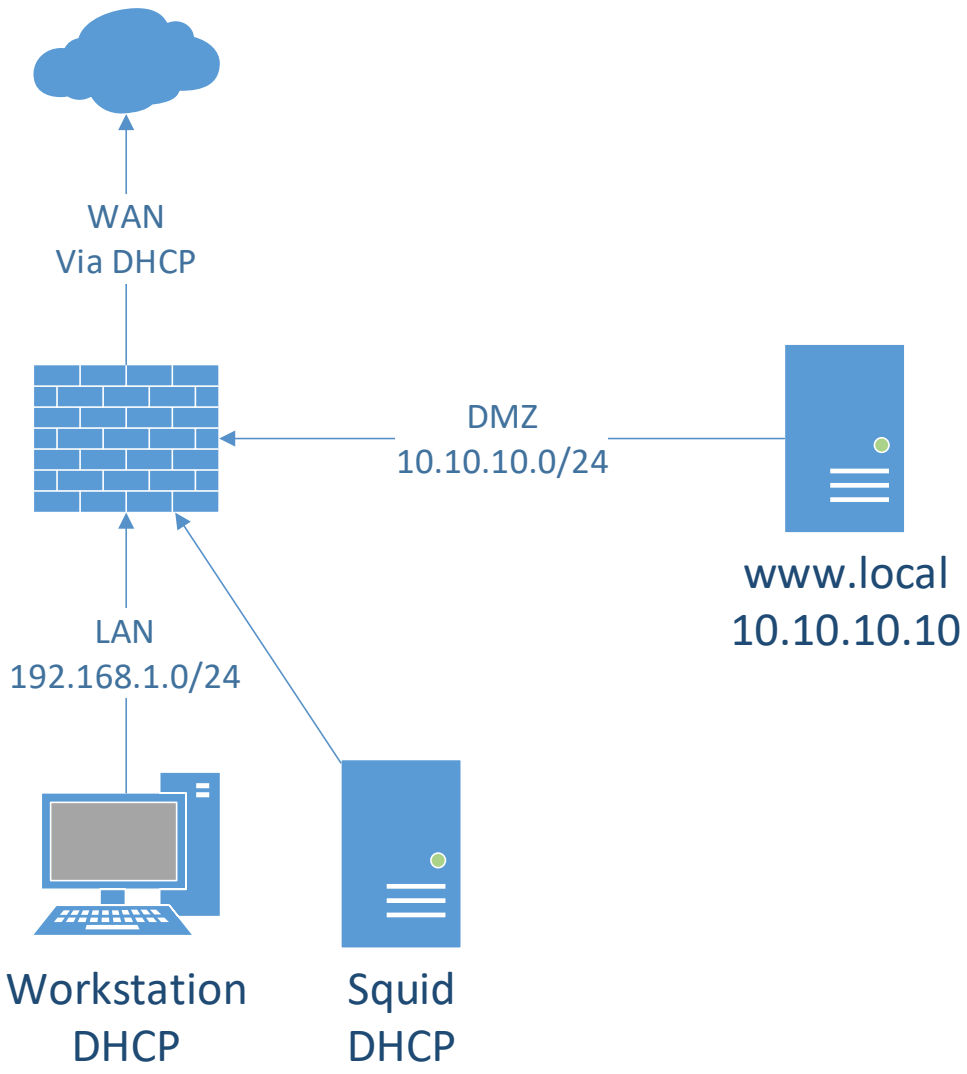
Lab3 – Forward Proxy

Document your commands or take screenshots. Answer questions in english or finnish. Replace student-id with your own student-id in the labs.

The labs use the following topology, some VMs are already installed in the previous labs:



- ## Install Squid (1p)

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. Set VM interface as *Internal network (intnet)*

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
```

```
[root@localhost ~]# yum install -y epel-release squid
```

Edit squid config in /etc/squid/squid.conf and change http_port to 8080

```
  GNU nano 2.3.1            File: /etc/squid/squid.conf

http_access deny all

# Squid normally listens to port 3128
http_port 8080
```

Start and enable squid:

```
systemctl start squid
systemctl enable squid
```

```
[root@localhost ~]# systemctl start squid
[root@localhost ~]# systemctl enable squid
```

Let's create a firewall service for squid. Run:

```
firewall-cmd --new-service=squid -permanent
```

```
[root@localhost ~]# firewall-cmd --new-service=squid --permanent
success
```

Edit newly created /etc/firewalld/services/squid.xml and add following:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Squid</short>
  <description>Squid Web Proxy</description>
  <port protocol="tcp" port="8080"/>
</service>
```

