VPN: Protocolos e Segurança

Fábio Borges[1], **Bruno Alves Fagundes**[2], **Gerson Nunes da Cunha**[2,3]

[1]Coordenação de Sistemas e Redes – Laboratório Nacional de Computação Científica
Av. Getulio Vargas, 333, Quitandinha CEP: 25651-075 Petrópolis - Rio de Janeiro.

[2]Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis - ISTCC-P
Av. Getulio Vargas, 333, Quitandinha CEP: 25651-075 Petrópolis - Rio de Janeiro.

[3]Universidade Católica de Petrópolis - UCP
Rua Barão do Amazonas, 124, Centro - CEP: 25685-070 Petrópolis - Rio de Janeiro.

{borges,brunoaf,gerson}@lncc.br

Abstract. *VPN is a virtual net that allow two nets connect they self by a security way to confidentially communicate through a public communication channel, this technology create tunnels to transmit the cipher data between the nets. For implementation there are some protocols available at the market. From the analyzed protocols only two had been detached, the others analyzed protocols were not considered security therefore they has serious imperfections in the information security.*

Resumo. *VPN é uma rede virtual que permite a duas redes se conectarem de forma segura utilizando um canal público de comunicação, essa tecnologia cria túneis que transmitem os dados criptografados entre as redes. Para sua implementação existem alguns protocolos disponíveis no mercado. Dos protocolos analisados apenas dois se destacaram, os outros protocolos analisados não foram considerados seguros pois possuem falhas graves na segurança das informações.*

Palavras-chave: Segurança, Protocolos, Redes, VPN, Criptografia.

1. Introdução

Inicialmente quando surgiram as redes de computadores não havia uma preocupação tão grande quanto à segurança como hoje. Naquela época, era difícil imaginar que nos dias de hoje praticamente tudo funcionaria com o auxilio de máquinas [Santini 2005].

Com os avanços tecnológicos, obtemos diversas formas de conectarmos nossas máquinas nas redes de computadores. Tais conexões, nos permitem uma grande redução de custos com infra-estrutura e equipamentos, além de possibilitar uma grande variedade de novos serviços.

Com o aumento e convergência das redes surgem diversos problemas de segurança [Paulsamy and Chatterjee 2003]. Uma forma segura de se garantir acesso remoto a uma rede é o uso de algum protocolo de *Virtual Private Network* (VPN).

É interessante observar como as técnicas para usar *voice over IP* (VoIP) [Mehta 2001, Hillenbrand et al. 2005] se propagaram rápido pelas instituições, enquanto

VPN, apesar de predito como futuro da comunicação de dados [Herscovitz 1999], apesar das vantagens financeiras [Venkateswaran 2001], ainda não é amplamente usado nas instituições. As restrições no uso decorrem dos problemas de segurança envolvendo VPN. Ao final deste artigo temos uma indicação dos melhores protocolos e as vantagens e desvantagens de cada.

Na seqüência fazemos uma breve revisão dos tipos e características de VPN para entrarmos nos protocolos, caso o leitor esteja interessado nas implementações pode consultar [Khanvilkar 2004].

Em VPN, a palavra *Private* corresponde à forma como os dados trafegam, ou seja, os dados são criptografados garantindo a privacidade das informações. O termo *Virtual* indica que as máquinas conectadas na rede não fazem, necessariamente, parte do mesmo meio físico.

Ao criar uma conexão VPN estamos criando um túnel entre as extremidades da conexão assim os dados trafegam seguros de uma ponta até a outra.

A VPN deve dispor de ferramentas para permitir o acesso de clientes remotos autorizados aos recursos da rede corporativa e viabilizar a interconexão de redes geograficamente distantes, de forma a possibilitar acesso de filiais à matriz. Em geral, uma VPN, deve estar sempre possibilitando o compartilhamento de recursos e informações, além de assegurar privacidade e integridade dos dados que trafegam pela Internet.

