Trabalho de Redes: VPNs

UNIVERSIDADE CATÓLICA DO SALVADOR

DATA: 24/09/2003

TURNO: NOTURNO

ALUNOS: DANILLO ANDRADE
LEANDRO TORRES CAVALCANTI

Roteiro

1. **Definição**
2. **Motivação**
3. **Funções Básicas**
4. **Protocolos**
5. **Tipos**
6. **Soluções**
7. **Vantagens e Benefícios**
8. **Conclusão**
9. **Referências**

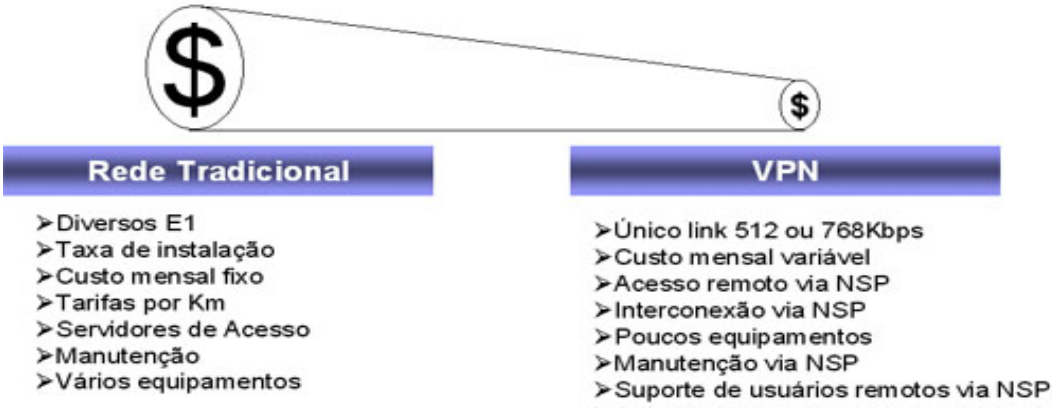
1. Definição:

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 são então redes que permitem "virtualizar" as comunicações de uma corporação, tornando-as "invisíveis" a observadores externos (criptografando o seu conteúdo) e aproveitando a infra-estrutura das comunicações existentes.

2. Motivação:

Enquanto as VPNs oferecem reduções de custos em métodos de comunicações – como links dedicados para diversas aplicações – podemos vislumbrar diversas outras vantagens, incluindo reduções de custos em treinamento e equipamento, aumento de flexibilidade e escalabilidade e facilidade no gerenciamento da rede. Primeiramente a comparação de custos entre redes corporativas tradicionais e redes corporativas que utilizam VPN. As rede tradicional é baseada em diversos links dedicados E1 (2Mbps), acarretando altos custos mensais fixos, custos de instalação e utilização de diversos equipamentos. Para usuários remotos, devem ser mantidos equipamentos provedores de acesso e alugadas diversas linhas da companhia telefônica local. Enquanto isso, redes baseadas em VPNs utilizam um único link com banda menor (512Kbps ou 768Kbps) com custo variável, necessitam de somente um roteador no lado do cliente reunindo todos os serviços – Internet e WAN – em um só, provêm acesso remoto através de um provedor de Internet que detêm os provedores de acesso e as linhas telefônicas e acarreta um diminuição nos custos com suporte/manutenção.

Veja abaixo um quadro comparativo :



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, um simples telefonema requisitando um aumento desta banda pode determinar uma melhora considerável no desempenho da rede. O gerenciamento da rede é realizado pela própria empresa utilizadora da VPN, sendo que as mudanças/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.

3. Funções Básicas:

A utilização de redes públicas tende a apresentar custos muito menores que os obtidos com a implantação de redes privadas, sendo este, justamente o grande estímulo para o uso de VPNs. No entanto, para que esta abordagem se torne efetiva, a VPN deve prover um conjunto de funções que garanta *Confidencialidade*, *Integridade* e *Autenticidade*.

Confidencialidade:

Tendo em vista que estarão sendo utilizados meios públicos de comunicação, a tarefa de interceptar uma seqüência de dados é relativamente simples. É imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos.

Integridade:

Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN**.**

Autenticidade:

Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados por um segundo elemento que seguramente tenha autorização para fazer parte da VPN. Dependendo da técnica utilizada na implementação da VPN, a privacidade das informações poderá ser garantida apenas para os dados, ou para todo o pacote (cabeçalho e dados).

