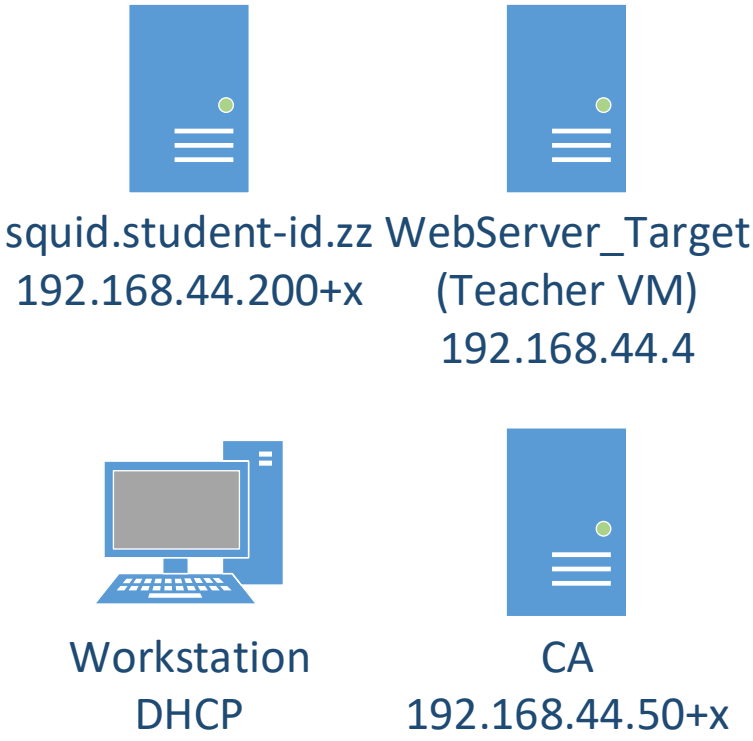
Lab10 – Forward Proxy using Squid

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**.

All templates for VMs can be found in \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\

NOTE! Reuse CA VM and Workstation from previous labs (Certificates) to save time. If you are working at home, you need the WebServer_Target VM also, set the IP manually and make sure you can connect to it directly.

- **Install Squid**

Retrieve the pre-installed VM image for Centos7, \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\. Import it to Virtualbox with the name *Squid* and be sure to set "Reinitialize the MAC address…" tickbox in the import wizard. Remember to check the IP and set the hostname with hostnamectl as in previous labs.

Boot up the VM and login (**root/root66**). Check that it has got an IP. First we will install EPEL repo and then squid:

```
yum install epel-release
yum install squid
```

Start and enable squid and allow it through the firewall:

```
systemctl start squid
systemctl enable squid
firewall-cmd --add-service=squid --permanent
firewall-cmd –reload
```

```
 23  yum install epel-release
 24  yum update
 25  yum install squid
 26  systemctl status squid
 27  systemctl start squid
 28  systemctl star squid
 29  systemctl enable squid
 30  firewall-cmd --add-service=squid --permanent
 31  firewall-cmd --reload
 32  history
```

Then edit Firefox proxy settings. On firefox, you can find them in Options - General – Network Proxy. Set HTTP Proxy and your squid VM IP address, port 3128. Set also "Use this proxy server for all protocols".

NOTE: This will make all traffic go through your proxy. You can use Chrome if this breaks something. Also, please do not visit any important websites when doing this lab and remember to remove this setting from Firefox afterwards.

Let's try the proxy. On Squid VM, run:

```
tail -f /var/log/squid/access.log
```

Now try to access http://student.labranet.jamk.fi/ in your Workstation Firefox browser. You should see the GET requests in the access log. Refresh the page and try some other pages also.

```
[root@localhost.localdomain ~]# tail -f /var/log/squid/access.log
1580984223.201     19 192.168.44.131 TCP_MISS/200 527 GET http://detectportal.fi
refox.com/success.txt - HIER_DIRECT/193.166.4.71 text/plain
1580984266.512      5 192.168.44.131 TCP_MISS/302 676 GET http://student.labrane
t.jamk.fi/ - HIER_DIRECT/195.148.26.130 text/html
```

```
1580984406.853    110 192.168.44.131 TCP_MISS/301 367 GET http://youtube.com/ -
HIER_DIRECT/216.58.207.206 text/html
1580984407.481     68 192.168.44.131 TCP_MISS/200 869 POST http://ocsp.pki.goog/
gtslol - HIER_DIRECT/172.217.20.35 application/ocsp-response
1580984407.705     66 192.168.44.131 TCP_MISS/200 868 POST http://ocsp.pki.goog/
gtslol - HIER_DIRECT/172.217.20.35 application/ocsp-response
```

- **Modifying caching**

If you look at the log and browse multiple sites, you can see a lot of TCP_MISS. This means the pages are not cached (cached pages would be TCP_MEM_HIT). Let's force the squid to cache some elements.

