

## O que é "VPN"?

### 1. Definições:

VPNs (Virtual Private Networks) são redes que possibilitam um acesso privado de comunicação, utilizando-se redes públicas já existentes, como a Internet. O termo refere-se a combinação de tecnologias que asseguram a comunicação entre dois pontos, através de um "túnel" que simula uma comunicação ponto-a-ponto inacessível à "escutas clandestinas" e interferências.

As VPNs podem ser usadas de duas maneiras. No primeiro caso, existe uma conexão (sempre através de um tunelamento via Internet) entre duas redes privadas como por exemplo, entre a matriz de uma corporação, em um ponto, e um escritório remoto, em outro ponto, ou entre a rede da matriz e a rede de um parceiro. Neste tipo de conexão, a manutenção do túnel entre os dois pontos é mantida por um servidor VPN dedicado ou por existentes INTERNET FIREWALLS. Na verdade, para estes exemplos, as VPNs podem ser encaradas como funções firewalls melhoradas. Este tipo de VPN é chamada de extranet.

Outra forma de se usar uma VPN é conectando-se um computador remoto individual à uma rede privada, novamente através da Internet. Neste caso, a VPN é implementada através de um software dentro do computador remoto. Este computador poderá usar uma conexão dial-up local para conectar-se a Internet, possibilitando assim o alcance à rede privada. A figura 1 mostra estas duas abordagens de VPNs.



Figura 1: dois tipos de VPNs

As VPNs permitem portanto, "virtualizar" as comunicações de uma corporação, tornando-as "invisíveis" a observadores externos e aproveitando a infra-estrutura das comunicações existentes.

## 2. Motivações

Como visto anteriormente, as VPNs permitem estender as redes corporativas de uma empresa à pontos distantes da mesma, como outros escritórios, filiais, parceiros e até mesmo uma residência. Porém, ao invés de utilizar-se de um grande número de linhas dedicadas para a interconexão entre seus diversos pontos, o que onera muito o custo da rede (aluguel de linhas dedicadas, manutenção de diversos links para cada conexão, manutenção de equipamentos para diferentes conexões, uso de vários roteadores, monitoramento de tráfego nas portas de acesso remoto, grande número de portas, etc), uma VPN aproveita os serviços das redes IP espalhadas mundialmente, inclusive a Internet, ou até mesmo os provedores de serviços baseados em IP backbones privados, os quais apesar de limitados em alcance, poderão oferecer um uma melhor performance de serviço que a Internet, em detrimento do aumento de custos. Fazendo-se então, uma mistura de serviços prestados pela Internet e serviços prestados por IPs backbones privados, uma corporação poderá tirar vantagens sobre a performance do serviço e a redução dos custos.

Outra grande vantagem das VPNs é que elas podem permitir acesso a qualquer lugar acessado pela Internet e, como a Internet está presente em praticamente todos os lugares do mundo, conexões potenciais de VPNs poderão ser facilmente estabelecidas. Assim, no lugar de chamadas à longa distância, os usuários desta rede poderão, por exemplo, fazer ligações via Internet local, cuja tarifação é bem menor.

Como as VPNs possuem plataformas independentes qualquer computador configurado para uma rede baseada em IP, pode ser incorporado à VPN sem que uma modificação seja necessária, a não ser a instalação de um software para acesso remoto.

Ao contrário das redes privadas tradicionais que necessitam de vários links dedicados E1 (2Mbps), os quais, como dito anteriormente, acarretam diversos custos mensais fixos, mesmos quando os links não estão sendo utilizados, as redes VPNs utilizam um único link com uma banda menor (512Kbps a 768Kbps), com custo variável de acordo com sua utilização. Este único link também permite a existência de somente um roteador do lado do cliente para reunir todos os serviços de Internet e WAN, o que também permitirá redução nos custos de suporte e manutenção.

