #
TLS Key Usage Mode	TLS Authentication   In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction	Use default direction The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority	Openvpn_CA 🗸
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	Check client certificates with OCSP
Server certificate	Openvpn_Cert (Server: Yes, CA: Openvpn_CA, In Use)
DH Parameter Length	2048 bit  V Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve	Use Default  Use Default  The Elliptic Curve to use for key exchange.  The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-129-CFB (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block)

## Nicolas ERNST

Fallback Data Encryption	AES-256-CBC (256 bit key, 128 bit block)
	The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm	SHA256 (256-bit)
	The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto	No Hardware Crypto Acceleration
Certificate Depth	One (Client+Server)
	When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Client Certificate Key	Enforce key usage
Usage Validation	Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings	
IPv4 Tunnel Network	10.10.30.0/24
	This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts
	expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
	with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network	
	This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts
	expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.50.254/24
	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network
	type aliases. This may be left blank it not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)	
	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type
	aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections	100

## Nicolas ERNST

Allow Compression	Decomprose incoming do not comprose suitaging (Asymptotic)
Allow Compression	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.
Compression	Adaptive LZO Compression [Legacy style, comp-Izo adaptive]
	Deprecated. Compress tunnel packets using the LZO algorithm. Compression can potentially dangerous and insecure. See the note on the Allow Compression option above.
	Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
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	Allow multiple concurrent connections from the same user
	When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.
	Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings	
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet
	Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
Ping settings	
Inactive	300
induite	Causes OnenVDN to close a client connection after n seconds of inactivity on the TLIN/TAP device
	Activity is based on the last incoming or outgoing tunnel packet.
	A value of 0 disables this feature.
	This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a drank of /SU tunner network as it will cause the server to exit and not restart.
Ping method	keepalive – Use keepalive helper to define ping configuration
	keepalive helper uses interval and timeout parameters to define size and size restart values as follows: ninn = interval Explorateur de fichiers

Interval	10
Timeout	60
Advanced Client Sett	ings
DNS Default Domain	Provide a default domain name to clients
DNS Default Domain	securitecivile.local
DNS Server enable	Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.50.3
DNS Server 2	
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	Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	Provide an NTP server list to clients
NetBIOS enable	Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Node Type	none  Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast)
Scope ID	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID
WINS server enable	Provide a WINS server list to clients

Une fois la configuration terminée, cliquer sur Save.

Advanced Configurat	bn
Custom options	Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"
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 purposes such as determining Client Specific Overrides.
Send/Receive Buffer	Default Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.
Gateway creation	O Both     IPv4 only     O IPv6 only       If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.
Verbosity level	default          Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.         None: Only fatal errors         Default through 4: Normal usage range         5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.         6-11: Debug info range
	B Save

Il faut maintenant créer des règles afin que les clients à distance puissent se connecter via OpenVPN.

•	of pfSen	se.home.arpa	- VPN: Oper 🗙	+			
÷	$\rightarrow$ C	8 Non	sécurisé <del>http</del>	<del>)s</del> ://192.168.50.1	/vpn_open	vpn_server	.php?ac
c		System	- Interfaces	+ Firewall +	Services -	VPN +	Status
	VPN /	OpenVPN	/ Servers /	Aliases EC NAT			
	Servers	Clients	Client Specific O	verrid Schedules Traffic Shape	ient E er	xport	
	General	Information	1	Virtual IPs			
		Description	Corp_VPN A description o	f this VPN for admini	strative referen	ce.	
		Disabled	Disable this Set this option	server to disable this server	without remov	ing it from the	list.

Aller dans Firewall puis Rules.

Aller dans la section OpenVPN puis cliquer sur Add pour ajouter une nouvelle règle.

Fire	Firewall / Rules / OpenVPN											≢ 🗉 🕄
Floatir	ng	WAN1	LAN	WAN2	DMZ	OpenVPN	$\mathbf{>}$					
Rules	s (Dra	ag to Ch	nange Orde	er)								
0	5	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	/	0/0 B	IPv4*	*	*	*	*	*	none		Openvpn_Traffic	҈∜ <b>₽</b> ⊘ <b>ё</b> х
								$\rightarrow$	Add	l Add 🛅	Delete 🚫 Toggle	Copy 🕞 Save 🕂 Separator

Sélectionner Pass pour Action, IPv4 pour la famille d'adresse, et Any pour Protocol.

Firewall / Rules /	Edit				⊉ 💷 🗃 😧				
Edit Firewall Rule									
Action	Pass Choose what to do with packet Hint: the difference between b whereas with block the packet	ets that match the criteria specified below. Nock and reject is that with reject, a packet t is dropped silently. In either case, the orig	(TCP RST or ICMP inal packet is disca	port unreachable for UDP) is retur rded.	ned to the sender,				
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable this</li> </ul>	rule without removing it from the list.							
Interface	OpenVPN V Choose the interface from which packets must come to match this rule.								
Address Family	Select the Internet Protocol version this rule applies to.								
Protocol	Any Choose which IP protocol this rule should match.								
Source									
Source	Invert match	any	~	Source Address	/ 🗸				
Destination									
Destination	Invert match	any	~	Destination Address	/ 🗸				
Extra Options									
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).								
Description	Openvpn_Traffic A description may be entered log.	here for administrative reference. A maxim	) num of 52 character	s will be used in the ruleset and di	isplayed in the firewall				
Advanced Options	Display Advanced								

Ajouter une description à la règle et cliquer sur Save.

Extra Options	
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Openvpn_Traffic Accepted to the second of th
Advanced Options	Complex Advanced
Rule Information	
Tracking ID	1744702773
Created	4/15/25 07:39:33 by admin@192.168.50.3 (Local Database)
Updated	4/15/25 07:39:33 by admin@192.168.50.3 (Local Database)
	B Save

Cliquer sur Apply Changes.

Nicolas ERNST

Fir	ewa	ll / Rul	es / Ope	nVPN					<b>幸</b> ₩ 🗏 🕄			
The The	firewa chang	ll rule confi es must be	guration has applied for the	been change hem to take e	d. effect.							Apply Changes
Floa	ating	WAN1	LAN	WAN2	DMZ	OpenVPN	_					
Rul	es (D	rag to C	hange Ord	er)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/0 B	IPv4*	*	*	*	*	*	none		Openvpn_Traffic	҈∜⊈⊘ <b>а́×</b>
									1 Add	l Add	Delete 🚫 Toggle	🖸 Copy 🕞 Save 🕂 Separator

Aller ensuite sur l'interface WAN principale (WAN1) toujours dans les Rules. Cliquer sur Add pour ajouter une nouvelle règle.

Fi	rew	all / Ru	iles / W	AN1			幸風間					
Flo	ating	WAN		WAN2 DMZ	Ope	nVPN						
Ru	les	(Drag to	Change O	rder)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	0/672 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	\$
	×	0/4 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	٥
	~	0/0 B	IPv4 TCP	*	*	This Firewall	11940	*	none		Autoriser OpenVPN	℀ℛℿѺ面×
							->	Ad	d 🕽 A	dd <u> </u> Dele	ete 🛇 Toggle 🔲 Copy	Save + Separat

Choisir Pass en Action, IPv4 pour la famille d'adresse, TCP pour Protocol, et plus bas dans la section Destination, choisir le port 11940 pour le port de destination (celui que l'on a configuré et choisi avant dans la configuration de OpenVPN).

Firewall / Rules /	Edit				<b>≢ ⊡ ≡ 0</b>			
Edit Firewall Rule								
Action	Pass Choose what to do with pack Hint: the difference between whereas with block the pack	kets that match the criteria spec block and reject is that with rej et is dropped silently. In either o	v ified below. ect, a packet (TCP RST or ICM ase, the original packet is disc	<sup>9</sup> port unreachable for UDP) is return arded.	ied to the sender,			
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable this</li> </ul>	s rule without removing it from :	the list.					
Interface	WAN1 Choose the interface from w	hich packets must come to ma	► tch this rule.					
Address Family	Pv4 Select the Internet Protocol version this rule applies to.							
Protocol	CP Choose which IP protocol thi	is rule should match.	~					
Source								
Source	Invert match	any	~	Source Address	/ ~			
	Display Advanced The Source Port Range for a its default value, any.	connection is typically random	and almost never equal to the	destination port. In most cases this	setting must remain at			
Destination								
Destination	Invert match	This firewall (self)	~	Destination Address	/ 🗸			
etestination Port Range	(other) 🗸	11940	(other)	11940				
	Specify the destination port	or port range for this rule. The "	To" field may be left empty if o	ly filtering a single port.				
Extra Options								
Log	Log packets that are hand     Hint: the firewall has limited	dled by this rule local log space. Don't turn on lo	gging for everything. If doing a	lot of logging, consider using a rem	ote syslog server (see			

Ajouter une description et cliquer sur Save.

Extra Options	
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description (	Autoriser OpenVPN A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Display Advanced
Rule Information	
Tracking ID	1742198848
Created	3/17/25 08:07:28 by admin@192.168.50.10 (Local Database)
Updated	4/15/25 07:40:46 by admin@192.168.50.3 (Local Database)
	B Save

Cliquer sur Apply Changes.

Nicolas ERNST

Fir	ewa	ll / Rul	es / Ope	nVPN					幸 📖 🗐 😧			
The The	firewa chang	ll rule conf es must be	iguration has e applied for tl	been change nem to take e	d. effect.							✓ Apply Changes
Floi	ating	WAN1	LAN	WAN2	DMZ	OpenVPN	_					
Rul	es (D	rag to C	hange Ord	er)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	<b>~</b>	0/0 B	IPv4 *	*	*	*	*	*	none		Openvpn_Traffic	҈ѽ <i>҈</i> ∕⊡Ѻ <u></u> а́х
									1 Add	l Add	Delete 🚫 Toggle	🖸 Copy 🖪 Save 🕇 Separator

Retourner ensuite dans OpenVPN depuis la section VPN.



Aller sur Client Export.

OpenVPN / Clien	t Export Utility 📀						
Server Client Cl	lient Specific Overrides Wizards Client Export						
OpenVPN Server							
Remote Access Server	Corp_VPN TCP4:11940						
Client Connection Be	havior						
Host Name Resolution	Interface IP Address						
Verify Server CN	Automatic - Use verify-x509-name where possible						
Block Outside DNS	Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.						
Legacy Client	Do not include OpenVPN 2.5 and later settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.						
Silent Installer	Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.						
Bind Mode	Do not bind to the local port  If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.						

Il n'y a aucun paramètre à changer, aller tout en bas et sélectionner Most Clients pour installer le fichier de configuration de OpenVPN.

OpenVPN Clients		
User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul> <li>Inline Configurations:</li> <li>Most Cirents ▲ Android</li> <li>Bound Cirents ▲ Android</li> <li>Current Windows Installer (2.6.7-Ix001):</li> <li>▲ Achive ▲ 32-bit</li> <li>Previous Windows Installer (2.5.9-Ix601):</li> <li>▲ 4-bit ▲ 32-bit</li> <li>Legacy Windows Installers (2.4.12-Ix601):</li> <li>▲ 10/2016/2019 ▲ 7/8/8.1/2012/2</li> <li>Viscosity Bundle</li> <li>Viscosity Bundle</li> <li>Viscosity Inline Config</li> </ul>

Il faut maintenant installer le client OpenVPN Connect pour tester si OpenVPN fonctionne (le client sera aussi à installer et à configurer sur les postes clients).

Sur le navigateur de recherche, rechercher openvpn connect et cliquer sur le premier lien.