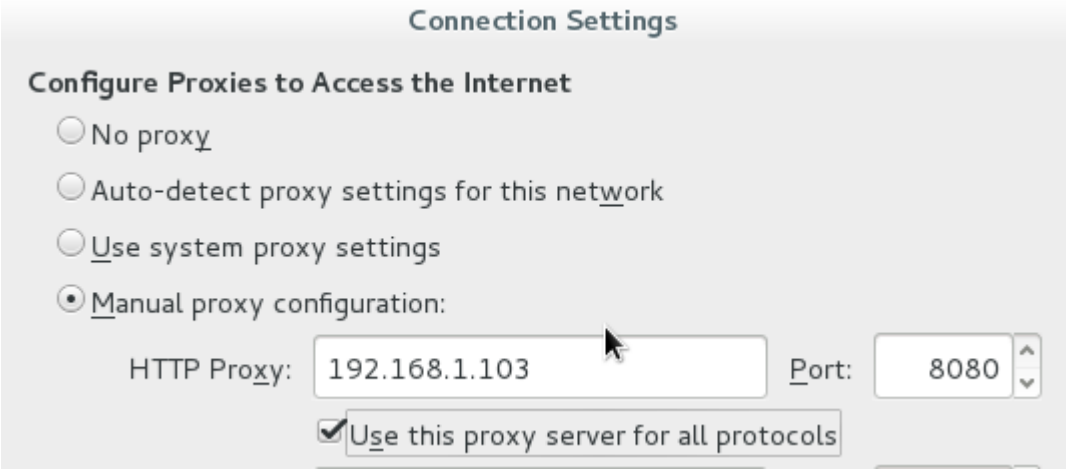
```
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>Squid</short>
<description>Squid Web Proxy</description>
<port protocol="tcp" port="8080"/>_
</service>
```

Save the file, reload the firewall and apply the service:

```
firewall-cmd --reload
firewall-cmd --add-service=squid --permanent
firewall-cmd --reload (Yes it needs to be reloaded again)
```

```
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --add-service=squid --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
```

No boot up your Workstation VM and edit Firefox proxy settings. On firefox, you can find them in Options - Advanced - Network - Settings. Set HTTP Proxy and your IP address, port 8080. Set also “Use this proxy server for all protocols”



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

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

```
1485428545.670   15181 192.168.1.101 TCP_TUNNEL/200 4234 CONNECT pixel.eve
h.net:443 - HIER_DIRECT/66.117.28.68 -
1485428545.671   15578 192.168.1.101 TCP_TUNNEL/200 4234 CONNECT cm.everes
et:443 - HIER_DIRECT/66.117.28.86 -
1485428545.803     830 192.168.1.101 TCP_MISS/200 393 GET http://ping.char
```

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

```
1485428639.329     69 192.168.1.101 TCP_TUNNEL/200 1787 CONNECT student.l
.jamk.fi:443 - HIER_DIRECT/195.148.26.130 -
1485428642.689 122866 192.168.1.101 TCP_TUNNEL/200 6753 CONNECT d2wjg2uht
loudfront.net:443 - HIER_DIRECT/54.192.129.216 -
1485428642.689 122867 192.168.1.101 TCP_TUNNEL/200 6519 CONNECT d2wjg2uht
loudfront.net:443 - HIER_DIRECT/54.192.129.216 -
1485428642.689 123149 192.168.1.101 TCP_TUNNEL/200 15919 CONNECT d2wjg2uh
cloudfront.net:443 - HIER_DIRECT/54.192.129.216 -
```

```
1485428631.020     14 192.168.1.101 TCP_MISS/200 2756 GET http://student.
t.jamk.fi/wp/wp-content/themes/contrast-style/images/page-bg.gif - HIER_D
95.148.26.130 image/gif
```

- **Modifying caching (1p)**

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.

First 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
```

Also add:

```
maxmimum_object_size 1024 MB
```

```
  GNU nano 2.3.1          File: /etc/squid/squid.conf

http_access deny all

# Squid normally listens to port 3128
http_port 8080

# Uncomment and adjust the following to add a disk cache
cache_dir ufs /var/spool/squid 250 16 256
maximum_object_size 1024 MB_
```

Question: Find out from documentation what those number parameters do?

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
```

```
  GNU nano 2.3.1          File: /etc/squid/squid.conf                 Modified

coredump_dir /var/spool/squid

#
# 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-ex$
```

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
```

```
[root@localhost ~]# systemctl stop squid
[root@localhost ~]# squid -z
[root@localhost ~]# 2017/01/26 13:13:58 kid1| Set Current Directory to /var/spoo
l/squid
```

```
systemctl start squid
```

```
[root@localhost ~]# 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.

