

**ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM
REDES DE COMPUTADORES**

WELLINGTON LAGE LOPES

**IMPLEMENTAÇÃO DE UMA VPN UTILIZANDO O OPENVPN EM UM
SERVIDOR LINUX**

**VILA VELHA – ES
2010**

WELLINGTON LAGE LOPES

**IMPLEMENTAÇÃO DE UMA VPN UTILIZANDO O OPENVPN EM UM
SERVIDOR LINUX**

Monografia apresentada ao Curso de Redes de Computadores da Escola Superior Aberta do Brasil como requisito para o título de Especialista em Redes de Computadores, sob orientação do Prof. Marcos Alexandre do Amaral Ramos.

**VILA VELHA - ES
2010**

WELLINGTON LAGE LOPES

**IMPLEMENTAÇÃO DE UMA VPN UTILIZANDO O OPENVPN EM UM
SERVIDOR LINUX**

Monografia aprovada em de de 2010.

Banca Examinadora

**VILA VELHA-ES
2010**

AGRADECIMENTOS

Agradeço a Deus pela saúde e pela família, e aos amigos, que me ajudaram nesta caminhada.

RESUMO

Palavras-chave: VPN, redes de computadores, linux

Com a crescente expansão de empresas e universidades surge, cada vez mais, a necessidade de troca de informações e acesso a sistemas entre diferentes pólos destas instituições. Este trabalho pretende demonstrar o conceito de VPN (Virtual Private Network) e suas características principais como funcionalidade, segurança, custos e benefícios, valendo-se de algumas ferramentas de software livre em ambiente Linux. Para a implementação da VPN optou-se pelo OpenVPN, que tem como base o protocolo TLS/SSL e é bastante flexível. Serão apresentados alguns conceitos sobre redes de computadores e segurança que servirão como base para o entendimento do funcionamento de uma VPN. Serão abordadas as principais formas de criptografia no meio computacional e outras formas de segurança como firewalls, por exemplo, além das principais características de protocolos que podem ser utilizados na VPN. Ao final, é demonstrada a instalação da VPN através do OpenVPN em um servidor com o sistema operacional Debian Linux.

LISTA DE ILUSTRAÇÕES

Figura 1 - Exemplo de redes de computadores.....	12
Figura 2 - Exemplo de rede ponto-a-ponto	14
Figura 3 - Exemplo de rede cliente/servidor	16
Figura 4 - Topologia em estrela.....	20
Figura 5 - Topologia em anel.....	21
Figura 6 - Topologia em barramento	22
Figura 7 - Camadas da arquitetura TCP/IP e respectivos protocolos.....	24
Figura 8 - Datagrama do protocolo IP	26
Figura 9 - Transmissão de uma mensagem usando chave simétrica	33
Figura 10 - Transmissão de uma mensagem usando chave assimétrica.....	34
Figura 11 - Disposição do Firewall de uma VPN	36
Figura 12 - Criação do Túnel virtual	41
Figura 13 - Estrutura do pacote PPTP que contém um datagrama IP	49
Figura 14 - Configuração do cliente OpenVPN.....	63
Quadro 1 - Script de configuração do OpenVPN.....	60
Quadro 2 - Arquivo de configuração do servidor	61
Quadro 3 - Arquivo de configuração do cliente.....	62

SUMÁRIO

1	INTRODUÇÃO.....	9
1.1	PROBLEMA.....	10
1.2	OBJETIVO GERAL.....	10
1.3	OBJETIVOS ESPECÍFICOS.....	10
1.4	JUSTIFICATIVA	11
1.5	METODOLOGIA.....	11
2	REDES DE COMPUTADORES.....	12
2.1	TOPOLOGIAS DE REDES	13
2.1.1	Redes ponto-a-ponto	13
2.1.2	Redes cliente/servidor	15
2.2	CLASSIFICAÇÃO.....	16
2.2.1	Redes Locais.....	17
2.2.2	Redes geograficamente distribuídas.....	18
2.3	TOPOLOGIAS	19
2.3.1	Redes Locais.....	19
2.3.1.1	Topologia em estrela	19
2.3.1.2	Topologia em anel	20
2.3.1.3	Topologia em barramento	22
2.3.2	Redes geograficamente distribuídas.....	23
2.4	MODELO DE REFERÊNCIA TCP/IP	23
2.4.1	Camada Física.....	25
2.4.2	Camada Inter-redes	25
2.4.3	Camada de Transporte	26
2.4.4	Camada de Aplicação	27
3	VPN (VIRTUAL PRIVATE NETWORK)	29
3.1	CONCEITOS	29
3.1.1	Segurança.....	30
3.1.1.1	Autenticação e integridade	30
3.1.1.2	Confidencialidade.....	31
3.1.1.3	Criptografia	31
3.1.1.3.1	Chave simétrica	32

3.1.1.3.2	Chave assimétrica	33
3.1.1.4	Firewall.....	34
3.1.1.4.1	Firewall de nível de rede	35
3.1.1.4.2	Firewall de aplicativo	35
3.1.2	Topologias.....	36
3.1.2.1	Host-host	36
3.1.2.2	Host-rede	37
3.1.2.3	Rede-rede	37
3.1.3	Appliance.....	37
3.1.4	Endereçamento IP	38
3.1.5	IPV6	38
3.1.6	DHCP	39
3.1.7	DNS.....	40
3.1.8	Tunneling.....	40
3.1.9	NAT.....	42
3.2	VULNERABILIDADES.....	42
3.2.1	DoS	43
3.2.2	DDoS	44
3.2.3	Ataque DNS	44
3.2.4	Worms	45
3.2.5	Ataques a roteadores.....	45
3.3	PROTOCOLOS	46
3.3.1	GRE	46
3.3.2	PPP	46
3.3.2.1	PAP	47
3.3.2.2	CHAP	48
3.3.3	PPTP.....	48
3.3.4	L2F.....	50
3.3.5	L2TP	50
3.3.6	MPLS	52
3.3.7	SSH.....	53
3.3.8	IPSec	54
3.3.8.1	Authentication header	54
3.3.8.2	Encapsulating security payload.....	55

3.3.8.3 Algoritmos criptográficos	56
4 INSTAÇÃO DA VPN NO SERVIDOR LINUX	57
4.1 INTRODUÇÃO.....	57
4.2 INSTALAÇÃO DA VPN	58
4.3 CONFIGURAÇÕES DE SEGURANÇA	59
4.4 CONFIGURAÇÕES DE ACESSO	61
4.5 CONFIGURAÇÃO DO CLIENTE	63
CONCLUSÃO	64
REFERÊNCIAS	65

1 INTRODUÇÃO

Com o crescimento de uma organização, que geralmente passa a contar com uma ou mais filiais, cresce também sua rede de computadores, aumentando o número de usuários e surgem necessidades especiais de se interligar essas filiais à matriz e vice-versa, para gerenciamento e troca de informações. Essa troca de informações úteis e sigilosas deve ocorrer de maneira segura, impedindo a perda da informação e garantindo sua autenticidade e integridade. Para isso foram criados diversos métodos com o objetivo de interligar essas organizações de forma segura.

A *Virtual Private Network* (VPN) ou Rede Privada Virtual é um destes métodos de se unir diferentes redes de uma organização. Ela é privada porque só quem possuir autorização poderá acessá-la e Virtual porque ela constrói um canal virtual que ligará uma rede a outra, tornando possível uma comunicação segura entre elas. Para isso elas se utilizam de infra-estruturas privadas ou públicas como a Internet. Ou seja, pode-se utilizar links dedicados ou redes de pacotes (como *Frame Relay* ou X.25) para conectar redes remotas, assim como a infra-estrutura da Internet, que será abordada e utilizada neste trabalho.

Com o crescimento da Internet, o constante aumento de sua área de abrangência, a expectativa de uma rápida melhoria na qualidade dos meios de comunicação e o grande aumento nas velocidades de acesso, a VPN passou a ser vista como um meio prático e conveniente para as comunicações corporativas. Como a Internet não oferece segurança na passagem de dados privados, somente torna-se viável utilizá-la com o uso de alguma tecnologia que torne esse meio inseguro em um meio confiável. Uma das características da VPN é exatamente isso, criar “túneis virtuais” na Internet para garantir a comunicação entre essas redes de forma que os dados trafeguem criptografados por esses túneis, aumentando a segurança na transmissão e recepção de dados.

Além da segurança de dados, uma VPN possui a capacidade de aumentar a quantidade de usuários que podem ter acesso a esta rede, investindo-se pouco em

infra-estrutura e permitindo aos usuários acesso de qualquer local que possua acesso a Internet.

1.1 PROBLEMA

Com a crescente expansão de empresas e universidades surge, cada vez mais, a necessidade de troca de informações e acesso a sistemas entre diferentes pólos das instituições. Mas é possível criar um ambiente seguro, utilizando software livre, para troca de informações através da internet e acesso a sistemas que necessitam de autenticação? Este trabalho de conclusão de curso busca esclarecer essa questão.

1.2 OBJETIVO GERAL

O objetivo principal deste trabalho é investigar como criar um ambiente seguro para troca de informações e acesso a sistemas entre pólos distantes de uma instituição, utilizando uma VPN com o aplicativo OpenVPN e softwares livres.

1.3 OBJETIVOS ESPECÍFICOS

- Estudar os conceitos básicos de uma VPN como criptografia, autenticidade e integridade;
- Compreender os processos de configuração de servidores Linux para implantação da VPN utilizando software livre;

- Descrever as principais características dos protocolos de tunelamento que podem ser utilizados, como PPTP, L2TP, IPSec e OpenVPN (SSL).

1.4 JUSTIFICATIVA

A necessidade de acesso a informações através de redes de computadores se tornou essencial para o sucesso das organizações. Para garantir que essas informações sejam transmitidas com segurança são necessárias medidas eficazes. Quando se torna necessário acessar informações através de redes externas, como a internet, a utilização de uma Rede Privada Virtual, ou VPN, pode garantir o acesso de forma segura.

Utilizar uma VPN permite o compartilhamento de arquivos e a utilização de aplicativos de produtividade e gerenciamento, fornecendo o acesso a rede interna da organização de qualquer local em que haja uma conexão com a internet.

Este trabalho busca demonstrar conceitos sobre os fundamentos e a implementação do serviço VPN utilizando softwares livres.

1.5 METODOLOGIA

Este trabalho será desenvolvido com uma pesquisa bibliográfica, em livros, artigos e trabalhos científicos, abrangendo os conceitos de VPN e da segurança necessária para implementá-la. O trabalho baseia-se também em uma pesquisa exploratória criando uma rede virtual privada entre dois pontos fisicamente distantes com o objetivo de aprimorar os conhecimentos teóricos.

2 REDES DE COMPUTADORES

Uma rede de computadores é um sistema de comunicação que permite conexões em vários pontos distintos, ou seja, permite a troca de informações entre diversos usuários. Os componentes básicos de uma rede computadores são um emissor (origem da informação), o meio através do qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si (SILVA, 2002).

Uma rede de computadores (Figura 1) é formada por um conjunto de módulos processadores (MPs) capazes de trocar informações e compartilhar recursos interligados por um sistema de comunicação (SOARES, 1995).



Figura 1 - Exemplo de redes de computadores
Fonte: SENA (2002)

Segundo Silva (2002), uma rede de computadores baseia-se nos princípios de rede de informações, implementando técnicas de hardware e software de modo a torná-la efetivamente mais dinâmica, para atender às necessidades que o mundo moderno impõe. Redes de computadores incluem todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras. Esses dispositivos que se comunicam entre si são chamados de nós, hospedeiros, estações de trabalho, pontos ou simplesmente dispositivos de rede.

Dois computadores, ou nós, seria o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, teoricamente todos os computadores do mundo poderiam estar interligados unindo várias redes na formação de uma grande rede. Um exemplo típico deste modelo é a Internet.