1.1. Elementos de uma conexão VPN

Os principais elementos de uma conexão VPN são:

- **Tunelamento -** O tunelamento se dá pela forma como os dados trafegam pela conexão VPN. A idéia do túnel surge quando ao enviar os dados uma das extremidades da conexão, primeiro se criptografa e depois se encapsula o pacote original dentro de um novo pacote.
- **Autenticação das Extremidades -** Ao utilizar a autenticação das extremidades em uma conexão VPN garantimos que somente usuários válidos estão participando da transmissão, através de protocolos de autenticação, que em sua maioria implementam algoritmos de *hash* como MD5. O que garante a integridade das mensagens.
- **Transporte Subjacente -** Devido ao protocolo TCP/IP ser a base da Internet, ele é amplamente utilizado para a comunicação entre redes. Entretanto, este protocolo é muito inseguro. Por isso uma VPN utiliza a infra-estrutura da rede já existente do TCP/IP, para transmitir os seus pacotes pela Internet adicionando alguns cabeçalhos, o que possibilita a instalação destes em qualquer parte da rede [Kolesnikov and Hatch 2002].

1.2. Topologias

Existem três topologias no uso de VPN:

- **Host-host**: Comunicação entre dois microcomputadores separados fisicamente, podendo estar ou não em uma mesma rede.
- **Host-gateway**: Conexão de um microcomputador a uma rede fisicamente distante.
- **Gateway-gateway**: Conexão entre duas redes, onde os *gateways* de VPN estarão sempre conectados.

2. Protocolos

Os protocolos de VPN são os responsáveis pela abertura e gerenciamento das sessões de túneis.

2.1. Point-to-Point Tunneling Protocol (PPTP)

Desenvolvido por um fórum de empresas denominado PPTP Fórum, tinha por objetivo facilitar o acesso de computadores remotos a uma rede privada através da Internet ou outra rede baseada em IP, sendo um dos primeiros protocolos de VPN que surgiram.

Está incorporado no Windows a partir do NT 4.0 e em clientes do Windows 95 através de um *patch*. Agrega as funcionalidades do *Point-to-Point Protocol* (PPP) [Simpson 1994] para que o acesso remoto faça um túnel até o destino. O PPTP encapsula pacotes PPP utilizando uma versão modificada do protocolo *Generic Routing Encapsulation* (GRE) [Farinacci et al. 2000]. Permitindo ao PPTP [Hamzeh et al. 1999] flexibilidade em lidar com outros tipos de protocolos como IPX, NetBEUI etc.

O protocolo se baseia nos mecanismos de autenticação do PPP, os protocolos CHAP [Simpson 1996], MS-CHAP [Zorn 2000] e o inseguro PAP [Lloyd and Simpson 1992].

Existem três elementos envolvidos em uma conexão PPTP (figura 1). O cliente, o servidor de acesso à rede e o servidor PPP.

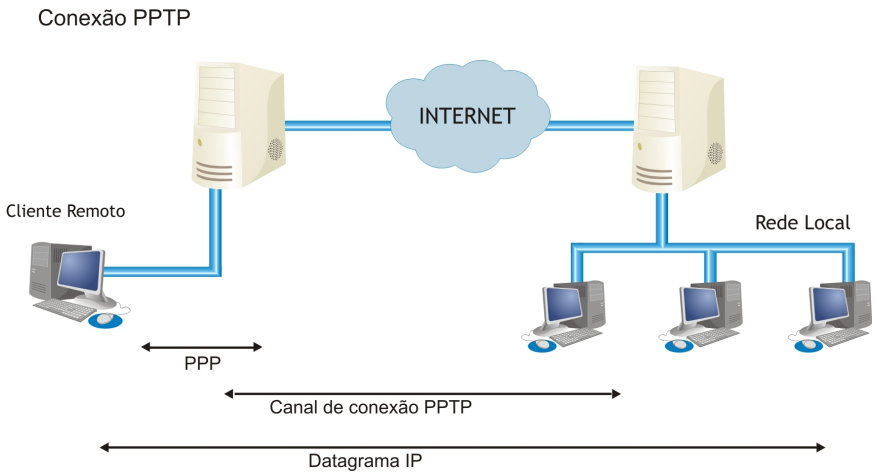

Figura 1 - Conexão PPTP

A comunicação criada pelo PPTP envolve três processos, onde cada um exige que os anteriores sejam satisfeitos.

