

Configuração do servidor Apache com SSL no sistema operativo Windows 2000/XP

André P. Muga
apmuga@apmuga.com

Índice

1.	Introdução	3
2.	Configuração e criação dos certificados ssl.....	4
2.1.	<i>Instalação e configuração do OpenSSL.....</i>	4
2.1.1.	Geração de certificados para o CA	4
2.1.2.	Geração de certificados para o web-server	4
2.1.3.	Geração de certificados para o web-browser	4
3.	Configuração do Apache	6
3.1.	<i>Configuração base</i>	6
3.2.	<i>Activação do SSL para todas as áreas</i>	6
3.3.	<i>Restrição pelo método clássico usando o htpassfile</i>	6
3.4.	<i>Restrição usando certificados.....</i>	7
3.5.	<i>Restrição usando certificados controlados.....</i>	7
3.6.	<i>Testes</i>	8

Índice de figuras

FIGURA 1 – FALHA NA TENTATIVA DE ACESSO AOS CONTEÚDOS SSL.	8
FIGURA 2 - TESTE COM MÉTODO DE AUTENTICAÇÃO BÁSICO.	8
FIGURA 3 – PEDIDO DA PALAVRA CHAVE NO FIREFOX.	9
FIGURA 4 – PEDIDO DE CERTIFICADO NO IE.	9

1. Introdução

Este documento foi escrito com intuito ajudar na instalação do servidor web Apache no sistema operativo Microsoft Windows 2000 e XP. Trata-se apenas de um guia e não pretende substituir os manuais de utilização do Apache e do openssl.

2. Configuração e criação dos certificados ssl

2.1. Instalação e configuração do OpenSSL

2.1.1. Geração de certificados para o CA

Para facilitar na tarefa de criação e geração de certificados é necessário configurar o ficheiro openssl.cnf.

```
Criação chave do CA com 1024 bit
openssl genrsa -out ssl.key/CA/CA.KEY

Criação do pedido de certificado
openssl req -new -key ssl.key/CA/CA.KEY \
-out ssl.key/CA/CA.CSR -config openssl.cnf

Certificado "Self-sign"
openssl x509 -req -days 365 -in ssl.key/CA/ CA.CSR \
-out ssl.key/CA/ CA.CRT -signkey ssl.key/CA/CA.key

converter para pem
openssl x509 -in ssl.key/ca/CA.CRT -outform DER \
-out ssl.key/ca/CA.der
```

2.1.2. Geração de certificados para o web-server

```
Criação chave do CA com des3 como método de encriptação
openssl genrsa -des3 -out ssl.key/server/keys/localhost.KEY

Criação do pedido de certificado
openssl req -new -key ssl.key/server/keys/localhost.KEY \
-out ssl.key/server/requests/localhost.CSR \
-config openssl.cnf

Assinar certificado com base no CA
openssl ca -config openssl.cnf \
-in ssl.key/server/requests/localhost.CSR \
-cert ssl.key/CA/CA.CRT \
-keyfile ssl.key/CA/CA.KEY \
-out ssl.key/server/certificates/localhost.CRT
```

2.1.3. Geração de certificados para o web-browser

```
Criação chave do CA com des3 como método de encriptação
openssl genrsa -des3 -out ssl.key/user/keys/user.KEY
```

```
Criação do pedido de certificado
openssl req -new \
-key ssl.key/user/keys/user.KEY \
-out ssl.key/user/requests/user.CSR \
-config openssl.cnf
```

```
Assinar certificado com base no CA
openssl ca -config openssl.cnf \
-in ssl.key/user/requests/user.CSR \
-cert ssl.key/CA/CA.CRT \
-keyfile ssl.key/CA/CA.KEY \
-out ssl.key/user/certificates/user.CRT
```

```
Conversão de certificado para formato PKCS#12 para importação no
webbrowser
openssl pkcs12 -export -clcerts \
-in ssl.key/user/certificates/user.CRT \
-inkey ssl.key/user/certificates/user.KEY \
-out ssl.key/user/certificates/user.P12
```

3. Configuração do Apache

3.1. Configuração base

Na webroot do apache, no nosso caso /web/webroot, três directorias:

- normal, aonde temos apenas ssl activado.
- pro_normal, aonde pretendemos uma protecção básica.
- pro_cert, aonde pretendemos apenas utilizadores com certificados válidos.
- pro_sel_cert, aonde pretendemos apenas utilizadores escolhidos com certificados válidos.

3.2. Activação do SSL para todas as áreas

Para ter conteúdos protegidos com ssl, temos duas soluções:

- Proteger todo o site, removendo o porto 80 mantendo o porto ssl 443.
- Proteger cada directoria pretendendo no ficheiro httpd.conf.

