Cisco ASA5500 series SSL configuration

After the recent POODLE SSL vulnerabilities, I locked down the SSL configuration of our web servers, so that only TLS 1.0 and better are offered.

However, our Cisco ASA5505 box also runs HTTPS, and it's defaults are to offer SSLv3 and TLS 1.0.

Easy enough to fix that:

```
ssl server-version tlsv1-only
ssl client-version tlsv1-only
```

Now POODLE is fixed, but the ASA still offers several lower grade cipher suites.

I'd like it to offer the best ciphers, and only the stuff that is actually used, in our case we only use AnyConnect clients on Mac and Windows.

After some testing I found that the AnyConnect clients work fine if only aes256-sha1 is offered.

However, after that I couldn't manage the boxes anymore with ASDM 😉

This turns out to be a Java limitation, Java doesn't work with AES256: https://www.ssllabs.com/ssltest/viewClient.html?name=Java&version=8b132.

After adding that everything worked fine again.

The config thus is:

```
ssl server-version tlsv1-only
ssl client-version tlsv1-only
ssl encryption dhe-aes128-sha1 aes256-sha1
```

The SSLlabs test now gives it a B: https://www.ssllabs.com/ssltest/analyze.html?d=vpn.terena.org.

You can also tell that you should use Java 7 or 8 if you run ASDM - 6 won't work.

The ASA unfortunately doesn't support TLS 1.1 or 1.2, and Cisco are not going to add this to it, at least not for the models at the start of the range (ASA5505 and ASA5510).