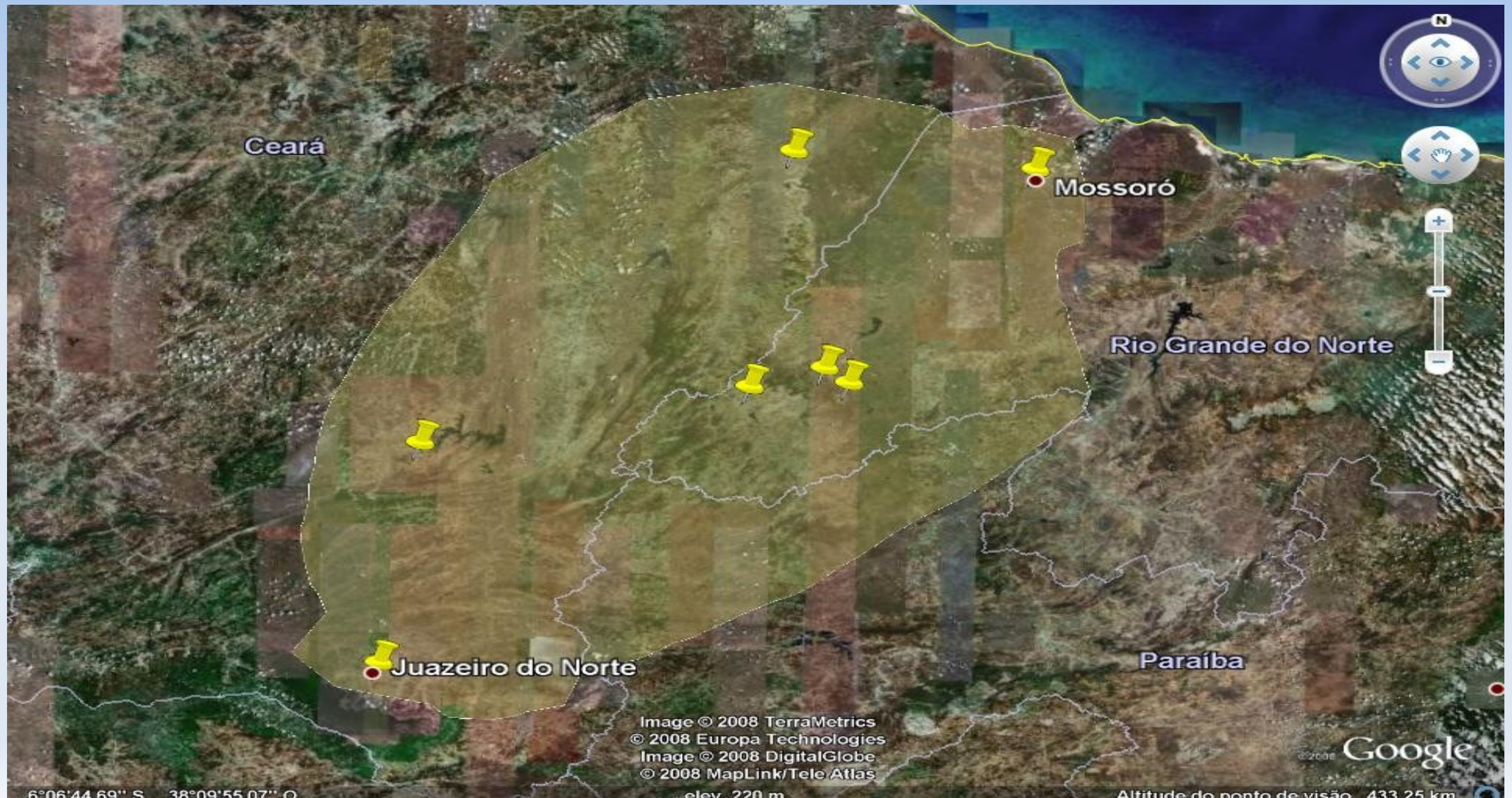
Autenticação de WiFi com L2TP/IPSEC

Rubens Marins Schner
Gerente de Tecnologia e Desenvolvimento
<rubens@brisanet.com.br>

