

Reverse http proxy op CentOS7

Een reverse http proxy met apache voor zowel gewoon verkeer als SSL verkeer.

Begin met een [Clone van de CentOS7 minimal](#)

installeer vervolgens apache en SSL:

```
yum install httpd
yum install openssl mod_ssl
```

zet de modules aan in apache:

```
sudo a2enmod ssl
sudo a2enmod rewrite\\
```

Om het dataverkeer te beveiligen met SSL moeten we een certificaat en een key aanmaken. We maken een “self-signed-certificate” omdat een geverifieerd certificaat te duur is voor nu.

Maak de directory aan waar het certificaat wordt opgeslagen:

```
mkdir /etc/httpd/ssl
```

en maak het certificaat en de key aan:

```
openssl req -x509 -nodes -days 1000 -newkey rsa:2048 -keyout
/etc/httpd/ssl/apache.key -out /etc/httpd/ssl/apache.crt
```

Het programma vraagt je om enkele gegevens, waarvan de belangrijkste de “Common Name” is. Vul hier je domeinnaam in:

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:NL
State or Province Name (full name) [Some-State]:Zuid Holland
Locality Name (eg, city) []:Den Haag
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Boerema CI&ND
Organizational Unit Name (eg, section) []:IT Dept.
Common Name (e.g. server FQDN or YOUR name) []:calendar.auriel.nl
Email Address []:support@auriel.nl
```

Vervolgens maken we virtual host files aan:

één voor gewoon web verkeer over poort 80:

vi /etc/httpd/conf.d/default.conf

en zet hierin:

Listen 80

```
<VirtualHost *:80>
    ServerName server-naam.auriel.nl
    ProxyRequests off

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>
    ProxyPass / http://server-naam.auriel.nl/
    ProxyPassReverse / http://server-naam.auriel.nl/
</VirtualHost>
```

en één voor het SSL verkeer, bijvoorbeeld voor de calendar server:

vi /etc/httpd/conf.d/default.conf

Listen 443

```
<VirtualHost *:443>

    ServerName calendar.auriel.nl
    SSLEngine On
    SSLProxyEngine On
    SSLCertificateFile /etc/httpd/ssl/apache.crt
    SSLCertificateKeyFile /etc/httpd/ssl/apache.key

    ProxyRequests off

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>
    ProxyPass / https://calendar.auriel.nl/
    ProxyPassReverse / http://calendar.auriel.nl/

</VirtualHost>
```

Zet de nodige poorten in de firewall open zodat er van buitenaf verbinding kan worden gemaakt:

```
firewall-cmd --permanent --add-port=80/tcp  
firewall-cmd --permanent --add-port=443/tcp  
firewall-cmd --reload
```

harden de httpd install door de volgende entries toe te voegen aan: vi
/etc/httpd/conf.d/options.conf

```
TraceEnable off  
  
## Disable Signature  
ServerSignature Off  
  
## Disable Banner  
ServerTokens Prod
```

en zorg dat de server start:

```
systemctl enable httpd.service  
systemctl restart httpd.service
```

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=installatie_handleidingen:reverse_proxy&rev=1442823025



Last update: **2015/09/21 10:10**