Módulos processadores são dispositivos capazes de se comunicar através de sistemas de comunicação – como uma rede de computadores - por troca de mensagens. Microcomputadores, impressoras e servidores são exemplos destes dispositivos.

Estes sistemas de comunicação são constituídos por vários módulos processadores interligados através de enlaces físicos, como cabos de rede UTP. A comunicação entre estes dispositivos é organizada por um conjunto de regras, definidas pelos protocolos de comunicação (SOARES, 1995).

2.1 TOPOLOGIAS DE REDES

2.1.1 Redes ponto-a-ponto

As redes ponto-a-ponto possuem algumas características importantes que devem ser lembradas. Elas são utilizadas em locais geograficamente menores, são fáceis de serem implementadas, possuem baixo custo, o sistema de cabeamento é simples, não necessitam de um administrador e não existem computadores servidores. Porém possuem pouca segurança, exigem que os computadores sejam independentes e instalados em um mesmo ambiente de trabalho e são de difícil expansão. A Figura 2 mostra um exemplo de rede ponto-a-ponto.

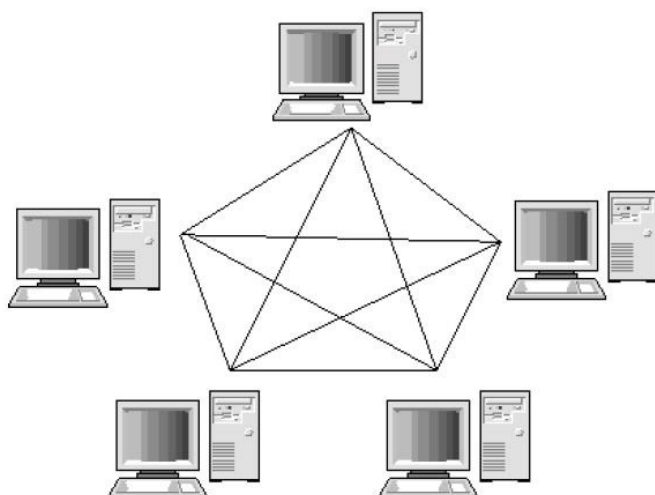


Figura 2 - Exemplo de rede ponto-a-ponto
Fonte: MIRANDA (2008)

Na rede ponto-a-ponto, os computadores compartilham dados e periféricos sem muita “burocracia”. Qualquer computador pode facilmente ler e escrever arquivos armazenados em outros computadores da rede bem como utilizar periféricos que estejam instalados em outros PC's. Obviamente tudo isso depende da configuração, que é feita em cada computador individualmente. Ou seja, não há papel de um computador “servidor” como nas redes cliente/servidor (TORRES, 2001).

Os computadores presentes em uma rede ponto-a-ponto são computadores “completos”, isto é, funcionam normalmente quando não estão ligados em rede, tanto no que diz respeito ao hardware quanto ao software.

A grande vantagem das redes ponto-a-ponto é a facilidade de instalação e de configuração, onde os próprios usuários podem configurar manualmente quais serviços estarão disponíveis em seu computador. Essa vantagem, entretanto, traz alguns inconvenientes como, por exemplo, a vulnerabilidade em relação à segurança da rede (TORRES, 2001).

As redes ponto-a-ponto são ideais para escritórios onde existem poucas estações, podendo haver o controle dos arquivos, pois nesse tipo de rede todas as estações podem ler e gravar informações em qualquer outra estação, perdendo a integridade das informações. O correto é haver regras entre os usuários da rede, definindo apenas uma estação para armazenamento das informações.

O custo de implementação deste tipo de rede é baixo, pois não são necessários servidores e outros recursos de infra-estrutura, que são caros para pequenas organizações. Não há grandes gastos com a administração da rede, pois somente as próprias estações dos usuários são configuradas. Também não se gasta muito com cabeamento, este tipo de rede são destinadas a estruturas de pequeno porte, não sendo necessários recursos como fibras ópticas ou pontos para acesso sem fio.

2.1.2 Redes cliente/servidor

Nesse tipo de rede existe a figura do servidor, geralmente um computador dedicado a fornecer recursos aos usuários da rede. O servidor é um computador especializado que executa apenas tarefas específicas como armazenar e compartilhar dados, por exemplo. A utilização de Servidores traz vários benefícios como segurança, disponibilidade e integridade das informações, além da otimização de recursos (TANENBAUM, 2003).

A configuração de uma rede cliente servidor e toda administração é feita de forma centralizada, ou seja, as configurações estão no servidor. Desta forma é possível executar processos diretamente no servidor, processos estes resultantes de aplicativos executados nas estações, aumentando a organização e segurança da rede.

O custo de implementação desse tipo de rede depende das necessidades da organização, pois essa rede poderá possuir vários servidores, cada um com uma função específica. É necessário um administrador de redes para configuração e manutenção dessa rede. Geralmente também são necessários investimentos maiores em infra-estrutura como um *Data Center* para alocar estes servidores e cabeamento mais específico como fibras ópticas para interligação dos servidores e outros dispositivos da rede (TANENBAUM, 2003).

O desempenho dessa estrutura em relação a ponto-a-ponto, considerando um servidor que atenda às necessidades, é maior pois, as estações não ficam responsáveis pelo processamento referente à rede, ou seja, o armazenamento de arquivos ou o compartilhamento da Internet, são de responsabilidade dos servidores específicos.

Os servidores desse tipo de rede podem ser computadores simples ou equipamentos sofisticados. A definição de qual utilizar depende das necessidades da organização, dos recursos disponíveis e da necessidade de futura expansão dos serviços disponibilizados.

Nesse tipo de arquitetura é possível implementar bancos de dados oferecendo serviços de armazenamento e disponibilidade de informações para as demais estações, como mostra a Figura 3:

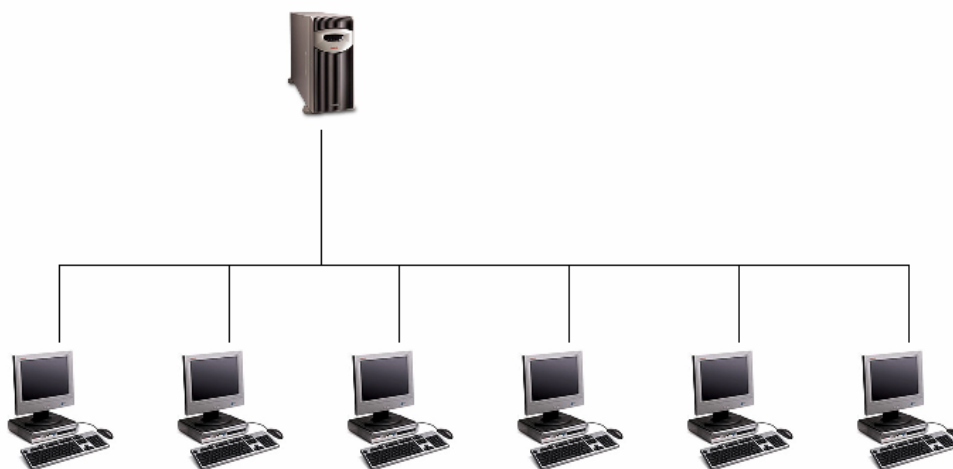


Figura 3 - Exemplo de rede cliente/servidor

Fonte: http://sweet.ua.pt/~pf/Linux/Foco/servidor/rede_cli_srv.png

2.2 CLASSIFICAÇÃO

As redes podem ser classificadas quanto ao seu tamanho em três tipos: LAN, MAN e WAN, porém neste trabalho estudaremos apenas as LAN's e WAN's.

2.2.1 Redes Locais

As Redes Locais (*Local Area Network* – LAN) surgiram dos ambientes de institutos de pesquisa e universidades. As mudanças no enfoque dos sistemas de computação que ocorriam durante a década de 1970 levaram em direção à distribuição do poder computacional. O desenvolvimento de microcomputadores de bom desempenho permitiu a instalação de considerável poder computacional em várias unidades de uma organização ao invés da anterior concentração em uma determinada área. Redes locais surgiram, assim, para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo (SOARES, 1995).

Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados em uma pequena região. De fato, tal definição é bastante vaga principalmente no que diz respeito às distâncias envolvidas. Consideraremos essa “pequena região” uma distância compreendida entre 100 m e 25 km, embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias. Outras características típicas encontradas e comumente associadas às redes locais são as altas taxas de transmissão (de 0,1 a 1000Mbps) e as baixas taxas de erro. É importante notar que os termos “pequena região”, “altas taxas de transmissão” e “baixas taxas de erro” estão sujeitos à evolução tecnológica; os valores associados a estes termos estão ligados à tecnologia atual e certamente não serão mais os mesmos dentro de alguns anos. Outra característica dessas redes é que elas são, em geral, de propriedade privada (SOARES, 1995).

2.2.2 Redes geograficamente distribuídas

As Redes Geograficamente Distribuídas (*Wide Area Network* – WAN) surgiram da necessidade de se compartilhar recursos por uma maior comunidade de usuários geograficamente dispersos. Elas proporcionam a transmissão de dados, voz, imagens e vídeos a grandes distâncias geográficas, podendo compreender um país, um continente ou até mesmo todo o mundo (FOROUZAN, 2008).

As WAN's podem utilizar as redes públicas de comunicação (como a Internet), redes sob concessão ou alugadas, equipamentos privados de comunicação ou a combinação destas para atingir grandes distâncias de comunicação. Para aumentar a confiabilidade destas redes geralmente são oferecidas rotas alternativas de comunicação (FOROUZAN, 2008).

Segundo Tanenbaum (2003), na maioria das WAN's a rede contém numerosas linhas de transmissão, todas conectadas a um par de roteadores - que são os equipamentos responsáveis pelo encaminhamento dos pacotes entre redes. No entanto, se dois roteadores que não compartilham uma linha de transmissão desejarem se comunicar, eles só poderão fazê-lo indiretamente, através de outros roteadores. Quando é enviado de um roteador para outro por meio de um ou mais roteadores intermediários, o pacote é recebido integralmente em cada roteador intermediário, onde é armazenado até a linha de saída solicitada ser liberada, para então ser encaminhado. Uma sub-rede organizada de acordo com este princípio é chamada de *store-and-forward* (armazena e encaminha) ou de comutação por pacotes. Quase todas as redes geograficamente distribuídas (com exceção das que utilizam satélites) têm sub-redes *store-and-forward*. Quando são pequenos e possuem o mesmo tamanho, os pacotes são chamados de células.

2.3 TOPOLOGIAS

Uma topologia de rede se refere ao modo segundo o qual uma rede é conectada fisicamente. Ela garante a redução de custos e o aumento da eficiência da rede, pois permite um melhor aproveitamento dos recursos. A escolha da topologia a ser utilizada varia de acordo com a necessidade, os objetivos e os investimentos envolvidos, podendo ser utilizadas duas ou mais topologias em conjunto para se obter uma solução ideal e um menor custo (MENDES, 2007). A seguir, serão demonstradas as principais topologias de rede disponíveis:

2.3.1 Redes Locais

As redes locais possuem características que levam a diferenciá-las das redes geograficamente distribuídas, pois o custo para as LAN's é inferior ao das WAN's, permitindo assim aumentar a qualidade e a velocidade de transmissão. As três topologias mais utilizadas são: estrela, anel e barramento.

2.3.1.1 Topologia em estrela

Na topologia em estrela (Figura 4) os segmentos de cabo de cada computador da rede estão conectados a um componente central ou concentrador, que é um dispositivo que conecta vários computadores. Nessa topologia, os sinais são transmitidos do computador, através do concentrador, para todos os computadores da rede. Em uma escala maior, várias redes locais podem estar conectadas em uma topologia estrela. Uma das vantagens dessa topologia é que se um computador falhar somente este computador não poderá enviar ou receber dados e o restante da

rede continuará funcionando normalmente. A sua desvantagem é que como cada computador está conectado a um concentrador, se o concentrador falhar toda a rede deixará de funcionar, de modo que uma das características dessa topologia é a geração de colisões na rede (CIOTTI, 2003).