Sobre a Brisanet Internet

- Provedor de Internet no nordesde, atende mais de 90 Municipíos nos estados do Ceará, Rio Grande do Norte e Paraíba
- Nossa Rede tem um raio de 300 KM
- Tem 6 pontos de interconexão com a Internet
- Mais de 200 servidores linux entre torres e CPD
- Aproximadamente 13.500 links de rádio
- Tinha aproximadamente 7000 clientes quando o projeto começou, todos os modelos de placa de rádio é usado na ponta do cliente

Alcance da Rede Brisanet



Desafio

- Autenticar os usuários do provedor, evitando uso não autorizado
- Operar independente do modelo de rádio
- Ser independente de Sistema Operacional
- Baixo custo de implementação
- Grande número de usuários já instalados, que precisa alterar

HOTSPOT

- Prós:
  - O metodo de maior facilidade para Instalação e configuração no lado do servidor
  - Não é preciso reconfigurar a ponta do usuário
  - Funciona com qualquer topologia de Rede
  - Custo muito baixo
  - Implementação instantânea

HOTSPOT

- Contra:
  - Fácil de ser vencido, mac pode ser clonado e pegar carona na sessão autenticada
  - Pode ser preciso deixar um pop-up aberto no lado do cliente para revalidação da sessão de tempos em tempos, isso não é bem aceito pelos usuário;

PPPOE

- Prós:
  - Fácil implementação e configuração no lado do servidor
  - Padrão de mercado, existindo para muitas plataformas, inclusive APs e Roteadores que os usuários possam ter para compartilhar o acesso

PPPOE

- Contra:
  - A Criptografia e segurança da senha é fraca, podendo inclusive ser capturada e reenviada criptografada
  - Somente os pacotes de dados são criptografados, os pacotes de controle da sessão não são
  - Pode ser feito replay da autenticação, para se autenticar
  - Vulnerável a Man-In-the-Middle, pois não há validação do servidor
  - Precisa Reconfigurar a ponta do usuário
  - Precisa fazer um script/programa para controlar a banda depois da conexão

WPA Enterprise

- Prós:
  - Atual padrão do mercado, para segurança de acesso sem fio
  - Valida o servidor quando usado com certificados
  - Criptografia Robusta (AES)
  - Fácil implementação no lado do usuário, encontrando suporte em diversas plataformas

WPA Enterprise

- Contra:
  - Precisa Reconfigurar a ponta do usuário
  - Não há suporte em hardware antigo (mais de 4 anos)
  - Causa sobrecarga de processamento no Access Point, devido a criptografia adicional,reduzindo o número máximo de clientes por AP

L2TP/IPSEC

- Prós:
  - Padrão de Mercado
  - Valida o lado do usuário e o lado do servidor
  - Extremamente Seguro
  - Suporte nativo em várias plataformas

L2TP/IPSEC

- Contra:
  - Precisa reconfigurar a ponta do usuário
  - Difícil implementação no lado do servidor
  - Para ser segura precisa de certificados, o que exige software adicional para geração e manutenção dos mesmos
  - Difícil configuração pelo usuário fora do mundo Microsoft (especialmente em linux)
  - Há duas camadas de tuneis, um de ipsec e outro de l2tp, isso pode dificultar o diagnóstico de problemas
  - Overhead de pacotes, PPP sobre L2TP sobre IPSEC, é preciso lidar com a MTU

Software/Hardware Utilizado

- Dual Core/2Ghz, 2Gb de RAM, suficiente para uns 1000 tuneis
- Slackware devido simplicidade e facilidade em montar um sistema enxuto
- Freeradius para servidor radius
- Foram feitos scripts PHP/Openssl para gerar os certificados de clientes
- Clientes logam em uma pagina do provedor onde pode ser gerado o certificado
- Nesta pagina pode ser baixado o certificado do cliente (usuario.p12) , e os programas para importar certificado e instalador da VPN