👻 📝 pfSense.home.arpa - OpenVPN: 🗙 🔓 openvpn connect - Recherche 🤄 🗙	+	
← → C 😋 google.com/search?q=openvpn+connect&oq=open&gs	_lcrp=EgZjaHJvbWUqBggCEEUYOzIGCAAQ	RRg5M
Google openvpn connect	× ए छ ९ 🕸	000 000 000
Tous Vidéos Images Actualités Vidéos courtes Web Livres	: Plus	(
OpenVPN https://openvpn.net > client · Traduire cette page		
OpenVPN Connect - VPN For Your Operating System		
Connect to Access Server, CloudConnexa or any OpenVPN protocol-compate Superior Authentication Supports 2FA and SAML authentication.	ible server or service.	

Cliquer sur le bouton d'installation.



Une fois l'installation terminée, ouvrir l'installer et suivre les étapes d'installation.

## Historique des téléchargements récents $\times$



openvpn-connect-3.6.0.4074\_signed (1).msi + 51,6/98,2 Mo • 12 secondes restantes

Historique complet des téléchargements

Ouvrir OpenVPN Connect.

OpenVPN Connect - ×				
Import Profile				
URL	UPLOAD FILE			
<b>Drag and drop</b> You can import	OVPN to upload *.OVPN profile only one profile at a time.			
	BROWSE			

Sélectionner le fichier de configuration de OpenVPN installé avant (se trouve sur mon bureau) et le glisser dans la zone d'upload de fichier de configuration sur OpenVPN Connect.



Entrer les paramètres suivants. Choisir 192.168.1.140 pour Server Hostname et utiliser les identifiants d'un utilisateur de l'AD pour se connecter.

A la fin de la configuration, cliquer sur Save en haut à droite.

OpenVPN Connect	- ×
<b>K</b> Edit Profile	Save
Profile Name Corp_VPN	
Server Hostname (locked) 192.168.1.140	_
Server Override (optional)	_
Username arthur.fix	
Save password	
Password	
Profile ID Unique identifier of this profile 1745067626075	

Cliquer ensuite sur le bouton de connexion.



Le VPN fonctionne.

OpenVPN Connect ->			- ×	
	Pr	10		
CONNECTED				
	OpenVPN P Corp_VPN	rofile		
CONNEC	TION STATS			
3.1KB/s				
0B/s				
BYTES IN 483 B/S	↓	18 BY	TES OUT 0 B/S	
DURATION 00:00:08	4 8	PACKET RECEIVE 4 sec ago	ED	
YOU				
arthur.fix	K			

Documentation d'exploitation, L'utilisation et la gestion du Lot 1

# Microsoft **Active Directory** PRTG NETWORK MONITOR

# Introduction :

L'administration des réseaux informatiques repose sur des services essentiels qui assurent une gestion centralisée des utilisateurs, des ressources et des communications. Parmi ces services, Active Directory, DNS et DHCP jouent un rôle crucial. Active Directory permet de centraliser la gestion des comptes utilisateurs et des permissions, DNS assure la résolution des noms de domaine, tandis que DHCP automatise l'attribution des adresses IP dans le réseau. Ce document vous guidera à travers les étapes d'installation et d'utilisation de ces trois services fondamentaux, en mettant l'accent sur les bonnes pratiques pour garantir un fonctionnement optimal.
Nicolas ERNST

## Installation des rôles

Lorsque vous allumez votre Windows Serveur cliquait sur Ajouter des rôles et des fonctionnalités.

🚡 Gestionnaire de serveur			– Ø ×
Gestionnai	ire de serveur	• Tableau de bord 🛛 🛛 🐨 🕼 🚩 Gérer Out	ils Afficher Aide
🔛 Tableau de bord	BIENVENUE DANS G	ESTIONNAIRE DE SERVEUR	^
Serveur local			
Tous les serveurs		1 Configurer ce serveur local	
Services de fichiers et d ▷	DÉMARRAGE RAPIDE		
		2 Ajouter des rôles et des fonctionnalités	
		3 Ajouter d'autres serveurs à gérer	
	NOUVEAUTÉS	4 Créer un groupe de serveurs	
		5 Connecter ce serveur aux services cloud	
	EN SAVOIR DUUS		Masquer
	EN SAVOIR PEUS		
	Pôlos et groupes de		

Cliquer deux fois sur suivant puis quand vous arrivez dans sélection du serveur sélectionnez votre serveur Windows.

Assistant Ajout de rôles et de	fonctionnalités		- 0
électionner le s	erveur de destina	tion	SERVEUR DE DESTINATION WIN-6AMP6JOI65N.CDI.college
Avant de commencer Type d'installation	Sélectionnez le serveur ou l	e disque dur virtu du pool de server	el sur lequel installer des rôles et des fonctionnalités.
Sélection du serveur	<ul> <li>Sélectionner un disque</li> </ul>	dur virtuel	
Rôles de serveurs	Pool de serveurs		
Fonctionnalités Confirmation	Filtre :		
	Nom	Adresse IP	Système d'exploitation

Dans rôles de serveurs sélectionnez les rôles Services AD DS et Serveur DHCP.

Type d'installation	Rôles
Sélection du serveur	Accès à distance
Rôles de serveurs	Attestation d'intégrité de l'appareil
Fonctionnalités	Contrôleur de réseau
Confirmation	Serveur de télécopie
Résultats	Serveur DHCP     Serveur DNS     Serveur Web (IIS)     Service Guardian hôte     Services AD DS     Services AD LDS Active Directory Lightweight Dire     Services AD RMS (Active Directory Rights Manager     Services Bureau à distance

## Cliquez sur suivant.

électionner des	fonctionnalités	WIN-6AMP6JOI6SN.CDI.colleg
Avant de commencer Type d'installation	Sélectionnez une ou plusieurs fonctionnalités à installer sur le s	serveur sélectionné. Description
Sélection du serveur Rôles de serveurs	Image: International Action of the second sec	.NET Framework 4.8 provides a comprehensive and consistent
Fonctionnalités	Assistance à distance Base de données interne Windows	programming model for quickly an easily building and running
AD DS Confirmation	BranchCache Chiffrement de lecteur BitLocker Client d'impression Internet	platforms including desktop PCs, Servers, smart phones and the pub and private cloud
	Client pour NFS	
	Cullection des événements de configuration et de Collection des événements de configuration et de Compression différentielle à distance Conteneurs Data Center Bridging	
	Déverrouillage réseau BitLocker     DirectPlay     Enhanced Storage     Équilibrage de la charge réseau	

## Cliquez sur suivant.

Services de dom				
Avant de commencer	Les services de domaine Active Directory (AD DS) stockent de ordinateurs et les périphériques sur le réseau. Les services AD	SERVEUR DE WIN-GAMPGIOG s informations sur les utilisat DS permettent aux administ	eurs, les	ION lege
Sélection du serveur	gerer ces informations de façon securisee et facilitent le parta les utilisateurs.	ge des ressources et la collai	boration	entre
Rôles de serveurs Fonctionnalités	A noter :     Pour veiller à ce que les utilisateurs puissent quand même s     de serveur installez un minimum de deux contrôleurs de de	se connecter au réseau en ca omaine par domaine.	s de pani	ne
AD DS Confirmation Résultats	<ul> <li>Les services AD DS nécessitent qu'un serveur DNS soit insta n'est installé, vous serez invité à installer le rôle de serveur l</li> </ul>	sllé sur le réseau. Si aucun se DNS sur cet ordinateur.	rveur DN	S
	Azure Active Directory, un service en ligne distir des identités et des accès, des rapports de sécu applications web dans le cloud et sur site.	nct, peut fournir une gestion rrité et une authentification u	simplifié inique au	e IX
	En savoir plus sur Azure Active Directory Configurer Office 365 avec Azure Active Directo	bry Connect		
	< Précédent Suive	nt > Installer	Annu	ler <sup>e</sup> W

Cliquez sur installer.

onfirmer les sé	lections d'installation	SERVEUR DE D	ESTINATION
Avant de commencer Type d'Installation Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats	Pour installer les rôles, services de rôle ou fonctionnalités suivar Installer. Redémarrer automatiquement le serveur de destination, si Il se peut que des fonctionnalités facultatives (comme des outil cette page, car elles ont été sélectionnées automatiquement. Si fonctionnalités facultatives, cliquez sur Précédent pour désactiv Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS Centre d'administration Active Directory Composants logiciels enfichables et outils e Services AD DS	nts sur le serveur sélectionné, nécessaire s d'administration) soient affi i vous ne voulez pas installer rer leurs cases à cocher. en ligne de commande AD DS	cliquez su chées sur ces
	Exporter les paramètres de configuration Spécifier un autre chemin d'accès source		

Attendez que l'installation se termine puis fermez la fenêtre lorsque c'est fini.

Assistant Ajout de rôles et de	onctionnalités	>
Progression de l'	installation	SERVEUR DE DESTINATION WIN-6AMP6JOI6SN.CDI.college
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats	Afficher la progression de l'installation  Démarrage de l'installation  Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS Outils AD DS Centre d'administration Active Directory	
	Composants logiciels enfichables et outils Services AD DS	en ligne de commande AD DS
	Vous pouvez fermer cet Assistant sans interrompre les tâc leur progression ou rouvrez cette page en cliquant sur No commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration	hes en cours d'exécution. Examinez otifications dans la barre de
	< Précédent Suivant	Installer

Pour installer des rôles sur un autre serveur (en l'occurrence le serveur secondaire en version core ici), cliquez sur "ajouter d'autres serveurs à gérer".

🕘 - 🛛 • • Tableau	ı de bord	🕶 🥑   🧗 <u>G</u> érer Outils Afficher <u>A</u> id
ableau de bord	BIENVENUE DANS GE	ESTIONNAIRE DE SERVEUR
ous les serveurs ervices de fichiers et d Þ	DÉMARRAGE	1 Configurer ce serveur local
	MARINE .	2 Ajouter des rôles et des fonctionnalités
	NQUVEAUTÉS	4 Créer un groupe de serveurs
	EN SAVOIR P <u>L</u> US	Masquer

Recherchez ensuite le nom exact du serveur secondaire que vous voulez joindre et gérer à partir de votre serveur principal.

Nicolas ERNST

r	🚡 Ajouter des serveurs		- 🗆 X	
r	Active Directory DNS Importer	_	Sélectionné	
r	Emplacement : 👔 ccicampus 🕨 🕝		Ordinateur	
	Système d'exploitation : Tous 🗸			
1	Nom (CN) : Nom ou début du nom			
d	Rechercher maintenant			
	Nom Système d'exploitation	1		
		•		
J				
				2
3				
	0 ordinatour(c) trouvé(c)		0 ordinatour(s) sólostionnó(s)	
	Aide		OK Annuler	

## Installation de l'Active Directory et DNS

Cliquez sur le drapeau en haut.

• 🗇 I	ľ,	Gérer	Outils
	Notifi	cations	

# ur local

#### 

Cliquez sur promouvoir ce serveur en contrôleur de domaine.

4	Configuration post-déploie TÂCH	× X
	Configuration requise pour : Services AD D WIN-6AMP6JOI6SN	)S à
	Promouvoir ce serveur en contrôleur de de	omaine
6	Installation de fonctionnalité	

Sélectionnez Ajouter une nouvelle forêt puis entrez le nom de votre nouvelle forêt.

RIENVENILE DANS	GESTIONNAIRE DE SERVEUR			
Assistant Configuration des serv	vices de domaine Active Directory	-		×
Assistant Configuration des serv Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Verification de la configur Installation Résultats	rices de domaine Active Directory	SI WIN-6AMP6JOI65	CRVEUR C	X IBLE lege
	En savoir olus sur las configurations de déploiement			

Mettez un mot de passe pour permettre de se connecter sur d'autres postes.