Quatro técnicas podem ser usadas para a implementação de soluções VPN:

Modo Transmissão:

Somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes.

Modo Transporte:

Somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes. É uma solução de segurança adequada, para implementações onde os dados trafegam somente entre dois nós da comunicação.

Modo Túnel Criptografado:

Tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e de destino.

Modo Túnel Não Criptografado:

Tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino. No entanto, cabeçalho e dados são mantidos tal como gerados na origem, não garantindo a privacidade.

Para disponibilizar as funcionalidades descritas anteriormente, a implementação de VPN lança mão dos conceitos e recursos de criptografia, autenticação e controle de acesso.

3.1 Criptografia:

A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma seqüência de bits (chave) como padrão a ser utilizado na criptografia. Partindo dos dados que serão transmitidos, o objetivo é criar uma seqüência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma chave.

São chamadas de Chave Simétrica e de Chave Assimétrica as tecnologias utilizadas para criptografar dados:

- Chave Simétrica ou Chave Privada:

  É a técnica de criptografia onde é utilizada a mesma chave para criptografar e descriptografar os dados. Sendo assim, a manutenção da chave em segredo é fundamental para a eficiência do processo.

- Chave Assimétrica ou Chave Pública:

É a técnica de criptografia onde as chaves utilizadas são diferentes. A chave utilizada para criptografar os dados é pública, e para descriptografar é privada.

3.1.1 Algoritmos para Criptografia:

DES - Data Encryption Standard:

É um padrão de criptografia simétrica, adotada pelo governo dos EUA em 1977.

Triple-DES:

O Triple-DES é uma variação do algoritmo DES, sendo que o processo tem três fases: A seqüência é criptografada, sendo em seguida decriptografada com uma chave errada, e é novamente criptografada.

RSA - Rivest Shamir Adleman:

É um padrão criado por Ron Rivest, Adi Shamir e Leonard Adleman em 1977 e utiliza chave pública de criptografia, tirando vantagem do fato de ser extremamente difícil fatorar o produto de números primos muito grandes.

Diffie-Hellman:

Foi desenvolvido por Diffie e Hellman em 1976. Este algoritmo permite a troca de chaves secretas entre dois usuários. A chave utilizada é formada pelo processamento de duas outras chaves uma pública e outra secreta.

3.2 Integridade:

A garantia de integridade dos dados trocados em uma VPN pode ser fornecida pelo uso de algoritmos que geram, a partir dos dados originais, códigos binários que sejam praticamente impossíveis de serem conseguidos, caso estes dados sofram qualquer tipo de adulteração. Ao chegarem no destinatário, este executa o mesmo algoritmo e compara o resultado obtido com a seqüência de bits que acompanha a mensagem, fazendo assim a verificação.

3.2.1 Algoritmos para Integridade:

SHA-1 - Secure Hash Algorithm One:

É um algoritmo de hash que gera mensagens de 160 bits, a partir de uma seqüência de até 2^{64} bits.

MD5 - Message Digest Algorithm 5:

É um algoritmo de hash que gera mensagens de 128 bits, a partir de uma seqüência de qualquer tamanho.

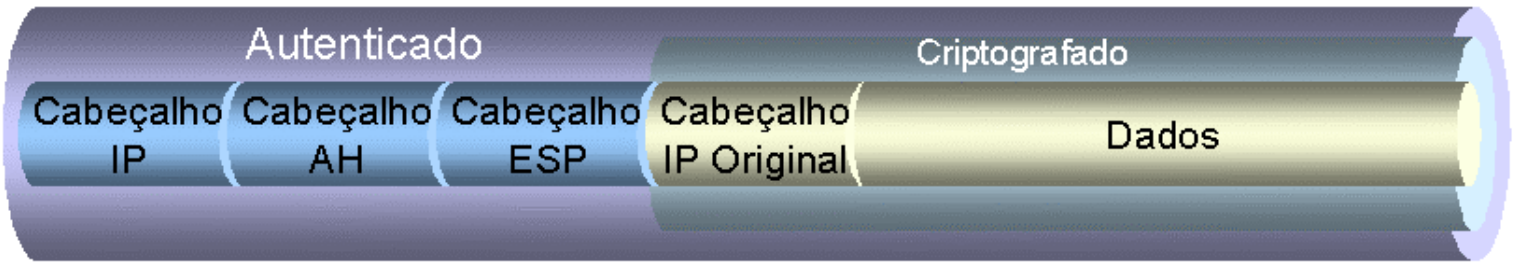
3.3 Autenticação:

