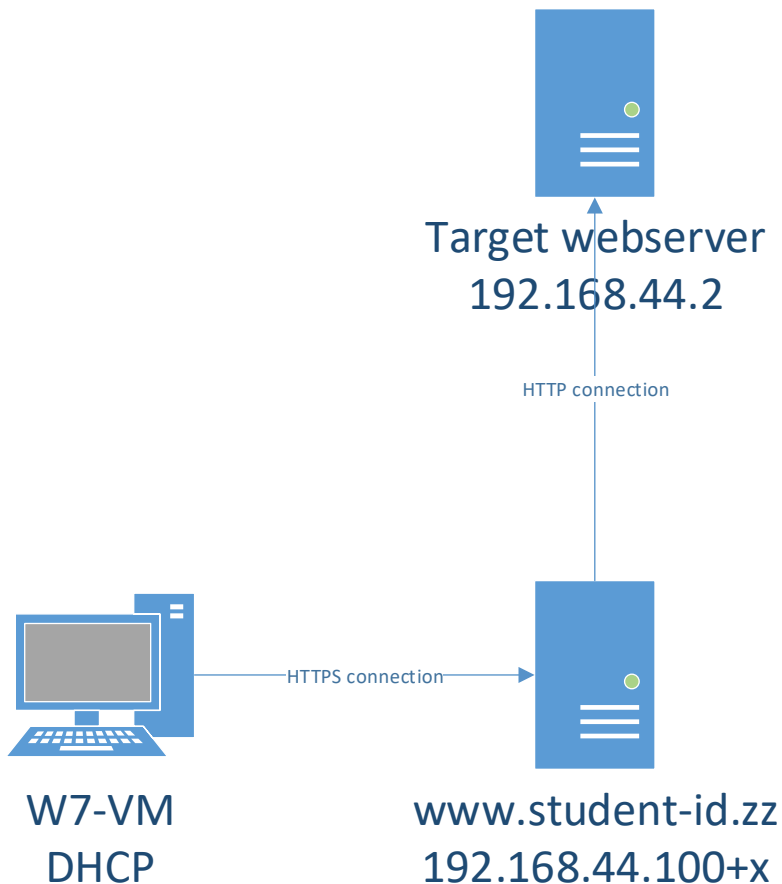## Lab2 – Reverse Proxy

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

The labs use the following topology:

Target webserver
192.168.44.2

HTTP connection

HTTPS connection

W7-VM
DHCP

www.student-id.zz
192.168.44.100+x

All VMs in this lab are in VirtualBox **Bridged** network. The machines that have static IP need to have an offset, check the topology image for reference. USE YOUR WIN7 WORKSTATION IP ADDRESS AS **x**.

Target webserver is handled by teacher. If you are working at home, grab a copy of it from the template folder and set a static IP for it. All templates for VMs can be found in
\\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\
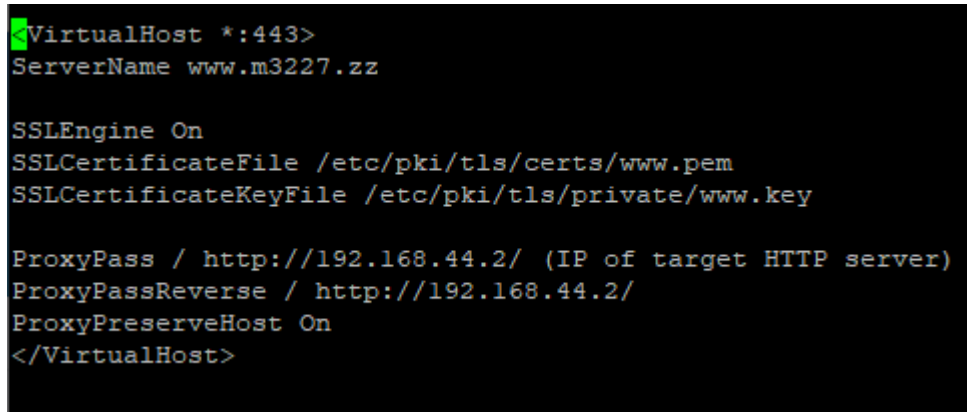
- **Configure SSL Reverse Proxy**

Since we are using Apache to create a reverse proxy, we can use the Apache web server from the previous lab. If for some reason you haven't done Lab1 yet, install Apache + mod_ssl, create a certificate for the webserver and continue from there.

