

# Sécurisation des accès distants



## ESICAD

### SOMMAIRE

1. Contexte et cahier des charges3
1.1. Objectifs
1.2. Architecture
2. Mise en œuvre5
2.1. Poste serveur "DMZ"5
2.1.1. Configuration IP5
2.1.2. Paramétrage Apache 26
2.1.3. Configuration du serveur DNS7
2.1.4. Mise en place du protocole HTTPS11
2.1.5. Serveur FTP14
2.1.6. Php pour Apache216
2.1.7. Installation de MariaDB18
2.2.Routeur
2.3. Serveur de fichiers Windows21
2.4. Serveur Mariadb24
2.6. VPN
2.5.1. Création de l'autorité certificative et d'un certificat Server
2.5.2. Création d'un utilisateur et d'un certificat utilisateur
2.5.3. Configuration du serveur VPN33
2.5.4. Export de la configuration VPN37
2.5.5. Utilisation du client VPN sur un poste utilisateur
2.6. Règles ACL



### 1. Contexte et cahier des charges

Notre client souhaite mettre en place un site web sécurisé (serveur web et base de données). Un seul utilisateur pourrait accéder, déposer et modifier des fichiers sur le serveur web.

Il veut également une zone sécurisée pour éviter les attaques extérieures malveillantes en passant par le site web.

Puis, une solution doit être mise en place pour que des fichiers de différents utilisateurs soient partagés et accessibles facilement.

Enfin, il souhaiterait mettre à la disposition de ses employés une solution d'accès à distance sécurisée à son réseau interne.

Les employés doivent pouvoir accéder au serveur de fichier et avoir les mêmes autorisations qu'en étant connecté dans l'entreprise.

Le serveur web doit également être accessible en connexion VPN.

Une des seules contraintes matérielles imposée est l'utilisation d'un routeur virtuel.

Pour cela, nous allons créer une zone démilitarisée (DMZ) dans laquelle nous mettrons le serveur WEB, FTP, DNS. Une DMZ, littéralement une « zone démilitarisée » en anglais est une zone spéciale exposée. C'est vers elle que circule tous les informations qui vont vers internet. Cela sert à protéger le réseau contre les menaces extérieures.

Nous aurons un deuxième réseau, LAN, dans lequel se trouvera le serveur de base de données, le serveur de fichiers et un poste administrateur.

Nous allons utiliser comme routeur virtuel PFsense.

Nous utiliserons OpenVPN comme solution pour se connecter de manière sécurisée au réseau interne depuis l'extérieur.

#### 1.1. Objectifs

- Mettre en place et configurer un routeur virtuel
- Tout le monde peut accéder au serveur web

## ESICAD

- Seul le poste serveur où se trouve le serveur web a accès à la bdd
- Les réseaux LAN et DMZ ont accès à internet
- Accès au FTP seulement par le poste administrateur du réseau LAN
- Permettre aux clients nomades ou en télétravail d'accéder aux services hébergés dans un réseau interne à l'entreprise dans une LAN et/ou une DMZ
- Mettre en place des tests de validation répondant aux demandes





#### 2. Mise en œuvre

#### 2.1. Poste serveur "DMZ"

#### 2.1.1. Configuration IP

Au début du projet, ce poste comporte 2 cartes réseaux, une pour aller sur internet et donc pouvoir télécharger les paquets nécessaire et l'autre qui est dans le même réseau que l'interface OPT1 du routeur virtuel.

Lorsque le routeur virtuel est configuré, l'utilisation de la première carte réseau n'est plus nécessaire, donc nous l'enlevons.

- Fichier de configuration des cartes réseaux

GNU nano 3.2	/etc/network/interfaces
# This file desc # and how to act	ribes the network interfaces available on your system ivate them. For more information, see interfaces(5).
source /etc/netw	vork/interfaces.d/*
<pre># The loopback n auto lo iface lo inet lo</pre>	opback
auto eth0	
iface eth0 inet address	static 192.168.43.3
netmask	255.255.255.0
gateway	192.168.43.1
auto ethl	
iface ethl inet	static
address	192.168.1.1
netmask	255.255.255.0



- Vérification des adresses

```
root@dmz:~# ip a
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid lft forever preferred lft forever
    inet6 ::1/128 scope host
       valid lft forever preferred lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:38:01:2c brd ff:ff:ff:ff:ff
    inet 192.168.43.30/24 brd 192.168.43.255 scope global eth0
       valid lft forever preferred lft forever
    inet6 fe80::215:5dff:fe38:12c/64 scope link
       valid lft forever preferred lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:38:01:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth1
       valid lft forever preferred lft forever
    inet6 fe80::215:5dff:fe38:12d/64 scope link
       valid_lft forever preferred_lft forever
```

```
\rightarrow ok
```

#### 2.1.2. Paramétrage Apache 2

Nous avons au préalable téléchargé le paquet Apache2 et vérifié son bon fonctionnement.

Nous allons donc à présent mettre en place le serveur web composé d'un site web.

- Dans le dossier html, le fichier *index.html* est renommé et un dossier du nom du site est créé, ici bl.



- Dans ce dossier, un fichier *index.html* est rajouté. C'est dans ce dossier que tous les éléments du site internet vont être mis.



- Vérification de l'accès au site avec un navigateur

$\leftarrow \rightarrow C$ $\bigcirc \& 192.168.1.1/bl/$ Boniour de Berger-Levrau	۲	192.168.1.1/bl/	× +
Boniour de Berger-Levrau	$\leftarrow$	$\rightarrow$ G	◯ 🏠 192.168.1.1/bl/
Donjour ut Derger-Leviut	Bo	onjour o	de Berger-Levrault

#### 2.1.3. Configuration du serveur DNS

Le DNS (Domain Name System) a pour fonction principale la traduction des noms de domaines en adresses IP. Il fait correspondre un nom de domaine avec une adresse IP que ce soit pour un site internet mais aussi pour des ordinateurs internes au réseau local.

Pour notre projet, Bind9 et dnsutils ont été installés au préalable sur le poste.

- Le nom FQDN du serveur est renseigné



 Dans le fichier hosts, nous entrons une ligne "localhost", une ligne avec le nom FQDN et l'ip localhost et enfin une ligne avec le nom FQDN et l'ip de notre serveur. Cela permet d'associer l'adresse IPV4 du serveur au nom FQDN.



GNU nano 3.2		/etc/hosts
127.0.0.1 127.0.1.1 192.168.1.1	localhost dmz.bl.lan dmz.bl.lan	

- Nous indiquons le domaine et la zone de recherche dans le fichier résolv.conf



 Déclaration de la zone DNS "bl.lan" et sa zone inverse pour que les adresses IP puissent être traduites en noms de domaines

GNU nano 3.2	/etc/bind/named.conf.local
// // Do any local configuration here //	
// Consider adding the 1918 zones here, if they // organization //include "/etc/bind/zones.rfc1918";	are not used in your
<pre>zone "bl.lan" {     type master;     file "etc/bind/db.bl.lan";     notify yes;</pre>	
};	
<pre>zone "1.168.192.in-addr.arpa" {     type master;     file "/etc/bind/db.1.168.192.in-addr.ar };</pre>	pa";

- Dans le dossier bind, création des fichiers de la zone directe et la zone inversée. Modification des deux fichiers

ESICAD

- zone directe :

GNU nano 3.2

```
$TTL
        10800
$ORIGIN bl.lan.
        IN SOA dmz.bl.lan. root.dmz.bl.lan (
0
        20160505;
        3h;
        1h;
        1w;
        1h)
6
        IN NS
                dmz.bl.lan.
dmz IN A 192.168.1.1
www IN A 192.168.1.1
localhost IN A 127.0.0.1
```

- zone inversée :

GNU na	no 3.2		db.1.168.192.in-addr.arpa
\$TTL 108	00		
\$ORIGIN	1.168.19	92.in-addr.arpa.	
0	IN SOA o	dmz.bl.lan. root.bl.lan. (	
	20160505	5;	
	3h;		
	1h;		
	lw;		
	1h);		
0	IN NS	dmz.bl.lan.	
1	IN PTR	dmz.bl.lan.	

