Add SSL Termination to HAProxy on Ubuntu 14.04

This article will walk you through setting up SSL termination on HAProxy, for encrypting traffic over HTTPS. We will be using a self-signed SSL certificate for new frontend. It is assumed that you already have HAProxy installed and configured with a standard HTTP frontend.

Requirements

- Vultr VPS
- HAProxy 1.5
- Ubuntu 14.04 LTS (Should work on other versions and distribution)

Generate Certificate and Private Key

Run the following lines of code to generate a private key and a self-signed certificate that will work with HAProxy.

```
openssl genrsa -out /etc/ssl/private/server.key 2048
mkdir /etc/ssl/csr
openssl req -new -key /etc/ssl/private/server.key -out /etc/ssl/csr/server.csr
openssl x509 -req -days 365 -in /etc/ssl/csr/server.csr -signkey /etc/ssl/private/server.key
cat /etc/ssl/certs/server.crt /etc/ssl/private/server.key > /etc/ssl/certs/server.bundle.pem
```

Configure HAProxy

The first thing that you should do is to make sure that SSLv3 is disabled. Due to the POODLE attack, SSLv3 is no longer considered secure. All applications and servers should be using TLS 1.0 and above. Using your favorite text editor, open the file `/etc/haproxy/haproxy.cfg` . Inside, look for the line `ssl-default-bind-options no-sslv3` under the `global` section. If you do not see it, add that line at the end of the section before the `defaults` section. This will ensure that SSLv3 is disabled globally. You can also set it inside your frontend sections, but it is recommended to disable it globally.

Onto the HTTPS setup. Create a new frontend section named `web-https` .

```
frontend web-https
        bind public_ip:443 ssl crt /etc/ssl/certs/server.bundle.pem
        reqadd X-Forwarded-Proto:\ https
        rspadd Strict-Transport-Security:\ max-age=31536000
        default_backend www-backend
```

To explain:

- `bind public_ip:443` (change `public_ip` to your VPS public ip) tells HAProxy to listen to any request that is sent to the ip address on port `443` (the HTTPS port).
- `ssl crt /etc/ssl/certs/server.bundle.pem` tells HAProxy to use the SSL certificate previously generated.
- `reqadd X-Forwarded-Proto:\ https` adds the HTTPS header to the end of the incoming request.
- `rspadd Strict-Transport-Security:\ max-age=31536000` a security policy to prevent against downgrade attacks.

You do not need to make any additional changes to your backend section.

If you wish to have HAProxy use HTTPS by default, add `redirect scheme https if !{ ssl_fc }` to the beginning of the `www-backend` section. This will force HTTPS redirection.

Save your configuration and run `service haproxy restart` to restart HAPRoxy. Now you're all set to use HAProxy with an SSL endpoint.