

Segurança em HOTSPOT MIKROTIK com certificado SSL

1. Entendendo:

Páginas seguras são aquelas transmitidas com **criptografia**, evitando que informações sigilosas possam ser captadas no caminho entre o browser e o servidor.

O servidor do site que está sendo acessado envia uma chave pública ao browser, usada por este para enviar uma chamada secreta, criada aleatoriamente. Desta forma, fica estabelecida a trocas de dados criptografados entre dois computadores.

2. Procedimento:

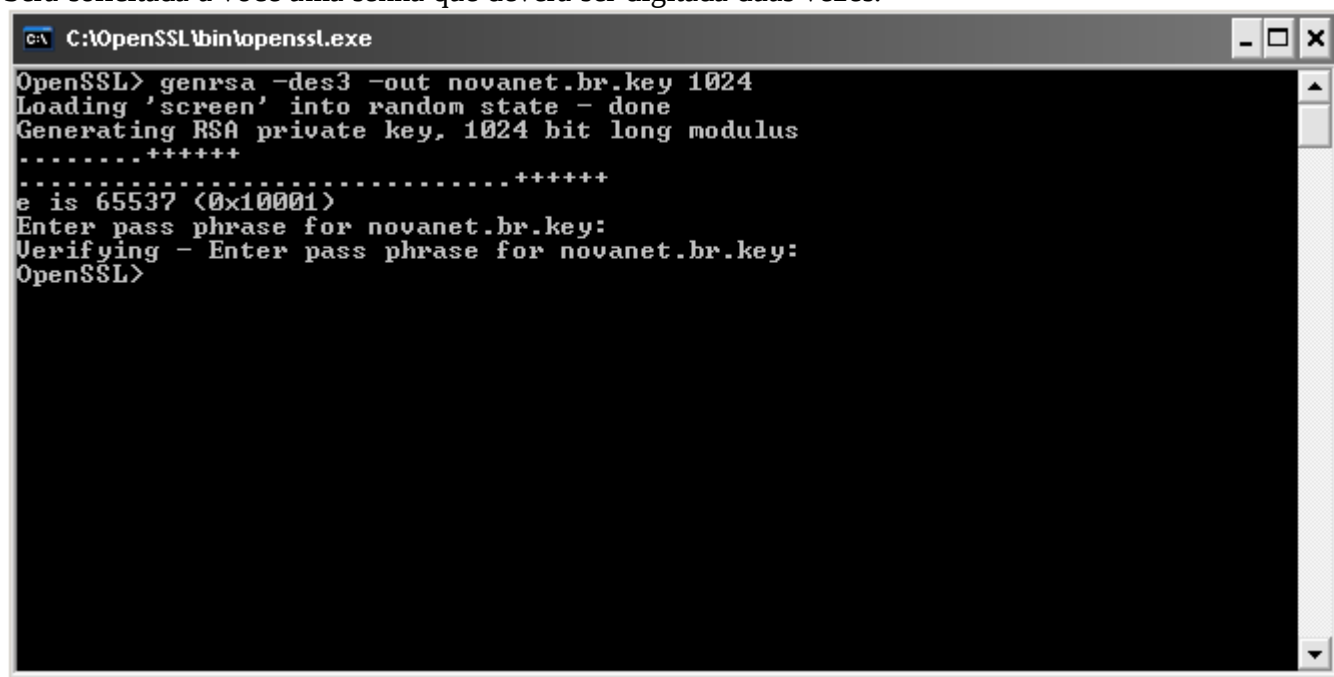
Baixar o [Win32OpenSSL Light-0.9.8g.exe](#), instalar na raiz do Windows, ir para o diretório C:\OpenSSL\bin, executar o openssl.exe.

Exemplo:

```
SERVIDOR=novanet.br  
CHAVE=novanet.br.key  
CERTIFICADO=novanet.br  
DIAS VALIDOS=1095  
genrsa -des3 -out novanet.br.key 1024  
req -new -x509 -days 1095 -key novanet.br.key -out novanet.br
```

COMANDO1

Será solicitada a você uma senha que deverá ser digitada duas vezes.



```
C:\OpenSSL\bin\openssl.exe  
OpenSSL> genrsa -des3 -out novanet.br.key 1024  
Loading 'screen' into random state - done  
Generating RSA private key, 1024 bit long modulus  
.....++++++  
.....++++++  
e is 65537 (0x10001)  
Enter pass phrase for novanet.br.key:  
Verifying - Enter pass phrase for novanet.br.key:  
OpenSSL>
```

COMANDO2

Será solicitada novamente a senha criada anteriormente e suas informações, conforme imagem abaixo:

```
C:\OpenSSL\bin\openssl.exe

OpenSSL> req -new -x509 -days 1095 -key novanet.br.key -out novanet.br
Enter pass phrase for novanet.br.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Amazonas
Locality Name (eg, city) []:Manaus
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NovaNET Internet
Organizational Unit Name (eg, section) []:NovaNET Internet
Common Name (eg, YOUR name) []:Vladimir Aleksei
Email Address []:
OpenSSL> _
```

Foram criados dois arquivos com o nome *novanet.br* (certificado) e *novanet.br.key* (chave) dentro da pasta BIN, citada no início do tutorial. Elas deverão ser enviadas para a raiz do MIKROTIK, via FTP ou winbox.