Outra desvantagem da topologia estrela é relativa à modularidade. A configuração pode ser expandida até certo limite imposto pelo nó central: em termos de capacidade de chaveamento, número de circuitos concorrentes que podem ser gerenciados e número total de nós que podem ser servidos. Embora não seja frequentemente encontrado, é possível a utilização de diferentes meios de transmissão para ligação dos nós escravos ao nó central (SOARES, 1995).

O desempenho obtido em uma rede em estrela depende da quantidade de tempo requerido pelo nó central para processar e encaminhar uma mensagem, e da carga de tráfego na conexão, isto é, o desempenho é limitado pela capacidade de processamento do nó central. Um crescimento modular visando o aumento do desempenho torna-se a partir de certo ponto impossível, tendo como única solução a substituição do nó central (SOARES, 1995).

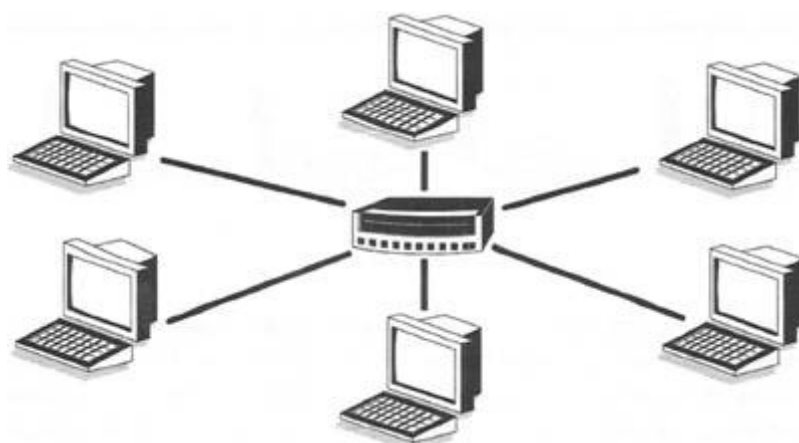


Figura 4 - Topologia em estrela
Fonte: <http://www.fazerfacil.com.br/rede/topologia.htm>

2.3.1.2 Topologia em anel

Na topologia em anel (Figura 5), os computadores estão conectados em um único círculo de cabeamento. Diferente da topologia em barramento, não há terminadores nas extremidades, de maneira que os sinais percorrem o caminho em uma só direção e passam através de cada computador, que funciona como um repetidor, amplificando o sinal e o enviando ao computador seguinte, possibilitando a preservação da intensidade do sinal. O método de transmissão de dados ao redor do anel é denominado passagem do *token*. O *token* é uma série especial de bits que contém informações de controle. A posse do *token* permite que um dispositivo transmita dados à rede. O computador emissor remove o *token* e envia os dados ao anel. Cada computador passa os dados adiante até que o pacote localize o computador com o endereço correspondente ao endereço dos dados. Depois o computador receptor reenvia uma mensagem para o computador emissor, indicando que os dados foram recebidos. Após a verificação, o computador emissor cria um novo *token* e o libera para a rede. A vantagem da topologia em anel é lidar com ambientes de tráfego elevado melhor dos que as redes em barramento. Já a desvantagem é que somente um computador de cada vez pode enviar dados em um único *token ring*. Além disso, a topologia em anel geralmente tem um custo mais elevado do que a topologia de barramento (CIOTTI, 2003).

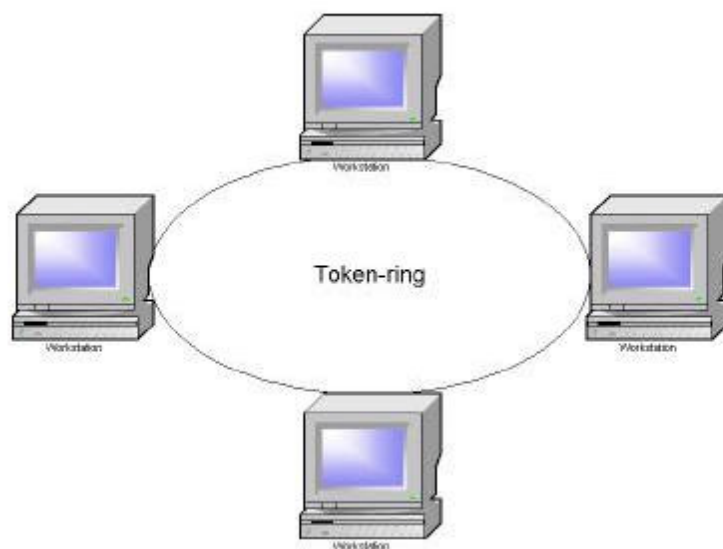


Figura 5 - Topologia em anel
Fonte: CIOTTI (2003)

2.3.1.3 Topologia em barramento

A topologia em barramento ou linear (Figura 6) é simples e fácil de ser implementada. Todos os computadores são interligados por meio de um cabo contínuo. Os dados são enviados e circulam por todos os computadores. Cada computador é identificado através de seu endereço físico (MAC address) (MENDES, 2007).

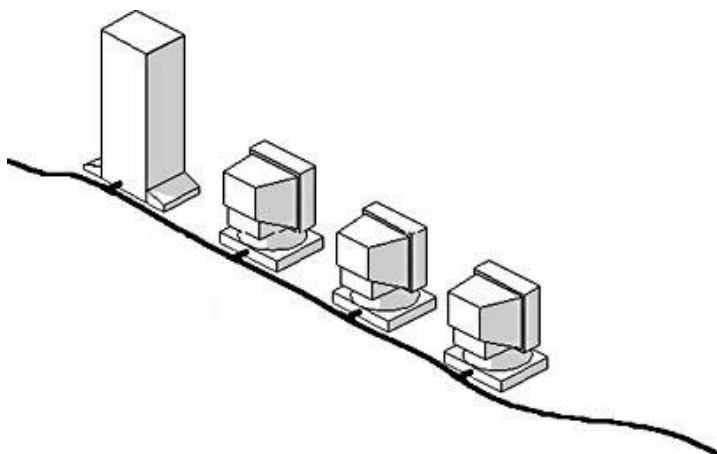


Figura 6 - Topologia em barramento
Fonte: MIRANDA (2008)

Nessa topologia os sinais elétricos são transmitidos através do cabo. As extremidades devem ser finalizadas com dispositivos de hardware, chamados terminadores, que funcionam como os limites para o sinal e definem o segmento. Se houver um rompimento do cabo ou não existir um terminador, o sinal será transportado continuamente através da rede e toda comunicação será interrompida. O número de computadores conectados a um barramento também afeta o desempenho da rede, pois, quanto maior for o número de computadores no barramento, maior será o tempo de espera para enviar os dados e, conseqüentemente mais lenta será a rede. Além disso, devido ao modo como os equipamentos se comunicam em uma topologia em barramento, poderá existir muita colisão, ou seja, o tráfego que é gerado quando computadores tentam se comunicar uns com os outros simultaneamente. O aumento do número de computadores resulta em colisões, reduzindo a eficiência da rede (CIOTTI, 2003).

O controle desse tipo de rede pode ser centralizado ou distribuído, não existindo um controlador central, mas em cada nó individual da rede. Uma interrupção na barra de transporte causará impactos em todos os nós a ela conectados. Erros intermitentes são dificilmente isolados e determinados. Os protocolos de controle de acesso podem ser tanto por demanda como controlado, sendo que o protocolo mais utilizado para este tipo de topologia é o CSMA (*Carrier Sense Multiple Access*) (CIOTTI, 2003).

2.3.2 Redes geograficamente distribuídas

As topologias nas WAN's podem variar devido ao alto custo e às necessidades da organização. Geralmente são utilizados serviços de comunicação contratados de organizações de telecomunicações para realizar este tipo de conexão. As organizações de telecomunicações fornecem diversos serviços como conexões com a Internet, conexões como X.25, Frame Relay e ATM e até conexões especializadas, como de tempo real (FOROUZAN, 2008).

2.4 MODELO DE REFERÊNCIA TCP/IP

Esse modelo baseia-se principalmente em um serviço de transporte orientado à conexão fornecido pelo *Transmission Control Protocol* (TCP), e em um serviço de rede não orientado à conexão (datagrama não confiável), fornecido pelo protocolo *User Datagram Protocol* (UDP) (TANENBAUM, 2003).

Diferente dos sistemas proprietários, o TCP/IP foi desenvolvido como padrão aberto onde qualquer um pudesse usar em uma grande escala de interoperabilidade de

sistemas. A idéia deste modelo surgiu no Departamento de defesa Americano, que tinha como objetivo manter a comunicação entre as bases militares em uma ocorrência de ataques ou catástrofes que afetassem os meios de comunicação (MENDES, 2007).

Os padrões da arquitetura TCP/IP não são elaborados por órgãos internacionais de padronização, como a ISO ou a IEEE. O coro técnico que coordena o desenvolvimento dos protocolos dessa arquitetura é um comitê denominado IAB (*Internet Activity Board*). O IAB é formado por pesquisadores seniores, tendo a maioria deles projetado e implementado os protocolos da arquitetura internet. O IAB, na realidade, produz poucos documentos. Qualquer pessoa pode projetar, documentar, implementar e testar um protocolo para ser usado na internet (SOARES, 1995).

Segundo Odom (2003), o TCP/IP possui uma série de protocolos menores: na verdade, o próprio nome TCP/IP é uma combinação de dois desses protocolos: o *Transmission Control Protocol* e o *Internet Protocol*. A arquitetura TCP/IP é composta por quatro camadas conforme a Figura 7, que serão mostrados a seguir:

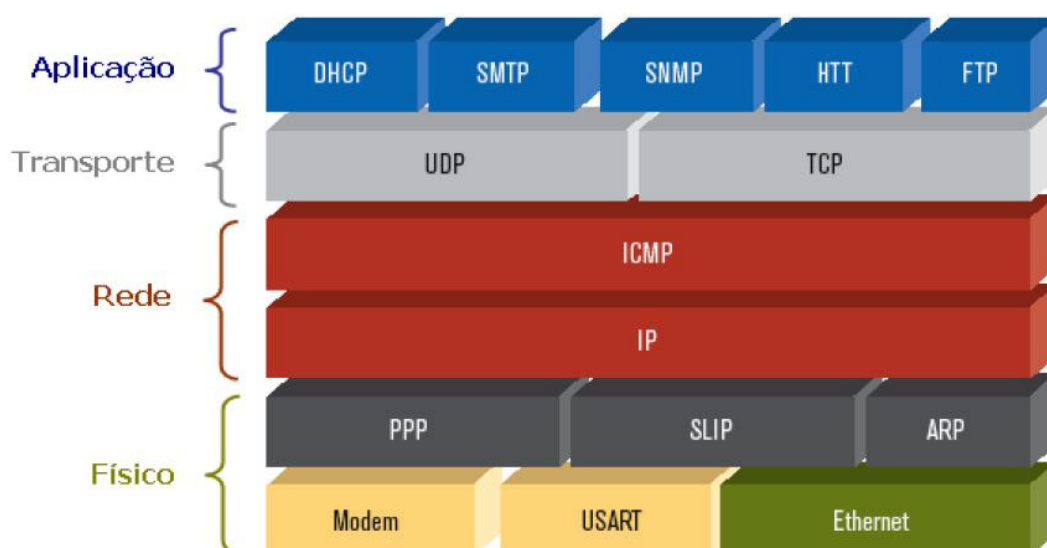


Figura 7 - Camadas da arquitetura TCP/IP e respectivos protocolos
Fonte: MIRANDA (2008)

2.4.1 Camada Física

A camada de rede, ou física, é responsável por converter as tensões elétricas recebidas pela placa de rede em bits 1 ou 0. Em seguida, esses bits são agrupados em pacotes e entregues à camada superior que, por sua vez, continuará repassando até chegar à camada de aplicação, na qual o conteúdo recebido será processado e apresentado ao usuário (MENDES, 2007).