<u>Vérification</u> de la syntaxe des fichiers de configuration named.conf. L'article
 "-z" permet de trouver et vérifier les zones DNS.

```
root@dmz:/etc/bind# named-checkconf -z
zone bl.lan/IN: loaded serial 20160505
zone 1.168.192.in-addr.arpa/IN: loaded serial 20160505
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
```

 $\rightarrow \text{ok}$ 

db.bl.lan



- Vérification du bon fonctionnement du serveur DNS

- zone directe

```
root@dmz:/# dig dmz.bl.lan
: <<>> DiG 9.11.5-P4-5.1+deb10u9-Debian <<>> dmz.bl.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56639
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5be15976f34916d6dd703f0d653f8de4de95d376bce1eb0d (good)
;; QUESTION SECTION:
;dmz.bl.lan.
                                IN
                                         A
;; ANSWER SECTION:
dmz.bl.lan.
                        10800
                                ΤN
                                         Α
                                                 192.168.1.1
;; AUTHORITY SECTION:
bl.lan.
                                IN
                                         NS
                                                 dmz.bl.lan.
                        10800
;; Query time: 0 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: lun. oct. 30 12:05:08 CET 2023
```

```
\rightarrow ok
```

- zone inversée

```
root@dmz:/# dig -x 192.168.1.1
; <<>> DiG 9.11.5-P4-5.1+deb10u9-Debian <<>> -x 192.168.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64987
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
 ; COOKIE: c191d0123f723be518028f71653f8ea2a2118245315819a9 (good)
; QUESTION SECTION:
1.1.168.192.in-addr.arpa.
                                IN
                                         PTR
;; ANSWER SECTION:
1.1.168.192.in-addr.arpa. 10800 IN
                                         PTR
                                                 dmz.bl.lan.
;; AUTHORITY SECTION:
 L.168.192.in-addr.arpa. 10800
                                 IN
                                         NS
                                                 dmz.bl.lan.
;; ADDITIONAL SECTION:
dmz.bl.lan.
                        10800
                                IN
                                         Α
                                                 192.168.1.1
```



- <u>Vérification</u> du bon fonctionnement de notre serveur DNS : ping vers le nom de notre site internet (DNS)

root@dmz:/# ping www.bl.lan PING www.bl.lan (192.168.1.1) 56(84) bytes of data. 64 bytes from dmz.bl.lan (192.168.1.1): icmp\_seq=1 ttl=64 time=0.019 ms 64 bytes from dmz.bl.lan (192.168.1.1): icmp\_seq=2 ttl=64 time=0.042 ms 64 bytes from dmz.bl.lan (192.168.1.1): icmp\_seq=3 ttl=64 time=0.044 ms ^C --- www.bl.lan ping statistics ---3 packets transmitted, 3 received, 0% packet loss, time 31ms rtt min/avg/max/mdev = 0.019/0.035/0.044/0.011 ms

 $\rightarrow ok$ 

#### 2.1.4. Mise en place du protocole HTTPS

Le protocole HTTPS, «Hypertext Transfer Protocol Secure», permet une communication entre le client web et le serveur web chiffrée, donc plus sécurisée qu'avec le protocole HTTP. Ce chiffrement se fait par une extension du protocole TCP, le TLS (anciennement SSL).

Le serveur web, en HTTPS, a un certificat d'authentification qui est envoyé au client web lorsque ce dernier se connecte au site, pour qu'il se connecte au site et que la crédibilité du domaine soit attestée.

Sur notre poste, openssl est installé.

- Activation du ssl au niveau d'Apache2

```
root@dmz:/etc/apache2/sites-available# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module sol.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
```



GNU nano 3.2

 génération clé privée et certificat auto-signé (clé publique) avec une validité de vie d'1 an pour les besoins du projet dans un sous-dossier ssl créé dans le dossier apache2



Dans une situation d'entreprise, nous n'aurions pas utilisé des certificats autosignés mais serions passé par un organisme tel que "Let's ENCRYPT" pour rendre les certificats viables (service payant).

#### Configuration des Virtual Host sur les ports 80 et 443

 Nous copions le fichier " " et le renommons avec le nom de notre domaine.
 Nous le configurons ensuite pour que les personnes allant sur le site soit automatiquement redirigé vers le site en https.

bl conf

Nous notons également les paramétrages pour le port 443.

<virtua< th=""><th>lHost *:80&gt;</th></virtua<>	lHost *:80>
	<pre># The ServerName directive sets the request scheme, hostname and port that # the server uses to identify itself. This is used when creating # redirection URLs. In the context of virtual hosts, the ServerName # specifies what hostname must appear in the request's Host: header to # match this virtual host. For the default virtual host (this file) this # value is not decisive as it is used as a last resort host regardless. # However, you must set it for any further virtual host explicitly. ServerName www.bl.lan</pre>
	ServerAdmin webmaster@localhost DocumentRoot /var/www/html
	Redirect Permanent / https://www.bl.lan/
	<pre># Available loglevels: trace8,, trace1, debug, info, notice, warn, # error, crit, alert, emerg. # It is also possible to configure the loglevel for particular # modules, e.g.</pre>
	<pre># Available loglevels: trace8,, trace1, debug, info, notice, warn, # error, crit, alert, emerg. # It is also possible to configure the loglevel for particular # modules, e.g. #LogLevel info ssl:warn</pre>
	ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined
Emilie '	<pre># For most configuration files from conf-available/, which are # enabled or disabled at a global level, it is possible to # include a line for only one particular virtual host. For example the 12/46 # following line enables the CGI configuration for this host only # after it has been globally disabled with "a2disconf".</pre>

ESICAD	
	<virtualhost *:443=""></virtualhost>
	ServerName www.bl.lan:443 ServerAdmin webmaster@localhost DocumentRoot /var/www/html/bl ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined SSLEngine on SSLCertificateFile /etc/apache2/ssl/apache.crt SSLCertificateKevEile /etc/apache2/ssl/apache.kev
– Activ	ation du site "bl"

```
root@dmz:/etc/apache2/sites-available# a2ensite bl.conf
Enabling site bl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@dmz:/etc/apache2/sites-available# systemctl reload apache2
root@dmz:/etc/apache2/sites-available#
```

		Document	Root /var	/www/h	tml/bl						
		ErrorLog CustomLo SSLEngir SSLCerti	g \${APACHE og \${APACH ne on ificateFil	E_LOG_D HE_LOG_N Le VFile	IR}/erro DIR}/acc /etc/ap	r.log ess.log ache2/s	g combi ssl/apa	ned che.	crt kev		
	<th>alHost&gt;</th> <th>i i i ca concej</th> <th></th> <th>/ e c c / ap</th> <th>denez, s</th> <th>o c, apa</th> <th>ener</th> <th>illey</th> <th></th> <th></th>	alHost>	i i i ca concej		/ e c c / ap	denez, s	o c, apa	ener	illey		
– Activ root( Enabl To ac sys root(	ation du @dmz:/et ling sit ctivate stemctl	c/apache: c/apache: e bl. the new o reload a	2/sites-a configura pache2	vailabl tion, y	le# a2en /ou need	site b to run	l.conf n:	anar			
roota - V <u>érifi</u>	admz:/et	c/apache: c/apache: accès ai	2/sites-a 2/sites-a u site "bl.l	vailabl	https su	ir un nc	avigate	eur w	/eb		
– V <u>érifi</u> A Non sécurisé http	cation:	c/apache: c/apache: accès au	2/sites-a 2/sites-a u site "bl.l	an" en	https su	ir un no	avigate	eur w	veb		
– V <u>érifi</u>	cation:	c/apache: c/apache: accès ai	2/sites-a 2/site "bl.l	an" en	https su		avigate	eur w	veb +		
– V <u>érifi</u>	cation:	c/apache: c/apache: accès ai	2/sites-a 2/site "bl.l	an" en	https su ☆	Ir un nc	avigate	eur w × − & http	/eb +	an	
– V <u>érifi</u> <u>&amp; Non sécurisé</u> http Attention : risqu	e probable of	c/apache: c/apache: accès ai	2/sites-a 2/site "bl.I	an" en	https su ⇒ Bol	lan/ c <b>ijour</b>	ovigate		/eb + ger-L	<sup>an</sup>	ult
− V <u>érifi</u> ∧ Non sécurisé http     Attention : risqu     Firefox a détecté une n     accédez à ce site, des a     e-mails, ou données de	cation : probable c nenace de sécurite ttaquants pourrai o carte bancaire.	c/apache: c/apache: accès ai de sécurité	2/sites-a 2/site "bl.l u site "bl.l	vailabi an" en	https su ⇔ bi ← → Boi	r un nc lan/ כ <b>njour</b>	ovigate		/eb + <b>ger-L</b>	<sup>an</sup> .evra	ult
− Vérifie     Attention : risqu     Firefox a détecté une n     accédez à ce site, des a     e-mails, ou données de     En savoir plus	cation : cation : e probable c nenace de sécurite ttaquants pourrai e carte bancaire.	c/apache: c/apache: accès ai de sécurité é potentielle et n'a ent dérober des inf	2/sites-a 2/sites-a U site "bl.l	vailabi an" en	https su ⇔ bi ← → Bon	r un nc lan/ כ <b>1jour</b>	o <b>de E</b>		/eb + <b>ger-L</b>	<sup>an</sup>	ult
- Vérifie     Attention : risqu     Firefox a détecté une n     accédez à ce site, des a     e-mails, ou données de     En savoir plus	cation : cation : ps://www.bl.lan le probable contraited a carte bancaire.	c/apache: c/apache: accès ai de sécurité é potentielle et n'a ent dérober des inf	2/sites-a 2/sites-a U site "bl.l pas poursuivi vers w formations comme v Retour (recomm	vailabi an" en vww.bl.lan. Si v vos mots de par nandé) Av	https su ⇔ bi ← → Bon rous sse,	ir un nc lan/ כ <b>njour</b>	ovigate		/eb + <b>ger-L</b>	<sup>an</sup>	ult
- Vérifie     Ann sécurisé http     Attention : risqu     Firefox a détecté une n     accédez à ce site, des a     e-mails, ou données de     En savoir plus      www.bl.lan utilise u	admz : /et admz : /et cotion : cotion :	c/apache: c/apache: accès au de sécurité é potentielle et n'a ent dérober des inf	2/sites-a 2/sites-a U site "bl.l pas poursuivi vers w formations comment Retour (recomm	vailabi an" en www.bl.lan. Si v vos mots de par	https su trips	lan/ C	ovigate	eur w	/eb + <b>ger-L</b>	an , <b>evra</b>	ult
- Vérifiu     Ann sécurisé http     Attention : risqu     Firefox a détecté une n     accédez à ce site, des a     e-mails, ou données de     En savoir plus      www.bl.lan utiliseu     Le certificat n'est pi     Code d'arrour utiliseu	ie probable o nenace de sécurite itaquants pourrai a carte bancaire.	c/apache: c/apache: accès au de sécurité é potentielle et n'a ent dérober des inf ité invalide. signé.	2/sites-a 2/sites-a U site "bl.l pas poursuivi vers w formations comment Retour (recomment	vailabi an" en	https su	lan/ C	o <b>de E</b>	eur w	/eb + <b>ger-L</b>	<sup>an</sup>	ult

