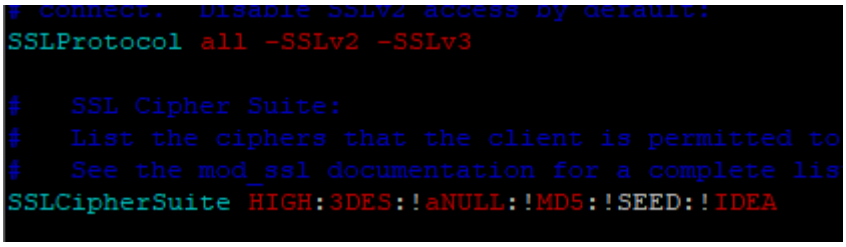
Cifrado Seguro en Servidores Apache

Para activar el Cifrado Seguro en servidores Apache (sea Windows o Linux), tendremos que acceder al archivo de configuración del VirtualHost 443.

- En Apache-HTTPD el archivo por defecto es: /etc/httpd/conf.d/ssl.conf
- En Apache2 el archivo por defecto es: /etc/apache2/mods-available/ssl.conf
- En Apache Windows el archivo por defecto es: /etc/httpd/conf/extra/httpd-ssl.conf

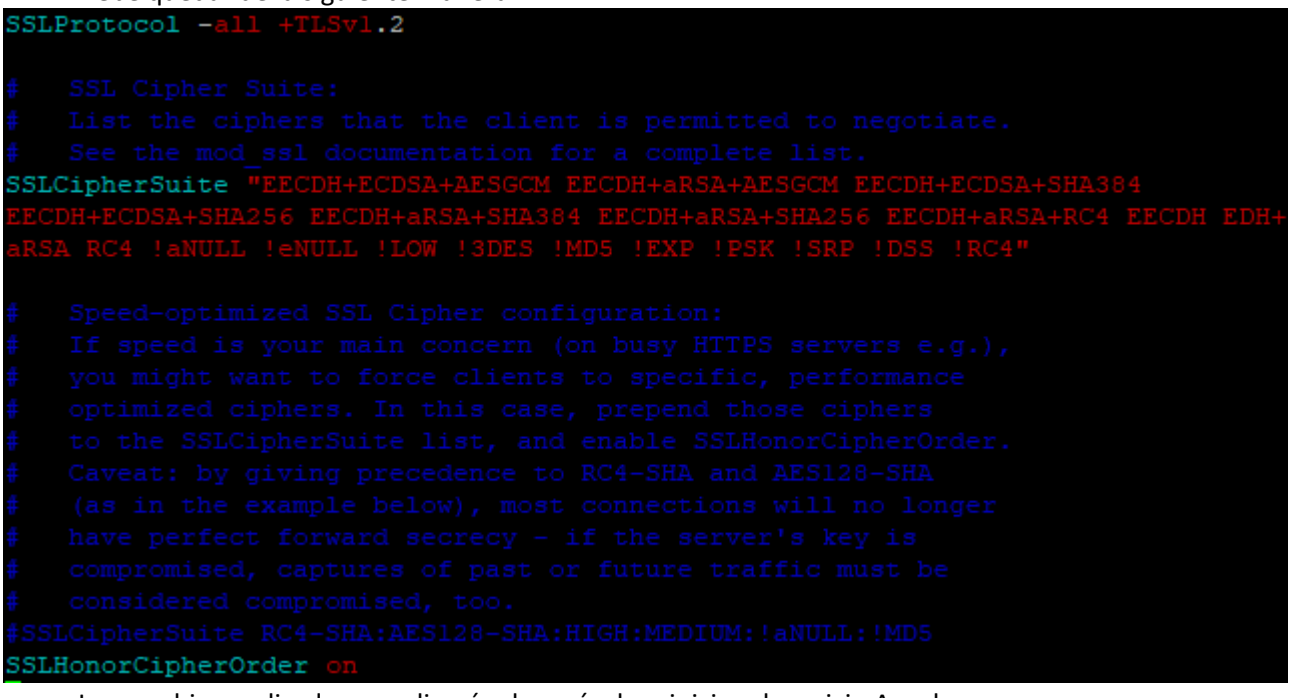


En este archivo, deberemos hacer 3 configuraciones:

1. Buscar el atributo SSLProtocol y modificar a: SSLProtocol -all +TLSv1.2
2. Buscar el atributo SSLHonorCipherOrder y descomentarlo o agregarlo: SSLHonorCipherOrder on
3. Buscar el atributo SSLCipherSuite y editarlo de la siguiente manera:

SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4"

Debe quedar de la siguiente manera:



Los cambios realizados se aplicarán después de reiniciar el servicio Apache.

Nota: Si quieres un cifrado más seguro, reemplazar los Cipher Suites por:

SSLCipherSuite ALL:!RSA:!CAMELLIA:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!SHA1:!SHA256:!SHA384

Tener en cuenta que, si el cliente no es compatible con alguno de los Cipher Suites seguros, no se podrá establecer la comunicación.

HSTS en Servidores Apache

Si quieres activar HSTS para obtener un A+ en la prueba de SSLQualys, se debe agregar la siguiente cabecera al VirtualHost 443:

Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains; preload"

```
Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains
; preload"
```

Luego de un reinicio del servicio Apache, el subdominio incluirá las cabeceras de HSTS en los paquetes que viajen desde el servidor.