Na arquitetura internet (TCP/IP) não há restrições às redes que são interligadas para formar a inter-rede. Para uma rede ser conectada ela deve apenas possuir uma interface que a torne compatível com o protocolo IP. Essa função se encontra mais especificamente no nível de interface da rede, que encaminha os datagramas IP para os destinos específicos. Para realizar este encaminhamento os endereços IP são traduzidos para os endereços de hardware dos dispositivos conectados à rede (SOARES, 1995).

2.4.2 Camada Inter-redes

O nível inter-redes é responsável pela interligação de redes de comunicação. Suas tarefas são permitir que os hosts enviem e recebam pacotes em qualquer rede e garantir que estes pacotes trafegarão corretamente até seu destino. O roteamento de pacotes é uma questão de grande importância neste nível, assim como o controle de congestionamentos na rede (TANENBAUM, 2003).

Estas mensagens podem chegar em uma ordem diferente daquela em que foram enviadas, obrigando as camadas superiores a reorganizá-las, caso a entrega em ordem seja desejável (TANENBAUM, 2003).

A camada inter-rede define um formato de pacote oficial e o protocolo IP. O pacote ou datagrama (Figura 8) utilizado pelo protocolo IP consiste em um cabeçalho e um payload (pacotes de dados), sendo que o cabeçalho possui um comprimento fixo de 20 bytes mais um comprimento variável. A tarefa da camada inter-redes é entregar os pacotes IP onde são necessários. O roteamento é uma questão de grande importância nessa camada, assim como a necessidade de evitar congestionamentos (TANENBAUM, 2003).

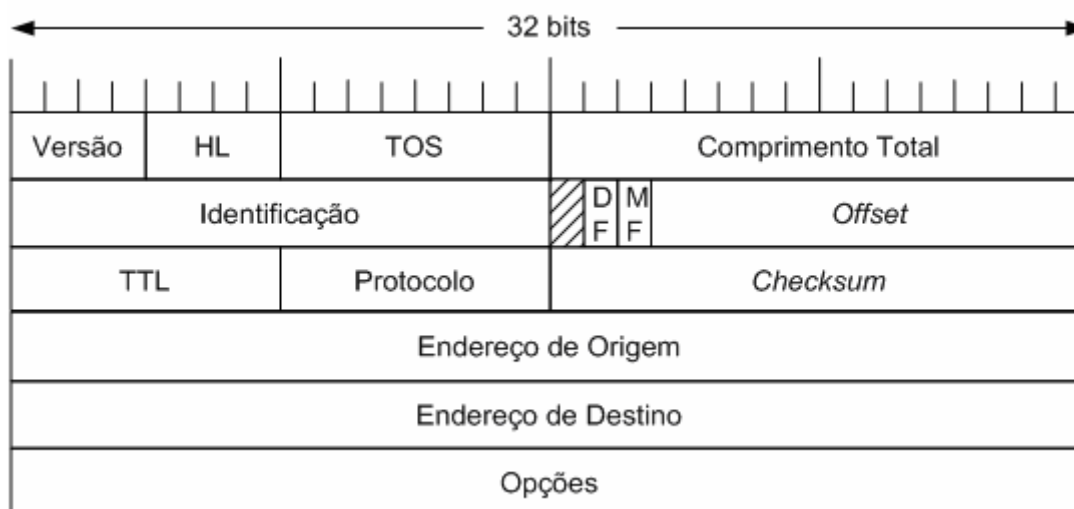


Figura 8 - Datagrama do protocolo IP
Fonte: TANENBAUM (2003)

2.4.3 Camada de Transporte

O nível de transporte provê uma conexão entre a camada de aplicação e os serviços oferecidos pelas camadas mais baixas (Física e Inter-redes). Isso torna as redes físicas transparentes para a camada de aplicação. A camada de transporte trata também do controle de conexão, oferecendo serviços orientados à conexão e serviços sem conexão (FOROUZAN, 2008).

Dois protocolos fim a fim atuam nesta camada. O primeiro deles, o TCP (*Transmission Control Protocol*), é um protocolo orientado a conexão confiável que

permite a entrega sem erros de um fluxo de bytes, originado de um determinado computador, em qualquer outro computador da inter-rede. Esse protocolo fragmenta o fluxo de bytes de entrada em mensagens e encaminha cada uma delas para a camada inter-redes. No destino, O TCP cuida também do controle de fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens maior do que ele pode manipular (TANEMBAUM, 2003).

O segundo protocolo, o UDP (*User Datagram Protocol*), é um protocolo de conexão não confiável destinado a aplicações que não requerem controle de fluxo nem a manutenção da sequência das mensagens enviadas. Ele é amplamente usado em consultas e aplicações diretas do tipo cliente/servidor com solicitação e resposta, nas quais a entrega é mais importante do que a entrega precisa, como transmissão de dados de voz ou de vídeo (TANEMBAUM, 2003).

2.4.4 Camada de Aplicação

A camada de aplicação trata de protocolos de alto nível. No modelo TCP/IP questões de representação, codificação e controle de diálogo foram tratados em uma única camada. O TCP/IP combina todas as questões relacionadas a aplicações e presume que esses dados estejam empacotados corretamente para a próxima camada (MENDES, 2007).

A camada de aplicação contém os protocolos de alto nível. Dentre eles estão o protocolo de terminal virtual (*Telnet*), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP – *Simple Mail Transfer Protocol*). O protocolo de terminal virtual permite que o usuário de um computador estabeleça login em uma máquina remota e a utilize. O protocolo de transferência de arquivos permite mover dados com eficiência de uma máquina para outra. Originalmente, o correio eletrônico era um tipo de transferência de arquivos. Posteriormente um protocolo especializado foi desenvolvido para essa função. Muitos outros protocolos

foram incluídos com o decorrer dos anos como o DNS (*Domain Name Service*), que realiza o mapeamento dos nomes de hosts para seus respectivos endereços de rede, o NNTP (*Network News Transfer Protocol*), protocolo usado para mover novos artigos e o http (*Hyper Text Transfer Protocol*), utilizado para acessar páginas web, entre outros (TANEMBAUM, 2003).

3 VPN (VIRTUAL PRIVATE NETWORK)

Uma VPN (*Virtual Private Network*), ou rede privada virtual, como o nome sugere, é uma rede virtual, criada para interligar duas redes distantes, através da internet. Usar uma VPN permite que você compartilhe arquivos e use aplicativos de produtividade e de gerenciamento, como se todos os computadores estivessem conectados à rede local (MORIMOTO, 2008).

As redes privadas virtuais podem ser implementadas sobre Frame Relay e ATM, porém a abordagem mais utilizada atualmente é sobre a Internet. Para implementar este tipo de rede, a matriz e as filiais da organização - ou os diversos campus de uma universidade – devem possuir uma conexão com a Internet protegida por um firewall, para que seja possível criar o ambiente de conexão de maneira segura e confiável. As informações transmitidas por esse “túnel” criado pela VPN serão criptografadas e autenticadas, o que garante a segurança e a integridade da transmissão.

Uma das grandes vantagens das redes privadas virtuais é a transparência, pois, os usuários irão navegar como se estivessem na própria rede local.

Essas conexões virtuais podem ser feitas de diversas maneiras, conectando apenas dois computadores, duas redes, ou até mesmo usuários móveis.

3.1 CONCEITOS

Serão explicados agora alguns conceitos básicos para o entendimento e a implementação da VPN.

3.1.1 Segurança

Atualmente, tanto os sistemas do mundo real quanto os do mundo virtual, por maior que seja o investimento em segurança, ainda sofrem ataques, invasões e roubos. Por isso devemos conhecer as formas mais comuns de ataques e como preveni-las.

A internet traz diversos perigos relacionados à segurança, e justamente com o desconhecimento dos usuários, pode causar diversos problemas. Serviços de bancos, de compras e até mesmo trocas de informações por e-mail podem estar sendo monitorados por algum invasor, que irá utilizar as informações coletadas.

A segurança é a principal função da VPN, pois seus dados são trafegados pela chamada rede pública (a Internet), que, conforme vimos, é um meio inseguro. A VPN utiliza mecanismos de segurança para identificar os usuários, ou seja, definir se um usuário pode ou não acessar a rede. Utiliza também mecanismos de criptografia para validar a confidencialidade das informações. Além disso, a VPN verifica autenticidade dos pacotes, identificando se os pacotes recebidos são os mesmos que foram enviados (SILVA, 2002).

Para se proteger de ataques, uma VPN contém diversos métodos que garantem um nível de segurança entre os pontos transmissores e receptores de mensagens.

3.1.1.1 Autenticação e integridade

Os sistemas computacionais atuais permitem a conexão de vários usuários verificando com precisão cada um que esteja fazendo uma solicitação. Este tipo de verificação é realizada validando a senha e o nome de login durante a conexão. Através deste login e desta senha o sistema pode determinar quais recursos o

usuário terá permissão de acesso. Este processo de validação de login e senha é chamado de autenticação (STALLINGS, 2008).

Este tipo de serviço é importante, pois, usuários não autorizados não poderão utilizar os recursos do sistema, dificultando o acesso ou invasão de pessoas não autorizadas.

A autenticidade e a integridade têm como objetivo garantir que a mensagem enviada pelo transmissor não seja modificada em seu percurso. Para isso ela recebe um tratamento em seus caracteres, tornando-os não legíveis. Isso não impede que os dados sejam capturados, mas sim que estes dados sejam modificados, garantindo que a informação será a mesma do transmissor ao receptor (STALLINGS, 2008).

3.1.1.2 Confidencialidade

Confidencialidade trata do sigilo das informações. Nem todas as informações são sigilosas, mesmo algumas que são críticas podem não exigir esse cuidado. O princípio da confidencialidade tem como objetivo assegurar que apenas pessoas autorizadas tenham acesso à informação (STALLINGS, 2008).

A confidencialidade é um mecanismo utilizado pela VPN com o objetivo de “misturar” as informações enviadas através dela para que invasores não possam acessar seu conteúdo, ou seja, protege as informações contra o uso impróprio (SILVA, 2002).

3.1.1.3 Criptografia

A criptografia é o estudo de códigos e cifras, cujo nome vem do grego Kryptos, que significa oculto, e graphe, que significa escrever. Já a palavra cifra vem do hebraico saphar, que significa dar números (SILVA, 2002).

Segundo Tanenbaum (2003), quatro grupos contribuíram para a arte da criptografia: os militares, os diplomatas, as pessoas que gostam de guardar memórias e os amantes. Dentre eles, os militares tiveram o papel mais importante e definiram as bases para a tecnologia. Dentro das organizações militares as mensagens a serem criptografadas eram entregues à auxiliares mal remunerados que se encarregavam de criptografá-las e transmiti-las. O grande volume de mensagens impedia que esse trabalho fosse feito por poucos especialistas.

De acordo com Stallings (2008), a criptografia é a ferramenta automatizada mais importante para a segurança das redes de computadores. Duas formas de criptografia são usadas normalmente: a criptografia convencional, ou simétrica, e a criptografia por chave pública, ou assimétrica. Estes dois métodos serão detalhados a seguir.