Assistant Configuration des serv	rices de domaine Active Directory			-		×
Options du contrá	ôleur de domaine		WIN-6AMP6J	SE OI6SI	RVEUR ( N.CDI.co	CIBLE
Configuration de déploie	Sélectionner le niveau fonctionnel de	la nouvelle forêt et du dom	aine racine			
Claring DNS	Niveau fonctionnel de la forêt :	Windows Server 2016	~			
	Niveau fonctionnel du domaine :	Windows Server 2016	٣			
	Specifier les fonctionnalites de contro	bieur de domaine				
	Catalogue global (GC)	em)				
	Contrôleur de domaine en lectur	e seule (RODC)				
	Taper le mot de passe du mode de re	stauration des services d'an	nuaire (DSRM)			
	Mat da parra :					
	mot de passe :					
	Confirmer le mot de passe :					
		N				
		43				

Cliquez sur suivant.

Nicolas ERNST

ptions DNS	WIN-6AMP6JOI6SN.CDL.c	olle
Il est impossible de créer un	e délégation pour ce serveur DNS car la zone parente faisant autorité est intro Afficher plus	,
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Spécifier les options de délégation DNS	
	En savoir plus sur la délégation DNS	

Attendez que Windows vous génère un nom de domaine.

Assistant Configuration des serv	ices de domaine Active Directory	-		×
Options suppléme	entaires	WIN-6AMP6JOI	SERVEUR 6SN.CDI.co	CIBLE
Configuration de déploie Options du contrôleur de Options DNS	Vérifiez le nom NetBIOS attribué au domaine et modifi Le nom de domaine NetBIOS :	ez-le si nécessaire.		
Options supplémentaires				

Cliquez sur suivant.

Assistant Configuration des sen	vices de domaine Active Directory		-		×
Chemins d'accès			SI WIN-6AMP6JOI6S	ERVEUR	CIBLE
Configuration de déploie Options du contrôleur de	Spécifier l'emplacement de la base o	le données AD DS, des fichiers	journaux et de SYS	SVOL	_
Options DNS	Dossier de la base de données :	C:\Windows\NTDS			+=+
Options supplémentaires	Dossier des fichiers journaux :	C:\Windows\NTDS			
Chemins d'accès	Dossier SYSVOL :	C:\Windows\SYSVOL			***
	En savoir plus sur les chemins d'acce	s Active Directory			
		Précédent Suivant >	Activat	e Win	do ler

Cliquez sur suivant.

Examiner les optio	ons	SE WIN-6AMP6JOI6S	N.CDI.co	ciel
Configuration de déploie	Vérifiez vos sélections :			
Options du contrôleur de Options DNS	Configurez ce serveur en tant que premier contrôleur de domair nouvelle forêt.	ne Active Directory d'i	une	^
Options supplémentaires	Le nouveau nom de domaine est « mogacademy.ca ». C'est auss	i le nom de la nouvel	le forêt.	
Chemins d'accès	Nom NetBIOS du domaine : MOGACADEMY			
Examiner les options	Niveau fonctionnel de la forêt : Windows Server 2016			
Vérification de la configur	Niveau fonctionnel du domaine : Windows Server 2016			
Installation				
	Options supplementaires :			
	Catalogue global : Oui	т		
	Serveur DNS : Oui			
				~
	Ces paramètres peuvent être exportés vers un script Windows Po automatiser des installations supplémentaires	owerShell pour	her le sc	ript
	En savoir plus sur les options d'installation			
		Activate	e Win	ide

Puis cliquez sur suivant et Installer.

		SE	RVEUR	CIBLE
Examiner les oplic	STIS .	WIN-6AMP6JOI6S	N.CDI.co	llege
Configuration de déploie	Vérifiez vos sélections :			
Options du contrôleur de Options DNS	Configurez ce serveur en tant que premier contrôleur de doma nouvelle forêt.	sine Active Directory d'	une	^
Options supplémentaires	Le nouveau nom de domaine est « mogacademy.ca ». C'est au	ssi le nom de la nouvel	le forêt.	
Chemins d'accès	Nom NetBIOS du domaine : MOGACADEMY			
Examiner les options	Niveau fonctionnel de la forêt : Windows Server 2016			
Vérification de la configur	Minere fractional de dessina Windows Caras 2016			
Installation	Niveau tonctionnel du domaine : windows server 2016			
	Options supplémentaires :			
	Catalogue global : Oui	*		
	Serveur DNS : Oui	1		
				$\sim$
	Ces paramètres peuvent être exportés vers un script Windows l automatiser des installations supplémentaires	PowerShell pour	her le sc	ript
	En savoir plus sur les options d'installation			
		Activate	e Win	urter

Attendez que ça s'installe puis fermer la fenêtre et redémarrez votre serveur.

Ce serveur a été correctem	ent configuré en tant que contrôleur de domaine	Afficher	plus )
	Afficher les résultats détaillés de l'opération		
l'emone du constitue de .	👍 Les contrôleurs de domaine Windows Server 2022 d	offrent un paramètre de sécu	rité par
OUS allez etre ordinateur est redémarré	car les services de domaine Active Directory ont é	áté installés ou	
ipprimés.		Fermer	faisant cédez à r une

## 2. Installation PRTG

Aller sur le lien de téléchargement prtg:

https://www.paessler.com/fr/prtg

Cliquez ensuite sur "Téléchargement gratuit":

**Nicolas ERNST** 



Nos utilisateurs donnent les meilleures notes à la supervision avec Paessler PRTG

#### Laissez l'installeur PRTG se télécharger :

PAESSLER PRODUITS SOLUTIONS PRIX SERVICES RESSOURCES PARTENAIRES	
Merci d'avoir téléchargé PRTG. Presque prêt	
Le téléchargement a commencé automatiquement. Attendez que le téléchargement soit terminé. Lancez l'installation. La clé de licence ci-dessous est déjà incluse dans votre fichier .exe. Besoin d'aide pour démarrer ? Participez à nos <u>webinaires</u> gratuits.	
Nom de licence: prtgtrial Votre clé de licence 000023-MEBUALHXTLRL/-3EVR6.J-KS3NYF- 458TON-2GIUYD-E0AP6C-75DR0B-BFULM6	
Si votre téléchargement ne démarre pas automatiquement, veuillez réessayer.	

Cliquez sur l'installeur PRTG :

#### ✓ Aujourd'hui

🔿 prtg\_installer\_with\_trial\_key\_000023-MEB... 12/04/2025 18:26 Application 359 425 Ko

Choisissez votre langue en français :



Acceptez les termes puis cliquez sur Suivant.



Mettez votre adresse mail (optionnel) puis cliquez sur Suivant.

Nicolas ERNST

3			_		~
Votre adresse e-mail				- 0	
Fournissez les informations suivant	es pour poursuivre l'inst	allation			PRT
Entrez votre adresse e-mail ! Votre systèmes d'alertes importants et ur pour vous apporter notre support.	serveur PRTG enverra rgents. Paessler utilisera	à cette ad égalemen	resse di it cette	es adresse	
Votre adresse e-mail:					
Votre adresse e-mail:	sonnelles.				
Votre adresse e-mail: Nous protégeons vos données pers Consultez notre politique de confid	sonnelles. entialité pour en savoir p	<del>kus.</del>			
Votre adresse e-mail: Nous protégeons vos données pers Consultez notre politique de confide	sonnelles. entialité pour en savoir p	<del>lus.</del>			
Votre adresse e-mail: Nous protégeons vos données pers Consultez notre politique de confid	sonnelles. entialité pour en savoir p	<u>kus.</u>			

## Attendez que PRTG s'installe.

nstallation - PRTG Network Ngnitor	-	×
Installation en cours		
Veuillez patienter pendant que l'assistant installe PRTG Network Moni votre ordinateur.	tor sur	PRTG
Décompression des fichiers		
		 -
		_
www.paessler.com		 

Entrez votre adresse IP pour sur un navigateur web puis entrez vos identifiants admin (par défaut prtgadmin), puis cliquez sur Connexion.

PRTG Network N	Monitor (LABDC)	
Nom d'utilisateur	prtgadmin	
Mot de passe	prtgadmin	
	Connexion	

Entrez votre licence qui apparaissez lors du téléchargement de l'installeur PRTG puis cliquez sur Activer la licence.

prtgtrial	
Clé de licence	
000014-0R0KFM-8FFH20-U2G47P-U8BVFA-GCRUQJ-2D3JV8-QFDA3P-M	IFTJRM-RUJGM2
ÉTAPE 3 : Activer votre PRTG	
Jne connexion HTTPS au serveur d'activation Paessler (activation.paess utiliser un proxy HTTP pour la connexion.	ler.com) est nécessaire. Vous pouvez
Jtiliser un serveur proxy	
Non, utiliser une connexion directe à Internet (par défaut)	
Oul, dans notre réseau un proxy est obligatoire	
Annuler	Activer la licence
	N

Vous êtes sur la page d'accueil PRTG.

						N	uvelles entrées de	log 2 11 11	Recherche	QΦ
O Page d'accueil	Équipements	Bibliothèques	Capteurs	Alertes	Cartes	Rapports	Logs	Tickets	Configuration	
Configuration Li	icence									_
		~	État			📼 Log			G	
		Information sur la l	icence					Définir un mot	de passe sécurisé	×
		État de la licence	La version d'essai	a expiré.				Le compte d'u système de PF défaut « prtga	tilisateur de l'administrate TG utilise le mot de pass dmin ». Modifiez-le pour s	eur e par lécuriser
		Nom de licence	prtgtrial					Ceci est absol	web PRIG. ument obligatoire si vous	autorisez
		Clé de licence	000014-0R0KFM-8	FFH20-U2G47P-U8	BVFA-GCRU	3JV8-QFDA3P-MFTJI	RM-RUJGM2	l'accès à votre internet (l'exté	interface Web PRTG depu rieur de votre pare-feu) !	uis
		ID de système	SYSTEMID-IOEMC	CJO-PCIHPRO5-ID2	ZVDYKD-BB2DB7N	L-Q2G5FWAA		Modifier le m	ot de passe par défaut	
		Version sous licence	PRTG Freeware (Tr	ial Expired) (expiré	le 8/9/2019)					_
		Dernière mise à jour	2/23/2021 2:53:18	AM				Activer SSL/TI	LS pour l'interface Web Pl	rtg. 🗙
		Nombre de capteurs	100 Avez-vous be niveau !	esoin de capteurs s	supplémentaires ?	Cliquez ici pour effec	tuer la mise à	La connexion o serveur centra SSL/TLS.	de votre navigateur à ce c I PRTG n'est pas sécurisée	entral e par
				1	Modifier la clê de l	icence Actualiser I	es informations	Il est préférabl particulièreme accessible dep pare-feu).	e de passer à SSL/TLS, nt si votre interface Web I puis internet (en dehors de	PRTG est e votre
		-						Passer à SSL	/TLS	

Documentation situation professionnelle 2 131 sur 247

## 3. Gestion Active Directory

- Ouvrez "Utilisateurs et Ordinateurs Active Directory" (dsa.msc).
- Naviguez jusqu'à l'OU (Unité d'Organisation) où vous souhaitez créer l'utilisateur.

