VPN: Uma solução prática e economicamente viável

Fernando Santos Lima; Jefferson Alves da Silva; Thiago dos Reis de Moura; Jocênio Marquios Epaminondas, Israel Rodrigues Gonçalves

Resumo

Com o crescente de aplicações informatizadas de âmbito trabalhistas, comerciais e financeiras, o uso de dados íntegros e seguros na rede se faz cada vez mais necessário. Para responder esses anseios a rede privada virtual surge como uma alternativa eficaz, de baixo custo e de implementação descomplicada para conectar uma estação de dados com aqueles que dependem de soluções rápidas para o gerenciamento de situações que façam uso da Internet.

Palavras-chave: Dados íntegros. Rede privada virtual. Segurança. Internet.

Abstract

With the growing labor-wide, commercial and financial computerized applications, the use of safe data on the network is increasingly necessary. In order to answer these concerns the Virtual Private Network is an effective alternative, low cost and easy implementation to connect a data station with those who depend on quick solutions for managing situations that make use of the Internet.

Keywords: Data integrity. Virtual Private Network. Security. Internet.

1 Introdução

É notória a expansão dos sistemas informatizados, compras e vendas sendo realizadas de maneira prática em tempo real, relações de trabalho dinâmicas e fundamentadas em homeworks, onde profissionais da área de Tecnologia da Informação gerenciam serviços, bancos de dados e relações cliente-servidor sem sair do conforto de suas casas e indivíduos que necessitam de acesso à informação rápida, segura e íntegra. Mas, como fazer várias de tarefas em tempo hábil, sem os custos de uma conexão dedicada e com segurança?

A resposta a essa pergunta está fundamentada no uso de uma rede prática e eficaz quando bem estruturada, a Virtual Private Network (VPN), que tem em sua composição uma gama de configurações que permitem a criação de uma “ponte direta” entre a origem dos dados e o seu devido destino.

Ao longo deste artigo, serão tratados os conceitos, as configurações, bem como a funcionalidade de alguns elementos de uma VPN, procurando elucidar temas como segurança, integridade de dados, bem como a confiabilidade em uma VPN, sendo eficaz e de baixo custo a sua implementação, assim como a sua manutenção.

2 Compreendendo o conceito de VPN

Com o crescimento da rede mundial de computadores, a comunicação passa a ter papel essencial para a dinamização das mais diversas relações humanas. Comércio, trabalho, ambientes acadêmicos entre outros necessitam cada vez mais de redes de dados mais rápidas e eficazes nas trocas de informações. Seguindo esse paradigma de resposta rápida às mais diversas situações cotidianas, o custo com a tecnologia de redes, a integridade da informação requisitada, bem como a segurança dessa informação passam a integrar um conjunto de metas a serem alcançadas para o desenvolvimento de redes seguras, não onerosas e que viabilize a informação de maneira rápida, proporcionando a execução de novas tarefas.

Segundo Tyson (2007), a VPN vem como uma resposta aos anseios dos usuários que buscam eficácia e preço acessível a uma rede dedicada para o fluxo de suas informações sem interferência de meios alheios a ele. Este "usuário" está nas mais amplas esferas dos indivíduos que fazem uso da rede mundial de computadores, seja ele um usuário doméstico, assim como um usuário empresarial. Em seu artigo, Tyson fala sobre a necessidade da expansão do uso de redes íntegras sem a implementação de uma rede de longa distância, ou seja, uma Wide Area Network (WAN), pois desenvolver uma rede exclusiva para o tráfego de dados de uma empresa para uma de suas sedes seria um gasto dispendioso de recursos bem como de serviços necessários para o surgimento de tal rede:

> Muitas empresas têm instalações espalhadas por todo o país ou mesmo pelo mundo e todas precisam de uma coisa: uma maneira de manter uma comunicação rápida, segura e confiável onde quer que seus escritórios estejam. Até recentemente, isso significou o uso de linhas dedicadas para manter uma rede de longa distância. (TYSON, 2007).

Na leitura de Tyson, depreende-se o conceito de que um VPN seria uma maneira de trafegar informações de maneira segura em uma rede não confiável, com baixo custo e sem dispêndio demasiado de serviços de implementação. O uso de infraestrutura pública ao invés de links dedicados e redes de pacotes (Frame Relay e X.25) atrai cada vez mais usuários para o uso de redes VPN.

