网站提示“NET::ERR_SSL_OBSOLETE_VERSION 使用了不受支持的协议”

原因：

是由于服务器的证书配置使用的旧的 ssl_protocols 协议或者是 ssl_ciphers 加密协议套件，从去年开始主流浏览器的最新几个版本都已经禁用了 TLSV1.0 协议或旧的加密套件，所以访问的时候才会提示使用了不支持协议。

解决方案

Nginx web 环境:

ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;

ssl_ciphers EECDH+CHACHA20:EECDH+CHACHA20-draft:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5;

apache web 环境:

```
SSLProtocol             all -SSLv3
                            -TLSv1
                            -TLSv1.1

SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

Tomcat 环境:

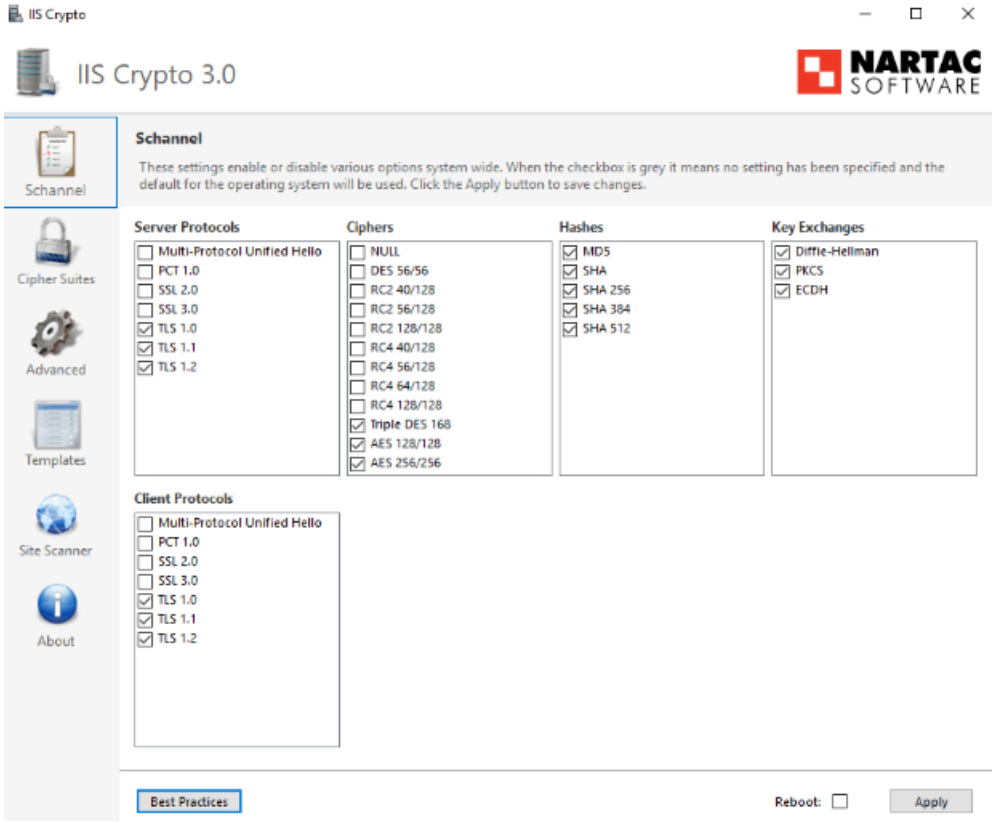
```
<SSLHostConfig
      ciphers="ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA"
      disableSessionTickets="true"
      honorCipherOrder="true"
      protocols="TLSv1, TLSv1.1, TLSv1.2, TLSv1.3"/>
```

IIS 环境

优化 SSL

运行工具：https://www.ihuandu.com/download/wind%20%E5%8D%87%E7%BA%A7.zip

设置部分：先点击左侧 Best Practices 按钮，再点击右侧 Apply 按钮



需要重启服务器才能生效

如果有第三方的 waf 防火墙则需要在 waf 防火墙面板中做相对应的设置，把 tlsv1.0 1.1 1.2 1.3 都勾选