Intégration des Certificats — Projet DMZ

pfSense (Fgtw + Bgtw) · OpenVPN · Apache2 · Équipe 2 · m2l.fr

Vue d'ensemble — Ce que l'on crée

#	Nom	Type	Crée sur	Utilisé sur
1	CA-M2L-2	CA racine	Bgtw	Toute la PKI
2	Fgtw.pub.https	Serveur	Bgtw	Fgtw — GUI HTTPS
3	Fgtw.vpna	Serveur	Bgtw	Fgtw — OpenVPN admin
4	Fgtw.vpnd	Serveur	Bgtw	Fgtw — OpenVPN dev
5	WebR.https	Serveur	Bgtw	WebR — Apache2 TLS
6	Bdd.https	Serveur	Bgtw	Bdd — MariaDB TLS
7	Bgtw.adm.https	Serveur	Bgtw	Bgtw — GUI HTTPS
8	adm.vpna	Client (Amine)	Bgtw	adm.vpn — .ovpn
9	dev.vpnd	Client (Dave)	Bgtw	dev.vpn — .ovpn

PARTIE 1 — Créer la PKI sur Bgtw

1.1 — Créer l'autorité de certification (CA)

Aller dans : System > Cert Manager > CAs > + Add

Champ	Valeur à saisir
Descriptive Name	CA-M2L-2
Method	Create an internal Certificate Authority
Key type / Length	RSA / 4096
Digest Algorithm	SHA256
Lifetime (days)	3650
Common Name (CN)	CA-M2L-2
Country Code	FR
Organisation	M2L

Cliquer Save. Le CA apparait dans la liste.

1.2 — Exemple : créer un certificat serveur (ici Fgtw.pub.https)

Aller dans : System > Cert Manager > Certificates > + Add/Sign

Champ	Valeur à saisir
Method	Create an internal Certificate
Descriptive Name	Fgtw.pub.https
Certificate Authority	CA-M2L-2 ← toujours choisir votre CA
Type	Server Certificate
Key type / Length	RSA / 2048
Digest Algorithm	SHA256

Lifetime (days)	398
Common Name (CN)	fgtw2.m2l.fr
Alternative Names (SAN)	DNS : fgtw2.m2l.fr

Cliquer Save. Répéter ce processus pour chaque certificat serveur (changer Descriptive Name et CN a chaque fois).

Tableau des CN pour chaque certificat serveur :

Descriptive Name	Common Name (CN)	SAN DNS
Fgtw.pub.https	fgtw2.m2l.fr	fgtw2.m2l.fr
Fgtw.vpna	vpna.fgtw2.m2l.fr	vpna.fgtw2.m2l.fr
Fgtw.vpnd	vpnd.fgtw2.m2l.fr	vpnd.fgtw2.m2l.fr
WebR.https	webr2.m2l.fr	webr2.m2l.fr
Bdd.https	bdd2.m2l.fr	bdd2.m2l.fr
Bgtw.adm.https	bgtw2.m2l.fr	bgtw2.m2l.fr

1.3 — Créer les certificats clients (Amine et Dave)

Aller dans : System > Cert Manager > Certificates > + Add/Sign

Champ	Amine (admin)	Dave (dev)
Method	Create an internal Certificate	Create an internal Certificate
Descriptive Name	adm.vpna	dev.vpnd
Certificate Authority	CA-M2L-2	CA-M2L-2
Type	User Certificate	User Certificate
Common Name (CN)	aystrater	dlopper
Key type / Length	RSA / 2048	RSA / 2048

Cliquer Save pour chacun.

PARTIE 2 — Intégrer les certificats dans Fgtw (pfSense)

2.1 — Exporter depuis Bgtw

Etape 1 — Sur Bgtw : System > Cert Manager > CAs — trouver CA-M2L-2 et cliquer l'icone **Export CA** (telecharger le .crt)

Etape 2 — Sur Bgtw : System > Cert Manager > Certificates — pour chaque cert de Fgtw (Fgtw.pub.https, Fgtw.vpna, Fgtw.vpnd) cliquer **Export Certificate** puis **Export Key**

2.2 — Importer le CA dans Fgtw

Sur Fgtw : System > Cert Manager > CAs > + Add

Champ	Valeur
Method	Import an existing Certificate Authority
Descriptive Name	CA-M2L-2
Certificate data	Coller le contenu du fichier .crt exporte depuis Bgtw

Cliquer Save.

2.3 — Importer les certificats serveurs dans Fgtw

Repeter pour Fgtw.pub.https, Fgtw.vpna, Fgtw.vpnd :

Sur Fgtw : System > Cert Manager > Certificates > + Add

Champ	Valeur
Method	Import an existing Certificate
Descriptive Name	Fgtw.pub.https (ou vpna / vpnd selon le cert)
Certificate data	Coller le .crt correspondant
Private key data	Coller la .key correspondante

Cliquer Save. Verifier que le CA affiché est bien CA-M2L-2.

2.4 — Appliquer le cert HTTPS sur la GUI Fgtw

Sur Fgtw : System > Advanced > Admin Access

Etape 1 — Dans le champ **SSL/TLS Certificate** : choisir **Fgtw.pub.https**

Etape 2 — Cliquer Save — pfSense redemarre la GUI en HTTPS avec le nouveau cert

Reconnectez-vous. Le navigateur doit reconnaitre le cert signe par CA-M2L-2 (installer le CA dans le navigateur si necessaire).