De fato que, ao se falar em VPN, as noções de segurança, integridade e confidencialidade estão intimamente ligadas a composição dessa rede virtual, sendo imprescindível ao implementar uma rede a busca por diretrizes que contemplem essas três vertentes de funcionalidade de uma rede virtual VPN.

2.1 A VPN e suas características

A VPN pode ser desenvolvida em redes públicas ou privadas, ficando a cargo de analistas de requisitos, bem como analistas de redes, qual o tipo de implementação necessária para um determinado projeto (Figura 1).

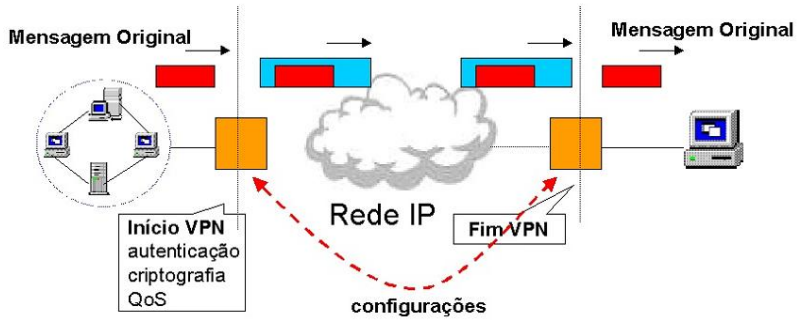

Figura 1:Modelo de Uma VPN.
Fonte: http://www.gta.ufrj.br-seminarios-semin2002_1-Ivana

Uma VPN é constituída para garantir a seus usuários segurança, integridade e confiabilidade no transporte de dados, sendo alternativa a links dedicados ou conexões exclusivas de redes. Dessa maneira, precisamos considerar alguns fatores para a sua constituição.

O primeiro fator a ser levado em consideração ao criar-se uma VPN é o tipo de tunelamento, onde são desenvolvidos túneis blindados para a passagem de dados, e somente os usuários que detenham "autenticação" para trafegar na rede VPN tenha acesso aos dados enviados e recebidos nesse "túnel".

Um exemplo prático do funcionamento de um túnel em uma VPN seria de uma rodovia. A internet seria como uma grande via onde trafegam os mais variados modelos de automóveis. Esses automóveis seriam os dados circulantes na rede, sem proteção alguma, podendo ser desviados em qualquer parte da rede, direcionados à residências, indústrias, bancos entre outros. Esses caminhos finais (possivelmente terminais) seriam caracterizados como os usuários, de fato, alguns desses automóveis poderiam ser desviados de seu percurso, em algum momento esses automóveis seriam "sequestrados" e enviados a outras vias, a outros pontos terminais, desviando o destino e até mesmo a finalidade que cada automóvel possui ao concluir seu "caminho". Porém, se nessa "rodovia" fosse criado um túnel, com um ponto de chegada e partida, com acessos limitados por "barreiras policiais" (tais barreiras seriam os protocolos de segurança implementados na rede), a eventualidade de desvio desses "automóveis" (dados) seria mínimo, pois trafegariam nesse túnel somente àqueles que foram concedidos acesso para esse trafego.

O didatismo do exemplo supracitado pode elucidar os tunelamentos utilizados em uma VPN. Por analogia, o exemplo trata somente de um tipo de implementação, onde o túnel de dados é criado no ponto de saída com rota direta ao ponto de chegada com criptografia de dados, ou seja, com implementação de segurança de chaves para que os dados trafegados sejam seguros, íntegros e confiáveis. Mas, em uma VPN pode existir túneis não criptografados, orientado a um cabeçalho da mensagem e os dados segundo um novo endereçamento de IP, levando o quesito privacidade a cair por terra.

Nesse sentido, considera-se como definição desses termos tão valiosos para a implementação de uma VPN:

- **Integridade:** Segundo Rossi e Franzin (2000), caso os dados sejam capturados na rede, é necessário garantir que estes não sejam alterados e reencaminhados, sendo que qualquer fraude ou alteração não tenham sucesso, sendo os dados validados recebidos pelas aplicações suportadas pela VPN.
- **Confidencialidade:** Ainda sobre a óptica de Rossi e Franzin (2000), será imperativo que os dados trafegados em uma rede sejam absolutamente privados de tal forma que estes dados quando interceptados não sejam compreendidos por aqueles alheios a VPN constituída para um determinado meio.
- **Autenticidade:** Para Miranda (2002), os dados trafegados em uma VPN seriam trocados somente entre equipamento e usuários habilitados a fazer parte de uma VPN em específico. Em síntese, um usuário de uma VPN somente reconhecerá os dados originados por um segundo usuário devidamente habilitado tenha autorização para ingressar e trocar dados nessa VPN.

