ISSN 1679-2599
Dezembro, 2006

Empresa Brasileira de Pesquisa Agropecuária
Embrapa Florestas
Ministério da Agricultura e do Abastecimento

Documentos 142

Rede Virtual Privada *Embrapa Florestas*

Gerson Rino Prantl Oaida

Colombo, PR
2006

Exemplares desta publicação podem ser adquiridos na:

Embrapa Florestas
Estrada da Ribeira, Km 111, CP 319
83411 000 - Colombo, PR - Brasil
Fone/Fax: (41) 3675 5600
Home page: www.cnpf.embrapa.br
E-mail: sac@cnpf.embrapa.br
Para reclamações e sugestões: www.embrapa.br/ouvidoria

Supervisor editorial: Luiz Roberto Graça
Revisor de texto: Mauro Marcelo Berté
Normalização bibliográfica: Elizabeth Denise Câmara Trevisan, Lidia Woronkoff
Capa: Mauro Marcelo Berté
Editoração eletrônica: Mauro Marcelo Berté

1ª edição
1ª impressão (2006): sob demanda

Dados Internacionais de Catalogação na Publicação - CIP
Embrapa Florestas

Oaida, Gerson Rino Prantl.

Rede virtual privada Embrapa Florestas [recurso eletrônico] / Gerson Rino Prantl Oaida. - Dados eletrônicos. - Colombo : Embrapa Florestas, 2006.

1 CD-ROM. - (Documentos / Embrapa Florestas, ISSN 1679-2599 ; 142)

1. Protocolo de rede. 2. Rede virtual. 3. Comunicação privada. 4. Rede de comunicação. I. Título. II. Série.

CDD 004.62 (21. ed.)

Autor

Gerson Rino Prantl Oaida
Analista de Sistemas,
Analista da *Embrapa Florestas.*
gerson@cnpf.embrapa.br

Apresentação

A internet está presente em quase todos os lugares, facilitando o acesso às informações para a vida e o trabalho das pessoas. Porém esta facilidade de acessar todo tipo de informação criou também a necessidade de proteger dados valiosos contra o acesso de pessoas mal intencionadas. As empresas então passaram a disponibilizar suas informações para a sociedade através de sistemas protegidos onde os usuários teriam acesso apenas às informações autorizadas, ficando inacessível o restante. Isto criou uma dificuldade para os empregados destas empresas, pois somente poderiam acessar informações sigilosas de dentro da empresa, e no caso de estarem em transito, dependeriam de colegas para tal. Nesse contexto, mostrou-se necessário prover acesso às informações da empresa para todos os empregados mesmo estando fora da empresa. Para cumprir esta tarefa foram criadas as redes privadas virtuais VPN (*Virtual Private Network*), que através de uma senha e conexão com criptografia, dariam aos empregados destas empresas a possibilidade de trabalhar com as informações de maneira segura independente do local.

Este estudo de caso pretende demonstrar o que é uma VPN e qual o processo de implementação utilizando dados criptografados.

Vanderley Porfírio-da-Silva

Chefia Adjunta de Comunicação e Negócios

Embrapa Florestas

Sumário

Rede Virtual Privada *Embrapa Florestas*

Gerson Rino Prantl Oaida

1. INTRODUÇÃO

A Embrapa, por ser um empresa de destaque em pesquisa agropecuária, trabalha com informações consideradas sigilosas. Se o resultado ou parte do andamento de pesquisas caírem em mãos erradas, vários anos de pesquisa podem se perder, dando prejuízo enorme aos cofres públicos.

Para a condução de suas pesquisas, a Embrapa possui um efetivo de técnicos e pesquisadores que mesmo fora do ambiente de trabalho precisam consultar informações em bases de dados e *sites* que só podem ser acessados de dentro da empresa, dificultando a produção longe da empresa.

Hoje o acesso às informações da Embrapa é feito por meio de diretórios FTP ou páginas HTML protegidas por senha. Estes métodos são bastante precários pois podem ser facilmente burlados por programas especialistas deixando informações valiosas vulneráveis.

Pretende-se então implementar uma forma dos empregados acessarem seus dados e informações de qualquer lugar do mundo de maneira segura e eficaz. Para esta implementação utilizou-se o acesso à internet disponível para todos através de provedores e companhias telefônicas.

Segundo Liou (1998) a idéia de utilizar uma rede pública como a internet em vez de linhas privativas para implementar redes corporativas é denominada de *Virtual*

Private Network (VPN) ou Rede Privada Virtual**.** As VPNs são túneis de criptografia entre pontos autorizados, criados através da internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A estrutura de VPN através de uma rede pública foi escolhida principalmente pela versatilidade e pelo custo, pois as redes públicas estão em quase todo lugar e, para se acessar, basta ter um modem e um computador.

Como o acesso pelas redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura, tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

A segurança é a função mais importante da VPN. Uma vez que dados particulares serão transmitidos pela internet devem ser protegidos de forma a não permitir que sejam alterados ou vistos por pessoas não idôneas.

Com essa abordagem, o uso de VPN sobre a internet parece ser uma alternativa viável e adequada. No entanto, observou-se que não é apenas em acessos públicos que a tecnologia de VPN pode e deve ser empregada.

Outro serviço oferecido pelas VPNs é a conexão entre corporações (Extranets) através da internet, além de possibilitar conexões *dial-up* criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

Uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de *links* dedicados de longa distância que podem ser substituídos pela internet. As LANs (*Local Área Network* ou Rede Local) podem, através de *links* dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se à outras LANs, possibilitando o fluxo de dados através da internet.

2. METODOLOGIA

Na ausência de uma metodologia específica para o processo de implantação de uma Rede VPN, foi desenvolvida uma, com procedimentos próprios, baseada em manuais técnicos dos sistemas operacionais, *softwares* envolvidos e também *hardware* utilizado. Foram consultadas também algumas literaturas encontradas na internet.

Sistemas operacionais:

Foram efetuados testes de instalação e funcionamento de dois sistemas operacionais, Freebsd e Fedora-Core para verificar qual apresentava uma interface mais intuitiva.

- FreeBSD: Sistema operacional desenvolvido na faculdade de Berkeley na California EEUU, baseada na plataforma UNIX.

- Fedora-Core: Sistema operacional linux, de fácil instalação baseado na distribuição Red Hat.