O cliente PPTP utiliza o PPP para se conectar ao *Internet service provider* (ISP), por exemplo, utilizando uma linha telefônica. Nesta etapa o PPP é utilizado para estabelecer a conexão e criptografar os dados.

Utilizando a conexão estabelecida pelo PPP cria-se uma conexão de controle desde o cliente até o servidor PPTP através da Internet. É nesta etapa que todos os parâmetros de configuração da conexão são definidos entre as extremidades do túnel. Esta conexão utiliza pacotes TCP e é chamada de Túnel PPTP.

Os pacotes de dados são primeiro criptografados e encapsulados com um cabeçalho PPP. O quadro PPP resultante é então encapsulado com um cabeçalho GRE. Este quadro por fim é encapsulado com um cabeçalho IP que contém os endereços de origem e destino correspondentes às extremidades da conexão PPTP (figura 2).

Figura 2 - Tunelamento PPTP

Existem três desvantagens neste protocolo. O processo de negociação dos parâmetros de conexão é feito com criptografia muito fraca [Schneier and Mudge 1998]. As mensagens do canal de controle são transmitidas sem qualquer forma de autenticação ou proteção de integridade. Não existe autenticação no período de negociação dos parâmetros da conexão.

2.2. Layer Two Forwarding (L2F)

Desenvolvido pela empresa CISCO, surgiu nos primeiros estágios da tecnologia VPN.

O L2F [Valencia et al. 1998], diferente do PPTP, possui tunelamento independente do IP, sendo capaz de trabalhar diretamente com outros meios como ATM e *Frame Relay*. O L2F sempre assume que a rede privada do cliente estará atrás de um *gateway*, podendo ser um roteador ou um *firewall*.

O L2F utiliza o PPP para autenticação de usuários remotos mas também pode incluir suporte para autenticação via RADIUS, TACACS e TACACS+.

Existem dois níveis de autenticação de usuário: um no ISP antes de estabelecer o túnel e outro quando se estabelece a conexão com o *gateway*.

Primeiro o usuário estabelece uma conexão PPP com o servidor de acesso a rede (NAS) do ISP, então o NAS estabelece um túnel L2F com o *gateway*. Finalmente o *gateway* autentica o nome do usuário e a senha e estabelece a conexão PPP ou *Serial Line IP* (SLIP) (figura 3).

A autenticação é feita quando uma sessão VPN-L2F é estabelecida, o cliente, o NAS e o *gateway* da Internet usam um sistema triplo de autenticação via CHAP.

A grande desvantagem do L2F, é não definir criptografia e encapsulamento de dados.

2.3. Layer Two Tunneling Protocol (L2TP)

Em uma tentativa de se criar um padrão para protocolos de tunelamento o IETF reuniu neste protocolo as melhores características dos dois protocolos existentes o PPTP e o L2F.

Ele oferece a flexibilidade e a escalabilidade do IP com a privacidade do *Frame Relay* ou ATM, permitindo que os serviços de rede sejam enviados nas terminações dos túneis. O L2TP [Townsley et al. 1999] realiza o encapsulamento de pacotes PPP, podendo então fazer uso dos mecanismos de autenticação PPP. Também provê suporte para autenticação do Túnel, permitindo que as extremidades do túnel sejam autenticadas.

