Reverse Proxy Installation auf Debian / Ubuntu

Als Grundlage für den Reverse Proxy wurde ein **Ubuntu 16.04** aufgesetzt. Im folgenden werden alle Schritte nach der fertigen OS Installation zum einrichten des Proxys beschrieben.

Was ist ein Reverse Proxy? *Grundsätzlich handelt es sich bei einem Proxy um eine Kommunikationsschnittstelle im Netzwerk, die Anfragen entgegennimmt und stellvertretend an einen Zielrechner weiterleitet. Ein Reverse Proxy wird nun aber meistens als zusätzliche Sicherheitskomponente vor einen oder mehrere Webserver geschaltet, um Anfragen aus dem Internet stellvertretend entgegen-zunehmen und an einen Backend-Server im Hintergrund weiterzuleiten.*

Eine ausführlichere Beschreibung hier: Reverse-Proxy – Kernkomponente in Sicherheitsarchitekturen

Weitere interessante Hardware für standalone Proxies (Falls kein Odroid gebraucht wird)

System Konfiguration

Schon zu Beginn wird dem Proxy-Server *eine eigene fixe IP* Adresse zugeteilt. Dies ist hierbei sehr wichtig, da der Traffic zu einem späteren Zeitpunkt von **Port 80** HTTP und **Port 443** HTTPS des Routers direkt an den Proxy per Portweiterleitung vermittelt wird.

```
# vim /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.6
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 192.168.1.1
```

Nach erfolgreicher Speicherung, wird das System neugestartet.

```
# init 6
```

Installation der Grundkomponenten

Zu Beginn werden erst einmal alle Grundpakete, welche zum einrichten unseres Proxys gebraut werden installiert. **ACHTUNG: Das Paket "`libapache2-mod-proxy-html`" ist bei Ubuntu `16.04` schon in der Base Installation enthalten!**

```
UBUNTU 14.04:
# apt-get install apache2 libapache2-mod-proxy-html libxml2-dev

UBUNTU 16.04:
# apt-get install apache2 libxml2-dev
```

Aktivierung der Proxy Komponenten aus dem Apache2 Paket.

```
# a2enmod proxy proxy_ajp proxy_http proxy_wstunnel rewrite deflate headers
proxy_balancer proxy_connect proxy_html xml2enc vhost_alias ssl
```

Nun wird Letsencript installiert, damit wir später damit auch unser eigenes SSL Zertifikat generieren können.

```
# apt-get install git-core
```

```
# cd /opt
# git clone https://github.com/letsencrypt/letsencrypt
```

Konfigurieren der Virtual-Hosts

Nun wenn wir die Basis der gebrauchten Pakete installiert haben, können wir im nächsten Schritt die Virtual-Hosts unseres Reverse Proxys definieren. Bei diesem Schritt, ist es **wichtig**, dass wir anfangs nur die *proxy_http.conf* aktivieren, da in der *proxy_http**s**.conf* bereits bei allen Virtual-Host der Zertifikatspfad angegeben ist, würde dies zu einem kritischen Fehler beim restarten des Webservers führen.

Bereinigen der Virtual-Hosts

Zuerst werden die Standart *sites* deaktiviert und gelöscht:

```
# a2dissite 000-default.conf
```

```
# a2dissite default-ssl.conf

# rm /etc/apache2/sites-available/000-default.conf
# rm /etc/apache2/sites-available/default-ssl.conf
```

Hinzufügen der eigenen Virtual-Hosts

Nun werden alle nachfolgenden Virtual-Host-files, welche vom Proxy gebrauchten auf das System nach **/etc/apache2/sites-available/** kopiert.

Stand letzte Sicherung der files vom 17.März 2017

blackgate.org.conf

```
# vim /etc/apache2/sites-available/blackgate.org.conf
```

```
<VirtualHost *:80>
# ServerName blackgate.org
ServerName localhost
 #
   ServerAdmin michael.r467@gmail.com
   DocumentRoot /var/www/html
 #
</VirtualHost>
```