No que diz respeito à privacidade, quatro tipos de técnicas podem ser implementadas para o funcionamento de uma VPN, onde há a garantia dos dados, bem como a garantia de todo o pacote:

- **Modo Transmissão:** De acordo com Rossi e Franzin (2000),

> somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes. (ROSSI E FRANZIN, 2000).

- **Modo Transporte:** Para esse modelo somente os dados é que passariam pelo processo de criptografia, surgindo mudanças no tamanho dos pacotes enviados e recebidos. Em uma análise mais detalhada o procedimento emprega segurança adequada para implementações em que os dados tenham seu trafego exclusivamente entre dois nós da rede (comunicação entre as máquinas).

- **Modo Túnel Criptografado:** Segundo a análise de Miranda (2002),

> 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. (MIRANDA, 2002).

- **Modo Túnel Não Criptografado:** Segundo a concepção de Chin (1998), o tunelamento não criptografado trabalha com o cabeçalho de pacotes e dados em um novo empacotamento e transmissão de acordo com um novo endereço de IP, o cabeçalho e os dados serão mantidos tais como foram geridos, porém tal processo leva a quebra da integridade, o que colocaria em cheque a segurança dos dados

transmitidos.

No tópico a seguir discorrerá sobre os tipos de criptografia, sua finalidade e os tipos de chaves utilizadas para garantir a segurança da VPN.

4. Criptografia em uma VPN

Em uma VPN há dois tipos de processos de criptografia:

- **Chave Simétrica ou Privada:** Mesma chave para criptografar e descriptografar os dados, sendo a sua manutenção fundamental para segurança da VPN implementada.
- **Chave Assimétrica ou Pública:** Essa Chave tem a utilidade de criptografar e descriptografar, porém a chave para criptografar é diferente daquela que descriptografa. Essa é chave é constituída por dois modelos de chaves, uma pública e outra privada sendo ambas usadas para criptografia e descriptografia.

Para a implementação de criptografia em uma VPN, utilizam-se os seguintes algoritmos:

- **DES –** Data Encryption Standard: Algoritmo criado em 1977 pelo governo dos Estados Unidos para implementar segurança em rede.
- **TRIPLE-DES:** O Triple-DES é uma variação do DES, com três fases distintas:
  - ✓ Criptografia.
  - ✓ Descriptografia com o uso de uma chave errada.
  - ✓ Nova Criptografia.
- **RSA** – Rivest Shamir Adleman: De acordo com Rossi e Franzin (2000),

> 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. (ROSSI E FRANZIN, 2000).

- **Diffie - Hellman** – Este algoritmo fora desenvolvido por Diffie e Hellman em 1976. Com este algoritmo é possível a troca de chaves secretas entre dois usuários. De maneira que chave utilizada é formada pelo processamento de duas outras chaves uma pública e outra privada.

5. O fator integridade: algoritmos de integridade

- **SHA -1** (Security Hash[1] Algorithm One): Gera 160 bits a partir de uma sequência de até 2^{64} bits, constituindo uma maneira segura para composição de chaves em uma VPN.
- **MD5** – (Message Digest Algorithm 5): Trata-se de um algoritmo de hash que gera

1 Hash: Um **hash** (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada. Disponível em < http://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm> Acesso em: 10 abr. 2013.

uma mensagem de 128 bits, a partir de uma sequência de qualquer tamanho.

No que diz respeito à autenticação dos dados, o serviço RADIUS (Remote Authentication Dial-In User Service) possui a função de gerar senhas dinamicamente, onde os usuários da VPN acessam os dados sem o risco de serem usurpados. Além do RADIUS, há também o serviço de código duplo, que oferece aos usuários a construção de senhas para a habilitação do envio e recebimento de dados na rede, sendo delegados a estes a função de manutenção da criptografia de senhas para sustentar a integridade e autenticidade da rede.

Figura 2: Exemplo de hash em site de compartilhamento de arquivos.
Fonte: http://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm

6. Protocolos utilizados em um VPN

Ao longo deste tópico serão citados os protocolos mais utilizados na implementação de uma VPN.

