5.8 Configuração de um servidor seguro

O protocolo HTTP não possui nenhum recurso de criptografia e, por consequência, todo o tráfego de rede gerado entre clientes e servidor poderia ser visualizado por um atacante. Para aumentar a segurança de aplicações web é interessante habilitar o suporte a conexões cifradas através do SSL.

Para isso, faz-se necessário a instalação do pacote "openssl":

```
root@www:/# apt-get install openssl
```

Instalado o pacote, será necessário realizar os seguintes passos: Inicialmente crie um diretório para armazenar os certificados digitais:

```
root@www:/# mkdir /etc/apache2/ssl
```

Gere um certificado:

```
root@www:/# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/apache2/ssl/empresax.com.br.key -out /etc/apache2/ssl/empresax.com.br.crt
```

Serão realizadas as seguintes perguntas:

- Nome do País: digite BR para Brasil
- Nome do estado: digite Rio Grande do Sul
- Nome da Localidade: digite Porto Alegre
- Nome da Organização: digite EmpresaX
- Nome do Setor: digite Setor de TI
- FQDN ou seu Nome: www.empresax.com.br
- Endereço de email: webmster@empresax.com.br

Para ativar o suporte a SSL é necessário executar o comando:

```
root@www:/# a2enmod ssl
```

Reinicie o serviço apache2 e posteriormente verifique seu *status*.

```
root@www:/# systemctl restart apache2
root@www:/# systemctl status apache2
```

Agora será editado o arquivo referente ao site www.empresax.com.br "/etc/apache2/sites-available/empresax.com.br.conf", criado anteriormente:

```
root@www:/# vim /etc/apache2/sites-available/empresax.com.br.conf
```

Neste laboratório será mantida as linhas das configurações referente a porta 80, fazendo com que o servidor responta, tanto por HTTP (80), quanto por HTTPS (443).

Para isso, copie todas as linhas já existentes e realize as modificações referente a configuração do SSL, conforme destaque abaixo:

```
<VirtualHost *:443>
        ServerAdmin   webmaster@empresax.com.br
        ServerName    empresax.com.br
        ServerAlias   www.empresax.com.br
        DocumentRoot    /var/www/empresax.com.br/public_html
        ErrorLog /var/log/apache2/error-empresax.com.br.log
        CustomLog /var/log/apache2/access.log combined
        Options ExecCGI
        AddHandler  cgi-script  .pl

        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/empresax.com.br.crt
        SSLCertificateKeyFile /etc/apache2/ssl/empresax.com.br.key

<Directory  "/var/www/empresax.com.br">
                Order allow,deny
                Allow from all
</Directory>
</VirtualHost>
```

Terminada a configuração do Virtual Host, execute um teste de sintaxe de arquivo de configuração.

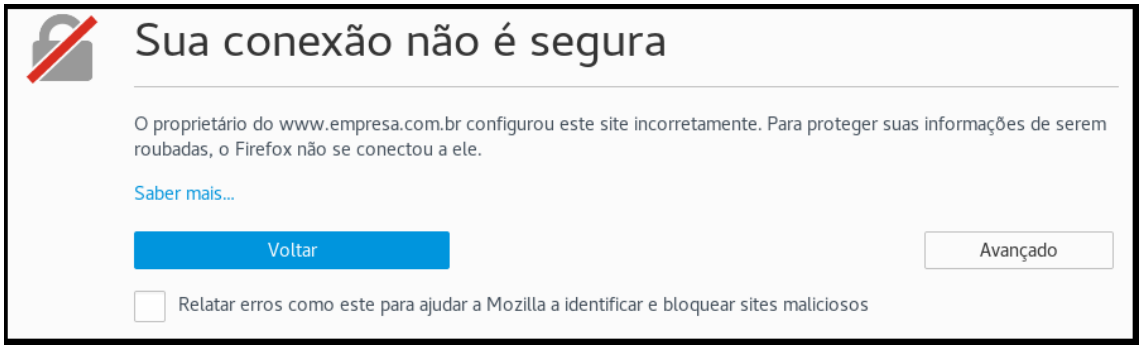
```
root@www:/# apachectl configtest
```

Reinicie o serviço apache2 e posteriormente verifique seu *status*.

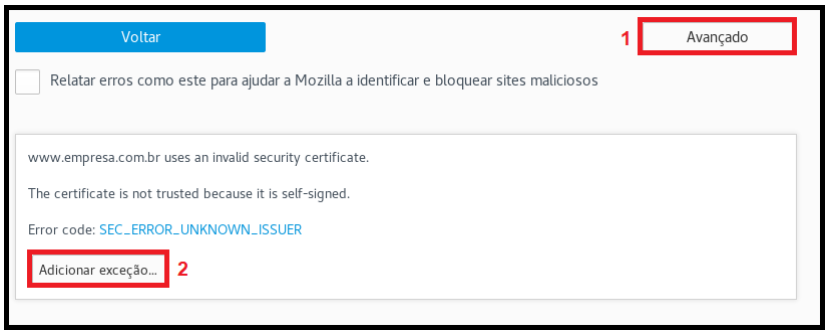
```
root@www:/# systemctl restart apache2
root@www:/# systemctl status apache2
```

Para testar, abra o navegador da máquina virtual Cliente e acesse https://www.empresax.com.br

Devido a instalação de um certificado auto-assinado, deverá aparecer o aviso de conexão não segura:



Para instalar o certificado, clique em “Avançado” e posteriormente em “Adicionar exceção”:



Para visualizar o certificado clique em “Ver (X)”:

Para evitar este alerta, basta adicionar o certificado à lista de exceções do browser clicando em “Confirmar Exceção de Segurança”.