Fichier       Action       Affichage       ?         Image: Control of the second seco	Utilisateurs et ordinateurs Active I	Directory		
Image: Second	Fichier Action Affichage ?			
<ul> <li>Utilisateurs et ordinateurs Active</li> <li>Requêtes enregistrées</li> <li>Requêtes enregistrées</li> <li>Builtin</li> <li>Computers</li> <li>Computers</li> <li>Compourters</li> <li>CorregnSecurityPrincipate</li> <li>Managed Service Accout</li> <li>Users</li> </ul>	🗢 🄿 🙋 📅 📋 🗎 🖬 🗔	è 🛛 🖬 🗏 🐮 🐨 🍸 🚨 🕷	)	
Implete de sec       Industes invites du domaine         Implete de sec       Industes invites du domaine         Implete de sec       Forupe de sec         Implete de sec       Toutes les stations de tra         Implete de sec       Groupe de séc         Implete de sec       Toutes les stations de tra         Implete de sec       Groupe de séc         Implete de sec       Les membres de ce grou         Implete de sec       Groupe de séc         Implete de sec       Les membres de ce grou         Implete de sec       Groupe de séc         Implete de sec       Les serveurs de ce grou         Implete de sec       Les membres qui ont un         Implete de sec       Les membres qui ont un         Implete de sec       Groupe de séc       Tous les utilisateurs du d	<ul> <li>Utilisateurs et ordinateurs Active</li> <li>Requêtes enregistrées</li> <li>parcus.fr</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>GLPI</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	Nom Administrateur Administrateurs clés Administrateurs clés Enterprise Administrateurs de l'entreprise Administrateurs du l'entreprise Administrateurs du schéma Administrateurs du schéma Contrôleurs de domaine Contrôleurs de domaine clonabl Contrôleurs de domaine d'entre Contrôleurs de domaine en lect Contrôleurs de certificats Groupe de réplication dont le m Groupe de réplication dont le m Contrátique Invité Invité Propriétaires créateurs de la stra Protected Users Serveurs RAS et IAS Utilisateurs DHCP Utilisateurs du domaine	Type Utilisateur Groupe de séc Groupe de séc	Description Compte d'utilisateur d'a Les membres de ce grou Administrateurs désigné Les membres qui ont un Administrateurs désigné Tous les contrôleurs de Les membres de ce grou Les mots de passe des Les mots de passe des Les mots de passe des Les membres de ce grou Les membres qui ont un Tous les utilisateurs du d

• Cliquez avec le bouton droit, sélectionnez "Nouveau" puis "Utilisateur".

👤 Créer da	nns : parcus.fr/Users	
<b>U</b>		
Prénom :	Initiales :	
Nom :		
Nom complet :		
Nom complet : Nom d'ouverture d	de session de l'utilisateur :	
Nom complet : Nom d'ouverture d	de session de l'utilisateur : @parcus.fr ~	
Nom d'ouverture d	de session de l'utilisateur : @parcus.fr  v de session de l'utilisateur (antérieur à Windows 2000) :	
Nom d'ouverture d	de session de l'utilisateur : @parcus.fr  de session de l'utilisateur (antérieur à Windows 2000) :	

• Remplissez les informations requises et suivez l'assistant pour créer le compte utilisateur.

- Les groupes sont utilisés pour simplifier la gestion des permissions.
- Pour créer un groupe, ouvrez "Utilisateurs et Ordinateurs Active Directory".
- Cliquez avec le bouton droit sur l'OU appropriée, sélectionnez "Nouveau" puis "Groupe".
- Nommez le groupe et définissez son type (Distribution ou Sécurité) et sa portée (Domaine local, Global, Universel).

Nouvel objet - Groupe	×	
Créer dans : parcus.fr/l	Users	
Nom du groupe :		
1		
Nom de groupe (antérieur à Windows 2	2000) :	
Étendue du groupe	Type de groupe	
O Domaine local	● Sécurité	
<ul> <li>Globale</li> </ul>	Obistribution	
OUniverselle		
	OK Annuler	

Ajout d'un Ordinateur au Domaine

• Sur le poste de travail ou le serveur à ajouter, accédez aux paramètres système.

Paramètres associés Gestionnaire de périphériques Bureau à distance Protection du système Paramètres avancés du système Renommer ce PC (avancé) Paramètres graphiques

- Cliquer sur "Renommer ce PC (avancé)".
- Sous "Nom de l'ordinateur", cliquez sur "Modifier".

Ir F	Propriétés système			$\times$		
	Paramètres système Nom de l'ordir	e avancés nateur	Utilisation à distance Matériel			
	Windows utilis ordinateur sur	e les informations s le réseau.	uivantes pour identifier votre			
	Description de l'ordinateur :	Par exemple : "Serveur de production IIS" ou				
	Nom complet de l'ordinateur :	"Serveur de gestion". WINSERV-AD.parcus.fr				
e	Domaine :	parcus.fr				
c	Pour renommer cet ordina ou de groupe de travail, o	ateur ou changer d cliquez sur Modifier	le domaine Modifier r.			
i						
e		ОК	Annuler Applique	r		

• Sélectionnez "Domaine", entrez le nom de votre domaine, puis suivez les instructions pour redémarrer l'ordinateur.

#### Création et Gestion des OU

- 1. Les Unités d'Organisation permettent de structurer et de gérer les objets AD de manière hiérarchique.
- 2. Pour créer une OU, ouvrez "Utilisateurs et Ordinateurs Active Directory".
- 3. Cliquez avec le bouton droit sur le domaine ou l'OU existante, sélectionnez "Nouveau" puis "Unité d'Organisation".
- 4. Nommez l'OU et configurez les paramètres nécessaires.

#### Conclusion :

La mise en place et l'utilisation combinée d'Active Directory, DNS et DHCP renforcent la sécurité, la stabilité et l'efficacité des infrastructures réseau. Active Directory facilite la gestion centralisée des utilisateurs et des ressources, tandis que DNS et DHCP assurent respectivement une communication fiable et une configuration simplifiée des adresses IP. En suivant les étapes et les recommandations présentées dans ce guide, vous pourrez exploiter pleinement ces outils pour optimiser la gestion de votre réseau et améliorer l'expérience utilisateur.

## Documentation d'installation Modoboa (Ubuntu)



## Introduction

Modoboa est un serveur de messagerie 100% gratuit et open source. Il s'agit d'un serveur de messagerie Python hautement évolutif avec simplicité et vitesse à la base. Modoboa rassemble les meilleurs outils open source pour installer, configurer et sécuriser votre propre serveur de messagerie.

Nicolas ERNST

### Installation

Installer python3:

root@mail:~# apt-get install python3-virtualenv python3-pip git curl gnupg2 -y

Installer le paquet Modoboa:

root@mail:~# git clone https://github.com/modoboa/modoboa-installer

Donner la permission au dossier modoboa-installer:

root@mail:~# chmod -R 777 modoboa-installer

Aller dans le dossier modoboa-installer:

root@mail:~# cd modoboa-installer

Créez un installeur modoboa:

root@mail:~/modoboa-installer# python3 ./run.py --stop-after-configfile-check yourdomain.com Welcome to Modoboa installer! Configuration file installer.cfg not found, creating new one.

Modifier le fichier d'installation créé :

root@mail:~/modoboa-installer# nano installer.cfg

```
[general]
hostname = mail.%(domain)s
[certificate]
generate = true
type = self-signed
[letsencrypt]
email = admin@example.com
[database]
engine = postgres
host = 127.0.0.1
install = true
[postgres]
user = postgres
password =
[mysql]
user = root
password = dnnUzG2BsM9RZ7PC
charset = utf8
collation = utf8_general_ci
```

Lancer l'installation de Modoboa:



Vérifier si le site modoboa est en ligne:



Allez dans un navigateur web est entrez l'adresse ip du serveur modoboa puis entrez vos identifiants admin :

	modob mail hosting	made simple
Username	1 I	
Password		
	Remember me	
	Log in	Forgot password?

Vous êtes maintenant dans Modoboa.

Latest news       May 12, 2020         A bunch of new releases       May 12, 2020         Modoboa @ PyConFr 2018       Sept. 3, 2018         A calendar for Modoboa       April 6, 2018         Code sprint in Alençon, France       March 16, 2018         Bitcoin Cash donations       Jan. 5, 2018         Visit the official weblog for more information.         Statistics         Type       Quantity         Domains       0         Domain aliases       0	*	Statistics	Quarantine	Domains	Identities	Modoboa		
Latest news       May 12, 2020         A bunch of new releases       May 12, 2020         Modoboa @ PyConFr 2018       Sept. 3, 2018         A calendar for Modoboa       April 6, 2018         Code sprint in Alençon, France       March 16, 2018         Bitcoin Cash donations       Jan. 5, 2018         Visit the official weblog for more information.       Cilobal statistics         Type       Quantity         Domains       0         Domain aliases       0		He	llo adı	min.				
A bunch of new releases       May 12, 2020         Modoboa @ PyConFr 2018       Sept. 3, 2018         A calendar for Modoboa       April 6, 2018         Code sprint in Alençon, France       March 16, 2018         Bitcoin Cash donations       Jan. 5, 2018         Visit the official weblog for more information.         Global statistics         Type       Quantity         Domains       0         Domain aliases       0		Late	Latest news				Features looking for sponsoring	F
Modoboa @ PyConFr 2018       Sept. 3, 2018         A calendar for Modoboa       April 6, 2018         Code sprint in Alençon, France       March 16, 2018         Bitcoin Cash donations       Jan. 5, 2018         Visit the official weblog for more information.       Global statistics         Type       Quantity         Domains       0         Domain aliases       0		A bun	A bunch of new releases			May 12, 2020		
A calendar for Modoboa     April 6, 2018       Code sprint in Alençon, France     March 16, 2018       Bitcoin Cash donations     Jan. 5, 2018       Visit the official weblog for more information.         Clobal statistics       Type     Quantity       Domains     0       Domain aliases     0		Modol	Modoboa @ PyConFr 2018			Sept. 3, 2018	Nothing to sponsor yet.	
Code sprint in Alençon, France     March 16, 2018       Bitcoin Cash donations     Jan. 5, 2018       Visit the official weblog for more information.         Global statistics       Type     Quantity       Domains     0       Domain aliases     0		A cale	ndar for Modol	boa		April 6, 2018		
Bitcoin Cash donations     Jan. 5, 2018       Visit the official weblog for more information.       Global statistics       Type     Quantity       Domains     0       Domain aliases     0		Code	Code sprint in Alençon, France			March 16, 2018		
Visit the official weblog for more information.       Global statistics       Type     Quantity       Domains     0       Domain aliases     0		Bitcoir	Bitcoin Cash donations		Jan. 5, 2018			
Global statistics       Type     Quantity       Domains     0       Domain aliases     0			Visit the official weblog f			rmation.		
TypeQuantityDomains0Domain aliases0		Glob	Global statistics Type Quar					
Domains     0       Domain aliases     0		Туре			itity			
Domain aliases 0		Domai	ins		0			
		Domai	Domain aliases		0			
Identities 1		Identit	ies		1			

## Configuration d'Asterisk



09/04/2025

## 1) Installation d'Asterisk

L'installation et la configuration d'Asterisk se fera sur le même serveur ubuntu que Modoboa, donc pas besoin de montrer comme configurer le serveur.

A) Mise à jour du serveur + installations des dépendances requises

Mettre à jour le serveur avec cette commande.

hollo@hollo:~\$ sudo apt update && sudo apt upgrade −y\_
Installer les dépendances avec cette commande.

hollo@hollo:~\$ sudo apt install build–essential git curl wget subversion libncurses5–dev libxml2–dev libsqlite3–dev uuid–dev libjansson–dev libssl–dev –y

Nicolas ERNST

B) Téléchargement et pré-installation de Asterisk

Accéder au répertoire /usr/src.

hollo@hollo:~\$ cd /usr/src hollo@hollo:/usr/src\$ Télécharger le paquet de Asterisk via le site web officiel.

hollo@hollo:/usr/src\$ sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk–20-cur rent.tar.gz

L'installation n'est pas très longue.



Extraire le paquet téléchargé dans le répertoire.

hollo@hollo:/usr/src\$ sudo tar xvf asterisk-20-current.tar.gz

Accéder au répertoire de Asterisk.

hollo@hollo:/usr/src\$ cd asterisk–20.13.0/

Documentation situation professionnelle 2

Nicolas ERNST

Démarrer la pré-installation de Asterisk en effectuant ces 2 commandes.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo contrib/scripts/install\_prereq install

hollo@hollo:/usr/src/asterisk-20.13.0\$ sudo ./configure\_

Effectuer cette commande.

hollo@hollo:/usr/src/asterisk-20.13.0\$ sudo make menuselect

Une fois sur cette partie cliquer sur la touche S puis Q. Il n'y a aucune modification à apporter.

жжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжжж
Press 'h' for help.
> Add-ons (See README-addons.txt) Applications Bridging Modules Call Detail Recording Channel Event Logging Channel Drivers Codec Translators Format Interpreters Dialplan Functions PBX Modules Resource Modules Test Modules Compiler Flags Utilities AGI Samples Core Sound Packages Music On Hold File Packages Extras Sound Packages

C) Compilation et installation de Asterisk

Effectuer cette commande.

hollo@hollo:/usr/src/asterisk-20.13.0\$ sudo make -j\$(nproc)\_

Lancer cette commande.

hollo@hollo:/usr/src/asterisk=20.13.0\$ sudo make install

Lancer cette commande.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo make samples\_

Effectuer cette commande.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo make config

Lancer cette commande pour terminer l'installation de Asterisk.

hollo@hollo:/usr/src/asterisk=20.13.0\$ sudo ldconfig\_

Démarrer Asterisk.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo systemctl start asterisk

Activer Asterisk.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo systemctl enable asterisk

Vérifier si Asterisk est bien actif.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo systemctl status asterisk
<ul> <li>asterisk.service – LSB: Asterisk PBX</li> </ul>
Loaded: loaded (/etc/init.d/asterisk; generated)
Active: active (running) since Sat 2025–04–12 14:48:55 UTC; 49s ago
Docs: man:systemd–sysv–generator(8)
Tasks: 66 (limit: 4519)
Memory: 38.9M
CPŪ: 2.636s
CGroup: /system.slice/asterisk.service
└─59527 /usr/sbin/asterisk
avril 12 14:48:55 hollo systemd[1]: Starting LSB: Asterisk PBX
avril 12 14:48:55 hollo asterisk [59514]: * Starting Asterisk PBX: asterisk
avril 12 14:48:55 hollo asterisk[59514]:
avril 12 14:48:55 hollo sustemd[1]: Started LSB: Asterisk PBX
hollo@hollo:/usr/src/asterisk_20 13 0\$

Accéder à la console de Asterisk pour voir si ça fonctionne.

#### hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo asterisk –rvv

Si ceci s'affiche, Asterisk s'est bien installé.

Asterisk 20.13.0, Copyright (C) 1999 – 2025, Sangoma Technologies Corporation and others. Created by Mark Spencer <markster@digium.com></markster@digium.com>
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
connected to Asterisk 20.13.0 currently running on hollo (pid = 59527) hollo*CLI>

Faire exit pour quitter la console Asterisk.

hollo\*CLI> exit Asterisk cleanly ending (0). Executing last minute cleanups hollo@hollo:/usr/src/asterisk–20.13.0\$ \_

# 2) Configuration des utilisateurs SIP pour le softphone

Accéder au fichier de configuration pjsip.conf.

hollo@hollo:/usr/src/asterisk-20.13.0\$ sudo nano /etc/asterisk/pjsip.conf

Chercher cette partie, il faut la modifier.



Voici le rendu final pour que le transport UDP fonctionne.



Descendre tout en bas du fichier pour ajouter un nouvel utilisateur SIP.

Voici un exemple de configuration pour un utilisateur (1001 ici).

Nicolas ERNST

[1001] type=endpoint context=internal disallow=all allow=ullaw auth=auth1001 aors=1001	
[auth1001] type=auth auth_type=userpass username=1001 password=p@sswOrd	
[1001] type=aor max_contacts=1	

Créer un deuxième utilisateur (1002 par exemple) afin de réaliser des tests plus tard.

Faire Ctrl + X, puis Y et Enter pour quitter et sauvegarder le fichier.

Accéder au fichier du plan de numérotation.

hollo@hollo:/usr/src/asterisk–20.13.0\$ sudo nano /etc/asterisk/extensions.conf

Documentation situation professionnelle 2

Nicolas ERNST

Ajouter ces lignes à la fin du fichier puis quitter et sauvegarder.

[internal]
exten => 1001,1,Dial(PJSIP/1001)
exten => 1002,1,Dial(PJSIP/1002)

Documentation situation professionnelle 2

Nicolas ERNST

Redémarrer Asterisk.

hollo@hollo:/usr/src/asterisk-20.13.0\$ sudo systemctl restart asterisk

# 3) Installation et configuration d'un client Softphone

Accéder à une machine Windows Client connectée au domaine.

Nous allons installer Zoiper, un client Softpone très fiable et répandu.

Rechercher Zoiper download et accéder au premier lien.



#### Choisir la version Windows.

Download Zoiper 5, a free VoIP × +		-	a ×
← → C 5 zoiper.com/en/voip-softphone/download/current		₿ ☆	<b>®</b> :
💋 ZoiPer	BRANDING SDK <b>DOWINLOAD</b> PRODUCTS HELP CONTACT <b>SHOP</b> LOGIN		
	Latest versions		
	Zoiper 5		
	201601-0		
	free VoIP softphone for non-commercial use		
	Desktop		
	Windows		
	Mac Download		
	▲ Linux Download		
	Mobile		
	Android Download		
	iOS iOS Download		



#### Dans le cadre du projet, choisir la version gratuite.

<ul> <li>Ø Download Zoiper 5, a free VolP × +</li> </ul>		- 0
← → ♂ toiper.com/en/voip-softphone/downlo	ad/current	목 🌣 🅑 🤅
💋 ZoiPer	Your download will start automatically in 0 seconds         Click here if it doesn't       Buy         Click here for download / installation instructions.         non-commercial use only         These are the most popular providers in your country       Bulgaria         Sign up       Rate         Image: Sign up       Rate         Image: Sign up       Rate	Historiana des teléchargemenns vionats X 2 Colpers Installer, y5.6.6 (1) exe 1 & U214 Mo - 2 moder relations Historique rendet des téléchargement C

L'installation se lancera tout seul, attendre la fin.

Une fois installer, lancer le programme d'installation de Zoiper.

Entrer les droits admins puis cliquer sur OUI.

Contrôle de compte d'utilisateur X	
Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?	
Zoiper5_Installer_v5.6.6.exe	
Éditeur vérifié : Securax EOOD Origine du fichier : Disque dur sur cet ordinateur	
Afficher plus de détail	and the
Pour continuer, tapez un nom et un mot de passe d'administrateur.	1
Administrateur	3 To
••••••••••••••	
 Domaine : SECURITECIVILE	
Oui Non	
Wit and	

Cliquer sur Next.



Accepter les termes de licence puis cliquer sur Next.



### Cliquer sur Next.

	🥖 Zoiper5 Setup	- 🗆 X
15	Select Components	🤣 ZoiPer
	Select the components you want to inst	all. Click Next when you are ready to continue.
	Zoiper5	click on a component to get a detailed description
	InstallBuilder	
		< Back Next > Cancel

# Cliquer sur Next.

🤣 Zoiper5 Setup	-		×
Select Start Menu Folder	Ø	Zoil	Per
Please specify the Start Menu Folder in which you would like to cr shortcuts. You can also enter a name to create a new folder.	reate the	program's	5
Zoiper5			
Don't Create Start Menu Folder.			
InstallBuilder			
< Back	Next >	Car	ncel

Sélectionner la version 64-bit et cliquer sur Next.

	🤣 Zoiper5 Setup — 🗆 🗙
2	Select architecture (32 or 64 bit)
	Please specify which version of Zoiper5 would you like to install?
	○ 32 Bit version - compatible with 32 bit Microsoft Office.
	64 Bit version - compatible with 64 bit Microsoft Office.
	InstallBuilder
	< Back Next > Cancel

# Sélectionner All Users et cliquer sur Next.

	Ø Zoiper5 Setup − □ ×
25	Select Installation Scope ZoiPer
	Please specify whether you wish to make this software available to all users or just yourself.
	All Users
	O Current User
	InstallBuilder
	< Back Next > Cancel

# Cliquer sur Next.

Ø	Zoiper5 Setup —		×
25 R	eady to Install	Zo	iPer
Se	tup is now ready to begin installing Zoiper5 on your computer.		
Inst	tallBuilder		
	< Back Next >	(	Cancel



Attendre la fin de l'installation et cliquer sur Finish.
🤣 Zoiper5	- 🗆 X
<b>ZoiPer</b>	FREE
You are running Zoiper5 Community Edition Free for non commercial use	
Activate your PRO license Learn more about PRO	
OR OR Continue as a Free user	

Ouvrir Zoiper et cliquer sur Continue as a Free user.

Nicolas ERNST

Se connecter en entrant le nom d'utilisateur (1001 par exemple) suivi de @192.168.50.5 (adresse IP du serveur Ubuntu). Rentrer aussi le mot de passe puis cliquer sur Login.





#### Rentrer à nouveau l'IP du serveur puis cliquer sur Next.

#### Cliquer sur Skip.



Sélectionner UDP pour le transfert et cliquer sur Next.



Nous avons réussi à nous connecter au compte SIP que l'on a créé avant.

#### Nicolas ERNST



## 4) Tests

Sur un deuxième client Windows connecté au domaine, installer à nouveau Zoiper et se connecter avec le 2ème compte créé avant (1002 dans mon cas).

Essayer d'appeler 1002 sur le client Windows (sur le client Windows avec l'utilisateur 1001).

Rechercher 1002 puis cliquer sur Enter.



Le téléphone sonne bien.



Sur le deuxième client, décrocher en appuyant sur l'icône de téléphone vert.

**Nicolas ERNST** 



Les appels fonctionnent.



# Configuration de eBrigade + DMZ



09/04/2025

Documentation situation professionnelle 2 191 sur 247

## 1) Configuration de l'interface DMZ sur les routeurs

Après avoir ajouté une nouvelle carte réseau en host-only sur nos deux routeurs (avec une plage d'adresse différente de celle des LAN), on peut configurer l'interface DMZ.

Sur l'interface web de PfSense, aller dans Interfaces puis Assignments.



On peut voir qu'une interface est libre et prête à être configurée : c'est la carte réseau qui a été ajoutée.

Cliquer sur Add.



La nouvelle interface a été créée et s'appelle OPT3.

Cliquer dessus pour la configurer.

of pfSense.home.arpa - Interfaces: × +			
→ C S Non sécurisé https://192.168.	.1/interfaces_assign.php		
	Sense System - Interfaces - Firewall -	Services - VPN - Status - Diagnostics -	Help - 🕞
	Interfaces / Interface Assignments		ш 😧
	Interface has been added.		Μ
	Interface Assignments Interface Groups Wireless	VLANS QinQs PPPs GREs GIFs	Bridges LAGGs
	Interface Network port		
	WAN1 em0 (00:0c:29	:43:e4:bb)	~
	LAN em1 (00:0c:29	:43:e4:c5)	Celete
	WAN2 em2 (00:0c:29	:43:e4:cf)	Celete
	OVPN_Interface ovpns1 (VPN)		Celete
	OPT3 em3 (00:0c:29	:43:e4:d9)	Celete
	Save		
	Interfaces that are configured as members of a lagg(4) interface will Wireless interfaces must be created on the Wireless tab before they	I not be shown. can be assigned.	

Activer l'interface en cochant enable, renommer l'interface en "DMZ", choisir Static IPv4 Pour la configuration IPv4, et entrer une adresse sur la plage de la nouvelle carte réseau (dans mon cas 192.168.200.0, j'ai mis 192.168.200.251).

Interfaces / OPT	3 (em3) 幸 Ш 😧
General Configuratio	n
Enable	Enable interface
Description	DMZ
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	x00000000000
	This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.
МТО	
	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	
	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect)
	Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configura	ation
IPv4 Address	192.168.200.251
IPv4 Upstream gateway	None   Add a new gateway
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

Une fois les paramètres rentrés, cliquer sur Save.