proxy_http.conf

```
# vim /etc/apache2/sites-available/proxy_http.conf
```

```
#-------------------------------------------------------------------------
---------------------
#                             REDIRECTION FOR NON EXISTENT SUBDOMAINS
#-------------------------------------------------------------------------
---------------------
<VirtualHost *:80>
    ServerName blackgate.org
    RewriteEngine On
    RewriteRule ^/?(.*) https://www.blackgate.org/$1 [R,L]
</VirtualHost>
#-------------------------------------------------------------------------
---------------------
<VirtualHost *:80>
    ServerName plexdash.com
```

```
    RewriteEngine On
    RewriteRule ^/?(.*) https://www.plexdash.com/$1 [R,L]
</VirtualHost>


#------------------------------------------------------------------------------
---------------------
#                                        MAIN REDIRECTIONS
#------------------------------------------------------------------------------
---------------------
<VirtualHost *:80>
 ServerName blackgate.org
 #
     ServerAdmin michael.r467@gmail.com

     ServerAlias www.blackgate.org
     ServerAlias su-login.blackgate.org
     ServerAlias serv.blackgate.org
     ServerAlias piwik.blackgate.org

     ServerAlias plexpy.blackgate.org
     ServerAlias plexdash.blackgate.org
     ServerAlias emby.blackgate.org
     ServerAlias stream.blackgate.org
     ServerAlias request.blackgate.org

     ServerAlias cloud.blackgate.org
     ServerAlias ucloud.blackgate.org

     ServerAlias wiki.blackgate.org
     ServerAlias index.blackgate.org
     ServerAlias xxx.blackgate.org
     ServerAlias test.blackgate.org

     RewriteEngine On
     RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>

<VirtualHost *:80>
 ServerName plexdash.com
 #
     ServerAdmin michael.r467@gmail.com

     ServerAlias www.plexdash.com
     ServerAlias demo.plexdash.com
     ServerAlias get.plexdash.com

     RewriteEngine On
     RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>
```

```
#-------------------------------------------------------------------------
---------------------
#                                          WEITERE DIENSTE
#-------------------------------------------------------------------------
---------------------
<VirtualHost *:80>
 ServerName 83.150.6.68
 #
     ProxyPreserveHost On
     ProxyRequests off
     ProxyPass / http://www.google.ch/
     ProxyPassReverse / http://www.google.ch/
</VirtualHost>

<VirtualHost *:80>
 ServerName test.blackgate.org
 #
     ProxyPreserveHost On
     ProxyRequests off
     ProxyPass / http://192.168.1.21/
     ProxyPassReverse / http://192.168.1.21/

 # !!!Wenn ohne HTTPS erwünst ist.
 #    <Proxy http://192.168.1.21/>
 #        Require all granted
 #    </Proxy>
</VirtualHost>
```