- **IPSec**: Segundo Rossi e Franzin,

> 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). O IPSec especifica os cabeçalhos AH (Authentication Header) e ESP (Encapsulated Security Payload), que podem ser utilizados independentemente ou em conjunto, de forma que um pacote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP) ou os dois cabeçalhos (ROSSI E FRANZIN, 2000).

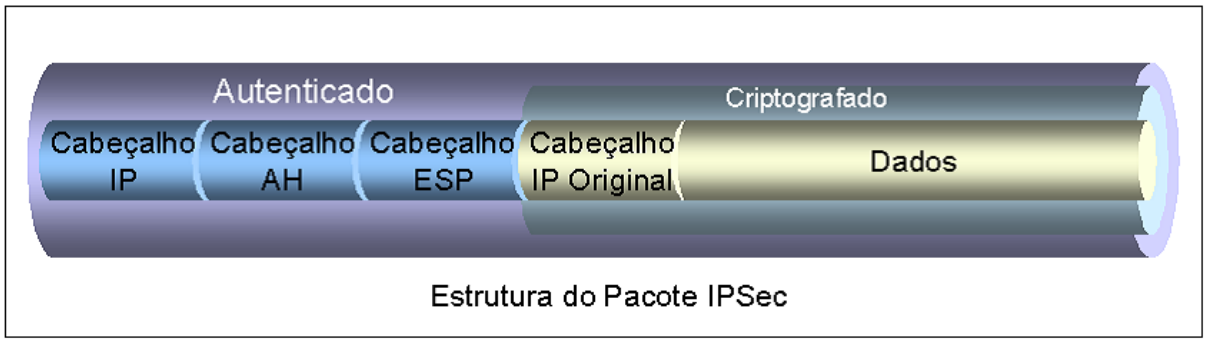

Figura 3: Exemplo de Estrutura do Pacote IPSec.
Fonte: http://www.gpr.com.br/download/vpn.pdf

Seguindo essa definição, há dois importantes elementos na composição do IPSec:

O *AH (Authentication Header)* tem como função garantir a integridade dos dados presentes no pacote incluindo a parte invariante (não alterável) do cabeçalho, no entanto, tal função não garante a confidencialidade dos dados.

Quanto ao *ESP (Encapsulated Security Payload)* Miranda (2002) o conceitua como uma função que garante integridade, autenticidade e criptografia a área dos dados do pacote, sendo uma opção adequada para a implementação de um protocolo que cumpre as três vertentes de uma VPN segura, ou seja, integridade, confidencialidade e autenticidade.

O IPSec pode ser implementado tanto no Modo Transporte, quanto no Modo Túnel, como representa o modelo a seguir

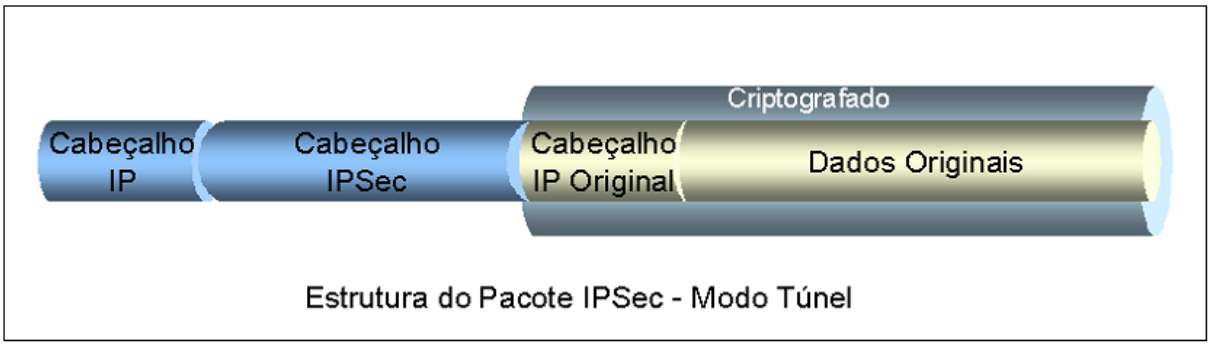

Figura 4: Exemplo de Estrutura do Pacote IPSec – Modo Túnel.
Fonte: http://www.gpr.com.br/download/vpn.pdf.