Este protocolo foi desenvolvido para suportar dois modos de tunelamento:

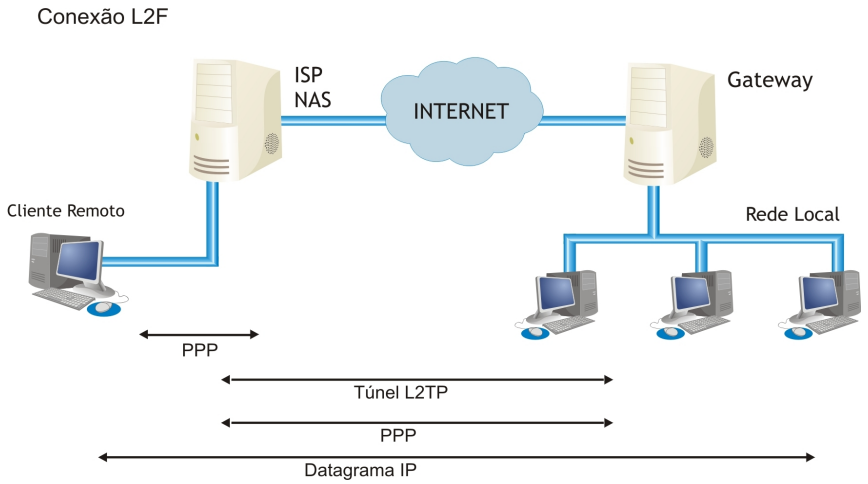

Figura 3 - Conexão L2F

- **Voluntário** - é iniciado pelo computador remoto, sendo mais flexível para usuários em trânsito que podem discar para qualquer provedor de acesso, como o provedor não participa da criação dos túneis, este pode percorrer vários servidores sem precisar de uma configuração explicita.
- **Compulsório** - é criado automaticamente e iniciado pelo servidor de acesso a rede sob a conexão discada. Isto necessita que o servidor de acesso à rede seja pré-configurado para saber a terminação de cada túnel baseado nas informações de autenticação de usuário.

O funcionamento se baseia em um concentrador de acessos L2TP localizado no ISP, troca mensagens PPP com o servidor de rede L2TP para criação dos túneis. O L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão. Os quadros enviados pelo usuário são aceitos pelo ISP, encapsulados em pacotes L2TP e encaminhados pelo túnel. No *gateway* de destino os quadros L2TP são desencapsulados e os pacotes originais são processados para interface apropriada (figura 4).

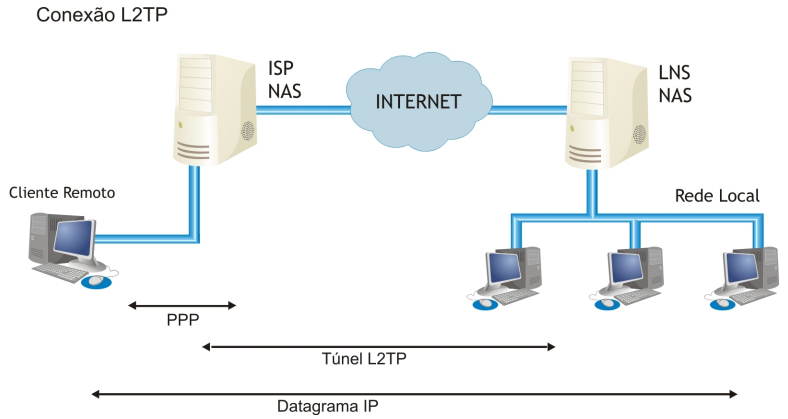

Figura 4 - Conexão L2TP

Devido ao uso do PPP para *links dial-up*, o L2TP inclui mecanismos de autenticação dentro do PPP, os protocolos PAP e CHAP. Outros sistemas de autenticação também podem ser utilizados como RADIUS e o TACACS. Porém, o L2TP não possui

processos para gerenciamento de chaves criptográficas. Além do mais, é suscetível a ataques de DoS [Kara et al. 2004]. Diante destes problemas, não é recomendado o uso em uma rede insegura como a Internet. Para poder usá-lo devemos combiná-lo com outros protocolos que corrijam estas vulnerabilidades como o IPSec [Patel et al. 2001].

2.4. IP Security (IPSec)

Em 1995 como uma resposta às carências de segurança existentes no protocolo IP o Grupo de Trabalho de Segurança IP do IEFT desenvolveu o IPSec, criando uma alternativa para a nova geração do IPv4, o IPv6.