Foi escolhido para instalação o Fedora-Core por ser mais acessível e possuir uma versão compatível com o hardware que seria usado.

Softwares Envolvidos:

Baseado nas instruções dos manuais, foram instalados vários aplicativos, cada um com uma função específica.

- Kernel_ppp_mppe-0.0.5-2dkms.noarch, Modulo Microsoft para conexão PPP;

- Dkms-2.0.5.1noarch.rpm, Biblioteca dinâmica de suporte ao kernel;

- Libpcap-0.8.3-5.i385.rpm, Bibliotecas POSIX;

- Logrotate-3.6.8-6tr.i586.rpm, Gerenciador de log;

- Mailx-8.1.1-32i386.rpm, Sistema de E-mail com suporte PPP;

- Ppp-2.4.3-4.fc3i386.rpm, Protocolo PPP;

- Pptpd-1.2.1-1.i386.rpm, Protocolo PPTP;

Hardware utlizado:

Foi utilizado um Pentium IV com 120 Gb de disco e 1 Gb de memória RAM.

O restante do processo foi feito por tentativa e erro ou acerto, analisando-se os logs de depuração do sistema e resultados obtidos, refazendo, se necessário, alguns passos e, no caso de não se achar uma solução, recomeçando do zero.

3. DESENVOLVIMENTO

A solução proposta pode ser bastante interessante sob o ponto de vista financeiro, sobretudo nos casos em que enlaces nacionais e ou internacionais estão envolvidos, já que o meio físico será fornecido por provedores de serviço.

Como na *Embrapa Florestas* existe um bom número de empregados que trabalham em casa ou em universidades, decidiu-se criar uma estrutura VPN ponto a ponto, ligando um cliente autorizado à rede departamental local restrita.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa ou cliente, uma vez que o roteador possibilitaria a conexão entre as duas redes, permitindo o acesso de qualquer usuário à rede departamental local restrita.

Com o uso da VPN, o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede local departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada, assegurando a “confidencialidade” das informações. Os demais usuários não credenciados sequer enxergarão a rede local departamental restrita.

Para se estabelecer um túnel, é necessário que as suas extremidades utilizem o mesmo protocolo de tunelamento.

O tunelamento pode ocorrer na camada 2 ou 3 (respectivamente enlace e rede) do modelo de referência OSI (*Open Systems Interconnection*).

- Tunelamento em Nível 2 - Enlace - (PPP sobre IP)

O objetivo é transportar protocolos de nível 3, tais como o IP e IPX na internet. Os protocolos utilizam quadros como unidade de troca, encapsulando os pacotes da camada 3 (como IP/IPX) em quadros PPP (*Point-to-Point Protocol*).

Como exemplos, podemos citar:

- PPTP (*Point-to-Point Tunneling Protocol*) da Microsoft permite que os tráfegos IP, IPX e NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas como a internet.

- (L2TP (*Layer 2 Tunneling Protocol*) da IETF (*internet Engineering Task Force*) permite que os tráfegos IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto tais como IP, X25, Frame Relay ou ATM.

· L2F (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.

- Tunelamento em Nível 3 - Rede - (IP sobre IP)

Encapsulam pacotes IP com um cabeçalho adicional deste mesmo protocolo antes de enviá-los através da rede.

O *IP Security Tunnel Mode* (IPSec) da IETF permite que pacotes IP sejam criptografados e encapsulados com cabeçalho adicional deste mesmo protocolo para serem transportados numa rede IP pública ou privada. O IPSec é um protocolo desenvolvido para IPv6, devendo, no futuro, se constituir como padrão para todas as formas de VPN caso o IPv6 venha de fato substituir o IPv4. O IPSec sofreu adaptações possibilitando, também, a sua utilização com o Ipv4.

O IPSec é um protocolo padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de

segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos.

As funções de gerenciamento de chaves também fazem parte das funções do IPSec. Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser utilizados de forma conjunta ou separada, de acordo com a necessidade de cada usuário:

- Autenticação e Integridade;

- Confidencialidade.

Para implementar estas características, o IPSec é composto de três mecanismos adicionais de gerência de chaves e serviços de criptografia:

- AH - *Autentication Header:* É um serviço de autenticação dos pacotes IP usando o protocolo utilizado pelo IPSec.);

- ESP - *Encapsulation Security Payload:* Fornece meios para cifragem e autenticação de pacotes IP usado pelo IPSec);

- IKE (Internet Key Exchange): Negocia parâmetros de conexão para os outros serviços AH e ESP incluindo chaves criptográficas [HC98];

- ISAKMP - *Internet Security Association and Key Management Protocol: É* um protocolo usado para estabelecer as associações de segurança entre as chaves criptografadas e a internet.

Nas figuras abaixo temos um gráfico demonstrando a arquitetura de criptografia e verificação em um sistema IPSec (Figura 01) e uma amostra do tunelamento feito por diversas máquinas (Figura 02).

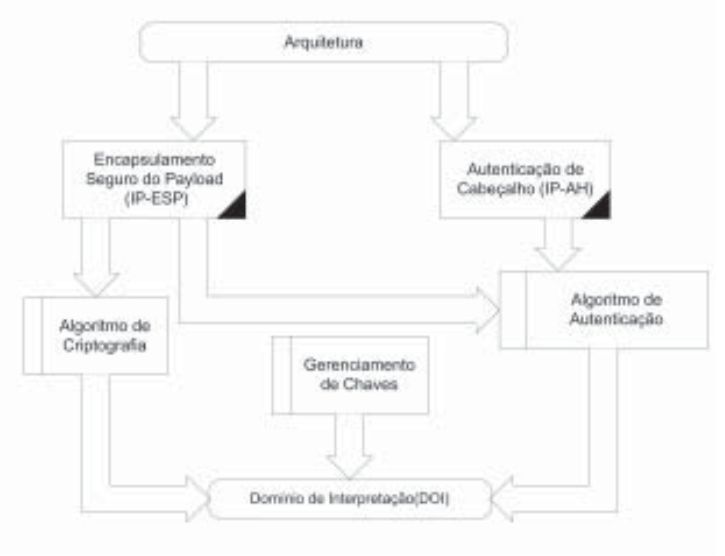

Figura 01. Arquitetura de criptografia.