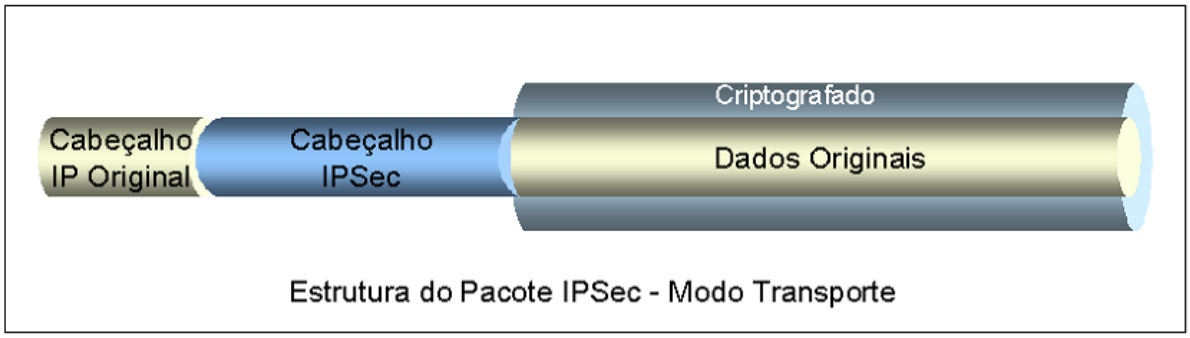

Figura 5: Exemplo de Estrutura do Pacote IPSec – Modo Transporte.
Fonte: http://www.gpr.com.br/download/vpn.pdf.

- **L2TP** (Level 2 Tunneling Protocol): De acordo com Rossi e Franzin (2000) Esse protocolo tem como função tunelamento de PPP (Point-to-Point, ou seja Ponto-a-Ponto) utilizando vários protocolos de rede (IP, ATM, etc.) sendo utilizado para prover acesso discado a múltiplos protocolos.

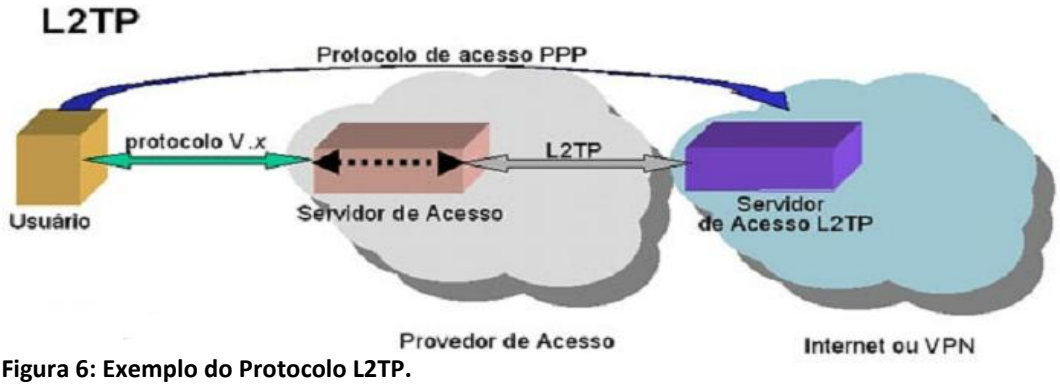

Figura 6: Exemplo do Protocolo L2TP.
Fonte: http://www.gta.ufrj.br-seminarios-semin2002_1-Ivana.

- **L2F** (Layer 2 Forwarding): Segundo Chin (1998), esse protocolo é de desenvolvimento da Cisco é utilizada para VPNs discadas.
- **PPTP** (Point to Point Tunneling Protocol): De acordo com Miranda (2002),

> o PPTP, um protocolo "voluntário", permite que os próprios sistemas dos usuários finais estabeleçam um túnel a uma localidade arbitrária sem a intermediação do provedor de acesso (MIRANDA, 2002).

Em linhas gerais, um protocolo “voluntário” permite ao usuário a definição de suas próprias configurações em uma VPN, sem depender de ônus adicionais com serviços prestado por operadoras de rede, tal serviço, onde uma empresa de telecomunicações determina o tipo de protocolo a ser usado em uma VPN é conhecido como “compulsório”.