Este conjunto de protocolos fornece principalmente serviços de integridade, autenticação, controle de acesso e confidencialidade permitindo interoperabilidade com protocolos de camadas superiores como: TCP, UDP, ICMP etc.

O IPSec pode trabalhar de dois modos diferentes.

- *Modo Transporte*
  É o modo nativo do IPSec. Nele, há transmissão direta dos dados protegidos entre os *hosts*. Toda autenticação e cifragem são realizadas no *payload*. Utilizado em clientes que implementam o IPSec (figura 5).

Figura 5 - IPSec modo transporte

- *Modo Túnel*
  É mais utilizado por *gateways* que manipulam trafego de *hosts* que não têm suporte ao IPSec. O pacote original é encapsulado em um novo pacote com a criptografia do IPSec incluindo o cabeçalho original, então é enviado para o outro *gateway* IPSec que desencapsula e o encaminha ao destinatário (figura 6).

Figura 6 - IPSec modo túnel

Security Association (SA) ou Associações de Segurança, são muito importantes dentro do IPSec, são elas que contém todas as informações que serão necessárias para "configurar" as conexões entre as entidades do IPSec. Elas são criadas durante o processo de negociação dos parâmetros da conexão, uma SA contém informações como algoritmo de criptografia, chaves secretas ou seqüências de números, funções *hash*, modo de funcionamento (túnel ou transporte), porta de comunicação e outros.

Existem dois bancos de dados utilizados pelo IPSec, o *Security Police Database* (SPD) e o *Security Association Database* (SAD). Os SPD possuem as políticas de

segurança, as quais os pacotes irão se submeter. Estas políticas são definidas pelo administrador do sistema e serão utilizadas pelas SA durante o processamento do pacote IP. Os SPD submetem os pacotes a uma lista de regras e o pacote que atendera pelo menos uma destas regras sofrerá a ação determinada pelo administrador. Esta ação pode ser: recusar o pacote, aceitar o pacote e aplicar o IPSec sobre ele ou deixá-lo entrar sem aplicar o IPSec.

O IPSec apresenta três características principais:

1) Authentication Header (AH): A utilização do protocolo AH previne ataques do tipo *replay, spoofing* e *hijacking*. Isso porque o protocolo faz uso de mecanismos de autenticação. A figura 7 descreve os campos do protocolo AH.

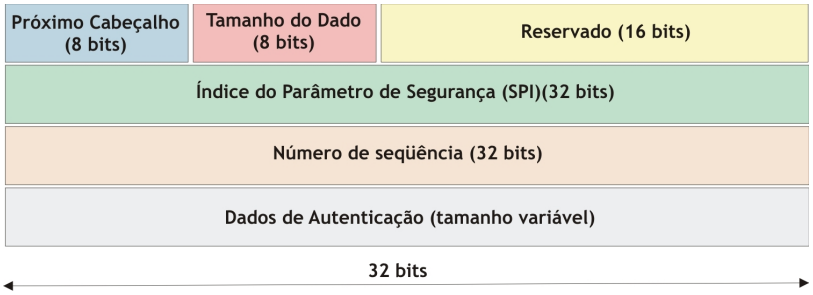

Figura 7 - Campos do cabeçalho AH

Para proteger um pacote o AH insere um cabeçalho dentro do pacote a ser protegido, utiliza um número seqüencial, que é zerado a cada estabelecimento de uma nova associação segura e adiciona funções de *hash* ao AH.

2) Encapsulation Security Payload (ESP): Além de fornecer as características do AH, este protocolo também oferece a confidencialidade como podemos observar na figura 8. Ele adiciona um cabeçalho ESP logo após o cabeçalho AH (caso este esteja sendo utilizado) e criptografa toda a parte correspondente aos dados *payload* com um algoritmo que foi negociado durante o estabelecimento da SA.