→ le «risque probable de sécurité » qui apparaît lors de l'entrée dans le site est normal puisque nous avons un certificat auto-signé. Il n'est donc pas reconnu par les navigateurs comme étant sécurisé.  $\rightarrow ok$ 

Emilie Wanaverbecq

### ESICAD 2.1.5. Serveur FTP

Le protocole FTP est prévu pour pouvoir réaliser des uploads et des downloads, c'est a dire pouvoir transférer des fichiers vers un serveur ou pour les télécharger par exemple.

- Installation de proFTPD
- Vérification du statut

```
root@dmz:/# systemctl status proftpd.service

proftpd.service - LSB: Starts ProFTPD daemon
Loaded: loaded (/etc/init.d/proftpd; generated)
Active: active (running) since Mon 2023-10-30 11:37:49 CET; 40min ago
Docs: man:systemd-sysv-generator(8)
Process: 592 ExecStart=/etc/init.d/proftpd start (code=exited, status=0/SUCCESS)
Tasks: 1 (limit: 4689)
Memory: 12.3M
CGroup: /system.slice/proftpd.service
_____691 proftpd: (accepting connections)
```

```
\rightarrow ok
```

 Configuration FTP dans /etc/proftpd/conf.d/ sur le fichier ftp-perso.conf. Nous avons créé ce fichier personnalise au lieu de modifier directement le fichier proftpd.conf pour éviter que la configuration ne soit écrasée par une mise a jour proFTPD.

GNU nano 3.2 ftp-perso.conf
#Nom du serveur ServerName "dmz.bl.lan"
#Message de connexion
DisplayLogin "La connexion au serveur FTP s'est bien effectuéee"
#Désactiver IPV6 UseIPV6 off
#Spécifie le répertoire FTP auquel l'utilisateur est autorisé à accéder DefaultRoot état
#Autoriser la connexion seulement aux membres du groupe "ftpadmin" <limit login=""> DenyGroup !ftpadmin </limit>



- Création du groupe 'ftpadmin'

```
root@dmz:/etc/proftpd/conf.d# addgroup ftpadmin
Ajout du groupe « ftpadmin » (GID 1002)...
Fait.
root@dmz:/etc/proftpd/conf.d#
```

- Ajout de l'utilisateur au groupe 'ftpadmin'

```
root@dmz:~# <mark>adduser annie ftpadmin</mark>
Ajout de l'utilisateur « annie » au groupe « ftpadmin »...
Adding user annie to group ftpadmin
Fait.
```

- <u>Test de connexion</u> à la session administrateur depuis un client FTP, ici Filezilla

Hôte : 192.1	68.1.1	Nom d'ut	ilisateur :	annie		Mot de passe	•	•••••	Port :		Connexi	on rapide 🔻		
Statut : L	e serveur ne	prend pas e	en charge pa	as les c	aractères non	ASCII.								1
Statut : Connecté														
Statut : Récupération du contenu du dossier														
Statut : C	statut : Contenu du dossier « /home/annie » affiché avec succès													
Site local : C	Site local : C:\Users\Fabien\											``		
	🗄 📜 All U	Jsers					^							
	🗄 📜 Defa	ault						📥 <mark>?</mark> home						
	— 📜 Defa	ault User						🗄 📜 an	nie					
	🗄 🖹 Fabi	en												
	🗄 📜 Publ	ic												
<b>.</b>	- 📙 Window	VS												
±-	- Mindow	vs.old												
<b>+ ≦</b>	D: (CCCOM	A_X86FRE_F	R-FR_DV9)				$\sim$							
Nom de fichi	ier	Taille de	Type de fic	hier	Dernière mo	di	^	Nom de fichier		Taille d	Type de	Dernière m	Droits d'	Propriéta
1.								1.						
3D Object	ts		Dossier de	fich	18/09/2023	10:		📕 Bureau			Dossier	16/10/2023	drwxr-xr-x	annie ann
📕 AppData			Dossier de	fich	18/09/2023	10:		Documents			Dossier	16/10/2023	drwxr-xr-x	annie ann
📕 Applicatio	on Data		Dossier de	fich	31/10/2023	13:		Images			Dossier	16/10/2023	drwxr-xr-x	annie ann
🔚 Contacts			Dossier de	fich	18/09/2023	10:		ModÃ <sup></sup> les			Dossier	16/10/2023	drwxr-xr-x	annie ann
📒 Cookies			Dossier de	fich	19/09/2023	12:		Musique			Dossier	16/10/2023	drwxr-xr-x	annie ann
Desktop			Dossier de	fich	18/09/2023	10:		Public			Dossier	16/10/2023	drwxr-xr-x	annie ann
🗄 Document	ts		Dossier de	fich	18/09/2023	10:		📜 TéIéchar	ge		Dossier	16/10/2023	drwxr-xr-x	annie ann
🕹 Download	ds		Dossier de	fich	31/10/2023	13:		📜 Vidéos			Dossier	16/10/2023	drwxr-xr-x	annie ann
Ravorites			Dossier de	fich	18/09/2023	10.	$\checkmark$							
7 fichiors at 2	A dossions Tr	valetata alla	2 003 500 0	ctote				0 docciore	_					



- Vérification de transfert d'un fichier

Site distant : /home/annie/Documents	~	
annie	^	
2 Bureau		
Documents		
- ? Images		
- ? Modèles		
Musique		
TA©IA©chargements	~	
Nom de fichier Taille d Type de Dernière m Droits d' Propriéta		
Tom de nemer lane d Type de Definere n Dibits d Proprieta.		
travail 0 Eichiar 21/10/2022 rur r appie app		
Citation de 6 Cabina Talla Antola de anto		
Selection de l'fichier. Taille totale : 0 oc		
ut 🗾 🔂 FileZilla		
Transferts réussis		
Tous les fichiers ont é	té transfér	és
avec succès		

#### 2.1.6. Php pour Apache2

Nous installons php car le site va utiliser une bdd. Pour que le site puisse utiliser les éléments de la bdd, il faut utiliser le langage php.

- Installation de php pour Apache2





- Vérification de la bonne installation de php —
  - création d'un fichier info.php dans /var/www/html/ avec lignes :



Ouverture dans le navigateur \_

	סר
C 0 & 192 168 1 1/info php 4	(

ystem	Linux dmz.bl.lan 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64		
uild Date	Sep 4 2023 21:49:25		
erver API	Apache 2.0 Handler		
/irtual Directory Support	disabled		
onfiguration File (php.ini) Path	/etc/php/7.3/apache2		
oaded Configuration File	/etc/php/7.3/apache2/php.ini		
can this dir for additional .ini files	/etc/php/7.3/apache2/conf.d		
dditional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php /7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2 /conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-ipon.ini, /etc/php/7.3/apache2/conf.d/20-ipon.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-sysumg.ini, /etc/php/7.3/apache2/conf.d/2		
HP API	20180731		
HP Extension	20180731		
end Extension	320180731		
end Extension Build	API320180731,NTS		
HP Extension Build	API20180731,NTS		
ebug Build	no		
hread Safety	disabled		
end Signal Handling	enabled		
end Memory Manager	enabled		
end Multibyte Support	disabled		
Pv6 Support	enabled		
Trace Support	available, disabled		
legistered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar		
legistered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2		
and the set of the set of the set	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk,		



→ ok (nous supprimons par la suite ce fichier pour éviter d'éventuels problèmes)

#### 2.1.7. Installation de MariaDB

Pour pouvoir accéder au serveur Mariadb, il faut que notre poste puisse être capable de communiquer avec. C'est pour cela que nous allons installer un client. Après quelques recherches, nous ne pouvons pas installer un client MYSQL, nous allons donc installer MariaDB et nous en servir seulement pour nous connecter au serveur Mariadb.