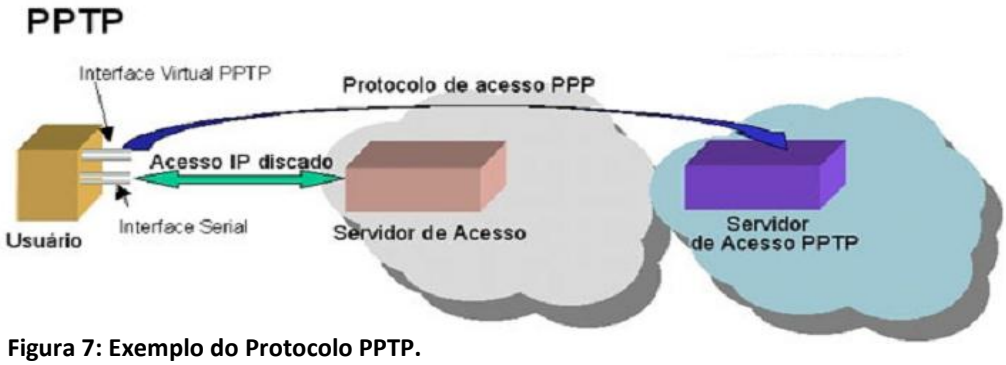

Figura 7: Exemplo do Protocolo PPTP.
Fonte: http://www.gta.ufrj.br-seminarios-semin2002_1-Ivana.

Há três tipos de VPNs:

- **Intranet VPN:** De acordo com as definições de Rossi e Franzin,

> Uma Intranet é utilizada para conectar sites que geralmente possuem uma infraestrutura completa de rede local, podendo, ou não, ter seus próprios servidores e aplicativos locais. Tais sites têm em comum a necessidade de compartilhar recursos que estejam distribuídos, como bases de dados e

aplicativos, ou mesmo de troca de informações, como no caso de e-mail. A Intranet pode ser entendida como um conjunto de redes locais de uma corporação, geograficamente distribuídas e interconectadas através de uma rede pública de comunicação. Esse tipo de conexão também pode ser chamado de LAN-to-LAN ou Site-to-Site (ROSSI E FRANZIN, 2000).

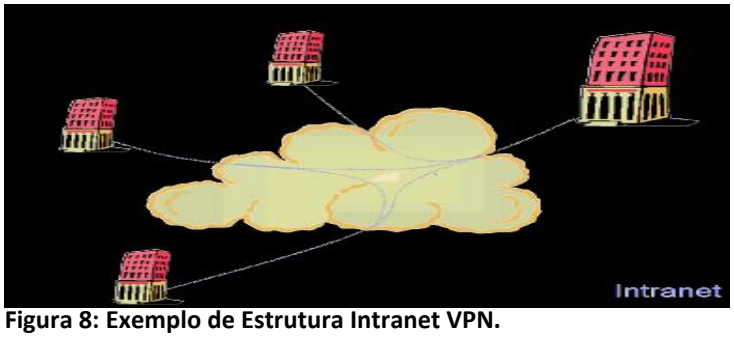

Figura 8: Exemplo de Estrutura Intranet VPN.
Fonte <http://www.gpr.com.br/download/vpn.pdf>. Acesso em: 10 abr. 2013.

- **Extranet VPN:** Segundo Miranda (2002) uma Extranet VPN será implementada para modelos informacionais que exijam dados em tempo hábil, correspondendo a cadeia de negócios existentes, como exemplo uma empresa que necessita ter os dados de seus sócios, fornecedores, clientes entre outros, dessa maneira é necessária uma solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Uma oura observação relevante é considerar o controle de tráfego, o que minimiza o efeito gargalo existente nos nós entre as redes e ainda garante uma resposta rápida para aplicações mais trabalhosas.

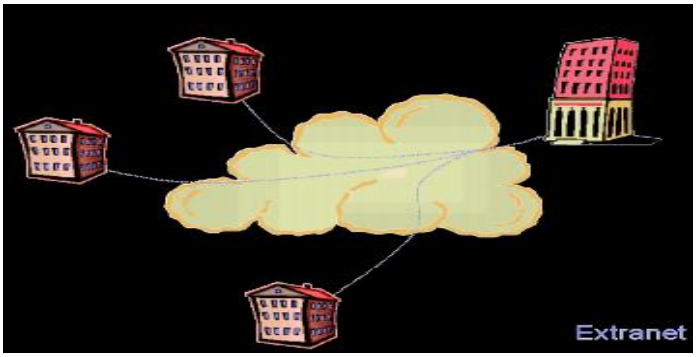

Figura 9: Exemplo de Estrutura Extranet VPN.
Fonte: http://www.gpr.com.br/download/vpn.pdf