Add caching to disk for more persistent cache. Uncomment and modify the following line in squid.conf:

```
cache_dir ufs /var/spool/squid 250 16 256
```

```
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 250 16 256
```

Also add:

```
maximum_object_size 1024 MB
```

```
maximum_object_size 1024 MB
```

Add a refresh-pattern, which forces images to be cached:

```
refresh_pattern -i \.(gif|png|jpg|jpeg|ico|bmp)$ 260000 90% 260009
override-expire ignore-no-cache ignore-no-store ignore-private
```

```
#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
refresh_pattern -i \.(gif|png|jpg|jpeg|ico|bmp)$ 260000 90% 260009 override-expire ignore-no-cache ignore-no-store ignore-private
```

This will force the images on the page to be cached as they usually are not. Run the following to create cache directories and restart squid:

```
systemctl stop squid
squid -z
systemctl start squid
```

Now clear the browser cache or open a private browsing window. Now see the log again and try refreshing various web pages (iltasanomat, ampparit, telkku.com etc.). You should get at least some TCP_MEM_HIT results.

```
1580987200.926      0 192.168.44.131 TCP_MEM_HIT/200 453 GET http://192.168.44.2/index.txt - HIER_NONE/- text/plain
```

- **Bypassing certain pages**

Try accessing the TestWebServer and see that it gets cached. We can control the squid settings so local content does not get cached. Add a rule that forces direct access in squid.conf:

```
acl webserver dst 192.168.50.4
always_direct allow webserver
cache deny webserver
```

```
# Should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl webserver dst 192.168.44.4
always_direct allow webserver
cache deny webserver
```

Restart squid and see how this changes the caching. Visits to the teachers TestWebServer should now go bypass the proxy.

- Ei tule mem-hittiä

• Configure SSL

If you haven't already, configure a CA like in *Lab1 Certificate*. Make sure the CA is installed as a trusted root CA in the Workstation.

Try to access www.jamk.fi or any other page that uses HTTPS. Squid cannot cache this kind of connection by default as it is SSL protected. We can however make squid act like a CA and write certificates on the fly.

```
1580987620.993     12 192.168.44.131 TCP_MISS/301 300 GET http://jamk.fi/ - HIER_DIRECT/195.148.129.49 -
```

QUESTIONNAIRE: How is a SSL connection shown in the Squid access.log when the proxy is NOT SSL-capable?

- TCP_TUNNEL

First, create a certificate request for the squid server:

```
cd /etc/squid
mkdir ssl_cert
chown squid:squid ssl_cert
chmod 700 ssl_cert
cd ssl_cert
openssl req -new -newkey rsa:2048 -sha256 -days 365 -nodes -extensions\
v3_ca -keyout squidCA.key -out squidCA.csr
```

Set the CN as squid.student-id.zz and Organisation again as ZZ-Tes.

```
[root@localhost.localdomain ssl_cert]# openssl req -new -newkey rsa:2048 -sha256 -days 365 -nodes -extensions v3_ca
keyout squidCA.key -out squidCA.csr
Generating a 2048 bit RSA private key
..............................+++
...........+++
writing new private key to 'squidCA.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) [XX]:squid.m3227.zz
string is too long, it needs to be less than  2 bytes long
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:ZZ-Test
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:squid.m3227.zz
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@localhost.localdomain ssl_cert]# ls
squidCA.csr  squidCA.key
```

Then again transfer this file to the CA and sign it. Note that this will now be an intermediary CA, signed by your previously generated root CA and so it will be trusted by default.

```
[root@elek-424-ws-01.labranet.jamk.fi ca]# scp root@192.168.44.235:/etc/squid/ssl_cert/squidCA.csr ./
```

```
openssl ca -config ca.cnf -extensions v3_ca -days 365 -keyfile ca.key\
-cert ca.pem -in squidCA.csr -out squidCA.pem
```

```
[root@elek-424-ws-01.labranet.jamk.fi ca]# openssl ca -config ca.cnf -extensions v3_ca -days 365 -keyfile ca.key -cert ca.pem -in squidCA.csr -out squidCA.pem
Using configuration from ca.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Feb  6 11:33:18 2020 GMT
            Not After : Feb  5 11:33:18 2021 GMT
        Subject:
            countryName               = XX
            localityName              = Default City
            organizationName          = ZZ-Test
            commonName                = squid.m3227.zz
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                73:6B:87:BE:FB:F1:AF:EB:5D:E5:D2:E0:B4:FA:D5:E2:D7:AF:5B:64
            X509v3 Authority Key Identifier:
                keyid:5F:5B:FC:28:CD:F1:44:92:18:B2:AE:97:F0:CD:71:35:6F:D5:D8:BF

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
Certificate is to be certified until Feb  5 11:33:18 2021 GMT (365 days)
```

Transfer the signed squidCA.pem back to the correct /etc/squid/ssl_cert folder.

```
[root@localhost.localdomain ssl_cert]# scp root@192.168.44.85:ca/squidCA.pem /etc/squid/ssl_cert/
root@192.168.44.85's password:
squidCA.pem                                                   100% 5611     4.4MB
[root@localhost.localdomain ssl_cert]# ls
squidCA.csr  squidCA.key  squidCA.pem
[root@localhost.localdomain ssl_cert]#
```