Kernel do Linux

Evitando ataques de Marte:

```
net.ipv4.conf.default.rp_filter = 0

net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.log_martians = 0
```

Aumentar a memória disponivel para o Kernel,
Padrao é 50-50 , Alterar para 100

```
CONFIG_VMSPLIT_1G=y
```

Openswan

- Para IPSEC Openswan
  - Excelente Performance
  - Memory leak com muitas conexões;
    - Precisa alterar o tam maximo de memoria para uso do kernel do Linux
    - resolvido com reboot na madrugada

L2TPNS

- Servidor L2TP usado foi l2tpns
  - Tudo em um único daemon, parte ppp e parte l2tp
  - Configuração cisco-like, usa a libcli
  - Tem uma interface telnet cisco-like, para visualizar usuarios e alterar parametros on-the-fly
  - Faz controle de banda nativo, podendo ler velocidade por usuário e ter um parâmetro padrão
  - Excelente estabilidade
  - Facilidade em ”grampear” o tráfego, para justiça
  - Expansibilidade via plugins, bem documentado

L2TPNS

- Suporta cluster de Autenticadores
- Usa BGP, onde deve ser configurado o multipath load-balance

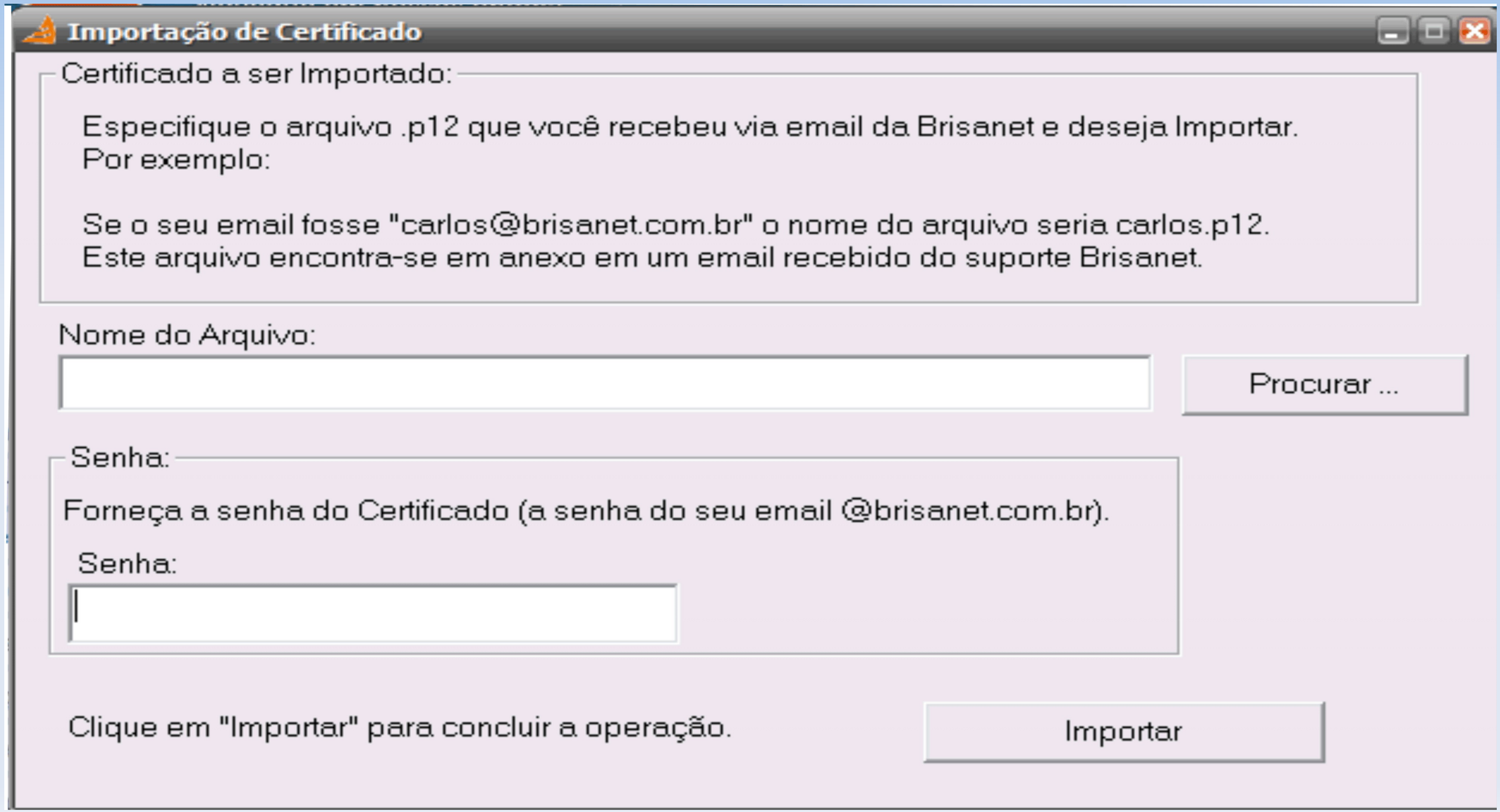
L2TPNS

- O controle de banda do l2tpns apresenta problemas de fairness de conexões tcp, quando tem muitos usuários conectados, (acima de 700 o problema começa a aparecer)
- Foi criado um plugin para usar o HTB do linux para controle de banda, o linux abriu o bico quando passou de 1000 tuneis
- O Windows suporta compressão de PPP, não de IPSEC, não há esse suporte no l2tpns, provavelmente iremos implementar