proxy_https_blackgate.conf

```
# vim /etc/apache2/sites-available/proxy_https_blackgate.conf
```

```
<IfModule mod_ssl.c>

#-------------------------------------------------------------------------
---------------------
#                                          MAIN SERVICES
#-------------------------------------------------------------------------
---------------------

<VirtualHost *:443>
 ServerName www.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
```

```
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem

     ProxyPass /error_docs !
     ErrorDocument 503 /error_docs/ServiceUnavailable.html

     ProxyPass      /netdata http://192.168.1.23:19999/
     ProxyPassReverse   /netdata http://192.168.1.23:19999/
     ProxyPass      / http://192.168.1.21/
     ProxyPassReverse   / http://192.168.1.21/

     <Proxy http://192.168.1.23:19999/>
             Order deny,allow
             Allow from all
     </Proxy>
     <Proxy http://192.168.1.21/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
     ServerName su-login.blackgate.org
     #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem

     RewriteEngine On
     RewriteCond %{HTTP:Upgrade} =websocket [NC]
     RewriteRule /(.*)ws://192.168.1.11:8080/guacamole/$1 [P,L]
     RewriteCond %{HTTP:Upgrade} !=websocket [NC]
     RewriteRule /(.*)http://192.168.1.11:8080/guacamole/$1 [P,L]

     ProxyPass / http://192.168.1.11:8080/guacamole/ flushpackets=On
     ProxyPassReverse / http://192.168.1.11:8080/guacamole/

     ProxyPassReverseCookiePath /guacamole /

     <Proxy *>
             Order deny,allow
```

```
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName serv.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.21:5066/
     ProxyPassReverse / http://192.168.1.21:5066/
     <Proxy http://192.168.1.21:5066/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName piwik.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://127.0.0.1/
     ProxyPassReverse / http://127.0.0.1/
     <Proxy http://127.0.0.1/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName emby.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
```

```
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.19:8096/
     ProxyPassReverse / http://192.168.1.19:8096/
     <Proxy http://192.168.1.19:8096/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>


#-----------------------------------------------------------------------------
---------------------
#                                        PLEX SERVICES
#-----------------------------------------------------------------------------
---------------------

<VirtualHost *:443>
 ServerName plexpy.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.23:8181/
     ProxyPassReverse / http://192.168.1.23:8181/
     <Proxy http://192.168.1.23:8181/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName plexdash.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
```

```
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.23/plexDash/
     ProxyPassReverse / http://192.168.1.23/plexDash/
</VirtualHost>

<VirtualHost *:443>
 ServerName request.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.23:3000/
     ProxyPassReverse / http://192.168.1.23:3000/
     <Proxy http://192.168.1.23:3000/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName stream.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     Options -Includes -ExecCGI
     LimitRequestBody 512000
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3 +TLSv1.2
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     Header always set X-Frame-Options DENY
     FileETag None
     TraceEnable off
     Header set X-XSS-Protection "1; mode=block"
     Timeout 60
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     <Location /:/websockets/notifications>
        ProxyPass wss://192.168.1.23:32400/:/websockets/notifications
        ProxyPassReverse wss://192.168.1.23:32400/:/websockets/notifications
     </Location>

     <Proxy *>
```

```
        Order deny,allow
        Allow from all
     </Proxy>

     ProxyRequests Off
     ProxyPreserveHost On
     SSLProxyEngine On
     RequestHeader set Front-End-Https "On"
     ProxyPass / http://192.168.1.23:32400/
     ProxyPassReverse / http://192.168.1.23:32400/
</VirtualHost>


#-------------------------------------------------------------------------------
--------------------
#                                        CLOUD SERVICES
#-------------------------------------------------------------------------------
--------------------

<VirtualHost *:443>
 ServerName cloud.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem

     ProxyPass /error_docs !
     ErrorDocument 503 /error_docs/ServiceUnavailable.html

     ProxyPass / http://192.168.1.24/ retry=1 acquire=3000 Timeout=5400
Keepalive=On
     ProxyPassReverse / http://192.168.1.24/
     <Proxy http://192.168.1.24/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName office.blackgate.org:443
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
```

```
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-
SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-
AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-
SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-
SHA:AES256-SHA:DES-CBC3-SHA:!DSS
     SSLHonorCipherOrder on
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     # Encode Slashes
     AllowEncodedSlashes On

     # No SSL-Cert validation!
     SSLProxyEngine On
     SSLProxyVerify None
     SSLProxyCheckPeerCN off
     SSLProxyCheckPeerName off

     # keep host name
     ProxyPreserveHost On

     ProxyPass           / https://192.168.1.24:9980/
     ProxyPassReverse    / https://192.168.1.24:9980/
     # static html, js, images, etc. served from loolwsd
     # loleaflet is the client part of LibreOffice Online
     ProxyPass           /loleaflet https://192.168.1.24:9980/loleaflet
retry=0
     ProxyPassReverse    /loleaflet https://192.168.1.24:9980/loleaflet
     # WOPI discovery URL
     ProxyPass           /hosting/discovery
https://192.168.1.24:9980/hosting/discovery retry=0
     ProxyPassReverse    /hosting/discovery
https://192.168.1.24:9980/hosting/discovery
     # Main websocket
     ProxyPassMatch "/lool/(.*)/ws$" wss://192.168.1.24:9980/lool/$1/ws
     # Admin Console websocket
     ProxyPass   /lool/adminws wss://192.168.1.24:9980/lool/adminws
     # Download as, Fullscreen presentation and Image upload operations
     ProxyPass           /lool https://192.168.1.24:9980/lool
     ProxyPassReverse    /lool https://192.168.1.24:9980/lool

</VirtualHost>
```

```
<VirtualHost *:443>
 ServerName ucloud.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.12/ retry=1 acquire=3000 Timeout=5400
Keepalive=On
     ProxyPassReverse / http://192.168.1.12/
     <Proxy http://192.168.1.12/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>


#-----------------------------------------------------------------------------
---------------------
#                                        OTHER SERVICES
#-----------------------------------------------------------------------------
---------------------

<VirtualHost *:443>
 ServerName xxx.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.14/ retry=1 acquire=3000 Timeout=7200
Keepalive=On flushpackets=On
     ProxyPassReverse / http://192.168.1.14/
     <Proxy http://192.168.1.14/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
```

```
 ServerName index.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.7/
     ProxyPassReverse / http://192.168.1.7/
</VirtualHost>

<VirtualHost *:443>
 ServerName wiki.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.10/
     ProxyPassReverse / http://192.168.1.10/
     <Proxy http://192.168.1.10/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName test.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://192.168.1.26/
     ProxyPassReverse / http://192.168.1.26/
</VirtualHost>
```

```
<VirtualHost *:443>
 ServerName demo.blackgate.org
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
     ProxyPass / http://google.ch/
     ProxyPassReverse / http://google.ch/
     <Proxy *>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

#<VirtualHost *:443>
#     ServerAlias *.blackgate.org
#     SSLEngine on
#     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
#     SSLProtocol All -SSLv2 -SSLv3
#     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
#     SSLCertificateFile /etc/letsencrypt/live/blackgate.org/cert.pem
#     SSLCertificateKeyFile /etc/letsencrypt/live/blackgate.org/privkey.pem
#     SSLCertificateChainFile /etc/letsencrypt/live/blackgate.org/chain.pem
#     RewriteEngine On
#     Redirect 301 / https://www.blackgate.org
#</VirtualHost>


</IfModule>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

proxy_https_plexdash.conf