- installation MariaDB
- modification du fichier de configuration '50-serv.cnf' : activation du port d'écoute (3306) et bind-address : 0.0.0.0 pour qu'il ne reste pas en localhost.



Le reste est fait lors de l'installation de MariaDB sur le poste serveur Mariadb.

#### 2.2.Routeur

Le routeur va permettre de faire le lien entre les différents réseaux.

Comme indique dans la partie "**Contexte**", nous avons fait le choix d'utiliser un routeur virtuel.

Pour le mettre en place, il faut l'installer sur une machine virtuelle.



Enter the Optional 1 interface name or 'a' for auto-detection (hn2 a or nothing if finished): hn2



- Attribution d'adresses IP pour chaque interface (option 2 : Set Interface(s) IP address )

- WAN : en DHCP pour aller sur internet
- LAN : ip static : 192.168.100.254
- OPT1 : ip static (serveur dmz) : 192.168.1.254

***	Welcome	to pfSense 2	.7.2-RELEASE	(amd64) on	pfSense ***
Mak	(wan)	-> hn0	-> v4/	/DHCP4: 192	.168.43.222/24
LAM	(lan)	-> hn1	-> v4:	192.168.16	30.254/24
OPT	[1 (opt1)	) –>hn2	-> v4:	192.168.1	.254/24

- Test de ping entre poste serveur DMZ et interface OPT1

root@dmz:/etc/proftpd/conf.d# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.745 ms
^c
192.168.1.254 ping statistics
3 packets transmitted, 3 received, 0% packet loss, time 5ms

#### → ok

- Ping entre Pfsense (OPT1) et poste serveur DMZ

Enter a host name or IP address: 192.168.1.1 PING 192.168.1.1 (192.168.1.1): 56 data bytes 64 bytes from 192.168.1.1: icmp\_seq=0 ttl=64 time=0.775 ms 64 bytes from 192.168.1.1: icmp\_seq=1 ttl=64 time=1.354 ms 64 bytes from 192.168.1.1: icmp\_seq=2 ttl=64 time=0.505 ms --- 192.168.1.1 ping statistics ---3 packets transmitted, 3 packets received, 0.0% packet loss

 $\rightarrow \text{ok}$ 

#### Mettre screen ping avec LAN

Depuis poste DMZ : accès pfsense sur le navigateur

utilisateur : admin mdp : pfsense



Status	/ Dashboard	+ 0
System I	nformation 🥜 🖨 😒	Netgate Services And Support $igodot igodot egi igodot ig$
Name	pfSense.home.arpa	Contract type Community Support
User	admin@192.168.1.1 (Local Database)	Community Support Only
System	Microsoft Azure Netgate Device ID: <b>f6d0613d5c09168d329b</b>	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Dec 12 14:35:37 UTC 2023 €	If you purchased your pfSense gateway firewall appliance from Netgate and elected <b>Community Support</b> at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the <b>NETGATE</b> <b>RESOURCE LIBRARY</b> .

#### 2.3. Serveur de fichiers Windows

Nous devons mettre en place un serveur de fichier. Dans notre cahier des charges, il est spécifié qu'il serait préférable qu'il soit sous Windows.

Nous avons donc installé sur un poste Windows server 2016. Nous avons configuré Active Directory et créé une session utilisateur.

a Gestionnaire de serveur					- 0
Gestionnaire	e de serveur 🔸 Tab	eau de	bord	🕶 🎯   🚩 Gérer O	lutils Afficher Aid
	DIEINVEINUE DAINS GESTIONI	AIRE DE SER	<b>VEUK</b>		
🎹 Tableau de bord					
Serveur local		Configui	rer ce serveur local		
Tous les serveurs	DÉMARRAGE	5			
AD DS	RAPIDE	Aiouter	r des rôles et des fonctio	nnalités	
Services de fichiers et d		, joare			
Services de liciliers et d P		3 Ajouter	r d'autres serveurs à gére	er	
	NOUVEAUTÉS	4 Créer u	in groupe de serveurs		
		Conner	rter ce serveur aux servi	ces cloud	
		Conney	eter ce serveur aux servi		Masquer
	EN SAVOIR PLUS				
F	Rôles et groupes de serveurs Rôles : 3   Groupes de serveurs : 1	Nombre to	tal de serveurs : 1	1 Services de fichiers et de stockage 1	]
	• Facilité de gestion		Facilité de gestion	• Facilité de gestion	
	Événements		Événements	Événements	
	Services		Services	Services	
	Performances		Performances	Performances	
	Résultats BPA		Résultats BPA	Résultats BPA	

Ounsaleurs et ordinaleurs Active	Nom	Туре	Description
> 🦰 Requêtes enregistrées	Administrateurs du schéma	Groupe de séc	Administrateurs désigné
V III BL.local	Admins du domaine	Groupe de séc	Administrateurs désigné
> Builtin	A Contrôleurs de domaine	Groupe de séc	Tous les contrôleurs de
Domain Controllers	Rontrôleurs de domaine clo	Groupe de séc	Les membres de ce grou
ForeignSecurityPrincipale	💐 Contrôleurs de domaine d'e	Groupe de séc	Les membres de ce grou
Managed Service Accourt	💐 Contrôleurs de domaine en l	Groupe de séc	Les membres de ce grou
Users	DefaultAccount	Utilisateur	Compte utilisateur géré
	A DnsAdmins	Groupe de séc	Groupe des administrate
	A DnsUpdateProxy	Groupe de séc	Les clients DNS qui sont
	Editeurs de certificats	Groupe de séc	Les membres de ce grou
	Roupe de réplication dont l	Groupe de séc	Les mots de passe des
	Roupe de réplication dont l	Groupe de séc	Les mots de passe des
	🛃 Invité	Utilisateur	Compte d'utilisateur inv
	🏝 Invités du domaine	Groupe de séc	Tous les invités du dom
	💐 Ordinateurs du domaine	Groupe de séc	Toutes les stations de tra
	Ropriétaires créateurs de la	Groupe de séc	Les membres de ce grou
	Rotected Users	Groupe de séc	Les membres de ce grou
	Serveurs RAS et IAS	Groupe de séc	Les serveurs de ce group
	🐣 Utilisateur1	Utilisateur	

Nous avons rattaché ce serveur au DNS de notre poste serveur DMZ.

Propriétés de : Protocole Internet vers	sion 4 (TCP/IPv4)	×
Général		
Les paramètres IP peuvent être déten réseau le permet. Sinon, vous devez d appropriés à votre administrateur rése	minés automatiquement si votre demander les paramètres IP eau.	
Obtenir une adresse IP automatic	quement	
• Utiliser l'adresse IP suivante :		
Adresse IP :	192 . 168 . 100 . 1	
Masque de sous-réseau :	255 . 255 . 255 . 0	
Passerelle par défaut :	192 . 168 . 100 . 254	
Obtenir les adresses des serveur	s DNS automatiquement	
• Utiliser l'adresse de serveur DNS	suivante :	
Serveur DNS préféré :	127.0.0.1	
Serveur DNS auxiliaire :	192.168.1.1	
Valider les paramètres en quittar	Avancé	
	OK Annule	er

ESICAD



#### - Création du dossier partagé et partage de ce dernier

Nom	Modifié le Type	Tail
<ul> <li>Partage</li> <li>PerfLogs</li> <li>Program Files (x86)</li> <li>Programmes</li> <li>Utilisateurs</li> <li>Windows</li> </ul>	<ul> <li>Propriétés de : Partage</li> <li>Partage avancé</li> <li>Partager ce dossier</li> <li>Paramètres</li> <li>Nom du partage :</li> <li>Partage\$</li> <li>Ajouter Supprimer</li> <li>Limiter le nombre d'utilisateurs simultanés à : 16777 ÷</li> <li>Commentaires :</li> <li>Autorisations Mise en cache</li> </ul>	×

#### - Autorisations pour les utilisateurs

Autorisations pour Partage\$		×	
Autorisations du partage			
Noms de arounes ou d'utilisateurs :			1
R Tout le monde			
Itilisateurs du domaine (BL\Uti	lisateurs du domair	ne)	
			-
	Ajouter	Supprimer	définir
Autorisations pour Utilisateurs du			
domaine	Autoriser	Refuser	
Contrôle total			-
Modifier			
Lecture			



- <u>Vérification</u>: utilisateur d'un autre ordinateur a accès à ce dossier



 $\rightarrow ok$ 

#### 2.4. Serveur Mariadb

Nous sommes à présent sur le poste Mariadb. Nous allons y installer le gestionnaire de bdd, le paramétrer et faire en sorte que le poste serveur dmz puisse se connecter à la bdd.