3.1.1.3.1 Chave simétrica

Este conceito foi criado em 1972 pela IBM, com o apelido de Lúifer Cipher e em 1977 foi revisto e publicado pelo *National Institute of Standards* (NIST), *Federal Information Processing Standards* (FIPS) e *American National Standards Institute* (ANSI), já com o nome de *Data Encryption Standard* (DES). O DES trabalha com chave de 64bits, sendo que 56 bits para a chave e 8 bits de paridade (SILVA, 2002).

O conceito de chave simétrica consiste em utilizar a mesma chave para criptografar e descriptografar a informação do emissor para o destinatário. Porém, este tipo de chave possui alguns problemas, como por exemplo, garantir que somente o emissor e o destinatário possuem esta chave. Antes de começar a enviar dados

criptografados o destinatário deve receber a chave do emissor, para isso é necessário um meio seguro de transmissão da chave.

A Figura 9 mostra uma mensagem sendo transmitida e utilizando a chave simétrica para criar um documento criptografado. No destino é utilizada a mesma chave para descriptografar o documento e mostrar a mensagem original.

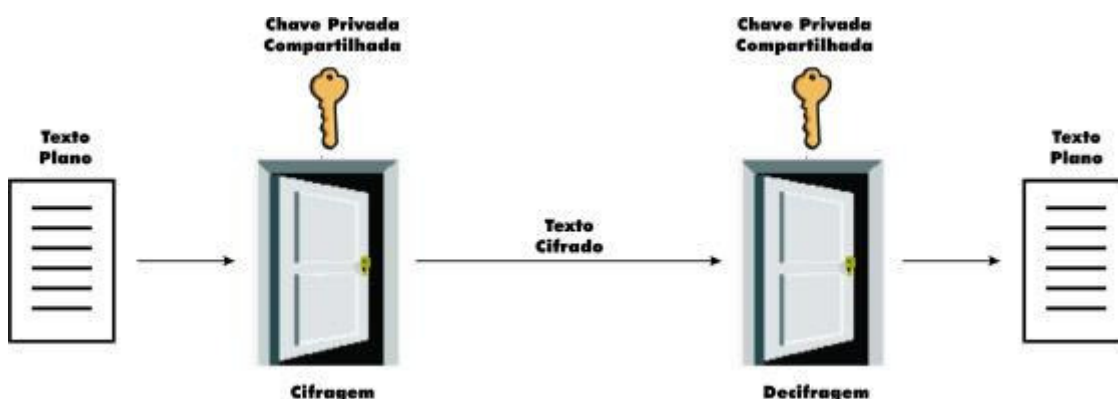


Figura 9 - Transmissão de uma mensagem usando chave simétrica
Fonte: VASQUES (2002)

3.1.1.3.2 Chave assimétrica

O conceito de chave assimétrica é bem mais complexo do que o da chave simétrica. A chave é dividida em duas: uma chave privada e uma chave pública. Um usuário que deseja fazer a criptografia desta maneira cria as duas chaves. A chave Pública ele distribui ou coloca a disposição para quem quiser lhe enviar dados. A chave privada apenas o usuário criador das chaves possui e apenas esta chave pode descriptografar as informações previamente criptografadas com a chave pública correspondente.

Caso dois usuários queiram trocar informações utilizando o conceito de chave assimétrica, cada um deve criar suas duas chaves e disponibilizar para o outro sua chave pública, ou seja, o usuário A gera uma chave composta da chave privada dele com a chave pública do usuário B. O usuário B cria uma chave composta por sua

chave privada e pela chave pública do usuário A. Na transmissão das mensagens do usuário A para o B é utilizada a chave de A para criptografar e a chave de B para descriptografar a mensagem, como mostra a Figura 10.

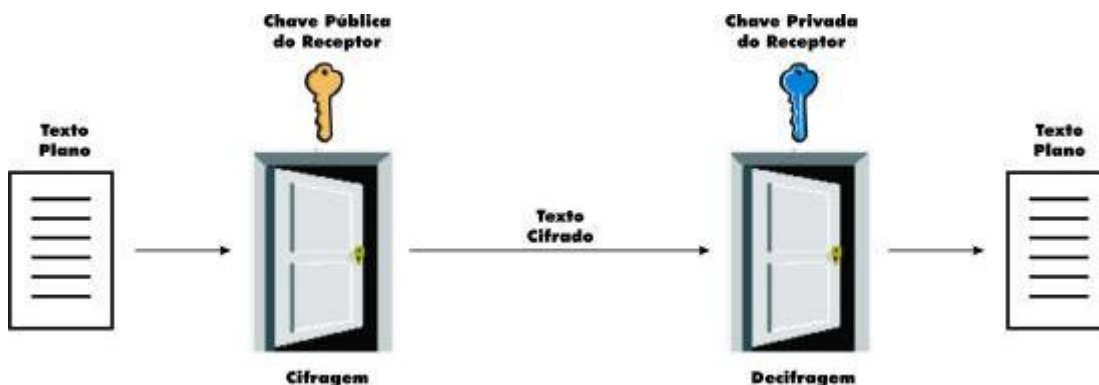


Figura 10 - Transmissão de uma mensagem usando chave assimétrica
Fonte: VASQUES (2002)

3.1.1.4 Firewall

A internet é um serviço bastante útil onde podemos buscar vários tipos de informação, trocamos informações entre organizações, entre amigos, etc. Porém temos que saber que a qualquer momento podemos ter nossos computadores e sistemas invadidos. Com o objetivo de evitar essas invasões foram criados os Firewalls.

Segundo Tanenbaum (2003), um firewall é apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Este recurso forçava todos aqueles que quisessem entrar ou sair do castelo passar por uma única ponte levadiça onde poderiam ser revistados por guardas. Nas redes é possível usar o mesmo artifício: uma organização pode ter muitas LAN's conectadas de forma arbitrária, mas todo o tráfego de entrada e saída da organização é feito através de uma ponte levadiça eletrônica.

Os Firewalls podem ser divididos em duas categorias: o Firewall de nível de rede e o Firewall de aplicativo.

3.1.1.4.1 Firewall de nível de rede

Os firewalls de nível de rede são muito eficientes para filtragem de pacotes, podendo barrar acessos pelo endereço de origem, protocolo, número da porta ou pelo conteúdo. Os roteadores são facilmente implementados para este tipo de solução, e por serem externos, eliminam a necessidade de parar a operação da rede caso necessite parar o Firewall. Uma desvantagem de alguns Firewalls com roteadores é que este é vulnerável a ataques de spoofing (tentativa de obter acesso a um sistema usando uma identidade falsa), de IP e de DNS.

3.1.1.4.2 Firewall de aplicativo

Este tipo de firewall é o mais seguro e sua configuração tem algumas vantagens. Pode ser configurado exigindo que todos os computadores de uma rede passem por ele antes de chegar à rede pública, e também restringindo o acesso através de um Proxy¹. O Proxy pode fornecer autenticação de usuários e armazenar logs de acesso no nível de aplicação.

Em uma VPN, o Firewall pode estar localizado integrado com o gateway VPN ou antes da mesma, como mostra a Figura 11:

¹ O termo Proxy vem de uma palavra em inglês que significa procuração. Em termos técnicos, o Proxy é um software que tem a “procuração” de um ou mais hosts para buscar na internet uma informação solicitada.

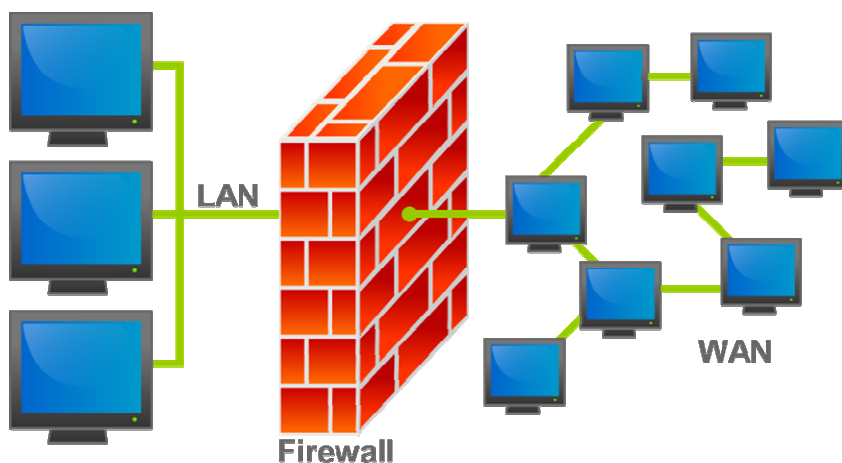


Figura 11 - Disposição do Firewall de uma VPN
Fonte: <http://www.churchtechy.com/2009/09/personal-firewalls/>

3.1.2 Topologias

Uma VPN pode ser montada de maneiras diferentes, dependendo da topologia que se utilizar. Serão mostradas estas topologias a seguir.

3.1.2.1 Host-host

A topologia host-host é utilizada quando um computador que pode ou não estar em uma rede comunica-se com outro computador que está fisicamente distante.

Esta topologia tem como principal objetivo reduzir os custos de interligação de redes inteiras, pois serão conectados apenas dois computadores, o que não evita os gastos com a disponibilidade da VN para a rede interna.

3.1.2.2 Host-rede

Esse tipo de topologia é utilizado por organizações que precisam que os usuários da rede se conectem através de hosts móveis, para buscar ou armazenar informações. Para o usuário móvel fazer esse tipo de conexão basta ter acesso à internet e algum software que possibilite a conexão com a VPN, de maneira segura e confiável.

3.1.2.3 Rede-rede

Pra implementação deste tipo de topologia é necessário que as duas redes que querem se conectar possuam um gateway VPN, para que exista uma conexão segura. Essa topologia é utilizada por organizações que precisam se interligar, porém, estão distantes fisicamente. A organização pode também compartilhar informações com parceiros, fornecedores ou consumidores, desde que estes possuam um gateway e uma permissão para conexão.

3.1.3 Appliance

O conceito de Appliance vem sendo muito difundido no mercado. Consiste em uma combinação de software e hardware para uso dedicado de aplicações específicas. Segundo Silva (2002), esses equipamentos foram projetados para serem uma solução única de segurança, agregando funcionalidades, tais como: roteador e filtro de pacotes, Firewall, servidor de antivírus, serviço de detector de invasão, etc. Existem também appliances com o serviço de VPN já integrado.

3.1.4 Endereçamento IP

Todo computador que faz parte de uma rede precisa de uma identificação para acessar essa rede. O endereçamento IP é a forma mais utilizada de identificação de equipamentos em uma rede de computadores, inclusive na internet. Os endereços IP podem ser utilizados para referenciar tanto a rede quanto a um host ou estação específica (SILVA, 2002).

Segundo Tanenbaum (2003), o método normalmente utilizado é definir os endereços de transporte que os processos podem “ouvir” para receber solicitações de conexão. Na internet essas extremidades são chamadas portas, que podemos definir como TSAP (*Transport Service Access Point* – ponto de acesso de serviço de transporte). Os pontos extremos análogos na camada de rede, ou seja, os endereços da camada de rede, são chamados então NSAP's (*Network Service Access Point*). Os endereços IP são exemplos de NSAP's.

3.1.5 IPV6

A necessidade de evolução do IP se tornou necessária a partir da década de 1990 quando a internet passou a ser utilizada por um número cada vez maior de usuários com necessidades distintas. Se considerarmos que aparelhos eletrônicos como celulares e televisores poderão em breve estar todos conectados à internet, serão necessários mais endereços de identificação. Surgiu então o IPV6 que possibilita um número maior de endereçamentos que o IPV4.