Figura 8 - Pacote ESP

3) Gerenciamento de chaves: O gerenciamento das SA no IPSec pode ser feito de maneira automática ou de maneira manual. O principal protocolo é o *Internet Key Exchange Protocol* (IKE), que combina o *Internet Security Association and Key Management Protocol* (ISAKMP), para definir o método de distribuição de chaves, com o OAKLEY [Orman 1998] para definir como as chaves serão determinadas. Existe uma alternativa para aumentar ainda mais a segurança, o *Perfect Forward Secrecy* (PFS) esta

opção faz com que a chave seja derivada do algoritmo de Diffie-Hellman [Stallings 2005] aumentando a segurança e reduzindo a performance.

2.5. Secure Socket Layer (SSL)

Originalmente, o protocolo SSL foi desenvolvido pela Netscape Communications para garantir a segurança entre aplicações cliente/servidor evitando influências externas, falsificação dos dados e "escutas". Ao ser padronizado recebeu o nome de *Transport Layer Security* (TSL) o TSL 1.0 é o mesmo que o SSL 3.0.

O SSL atua entre as camadas Transporte (TCP) e Aplicação, podendo rodar sobre outros protocolos como o http, Telnet, FTP, SMTP e outros de forma transparente.

O Protocolo SSL é dividido em duas partes:

1) SSL Handshake Protocol É o protocolo responsável pela autenticação do cliente e do servidor, além de fornecer os parâmetros para o funcionamento do SSL *Record Protocol*. Todas as mensagens de *handshake* são trocadas usando um *Message Authentication Code* (MAC) para dar mais segurança desde o inicio do processo. O protocolo de *handshake* é constituído de duas fases, numa é feita uma escolha de chave que será utilizada entre o cliente e o servidor, a autenticação do servidor e a troca da chave mestra, já a segunda é feita uma autenticação do cliente, sendo que esta fase pode não ser requerida.

2) SSL Record A comunicação deste protocolo se dá através do estabelecimento de uma sessão, caracterizado por um Estado de Sessão e um Estado de Conexão. Estes estados são criados após o protocolo de *handshake* concluir suas funções. O protocolo recebe os dados da camada superior e os fragmenta em tamanhos fixos para que possam ser melhor "manuseados" posteriormente, então dependendo dos parâmetros recebidos da fase de negociação do protocolo de *handshake* os dados são ou não compactados, em seguida aplica-se um MAC com uma das funções de *hash*. Agora os dados são encriptados com o algoritmo definido e finalmente transmitidos. A outra extremidade da conexão executa a operação inversa, junta os fragmentos e entrega a mensagem completa para os protocolos da camada superior. Como vantagens temos:

- Um dos protocolos mais convenientes e utilizados para implementação de transações seguras;
- Simples implantação;
- Trabalho independente das aplicações utilizadas e, após o *handshake* inicial, comporta-se como um canal seguro;
- Possui uma padronização do IETF.

Apresentamos na tabela 1 uma comparação entre o SSL e o IPSec.

3. Conclusão

Dentre os protocolos apresentados os que se demonstraram eficazes para elaboração de uma VPN foram: o IPSec e o SSL, os demais apresentaram falhas ou deficiências de segurança, portanto foram considerados inadequados. Tanto o IPSec quanto o SSL têm suas vantagens e desvantagens, a escolha deve se basear nas características da empresa, tipo de rede usada, necessidades. Em geral, recomenda-se o uso do SSL em redes com IPv4 e do IPSec em redes com IPv6 [Zhang et al. 2007]. Uma outra análise dos protocolos pode ser encontrada em [Berger 2006].

Tabela 1. SSL versus IPSec

Característica	**SSL**	**IPSec**
Autenticação	usando tokens ou certificados digitais	usando tokens e certificados digitais
Criptografia	forte, mas variável pois depende do *browser*	forte e constante, definido na implementação
Complexidade de implementar	moderada	alta
Complexidade de uso	simples	moderada
Escalabilidade	alta	muito alta
Segurança total	moderada, pois cada dispositivo pode ser usado para criar regras	alta, pois define cada dispositivo e implementações
Camada OSI de atuação	7: *Application*	3: *Network*
Suporte a UDP	não	sim
Monitora sessão	sim	não
Cifra	dados	pacote
Autentica	sistema e usuário	pacote
PFS	sim	sim
Esconde IP internos	não	sim

Somente a VPN não é suficiente, para permitir que usuários externos tenham acesso aos recursos da rede de forma segura, é extremamente recomendado possuir outras forma de proteção como *firewall* e uma política de segurança bem elaborada.