Existe ainda o fato de redes VPNs serem facilmente escaláveis. Para se interconectar mais um escritório a rede, deve-se contatar o provedor de serviço para a instalação do link local e respectiva configuração dos poucos equipamentos nas premissas do cliente. Da mesma forma, no momento em que a utilização da rede esbarrar na banda disponível no link local alugado do provedor, basta requisitar um aumento desta banda para se determinar uma melhora considerável no desempenho da rede.

O gerenciamento da rede pode ser realizado pela própria empresa utilizadora da VPN, sendo que as alterações ocorridas na rede, como endereçamento, autenticação de usuários e determinação de privilégios de rede, são efetuadas de forma transparente ao provedor de serviço, levando a uma maior flexibilidade.

### Figuras Comparativas:

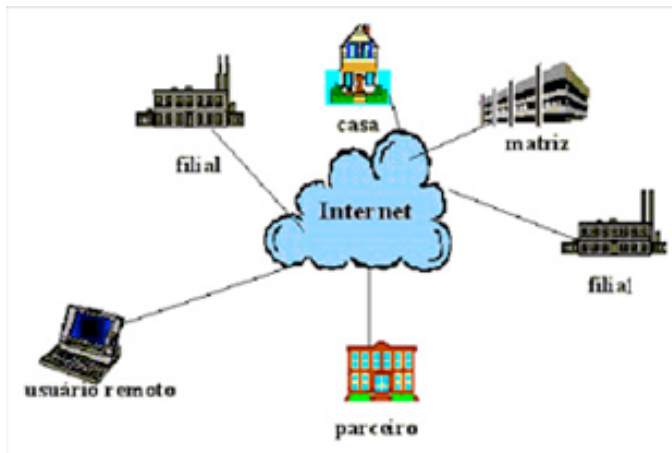


Figura 2: Rede VPN

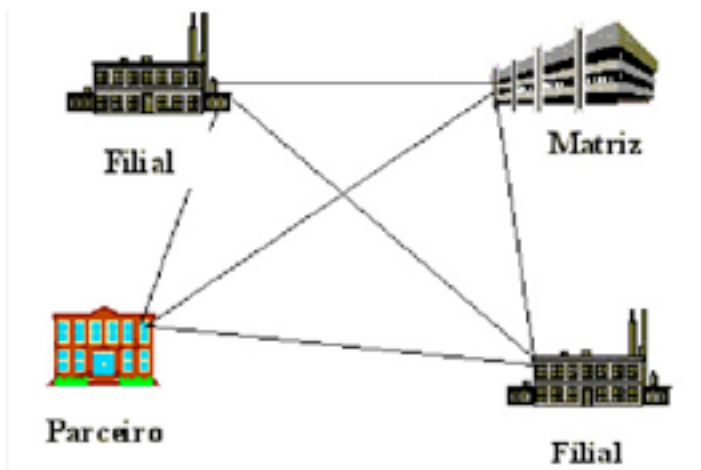


Figura 3: Rede Privada Convencional



Figura 4: comparação dos custos entre uma rede tradicional e uma VPN

As VPNs permitem então:

- uma difusão da rede corporativa de uma empresa a custos mais baixos;
- acesso seguro e fácil de usuários remotos às redes corporativas;
- comunicação segura ente usuários da rede;
- escalabilidade, etc

### 3. Algumas considerações para a implementação de uma VPN

Existe um aspecto primordial que deve ser levado em consideração para o desenvolvimento de VPNs sobre a estrutura da rede já existente: a segurança.

Os protocolos TCP/IP (Transmission Control Protocol /Internet Protocol) e a própria Internet, não foram originalmente projetados tendo a segurança como prioridade, porque o número de usuários e os tipos de aplicações não requeriam maiores esforços para a garantia da mesma. Mas, se as VPNs são substitutos confiáveis para as linhas dedicadas e outros links de WAN, tecnologias capazes de garantir segurança e performance tiveram que ser acrescentadas à Internet. Felizmente, os padrões para segurança de dados sobre redes IPs evoluíram de tal forma que permitiram a criação de VPNs.

