Single tenant use of Squid with OpenAthens

This page covers the use of Squid as a single tenant - i.e. with only one IP address. If you need to present different IP addresses for different parts of your organisation structure, see: Multi-tenant use of Squid with OpenAthens

This page concentrates on Linux. Other forwarding proxies are available and will work in similar ways.

Prerequisites

- Familiarity with your own systems.
- Sufficient access rights to install and configure software.
- No fear of the command line (although a healthy respect is always good).

Method

There are a couple of differences between Debian and Red Hat derived systems which are highlighted below. Other distros will be similar.

General

1. Install the package: `Squid`. Most repositories include it, but you can also get binaries from https://wiki.squid-cache.org/SquidFaq/BinaryPackages. CentOS 7 users will additionally need to install `apache2-utlis` for the htpasswd command
2. Navigate to your install directory (`/etc/squid`)
3. Create a password
    a. `> sudo htpasswd -c /etc/squid/passwd make_up_a_username`
    b. Make a note of the username and password for later - you will need to tell OpenAthens what they are
4. Edit `squid.conf` taking care to use the correct `auth_param` line for your distro

```
# Prevent X-Forwarded-For being overwritten by Squid
forwarded_for transparent

# Setup ACLs for OpenAthens
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd # RHEL / CentOS based distros
# auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd # Debian / Ubuntu based
distros
auth_param basic realm proxy
acl authenticated proxy_auth REQUIRED

# Allow authenticated access
http_access allow authenticated

# Deny all other access to this proxy
http_access deny all
```

5. Start Squid and set it to autostart according to your OS

    Modern RHEL and Debian based distros now both use systemctl so are the same. Which was a pleasant surprise.

    ```
    > sudo systemctl start squid
    > sudo systemctl enable squid
    ```

6. <squids_ip_address>:3128 should now show an error page generated by Squid

Securing the connection

You want to make sure that the inbound connection is limited to OpenAthens and this is secured using an X.509 client certificate. The process is a little different depending on which flavour of Linux you are using.

You should register your server in DNS before generating the certificate request.

- Red Hat based distros such as CentOS
- Debian based distros such as Ubuntu

Red Hat based distros such as CentOS

7. Add the following to your squid.conf file:

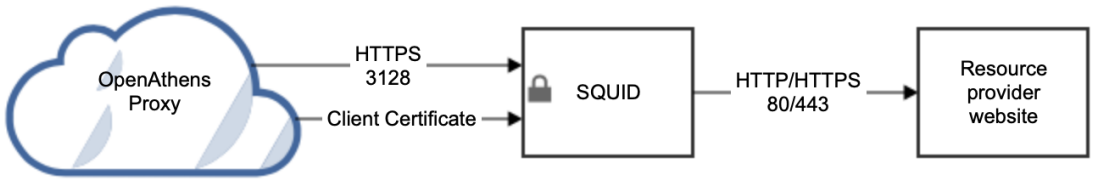
```
#http_port xxx.xxx.xxx.xxx:3128

# if certificate and key are in the same file use this one
https_port xxx.xxx.xxx.xxx:3128 cert=/etc/squid/ssl_cert/server.pem clientca=/etc/squid/ssl_cert/openathens-
client.pem

# if the certificate and key are in separate files, use this one
https_port xxx.xxx.xxx.xxx:3128 cert=/etc/squid/ssl_cert/server.pem key=/etc/squid/ssl_cert/privatekey.pem
clientca=/etc/squid/ssl_cert/openathens-client.pem #2
```

- `xxx.xxx.xxx.xxx` is the external IP address of your Squid instance. Remove any and all `http_port` directives, leaving only the `https_port` directive
- `server.pem` is your server's certificate. This needs to be from a valid certification authority or Let's Encrypt (https://letsencrypt.org).
- `openathens-client.pem` is the public key of the OpenAthens service and will ensure access is restricted. You can download it from https://proxy.openathens.net/tls/openathens-client.pem
- (Put all the certificates in the `/etc/squid/ssl_cert` folder)

8. Set your firewall rules to

- allow TCP inbound to port 3128 on this server from **any** source IP address (the connection from us can come from multiple IPs)
- allow outbound traffic on standard HTTP ports (80 and 443)

9. Securely pass our service desk the username and password you set up in step 3.



Debian based distros such as Ubuntu

At the time of writing the Squid package supplied by Debian is not compiled with the `-enable-ssl` flag which means the `https_port` configuration directive is not available and a little more work is required. Since you can't use a simple configuration directive you need to front Squid with something such as stunnel (https://www.stunnel.org/).

7. `>apt-get install stunnel4`

8. Create `/etc/stunnel/stunnel.conf`:

```
pid=/var/run/stunnel4/pid
setuid = stunnel4
setgid = nogroup

[squid-tls]
accept  = xxx.xxx.xxx.xxx:3128
#Don't need to expose squid directly to the internet.
connect = 127.0.0.1:3129
cert = /etc/stunnel/server.pem
CAfile=/etc/stunnel/openathens-client.pem
verify = 4
```

- `xxx.xxx.xxx.xxx` is the external IP address of your Squid instance.
- `server.pem` is your server's certificate. This needs to be from a valid certification authority or Let's Encrypt. We'll need a copy alongside the username and password you set up earlier. Our service desk will be able to advise on secure ways to transfer the information to us.

- `openathens-client.pem` is the public key of the OpenAthens service and will ensure access is restricted. You can download it from https://proxy.openathens.net/tls/openathens-client.pem
- (Put both certificates in the `/etc/stunnel` folder)
- Only root should have RW access to the `server.pem` file

9. Add the following to your `squid.conf` file:

```
http_port 127.0.0.1:3129
```

10. Set your firewall rules to

- allow TCP inbound to port 3128 on this server from **any** source IP address (the connection from us can come from multiple IPs)
- allow outbound traffic on standard HTTP ports (80 and 443)

11. Securely pass our service desk the username and password you set up in step 3