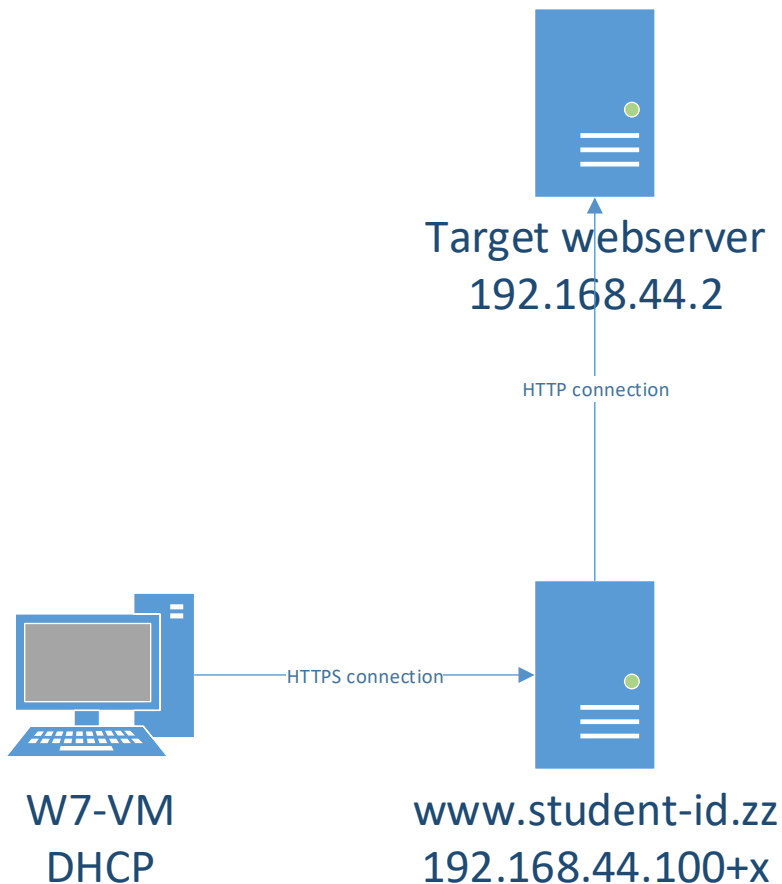


## Lab2 – Reverse Proxy

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:



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>
```

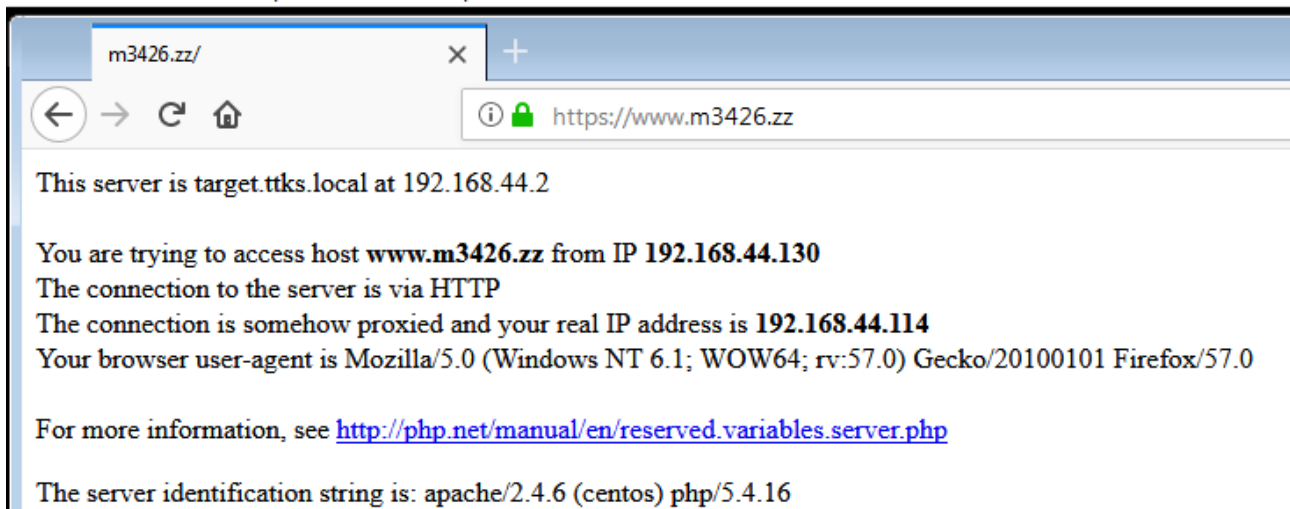
Reload apache (systemctl restart httpd) and check for errors. Then check by browsing to your server using HTTPS.

```
[root@localhost.localdomain ~]# touch /etc/httpd/conf.d/proxy.conf
```

```
<VirtualHost *:443>
ServerName www.M3426.zz

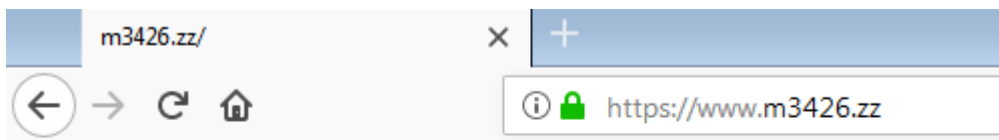
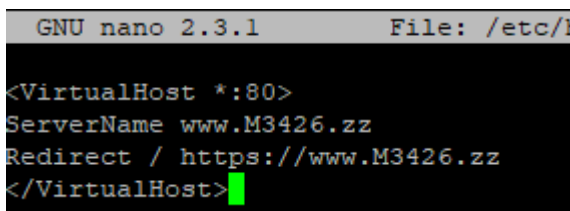
SSLEngine On
SSLCertificateFile /etc/pki/tls/certs/www.pem
SSLCertificateKeyFile /etc/pki/tls/private/www.key

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



### • Header information

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



This server is target.ttk.local at 192.168.44.2

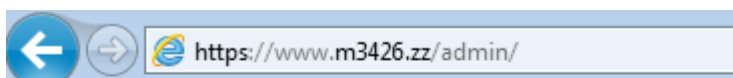
You are trying to access host **www.m3426.zz** from IP **192.168.44.130**

The connection to the server is via HTTP

### • 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 !**

Also create a Location –parameter for URI /local and point it to /var/www/html on the local server.



## Admin panel

This is the admin panel. Access to here should be limited.







# Forbidden



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

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



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

Index of /local



  https://www.m3426.zz/local/

## Index of /local

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>	-	-	
 <a href="#">asdf/</a>	2018-11-21 14:44	-	