As tecnologias que possibilitaram a criação de um meio seguro de comunicação dentro da Internet asseguram que uma VPN seja capaz de:

- Proteger a comunicação de escutas clandestinas: a privacidade ou proteção dos dados é conseguida pela criptografia que, através de transformações matemáticas complexas, "codifica" os pacotes originais, para depois, decodificá-los no final do túnel. Esta codificação é o aspecto mais difícil e crítico em sistemas que implementam a criptografia.
- Proteger os dados de alterações: esta proteção é alcançada através de transformações matemáticas chamadas de "hashing functions", as quais criam "impressões digitais" utilizadas para reconhecer os pacotes alterados.
- Proteger a rede contra intrusos: a autenticação dos usuários previne a entrada de elementos não autorizados. Vários sistemas baseados em "passwords" ou "challenge response", como o protocolo CHAP (Challenge Handshake Authentication Protocol) e o RADIUS (Remote Dial-in Service Protocol), assim como tokens baseados em hardware e certificados digitais, podem ser usados para a autenticação de usuários e para controlar o acesso dentro da rede.

#### **4. Etapas da conexão através de uma VPN**

Primeiramente é feita a autenticação entre os dois pontos. Essa autenticação permite ao sistema enxergar se a origem dos dados faz parte da comunidade que pode exercer acesso a rede. Será o laptop de algum funcionário ou um roteador de um filial? Ou será alguém se passando por um usuário que faz parte da comunidade?

Em seguida, o servidor VPN verifica quais serviços que o usuário tem permissão para acessar, monitorando assim, o subsequente tráfego de dados. Este passo é chamado de autorização e visa negar acesso a um usuário que não está autorizado a acessar a rede como um todo, ou simplesmente restringir o acesso de usuários.

Uma vez formado o túnel, seu ponto de partida adiciona cabeçalhos especiais aos pacotes que serão endereçados ao outro ponto do túnel, para em seguida, criptografar e encapsular toda a informação na forma de novos pacotes IPs. Os cabeçalhos internos permitirão então a autenticação da informação, e serão capazes de detectar qualquer alteração dos dados enviados.

#### **5. Protocolos de Tunelamento:**

Tunelamento é o encapsulamento ponto-a-ponto das transmissões dentro de pacotes IP. O tunelamento permite:

- tráfego de dados de várias fontes para diversos destinos em uma mesma infra-estrutura;

- tráfego de diferentes protocolos em uma mesma infra-estrutura;
- garantia de QoS (Quality of Service), direcionado e priorizando o tráfego de dados para destinos específicos.

As VPNs são, geralmente redes dinâmicas ou seja, as conexões são formadas de acordo com as necessidades das corporações. Assim, ao contrário das linhas dedicadas utilizadas por uma estrutura de rede privada tradicional, as VPNs não mantêm links permanentes entre dois pontos da rede da corporação, pelo contrário, quando uma conexão se faz necessária entre dois pontos desta corporação, ela é criada e quando a mesma não for mais necessária, ela será desativada, fazendo com que a banda esteja disponível para outros usuários.

Os túneis podem consistir de dois tipos de pontos finais: um computador individual ou uma LAN com um gateway seguro, que poderá ser um roteador ou um firewall. Porém, somente duas combinações desse pontos finais, são consideradas nos projetos de VPNs. No primeiro caso, tunelamento LAN-to-LAN, um gateway seguro em cada ponto servirá de interface entre o túnel e a LAN privada. Desta forma, usuários de ambas as LANs poderão utilizar o túnel transparentemente para comunicarem entre si.

Um segundo caso, tunelamento Client-to-LAN, é aquele utilizado por usuários remotos que desejam acessar a LAN corporativa. O cliente, ou seja, o usuário remoto, inicia o tunelamento em seu ponto, para a troca de tráfego com a rede corporativa. A ferramenta para esta comunicação é um software instalado em seu computador, que permite transpor o gateway que protege a LAN de destino.

