



## Exercise 12.1: Create a basic squid forward proxy

- Ensure your local network can utilize the proxy.
- Even though your RFC 1918 local network may already be in the default `squid.conf` file, explicitly set your current network as an ACL.

### Solution 12.1

#### 1. Ensure **squid** is installed:

- On **CentOS**:

```
# yum install squid
```

- On **OpenSUSE**:

```
# zypper install squid
```

- On **Ubuntu**:

```
# apt-get install squid
```

#### 2. Create an ACL for your network, edit the file `/etc/squid/squid.conf` and add the following just after the line which reads:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

NOTE: on some **Ubuntu** systems the file may located at `/etc/squid3/squid.conf` and may be very verbose. The place in the file to insert rules is above the line `http_access allow localhost`.

```
acl examplenetwork src <NETWORK ADDRESS>/24
```

#### 3. Explicitly allow HTTP access for the newly created ACL, by adding this line below the ACL added above:

```
http_access allow examplenetwork
```

#### 4. Test the syntax of `squid.conf`:

```
# squid -k parse
```

#### 5. Start the Squid daemon:

- On **CentOS** and **OpenSUSE**:

```
# systemctl restart squid
```

- On **Ubuntu**:

```
# systemctl restart squid3
```

## 6. Test the proxy:

- Configure a web browser to use your new proxy.
- Visit a known good URI (<http://www.foxnews.com>).
- Visit a known non-existent URI (<http://sdfa.klj.example.com>)

**NOTE:** You should see a Squid error page when you attempt to access the non-existent URI.