Abra o terminal ou acesse via telnet e execute *certificate*, siga os comandos abaixo:

Terminal vt102 detected, using multiline input mode

[vladimir@novanet] > certificate

[vladimir@novanet] certificate> print

Flags: K - decrypted-private-key, Q - private-key, R - rsa, D - dsa

[vladimir@novanet] certificate> import

passphrase: *****

certificates-imported: 1

private-keys-imported: 0

files-imported: 1

decryption-failures: 0

keys-with-no-certificate: 1

[vladimir@novanet] certificate> print

Flags: K - decrypted-private-key, Q - private-key, R - rsa, D - dsa

0 name="cert1"

subject=C=BR,ST=Amazonas,L=Manaus,O=NovaNET Internet,OU=NovaNET Internet,CN=Vladimir Aleksei

issuer=C=BR,ST=Amazonas,L=Manaus,O=NovaNET Internet,OU=NovaNET Internet,CN=Vladimir Aleksei

serial-number="8C84498EC89ACA75" invalid-before=mar/05/2009 16:08:04

invalid-after=mar/04/2012 16:08:04 ca=yes

[vladimir@novanet] certificate> decrypt

passphrase: *****

keys-decrypted: 0

[vladimir@novanet] certificate> print

Flags: K - decrypted-private-key, Q - private-key, R - rsa, D - dsa

0 name="cert1"

subject=C=BR,ST=Amazonas,L=Manaus,O=NovaNET Internet,OU=NovaNET Internet,CN=Vladimir Aleksei

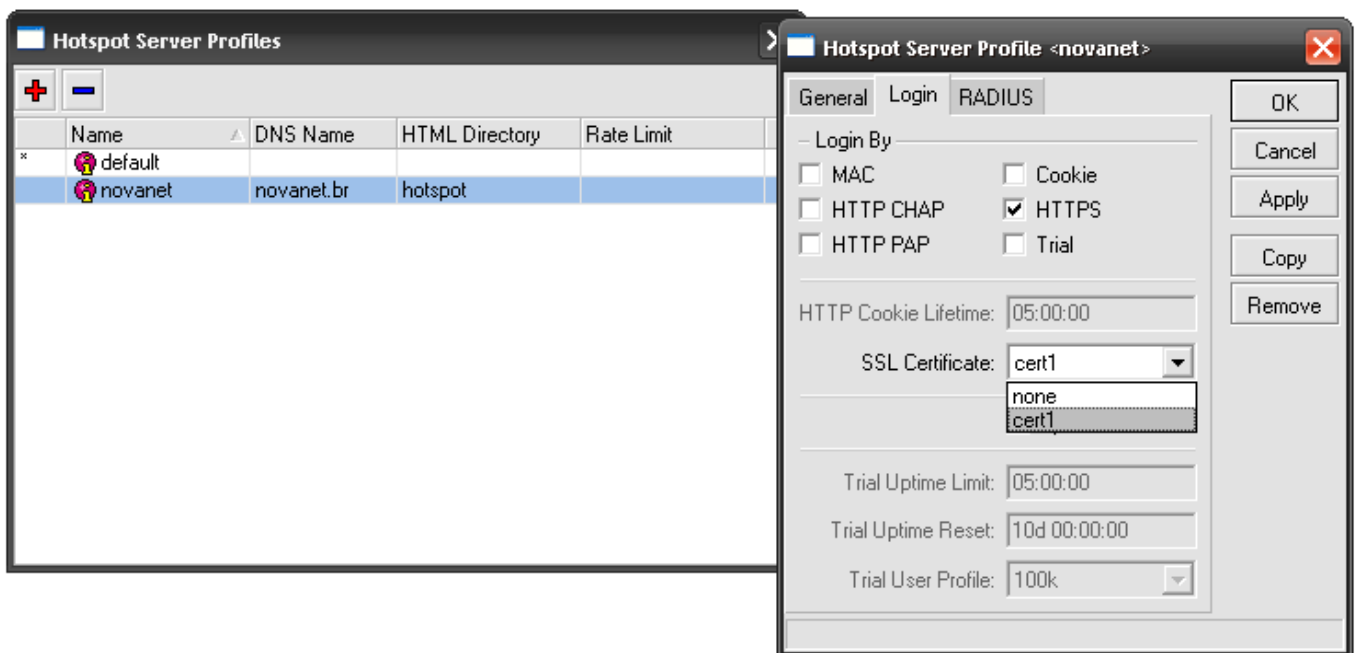
issuer=C=BR,ST=Amazonas,L=Manaus,O=NovaNET Internet,OU=NovaNET Internet,CN=Vladimir Aleksei

serial-number="8C84498EC89ACA75" invalid-before=mar/05/2009 16:08:04

invalid-after=mar/04/2012 16:08:04 ca=yes

[vladimir@novanet] certificate>

Agora vá ate IP>HOTSPOT>SERVERS>PROFILES e escolha a forma de autenticação por HTTPS, e selecione o certificado importado, segue imagem:



Está pronto!

Autor: Vladimir Aleksei

santiagoamerica@gmail.com

Fonte:

<http://forum.mikrotik.com/viewtopic.php?f=2&t=12063>