- Configuration IP

auto lo iface l	o inet lo	popback
auto et iface e	h0 th0 inet	static
	address	192.168.100.2
	netmask	255.255.255.0
	gateway	192.168.100.254

- Installation du paquet "mariadb-server"
- Configuration et sécurisation

root@dbmaria:~# mysql\_secure\_installation



Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? [Y/n] Y
... Success!

Création d'un compte administrateur et attribution de privilèges

MariaDB [(none)]> GRANT ALL PRIVILEGES ON \*.\* TO 'administrateur'@'localhost';
Query OK, 0 rows affected (0,000 sec)



- Tests de l'installation MariaDB en local

```
root@dbmaria:~# systemctl status mariadb.service
mariadb.service - MariaDB 10.3.39 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2023-11-05 15:03:12 CET; 16min ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
 Main PID: 2702 (mysqld)
   Status: "Taking your SQL requests now..."
   Tasks: 31 (limit: 2324)
   Memory: 75.1M
   CGroup: /system.slice/mariadb.service
            -2702 /usr/sbin/mysqld
nov. 05 15:03:12 dbmaria systemd[1]: Starting MariaDB 10.3.39 database server...
nov. 05 15:03:12 dbmaria systemd[1]: Started MariaDB 10.3.39 database server.
nov. 05 15:03:12 dbmaria /etc/mysql/debian-start[2737]: Upgrading MySQL tables if necessary.
root@dbmaria:~#
```

```
\rightarrow ok
```

- Connexion avec session administrateur

```
root@dbmaria:~# mysql -u administrateur -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.3.39-MariaDB-0+deb10ul Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

 $\rightarrow$  MariaDB est opérationnel et utilisateur est capable de s'authentifier avec succès

Par défaut, nous ne pouvons nous connecter sur MariaDB qu'en local. Notre but est de se connecter à un serveur distant (depuis poste serveur dmz dans notre cas).

 Dans/etc/mysql/mariadb.conf.d/50-server.cnf, nous allons modifier la valeur de "bind-address" qui est par défaut en localhost. Nous attribuons la valeur 0.0.0.0 pour que l'accès soit possible de tout poste qui a les identifiants pour s'identifier.



GNU nano 3.2	/etc/mysql/mariadb.conf.d/50-server.cnf
[mysqld]	
#	
# * Basic Settings	
#	
user	= mysql
pid-file	<pre>= /run/mysqld/mysqld.pid</pre>
socket	<pre>= /run/mysqld/mysqld.sock</pre>
port	= 3306
basedir	= /usr
datadir	= /var/lib/mysql
tmpdir	= /tmp
lc-messages-dir	= /usr/share/mysql
#skip-external-lock:	ing
<pre># Instead of skip-n</pre>	etworking the default is now to listen only on
<pre># localhost which is</pre>	<u>s more compati</u> ble and is not less secure.
pind-address	= 0.0.0.0

 Création d'un utilisateur et attribution de droits pour qu'il puisse se connecter depuis le poste dmz sur la bdd "sitebl"

MariaDB [(none)]> <mark>GRANT ALL PRIVILEGES ON sitebl.\* TO 'admin'@'192.168.1.1' IDENTIFIED BY 'motdepasse'</mark> WITH GRANT OPTION; Query OK, 0 rows affected (0,000 sec)

Pour que le serveur dmz puisse se connecter sur la bdd du poste Mariadb, nous devons entrer une règle dans le pare-feu pour accepter la communication sur le port d'écoute 3306.



 <u>Test de connexion</u> du poste dmz (192.168.1.1) vers la bdd hébergée sur le poste Mariadb

```
root@dmz:-# mysql -u admin -p -h 192.168.100.2 -P 3306
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.3.39-MariaDB-0+deb10ul Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

ESICAD

#### 2.6. VPN

Tout d'abord, VPN signifie « Virtual Private Network ». C'est un réseau privé virtuel.

Il va créer un lien virtuel, ici entre l'entreprise et l'ordinateur d'un employé chez lui. Dans ce lien, les données sont isolées et sécurisées de bout en bout. Un employé va donc pouvoir de chez lui accéder à des fichiers importants de l'entreprise en se connectant à distance avec un VPN.

Un VPN masque également l'adresse IP de l'ordinateur de l'utilisateur et utilise une adresse du serveur VPN qui devient donc lui-même l'élément visible sur le net. L'utilisateur est donc moins facilement identifiable avec son adresse IP.

Dans le cadre de ce projet, nous avons décidé d'utiliser OpenVPN. C'est un VPN open source mûr (crée en 2001) et ayant une bonne réputation. Il prend en charge la technologie Open SSL et des clés de cryptages 256bits.

Il est compatible avec beaucoup d'environnements (Linux, Mac, Windows...). Il est plus simple d'utilisation que le VPN Ipsec et est compatible avec davantage de services VPN que WireGuard même s'il est un peu plus lent que ce dernier. Un autre avantage est que le port d'écoute est personnalisable.

Nous avons également choisi ce VPN car il est facilement paramétrable avec le Pfsense.

Dans notre cas, le PC client va établir la connexion à l'aide d'un client OpenVPN auprès du pare-feu Pfsense sur lequel est activé et configuré OpenVPN.

#### 2.5.1. Création de l'autorité certificative et d'un certificat

#### Server

Nous allons, sur PFsense, créer une autorité de certification interne. Puis, nous mettrons en place un certificat "Server".



#### Création de l'autorité de certification interne dans System/Certificate / Autorities. Nous l'appelons "CA-BL-OPENVPN"

System / Cer	tificate / Authorities / Edit 0
Authorities Certifica	ates Revocation
Create / Edit CA	
Descriptive name	CA-BL-OPENVPN The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /,  *, '
Method	Create an internal Certificate Authority
Trust Store	Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Internal Certific	ate Authority
Key type	RSA
	2048
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)	3650
Common Name	bl
	The following certificate authority subject components are optional and may be left blank.
Country Code	FR v
State or Province	e.g. Texas
City	Toulouse
Organization	BL



#### Vérification de l'existence de l'autorité de certification \_

System / Co	ertificate	/ Authorit	ies			0
Authorities Certif	icates Revo	cation				
Search						•
Search term				Both v	Q Search	Clear
	Enter a	search string o	r *nix regular expr	ession to search certificate names and disting	uished names	
Certificate Au	thorities					
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-BL-OPENVPN	~	self-signed	0	O=BL, L=Toulouse, CN=bl, C=FR 🚺		<b>∅</b> ₩₽Ċ面
				Valid From: Tue, 21 Nov 2023 15:32:00 +0000 Valid Until: Fri, 18 Nov 2033 15:32:00 +0000		
						+ Add