A figura abaixo é uma ilustração genérica do processo de tunelamento:

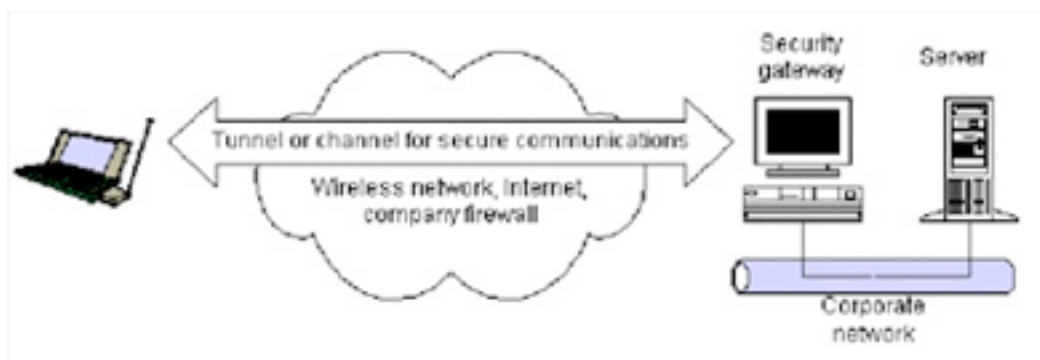


Figura 5: o túnel seguro da VPN

## Os principais protocolos de tunelamento são:

### GRE (Generic Routing Protocol)

Túneis GRE são geralmente configurados entre roteadores fonte e roteadores destino (pacotes ponto-a-ponto). Os pacotes designados para serem enviados através do túnel (já encapsulados com um cabeçalho de um protocolo como, por exemplo, o IP) são encapsulados por um novo cabeçalho (cabeçalho GRE) e colocados no túnel com o endereço de destino do final do túnel. Ao chegar a este final, os pacotes são desencapsulados (retira-se o cabeçalho GRE) e continuarão seu caminho para o destino determinado pelo cabeçalho original.



Figura 6: protocolo GRE

### Desvantagens:

- Os túneis GRE são, geralmente, configurados manualmente, o que requer um esforço grande no gerenciamento e manutenção de acordo com a quantidade de túneis: toda vez que o final de um túnel mudar, ele deverá ser manualmente configurado.
- Embora a quantidade de processamento requerida para encapsular um pacote GRE pareça pequena, existe uma relação direta entre o número de túneis a serem configurados e o processamento requerido para o encapsulamento dos pacotes GRE: quanto maior a quantidade de túneis, maior será o processamento requerido para o encapsulamento
- Uma grande quantidade de túneis poderá afetar a eficiência da rede.

## **PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding), L2TP (Layer 2 Tunneling Protocol)**

Ao contrário do GRE, estes protocolos são utilizados em VPDNs (Virtual Private Dial Network), redes que proporcionam acesso á rede corporativa por usuários remotos, através de uma linha discada (provedor de acesso).

### **PPTP**

O protocolo PPTP é um modelo "voluntário" de tunelamento, ou seja , permite que o próprio sistema do usuário final, por exemplo, um computador, configure e estabeleça conexões discretas ponto-a-ponto para um servidor PPTP, localizado arbitrariamente, sem a intermediação do provedor de acesso. Este protocolo constrói as funcionalidades do protocolo PPP (Point-to-Point Protocol - um dos protocolos mais utilizados na Internet para acesso remoto) para o tunelamento dos pacotes até seu destino final. Na verdade, o PPTP encapsula pacotes PPP utilizando-se de uma versão modificada do GRE, o que torna o PPTP capaz de lidar com outros tipos de pacotes além do IP, como o IPX (Internet Packet Exchange) e o NetBEUI (Network Basic Input/Output System Extended User Interface), pois é um protocolo baseado na camada 2 do modelo OSI (enlace).

Neste modelo, um usuário disca para o provedor de acesso á rede, mas a conexão PPP é encerrada no próprio servidor de acesso. Uma conexão PPTP é então estabelecida entre o sistema do usuário e qualquer outro servidor PPTP, o qual o usuário deseja conectar, desde que o mesmo seja alcançável por uma rota tradicional e que o usuário tenha privilégios apropriados no servidor PPTP.