- **Bypassing certain pages (1p)**

Try accessing your local webserver and see that it gets cached.

```
index/css/fonts/Bold/OpenSans-Bold.woff - HIER_DIRECT/10.10.10.10 text/html
1485429663.764      2 192.168.1.101 TCP_MISS/404 588 GET http://www.k1521.com/no
index/css/fonts/Light/OpenSans-Light.woff - HIER_DIRECT/10.10.10.10 text/html
1485429663.788      3 192.168.1.101 TCP_MISS/404 587 GET http://www.k1521.com/no
index/css/fonts/Light/OpenSans-Light.ttf - HIER_DIRECT/10.10.10.10 text/html
1485429663.788      3 192.168.1.101 TCP_MISS/404 585 GET http://www.k1521.com/no
index/css/fonts/Bold/OpenSans-Bold.ttf - HIER_DIRECT/10.10.10.10 text/html
1485429665.596  15404 192.168.1.101 TCP_TUNNEL/200 821 CONNECT adx.adform.net:44
3 - HIER_DIRECT/152.115.75.199 -
```

We do not want to cache pages from our own webserver. Let' add a rule that forces direct access in squid.conf:

```
acl webserver dst <webserver ip here>
always_direct allow webserver
cache deny webserver
```

```
  GNU nano 2.3.1          File: /etc/squid/squid.conf

#
# Recommended minimum configuration:
#
# Do not allow to be cached
acl webserver dst 10.10.10.10/24
always_direct allow webserver
cache deny webserver
```

Restart squid and see how this changes the caching.

- ## Configure SSL (2p)

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.

First, create a self-signed certificate 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 -x509 -
extensions v3_ca -keyout squidCA.pem -out squidCA.pem
```

```
[root@localhost ~]# cd /etc/squid
[root@localhost squid]# mkdir ssl_cert
[root@localhost squid]# chown squid:squid ssl_cert
[root@localhost squid]# chmod 700 ssl_cert
[root@localhost squid]# cd ssl_cert
[root@localhost ssl_cert]# openssl req -new -newkey rsa:2048 -sha256 -days 365
nodes -x509 -extensions v3_ca -keyout squidCA.pem -out squidCA.pem
```

You can set whatever info you want for the certificate. This will create the file squidCA.pem which will now include both the certificate and the private key.

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

```
http_port 8080 ssl-bump cert=/etc/squid/ssl_cert/squidCA.pem generate-
host-certificates=on dynamic_cert_mem_cache_size=4MB
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all
```

```
  GNU nano 2.3.1          File: /etc/squid/squid.conf                Modified

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-ex$

http_port 8080 ssl-bump cert=/etc/squid/ssl_cert/squidCA.pem generate-host-cert$
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
```

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

You will also have to turn off SELinux for squid:

```
setenforce 0
```

```
[root@localhost ssl_cert]# setenforce 0
```

(There is a better way of handling this so SELinux can stay on, but for lab purposes it is faster to turn it off.)

```
[root@localhost ~]# scp root@192.168.1.103:/etc/squid/ssl_cert/squidCA.pem squid
CA.pem
root@192.168.1.103's password:
Permission denied, please try again.
root@192.168.1.103's password:
squidCA.pem                                   100% 3156     3.1KB/s   00:00
```

```
Putin My Cookie
    nakki                                   Software Security Device
```

Restart squid. Fetch the squidCA.pem certificate from the proxy to your Workstation and import it as a trusted CA. Restart squid and 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.

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

```
1486028105.285    318 192.168.1.101 TCP_TUNNEL/200 5476 CONNECT image2.pubmatic.
com:443 - HIER_DIRECT/198.47.127.15 -
1486028112.800  10271 192.168.1.101 TCP_TUNNEL/200 5696 CONNECT flockler.com:443
 - HIER_DIRECT/134.213.3.151 -
1486028113.868  10165 192.168.1.101 TCP_TUNNEL/200 619 CONNECT static.ads-twitte
r.com:443 - HIER_DIRECT/104.244.43.144 -
1486028119.444  60945 192.168.1.101 TCP_TUNNEL/200 3961 CONNECT versioncheck-bg.
addons.mozilla.org:443 - HIER_DIRECT/52.27.123.81 -
1486028119.704  61199 192.168.1.101 TCP_TUNNEL/200 3699 CONNECT aus5.mozilla.org
:443 - HIER_DIRECT/54.186.22.115 -
1486028120.452  61503 192.168.1.101 TCP_TUNNEL/200 800 CONNECT versioncheck-bg.a
ddons.mozilla.org:443 - HIER_DIRECT/52.27.123.81 -
```

General | Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	*.jamk.fi
Organization (O)	Jyväskylän Ammattikorkeakoulu
Organizational Unit (OU)	ICT-Services
Serial Number	0D:85:E8:3C:9C:E5:7F:7A:02:4E:A5:4C:28:CF:F5:A7

Issued By

Common Name (CN)	TERENA SSL CA 3
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	08/15/2016
Expires On	08/20/2019

Fingerprints

SHA-256 Fingerprint	CB:0B:CC:BE:16:74:30:14:C6:82:E6:43:B3:85:35:C8:56:6B:C3:A5:83:2E:2B:24:FA:15:2D:12:83:A8:22:21
SHA1 Fingerprint	32:9D:39:6F:2C:C9:44:0B:A7:1D:F0:3E:BE:FC:38:EA:DC:E7:DF:50

BONUS: If you have time and want to experiment, try to recreate the squidCA.pem using the CA from the previous lab. You need to modify the OpenSSL config so you can sign a CA certificate for squid.