Segundo Tanenbaum (2003), os principais objetivos do IPV6 são:

- Aceitar bilhões de hosts, mesmo com alocação de espaço de endereçamento ineficiente;

- Reduzir o tamanho das tabelas de roteamento;
- Simplificar o protocolo, de modo a permitir que os roteadores processem os pacotes com rapidez;
- Oferecer mais segurança que o IPV4;
- Dar mais importância ao tipo de serviço, particularmente no caso de dados em tempo real;
- Permitir multidifusão, possibilitando a especificação de escopos;
- Permitir que um host mude de lugar sem precisar mudar de endereço;
- Permitir a evolução do protocolo;
- Permitir a coexistência de novos protocolos e antigos por alguns anos.

Uma das diferenças em relação ao tamanho do endereço é que o IPV4 é formado por 4 octetos de representação decimal. Já o IPV6 é formado por 16 grupos de 8 bits, que podem também ser representados sob a forma hexadecimal.

Ex. IPV4: 192.168.10.1

Ex. IPV6: 2001:bce4:5641:3412:341:45ae:fe32:65

3.1.6 DHCP

O DHCP (*Dynamic Host configuration Protocol*) é um protocolo utilizado nas redes de computadores que permite a distribuição automática de endereços IP aos hosts da rede, sem que haja conflitos de endereçamento. Esse protocolo foi desenvolvido pelo IETF e está documentado na RFC 2131 (www.ietf.org).

Em uma rede pequena é comum os administradores definirem um número IP para cada computador, porém, com a expansão da rede, torna-se muito difícil gerenciá-la desta maneira. Nesta situação pode ser configurado o serviço DHCP que fará a distribuição dos endereços de acordo com a configuração previamente estabelecida, otimizando a utilização da rede.

3.1.7 DNS

Os hosts podem se referir a outros através de seus endereços IP (192.168.10.10, por exemplo), porém, para guardar todos os endereços utilizados em grandes rede é uma tarefa difícil. Surgiu então a necessidade de um serviço que faça a conversão destes endereços para nomes mais fáceis de se interpretar.

Segundo Tanenbaum (2003), antigamente havia apenas o arquivo `hosts.txt` que listava os hosts e seus endereços. Toda noite este arquivo era acessado e copiado por todos os hosts. Para uma rede de algumas centenas de máquinas essa estratégia funcionava razoavelmente bem. Porém, com o aumento da necessidade de interconexões das redes, era praticamente impossível armazenar em um arquivo a quantidade de hosts e seus endereços IP. Para Solucionar estes problemas, foi criado o DNS, (*Domain Name Service*) ou serviço de nomes de domínio.

A essência do DNS é a criação de um sistema hierárquico de distribuição de nomes baseado no domínio, e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é utilizado principalmente para mapear nomes de hosts e destinos de mensagens de correio eletrônico em endereços IP, mas também pode ser utilizado para outros objetivos. O DNS é definido nas RFC's 1034 1035 (TANENBAUM, 2003).

3.1.8 Tunneling

A técnica chamada de tunneling (tunelamento) se refere à criação de um túnel virtual para transferência de informações, por uma rede pública ou privada, garantindo

maior segurança. As informações são trafegadas de forma encriptada, dando a idéia da criação de um túnel virtual, como mostra a Figura 12, onde os dados que estiverem trafegando por esse túnel permeassero inteligíveis para quem não faz parte dele. Isso garante que, se a informação for capturada, será muito difícil entendê-la sem a chave de criptografia utilizada.

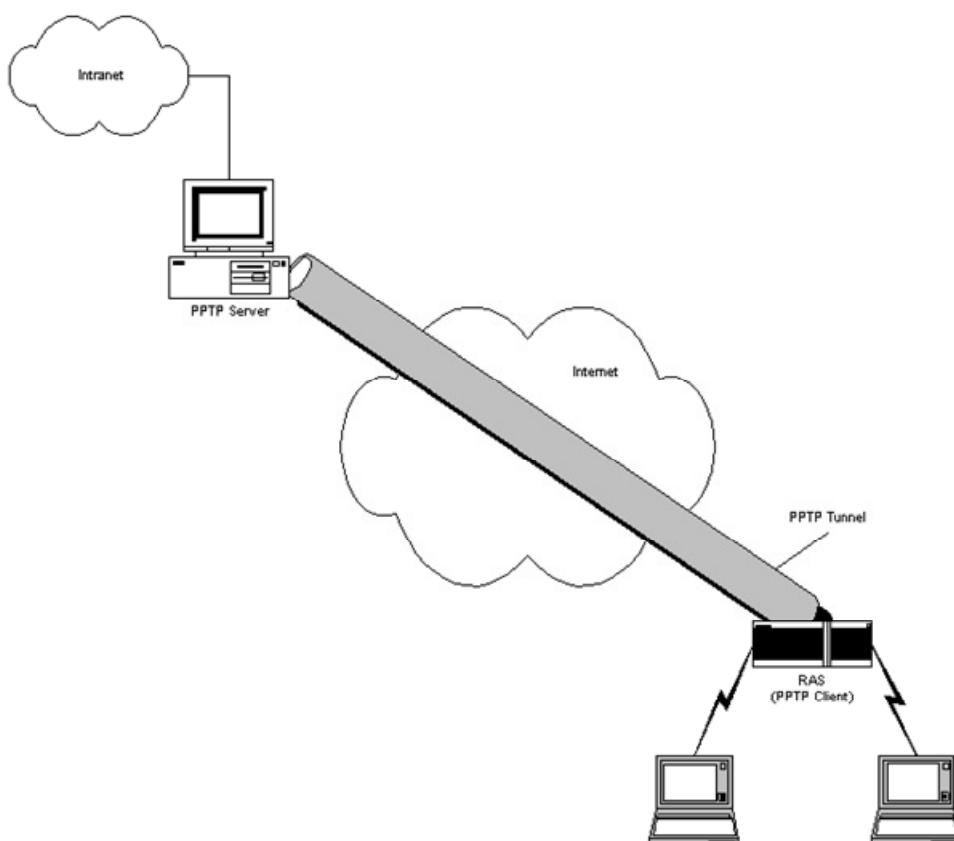


Figura 12 - Criação do Túnel virtual

Fonte: <http://technet.microsoft.com/en-us/library/cc768083.aspx>

Esta técnica é muito utilizada para interligação de redes onde as informações precisam trafegar por outras redes desprotegidas. Por exemplo, se uma organização que utiliza uma rede Ethernet baseada em TCP/IP precisa trafegar dados por uma rede ATM ou Frame-Relay para se comunicar com a rede da outra organização que também é Ethernet, precisa utilizar esta técnica.

3.1.9 NAT

O NAT (*Network Address Translation* – Tradução de Endereço de Rede) não é um protocolo e também não se refere a um padrão especificado por entidades internacionais. O NAT é apenas uma série de tarefas que um roteador (ou equipamento similar) deve realizar para converter endereços IP's entre redes distintas. Um equipamento que tem o recurso de NAT deve ser capaz de analisar todos os pacotes de dados que passem por ele e trocar os endereços destes pacotes de maneira adequada, ou seja, substituir o endereço IP de origem do pacote (endereço IP não roteável) pelo endereço IP do roteador (endereço IP roteável). Além dessa substituição de endereço, o roteador que possui NAT ainda cadastra em sua tabela a relação porta origem e IP origem, a fim de devolver ao emissor o pedido feito (MENDES, 2007).

O mesmo acontece quando um host externo tenta enviar um pacote para um host interno da rede local. O pacote vem com o endereço IP do roteador e este identifica para qual host interno deve encaminhar o pacote.

3.2 VULNERABILIDADES

Os requisitos de segurança da informação dentro de uma organização passaram por mudanças importantes nas últimas décadas. Com a introdução de sistemas distribuídos e o uso de recursos de comunicação, como as redes de computadores, surgiu a necessidade de se garantir a segurança e a disponibilidade destes serviços (STALLINGS, 2008).

Talvez os tipos mais sofisticados de ameaças a redes de computadores são apresentados por programas que exploram vulnerabilidades (STALLINGS, 2008).

A segurança da informação é um dos principais fatores de se utilizar uma VPN para realização de conexões. Existem várias maneiras de se tentar corromper esta segurança, seja para adquirir informações confidenciais ou até mesmo por diversão ou simplesmente para se provar que é possível corromper aquele sistema. Várias questões são consideradas na implantação da segurança da informação como, por exemplo, o custo. Uma estrutura de maior segurança exige maiores investimentos em equipamentos e capacitação dos administradores de redes.

Os maiores problemas de segurança relacionados à VPN podem estar na infraestrutura montada. Mesmo com a utilização de Firewalls e políticas de segurança ataques a essa infra-estrutura podem comprometer o bom funcionamento da rede e seus serviços.

A seguir serão mostrados alguns métodos de ataque a redes de computadores.

3.2.1 DoS

Um ataque de negação de serviço (DoS – *Denial of Service*) é uma tentativa de impedir que usuários legítimos de um determinado serviço utilizem este serviço. Estes ataques representam uma ameaça significativa para as organizações. Eles tornam os sistemas inacessíveis inundando os servidores, redes e até mesmo sistemas de usuário final com tráfego inútil, para que os usuários legítimos não possam mais ter acesso a estes recursos (STALLINGS, 2008).

Este talvez seja um dos piores ataques. O objetivo do atacante é deixar o sistema ou os servidores da vítima inoperantes, aumentando o volume de requisições destinadas a eles. O atacante dispara milhares de requisições a um servidor. O servidor tenta responder a todas as requisições em vão o que gera um atraso na resposta às requisições corretas tornando o serviço inoperante. Nesta situação deve-se tentar

descobrir a origem das requisições e configurar filtros nos roteadores, impedindo que as requisições cheguem ao servidor (SILVA 2002).

3.2.2 DDoS

O *Distributed Denial of Service* (negação de serviço distribuído) é a evolução do DoS. Esta técnica consiste em utilizar mais de uma máquina (denominadas zumbis) para causar a negação dos serviços na rede da vítima. Existem várias maneiras sofisticadas para interrupção dos serviços e uma delas é o ataque denominado de Smurf, no qual são enviados pacotes ICMP (*Internet Control Message Protocol*) de difusão em uma rede com o endereço de origem forjado com o endereço da vítima. Ao receberem a mensagem as máquinas respondem à vítima, interrompendo seus serviços (SILVA, 2002).

Nesta técnica o atacante toma o controle de vários hosts pela internet, instruindo-os a entrar em contato com o servidor web do alvo. Os hosts escravos começam a enviar pacotes SYN (sincronização/inicialização de conexões do TCP/IP) com informações de endereços IP de retorno erradas para o alvo. Com isso as conexões legítimas são negadas, tornando indisponíveis os serviços da rede (STALLINGS, 2008).

3.2.3 Ataque DNS

A função do DNS é traduzir nomes conhecidos em endereços IP para facilitar o tráfego de informações. O atacante invade o servidor DNS e altera os endereços de origem, fazendo um redirecionamento de todos os usuário. Em posse de um servidor

de nomes o atacante tem literalmente o controle de um ou mais servidores e o que ele poderá causar é, sem dúvida, catastrófico (SILVA, 2002).

3.2.4 Worms

A tradução seria verme, que é diferente de um vírus de computador. Ele tem uma característica própria em que é necessário alguém executar algum arquivo ou recebê-lo por e-mail. Os Worms vão se propagando na rede, sem intervenção humana, e danificando várias estações em frações de tempo bem pequenas (SILVA, 2002).

Um exemplo deste ataque ocorreu em 2001, quando o Worm Code Red tirou proveito de uma falha de segurança no Microsoft Internet Information Server (IIS) para penetrar e se espalhar. Durante certo período de tempo ele apenas se espalhou sondando endereços IP aleatórios. Depois ele iniciou um ataque de negação de serviço a um site do governo dos EUA, inundando o site com pacotes de diversos hosts (STALLING, 2008).