```
# vim proxy_https_plexdash.conf
```

```


#-------------------------------------------------------------------------
---------------------
#                                       MAIN SERVICES
```

```
#-------------------------------------------------------------------------
--------------------

<VirtualHost *:443>
 ServerName www.plexdash.com
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/plexdash.com/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/plexdash.com/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/plexdash.com/chain.pem

     ProxyPass /error_docs !
     ErrorDocument 503 /error_docs/ServiceUnavailable.html

     ProxyPass          / http://192.168.1.22/
     ProxyPassReverse   / http://192.168.1.22/

     <Proxy http://192.168.1.22/>
             Order deny,allow
             Allow from all
     </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName demo.plexdash.com
 #
     ServerAdmin michael.r467@gmail.com
     SSLEngine on
     SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
     SSLProtocol All -SSLv2 -SSLv3
     Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
     SSLCertificateFile /etc/letsencrypt/live/plexdash.com/cert.pem
     SSLCertificateKeyFile /etc/letsencrypt/live/plexdash.com/privkey.pem
     SSLCertificateChainFile /etc/letsencrypt/live/plexdash.com/chain.pem

     ProxyPass /error_docs !
     ErrorDocument 503 /error_docs/ServiceUnavailable.html

     ProxyPass          /netdata http://192.168.1.23:19999/
     ProxyPassReverse   /netdata http://192.168.1.23:19999/
     ProxyPass          / http://192.168.1.22/_pD-demo/
     ProxyPassReverse   / http://192.168.1.22/_pD-demo/

     <Proxy http://192.168.1.23:19999/>
             Order deny,allow
```

```
                Allow from all
        </Proxy>
        <Proxy http://192.168.1.22/>
                Order deny,allow
                Allow from all
        </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName dev.plexdash.com
 #
        ServerAdmin michael.r467@gmail.com
        SSLEngine on
        SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
        SSLProtocol All -SSLv2 -SSLv3
        Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
        SSLCertificateFile /etc/letsencrypt/live/plexdash.com/cert.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/plexdash.com/privkey.pem
        SSLCertificateChainFile /etc/letsencrypt/live/plexdash.com/chain.pem

        ProxyPass /error_docs !
        ErrorDocument 503 /error_docs/ServiceUnavailable.html

        ProxyPass          /netdata http://192.168.1.23:19999/
        ProxyPassReverse   /netdata http://192.168.1.23:19999/
        ProxyPass          / http://192.168.1.22/_pD-dev/
        ProxyPassReverse   / http://192.168.1.22/_pD-dev/

        <Proxy http://192.168.1.23:19999/>
                Order deny,allow
                Allow from all
        </Proxy>
        <Proxy http://192.168.1.22/>
                Order deny,allow
                Allow from all
        </Proxy>
</VirtualHost>

<VirtualHost *:443>
 ServerName get.plexdash.com
 #
        ServerAdmin michael.r467@gmail.com
        SSLEngine on
        SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
        SSLProtocol All -SSLv2 -SSLv3
        Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload"
        SSLCertificateFile /etc/letsencrypt/live/plexdash.com/cert.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/plexdash.com/privkey.pem
```

```
    SSLCertificateChainFile /etc/letsencrypt/live/plexdash.com/chain.pem

    ProxyPass /error_docs !
    ErrorDocument 503 /error_docs/ServiceUnavailable.html

    ProxyPass          / http://192.168.1.22/_buy/
    ProxyPassReverse   / http://192.168.1.22/_buy/

    <Proxy http://192.168.1.22/>
            Order deny,allow
            Allow from all
    </Proxy>
</VirtualHost>
```

letsencript_dummy.conf