### **L2F**

Foi um dos primeiros protocolos utilizado por VPNs. Como o PPTP, o L2F foi projetado como um protocolo de tunelamento entre usuários remotos e corporações. Uma grande diferença entre o PPTP e o L2F, é o fato do mesmo não depender de IP e, por isso, é capaz de trabalhar diretamente com outros meios como FRAME RELAY ou ATM.

Este protocolo utiliza conexões PPP para a autenticação de usuários remotos, mas também inclui suporte para TACACS+ e RADIUS para uma autenticação desde o início da conexão. Na verdade, a autenticação é feita em dois níveis: primeiro, quando a conexão é solicitada pelo usuário ao provedor de acesso; depois, quando o túnel se forma, o gateway da corporação também irá requerer uma autenticação.

A grande vantagem desse protocolo é que os túneis podem suportar mais de

uma conexão, o que não é possível no protocolo PPTP. Além disso, o L2F também permite tratar de outros pacotes diferentes de IP, como o IPX e o NetBEUI por ser um protocolo baseado na camada 2 do modelo OSI.

## **L2TP**

Este protocolo foi criado pela IETF (Internet Engineering Task Force) para resolver as falhas do PPTP e do L2F. Na verdade, utiliza os mesmos conceitos do L2F e assim como este, foi desenvolvido para transportar pacotes por diferentes meios, como X.25, frame-relay e ATM e também é capaz de tratar de outros pacotes diferentes de IP, como o IPX e o NetBEUI (protocolo baseado na camada 2 do modelo OSI).

O L2TP é porém, um modelo de tunelamento "compulsório", ou seja, criado pelo provedor de acesso, não permitindo ao usuário qualquer participação na formação do túnel (o tunelamento é iniciado pelo provedor de acesso). Neste modelo, o usuário discar para o provedor de acesso à rede e, de acordo com o perfil configurado para o usuário e ainda, em caso de autenticação positiva, um túnel L2TP é estabelecido dinamicamente para um ponto pré-determinado, onde a conexão PPP é encerrada.

## **PPTP x L2TP**

Apesar de parecidos, ambos os protocolos, L2TP ou PPTP, diferenciam-se quanto suas aplicações, ou melhor, a escolha do protocolo a ser utilizado é baseado na determinação da posse do controle sobre o túnel: controlado pelo usuário ou pelo provedor de acesso.

No protocolo PPTP, o usuário remoto tem a possibilidade de escolher o final do túnel, destino dos pacotes. Uma grande vantagem desta característica é que, quando os destinos mudam com muita frequência, nenhuma modificação (configuração) nos equipamentos por onde o túnel passa se torna necessária. Além disso, os túneis PPTP são transparentes aos provedores de acesso e nenhuma outra ação, além de prover serviço de acesso à rede, se faz necessária. Usuários com perfis diferenciados em relação aos locais de acesso - diferentes cidades, estados e países - se utilizam deste protocolo com mais frequência pelo fato de se tornar desnecessária a intermediação do provedor no estabelecimento do túnel. Somente é necessário saber o número local para o acesso e o sistema do usuário, seu laptop, realizará o resto.

A desvantagem do protocolo L2TP é que, como o controle está na mão do provedor, o mesmo está fornecendo um serviço extra que poderá ser cobrado.

