

Configuration d'un Proxy Inverse Apache dans une DMZ

Objectif

Ce document décrit comment configurer un proxy inverse Apache dans une DMZ pour accéder au portfolio hébergé sur <https://anthony-falla-portfolio-bts-sio.webnode.fr/>, sans disposer du code source.

1. Activer les modules Apache nécessaires

Sur le serveur Apache dans la DMZ, exécutez les commandes suivantes :

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod ssl
sudo systemctl restart apache2
```

2. Créer un hôte virtuel Apache

Créer un fichier : `/etc/apache2/sites-available/portfolio-proxy.conf`

Contenu :

```
<VirtualHost *:80>
    ServerName portfolio.local

    ProxyPreserveHost On
    ProxyPass / https://anthony-falla-portfolio-bts-sio.webnode.fr/
    ProxyPassReverse / https://anthony-falla-portfolio-bts-sio.webnode.fr/

    ErrorLog ${APACHE_LOG_DIR}/proxy_error.log
    CustomLog ${APACHE_LOG_DIR}/proxy_access.log combined
</VirtualHost>
```

Configuration d'un Proxy Inverse Apache dans une DMZ

3. Activer le site proxy

Exécutez les commandes suivantes :

```
sudo a2ensite portfolio-proxy.conf
```

```
sudo systemctl reload apache2
```

4. Ajouter une entrée dans /etc/hosts

Sur les clients, ajoutez cette ligne dans /etc/hosts pour pointer vers le serveur Apache de la DMZ :

```
192.168.20.10 portfolio.local
```

Résultat

Le client peut accéder au portfolio en visitant <http://portfolio.local>, via le proxy inverse Apache dans la DMZ.

Cela permet de sécuriser la DMZ tout en rendant le service disponible sans exposer directement Internet à la DMZ.