TLS Settings for the Deprecation of TLS 1.0 and 1.1

Apache

```
# Enable TLSv1.2, disable SSLv3.0, TLSv1.0 and TLSv1.1
SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1

# Enable modern TLS cipher suites
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256

# The order of cipher suites matters
SSLHonorCipherOrder     on

# Disable TLS compression
SSLCompression          off

# Necessary for Perfect Forward Secrecy (PFS)
SSLSessionTickets       off
```

Nginx

```
# Enable TLSv1.2, disable SSLv3.0, TLSv1.0 and TLSv1.1
ssl_protocols TLSv1.2;

# Enable modern TLS cipher suites
ssl_ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256;

# The order of cipher suites matters
ssl_prefer_server_ciphers on;
```