Roteiro para testes do Certificado

Acreditamos que a rotina abaixo pode ser usada para fazer um teste de conexão SSL usando o seu certificado ICP-Brasil. Esse teste pode identificar:

- se o cliente está enviando o certificado;
- se a cadeia de certificado na keystore do cliente está completa;
- se o certificado é ICP-Brasil;

O que este teste não identifica:

- erros no protocolo HTTP (parte posterior à conexão SSL ser fechada);
- problemas com cifras (não especifiquei abaixo as cifras que nosso proxy utiliza);
- problemas com ModSecurity -- apenas acessando o Apache isso será possível;

Requisitos:

- um sistema Unix (ou a ferramenta openssl e wget no Windows - v. [1] e [2] abaixo);
- porta 44330 liberada nesse sistema (pode ser qualquer outra porta não utilizada)
- caso se deseje executar comandos com certificado do cliente (comandos wget e curl no final), é necessário ter um certificado ICP-Brasil; supõe-se arquivos cert-client.crt e chave-privada.key, sem senha (atenção, a chave é um arquivo confidencial)

```
# configuração do servidor de teste
ssh user@HOST
mkdir /tmp/teste-certificado
cd /tmp/teste-certificado

openssl req -x509 -newkey rsa:2048 -sha256 -subj
'/C=BR/ST=DF/L=Brasilia/CN=teste.localdomain' -keyout serverkey.pem -out
servercert.pem -days 365 -nodes

wget http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasil.crt \
   http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv2.crt \
   http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv4.crt \
   http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv5.crt -O
CAs-ICP.crt

openssl s_server -key serverkey.pem -cert servercert.pem -accept 44330 -
Verify 4 -purpose sslclient -CAfile CAs-ICP.crt -www
# atenção: -Verify com V maiúsculo acima é necessário para que o servidor
exija certificado do cliente


# possíveis testes de cliente (em outra janela/sessão):
# - trocar https://ws-h.bndes.gov.br para https://HOST:44330 na aplicação
(não vai obter dados, mas deverá conectar e a saída do openssl será útil)
# - acessar https://HOST:44330 a partir de um browser no qual o
certificado está instalado
# - executar: wget --no-check-certificate -d --verbose --tries=1 --secure-
protocol=auto --certificate=cert-cliente.crt --private-key=chave-
privada.key https://HOST:44330
# - executar: curl --verbose --insecure --cert cert-cliente.crt --key
chave-privada.key https://HOST:44330
# não esquecer de apagar o arquivo chave-privada.key depois do teste
# saída do comando openssl s_server mostrará se o certificado foi aceito
```

[1] http://gnuwin32.sourceforge.net/packages/openssl.htm
[2] http://gnuwin32.sourceforge.net/packages/wget.htm