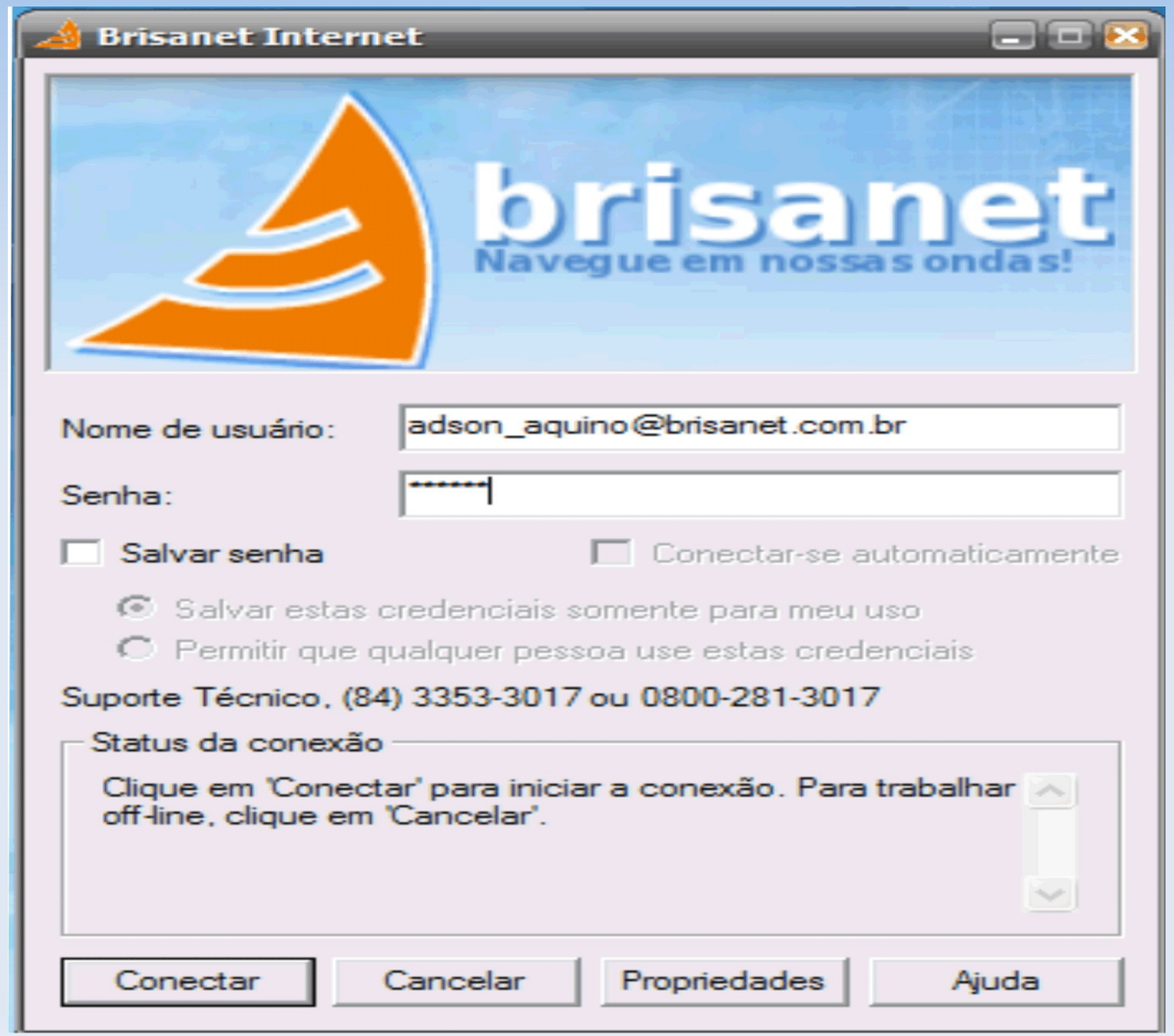
Lado do Cliente

- Importar o certificado no windows da muito trabalho, precisa fazer um wrapper para resolver
- Felizmente no CD do Windows Server vem uma ferramenta para criar instaladores de Tuneis l2tp/ipsec
- Alguns clientes usam sistemas de vpn corporativo, ainda não foi resolvido esta parte
- Esta para ser escrito um script/gui para automatizar o processo de Certificados, l2tp e ipsec no Linux