IPv4 Address	192.168.200.251	/ 24 🗸
v4 Upstream gateway	None	Add a new gateway
	If this interface is an Internet connection, select an ex On local area network interfaces the upstream gatew Selecting an upstream gateway causes the firewall to Gateways can be managed by clicking here.	ing Gateway from the list or add a new one using the "Add" button. should be "none". Nat this interface as a WAN type interface.
eserved Networks		
Block private networks Ind loopback addresses	Blocks traffic from IP addresses that are reserved for RFC 4193 (fc00::/7) as well as loopback addresses (1 private address space, too.	vate networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per /8). This option should generally be turned on, unless this network interface resides in such a
Block bogon networks	Blocks traffic from reserved IP addresses (but not RF routing table, and so should not appear as the source This option should only be used on external interface Note: The update frequency can be changed under Sy	918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet idress in any packets received. WANS), it is not necessary on local interfaces and it can potentially block required local traffic. mr > Advanced. Firewall & NAT settings.

Cliquer sur Apply Changes pour appliquer les changements.



Il faut réaliser la même opération sur le PfSense Backup en rentrant une autre adresse IPv4 (192.168.200.252 dans mon cas).

Ensuite il faut configurer un CARP DMZ, de cette façon si le routeur Master tombe, notre DMZ sera toujours disponible via le routeur Backup.

Aller dans Firewall puis Virtual IPs.



## Cliquer sur Add.

Virtual IP Address				
Virtual IP address	Interface	Туре	Description	Actions
192.168.50.254/24 (vhid: 1)	LAN	CARP	CARP	e 🖉 🖬
192.168.1.140/24 (vhid: 10)	WAN1	CARP	CARP WAN1	Ø 🛅
192.168.1.141/24 (vhid: 20)	WAN2	CARP	CARP WAN2	e 🖉 🖬
192.168.200.254/24 (vhid: 30)	DMZ	CARP	DMZ	e 🖉 🖬

Voici les paramètres à rentrer (l'adresse est à ajuster en fonction de votre plage IP). Mettre aussi un VHID Group différent des autres IP virtuelles déjà présentes.

Une fois tous les paramètres remplis cliquer sur Save.

Туре	O IP Alias	CARP	O Proxy ARP	O Other	
Interface	DMZ		~		
Address type	Single address		~		
Address(es)	192.168.200.254	potwork's with stragger, it does	not specify a CIDR range.	/ 24	~
Virtual IP Password	Enter the VHID group r	bassword	Confirm		
VHID Group	30	hat the machines will share	~		
dvertising frequency	1 Base The frequency that this master.	s machine will advertise. 0 mea	O     Skew ns usually master. Otherwise the lo	west combination of both values in the cl	luster determine
Description	DMZ				

Cliquer sur Apply Changes pour appliquer les changements.



Si l'on va dans Status puis CARP (failover), on peut voir que :

• Sur le PfSense Master le CARP DMZ est bien en MASTER.

y pfSense.home.arpa - Status: CAI × pf pfSense.ho	ome.arpa - Interfaces: ×   +				
← → C ON Non sécurisé https://192.168.50.1/s	'status_carp.php				
pf	SENSE System - Interfaces -	Firewall - Services -	√PN - Status - Diagr	nostics - Help -	0
s	Status / CARP				≢ ₩ 0
c	CARP Maintenance				
٥	Temporarily Disable CARP	t CARP Maintenance Mode			
c	CARP Status				
Inte	terface and VHID	Virtual IP Addr	ess	Status	
LA	AN@1	192.168.50.25	4/24	MASTER	
w	/AN1@10	192.168.1.140	/24	S MASTER	
w	/AN2@20	192.168.1.141	/24	S MASTER	
	MZ@30	192.168.200.2	54/24	MASTER	

• Sur le PfSense Backup le CARP DMZ est bien en BACKUP.

• ■ ptsenschonesarpa-Satus: CA ×         • ●         • ● ● ● ● Non sécuré https://192.168.502/status_carp.php           • ● ● ● ● Non sécuré https://192.168.502/status_carp.php             • ● ● ● ● Non sécuré https://192.168.502/status_carp.php           • ● ● ● ● ● ● ● Non sécuré https://192.168.502/status_carp.php             • ● ● ● ● ● ● Non sécuré https://192.168.502/status_carp.php           • ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●													
	•	🗾 pfSense	e.home.arpa - Status: CA	🗙 🚮 pfS	ense.home.arpa - Status: CA 🛛 🗙	+							
Operation         System         Interfaces         Firewall         Services         VPN         Status         Diagnostics         Help         Image: Comparison of the compari	←	$\rightarrow$ G	O Non sécurisé	https://192.168	8.50.2/status_carp.php								
Status / CARP       CARP Maintenance						- Interfaces -	Firewall +	Services +	VPN -	Status 🗸	Diagnostics +	Help +	¢
CARP Maintenance           Interface and VHID         Virtual IP Address         Status           LANQ1         192.168.50.254/24         © BACKUP           WAN1@10         192.168.50.254/24         © BACKUP           WAN1@10         192.168.1.140/24         © BACKUP           WAN2@20         192.168.1.141/24         © BACKUP           DM2@30         192.168.20.254/24         © BACKUP					Status / CARP								≢ ല 😧
CARP Status         Virtual IP Address         Status           LANG1         192.168.50.254/24         © BACKUP           WAN1@10         192.168.1.140/24         © BACKUP           WAN2@20         192.168.20.254/24         © BACKUP           DM2@10         192.168.20.254/24         © BACKUP					CARP Maintenance								
KARP Status           Interface and VHID         Virtual IP Address         Status           LAN@1         192.168.50.254/24         © BACKUP           WAN1@10         192.168.11.40/24         © BACKUP           WAN2@20         192.168.11.41/24         © BACKUP           DMZ@30         192.168.20.254/24         © BACKUP					S Temporarily Disable C	ARP 🎤 Enter Pers	sistent CARP Main	tenance Mode					
Interface and VHID         Virtual IP Address         Status           LAN@1         192.168.50.254/24              © BACKUP            WANI@10         192.168.1.140/24              © BACKUP            WAN2@20         192.168.1.141/24              © BACKUP            DMZ@0         192.168.20.0254/24              © BACKUP					CARP Status								
LAN@1         192.168.50.254/24         © BACKUP           WAN1@10         192.168.1.140/24         © BACKUP           WAN2@20         192.168.1.141/24         © BACKUP           DMZ@30         192.168.200.254/24         © BACKUP					Interface and VHID			Virtual IP A	ddress			Status	
WANI@10         192.168.1.140/24         © BACKUP           WANZ@20         192.168.1.141/24         © BACKUP           DMZ@30         192.168.200.254/24         © BACKUP					LAN@1			192.168.50	0.254/24			BACK	UP
WAN2@20         192.168.1.141/24         0 BACKUP           DMZ@30         192.168.200.254/24         0 BACKUP					WAN1@10			192.168.1.	140/24			🕕 BACK	UP
DMZ@30 192.168.200.254/24					WAN2@20			192.168.1.	141/24			🕕 BACK	UP
				$\rightarrow$	DMZ@30			192.168.20	00.254/24			U BACK	UP

La DMZ est bien configuré (nous reviendrons sur les règles de pare-feu plus tard).

## 2) Configuration du serveur Ubuntu hébergeant eBrigade

## A) Initialisation du serveur Ubuntu

L'installation et la configuration de eBrigade doit se faire sur un serveur différent de celui hébergeant déjà Modoboa et Asterisk.

Avant de lancer le serveur, configurer une carte réseau en host-only ayant la même plage IP que celle de l'interface DMZ sur les deux routeurs.

Une fois le serveur lancé, appuyer Enter sur l'option Try or Install Ubuntu Server.

	GNU GRUB	version 2.06		
*Try or Install Ubu	intu Server			
Ubuntu Server witl Test memoru	n the HWE kernel			
icst hendry				
Use the ↑ and ↓ Press enter to before booting The highlighted en	keys to select w boot the selected or 'c' for a comm ntry will be execu	hich entry is h OS, 'e' to edi and-line. ted automatical	ighlighted. t the соммаnds ly in 28s.	

Attendre jusqu'à la prochaine étape.

#### Nicolas ERNST

f (	эк і	Reached target Preparation for Remote File Systems.
ìì	пĸ	Reached target Remote File Systems.
ř	ικ	Finished Availability of block devices.
ř	пĸ	Listening on Socket activation for spappy daemon.
ř	пĸ	Reached target Socket Units
i i	nk -	Reached target Basic Sustem
		Starting LSB: automatic crash report generation
1		Started Regular background program processing daemon.
ř	ικ	Started D-Bus Sustem Message Bus
ř	пк –	Started Save initial kernel messages after hont.
		Starting Remove Stale Online ext4 Metadata Check Snapshots
1	nk .	Reached target Login Promots.
ř í	ικ	Started indbalance daemon.
		Starting Dispatcher daemon for systemd-networkd
		Starting Authorization Manager
		Starting Pollinate to seed the pseudo random number generator
		Starting System Logging Service
	эк с	Reached target Preparation for Logins.
		Starting Snap Daemon
		Starting User Login Management
		Starting Permit Üser Sessions
		Starting Disk Manager
	DK - 1	Started System Logging Service.
	JK –	Finished Permit User Sessions.
		Starting Hold until boot process finishes up
		Starting Terminate Plymouth Boot Screen
	JK –	Finished Hold until boot process finishes up.
		Starting Set console scheme
	JK 🛛	Finished Terminate Plymouth Boot Screen.
	DK - 1	Started LSB: automatic crash report generation.
	JK .	Finished Set console scheme.
	JK .	Started User Login Management.
	JK -	Started Unattended Upgrades Shutdown.
L (	JK .	Started Authorization Manager.
		Starting Modem Manager
ļ	JK	Started Dispatcher daemon for systemd-networkd.
ļļ	JK	Finished Remove Stale Unline ext4 Metadata Check Snapshots.
ļ	JK	Started Modem Manager.
	JK JK	Started DISK Manager.
		Finished Fullinate to seeu the pseudo Fandom homoer generator.
		Starting upenaso secure shell server
L L	אנ ער	Statist Uperload Secure Shell Server'.
		Starting Holde Spannu daemon pafrash
		Starting Wait until conduct is full conded
		Starting worth until shape is foring sector
Î d	אר אר	Started Notas and tyd honk install horastall harasta-4469-8155-dca9919d5f68 scone

Sélectionner Français.

#### Nicolas ERNST

Appuyer sur Terminé.

Nicolas ERNST

Configuration clavier	[Help]
Veuillez sélectionner votre disposition de clavier ci-dessous, ou sélectionner "Identifier le clavier" afin de détect disposition automatiquement.	er votre
Disposition : [French •]	
Variante : [French – French (legacy, alt.) ▼]	
[ Identifier le clavier ]	
[Terminé ] [Retour ]	

Sélectionner Ubuntu Server et appuyer sur Terminé.

#### Nicolas ERNST



Une fois dans les paramètres réseaux, aller sur ens33 puis Edit IPv4.

	Connections réseau	[ Help ]
	Configurez au moins une interface pour que ce serveur puisse communiquer avec les autres machines sur le réseau, préférablement un réseau avec accès aux mises à jour.	
1	NAME TYPE NOTES I ens33 eth - UHCPV4 - 00:0c:29:4e:ce:20 / Advanced Mid Edit IPV4 / 79c970 [PCnet32 LANCE] (PCnet - Fast 79C971) I Create bond • ] Add a vLAN tag •	

Choisir Manuel.