3.2.5 Ataques a roteadores

A função de um roteador é direcionar o tráfego de uma origem a um destino, roteando os pacotes como um serviço de correio, analisando o destino da carta e entregando-a. Na internet, milhares de pacotes encaminhados para o mesmo roteador e diretamente para ele, sem direcionar para outros roteadores pode causar sua indisponibilidade. Na verdade é uma variação da negação de serviço, direcionado a um roteador (SILVA 2002).

3.3 PROTOCOLOS

Os protocolos são utilizados para especificar quais os formatos dos dados e as regras a serem seguidas em uma rede. Ele especifica como um programa deve preparar seus dados para trafegarem no processo de comunicação. Serão mostrados a seguir alguns protocolos que podem ser utilizados na implementação de uma VPN.

3.3.1 GRE

O protocolo GRE (*Generic Routing Protocol*) é utilizado para configurar túneis entre um roteador solicitante e um roteador destino (ponto-a-ponto). Os pacotes que serão enviados, por exemplo, são encapsulados com o protocolo IP, são novamente encapsulados pelo protocolo GRE, agregando um novo cabeçalho. Após este encapsulamento o pacote é enviado pelo túnel e ao chegar ao destino são desencapsulados.

3.3.2 PPP

Segundo Tanenbaum (2003), o protocolo PPP trata da detecção de erros, aceita vários protocolos, permite a autenticação e inclui muitas outras características. Ele dispõe de três recursos principais:

- Um método de enquadramento que delinea de forma não ambígua o fim de um quadro e o início do quadro seguinte. O formato do quadro também lida com a detecção de erros.

- Um protocolo de controle de enlace usado para ativar linhas, testá-las, negociar opções e desativá-las novamente quando não forem mais necessárias. Esse protocolo é denominado LPC (*Link Control Protocol* – Protocolo de Controle de Enlace). Ele admite circuitos síncronos e assíncronos, e também codificação orientada a bytes e a bits.
- Uma maneira de negociar as opções da camada de rede de modo independente do protocolo da camada de rede a ser utilizado. O método escolhido deve ter um NCP (*Network Control Protocol* – Protocolo de Controle de Rede) diferente para cada camada de rede aceita.

Segundo Silva (2002), para prover o acesso dos usuários ao servidor VPN, o protocolo de tunelamento é dividido em duas partes: a parte cliente e a parte servidor. A parte cliente é chamada de concentrador de acesso (*Protocol Access Concentrator* – PAC) e fica bem perto do usuário remoto. Ela tem a função de encapsular frames PPP dentro de algo que possa ser roteável na Internet. A parte servidora é chamada de Servidor de Rede (*Network Server* – NS), que fica o mais próximo possível da rede interna. Desta forma, muito tráfego que antes era feito via linha telefônica ficou sob responsabilidade da Internet e do provedor de acesso.

Como foi mostrado anteriormente, o processo de autenticação é um ponto importante para a segurança. No caso do PPP, a autenticação pode ser feita pelas duas pontas, identificando tanto o usuário quanto o servidor. Com o protocolo PPP essa autenticação pode ser feita por dois protocolos: o PAP e o CHAP.

3.3.2.1 PAP

O protocolo PAP (*Password Authentication Protocol* – Protocolo de Autenticação de Senhas) trabalha basicamente da mesma forma que um procedimento de acesso normal. O cliente se autentica enviando um nome de usuário e uma senha, que opcionalmente pode estar encriptada, e que é comparada com a base de senhas

secretas no servidor. Esta técnica é vulnerável contra intrusos que tenham condições verificar todo o tráfego corrente na linha serial, e consigam capturar um usuário válido e sua senha, ou contra tentativas de “adivinhação” de senhas através do método de tentativas e erros (KIRCH, 1999).

3.3.2.2 CHAP

O CHAP (*Challenge Handshake Authentication Protocol* – Protocolo de Autenticação de Apresentação) por sua vez não possui essas deficiências. Com o CHAP o servidor envia para o cliente uma expressão aleatória contendo um desafio, em conjunto com seu nome de máquina. O cliente utiliza o nome de máquina para buscar a chave de solução, combina com a expressão aleatória e encripta o resultado utilizando uma função numérica que não pode ser revertida. O resultado é enviado para o servidor que executa a mesma tarefa e compara os resultados. Caso sejam idênticos o cliente é considerado autêntico (KIRCH, 1999).

Além do método de autenticação, o protocolo CHAP possui outra grande vantagem em relação ao PAP, pois o PAP realiza a autenticação somente no estabelecimento da conexão, enquanto o CHAP realiza sua autenticação em intervalos de tempo para se assegurar que não há intrusos.

3.3.3 PPTP

O PPTP (*Point-to-Point Tunneling Protocol*) foi desenvolvido pelo fórum PPTP que inclui a Microsoft em conjunto com alguns fabricantes de NAS (*Network Access Server*), como a Ascend Communication (parte da Lucent), US Robotics (parte da 3com) e ECI Telematics. Este fórum tinha por objetivo facilitar o acesso de

computadores remotos a uma rede privada através da Internet ou outra forma de rede baseada no protocolo IP. Por ser uma extensão do PPP funciona apenas em conjunto com o *Remote Access Server* (RAS), ou servidor de acesso remoto da Microsoft (SILVA, 2002).

O PPTP encapsula frames de PPP nos datagramas IP para transmissão pela rede IP, tal como a Internet. O PPTP pode ser usado para acesso remoto e conexões VPN roteador a roteador. Ele utiliza uma conexão TCP para o gerenciamento do “túnel virtual” e uma versão modificada do GRE para encapsular frames PPP para dados do túnel. As cargas dos frames PPP encapsulados podem ser criptografadas e/ou comprimidas. A Figura 13 mostra a estrutura do pacote PPTP que contém um datagrama IP.

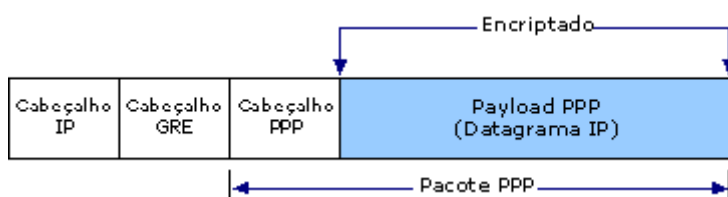


Figura 13 - Estrutura do pacote PPTP que contém um datagrama IP
 Fonte: [http://technet.microsoft.com/pt-pt/library/cc771298\(WS.10\).aspx](http://technet.microsoft.com/pt-pt/library/cc771298(WS.10).aspx)

Em uma conexão PPTP, existem três elementos envolvidos: o cliente PPTP, o servidor de acesso à rede e o servidor PPTP. O cliente se conecta a um servidor de rede utilizando o protocolo PPP. Uma vez conectado, o cliente pode enviar e receber dados via Internet. O servidor utiliza o protocolo TCP para todo o tráfego da Internet. É realizada então uma segunda conexão sobre a conexão PPP existente, interligando o servidor PPTP ao usuário remoto. Os dados desta segunda conexão são enviados na forma de datagramas IP que contêm pacotes PPP encapsulados dentro do PPTP, ou seja, o PPP encapsula o PPTP que, por sua vez encapsula o IP. É essa segunda conexão que cria o túnel com o servidor PPTP nas imediações da LAN corporativa privada. E por último, o usuário remoto envia pacotes IP ou outros datagramas dentro do frame PPP (SILVA, 2002).

3.3.4 L2F

Na mesma época do desenvolvimento do PPTP, a Cisco, a *Northern Telecom* (Nortel) e a *Shiva Corporation* (parte da Intel) estavam desenvolvendo a proposta do L2F (*Layer Two Forwarding*), que tinha como missão permitir que provedores de acesso ou empresas de telecomunicações oferecessem ao mercado acesso remoto para redes privadas; desta forma, as empresas não precisariam adquirir modem ou equipamentos de acesso remoto, podendo apenas pagar o serviço. Com este protocolo o usuário remoto faz uma conexão com o provedor de acesso e o servidor aceita o pedido se o usuário tiver autorização, sendo autenticado utilizando o PAP ou o CHAP. No momento da autenticação o servidor de rede constrói um túnel para a rede privada do cliente (SILVA, 2002).

Com o L2F são permitidos os seguintes protocolos para realizar a conexão ponto-a-ponto: UDP, X.25, ATM e Frame Relay. Uma grande diferença entre este protocolo e o PPTP é a terminação do túnel que no L2F a rede privada do cliente sempre será considerada atrás de um gateway, podendo ser um roteador ou firewall. Quando o túnel é construído entre o servidor e o gateway, o L2F envia indicadores de conexão e informações de autenticação para o gateway, que cria interfaces virtuais entre as conexões SLIP (Serial Line IP) ou PPP, similar a uma conexão discada. Neste ponto da comunicação, o usuário e o gateway podem tratar autenticação, autorização e contabilização. A grande desvantagem do L2F está na parte que define criptografia e encapsulamento de dados (SILVA, 2002).

3.3.5 L2TP

O L2TP (*Layer Two Tunneling Protocol*) foi projetado pela Cisco Systems e posteriormente homologado pela *Internet Engineering Task Force* (IETF) como protocolo padrão, baseia-se no L2F para solucionar problemas deste e do PPTP.

Algumas características como a utilização do PPP para fornecer o acesso remoto e a operação em ambientes como o NetBEUI e o IPX são mantidas do PPTP (VASQUES, 2002).

Segundo Sena (2002), uma das diferenças entre o L2TP e o PPTP está no protocolo utilizado na camada inferior. Enquanto o PPTP deve ser sempre utilizado acima do IP, o L2TP pode utilizar um conjunto de outros protocolos inferiores como o PPP, o IP e o Frame Relay. Sob o ponto de vista da segurança da comunicação o L2TP, diferentemente do PPTP, não possui serviços de criptografia e integridade dos dados. Porém as informações iniciais relativas ao processo de autenticação dos dois extremos do túnel são protegidas enquanto que no PPTP os parâmetros podem ser livremente obtidos.

Este protocolo foi desenvolvido para suportar os dois modos de tunelamento: voluntário e compulsório. O túnel voluntário é iniciado pelo computador remoto, sendo mais flexível para usuários em trânsito que podem discar para qualquer provedor de acesso. Como o provedor de acesso não participa da criação do túnel, este pode percorrer várias redes e vários provedores sem necessidade de configuração específica (SILVA, 2002).

O túnel compulsório é automaticamente criado, sendo iniciado pelo servidor de rede sob a conexão. Isto implica que o servidor de rede deve ser pré-configurado para conhecer a terminação de cada túnel baseado nas informações de autenticação dos usuários remotos. Isto é feito sem nenhuma intervenção do usuário remoto e não há necessidade de outros softwares nos computadores remotos, sendo o processo de tunelamento completamente transparente ao usuário final (SILVA, 2002).

Dado que o L2TP não foi projetado para configuração de ambientes seguros, seu uso em cenários onde existe uma rede não confiável, como a Internet, deve ser sempre combinado com outros protocolos capazes de suprir a sua ausência de serviços de segurança. Um conjunto de propostas tem sido desenvolvido para conciliar o uso do L2TP com o IPSec. Quando executado sobre o IP, o L2TP é transportado através do UDP. Desta forma, a aplicação da proteção do IPSec sobre

o L2TP pode basear-se simplesmente no uso de seletores que filtram o tráfego L2TP (SILVA, 2002).

3.3.6 MPLS

O principal objetivo do MPLS (*Multi Protocol Label Switching*) é reduzir o processamento necessário para cada roteador redirecionar o pacote, permitindo este caminho entre as redes ser baseado em informações que não estão dentro do cabeçalho do datagrama IP. No roteamento IP convencional, cada roteador no caminho toma uma decisão de roteamento independente para cada pacote. Essa decisão é tomada somente com as informações contidas no cabeçalho IP, logo, um cabeçalho IP contém as informações que são necessárias para o redirecionamento do pacote. A decisão de roteamento é feita para cada roteador no caminho do pacote, o que pode ser redundante (SILVA, 2002).