PARTIE 3 — Intégrer les certificats dans OpenVPN (sur Fgtw)

3.1 — Associer les certificats aux serveurs VPN

Sur Fgtw : VPN > OpenVPN > Servers — editer chaque serveur

Serveur VPN	Champ a modifier	Valeur
VpnA (port 1199)	Peer Certificate Authority	CA-M2L-2
VpnA (port 1199)	Server Certificate	Fgtw.vpna
VpnD (port 1200)	Peer Certificate Authority	CA-M2L-2
VpnD (port 1200)	Server Certificate	Fgtw.vpnd

Cliquer Save sur chaque serveur.

3.2 — Créer les utilisateurs VPN sur Fgtw (nécessaire pour SSL/TLS + User Auth)

Sur Fgtw : System > User Manager > + Add

Champ	Amine	Dave
Username	aystrater	dlopper
Password	(choisir un mdp fort)	(choisir un mdp fort)
Certificate	adm.vpna ← clic + pour associer	dev.vpnd ← clic + pour associer

Le certificat client doit etre presente au format User Certificate (cree en partie 1.3). L'associer directement dans le profil utilisateur.

3.3 — Exporter les profils .ovpn pour les clients

Sur Fgtw : VPN > OpenVPN > Client Export

Etape 1 — Selectionner le serveur (VpnA pour Amine, VpnD pour Dave)

Etape 2 — Dans la liste des utilisateurs : cliquer **Inline Configurations > Most Clients** pour telecharger le .ovpn

Etape 3 — Le fichier .ovpn contient : adresse serveur + port + CA + cert client + cle client + cle TLS — tout en un seul fichier

Etape 4 — Transmettre le fichier .ovpn a l'utilisateur. Il l'importe dans son client OpenVPN et entre son login/mdp a la connexion

PARTIE 4 — Intégrer le certificat TLS sur WebR (Apache2)

4.1 — Exporter depuis Bgtw et déposer sur WebR

Etape 1 — Sur Bgtw : exporter WebR.https (.crt + .key) + le CA (.crt)

Etape 2 — Copier les fichiers sur WebR via SCP depuis adm.adm :

```
scp webr.https.crt webr.https.key CA-M2L-2.crt aystrater@10.54.2.X:/tmp/
```

Etape 3 — Sur WebR, deplacer les fichiers :

```
sudo mv /tmp/webr.https.crt /etc/ssl/certs/webr.crt
sudo mv /tmp/webr.https.key /etc/ssl/private/webr.key
sudo mv /tmp/CA-M2L-2.crt /etc/ssl/certs/CA-M2L-2.crt
sudo chmod 640 /etc/ssl/private/webr.key
```

4.2 — Configurer le VirtualHost Apache2

Etape 1 — Activer le module SSL :

```
sudo a2enmod ssl
```

Etape 2 — Editer ou créer /etc/apache2/sites-available/glpi-ssl.conf :

```
<VirtualHost *:443>
   ServerName webr2.m2l.fr
   DocumentRoot /var/www/html/glpi
   SSLEngine on
   SSLCertificateFile /etc/ssl/certs/webr.crt
   SSLCertificateKeyFile /etc/ssl/private/webr.key
   SSLCACertificateFile /etc/ssl/certs/CA-M2L-2.crt
</VirtualHost>
```

Etape 3 — Activer le site et redemarrer :

```
sudo a2ensite glpi-ssl.conf && sudo systemctl restart apache2
```

Verifier avec : sudo apache2ctl configtest → doit afficher Syntax OK

4.3 — Redirection HTTP vers HTTPS (optionnel mais recommande)

```
Dans le VirtualHost port 80 (glpi.conf), ajouter :
Redirect permanent / https://webr2.m2l.fr/
```

PARTIE 5 — Installer le CA dans les navigateurs / OS clients

Exporter le CA depuis Bgtw : System > Cert Manager > CAs > Export CA (fichier CA-M2L-2.crt)

Sur Windows 10 (Otto, Dave)

Etape 1 — Double-cliquer sur CA-M2L-2.crt

Etape 2 — Installer le certificat > Ordinateur local > Autorites de certification racines de confiance

Etape 3 — Valider. Firefox : about:config > security.enterprise_roots.enabled = true

Sur Kali Linux (Amine)

```
sudo cp CA-M2L-2.crt /usr/local/share/ca-certificates/CA-M2L-2.crt
sudo update-ca-certificates
```

Pour Chromium/Firefox sur Kali : importer manuellement dans Preferences > Privacy > Certificates > Import.

Verification rapide — tout doit passer au vert

Quoi tester	Comment	OK si...
GUI Fgtw HTTPS	https://10.54.2.254 depuis adm.adm	Cadenas vert — cert signe CA-M2L-2
GUI Bgtw HTTPS	https://192.168.102.254 depuis adm.adm	Cadenas vert — cert signe CA-M2L-2
GLPI HTTPS	https://10.54.2.X depuis usr.usr ou usr.wan	Cadenas vert — page GLPI chargee
VPN Amine	Importer adm.vpna.ovpn + connexion avec login	Tunnel monte, ping LAN OK
VPN Dave	Importer dev.vpnd.ovpn + connexion avec login	Tunnel monte, acces WebR+Bdd OK
Cert client oblige	Tenter VPN sans cert (profil sans cert)	Connexion refusee