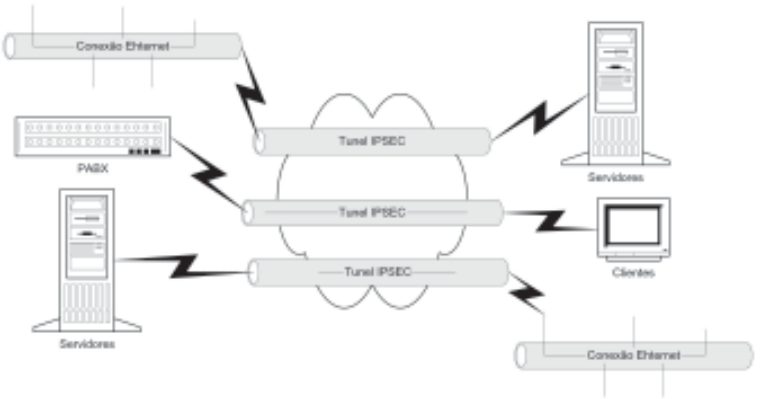

Figura 02. Tunelamento das máquinas nos vários níveis.

3. 1. O Funcionamento dos Túneis

O funcionamento é na prática bem simples, quando uma rede ou um cliente quer conectar-se a outra rede ou cliente, cria-se um túnel através de um protocolo que encapsula os cabeçalhos normais e adiciona um outro referente ao endereço de destino, este cabeçalho é quem cuida da criptografia e da segurança. Quando o pacote chega ao destino, ele é desencapsulado e entregue ao dono.

Nas tecnologias orientadas à camada 2 (enlace), um túnel é similar a uma sessão, onde as duas extremidades do túnel negociam a configuração dos parâmetros para estabelecimento do túnel, tais como endereçamento, criptografia e parâmetros de compressão. Na maior parte das vezes, são utilizados protocolos que implementam o serviço de datagrama.

A gerência do túnel é realizada através dos protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada 3, não existe a fase de manutenção do túnel.

Uma vez que o túnel é estabelecido, os dados podem ser enviados. O cliente ou servidor do túnel utiliza um protocolo de tunelamento de transferência de dados que acopla um cabeçalho preparando o pacote para o transporte. Só então o cliente envia o pacote encapsulado na rede que o roteará até o servidor do túnel.

Este recebe o pacote, desencapsula, removendo o cabeçalho adicional e encaminha o pacote original à rede destino. O funcionamento entre o servidor e o cliente do túnel é semelhante.

4. CENÁRIO ATUAL

O cenário atual é composto por um *firewall*, *freebsb* em um celeron 500 com o bloqueio de entrada e saída de pacotes em geral, sendo liberados os serviços básicos por servidor. Para os usuários estão liberadas todas as portas acima de 1023 e as abaixo apenas no caso de manter estado de conexão. Este servidor está ligado ao roteador da Universidade Federal do Paraná de onde sai para a internet. Este mesmo servidor está também ligado à rede interna da empresa.

A empresa possui ainda um servidor de banco de dados SOLARIS, onde estão as bases de dados de programas desenvolvidos para a Embrapa, um outro servidor SOLARIS que faz o serviços de DNS e e-mail e por fim um servidor

WEB para internet e intranet. Estes servidores estão ligados a um *switch*, onde os clientes se autenticam para executar os serviços.

Neste cenário, o usuário local pode acessar aos servidores locais a à rede Embrapa pois o *firewall* permite o trafego de pacotes da rede local para toda a rede. No caso do cliente estar vindo da rede pública, o *firewall* permite que os pacotes cheguem até os servidores locais, mas não permite acesso aos serviços da rede Embrapa, conforme exemplificado na Figura 03.

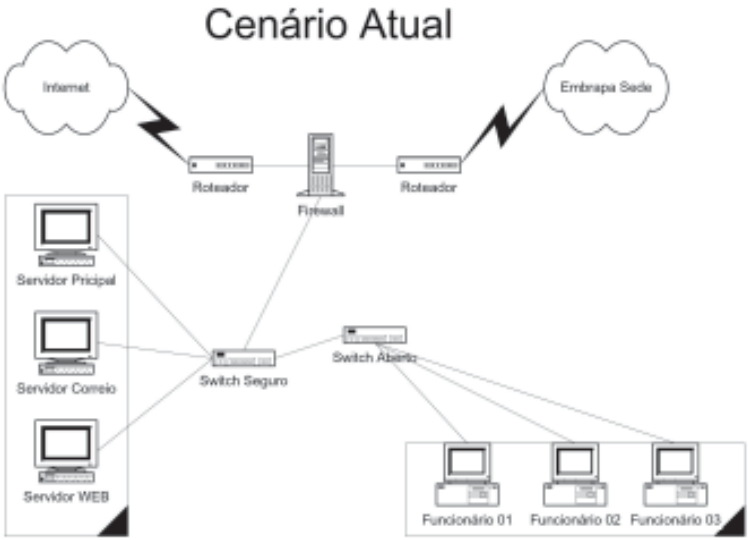

Figura 03. Logística de acesso externo - cenário atual.

5. CENÁRIO PROPOSTO

O cenário proposto fica basicamente parecido com o atual, porém é incluído mais um servidor VPN que é usado para dar suporte aos usuários que estejam fora da rede Embrapa, dando a possibilidade de acessar os serviços dessa rede de maneira segura.

Neste cenário, o cliente externo, usando um computado ligado à internet, chegará até o servidor VPN que o validará através de um login e uma senha e,

assim, fornecerá um endereço válido da rede a este computador, permitindo que a rede Embrapa possa ser acessada.

Este cliente deverá ter prévio conhecimento do endereço IP do servidor VPN e da chave de criptografia gerada pelo IPSec, conforme exemplificado na Figura 04.

Com este novo cenário, o empregado da Embrapa que estiver em trânsito, seja em casa ou em viagem, poderá a qualquer momento acessar os serviços da unidade ou da rede Embrapa.