- **Acesso Remoto VPN:** Uma VPN de acesso remoto conecta uma empresa à seus empregados que estejam distante fisicamente da rede. Neste caso torna-se necessário um software cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS (Quality of Service), isto porque, geralmente quando se acessa remotamente de um laptop, você está limitado à velocidade do modem. Outro item não menos importante é uma

autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E por último, um fator importante, é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação por exemplo, estejam centralizadas num único lugar. (MIRANDA, 2002).

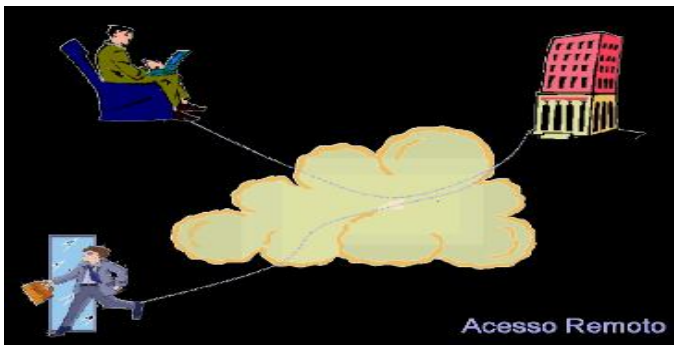

Figura 10: Exemplo de Estrutura Acesso Remoto VPN.
Fonte: http://www.gpr.com.br/download/vpn.pdf

7 Conclusões

O artigo apresentou a implementação de redes corporativas, de maneira que as VPNs são redes baseadas em túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas ou privadas para transferências de informações, de modo seguro, entre redes corporativas ou usuários remotos.

Descreveu-se sobre as aplicações mais importantes para as VPNs, os requisitos básicos, tunelamento, protocolos de tunelamento, protocolos e requisitos de tunelamento, funcionamento e tipo de túneis e internet protocol security.

Destacam-se como vantagens na utilização dessa tecnologia a redução de custos com comunicações corporativas, o oferecimento de confidencialidade e integridade no transporte de informações através de redes públicas e, também, segurança que é considerada a primeira e mais importante função das VPNs.

Observou-se como desvantagem dessa ferramenta a possibilidade de ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos, principalmente em aplicações onde o tempo de transmissão é crítico.

Dessa maneira, sugere-se que a decisão de implementar ou não redes privadas virtuais deve basear no tipo e necessidade de cada negócio, o que requer uma análise criteriosa dos

requisitos, principalmente àqueles relacionados à segurança, custos, qualidade de serviços e facilidade de uso.

Referências

CHIN, Liou Kuo**.** REDE NACIONAL DE ENSINO E PESQUISA. Rede Privada Virtual – VPN. **Boletim bimestral sobre tecnologia de redes**. Rio de Janeiro, v. 2, n. 8, nov. 1998. Disponível em: < http://www.rnp.br/newsgen/9811/vpn.html>. Acesso em: 10 abr. 2013.

ROSSI. Marco Antônio G. FRANZIN, Oswaldo. GPR SISTEMAS/ASP SYSTEMS – **Virtual Private Network (Rede Privada Virtual)**. Agosto de 2000. Disponível em: < http://www.gpr.com.br/download/vpn.pdf>. Acesso em: 10 abr. 2013.

MIRANDA, Ivana Cardial de. Grupo de Teleinformática e Automação **Virtual Private Network - Rede Privada Virtual).** Rio de Janeiro, 2002. Disponível em: < www.gta.ufrj.br-seminarios-semin2002_1-Ivana >. Acesso em: 10 abr. 2013.

TYSON, Jeff**."How Stuff Works – Como funciona uma VPN"**. Publicado em 15 de fevereiro de 2001 (atualizado em 20 de abril de 2007) Disponível em: <http://informatica.hsw.uol.com.br/vpn.htm>. Acesso em 9 de abr. 2013.

TECMUNDO. **O que é hash?** Atribuindo valores numéricos a uma estrutura é possível conferi-la e compará-la mesmo que não tenhamos acesso ao seu conteúdo. Disponível em: <http://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm>. Acesso em: 10 abr. 2013.