A Autenticação é importante para garantir que o originador dos dados que trafeguem na VPN seja, realmente, quem diz ser. Um usuário deve ser identificado no seu ponto de acesso à VPN, de forma que, somente o tráfego de usuários autenticados transite pela rede. Tal ponto de acesso fica responsável por rejeitar as conexões que não sejam adequadamente identificadas. Para realizar o processo de autenticação, podem ser utilizados sistemas de identificação/senha, senhas geradas dinamicamente, autenticação por RADIUS (Remote Authentication Dial-In User Service) ou um código duplo. A definição exata do grau de liberdade que cada usuário tem dentro do sistema, tendo como conseqüência o controle dos acessos permitidos, é mais uma necessidade que justifica a importância da autenticação, pois é a partir da garantia da identificação precisa do usuário que poderá ser selecionado o perfil de acesso permitido para ele.

4. Protocolos:

IPSec:

IPSec é um conjunto de padrões e protocolos para segurança relacionada com VPN sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security (IPSec) do IETF (Internet Engineering Task Force).



Estrutura do Pacote IPSec

Authentication Header (AH):

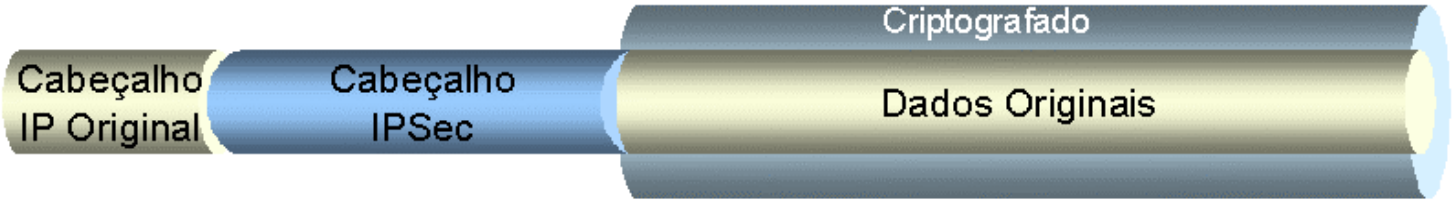
Utilizado para prover integridade e autenticidade dos dados presentes no pacote, incluindo a parte invariante do cabeçalho, no entanto, não provê confidencialidade.

Encapsulated Security Payload (ESP):

Provê integridade, autenticidade e criptografia à área de dados do pacote.

Estrutura do Pacote IPSec - Modo Túnel

A implementação do IPSec pode ser feita tanto em Modo Transporte como em Modo Túnel.



Estrutura do Pacote IPSec - Modo Transporte

PPTP - Point to Point Tunneling Protocol:

O PPTP é uma variação do protocolo PPP, que encapsula os pacotes em um túnel IP fim a fim.

L2TP - Level 2 Tunneling Protocol:

É um protocolo que faz o tunelamento de PPP utilizando vários protocolos de rede (ex: IP, ATM, etc) sendo utilizado para prover acesso discado a múltiplos protocolos.

SOCKS v5:

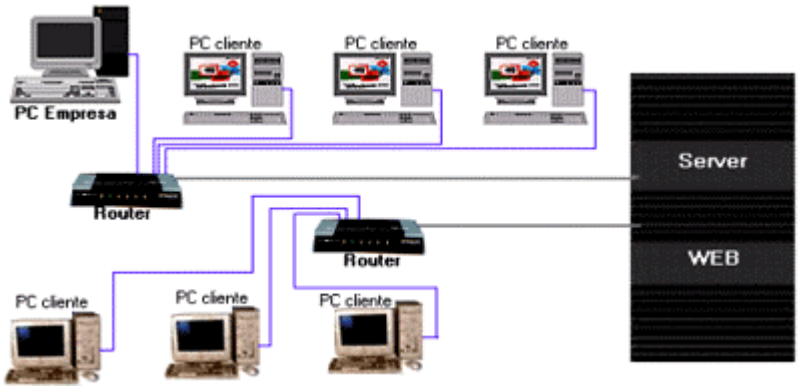
É um protocolo especificado pelo IETF e define como uma aplicação cliente - servidor usando IP e UDP estabelece comunicação através de um servidor proxy.

5. Tipos:

Nas redes de computadores do tipo VPN, utiliza-se de três tipos principais em que se podem realizar as conexões. Estes três tipos são conhecidos por Ponto-a-ponto VPN, Ponto-Multiponto VPN e Dial VPN (ou VPN de Acesso Remoto).