Vou apresentar o segundo caso.

Assim é necessário alterar, no httpd.conf, a configuração das pastas pro_normal, pro_cert e pro_sel_cert para ser alvo de protecção ssl.

Um exemplo dessa alteração é:

```
<Directory /web/webroot/pro_normal/>  
SSLRequireSSL  
</Directory>
```

3.3. Restrição pelo método clássico usando o htpassfile

Para definir que utilizadores podem aceder a directoria é necessário criar um ficheiro contendo os login/password dos utilizadores autorizados. Temos de criar então o ficheiro /web/apache/conf/htpasswd.txt.

Essa gestão é feita com base no comando htpasswd do apache. Como exemplo, dois utilizadores, admusr e usr1, os comandos serão algo como:

```
htpasswd -bc /web/apache/conf/htpasswd.txt admusr pass  
htpasswd -c /web/apache/conf/htpasswd.txt usr1 pass
```

A opção c permite que o htpasswd cria o ficheiro se não existir.

A opção b indica ao htpasswd que a password é definida como parâmetro.

Dentro da pasta `pro_normal`, é necessário criar um ficheiro `.htaccess` contendo o seguinte:

```
AuthUserFile /web/apache/conf/htpasswd.txt
AuthName "SR Autenticação"
AuthType Basic
require valid-user
```

Assim indicamos ao Apache que todos os acessos nesta directoria são para ser validados com base no ficheiro `htpasswd.txt`

3.4. Restrição usando certificados

Para restringir os utilizadores para apenas os que tenham certificados compatíveis com o do servidor é necessário configurar no ficheiro `httpd.conf` do apache de seguinte maneira:

```
<Directory /web/webroot/pro_cert/>
SSLRequireSSL
SSLVerifyClient require
</Directory>
```

3.5. Restrição usando certificados controlados.

Para restringir os utilizadores para apenas os que tenham certificados compatíveis com o do servidor e escolhidos é necessário configurar no ficheiro `httpd.conf` do apache de seguinte maneira:

```
<Directory /web/webroot/pro_cert/>
SSLRequireSSL
SSLVerifyClient require
SSLRequire    %{SSL_CLIENT_S_DN_O} eq "User xpto"
</Directory>
```

Nota: Podemos alterar a configuração do `SSLRequire` para validar com base noutros parâmetros tais como

- `SSL_CLIENT_S_DN_CN`, alcunha do utilizador, "Common Name"
- `SSL_CLIENT_S_DN_O`, nome da organização.
- `SSL_CLIENT_S_DN`, Nome completo do utilizador
- `SSL_CLIENT_CERT`, o certificado em base 64.

3.6. Testes.

Aqui estão exemplos de testes com o FireFox e o Internet Explorer.