Software para Importar Certificado no Windows



Tela de Logon na VPN personalizada

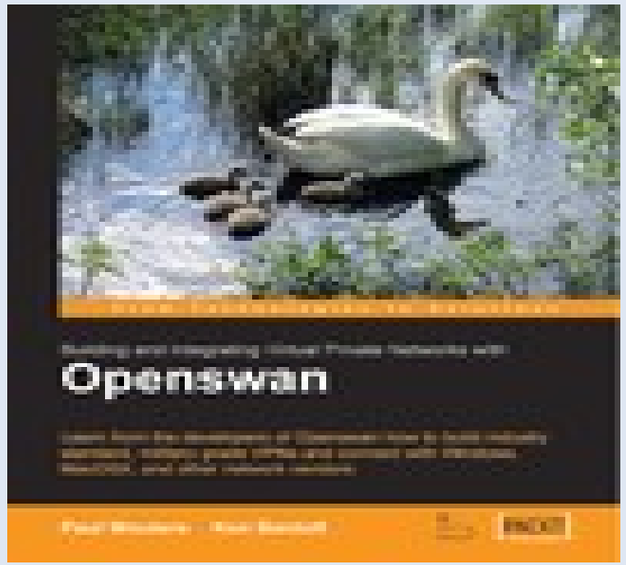


Icone na bandeja do Sistema

Referências:

http://www.jacco2.dds.nl/networking/openswan-l2tp.html

Livro: Openswan: Building and Integrating Virtual Private Networks



Obrigado

Rubens Marins Schner
<rubens@brisanet.com.br>