System / Ce	ertificate	/ Authorit	ties				0
Authorities Certifi	cates Revo	ocation					
Search							Θ
Search term	Enter a	search string o	or *nix regular eyn	Both	✓	Q Search	Clear
Certificate Aut	horities	i searen sunig e	nix regular exp		nes and disting	uisileu numes	
Name	Internal	Issuer	Certificates	Distinguished Name		In Use	Actions
CA-BL-OPENVPN	~	self-signed	0	O=BL, L=Toulouse, CN=bl, (	C=FR 🚺		<b>∅₩₽</b> Ċ面
				Valid From: <b>Tue, 21 Nov 2023 1</b> Valid Until: <b>Fri, 18 Nov 2033 15</b> :	5:32:00 +0000 32:00 +0000		
							+ Add
dans <mark>S</mark> Lifetime (days)	System	/ Certifico	cate / Ce	r en sappuyant ertificates	sur noi		
dans <mark>S</mark> Lifetime (days)	3650 The lengt Server ce	Certific / Certific th of time the s	igned certificate	ertificates ertificates will be valid, in days. time over 398 days or some pl	SUF NOT	onsider the c	ertificate invalid.
dans <mark>S</mark> Lifetime (days) Common Name	3650 The lengt Server cel	Certific / Certific th of time the s rtificates shou	igned certificate	ertificates will be valid, in days. time over 398 days or some pl	SUF NOT	onsider the c	ertificate invalid.
dans <mark>S</mark> Lifetime (days) Common Name	3650 The lengt Server cer Www.bl.i	Certific / Certific th of time the s rtificates shou lan	at Server cate / Ce igned certificate Id not have a life	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
dans Lifetime (days) <u>Common Name</u> Country Code	3650 The lengt Server ce (www.bl.) The follow	Certific / Certific th of time the s rtificates shou lan wing certificate	igned certificate Id not have a life	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl nents are optional and may be	atforms may c	onsider the c	ertificate invalid.
dans Lifetime (days) <u>Common Name</u> Country Code State or Province	3650 The lengt Server cel Www.bl.l The follow FR	Certific / Certific th of time the s rtificates shou lan wing certificate	at Server	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
dans Lifetime (days) Common Name Country Code State or Province City	3650 The lengt Server cel (www.bl.l The follow (FR (e.g. Texa)	Certific / Certific th of time the s ertificates shou lan wing certificate as e	igned certificate Id not have a life	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
Common Name Country Code State or Province City Organization	3650 The lengt Server cel www.bl.l The follow FR e.g. Texa Toulouse	Certific / Certific th of time the s rtificates shou lan wing certificate as	igned certificate Id not have a life	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
Common Name Country Code State or Province City Organization	System 3650 The lengt Server ce www.bl.l The follow FR e.g. Texa Toulousa BL e.g. My I	Certific / Certific th of time the s rtificates shou lan wing certificate as e	arm (optional)	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
dans Lifetime (days) <u>Common Name</u> Country Code State or Province City Organization rganizational Unit ertificate Attri	System 3650 The lengt Server cel (www.bl.l The follow (FR (e.g. Texa (Toulouse BL (e.g. My I butes	Certific / Certific th of time the s rtificates shou lan wing certificate as e Department Na	arm (optional)	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl	atforms may c	onsider the c	ertificate invalid.
dans Lifetime (days) Common Name Country Code State or Province City Organization rganizational Unit ertificate Attri	System 3650 The lengti Server cel www.bl.l The follow FR e.g. Texa Toulouss BL e.g. My I butes The follow differently	Certific / Certific th of time the s ertificates shou lan wing certificate as e Department Na wing attributes y depending or	arre added to cert	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl nents are optional and may be	atforms may control left blank.	onsider the c	ertificate invalid.
Common Name Country Code Country Code State or Province City Organization rganizational Unit ertificate Attri Attribute Notes	System 3650 The lengti Server cel www.bl.l The follow FR e.g. Texa Toulouse BL e.g. My I butes The follow differently For Intern	Certificates / Certificates th of time the s ertificates shou lan wing certificates as e Department Na wing attributes y depending or hal Certificates,	arr Server cate / Ce igned certificate ld not have a life e subject comport ame (optional) ame (optional)	r en sappuyant ertificates will be valid, in days. time over 398 days or some pl nents are optional and may be v rtificates and requests when th ode.	atforms may control atforms may control atforms may control at a structure at a shown ficate as shown	onsider the c or signed. Th n.	ertificate invalid.

ESĨCAD		
Alternative Names	FQDN or Hostname 🗸	
	Туре	Value
	Enter additional identifiers for the ce an Alternative Name. The signing C/	rtificate in this list. The Common Name field is automatically added to the certificate as A may ignore or change these values.
Add SAN Row	+ Add SAN Row	

#### manque un screen création certificat

- <u>Vérification</u> existence du certificat "Server"

	ates / Certifi	cates		6
Created internal certificate V	/PN-SSL-SRV			Þ
Authorities Certificates (	Certificate Revocati	ion		
Search				e
Search term		Both ~	Q Searc	ch 🎦 Clear
En	ter a search string (	or *nix regular expression to search certificate names and dis	tinguished na	mes.
En Certificates Name	iter a search string ( Issuer	or *nix regular expression to search certificate names and dis Distinguished Name	tinguished na In Use	mes. Actions
En Certificates Name webConfigurator default (654122e804262)	iter a search string ( Issuer self-signed	or *nix regular expression to search certificate names and dis Distinguished Name 0=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-654122e804262	tinguished na In Use	Actions
En Certificates Name webConfigurator default (654122e804262) Server Certificate CA: No Server: Yes	iter a search string ( Issuer self-signed	or *nix regular expression to search certificate names and dis Distinguished Name O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-654122e804262 Valid From: Tue, 31 Oct 2023 15:53:12 +0000 Valid Until: Mon, 02 Dec 2024 15:53:12 +0000	linguished na	Actions
En Certificates Name webConfigurator default (654122e804262) Server Certificate CA: No Server: Yes VPN-SSL-SRV Server Certificate	Issuer self-signed	or *nix regular expression to search certificate names and dis Distinguished Name O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-654122e804262 ① Valid From: Tue, 31 Oct 2023 15:53:12 +0000 Valid Until: Mon, 02 Dec 2024 15:53:12 +0000 O=BL, L=Toulouse, CN=www.bl.lan, C=FR ③	linguished na	Actions

#### 2.5.2. Création d'un utilisateur et d'un certificat utilisateur

Nous allons maintenant créer un utilisateur et générer en même temps un certificat "User" pour qu'il ait l'autorité de se connecter au serveur VPN.

- Création de l'utilisateur dans System / User Managers / Users



#### Jser Manager / Users / Edit

Users	Groups	Settings	Authentication Servers
00010	oroupo	oottingo	riatiferitioation oerreio

User Properties	
Defined by	USER
Disabled	This user cannot login
Username	Test
Password	••••••••
Full name	User's full name, for administrative information only
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	Use individual customized GUI options and dashboard layout for this user.
Group membership	admins

 Au même endroit, nous cochons sur 'Click to create a user certificate'. Ce certificat va également s'appuyer sur notre autorité certificative.

Certificate	Click to create a user certificate	
Create Certificat	e for User	
Descriptive name	VPN-SSL-USER	
Certificate authority	CA-BL-OPENVPN ~	
Key type	RSA v	
	2048 v The length to use when generating a new RSA key, in bits.	
	The Key Length should not be lower than 2048 or some plat	forms may consider the certificate invalid.
Digest Algorithm	sha256 ~	
	The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1 invalid	. Some platforms may consider weaker digest algorithms
Lifetime	3650	

0



#### venucation : existence de l'utilisateur + son certificat

	Ŭ	Users			e e
Users Groups Se	ettings Authentica	ation Servers			
Users Username	Fu	ll name	Status	Groups	Actions
🔲 💄 Test	Te	est	~	1000 TO REFE DOC	Ø 💼
VPN-SSL-USER	CA-BL-	O=BL, L=Toulouse, CN=Te	est, C=FR 🚺	User Cert	<b>∅₩₽</b> ∎C
User Certificate CA: <b>No</b>	OPENVPN	Valid From: Mon, 11 Dec 2023 Valid Until: Thu, 08 Dec 2033	10:59:15 +0000 10:59:15 +0000		
Server: No					
2	.5.3. Config	guration du serv	eur VPN		
– Paramé	trage dan	s <mark>VPN / OpenVI</mark>	PN / Servers .		
VPN / OpenV	PN / Servers	s / Edit			C'® 📖 🗏 8
VPN / OpenV	PN / Servers	s / Edit			C'• 🖩 🖲 🕄
VPN / OpenV Servers Clients Cl	PN / Servers	s / Edit des Wizards Client Expo	ort		C 🖲 🖿 🗐 🕄
VPN / OpenV Servers Clients Cl	PN / Servers	s / Edit des Wizards Client Expo	rt		C 🖲 🖿 🗐 🕄
VPN / OpenV Servers Clients Cl General Informat	PN / Servers	s / Edit des Wizards Client Expo	ort		C 🖲 📖 🗐 🕄
VPN / OpenV Servers Clients Cl General Informat Description	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re	ort eference.		C 🖲 🖿 🗃 🕄
VPN / OpenV Servers Clients Cl General Informat Description Disabled	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re erver	ort eference.		C 🖲 🖿 🗐
VPN / OpenV Servers Clients Cl General Informat Description Disabled	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re erver o disable this server without r	ort eference. emoving it from the list.		C 🖲 🔟 🗏 🕄
VPN / OpenV Servers Clients Cl General Informat Description Disabled Unique VPN ID	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re- erver o disable this server without r )	ort eference. emoving it from the list.		
VPN / OpenV Servers Clients Cl General Informat Description Disabled Unique VPN ID Mode Configurat	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re- erver o disable this server without r )	ort eference. emoving it from the list.		
VPN / OpenV Servers Clients Cl General Informat Description Disabled Unique VPN ID Mode Configurat Server mode	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re- erver o disable this server without r ) ( SSL/TLS + User Auth )	erference.		
VPN / OpenV Servers Clients Cl General Informat Description Disabled Unique VPN ID Mode Configurat Server mode Backend for authentication	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re- erver o disable this server without r ) (SSL/TLS + User Auth ) e	eference.		
VPN / OpenV Servers Clients Cl General Informat Description Disabled Unique VPN ID Mode Configurat <u>Server mode</u> <u>Backend for</u> <u>authentication</u>	PN / Servers	s / Edit des Wizards Client Expo this VPN for administrative re- erver o disable this server without r ) (SSL/TLS + User Auth ) e	eference.		