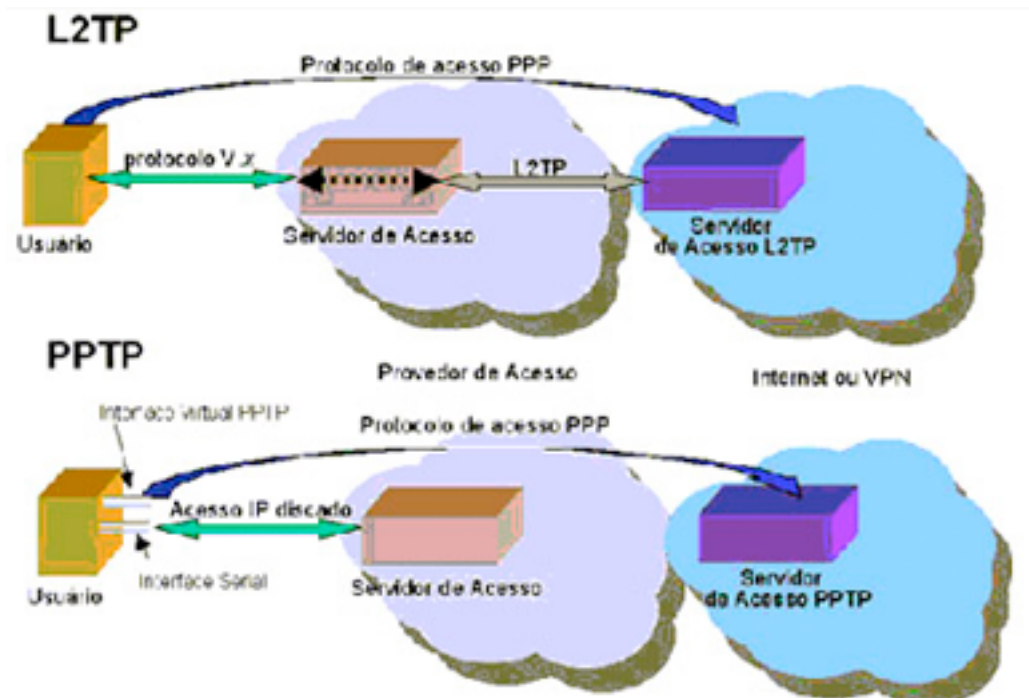


Figura 7: PPTP x L2TP

## IPSec

PPTP, L2F e L2TP não incluem criptografia ou processamento para tratar chaves criptográficas, o que é bastante recomendado para garantir a segurança dos pacotes. Por isso, surgiu um dos mais importantes protocolos, criado para garantir a segurança da próxima geração de pacotes IP (IPv6) e que, no momento, vem sendo utilizado com protocolos IPv4.

O IPSec permite ao usuário, ou ao gateway seguro que está agindo em seu favor, autenticar ou criptografar cada pacote IP, ou ainda, fazer os dois processos simultaneamente. Assim, separando os processos de autenticação e de criptografia, surgiram dois diferentes métodos para a utilização do IPSec, chamados de modos: no modo transporte, somente o segmento da camada de transporte de um pacote IP é autenticado ou criptografado; a outra abordagem, autenticação e criptografia de todo o pacote IP, é chamada de modo túnel. Enquanto que no modo transporte o IPSec tem provado ser eficiente para várias situações, no modo túnel ele é capaz de prover uma proteção maior contra certos ataques e monitoração de tráfego que podem ocorrer na Internet.

O IPSec é baseado em várias tecnologias de criptografias padronizadas para proverem confiabilidade, integridade de dados e confiabilidade. Por exemplo,

o IPSec utiliza:

- Diffie-Hellman-Key-exchanges para entregar chaves criptográficas entre as partes na rede pública.
- Public-key-cryptography para sinalizar trocas do tipo Diffie-Hellman e garantir a identificação das duas partes, evitando assim, ataques de intrusos no meio do caminho.
- DES e outros algoritmos para criptografar dados.
- Algoritmos para a autenticação de pacotes que utilizam "hashing functions".
- Certificados digitais para validar chaves públicas.

Existe duas maneiras para lidar com a troca de chaves e gerenciamento numa arquitetura IPSec: chaveamento manual (manual keying) e Internet Key Exchange (IKE) para gerenciamento automático de chaves. Enquanto o chaveamento manual pode ser usado em VPNs com um número pequeno de sites, o IKE deve ser obrigatoriamente em VPNs que suportam um grande número de sites e usuários remotos.