IPv4 Method: Automatique (DHCP) ◀ Manuel Désactivée ]		Edit ens33 IPv4 configuration
	IPv4 Method:	Automatique (DHCP) ◀ Manuel Désactivée
[Annuler ]		[Annuler]

Remplir avec ces paramètres (serveur DNS = le Windows Server GUI contrôleur de domaine). Cliquer ensuite sur Sauvegarder.



Attendre l'application des changements puis cliquer sur Terminé.

**Nicolas ERNST** 



Appuyer sur Terminé.

Nicolas ERNST



Attendre la fin du test miroir puis cliquer sur Terminé.



Appuyer sur Terminé.

Nicolas ERNST



#### Appuyer sur Terminé.

Configuration du stockage	[Help]				
SOMMAIRE DU SYSTÈME DE FICHIERS					
POINT DE MONTAGE TAILLE TYPE TYPE DE PÉRIPHÉRIQUE [/ 10.000G new ext4 nouveau LVM logical volume ▶] [/boot 1.771G new ext4 nouveau partition de disque local ▶]					
DISQUES DISPONIBLES					
PÉRIPHÉRIQUE TYPE TAILLE [ ubuntu-vg (nouveau) LVM volume group 18.222G ► ] espace libre 8.222G ►					
[ Create software RAID (md) ► ] [ Create volume group (LVM) ► ]					
PÉRIPHÉRIQUES UTILISÉS					
PÉRIPHÉRIQUE TYPE TAILLE [ubuntu-vg (nouveau) LVM volume group 18.2226 ▶ ] ubuntu-lv nouveau, to be formatted as ext4, mounted at / 10.0006 ▶					
<pre>[ /dev/sda disque local 20.0006 • ] partition 1 nouveau, BIOS grub spacer 1.000M • partition 2 nouveau, to be formatted as ext4, mounted at /boot 1.7716 • partition 3 nouveau, PV of LVM volume group ubuntu-vg 18.2256 •</pre>					
[Retour]					

Sélectionner continuer.



Entrer les identifiants puis cliquer sur Terminé.

Configuration du profil		1
Enter the username and password password is still needed for su	l you will use to log in to the system. You can configure SSH access on the next screen but a do.	
Votre nom :	hollo	
Le nom de cette machine:	dmzebrigade The name it uses when it talks to other computers.	
Choisir un nom d'utilisateur :	hollo	
Choisir un mot de passe :	and a second	
Confirmer votre mot de passe:	KARIPAK	•
	(Terminé )	
### Sélectionner Continuer.



### Appuyer sur Terminé, il n'y a pas besoin de OpenSSH.



## Attendre la fin de l'installation.

Installation du système	[Help]
<pre>subiquity/Early/apply_autoinstall_config subiquity/Reporting/apply_autoinstall_config subiquity/Earchy/apply_autoinstall_config subiquity/Package/apply_autoinstall_config subiquity/Package/apply_autoinstall_config subiquity/Ackage/apply_autoinstall_config subiquity/Ad/apply_autoinstall_config subiquity/Late/apply_autoinstall_config configuring apt curtin command in-target /</pre>	
[ View full log ]	

Installation terminée !	[ Help ]
configuring format: format-0	
configuring partition: partition-2	
configuring lvm_volgroup: lvm_volgroup=0	
configuring lvm_partition: lvm_partition-0	
configuring format: format–1	
configuring mount: mount–1	
configuring mount: mount-0	
executing curtin install extract step	
curtin command install	
writing install sources to disk	
running 'curtin extract'	
curtin command extract	
acquiring and extracting image from cp:///tmp/tmpdystgyn_/mount	
executing current install currenouss step	
configuring installed custom	
pulping printing installed system - cotuneerscous enly	
curring the time aget - setuptionsave-bing	
running 'runtin curthoks'	
curtin command curthooks	
configuring ant configuring ant	
installing missing packages	
configuring iscsi service	
configuring raid (mdadm) service	
installing kernel	
setting up swap	
apply networking config	
writing etc/fstab	
configuring multipath	
updating packages on target system	
configuring pollinate user-agent on target	
updating initramts configuration	
configuring target system bootloader	
final custom configuration	
configure for a loud-init	
configuring clobal inter	
duminading card appletation induces	
curtin compand in-target l	v
[ View full log ]	
[ Annuler la mise à jour et redémarrer ]	

Après avoir attendu, sélectionner Annuler la mise à jour et redémarrer.

Après s'être connecté avec les identifiants suite au redémarrage, mettre à jour le serveur avec cette commande.

hollo@dmz:~\$ sudo apt update && sudo apt upgrade -y\_

B) Installation des dépendances requises

Ajouter le dépôt PPA Ondřej en effectuant ces commandes (nous servira à installer la version 7.4 de php).

hollo@dmz:~\$ sudo apt install software-properties-common -y

hollo@dmz:~\$ sudo add-apt repository ppa:ondrej/php -y\_

hollo@dmz:~\$ sudo apt update\_

Installer les dépendances avec cette commande.

hollo@dmz:~\$ sudo apt install apache2 mariadb-server php7.4 libapache2-mod-php7.4 php7.4-mysql php7 .4-xml php7.4-mbstring php7.4-curl php7.4-zip php7.4-gd unzip wget git –y Activer les services apache2 et mariadb avec ces 2 commandes.

hollo@dmz:~\$ sudo systemctl enable apache2

hollo@dmz:~\$ sudo systemctl enable mariadb

Démarrer mariadb et apache2 avec cette commande.

hollo@dmz:~\$ sudo systemctl start apache2 mariadb

(OPTIONNEL) Effectuer cette commande pour installer de manière sécurisé mariadb.

hollo@dmz:~\$ sudo mysql\_secure\_installation

Effectuer cette commande pour entrer dans la console mariadb.

hollo@dmz:~\$ sudo mysql −u root

Taper ces commandes à la suite pour créer la base de données ebrigade.

Créer la base de données.

MariaDB [(none)]> CREATE DATABASE ebrigade\_db;\_

Créer un utilisateur.

MariaDB [(none)]> CREATE USER 'arthur'@'localhost' IDENTIFIED BY 'Monsieursossou67';

Accorder tous les privilèges au nouvel utilisateur créé.

MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigade\_db.\* TO 'arthur'@'localhost';

Mettre à jour les privilèges.

MariaDB [(none)]> FLUSH PRIVILEGES;\_

Quitter la base de donner en rentrant EXIT; .

MariaDB [(none)]> EXIT; Bye hollo@dmz:~\$ C) Téléchargement et déploiement de eBrigade

Télécharger le paquet de eBrigade avec cette commande.

hollo@dmz:~\$ sudo wget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade–5.3.2.zip\_

Décompresser le paquet de eBrigade avec cette commande.

hollo@dmz:~\$ unzip ebrigade-5.3.2.zip\_

Copier le répertoire de eBrigade dans le répertoire web.

hollo@dmz:~\$ sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade\_

Accorder les droits et les privilèges au répertoire de eBrigade avec ces 2 commandes.

hollo@dmz:~\$ sudo chown \_R www\_data:www\_data /var/www/html/ebrigade\_

hollo@dmz:~\$ sudo chmod \_R 755 /var/www/html/ebrigade

Créer le fichier de configuration de eBrigade pour apache2.

hollo@dmz:~\$ sudo nano /etc/apache2/sites-available/ebrigade.conf

Voici les paramètres à entrer (à adapter selon la configuration).



Faire CTRL + X, puis Y et Enter pour quitter et sauvegarder la configuration.

Activer le site en tapant ces commandes.

hollo@dmz:~\$ sudo a2ensite ebrigade.conf\_

hollo@dmz:~\$ sudo a2enmod rewrite\_

hollo@dmz:~\$ sudo systemctl reload apache2

#### D) Première connexion à l'interface web de eBrigade

Depuis un client Windows, accéder à l'interface web de eBrigade via l'adresse IP du serveur (192.168.200.10 dans mon cas).

Entrer un nouveau mot de passe puis cliquer sur Sauvegarder.

*	🗾 pfSens	e.home.arpa - Status: C	🚈 🗙 🕴 🗾 pfSens	e.home.arpa - Statu	s: C/ 🗙	🐝 CIS   eBrigad	e	× +	-
←	$\rightarrow$ G	▲ Non sécurisé	192.168.200.10/c	hange_password.	.php				© \$
				Modifier le mo ADMIN	t de passe	pour Admin			
				Veuillez pas	choisir u sse perso	un mot de onnel.			
				Nouveau mot de passe Confirmation		•••••			
			Pour plus	de sécurité, me	ettez auss	si des caractèr	es spéciaux!		
				s	auvegard	ler			

### Cliquer sur Continuer.





Voici les paramètres à entrer pour la configuration de eBrigade.

Ajouter l'adresse mail admin du serveur de messagerie Modoboa.

Cliquer ensuite sur Valider.



Type d'organisation *	
Sans préconfiguration	•
Nom court de votre organisation *	
SC	
Nom long de votre organisation *	
Sécurité civile	
Adresse Web *	
http://192.168.200.10	
Votre adresse email *	
admin@securitecivile.local	
Nom personnalisé de l'application *	
eBrigade	

### Cliquer sur Utiliser.



✓ of pfSense.home.arpa - Status: C/ ×	of Sense.home.arpa - Status: C 🗙 👫 SC   eBrigade	× + - 🗆 ×
← → C ▲ Non sécurisé 192.	168.200.10/index_d.php	☆ 🚨 :
斧 ≘	¢ 🛱 🛱 Q	
	Activités Sécurité civile Mois 0 Trimestre 0	Tâches Mes Alarmes Total 13
	Mes activités	Mains courantes
۷	Aucune prochain participation prévue	Aucune main courante
- civile ne 13 25 16:11 ∋ 15	Demande de congés eee Aucune demande de congé à valider	Calendrier des activités 10 40 ••• Sécurité civile
Deuxiè prénon À rensei ici	me n gner Véhicule	Heures de formation ••• Formations suivies depuis le début 2025.
Adress À renseig	ie gner	TOTAL 00:00 h
Code postal À renseij ici	gner	A propos de eBrigade
Lieu de naissa	nce Explorateur de fichiers	■ Documentation en ligne →

## Nous sommes bien connectés à l'interface web de eBrigade.

#### 3) Règles de pare-feu sur PfSense

Sur le PfSense Master, aller dans Firewall puis Rules.



## Ajouter une règle d'accès depuis LAN vers DMZ.

Firewall / Rules /	Edit				<b>∓</b> ₩ 🗏 🕄
Edit Firewall Rule					
Action	Pass Choose what to do with Hint: the difference betw whereas with block the	packets that match the criteria specified below. een block and reject is that with reject, a packet backet is dropped silently. In either case, the origi	(TCP RST or ICMP nal packet is disca	port unreachable for UDP) is re rded.	turned to the sender,
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable</li> </ul>	e this rule without removing it from the list.			
Interface	LAN Choose the interface fro	w which packets must come to match this rule.			
Address Family	IPv4 Select the Internet Proto	col version this rule applies to.			
Protocol	Any Choose which IP protoc	V of this rule should match.			
Source Source	Invert match	LAN net	*	Source Address	/ ~
Destination <u>Destination</u>	Invert match	Single host or alias	~	192.168.200.10	1
Extra Options Log	Log packets that are Hint: the firewall has lim the Status: System Logs	handled by this rule ited local log space. Don't turn on logging for eve : Settings page).	rything. If doing a l	lot of logging, consider using a	remote syslog server (see
Description	Accès eBrigade depuis A description may be en log.	LAN tered here for administrative reference. A maxim	um of 52 character	rs will be used in the ruleset and	d displayed in the firewall
Advanced Options	Cisplay Advanced				
Rule Information					

Ajouter une règle d'accès DMZ vers WAN.