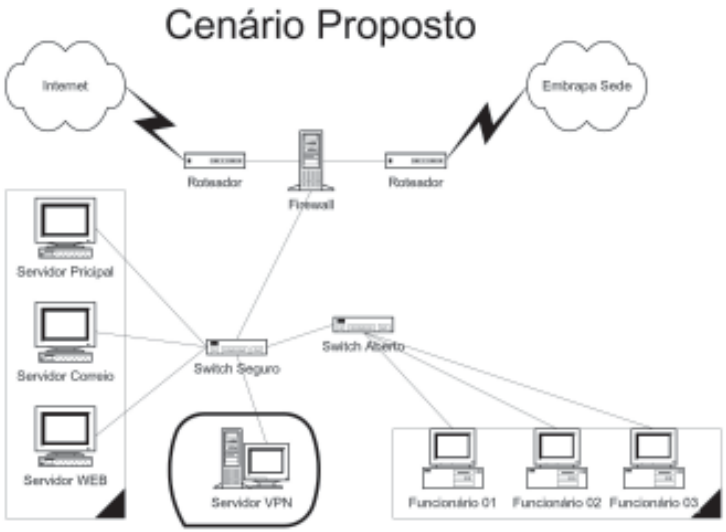

Figura 04. Logística de acesso externo - cenário proposto.

6. IMPLEMENTAÇÃO

A implementação da VPN ocorreu em um computador Pentium 4 com 120 GB de disco e 1 GB de memória RAM. O sistema operacional utilizado foi o Fedora Core 3, derivado do RedHat. O computador foi instalado do zero com todos os pacotes disponíveis na versão. Foram incluídos ou atualizados os seguintes pacotes RPM (Quadro 1).

Quadro 1. Relação de softwares dependentes.

Dkms-2.0.5.1noarch.rpm	Biblioteca dinâmica de suporte ao kernel
Kernel_ppp_mppe-0.0.5-2dkms.noarch	Modulo Microsoft para conexão PPP
Libpcap-0.8.3-5.i385.rpm	Bibliotecas POSIX
Logrotate-3.6.8-6tr.i586.rpm	Gerenciador de log
Mailx-8.1.1-32i386.rpm	Sistema de E-mail com suporte PPP
Ppp-2.4.3-4.fc3i386.rpm	Protocolo PPP
Pptpd-1.2.1-1.i386.rpm	Protocolo PPTP.

Os pacotes foram instalados e ou atualizados sem problemas, pois o Fedora Core 3 mostrou ser um sistema muito estável desde o início, reconhecendo inclusive todos os hardwares do sistema sem a necessidade de configuração manual.

6.1 Configuração do Servidor

Foi necessário criar ou alterar quatro arquivos, conforme mostra o Quadro 2.

Quadro 2. Arquivos de configuração, criados ou alterados.

/etc/modules.conf	Aliases para as chamados padrões necessários para a comunicação PPP.
/etc/pptp.conf	Arquivo de configuração do túnel PPTP.
/etc/ppp/options.pptpd	Configuração da parte de comunicação de dados.
/etc/ppp/mschap-secrets	Arquivo de senhas.

Os arquivos de configuração foram escritos de maneira a atender à necessidades mínimas de segurança e confiabilidade na comunicação PPP através de tunelamento.

Os arquivos ficaram com estes conteúdos (Quadros, 3, 4, 5 e 6).

Quadro 3. Arquivo modules.conf.

Alias char-major-108 ppp_generic
Alias tty-ldisc-3 ppp_async
Alias tty-ldisc-14 ppp_synctty
Alias ppp-compress-18 ppp_mppe
Alias ppp-compress-21 bsd_comp
Alias ppp-compress-24 ppp_deflate
Alias ppp-compress-26 ppp_deflate
Alias net-pf-47 ip_gre

Quadro 4. Arquivo pptp.conf.

Option /etc/ppp/options.pptpd	Localização do arquivo options.pptpd, base da configuração.
Logwtmp	Logar todos os acessos ao arquivo de login do sistema
Localip 200.134.20.241	IP servidor da VPN para uso do local interface eth0:1
Remoteip 200.202.158.1-254	Cadeia de IP´s para clientes

Quadro 5. Arquivo options.conf.

name pptpd	Nome da conexão, alias para facilitar a nomenclatura do servidor
refuse-pap	Recuse protocolo PAP
refuse-chap	Recuse protocolo CHAP
refuse-mschap	Recuse protocolo MSCHAP
Require-mschap-v2	Exija protocolo MSCHAPv2
Require-mppe-128	Exija Encriptação 128 bits
logfile /var/log/ppp/log_ppp	Arquivo para gravar log de todas as transações
Debug	Desmembre os logs
Lock	Trava a conexão de modo que não seja interceptada
bsdcomp 15,15	Compactar dados padrão BSDcommp

Quadro 6. Arquivo mschap-secrets

nabhen pptpd teste "*" germano pptpd teste "*" gerson pptpd a1a2a3a4 "*"	Arquivo contendo o usuário, o nome da conexão, a senha e o IP destinado. No caso de * será destinado o próximo IP livre

6.2. Configuração do Cliente

Como os usuários da empresa usam o windows como sistema operacional, elaborou-se a configuração do cliente baseada nesta interface. Os clientes foram testados nos ambientes operacionais Windows XP, Windows 2000, e Windows Milenium. Para configurar, é necessário o suporte a *dial up* com VPN, disponível em todas as versões.

Depois de instalado o suporte a *dial up* com vpn, o usuário deverá configurar as telas conforme a seguir:

6.2.1. Tela de configuração do Endereço de destino

Nesta tela (Figura 05) deve ser configurado o nome do servidor de VPN ou endereço IP, neste caso são, respectivamente, pomares.cnpf.embrapa.br, ou 200.134.20.5. Este endereço deve ser um endereço válido na internet, inclusive com reverso devidamente cadastrado.

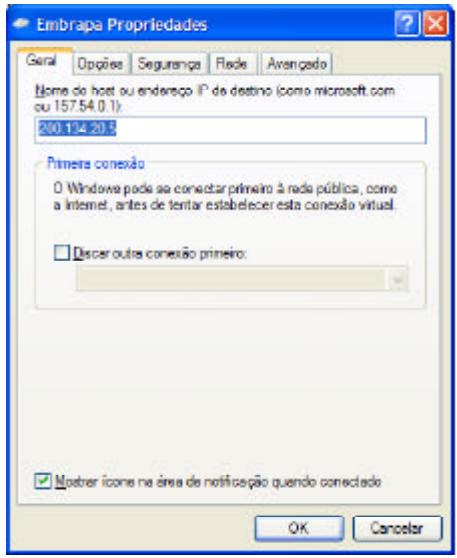

Figura 05. Tela de configuração do endereço de destino.