Next, modify the http_port-line and configure squid to use this CA certificate and do a “SSL-bump” in squid.conf:

```
http_port 3128 ssl-bump cert=/etc/squid/ssl_cert/squidCA.pem
key=/etc/squid/ssl_cert/squidCA.key generate-host-certificates=on
dynamic_cert_mem_cache_size=4MB
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all
```

```
# Squid normally listens to port 3128
http_port 3128 ssl-bump cert=/etc/squid/ssl_cert/squidCA.pem key=/etc/squid/ssl_cert/squidCA.key generate-host-certi$
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all
```

Lastly, create the folder used to store generated certificates:

```
/usr/lib64/squid/ssl_crtd -c -s /var/lib/ssl_db
chown squid:squid -R /var/lib/ssl_db
restorecon -R /var/lib/ssl_db
```

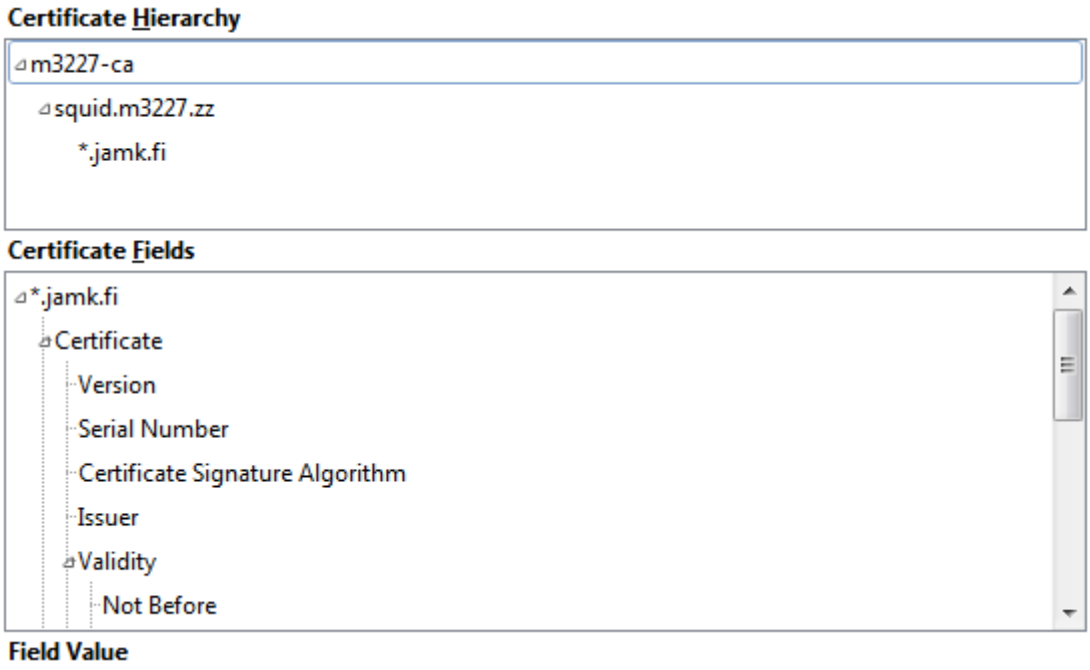
```
[root@localhost.localdomain squid]# /usr/lib64/squid/ssl_crtd -c -s /var/lib/ssl_db
Initialization SSL db...
Done
[root@localhost.localdomain squid]# chown squid:squid -R /var/lib/ssl_db
[root@localhost.localdomain squid]# restorecon -R /var/lib/ssl_db
[root@localhost.localdomain squid]#
```

Restart squid. Try to browse to https://www.jamk.fi. Check the logs that squid sees the traffic (it will not cache it on the first try). Try some other pages too and notice how you won't get a certificate error.

```
1580989805.167     22 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
1580989805.369    193 192.168.44.131 TCP_MISS/200 148270 GET https://www.jamk.fi/fi/Etusivu/ - HIER_DIRECT/195.148.12
9.49 text/html
1580989805.436     28 192.168.44.131 TCP_MISS/200 264991 GET https://www.jamk.fi/handlers/ScriptBundle.ashx? - HIER_D
IRECT/195.148.129.49 application/javascript
1580989805.441     30 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
1580989805.443     24 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
1580989805.508     57 192.168.44.131 TCP_MISS/200 16173 GET https://www.jamk.fi/handlers/ScriptBundle.ashx? - HIER_DI
RECT/195.148.129.49 application/javascript
1580989806.123    676 192.168.44.131 TCP_MISS/200 27559 GET https://www.jamk.fi/static/css/style.less? - HIER_DIRECT/
195.148.129.49 text/css
1580989806.159     33 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
1580989806.160     34 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
1580989806.162     21 192.168.44.131 TAG_NONE/200 0 CONNECT www.jamk.fi:443 - HIER_DIRECT/195.148.129.49 -
```

- tulee paljon kaikkee

When you are finished, check the certificate of the page and take a screenshot of the Certificate Hierarchy path (shown in View Certificate - Details).



QUESTIONNAIRE: How can you distinguish the certificate signed by Squid (other than the issuer field) from the legitimate one?

- signature value