5.1 Modelo P-a-P VPN:

Implanta-se este modelo de redes VPN do tipo Ponto-a-Ponto (veja esta figura abaixo) quando se deseja fazer conexões com redes do tipo "corporativas". Ou seja, conexões entre



a empresa matriz numa determinada cidade --Brasília, por exemplo-- com uma filial desta empresa, instalada numa outra cidade distante -Rio de Janeiro, por exemplo. Utilizando-se para isto, toda a infraestrutura da rede mundial, no caso, que a Internet disponibiliza.

Para se implantar este tipo de rede VPN, será preciso instalar dispositivos de hardware e softwares VPN, tanto na empresa matriz bem como na sua filial ou filiais.

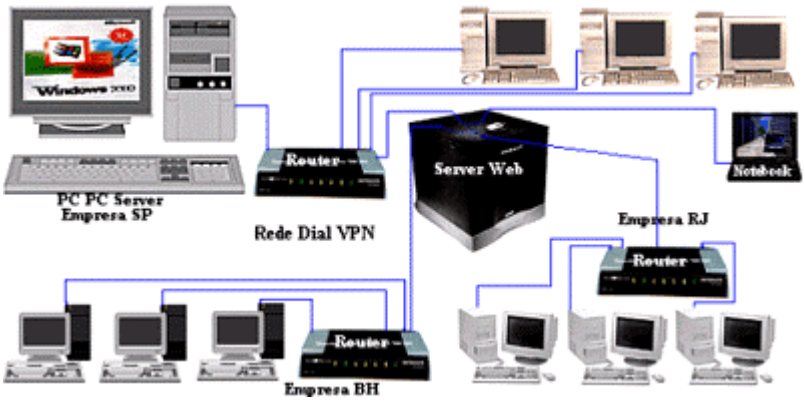
5.2 Modelo P-Mp VPN:

Implanta-se redes VPN do tipo Ponto-Multiponto (veja a figura abaixo) quando se deseja fazer interligações -trocas de informações altamente confidenciais, por exemplo-- entre a empresa matriz e suas filiais e, ainda, com seus distribuidores ou com seus clientes e fornecedores.

Também aqui, será preciso que cada ponto (PC site servidor e PCs site clientes) possua instalado o respectivo dispositivo (ou dispositivos) VPN. Para mais detalhes, dê uma observada na figura acima.

5.3 Rede Dial VPN:

Com a internet, podemos conectar uma empresa matriz ou a sua filial (ou filiais) desta empresa, de qualquer parte do planeta. Para isto, basta que ele instale em sua máquina um software VPN que possibilite a conexão direta (via Internet) com a rede corporativa da respectiva empresa. Utilizando meios de comunicações como a linha telefônica, por exemplo (meio mais lento), ou servindo-se dos serviços de ADSL (Assymmetric Digital Subscribe Line ou Linha de assinatura digital assimétrica) (meio mais rápido). Assim, implantando-se uma rede do tipo Dial VPN (veja a figura abaixo), um determinado usuário que esteja ligado diretamente a empresa matriz - um representante comercial, por exemplo, poderá se conectar a mesma de qualquer parte do planeta.



6. Soluções:

Existem 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 existem 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 tráfico 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 tráfico. A combinação de tunelamento e criptografia em firewalls será mais apropriada para redes pequenas com pouco volume de tráfico (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 autentificação 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 um a solução que apresenta um custo baixo, mas desaconselhada para redes que processam grande volume de tráfico. 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 tráfico 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.

6.1 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 ás 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	velocidade dial-up até 100Mbps
Produtos	Firewalls, Softwares de VPNS	Cartões de criptografia para roteadores, PCs (Personal Communication Services)	Hardware especializado

7. Vantagens e Benefícios:

7.1 Benefícios para as empresas:

De acordo com estudos realizados recentemente, as corporações que utilizam soluções VPN podem economizar até 60% em comparação com as redes privadas dedicadas.