6.2.2. Tela de opções

Nesta tela (Figura 06) deve ser configurado a forma de solicitar senhas e quantas tentativas antes de desistir. Isto é útil no caso de uma conexão lenta.

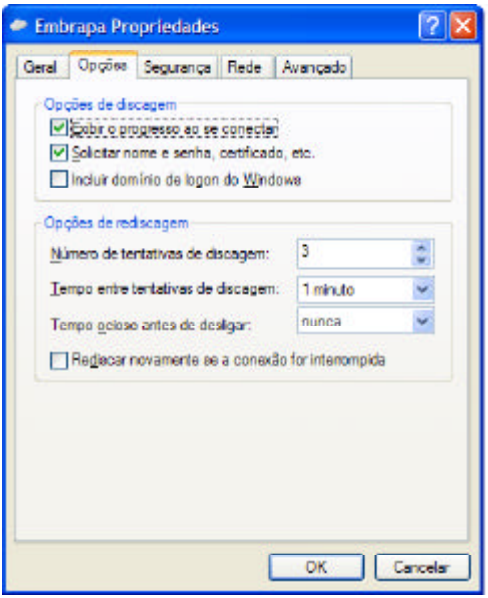

Figura 06. Tela de Opção.

6.2.3. Tela de parâmetros de segurança

Nesta tela (Figura 07), deve-se marcar a opção avançada ou personalizada, para poder entrar nos itens de configurações e marcar os parâmetros de criptografia e compactação de dados.

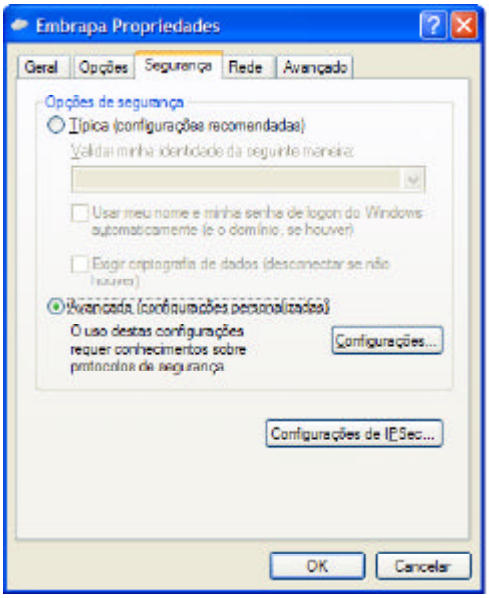

Figura 07. Tela de parâmetros ou segurança.

6.2.4. Tela de configurações avançadas

Nesta tela (Figura 08) devem ser marcados os itens “segurança máxima exigida” e “permitir apenas o protocolo Microsoft CHAP versão 2”. Recomenda-se não marcar outros protocolos, porém se forem marcadas eles serão ignorados.

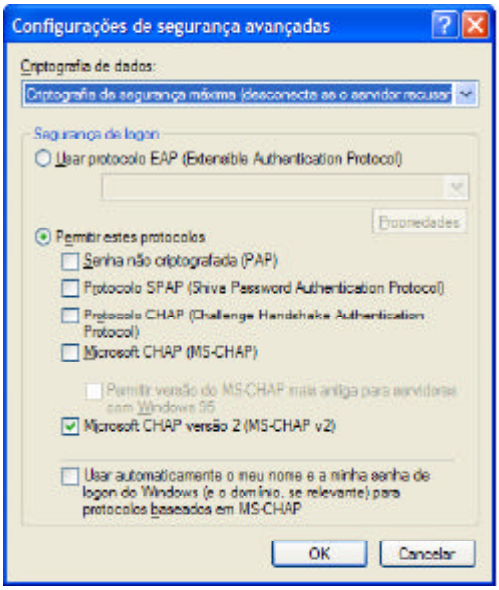

Figura 08.Tela de configurações.

6.2.5. Tela de opção de rede

Nesta tela (Figura 09) deve ser marcado a opção automático no tipo de VPN e deixar que o servidor e o cliente negociem a conexão. Os itens Protocolo TCP/IP, clientes para rede Microsoft obrigatoriamente devem estar marcados.

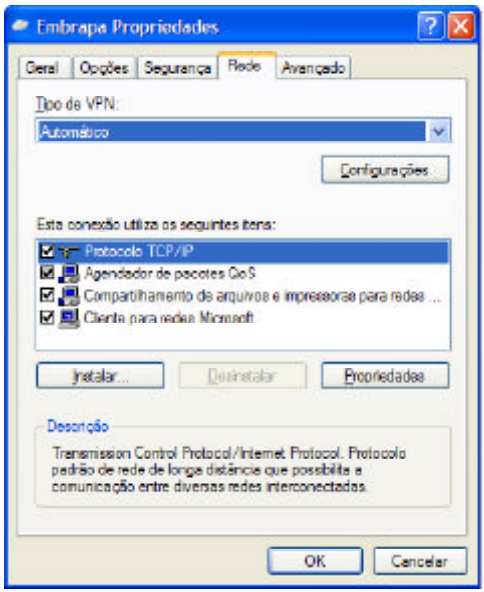

Figura 09.Tela de opção de rede.

6.2.6. Tela de login

Nesta tela (Figura 10), deve-se digitar o login e a senha fornecidos pelo pessoal de informática da unidade. Este login e senha tem validade determinadas para execução de serviços em casa ou no caso de viagem.

Figura 10. Tela de login.

6.3. Logs de Conexão

O servidor de VPN gera três tipos de logs para análise de uso da rede.

6.3.1. /var/log/messages

Local onde ficam armazenados os logs básicos das conexões entre cliente e servidor. Neste log ficam a maioria das mensagens do sistema operacional.

Arquivo de log da máquina pomares para o estabelecimento das conexões VPN, com arquivo /var/log/messages para uma conexão simples (Quadro 7).