Dans notre cas, le "Server mode" et en Remot Access car nous Jtiliser l'authentification utilisateur et utiliser SSL/TLS.

Endpoint Configu	ration
Protocol	UDP on IPv4 only ~
Interface	WAN   The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	The port used by OpenVPN to receive client connections.

#### Nous changeons le port par défaut pour que cela soit plus sécurisé.

	Use a TLS Key				
	A TLS key enhances security of an OpenVPN connection b perform a TLS handshake. This layer of HMAC authenticat dropped, protecting the peers from attack or unauthorized data.	y requiring both parties to have a common key before a peer can ion allows control channel packets without the proper key to be connections.The TLS Key does not have any effect on tunnel			
	Automatically generate a TLS Key.				
Peer Certificate Authority	CA-BL-OPENVPN				
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be create	ed here: System > Cert. Manager			
OCSP Check	Check client certificates with OCSP				
Server certificate	VPN-SSL-SRV (Server: Yes, CA: CA-BL-OPENVPN)	)			
DH Parameter	2048 bit ~				
Length	Diffie-Hellman (DH) parameter set used for key exchange.	6			
ECDH Curve	Use Default				
	The Elliptic Curve to use for key exchange.				
	The Elliptic Curve to use for key exchange.				
	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default who	en the server uses an ECDSA certificate. Otherwise. seco384r1 is			
Data Encryption Algorithms	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default who AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block)	en the server uses an ECDSA certificate. Otherwise. seco384r1 is			
Data Encryption Algorithms	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default who AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block) ACS-192-CFB8 (192 bit key, 128 bit block) AcS-192-CFB8 (192 bit key, 128 bit block) Available Data Encryption Algorithms Click to add or remove an algorithm from the list	AES-256-GCM Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list			
Data Encryption Algorithms	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default while AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block) Ares-192-CFB8 (192 bit key, 192 bit key	en the server uses an ECDSA certificate. Otherwise. seco384r1 is          AES-256-GCM         Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list         spected by OpenVPN. This list is ignored in Shared Key mode.			
Data Encryption Algorithms	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default while AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AVailable Data Encryption Algorithms Click to add or remove an algorithm from the list The order of the selected Data Encryption Algorithms is re AES-256-CBC (256 bit key, 128 bit block)	en the server uses an ECDSA certificate. Otherwise. seco384r1 is          AES-256-GCM         Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list         spected by OpenVPN. This list is ignored in Shared Key mode.			
Data Encryption Algorithms Fallback Data Encryption Algorithm	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default while AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-128-CFB (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) ACS-192-CFB (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) ACS-192-CFB (192 bit key, 128 bit block) Available Data Encryption Algorithms Click to add or remove an algorithm from the list The order of the selected Data Encryption Algorithms is re <b>1</b> AES-256-CBC (256 bit key, 128 bit block)	en the server uses an ECDSA certificate. Otherwise. seco384r1 is          AES-256-GCM         Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list         spected by OpenVPN. This list is ignored in Shared Key mode.         Image: packets when communicating with clients that do not if Key). This algorithm is automatically included in the Data			
Data Encryption Algorithms Fallback Data Encryption Algorithm	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default while AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AVailable Data Encryption Algorithms Click to add or remove an algorithm from the list The order of the selected Data Encryption Algorithms is re AES-256-CBC (256 bit key, 128 bit block) The Fallback Data Encryption Algorithm used for data charsupport data encryption algorithm negotiation (e.g. Shared Encryption Algorithms list.	en the server uses an ECDSA certificate. Otherwise. seco384r1 is          AES-256-GCM         Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list         spected by OpenVPN. This list is ignored in Shared Key mode.         Image: packets when communicating with clients that do not d Key). This algorithm is automatically included in the Data			



(

IPv4 Tunnel	10.10.10/24
Network	This is the IPv4 virtual network or network type alias with a single entry used for private commu server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable addre assigned to the server virtual interface. The remaining usable addresses will be assigned to cor
	A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which canno This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network	This is the IPv6 virtual network or network type alias with a single entry used for private commu server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the ne 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)	192.168.100.0/24 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separa ranges or host/network type aliases. This may be left blank if not adding a route to the local net
Le rés J VPN est le 10.1	seau sur lequel l'utilisateur sera connecté lorsqu'il se connecter 0.10.0/24.
Nous	rendons ensuite accessible à travers ce tunnel le réseau LA

Pour les phases de tests, nous laissons le nombre de connexions simultanées à 10. Nous adapterons par la suite selon les besoins du client.

Specify the maximum number of clients allowed to concurrently connect to this server.

Clie	ent Settings	
	Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
	Topology	Imet30 Isolated /30 network per client <ul> <li>Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.</li> <li>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".</li> </ul>
Emilie	e Wanaverbe	cq 35/40



Nous activons l'option "Dynamic IP" pour que l'utilisateur, si son adresse IP change lorsqu'il est connecté en VPN, ne perde pas sa connexion au serveur.

En ce qui concerne la topologie, nous choisissons "net30 – Isolated/30 network per client " pour que chaque utilisateur soit isolé dans un sous-réseau. Cela a pour conséquence que les utilisateurs ne peuvent pas communiquer entre eux. C'est une action qui est plus sécurisée mais qui prend 4 adresses IP pour chaque utilisateur (une pour l'ordinateur, une pour le pare-feu, l'adresse de réseau et celle de broadcast).

Advanced Configuration					
Custom options	auth-nocache				
	A.				
	Enter any additional options to add to the OpenVPN server configuration				
	EXAMPLE: push "route 10.0.0.0 255.255.255.0"				

En entrant ce texte, les identifiants ne sont pas mis en cache, ce qui peut être un peu plus sécurisé contre le vol d'identifiants.

- Vérification de l'existence du serveur créé

OpenVPN Servers						
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions	
WAN	UDP4 / 1195 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		<b>₽</b> 0 <b>0</b>	



- Entrer les règles sur le pare-feu pour autoriser le flux VPN et autoriser l'accès aux ressources, ici le serveur de fichiers

Fir	ewa	all / R	ules /	OpenVPN								ш 🗉 😮
Float	ting	WAN	LAN OF	T1 OpenVPN								
Rul	les (	Drag to	Change	order)								
		States	Proto	col Source I	Port	Destination	Port Ga	teway Q	ueue	Schedule	Description	Actions
	~	1/79 Kil	B IPv4	* *	*	*	* *	I	none			ℰℰ©©≣×
Floa	ating	WAN	LAN OP	T1 OpenVPN								
R	ules	(Drag to	) Change	Order)								
R	ules	(Drag to States	) Change Protocol	Order) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
R	ules ×	(Drag to States 0/6 KiB	Change Protocol *	Order) Source Reserved Not assigned by IANA	Port *	Destination *	Port *	Gateway *	Queue	Schedule	Description Block bogon networks	Actions
	×	(Drag to States 0/6 KiB 0/0 B	Protocol * IPv4 TCP	Order) Source Reserved Not assigned by IANA *	Port * *	Destination * 192.168.1.1	Port * 80 (HTTP)	Gateway *	V Queue *	Schedule	Description Block bogon networks	Actions
	vles × ×	(Drag to States 0/6 KiB 0/0 B 0/0 B	Change Protocol * IPv4 TCP	Order) Source Reserved Not assigned by IANA *	Port * * *	Destination  * 192.168.1.1 192.168.1.1	Port  * 80 (HTTP) 443 (HTTPS)	Gateway * ) * *	Queue     *     none     none	Schedule	Description Block bogon networks	Actions Act

#### 2.5.4. Export de la configuration VPN

Nous allons à présent télécharger la configuration sur les postes utilisateurs concernés. Les ordinateurs sont sous Windows 10 professionnel.

- Il est tout d'abord nécessaire de télécharge et installer un paquet permettant aux utilisateurs d'exporter la configuration VPN sur leur poste.



#### System / Package Manager / Installed Packages

Installed Packages Available Packages

In	stalled Packages				
	Name	Category	Version	Description	Actions
~	openvpn-client- export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	亩口 i
				Package Dependencies: Ø openvpn-client-export-2.6.7 Ø openvpn-2.6.8_1 Ø zip-3.0_1 Ø	-

 Dans VPN / OpenVPN / Client Export Utility, nous entrons les données pour l'export.

Server Client Client Specific Overrides Wizards Client Export	
Remote Access Server UDP4:1195 ~	
Client Connection Behavior	
Host Name 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 wignore the option as they are not affected.	II
Advanced	
Additional auth-nocache configuration options	
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semic	olon.
EXAMPLE: remote-random;	

0

### **ESICAD** 2.5.5. Utilisation du client VPN sur un poste utilisateur

Pour avoir le client, nous devons le télécharger depuis Pfsense. Pour cela, dans un premier temps, le poste est sur le réseau LAN. Une fois le client téléchargé, nous ferons en sorte que l'ordinateur ne soit plus sur un réseau de l'entreprise.