As soluções VPN permitem que as empresas possam:

- Eliminar linhas alugadas de longas distâncias, pois como a infraestrutura utilizada é a Internet, não há necessidade de se manter WANs com linhas dedicadas;
- eliminar chamadas de longa distância para modens analógicos e equipamentos de acesso ISDN;
- pagar apenas pela banda utilizada, sem o inconveniente ou a preocupação de se desperdiçar largura de banda em linhas dedicadas de alta capacidade. Além disso, se a banda se tornar insuficiente, basta uma simples requisição de aumento ao provedor para melhorar a capacidade do acesso;
- utilizar um número menor de equipamentos, pois uma única solução VPN pode prover tanto acesso VPN como acesso a Internet, o que elimina o uso de bancos de modems separados, adaptadores de terminais, servidores de acesso remoto, etc.;
- diminuir a estrutura de rede na extremidade do usuário e as responsabilidades de gerenciamento.

Além dos benefícios econômicos, as VPNs também oferecem vantagens técnicas, por prover seus serviços com a robustez inerente à infraestrutura de Internet. Entre estas vantagens podemos citar:

- Facilidade de acesso devida a presença de ISPs em qualquer localidade, criando uma cobertura de rede a nível mundial;
- Aumento de throughput devido à diminuição de ruídos na linha com o acesso local;
- Garantia de confiabilidade extremo a extremo pela redundância na rede e a tolerância de falhas;
- Simplificação de treinamento devida a familiaridade com o usuário.

Para exemplificar melhor, vejamos agora uma comparação de custos entre redes corporativas tradicionais e VPNs corporativas. As redes tradicionais são baseadas em diversos links dedicados E1 (2Mbps) de SDH, acarretando altos custos mensais fixos, custos de instalação e utilização de diversos equipamentos. Além disso, para os usuários remotos, equipamentos provedores de acesso devem ser mantidos e diversas linhas telefônicas locais precisam ser alugadas.

Enquanto isso, VPNs utilizam um único link com menor banda (apresentando taxas de 512kbps ou 768kbps conforme se queira) e custo variável. Essas VPNs necessitam de somente um roteador no lado do cliente reunindo todos os serviços (Internet e WAN) em um só, proporcionando acesso remoto através de um provedor de Internet, com uma diminuição considerável nos custos de suporte e manutenção. A figura abaixo mostra um quadro comparativo.

7.2 Benefícios para os Provedores de Acesso (ISPs):

Muitos dos benefícios das VPN são aparentes para usuários e corporações. Entretanto, os provedores de acesso a Internet (ISPs) também esperam lucrar com seu uso. O potencial de renda com a migração das redes corporativas para VPNs é enorme, e o retorno de investimento é ainda melhor. Muitos ISPs experimentam picos de tráfego apenas durante um período limitado do dia. Como resultado, muitos dos recursos necessários para suprir esta demanda de pico permanecem inativos na maior parte do tempo. Porém, as VPNs permitem uma utilização de recursos dia e noite com usuários corporativos criando picos de utilização durante o dia e usuários remotos criando picos durante a tarde. Com este balanceamento de negócios e de assinantes, os ISPs podem dobrar o retorno de investimento com as VPNs.