Quadro 7. Parte do log do arquivo messages.

```
May  2 20:11:55 pomares pptpd[8998]: CTRL: Client 200.146.22.15
control connection started
May  2 20:11:55 pomares pptpd[8998]: CTRL: Starting call (launching
pppd, opening GRE)
May  2 20:11:55 pomares pppd[8999]: pppd 2.4.3 started by root, uid 0
May  2 20:11:55 pomares pppd[8999]: Using interface ppp0
May  2 20:11:55 pomares pppd[8999]: Connect: ppp0 <--> /dev/pts/3
May  2 20:11:55 pomares pptpd[8998]: CTRL: Ignored a SET LINK INFO
packet with real ACCMs!
May  2 20:11:55 pomares pppd[8999]: MPPE 128-bit stateless
compression enabled
May  2 20:11:57 pomares pppd[8999]: local  IP address 200.134.20.5
May  2 20:11:57 pomares pppd[8999]: remote IP address 200.134.20.241
...
May  2 20:13:03 pomares pppd[8999]: LCP terminated by peer (^[M-
d^TQ^@ < M-Mt^@^@^@^@)
May  2 20:13:03 pomares pppd[8999]: Connect time 1.1 minutes.
May  2 20:13:03 pomares pppd[8999]: Sent 0 bytes, received 4829 bytes.
May  2 20:13:03 pomares pppd[8999]: Modem hangup
May  2 20:13:03 pomares pppd[8999]: Connection terminated.
May  2 20:13:03 pomares pppd[8999]: Exit.
May  2 20:13:03 pomares pptpd[8998]: CTRL: Client 200.146.22.15
control connection finished
```

E para duas conexões simultâneas (Quadro 8).

Quadro 8. Parte do log do arquivo messages para duas conexões.

```
May  2 20:29:36 pomares pptpd[9297]: CTRL: Client 200.139.116.161 control connection started
May  2 20:29:36 pomares pptpd[9297]: CTRL: Starting call (launching pppd, opening GRE)
May  2 20:29:36 pomares pppd[9298]: pppd 2.4.3 started by root, uid 0
May  2 20:29:36 pomares pppd[9298]: Using interface ppp0
May  2 20:29:36 pomares pppd[9298]: Connect: ppp0 <--> /dev/pts/3
May  2 20:29:37 pomares pptpd[9297]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
May  2 20:29:37 pomares pppd[9298]: MPPE 128-bit stateless compression enabled
May  2 20:29:39 pomares pppd[9298]: local  IP address 200.134.20.5
May  2 20:29:39 pomares pppd[9298]: remote IP address 200.134.20.242
May  2 20:32:21 pomares pptpd[9371]: CTRL: Client 200.146.22.15 control connection started
May  2 20:32:21 pomares pptpd[9371]: CTRL: Starting call (launching pppd, opening GRE)
May  2 20:32:21 pomares pppd[9372]: pppd 2.4.3 started by root, uid 0
May  2 20:32:21 pomares pppd[9372]: Using interface ppp1
May  2 20:32:21 pomares pppd[9372]: Connect: ppp1 <--> /dev/pts/4
May  2 20:32:21 pomares pptpd[9371]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
May  2 20:32:22 pomares pppd[9372]: MPPE 128-bit stateless compression enabled
May  2 20:32:23 pomares pppd[9372]: local  IP address 200.134.20.5
May  2 20:32:23 pomares pppd[9372]: remote IP address 200.134.20.241
May  2 20:34:13 pomares pppd[9298]: LCP terminated by peer (^R^V        ^_^@ < M-Mt^@^@^@^@)
May  2 20:34:13 pomares pppd[9298]: Connect time 4.6 minutes.
May  2 20:34:13 pomares pppd[9298]: Sent 0 bytes, received 5296 bytes.
May  2 20:34:13 pomares pppd[9298]: Modem hangup
May  2 20:34:13 pomares pppd[9298]: Connection terminated.
May  2 20:34:13 pomares pppd[9298]: Exit.
May  2 20:34:1
```

6.3.2. /var/log/ppp/log_ppp

Local onde ficam armazenados todos os logs da comunicação PPP. Inclusive pode-se analisar a encriptação de dados e a forma de compactação.

Este arquivo é o mais complexo para análise (Quadro 9), porém pode se perceber toda a troca de informação entre as máquinas. A servidora registra com *sent* os pacotes enviados e *received* os recebidos.

Quadro 9. Parte do log do arquivo log.ppp.

```
Plugin /usr/lib/pptpd/pptpd-logwtmp.so loaded.
pptpd-logwtmp: $Version$
using channel 120
Using interface ppp0
Connect: ppp0 <--> /dev/pts/2
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <auth chap MS-v2> <magic
0xbcaa961f> <pcomp> <accomp>]
rcvd [LCP ConfReq id=0x0 <mru 1400> <magic 0x129d7959> <pcomp>
<accomp> <callback CBCP> <mrru 1614> <endpoint
[local:a0.37.6f.13.24.d8.4c.8e.a4.e3.9f.c8.0a.46.99.03.00.00.00.02]>]
sent [LCP ConfRej id=0x0 <callback CBCP> <mrru 1614>]
rcvd [LCP ConfReq id=0x1 <mru 1400> <magic 0x129d7959> <pcomp>
<accomp> <endpoint
[local:a0.37.6f.13.24.d8.4c.8e.a4.e3.9f.c8.0a.46.99.03.00.00.00.02]>]
sent [LCP ConfAck id=0x1 <mru 1400> <magic 0x129d7959> <pcomp>
<accomp> <endpoint
[local:a0.37.6f.13.24.d8.4c.8e.a4.e3.9f.c8.0a.46.99.03.00.00.00.02]>]
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <auth chap MS-v2> <magic
0xbcaa961f> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <auth chap MS-v2> <magic
0xbcaa961f> <pcomp> <accomp>]
sent [CHAP Challenge id=0x27 <808326bd5084c5cff3fd951906718df0>, name =
"pptpd"]
rcvd [LCP code=0xc id=0x2 12 9d 79 59 4d 53 52 41 53 56 35 2e 31 30]
```