O IPSec tem sido considerado a melhor evolução para ambientes IP por incluir fortes modelos de segurança - criptografia , autenticação e troca de chaves - mas não foi desenvolvido para suportar outros tipos de pacotes além do IP. No caso de pacotes multiprotocolos, devem ser usados PPTP ou L2TP que suportam outros tipos de pacotes.

## 6. Soluções para VPNs

Existe quatro componentes básicos para a implementação de uma VPN baseada na Internet: a Internet, gateways seguros, servidores com políticas de segurança e certificados de autenticidade.

A Internet provê a "sustentação" de uma VPN e os gateways seguros são colocados na fronteira entre a rede privada e a rede pública para prevenirem a entrada de intrusos, e ainda são capazes de fornecer o tunelamento e a criptografia antes da transmissão dos dados privados pela rede pública. Os gateways seguros podem ser: roteadores, firewalls, hardwares específicos e softwares.

Como roteadores necessitam examinar e processar cada pacote que deixa a LAN, parece natural incluir-se a criptografia dos pacotes nos roteadores. Por isso existe no mercado dois produtos que desempenham esta função em roteadores: softwares especiais (software adicionado ao roteador) ou placas com coprocessadores que possuem ferramentas de criptografias (hardware

adicionado ao roteador). A grande desvantagem dessas soluções é que, se o roteador cair, a VPN também cairá.

As firewalls, assim como os roteadores, também devem processar todo o tráfego IP, neste caso, baseando-se em filtros definidos pelas mesmas. Por causa de todo o processamento realizado na firewalls, elas não são aconselhadas para tunelamento de grandes redes com grande volume de tráfego. A combinação de tunelamento e criptografia em firewalls será mais apropriada para redes pequenas com pouco volume de tráfego (1 a 2Mbps sobre um link de LAN). Da mesma forma que os roteadores, as firewalls podem ser um ponto de falha de VPNs.

A utilização de hardware desenvolvido para implementar as tarefas de tunelamento, criptografia e autenticação é outra solução de VPN. Esses dispositivos operam como pontes, implementando a criptografia, tipicamente colocadas entre o roteador e os links de WANs. Apesar da maioria desses hardwares serem desenvolvidos para configurações LAN-to-LAN, alguns produtos podem suportar túneis client-to-LAN. A grande vantagem desta solução é o fato de várias funções serem implementadas por um dispositivo único. Assim, não há necessidade de se instalar e gerenciar uma grande quantidade de equipamentos diferentes, fazendo com que esta implementação seja muito mais simples que a instalação de um software em um firewall, a reconfiguração de um roteador ou ainda a instalação de um servidor RADIUS, por exemplo.

Uma VPN desenvolvida por software também é capaz de criar e gerenciar túneis entre pares de gateways seguros ou, entre um cliente remoto e um gateway seguro. Esta é uma solução que apresenta um custo baixo, mas desaconselhada para redes que processam grande volume de tráfego. Sua vantagem, além do baixo custo, é que esta implementação pode ser configurada em servidores já existentes e seus clientes. Além disso, muitos desses softwares se encaixam perfeitamente para conexões client-to-LAN.

A política de segurança dos servidores também é outro aspecto fundamental para implementação de VPNs. Um servidor seguro deve manter uma lista de controle de acesso e outras informações relacionadas aos usuários, que serão utilizadas pelos gateways para a determinação do tráfego autorizado. Por exemplo, em alguns sistemas, o acesso pode ser controlado por um servidor RADIUS.

Por último, certificados de autenticidade são necessários para verificar as chaves trocadas entre sites ou usuários remotos. As corporações podem preferir manter seu próprio banco de dados de certificados digitais para seus usuários através de um servidor de certificado ou, quando o número de usuários for pequeno, a verificação das chaves poderá requerer o intermédio de uma terceira parte, a qual mantém os certificados digitais associados a chaves criptográficas, pois a manutenção de um servidor para isso será muito onerosa.