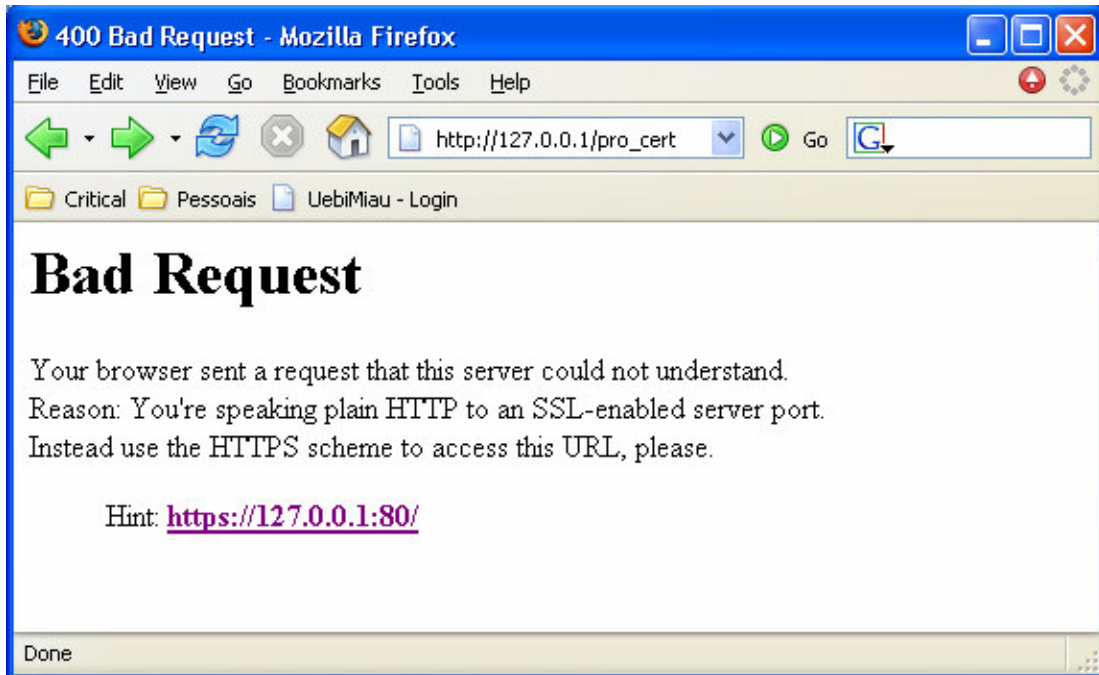


Figura 1 – Falha na tentativa de acesso aos conteúdos ssl.

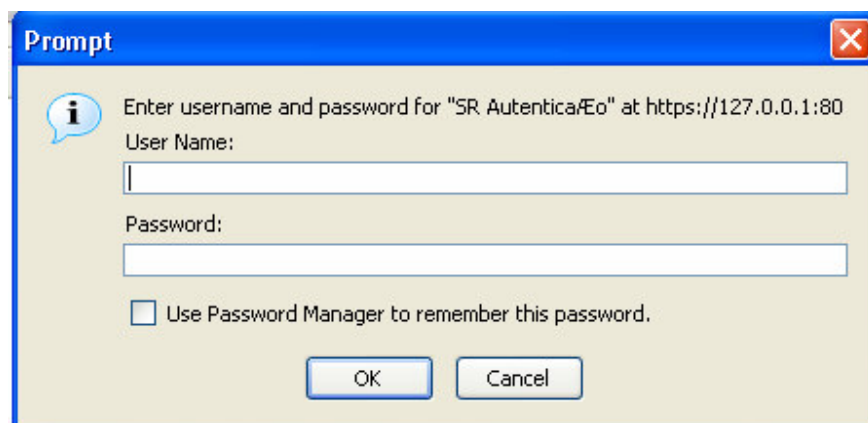


Figura 2 - Teste com método de autenticação básico.

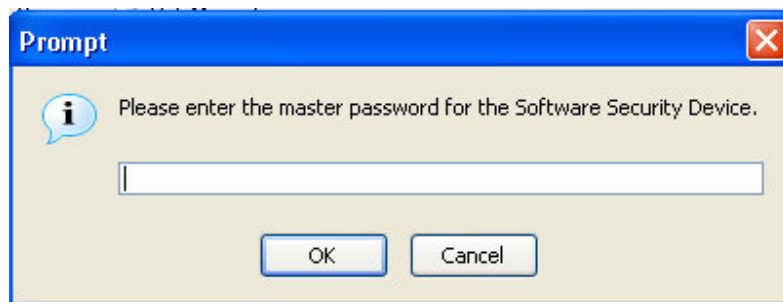


Figura 3 – Pedido da palavra chave no FireFox.

Foi interessante ver que o firefox, ao contrário do IE, pede a palavra-chave do certificado para poder ser utilizado.

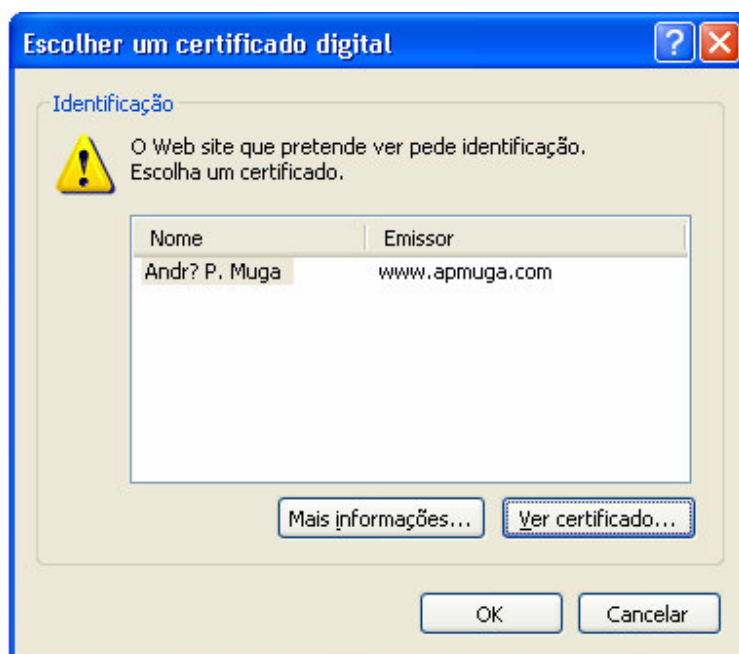


Figura 4 – Pedido de certificado no IE.