continua

Quadro 9. Continuação...

```
sent [LCP CodeRej id = 0x2 0c 02 00 12 12 9d 79 59 4d 53 52 41 53 56 35 2e 31 30]
rcvd [LCP code = 0xc id = 0x3 12 9d 79 59 4d 53 52 41 53 2d 30 2d 4d 45 53 54 52
45]
sent [LCP CodeRej id = 0x3 0c 03 00 16 12 9d 79 59 4d 53 52 41 53 2d 30 2d 4d 45
53 54 52 45]
rcvd [CHAP Response id = 0x27
< 59ad7e0609c781dd0401fc8f1afba2b60000000000000000003b24235d50b5d055162
81619a56ddd58b9727ea5b0218dd600 >, name = "gerson"]
sent [CHAP Success id = 0x27
"S = 2B729196BAF331FB3CA055E4D560D577DE4E58E9 M = Access granted"]
sent [CCP ConfReq id = 0x1 < mppe + H -M + S -L -D -C >]
rcvd [CCP ConfReq id = 0x4 < mppe + H -M + S -L -D + C >]
sent [CCP ConfNak id = 0x4 < mppe + H -M + S -L -D -C >]
rcvd [IPCP ConfReq id = 0x5 < addr 0.0.0.0 > < ms-dns1 0.0.0.0 > < ms-wins 0.0.0.0 >
< ms-dns3 0.0.0.0 > < ms-wins 0.0.0.0 >]
sent [IPCP TermAck id = 0x5]
rcvd [CCP ConfAck id = 0x1 < mppe + H -M + S -L -D -C >]
rcvd [CCP ConfReq id = 0x6 < mppe + H -M + S -L -D -C >]
sent [CCP ConfAck id = 0x6 < mppe + H -M + S -L -D -C >]
MPPE 128-bit stateless compression enabled
sent [IPCP ConfReq id = 0x1 < compress VJ 0f 01 > < addr 200.134.20.241 >]
rcvd [IPCP ConfRej id = 0x1 < compress VJ 0f 01 >]
sent [IPCP ConfReq id = 0x2 < addr 200.134.20.241 >]
rcvd [IPCP ConfAck id = 0x2 < addr 200.134.20.241 >]
rcvd [IPCP ConfReq id = 0x7 < addr 0.0.0.0 > < ms-dns1 0.0.0.0 > < ms-wins 0.0.0.0 >
< ms-dns3 0.0.0.0 > < ms-wins 0.0.0.0 >]
sent [IPCP ConfRej id = 0x7 < ms-wins 0.0.0.0 > < ms-wins 0.0.0.0 >]
rcvd [IPCP ConfReq id = 0x8 < addr 0.0.0.0 > < ms-dns1 0.0.0.0 > < ms-dns3
0.0.0.0 >]
sent [IPCP ConfNak id = 0x8 < addr 200.202.158.1 > < ms-dns1 200.134.20.1 > < ms-
dns3 200.134.20.1 >]
rcvd [IPCP ConfReq id = 0x9 < addr 200.202.158.1 > < ms-dns1 200.134.20.1 > < ms-
dns3 200.134.20.1 >]
```

continua

Quadro 9. Continuação...

```
sent [IPCP ConfAck id = 0x9  < addr 200.202.158.1 >  < ms-dns1 200.134.20.1 >
 < ms-dns3 200.134.20.1 > ]
local  IP address 200.134.20.241
remote IP address 200.202.158.1
pptpd-logwtmp.so ip-up ppp0 gerson 200.146.64.51
Script /etc/ppp/ip-up started (pid 3240)
Script /etc/ppp/ip-up finished (pid 3240), status  =  0x0
Modem hangup
pptpd-logwtmp.so ip-down ppp0
Connect time 1.8 minutes.
Sent 266623 bytes, received 366396 bytes.
Script /etc/ppp/ip-down started (pid 3256)
MPPE disabled
sent [LCP TermReq id = 0x4 "MPPE disabled"]
Connection terminated.
```

6.3.3. /var/log/wtmp

Local onde são armazenados os *logins* bem sucedidos (Quadro 10). Recupera-se estas informações com o comando *last.*

Onde o terminal é PTS, significa que o usuário está na máquina, onde o terminal consta **ppp**, o usuário está na VPN. Quando consta PTS e um nome de máquina, a conexão é SSH.

Quadro 10. Log do arquivo wtmp.

User	Terminal	Local	Data Conexão
root	pts/2	reserva01	Tue May 10 10:10 still logged in
root	pts/2		Tue May 10 09:58 - 09:58 (00:00)
root	pts/2	reserva01	Tue May 10 09:30 - 09:56 (00:25)
gerson	ppp0	200.146.64.51	Mon May 9 22:53 - 22:55 (00:01)
root	pts/2	200.146.64.51.ad	Mon May 9 22:36 - 22:39 (00:03)
gerson	ppp0	200.146.64.51	Mon May 9 22:26 - 22:32 (00:05)
germano	ppp0	200.146.82.75	Mon May 9 22:07 - 22:21 (00:13)
root	pts/2	200.146.64.51.ad	Mon May 9 21:17 - 22:31 (01:14)
gerson	ppp0	200.146.72.235	Mon May 9 18:30 - 18:55 (00:25)
root	pts/2		Mon May 9 10:45 - 10:48 (00:02)
root	pts/2		Mon May 9 10:05 - 10:20 (00:15)
gerson	ppp0	200.134.20.251	Mon May 9 09:46 - 09:47 (00:01)
root	pts/7		Mon May 9 09:32 - 09:49 (00:17)
gerson	ppp0	200.134.20.251	Mon May 9 09:21 - 09:24 (00:02)
gerson	ppp0	200.134.20.251	Mon May 9 09:17 - 09:21 (00:04)

7. CONCLUSÃO

Com a crescente necessidade das pessoas em ter acesso a suas informações, a falta de segurança dos meios públicos, e do custo para se fazer uma conexão segura, as VPNs têm papel fundamental na garantia de um serviço confiável e barato.

Este serviço tem facilitado muito o trabalho de pesquisadores que necessitam usar serviços exclusivos da unidade de pontos remotos, pois estando a trabalho em outras localidades ficam sem acesso a suas pastas pessoais e sem acesso aos serviços gerados pela intranet da empresa.

Por outro lado, estes mesmos funcionários podem ter acesso até mesmo de suas residências sem a necessidade se deslocar até empresa, o que hoje ocorre, facilitando, assim, o desenvolvimento de suas atividades.