a) Tráfego de Dados Corporativos Aproximado

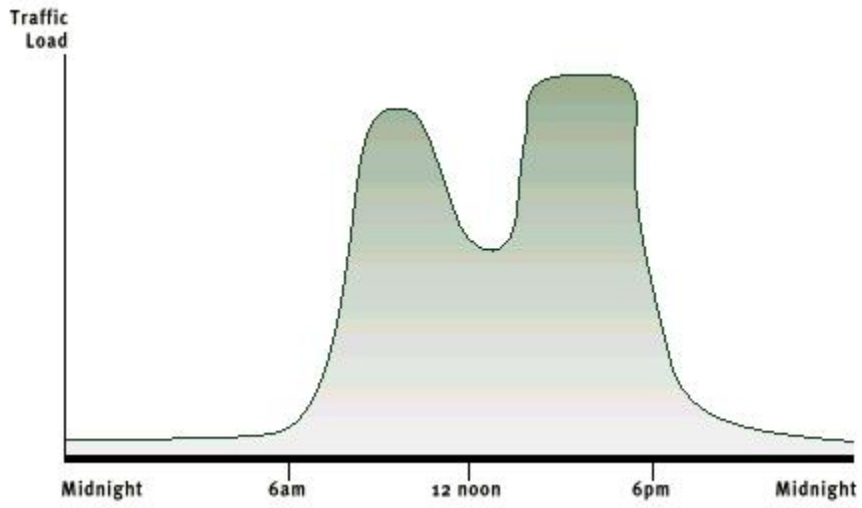
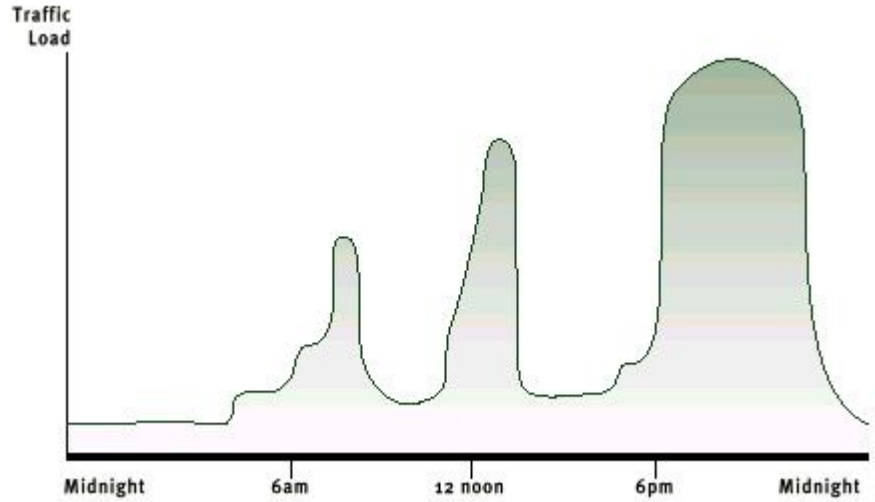
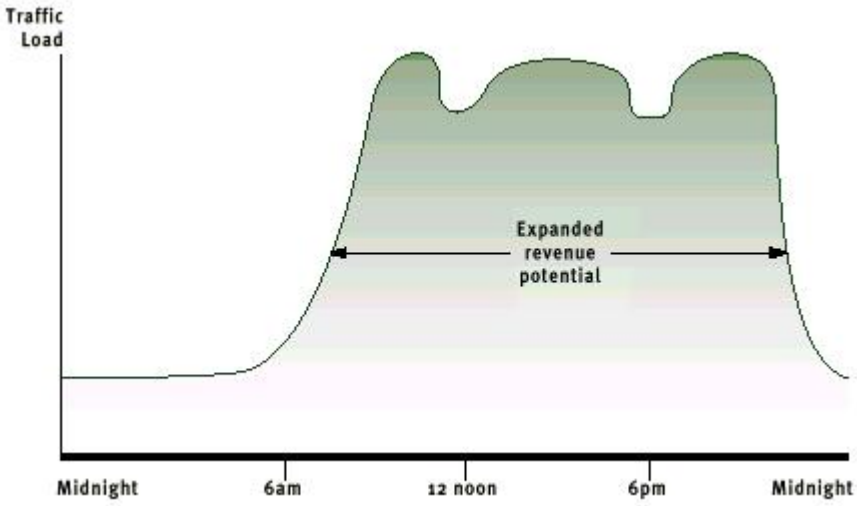


Figura: Estimativa de Potencial de Renda Expandido com as VPNs

b) Tráfego de Dados de Consumidores (Internet) Aproximado



c) Soma de Tráfegos de Negócios e de Consumidores



Além disso, podemos citar outros benefícios para os ISPs:

- Habilidade de atrair clientes corporativos;
- Oportunidade de estabelecer relações estratégicas a longo prazo com grandes corporações;
- Superioridade competitiva com relação a outros ISPs ou uma oportunidade de estabelecer acordos de serviços mutuamente lucrativos com outros ISPs;
- Possibilidade de impulsionar a infraestrutura existente com pouco investimento.

8. Conclusão:

Além dos benefícios econômicos e técnicos aplicados aos dias de hoje, as VPNs também têm a capacidade de estimular e impulsionar o desenvolvimento tecnológico.

Quando se fala em VPNs, imagina-se logo os enormes benefícios que elas oferecem às corporações, aos usuários e aos provedores de Internet, enfim, são apenas visualizados seus efeitos para a realidade presente. Porém, não podemos deixar de lado as oportunidades que a tecnologia VPN e sua demanda de QoS reservam para o futuro. As VPNs também têm sua parcela de contribuição no desenvolvimento de novas tecnologias de desempenho e segurança na Internet, proporcionando um esforço muito mais colaborativo e acelerado no tocante a estas questões.

9. Referências:

http://www.abusar.org/vpn/vpn3.htm

http://www.gpr.com.br/cursos/vpn/vpn.html

http://www.abusar.org/vpn/vpn2.htm

http://www.abusar.org/vpn/vpnport.htm