## 7. A escolha da melhor solução para VPN

Vejamos as vantagens e desvantagens de cada solução para a implementação de VPNs: apenas software, software auxiliado por hardware e hardware específico.

O encapsulamento aumenta o tamanho dos pacotes, conseqüentemente, os roteadores poderão achar que os pacotes estão demasiadamente grandes e fragmentá-los, degradando assim a performance da rede. A fragmentação de pacotes e a criptografia poderão reduzir a performance de sistemas discados a níveis inaceitáveis mas a compressão de dados poderá solucionar este problema. No entanto, a combinação de compressão com encapsulamento, irá requerer um poder computacional mais robusto para atender às necessidades de segurança. Por isso, uma VPN implementada através de hardware, devido á seu poder computacional irá alcançar uma melhor performance. Este tipo de implementação também fornece uma melhor segurança - física e lógica - para a rede, além de permitir um volume de tráfico maior. A desvantagem desta implementação é um custo mais alto e o uso de hardware especializado.

Já uma VPN implementada através de software terá critérios menos rígidos de segurança mas se encaixa perfeitamente para atender às necessidades de conexão de pequenos volumes que não precisam de grandes requisitos de segurança e possuem um custo menor.

Quanto a performance de VPNs implementadas por software assistido por hardware, está dependerá da performance dos equipamentos aos quais o software está relacionado.

A tabela a seguir resume os aspectos a serem considerados para a escolha do tipo de solução para a implementação de uma VPN.

Solução	Apenas software	Software assistido por Hardware	Hardware especializado
Performance	baixa	média-baixa	alta
Segurança	plataforma fisicamente e logicamente insegura	plataforma fisicamente e logicamente insegura	fisicamente e logicamente seguro
Aplicações possíveis	dial-up a uma taxa de 128Kbps para dados ISDN	ISDN à velocidades T1	Velocidades dial-up até 100 Mbps
Produtos	Firewalls, Softwares de VPNS	Cartões de criptografia para roteadores, PCs (Personal Communication Services)	Hardware especializado

## 8. Performance e QoS

Dois fatores determinam a performance das VPNs:

- . A velocidade das transmissões sobre a Internet ou sobre outra rede ou backbone IP
- . A eficiência do processamento dos pacotes (estabelecimento de uma seção segura, encapsulamento e criptografia de pacotes) em cada ponto da conexão: origem e destino.

A Internet não foi projetada inicialmente para garantir níveis confiáveis e consistentes de tempo de resposta. Na verdade, a Internet é um meio de comunicação "best effort", ou seja, realiza o máximo de esforço para prestar o serviço a qual é destinada: a transmissão de dados da origem ao destino. Além disso, o criptografia e o processo de tunelamento podem influir bastante na velocidade de transmissão dos dados pela Internet. Contudo, muitas redes corporativas, não podem ficar a mercê dessas flutuações de performance e acesso da Internet.

Alguns provedores de serviço resolveram o problema de velocidade de transmissão oferecendo acordos de Qualidade de Serviço (QoS), e garantia de banda á níveis específicos. Mas , atualmente, o método mais eficaz para adquirir QoS é mandar o tráfico VPN sobre o próprio IP backbone do provedor de serviço, ou seja, sobre o frame relay do provedor ou sobre circuitos ATM, e não sobre a Internet.

Também existem hoje, diversos grupos de estudos ou Task Forces da IETF tentando solucionar alguns dos problemas relacionados a performance e Qualidade de Serviço na Internet. São eles :

- RFC2211, "Specification of the Controlled-Load Network Element Service,", J. Wroclawski, September 1997.
- RFC2212, "Specification of Guaranteed Quality of Service,", S. Shenker, C. Partridge, R. Guerin, September 1997.
- RFC2208, "Resource ReSerVation Protocol (RSVP) Version 1 - Applicability Statement, Some Guidelines on Deployment," A. Mankin, F. Baker, S. Bradner, M. O'Dell, A. Romanow, A. Weinrib, L. Zhang, September 1997.