A implantação de um servidor VPN não é uma tarefa fácil, pois a literatura existente na rede apesar de ser muito extensa e repetitiva não fornece detalhamento de comandos ou explicação clara de todas as possibilidades. Foram consultados muitos manuais, todos com formato original em inglês.

A maior dificuldade apresentada foi garantir acesso com algum nível de segurança. Na implementação do processo, conseguiu-se o acesso de casa de alguns funcionários aos servidores de redes internos da Embrapa, o que foi, inclusive,na época, alvo de bons comentários na empresa em função dessa nova facilidade.

Este serviço além de facilitar o acesso remoto permite também economia de deslocamento e tempo à sede da empresa, localizada a cerca de 25 km da cidade.

8. REFERÊNCIAS

LIOU, K. C. Rede privada virtual. **News Generation**, v. 2, n. 8, 1998. Disponível em: <http://www.rnp.br/newsgen/9811/vpn.html>. Acesso em: 22 jul. 2006.

9. LITERATURA RECOMENDADA

HAMZEH, K.; PALL, G.; VERTHEIN, W.; TAARUD, J.; LITTLE, W.; ZORN, G. **RFC 2637**: Point-to-Point Tunneling Protocol (PPTP). [S.l.]: The Internet Society, 1999. Disponível em: <http://www.faqs.org/rfcs/rfc2637.html>. Acesso em: 10 jun. 2006.

PATEL, B.; INTEL, B.; ABOBA, W.; DIXON, M.; ZORN, G.; BOOTH, S. **RFC 3193**: securing L2TP using Ipsec. [S.l.]: The Internet Society, 2001. Disponível em: <http://www.faqs.org/rfcs/rfc3193.html>. Acesso em: 30 nov. 2006

RALIO, P. R. **VPN no Red hat Linux**. [S.l.]: Br-Linux-Org, 2003. Disponível em: <http://br-linux.org/tutoriais/000210.html>. Acesso em: 18 jul. 2006

ROSSI, M. A. G.; FRANZIN, O. Conceitos básicos de VPN. In: GPR SISTEMAS. **Portal**. Campinas, 2005. Disponível em: <http://www.gpr.com.br/download/vpn>. Acesso em: 15 out. 2006.

SIMPSON, W. **RFC 1994**: PPP Challenge Handshake Authentication Protocol (CHAP). Madison Heights: DayDreamer, 1996. Disponível em: <http://www.faqs.org/rfcs/rfc1994.html>. Acesso em: 16 jul. 2006.

ZORN, G. RFC 2759**: Microsoft PPP CHAP Extensions, Version 2. [S.l.]: Microsoft Corporation, 2000. Disponível em: <http://www.faqs.org/rfcs/rfc2759.html>. Acesso em:** 15 set. 2006.

VPN – Rede Privada Virtual: confidencialidade e integridade no transporte de informações: o que é VPN ?. São Paulo: Allnet Soluções Internet, 2003. Disponível em: <http://www.allnet.com.br/br/business/vpn/vpn.php#vpn1>. Acesso em: 15 nov. 2008.

10. VOCABULÁRIO

ATM	Asynchronous Transfer Mode, protocolo de telecomunicações.
Backbone	Esquema de ligações centrais que estruturam uma rede.
Criptografia	Formato de escrita codificada.
Datagrama	Pacote (ou trama ou datagrama) é a estrutura de dados.
Dial-Up	Conexão por linha discada.
DNS	O DNS (*D*omain *N*ame *S*ystem - Sistema de Nomes de Domínios).
Extranet	Parte de uma rede que usa a internet para compartilhar dados com segurança.
Firewall	Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou recepção de dados nocivos ou não autorizados de uma rede a outra.
Frame relay	O Frame Relay é uma eficiente tecnologia de comunicação de dados usada para transmitir de maneira rápida e barata a informação digital através de uma rede de dados, dividindo essas informações em frames (quadros) a um ou muitos destinos de um ou muitos e*nd-points*.
FreeBSD	O FreeBSD é um sistema operacional livre do tipo Unix descendente do BSD.
FTP	File Transfer Protocol; Protocolo de Transferência de Arquivos.
HTML	Hyper Text Markup Language; Linguagem de Marcação de Hipertexto.
HTTP	HyperText Transfer Protocol; Protocolo de Transferência de Hipertexto.
IETF	Internet Engineering Task Force; Força tarefa mundial para estruturar a Internet.
Internet	É um grupo de redes em escala mundial interligados por um mesmo protocolo.
Intranet	Rede local privada.
IP	Internet Protocol, o protocolo sob o qual assenta a infra-estrutura da Internet.

IPSEC	Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPSec) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos).
IPX	IPX é um protocolo proprietario da Novell.
Kernel	Kernel de um sistema operacional é entendido como o núcleo deste ou, numa tradução literal, cerne.
LANs	Local Area Network; Rede de area local.
Link	Uma ligação de ipertexto ou uma ligação de um computador à internet.
NETBEUI	NetBIOS Extended User Interface (Interface de Usuário Estendida NetBIOS.
OSI	(*Open Systems Interconnection*), ou Interconexão de Sistemas Abertos.
PPP	Point-to-Point Protocol, um protocolo para redes de computadores.
PPTP	Poit to Point Protocol; Protocolo para conexão ponto a ponto.
PTS	Pseudo-terminal Slave
RAM	Memória RAM (Random Access Memory), ou memória de acesso aleatório.
Switch	Um switch, que pode ser traduzido como comutador, é um dispositivo utilizado em redes de computadores para reencaminhar quadros (ou tramas em Portugal, e frames em inglês) entre os diversos nós.
SOLARIS	Solaris é um Sistema Operativo UNIX desenvolvido pela Sun Microsystems.
SSH	Secure Shell ou SSH é, simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede.
VPN	Virtual Private Network ; Rede Virtual Privada.
WAN	Wide Area Network ; Rede de área alargada ; Rede de longa distância.

WEB	A World Wide Web (que significa "rede de alcance mundial", em inglês; também conhecida como Web e WWW) é um sistema de documentos em hipermídia que são interligados e executados na Internet.
WWW	A World Wide Web (que significa "rede de alcance mundial", em inglês; também conhecida como Web e WWW) é um sistema de documentos em hipermídia que são interligados e executados na Internet.
X25	X.25 é conjunto de protocolos padronizado pela ITU-T para redes de longa distância.