Firewall / Rules /	Edit				≢ Ш 🗏 🕄
Edit Firewall Rule			_		
Action	Pass Choose what to do with pack Hint: the difference between t whereas with block the packe	ets that match the criteria specified belo olock and reject is that with reject, a pack tt is dropped silently. In either case, the c	w. ket (TCP RST or ICMP riginal packet is disca	port unreachable for UDP) is retur	rned to the sender,
Disabled	Disable this rule Set this option to disable this	rule without removing it from the list.			
Interface	DMZ Choose the interface from wh	ich packets must come to match this ru	▶ le.		
Address Family	IPv4 Select the Internet Protocol ve	ersion this rule applies to.	*		
Protocol	Any Choose which IP protocol this	s rule should match.	*		
Source					
Source	Invert match	DMZ net	~	Source Address	1 🗸
Destination					
Destination	Invert match	any	~	Destination Address	/ 🗸
Extra Options					
Log	Log packets that are hand Hint: the firewall has limited le the Status: System Logs: Sett	led by this rule ocal log space. Don't turn on logging for tings page).	everything. If doing a	lot of logging, consider using a rer	note syslog server (see
Description	Accès Internet depuis DMZ A description may be entered log.	here for administrative reference. A ma:	kimum of 52 characte	rs will be used in the ruleset and d	isplayed in the firewall
Advanced Options	Display Advanced				
	Save	Misseneth Educa			

Ajouter une règle d'accès Web à eBrigade depuis LAN.

Firewall / Rules /	Edit					≢ Ш 🗏	0
Edit Firewall Rule							
Action	Pass Choose what to do with packet Hint: the difference between b whereas with block the packet	ts that match the criteria spec lock and reject is that with reje i is dropped silently. In either ca	fied below. ct, a packet (TCP RST ase, the original packet	or ICMP   t is discar	port unreachable for UDP) is return rded.	ed to the sender,	
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable this</li> </ul>	rule without removing it from t	ne list.				
Interface	DMZ Choose the interface from wh	ich packets must come to mat	► Ch this rule.				
Address Family	IPv4 Select the Internet Protocol ve	rsion this rule applies to.	~				
Protocol	TCP Choose which IP protocol this	rule should match.	~				
Source		LAN pet		~	Source Address		×
Juit	Display Advanced The Source Port Range for a dits default value, any.	connection is typically random	and almost never equa	al to the d	estination port. In most cases this	setting must remai	n at
Destination							
Destination	Invert match	Single host or alias		~	192.168.200.10	1	*
Destination Port Range	HTTP (80)	Custom	HTTPS (443) To	▼ ▼	Custom		
Extra Ontions	specify the destination port of	portrange for this fulle. The fi	o field may be left em	ipty ir only	y intering a single port.		_
Log	Log packets that are hand Hint: the firewall has limited to the Status: System Logs: Sett	ed by this rule Ical log space. Don't turn on log ngs page).	gging for everything. If	doing a le	ot of logging, consider using a rem	ote syslog server (s	ee

Ajouter une règle vers Modoboa.

Firewall / Rules /	Edit				≢ 💷 🗐 😯
Edit Firewall Rule					
Action	Pass Choose what to do with packe Hint: the difference between b whereas with block the packet	ts that match the criteria specifie lock and reject is that with reject, is dropped silently. In either case	d below. a packet (TCP RST or ICMP e, the original packet is disca	port unreachable for UDP) is return rded.	ed to the sender,
Disabled	Disable this rule Set this option to disable this	rule without removing it from the	list.		
Interface	DMZ Choose the interface from whi	ch packets must come to match	► this rule.		
Address Family	IPv4 Select the Internet Protocol ve	rsion this rule applies to.	~		
Protocol	TCP Choose which IP protocol this	rule should match.	~		
Source					
Source	Invert match	Single host or alias	~	192.168.200.10	/ 🗸
	Display Advanced The Source Port Range for a contract the source Port Range for a contract the source of the sourc	onnection is typically random an	d almost never equal to the d	lestination port. In most cases this	setting must remain at
Destination					
Destination	Invert match	Single host or alias	~	192.168.50.5	/ ~
Destination Port Range	SMTP (25) V From	Custom	SMTP (25) 🗸	Custom	
	Specify the destination port or	port range for this rule. The "To"	field may be left empty if only	y filtering a single port.	
Extra Options					
Log	Log packets that are handl     Hint: the firewall has limited lo     the Status: Sustem Logs: Sati	ed by this rule cal log space. Don't turn on loggi	ng for everything. If doing a l	ot of logging, consider using a rem	ote syslog server (see

Ajouter une règle qui bloque DMZ > LAN.

Firewall / Rules /	Edit				幸 📖 🗏 😯
Edit Firewall Rule					
Action	Block Choose what to do with pao Hint: the difference between whereas with block the pac	kets that match the criteria specified below. block and reject is that with reject, a packet (T ket is dropped silently. In either case, the origina	CP RST or ICMP al packet is disca	port unreachable for UDP) is ret	turned to the sender,
Disabled	<ul> <li>Disable this rule</li> <li>Set this option to disable th</li> </ul>	is rule without removing it from the list.			
Interface	DMZ Choose the interface from v	$\checkmark$ which packets must come to match this rule.			
Address Family	IPv4 Select the Internet Protocol	✓ version this rule applies to.			
Protocol	Any Choose which IP protocol th	► v			
Source					
Source	Invert match	DMZ net	~	Source Address	/ ~
Destination Destination	Invert match	LAN net	~	Destination Address	/
Extra Options					
Log	Log packets that are har Hint: the firewall has limited the Status: System Logs: Se	ndled by this rule I local log space. Don't turn on logging for every ettings page).	thing. If doing a l	lot of logging, consider using a r	remote syslog server (see
Description	Bloquer DMZ vers LAN A description may be entere log.	d here for administrative reference. A maximum	n of 52 character	rs will be used in the ruleset and	displayed in the firewall
Advanced Options	🔅 Display Advanced				
	Save	Microsoft Edge			

Voici un screen de la configuration des règles sur l'interface LAN.

The changes have been applied successfully. The firewall rules are now reloading in the background.         Monitor the filter reload progress.       MAN1       LAN       WAN2       OVPN_INTERFACE       DMZ       OpenVPN         Rules (Drag to Charge Order)         Rules (Drag to Charge Order)       States       Protocol       Source       Port       Destination       Port       Gateway       Queue       Schedule       Description       Actions         ✓       22/6.79       *       *       LAN Address       443       *       *       Anti-Lockout Rule       Image: Color of the state of the sta	Firewa	all / Rule	s/ LAN	l							≢ 📖 🗉 😧
Floating WAN1 LAN WAN2 OVPN_INTERFACE DMZ OpenVPN   Rules (Drag to Charge Order)   Rules (Drag to Charge Order) Fortion Port Gateway Queue Schedule Description Actions     States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions      22/6.79 *. *. *. LAN Address 443 *. *. Anti-Lockout Rule *.      0/22 KiB IPv4* LAN net *. 192.168.200.10 *. *. none Accès eBrigade depuis LAN *.      0/55 KiB IPv4 J92.168.50.3 *. *. 161 *. none PRTG *.      0/0 B IPv4* LAN net *. *. *. WAN_FAILOVER none Default allow LAN to any rule *.      0/0 B IPv6* LAN net *. *. *. *. mone Default allow LAN IPv6 to any rule *.	The chan Monitor t	ges have beer he filter reload	n applied su d progress.	ccessfully. The f	irewall	i rules are now relo	ading in the	e background.			8
Rules (Drag to Change Order)       States       Protocol       Source       Port       Destination       Port       Gateway       Queue       Schedule       Description       Actions         ✓       22/6.79       *       *       *       LAN Address       443       *       *       Anti-Lockout Rule       *         ✓       0/22 KiB       IPv4*       LAN net       *       192.168.200.10       *       *       none       Accès eBrigade depuis LAN       *       *       ©       *       0/22 KiB       IPv4*       LAN net       *       192.168.200.10       *       *       none       Accès eBrigade depuis LAN       *       *       ©       ©       *       0/02 KiB       IPv4*       LAN net       *       161       *       none       PRTG       *       *       ©	Floating	WAN1	LAN	WAN2	OVPN	LINTERFACE	DMZ	OpenVPN			
✓       22/6.79       *       *       LAN Address       443       *       *       Anti-Lockout Rule       Image: Constraint of the second sec	Rules (	Drag to Ch States	ange Orde Protocol	er) Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
✓       0/22 KiB       IPv4*       LAN net *       192.168.200.10 *       *       none       Accès eBrigade depuis LAN       ★       ↓ <t< td=""><td>~</td><td>22/6.79 MiB</td><td>*</td><td>*</td><td>*</td><td>LAN Address</td><td>443 80</td><td>*</td><td>*</td><td>Anti-Lockout Rule</td><td>\$</td></t<>	~	22/6.79 MiB	*	*	*	LAN Address	443 80	*	*	Anti-Lockout Rule	\$
✓       0/55 KiB       IPv4       192.168.50.3 * *       161       *       none       PRTG       ↓ ✓ □ ♥         ✓       0/0 B       IPv4*       LAN net       *       *       WAN_FAILOVER       none       Default allow LAN to any rule       ↓ ✓ □ ♥         ✓       0/0 B       IPv6*       LAN net       *       *       wan_FAILOVER       none       Default allow LAN to any rule       ↓ ✓ □ ♥         ✓       0/0 B       IPv6*       LAN net       *       *       none       Default allow LAN IPv6 to any rule       ↓ ✓ □ ♥         ✓       0/0 B       IPv6*       LAN net       *       *       none       Default allow LAN IPv6 to any rule       ↓ ✓ □ ♥	- ~	0/22 KiB	IPv4*	LAN net	*	192.168.200.10	*	*	none	Accès eBrigade depuis LAN	ᢤ∥⊡©∎ ×
Image: Wangenerative of the second secon		0/55 KiB	IPv4 UDP	192.168.50.3	*	*	161 (SNMP)	*	none	PRTG	Ů∥⊡O∎ ×
□ ✔ 0/0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule ↑ Add 1 Add The Delete O Toggle □ Copy D Save + Set	- <b>č</b>	0/0 B	IPv4 *	LAN net	*	*	*	WAN_FAILOVER	none	Default allow LAN to any rule	∜∥⊡©≣ ×
1 Add 1 Add m Delete 🛇 Toggle 🔂 Copy 🕞 Save 🕂 Set		0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	∛৶⊘≣ ×
								Add	🕽 Add 面 Del	ete 🚫 Toggle 🚺 Copy 🖬	Save + Separate

Voici un screen de la configuration des règles sur l'interface DMZ.

Flo	ating	) WAN1	LAN	WAN2 OVF	PN_INT	ERFACE DMZ	OpenVF	PN			
Ru	les	(Drag to Cha	inge Ordei	r)							
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
	~	0/0 B	IPv4 TCP	192.168.200.10	*	192.168.50.5	25 (SMTP)	*	none	SMTP vers Modoboa	ৼৢ৻ৗ৾৾৾৾৾৾৾ঢ়৶৶ঢ়৾৾৾৾৾
	~	0/0 B	IPv4 TCP	LAN net	*	192.168.200.10	80 - 443	*	none	Web access à eBrigade	ৼৢ৾ঀ৾৾৾৾৾৾৾৾৾৾৾৾৾৾
	~	0/12 KiB	IPv4*	DMZ net	*	*	*	*	none	Accès Internet depuis DMZ	ৼৢ৻ৗ৾৾৾৾৾৾ঢ়৶৶ঢ়৾৾৾৾৾
	~	0/553.08 MiB	IPv4*	DMZ net	*	*	*	*	none	DMZ Internet	ৼৢ৾ঀ৾৾৾৾৾৾৾৾৾৾৾৾৾৾
	x	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none	Bloquer DMZ vers LAN	℄ℐⅅ℗面