The configuration for a reverse proxy using SSL differs slightly from a generic HTTPS server. First, create a new config file as /etc/httpd/conf.d/proxy.conf and add:

```
<VirtualHost *:443>
        ServerName www.student-id.zz

        SSLEngine On
        SSLCertificateFile … (Point these to the correct key/pem files)
        SSLCertificateKeyFile …

        ProxyPass / http://192.168.44.2/ (IP of target HTTP server)
        ProxyPassReverse / http://192.168.44.2/
        ProxyPreserveHost On
</VirtualHost>
```

```
<VirtualHost *:443>
ServerName www.m3227.zz

SSLEngine On
SSLCertificateFile /etc/pki/tls/certs/www.pem
SSLCertificateKeyFile /etc/pki/tls/private/www.key

ProxyPass / http://192.168.44.2/ (IP of target HTTP server)
ProxyPassReverse / http://192.168.44.2/
ProxyPreserveHost On
</VirtualHost>
```

Reload apache (systemctl restart httpd) and check for errors. Then check by browsing to your server using HTTPS.

This server is target.ttks.local at 192.168.44.2

You are trying to access host **www.m3227.zz** from IP **192.168.44.135**
The connection to the server is via HTTP
The connection is somehow proxied and your real IP address is **192.168.44.115**
Your browser user-agent is Mozilla/5.0 (Windows NT 6.1; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

For more information, see http://php.net/manual/en/reserved.variables.server.php

The server identification string is: apache/2.4.6 (centos) php/5.4.16

- **Header information**

Use Apache Redirect in the *:80 –VirtualHost to redirect HTTP connections to HTTPS automatically. Verify that redirect works. Toimii!: **NOTE!** It is recommended to use Private Browsing to avoid caching errors!

```
<VirtualHost *:443>
ServerName www.m3227.zz

SSLEngine On
SSLCertificateFile /etc/pki/tls/certs/www.pem
SSLCertificateKeyFile /etc/pki/tls/private/www.key

ProxyPass / http://192.168.44.2/
ProxyPassReverse / http://192.168.44.2/
ProxyPreserveHost On
</VirtualHost>

<VirtualHost *:80>
   ServerName www.m3227.zz
   Redirect permanent / https://www.m3227.zz/
</VirtualHost>
```

- **Limiting access and local content**

Try to access /admin –URI on the webserver. Prevent access to this location through the proxy. Use **Location**- parameter in the proxy.conf –file combined with **ProxyPass !**

```
<VirtualHost *:443>
ServerName www.m3227.zz

SSLEngine On
SSLCertificateFile /etc/pki/tls/certs/www.pem
SSLCertificateKeyFile /etc/pki/tls/private/www.key

ProxyPass / http://192.168.44.2/
ProxyPassReverse / http://192.168.44.2/
ProxyPreserveHost On
</VirtualHost>

<VirtualHost *:80>
   ServerName www.m3227.zz
   Redirect permanent / https://www.m3227.zz/
</VirtualHost>

<Location /admin>
ProxyPass !
Require all denied
</Location>
```

Also create a Location –parameter for URI /local and point it to /var/www/html on the local server. Try to access /admin –URI on the webserver. Prevent access to this location through the proxy. Use **Location**-parameter in the proxy.conf –file combined with **ProxyPass !**

```
<Location /admin>
ProxyPass !
Require all denied
</Location>

ProxyPass /local !
Alias /local /var/www/html

<Location /local>
ProxyPass !
Require all denied
</Location>
```

https://www.m3227.zz/local/

Forbidden

You don't have permission to access /local/ on this server.