Apache Reverse Proxy and Firewall

Install apache2

```
sudo apt install apache2
```

Activate modules

```
sudo a2enmod headers rewrite proxy proxy_html proxy_http ssl vhost_alias
```

Apache Reverse Proxy Configuration

```
sudo vim /etc/apache2/sites-available/dms.yourdomain.de_httpd.conf
```

```
<VirtualHost YOURPUBLICIP:7080 127.0.0.1:7080>
       ServerName dms.yourdomain.de
       RewriteEngine On
       RewriteCond %{HTTPS} off
       RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
</VirtualHost>
<VirtualHost YOURPUBLICIP:7081 127.0.0.1:7081>
        ServerName dms.YOURDOMAIN.de
        ServerAdmin info@YOURDOMAIN.de

        ErrorLog ${APACHE_LOG_DIR}/error-sismics.log
        CustomLog ${APACHE_LOG_DIR}/access-sismics.log combined

        SSLEngine on
        SSLCertificateFile /etc/letsencrypt/live/YOURDOMAIN.de/cert.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/YOURDOMAIN.de/privkey.pem
        SSLCertificateChainFile /etc/letsencrypt/live/YOURDOMAIN.de/chain.pem

        SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
        SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
        SSLHonorCipherOrder On
        Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains;
preload"
```

```
        #Header always set X-Frame-Options DENY
        Header always set X-Content-Type-Options nosniff
        #Header set Content-Security-Policy "default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';"
        Header unset X-Powered-By
        Header set Referrer-Policy "origin-when-cross-origin"
        Header always edit Set-Cookie (.*) "$1; HttpOnly; Secure"
        Header set X-XSS-Protection "1; mode=block"
        Header always set Content-Security-Policy "upgrade-insecure-requests;" #upgrade unsafe gravatar icons to load from https instead of http

        # Requires Apache >= 2.4
        SSLCompression off
        #SSLUseStapling on
        #SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
        # Requires Apache >= 2.4.11
        SSLSessionTickets Off

        ProxyRequests Off

        # Auth changes in 2.4 - see http://httpd.apache.org/docs/2.4/upgrading.html#run-time
        <Proxy *>
                Require all granted
        </Proxy>

        ProxyPass / http://localhost:8080/dms/
        ProxyPassReverse / http://localhost:8080/dms/
        <Location />
             SSLRenegBufferSize 100000000
             Require all granted
       </Location>

       <Location "/api/app">
           AllowOverride None
           Order deny,allow
           Deny from All
       </Location>

       <Location ~ "/api/app/.*">
           AllowOverride None
```

```
            Allow from All
        </Location>

        RewriteEngine on
        RewriteCond %{REQUEST_FILENAME} !-d
        RewriteRule ^(.*)/$ /$1 [R=301,L]
</VirtualHost>
```

Firewall Blocking Rule

Block direct access to Jetty9 on Port 8080 (ingoing and outgoing TCP traffic) to allow access only on SSL secured domain. Use iptables or similar.

Version #1
Erstellt: 2025-05-15 09:15:02 CEST von Mario Voigt
Zuletzt aktualisiert: 2025-05-15 09:16:33 CEST von Mario Voigt