- Téléchargement du client OpenVPN

🗾 pfSense.home.arpa - Op	benVPN: ⊂ × +	
C 🔥 Non sécuris	sé   192.168.100.253/vpn_openvpn_export.php	as AP 🏠 🛈 🗲 🔂 🥰
ocaron term		Search Ulear
	Enter a search string or *nix regular expression to searc	h.
OpenVPN Clients	s	
User	Certificate Name	Export
Test	VPN-SSL-USER	<ul> <li>Inline Configurations:</li> <li>Most Clients Android Configurations:</li> <li>Bundled Configurations:</li> <li>Archive Config File Only</li> <li>Current Windows Installers (2.6.7-Ix001):</li> <li>64-bit 232-bit</li> <li>Previous Windows Installers (2.5.9-Ix601):</li> <li>64-bit 232-bit</li> <li>Legacy Windows Installers (2.4.12-Ix601):</li> <li>10/2016/2019 27/8/8.1/2012r2</li> <li>Viscosity Bundle Viscosity Inline Config</li> </ul>

- Installation d'OpenVPN et de la configuration





#### - Connexion avec l'utilisateur créé

🔁 Connexion OpenVPN (pfSense-UDP4-1195-Test-config)	_		$\times$
Etat actuel: En cours de connexion			
Sun Dec 17 11:29:27 2023 OpenVPN 2.4.12 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [P         Sun Dec 17 11:29:27 2000 Minute and the second sec	KCS11][	AEAD] buil	ton
<			>
OpenVPN Déconnecter	GUI 11.2	8.0.0/2.4.12	2
	I	enner	

 L'ordinateur s'est bien connecté au serveur VPN et une adresse du réseau VPN a été attribuée





- <u>Vérification</u>: adresse IP et ping vers le poste serveur de fichiers

Adresse IPv4
Masque de sous-réseau
Passerelle par défaut
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion :         Adresse IPv6 : 2a04:cec0:122a:7f0d:638c:976a:17fb:739d         Adresse IPv6 temporaire : 2a04:cec0:122a:7f0d:5042:524f:69bc:78bc         Adresse IPv6 de liaison locale : fe80::e7ff:be77:766d:eb88%6         Adresse IPv4 : 192.168.43.101         Masque de sous-réseau : 255.255.255.0         Passerelle par défaut : fe80::b2e1:7eff:fe51:151d%6         192.168.43.1
C:\Users\Felix>ping 192.168.100.1
Envoi d'une requête 'Ping' 192.168.100.1 avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=127
<pre>Statistiques Ping pour 192.168.100.1:     Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes :     Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms</pre>
$\rightarrow \text{ok}$

- Accès au serveur de fichier : dans l'explorateur de fichiers, entrer 192.168.100.1

Sécurité Windows
Entrer les informations d'identification réseau
Entrez vos informations d'identification pour vous connecter à : 192.168.100.1
Administrateur ×
••••••
Mémoriser mes informations d'identification
Le nom d'utilisateur ou le mot de passe est incorrect.
OK Annuler

- <u>V</u> e	<u>érification</u> accès aux d	ossiers :			
partage\$					
l Parta	ge Affichage				
👢 <mark>&gt; R</mark> e	éseau > 192.168.100.1 > partage\$			~ <sup>(1)</sup>	Rechercher
* ^	Nom	Modifié le	Туре	Taille	
jem∈ 🖈	Commandes	17/12/2023 13:55	Dossier de fichiers		
nts 🖈	📕 Factures	17/12/2023 13:55	Dossier de fichiers		
*	Test_utilisateur1	21/11/2023 16:19	Document texte	1 Ko	

Ensuite, il aurait fallu mettre en place un 2ème tunnel VPN pour que l'employé, à son domicile, ait accès au serveur web. Pour cela, nous aurions créé un autre certificat serveur, un autre utilisateur avec son certificat.

### 2.6. Règles ACL

ESICAD

Nous allons à présent paramétrer le pare-feu sur le routeur virtuel.

Pour rappel, il faut :

- DMZ (OPT1) : accès au serveur bdd (LAN) et accès internet
- WAN : accès seulement au serveur web
- LAN : accéder au serveur web et à internet en général + seul poste administrateur ait accès au FTP

DMZ (OPT1)

#### ESICAD LAN OPT1 OpenVPN to Change Order) Actions States Protocol Source Port Destination Port Gateway Queue Schedule Description €100 🗖 🗸 0/9 KiB \* \* \* \* \* IPv4 ICMP none 亩× any €100 □ ✓ 0/1.04 IPv4 53 (DNS) \* \* \* \* none accepter dns TCP/UDP MiB 亩× IPv4 TCP €100 🗖 🖌 0/68 KiB \* \* \* 80 (HTTP) \* none accepter accès srv web 80 亩× □ ✓ 0/1.14 IPv4 TCP 443 \* accepter accès srv €∥□0 \* none web 443 MiB (HTTPS) 亩×

#### <u>Vérification</u>

#### Accès internet :

🤩 DM	Z sur LAPTOP-Q3TTMHOC - (	Connexion à un ordina	teur virtuel
Fichie	r Action Média Presse	-papiers Affichage	Aide
<b>8</b>	• • • • • • • • •	כ 😻 👔	
Activ	vités 🛛 🕑 Firefox ESR	•	sam. 10:02
	G Google	× +	
4	→ C	Q Rechercher	avec Google ou saisir une adresse

 Q
 Image: Constraint of the second second

- Accès serveur bdd : cf connexion au serveur bdd page 27

Gma

## ESICAD

#### LAN OPT1 OpenVPN

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
~	0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$
*	0/21 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Accepter dns	҄ €
~	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		port 443 https	҄ €
~	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			҈∜ // [] О́́́ах
~	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<u></u> € / □ О іі ×
~	0/0 B	IPv4 TCP	192.168.100.2	*	192.168.1.1	3306	*	none		Port mysql, communication	҄ ± ́ / □ О іі ×
~	0/0 B	IPv4 TCP	192.168.100.3	*	192.168.1.1	21 (FTP)	*	none		accès ftp port 20 pour 192.168.100.3	҄ ± ́ / □ О іі ×
~	0/0 B	IPv4 TCP	192.168.100.3	*	192.168.1.1	20	*	none		accès ftp port 21 pour 192.168.100.3	҈⊎́/́⊡ О́≣×

#### <u>Vérification</u>



44/46



#### - Accès ftp seulement depuis 192.168.100.3

#### Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . :
 Adresse IPv6 de liaison locale. . . . .: fe80::45a7:4c05:fd08:f52c%9
 ....: fe80::b2e1:7eff:fe51:151d%9
 Passerelle par défaut. . . .
                        192.168.100.253
C:\Users\Administrateur>ftp 192.168.1.1
Connecté à 192.168.1.1.
220 ProFTPD Server (dmz.bl.lan) [192.168.1.1]
200 UTF-8 activé
Utilisateur (192.168.1.1:(none)) : annie
331 Mot de passe requis pour annie
Mot de passe :
230 Utilisateur annie authentifié
ftp>
```

#### Refus depuis un autre poste

```
Carte Ethernet Ethernet :
```

```
      Suffixe DNS propre à la connexion. . . :

      Adresse IPv6. . . . . . . . . . . . . : 2a04:cec0:1222:9979:1875:8dd8:9d1f:e9bb

      Adresse IPv6 de liaison locale. . . . : fe80::1875:8dd8:9d1f:e9bb%9

      Adresse IPv4. . . . . . . . . . . : 192.168.100.1

      Masque de sous-réseau. . . . . . . . : 255.255.255.0

      Passerelle par défaut. . . . . . . . : fe80::b2e1:7eff:fe51:151d%9

      192.168.100.253
```

Carte Tunnel Connexion au réseau local\* 11 :

Statut du média. . . . . . . . . . . . . . . Média déconnecté Suffixe DNS propre à la connexion. . . :

```
C:\Users\Administrateur.WIN-5V6S12CAN6S>ftp 192.168.1.1
> ftp: connect :Délai de connexion dépassé
ftp> _
```

 $\rightarrow ok$ 

#### WAN

Flo	ating	WAN	LAN	OPT1 OpenVPN								
Rules (Drag to Change Order)												
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	٥
	~	0/0 B	IPv4 TCP	*	*	192.168.1.1	80 (HTTP)	*	none			∜ ∕ □ ○ ā×
	~	0/0 B	IPv4 TCP	*	*	192.168.1.1	443 (HTTPS)	*	none			<b>∛ ৶</b> ⊘ ≣×