```
# vim /etc/apache2/sites-available/letsencript_dummy.conf
```

```
<VirtualHost *:80>
 ServerName blackgate.org
 #
    ServerAdmin michael.r467@gmail.com

    ServerAlias www.blackgate.org
    ServerAlias su-login.blackgate.org
    ServerAlias serv.blackgate.org
    ServerAlias piwik.blackgate.org

    ServerAlias plexpy.blackgate.org
    ServerAlias plexdash.blackgate.org
    ServerAlias emby.blackgate.org
    ServerAlias stream.blackgate.org
    ServerAlias request.blackgate.org

    ServerAlias cloud.blackgate.org
    ServerAlias office.blackgate.org
    ServerAlias ucloud.blackgate.org

    ServerAlias wiki.blackgate.org
    ServerAlias index.blackgate.org
    ServerAlias xxx.blackgate.org
    ServerAlias test.blackgate.org
   DocumentRoot /var/www/html
 #
</VirtualHost>
```

Aktivieren der dummy.conf

Für den nächsten Schritt, müssen wir die **letsencript_dummy.conf** aktivieren. **Alle anderen sites bleiben deaktiviert.**

```
# a2ensite letsencript_dummy.conf
# service apache2 reload
```

LetsEncript Konfigurieren

Im ersten Schritt, wird nun zuerst ein **neues Zertifikat** für die Domäne “blackgate.org” und deren Sub-Domains des Reverse Proxys generiert. Die **Key-size** setzen wir hier für eine bessere Sicherheit auf **4096** anstatt den herkömmlichen 2048 Bit!

```
# cd /opt/letsencrypt/
```

```
# ./letsencrypt-auto certonly --rsa-key-size 4096 -d blackgate.org -d
xxx.blackgate.org -d cloud.blackgate.org -d su-login.blackgate.org -d
plexpy.blackgate.org -d wiki.blackgate.org -d serv.blackgate.org -d
www.blackgate.org -d stream.blackgate.org -d emby.blackgate.org -d
request.blackgate.org -d index.blackgate.org -d ucloud.blackgate.org -d
piwik.blackgate.org -d plexdash.blackgate.org -d test.blackgate.org
```

Nach erfolgreichem Durchlauf und der Meldung, dass das Zertifikat erfolgreich unter: **/etc/letsencrypt/live/blackgate.org/cert.pem** erstellt wurde, kann mit dem nächsten Schritt weitergefahren werden.

Automatisiertes Key Update

Da das Letsencript Zertifikat nur eine Gültigkeit von drei Wochen hat, wird hier eine automatische Aktualisierung des Zertifikates empfohlen. Dies wird bei mir über einen crontab Eintrag erreicht.

```
# vim /etc/crontab
```

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
```

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.daily )
47 6    * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.weekly )
52 6    1 * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.monthly )

0  12   * * 6   root    /opt/letsencrypt/letsencrypt-auto renew >>
/var/log/le-renew.log
#
```

Scharf schalten der Proxy Konfiguration

Wenn bis hierhin alles funktioniert hat; kann nun die proxy_dummi.conf deaktiviert werden und der eigentliche Proxy scharf geschalten werden.

```
# a2dissite letsencript_dummy.conf

# a2ensite blackgate.org.conf
# a2ensite proxy_http.conf
# a2ensite proxy_https_blackgate.conf
```

```
# service apache2 reload
# rm /etc/apache2/sites-available/letsencript_dummy.conf
```

Der “proxy_https_plexdash.conf” darf erst angeschalten werden, wenn für diesen auch Zertifikate vorhanden sind. (Andernfalls Zertifikat Pfad in dieser conf Datei anpassen.)

Zusätzliche Konfigurationen

Alle hier gemachten Konfigurationsänderungen, haben keinen direkten Einfluss auf die Proxy Funktion. Sie dienen legindlich der Sicherheit und der personalisierung.

Härten des Apache-Proxys

Zum härten des Apache2 Webservers werden wir nun die security.conf Konfigurationsdatei folgendermassen anpassen:

```
# vim /etc/apache2/conf-enabled/security.conf
```

```
# ServerTokens
ServerTokens Prod

ServerSignature Off

# Allow TRACE method
TraceEnable Off

# Setting this header will prevent other sites from embedding pages from
this
# site as frames. This defends against clickjacking attacks.
# Requires mod_headers to be enabled.
#
Header set X-Frame-Options: "sameorigin"
```