O grande problema de segurança em aplicações em VPN, numa topologia *host-gateway*, é a triangulação, onde o atacante invade inicialmente a máquina do cliente e então através da VPN tem acesso ao conteúdo da rede interna, este problema é muito difícil de se prevenir, pois não temos controle sobre os clientes que se conectam em nossa rede.

Referências

Berger, T. (2006). Analysis of current vpn technologies. *ares*, 0:108–115.

Farinacci, D., Li, T., Hanks, S., Meyer, D., and Traina, P. (2000). Generic routing encapsulation (gre). *RFC Editor - IETF*, RFC2784.

Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and Zorn, G. (1999). Point-to-point tunneling protocol. *RFC Editor - IETF*, RFC2637.

Herscovitz, E. (1999). Secure virtual private networks: the future of data communications. *Int. J. Netw. Manag.*, 9(4):213–220.

Hillenbrand, M., Gotze, J., and Muller, P. (2005). Voice over ip - considerations for a next generation architecture. *euromicro*, 00:386–395.

Kara, A., Suzuki, T., Takahashi, K., and Yoshikawa, M. (2004). A dos-vulnerability analysis of l2tp-vpn. *cit*, 00:397–402.

Khanvilkar, S.; Khokhar, A. (2004). Virtual private networks: an overview with performance evaluation. *Communications Magazine*, 42, Iss.10:146– 154.

Kolesnikov, O. and Hatch, B. (2002). *Building Linux virtual private networks (VPNs)*. New Riders Publishing, Indianapolis, IN, USA.

Lloyd, B. and Simpson, W. (1992). Ppp authentication protocols. *RFC Editor - IETF*, RFC1334.

Mehta, P.; Udani, S. (2001). Voice over ip. *Potentials*, 20 Iss.4:36–40.

Orman, H. (1998). The oakley key determination protocol. *RFC Editor - IETF*, RFC2412.

Patel, B., Aboba, B., Dixon, W., Zorn, G., and Booth, S. (2001). Securing l2tp using ipsec. *RFC Editor - IETF*, RFC3193.

Paulsamy, V. and Chatterjee, S. (2003). Network convergence and the nat/firewall problems. *hicss*, 05:152c.

Santini, S. (2005). We are sorry to inform you ... *Computer*, 38(12):128, 126–127.

Schneier, B. and Mudge (1998). Cryptanalysis of microsoft's point-to-point tunneling protocol (pptp). In *CCS '98: Proceedings of the 5th ACM conference on Computer and communications security*, pages 132–141, New York, NY, USA. ACM Press.

Simpson, W. (1994). The point-to-point protocol (ppp). *RFC Editor - IETF*, RFC1661.

Simpson, W. (1996). Ppp challenge handshake authentication protocol (chap). *RFC Editor - IETF*, RFC1994.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition*. Prentice Hall.

Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and Palter, B. (1999). Layer two tunneling protocol "l2tp". *RFC Editor - IETF*, RFC2661.

Valencia, A., Littlewood, M., and Kolar, T. (1998). Cisco layer two forwarding (protocol) "l2f". *RFC Editor - IETF*, RFC2341.

Venkateswaran, R. (2001). Virtual private networks. *Potentials*, 20, Iss.1:11–15.

Zhang, J., Yu, F., Sun, J., Yang, Y., and Liang, C. (2007). Dicom image secure communications with internet protocols ipv6 and ipv4. *Transactions on Information Technology in Biomedicine*, 11, Iss.1:70–80.

Zorn, G. (2000). Microsoft ppp chap extensions, version 2. *RFC Editor - IETF*, RFC2759.