```
# service apache2 reload
```

Eigene ErrorPages definieren

Um eigene ErrorPages unter einem Apache Reverse Proxy einzubinden muss **folgendes snipped** in der Hauptkonfigurationsdatei von Apache2 *nach dem letzten </Directory> Eintrag* eingetragen werden:

snippet

```
Alias /error_docs /var/www/error_pages
ProxyPass /error_docs !
ErrorDocument 400 /error_docs/BadRequest.html
ErrorDocument 401 /error_docs/Unauthorized.html
ErrorDocument 403 /error_docs/Forbidden.html
ErrorDocument 404 /error_docs/NotFound.html
ErrorDocument 500 /error_docs/ServerError.html
ErrorDocument 503 /error_docs/server_offline.html
```

```
# vim /etc/apache2/apache2.conf
```

Nach dem speichern, werden anschliessend die besagten ErrorDocs *(Gleiche Namensgebung wie oben; z.B: BadRequest.html)* **nach /var/www/error_pages kopiert**.

ErrorPages:

- error_pages.zip

```
# chown -R www-data:www-data /var/www/error_pages/
```

```
# service apache2 reload
```

Zusätzliche Sub-Domains hinzufügen

Sollen weitere sub-Domains zu den bestehenden hinzugefügt werden, so wird folgendermassen vorgegangen:

1. Anpassen der proxy-sites und neuer Sub-Domain Namen erfassen.

   ```
   # vim /etc/apache2/sites-available/proxy_http.conf
   # vim /etc/apache2/sites-available/proxy_https.conf
   ```

2. Zum letsencript Binary wechseln und den letzten certonly Befehl *(Suchen mit CTRL + R)* mit der am Schluss neu angehängter Domain z.B. "**-d NEU-SUBDOM.DOMAIN.COM**" ausführen.

   ```
   # cd /opt/letsencrypt/
   # ./letsencrypt-auto certonly --rsa-key-size 4096 -d blackgate.org -d
   xxx.blackgate.org -d cloud.blackgate.org -d su-login.blackgate.org -d
   plexpy.blackgate.org -d wiki.blackgate.org -d serv.blackgate.org -d
   www.blackgate.org -d stream.blackgate.org -d emby.blackgate.org -d
   request.blackgate.org -d index.blackgate.org -d ucloud.blackgate.org -d
   proxy.blackgate.org -d plexdash.blackgate.org -d test.blackgate.org -d
   piwik.blackgate.org
   ```

3. Zum Schluss muss noch der Apache Service neu geladen werden, damit das neue Zertifikat angezogen wird.

   ```
    # service apache2 reload
   ```

Setzen der korrekten Timezone

1. Die aktuelle Konfiguration kann mit **`timedatectl`** eingesehen werden.

   ```
   # timedatectl
   ```

   ```
        Local time: Sun 2017-04-23 07:56:23 UTC
    Universal time: Sun 2017-04-23 07:56:23 UTC
          RTC time: Sun 2017-04-23 07:56:25
         Time zone: Etc/UTC (UTC, +0000)
   Network time on: yes
   NTP synchronized: yes
   ```

```
 RTC in local TZ: no
```

2. Auflisten aller verfügbaren Timezones..

```
# timedatectl list-timezones
```

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
...
```

3. **Setzen der neuen, korrekten Timezone:** in meinem Fall: ***Zürich Schweiz***

```
# timedatectl set-timezone Europe/Zurich
```

```
 Local time: Sun 2017-04-23 09:57:37 CEST
  Universal time: Sun 2017-04-23 07:57:37 UTC
        RTC time: Sun 2017-04-23 07:57:39
       Time zone: Europe/Zurich (CEST, +0200)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
```

WakeOnLAN über Proxy automatisieren

```
# apt-get update
# apt-get install etherwake
```

Anschliessend, müssen nuch noch die Etherwake einträge in der crontab mit der korrekten MAC-Adresse des Ziel Servers erfasst werden.

```
# vim /etc/crontab
```

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
```

```
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.monthly )
#
0  12   * * 6   root    /opt/letsencrypt/letsencrypt-auto renew >>
/var/log/le-renew.log

0  7    * * 1-5   root    etherwake -i eth0 28:92:4a:39:e3:62 && date >>
/var/log/wakeOnLAN.log
0  9    * * 6-7   root    etherwake -i eth0 28:92:4a:39:e3:62 && date >>
/var/log/wakeOnLAN.log

#0  3    * * *   root    reboot
#
```

Last update: **2017/09/19 15:27**