No MPLS, os pacotes são redirecionados baseados num valor de tamanho fixo, chamado Label (rótulo), que é inserido entre o cabeçalho de link e o cabeçalho de rede. Vários cabeçalhos Shim (cabeçalhos MPLS) podem ser inseridos dentro do pacote. Um roteador capaz de entender um pacote MPLS é chamado de *Label Switching Router* (LSR). O caminho que o pacote percorre é chamado de *Label Switching Path* (LSP). E por fim, o protocolo de comunicação entre os elementos de rede ou roteadores é chamado de *Label Distribution Protocol* (LDP). O roteador MPLS usa um label; um índice da tabela de roteamento que especifica o próximo hop e o novo label, diferentemente dos roteadores que se baseiam nas informações contidas no cabeçalho IP. O label antigo é colocado em um novo e o pacote é direcionado para o próximo hop. Este processo se repete em cada hop no caminho até chegar ao roteador final que irá colocar o pacote dentro da rede (SILVA, 2002).

O MPLS permite a criação de VPN's porque garante um isolamento completo do tráfego com a criação de tabelas de rótulos usadas para roteamento exclusivas de

cada circuito virtual. Por outro lado, O MPLS não pode ser visto como tecnologia de implementação de tunelamento, pois embora haja isolamento de pacotes, estes trafegam por uma rede pública por rotas que serão selecionadas de acordo com os algoritmos utilizados (SILVA, 2002).

3.3.7 SSH

O SSH (*Secure Shell*) foi desenvolvido pela SSH Communications Security Ltda. com o intuito de substituir os comandos de acesso remoto originais dos sistemas Unix BSD por versões seguras prevenindo a captura de informações como senhas de usuários. Atualmente duas especificações do SSH são utilizadas: o SSH1 e o SSH2. Ambas as versões suportam o uso do SSL (*Secure Sockets Layer*) que é uma tecnologia de segurança comumente usada para codificar dados trafegados em rede. O SSH 2 também tem suporte ao TLS (*Transport Layer Security*). O estabelecimento de conexões seguras é precedido, da mesma forma que no IPsec e no SSL, pela negociação de algoritmos criptográficos (SENA, 2002).

Aproveitando os esforços empregados no desenvolvimento de soluções para a distribuição e verificação de chaves públicas, o SSH 2 suporta a consulta a autoridades certificadoras para obtenção e validação de chaves públicas. Além disso, o mecanismo original, desenvolvido no SSH 1, onde o próprio servidor envia sua chave pública caso o cliente ainda não a tenha, também é suportado pelo SSH 2. É importante notar que este mecanismo expõe o cliente a servidores forjados por atacantes no primeiro contato entre os dois hosts onde certamente as chaves públicas de ambos serão conhecidas. Por outro lado, caso a chave pública do servidor seja recebida com sucesso, conexões futuras não estarão sujeitas a este tipo de ataque, o que representa um nível de segurança maior do que aquele provido pelos protocolos Telnet, onde cada estabelecimento de conexão é suscetível a ataques como o anterior. Uma das maneiras possíveis de evitar este problema no SSH é obter, de maneira segura, as chaves públicas de servidores onde serão

estabelecidas conexões SSH e mantê-las em base de dados locais, evitando que os servidores a enviem de maneira insegura e não confiável durante o primeiro contato (SENA, 2002).

3.3.8 IPSec

O IPSec é, fundamentalmente, baseado no uso de dois protocolos de segurança: o AH (*Authentication Header*) e o ESP (*Encapsulating Security Payload*), implementados como cabeçalhos adicionais inseridos em datagramas após o cabeçalho IP. Seu objetivo é evitar que o conteúdo de pacotes seja lido, alterado, modificado, ou ainda, reenviado (SENA, 2002).

O IPSec fornece alguns serviços de segurança, como integridade das informações, autenticação da origem dos dados, confidencialidade e o controle de acesso. A principal diferença entre os serviços de autenticação e integridade providos pelo AH e pelo ESP estão na abrangência da proteção. O AH protege todos os campos de um pacote, excetuando-se aqueles cujos valores são alterados em trânsito, como o Hop Limit, manipulado pelos roteadores que processam o pacote. Quando oferecidos pelo ESP, estes serviços abrangem somente o próprio cabeçalho do ESP e a porção de dados do pacote (SENA, 2002).

3.3.8.1 Authentication header

O protocolo IP em sua forma original, sem o uso do IPSec, não contém qualquer proteção contra o envio de pacotes capturados em trânsito. Estas fragilidades, combinadas com outros fatores, permitiram o desenvolvimento de ataques como o IP spoofing, DNS spoofing, rejeição de pacotes, entre outros (SENA, 2002).

O mecanismo de checksum, existente no IPV4, foi projetado apenas para detectar problemas decorrentes da manipulação incorreta dos pacotes por parte de periféricos, sendo incapaz de detectar a manipulação maliciosa de pacotes capturados e posteriormente reenviados. Desta forma, necessidades fundamentais para definição de mecanismos capazes de prover segurança ao protocolo IP são a autenticação e a integridade dos dados, providas no IPSec pelo AH. A autenticação garante que um pacote foi realmente enviado pelo endereço indicado. A integridade garante que as informações recebidas não foram alteradas durante seu trajeto entre a origem e o destino (SENA, 2002).

3.3.8.2 Encapsulating security payload

Além da ausência de serviços de autenticação e integridade, o protocolo IP também não possui qualquer mecanismo capaz de prover criptografia ao conteúdo dos seus pacotes. Desta forma, aplicações antigas como Telnet e FTP, que não contêm qualquer preocupação com segurança, permitem que suas informações, incluindo login e senha, sejam facilmente obtidas através da captura de pacotes, representando um risco para toda a rede da qual fazem parte (SENA, 2002).

Para impedir a obtenção de informações sigilosas, foram desenvolvidos protocolos como o SSH e o SSL, que passaram a proteger suas informações através do uso de algoritmos criptográficos, impedindo que a obtenção de seus pacotes pudesse comprometer os dados transmitidos. Porém, estas soluções foram desenvolvidas para fins específicos e ainda deixavam expostas informações importantes, como os dados do protocolo de transporte. Sendo assim, para prover um mecanismo genérico capaz de garantir o sigilo dos dados transmitidos, o IPSec provê o ESP (SENA, 2002).

3.3.8.3 Algoritmos criptográficos

Apesar dos serviços do protocolo AH e ESP serem independentes de quaisquer algoritmos criptográficos em particular, sob a justificativa de manter um nível mínimo de compatibilidade entre as diversas implementações, um conjunto básico de algoritmos é obrigatório.

- HMAC-MD5-96 e HMAC-SHA-1-96: algoritmos de autenticação e integridade utilizados pelo AH e, opcionalmente pelo ESP;
- DES-CBC: algoritmo de criptografia utilizado pelo ESP;
- Algoritmos nulos de autenticação e criptografia utilizados pelo ESP.

A presença dos algoritmos de autenticação e criptografia associados ao ESP se dá pelo fato dos serviços de confidencialidade e autenticação/integridades serem opcionais.

Porém estes dois algoritmos não podem ser utilizados ao mesmo tempo em um dado pacote. Em outras palavras, o protocolo ESP deve prover pelo menos um dos seus serviços, quando utilizado na proteção de pacotes. Os algoritmos de autenticação e integridade obrigatórios HMAC-MD5-96 e HMAC-SHA-1-96 geram MAC's de 128 e 160 bits respectivamente (SENA, 2002).

4 INSTAÇÃO DA VPN NO SERVIDOR LINUX

4.1 INTRODUÇÃO

Com o crescimento das redes de computadores de empresas e universidades tornou-se necessário desenvolver novas soluções que propiciem uma boa comunicação entre pontos distantes destas redes, para fornecer compartilhamento de arquivos e informações e aproximar as pessoas. Existem algumas soluções que podem suprir estas necessidades, porém a grande maioria tem custo elevado e implantação complexa.

A VPN entra como uma solução viável, com resultados tão bons quanto os de outras soluções, com custo significativamente menor que o custo das demais. Além disso, a VPN pode ser implementada e mantida com mais facilidade.

A solução proposta neste trabalho foi implementada na Universidade Federal de Itajubá - UNIFEI. A UNIFEI está implantando um novo Campus na cidade de Itabira, que se localiza a aproximadamente 600 km da cidade de Itajubá, local do Campus principal. Para prover acesso a recursos do Campus Itajubá a professores, alunos e técnicos do Campus de Itabira foi utilizada uma VPN como a descrita neste trabalho, salvo algumas particularidades.

Para realizar a implementação da VPN devem-se avaliar as necessidades da organização e os investimentos disponibilizados. Iremos utilizar, para nosso estudo, um ambiente de software livre para instalação e configuração da VPN. Devido à sua reconhecida estabilidade, ser usado em servidores em todo mundo e servir de modelo para o desenvolvimento de outras distribuições linux, além de vasto suporte e documentação, utilizaremos o sistema operacional Debian Linux em nosso servidor da VPN. Neste servidor será instalado o OpenVPN, que é um software livre, também com vasto suporte e documentação, destinado à criação da VPN.

4.2 INSTALAÇÃO DA VPN

O OpenVPN é baseado no protocolo TLS/SSL, que oferecem um bom nível de segurança, e é relativamente simples de se configurar, além de ser bastante flexível. Ele, apesar de ser instalado em um servidor com sistema operacional Linux, permite conexões de clientes Linux e Windows.

Em relação à segurança, o OpenVPN pode ser configurado para utilizar chaves estáticas, que oferecem um nível mediano de segurança, em troca de uma configuração mais simples, ou para utilizar certificados X509, onde a segurança é muito maior (superior até às soluções comerciais). Isso permite uma relação entre a praticidade e a segurança de acordo com a situação (MORIMOTO, 2008).

Não será detalhada a instalação do sistema operacional Debian Linux, pois, além de não ser o foco deste trabalho, há grande documentação sobre o assunto. Abordaremos primeiro a instalação do OpenVPN no servidor e, em seguida, sua instalação em clientes que utilizam sistema operacional Windows, a fim de verificar sua independência quanto à plataforma do cliente.

Para instalação do servidor Debian Linux deve-se utilizar o seguinte comando como usuário administrador (ou root) do sistema:

- `# apt-get install openvpn`

No final da instalação, ele exibirá uma mensagem perguntando se o OpenVPN deve ser desativado antes de ser atualizado (*“Would you like to stop openvpn before it gets upgraded?”*). Deve-se responder sim. (MORIMOTO, 2008).

Depois de instalar o pacote, o próximo passo é carregar o módulo “tun” do Kernel do Debian Linux. Este módulo é utilizado pelo OpenVPN para criar as interfaces virtuais

de conexão. Cada VPN criada se comporta como uma nova interface de rede, conectada à rede de destino.

Para carregar o módulo o comando é o seguinte:

- `# modprobe tun`

Para que o módulo seja carregado automaticamente em alguma reinicialização do servidor deve-se utilizar o seguinte comando:

- `# echo tun >> /etc/modules`

4.3 CONFIGURAÇÕES DE SEGURANÇA

Para atingir um bom nível de flexibilidade e segurança a VPN será configurada para utilizar certificados X509. Este método é chamado de PKI (*public Key Infrastructure*) e permite criar VPN's complexas envolvendo vários servidores e vários clientes, além de oferecer maior segurança.

O Open VPN fornece scripts de configuração para gerar os certificados que serão utilizados pelo servidor e pelos clientes. É gerado um certificado mestre, armazenado no próprio servidor, que é usado para gerar os certificados utilizados pelos clientes. Isso permite a identificação dos agentes envolvidos na comunicação (usuários clientes e o servidor) fortalecendo a segurança e evitando técnicas de ataque (MORIMOTO, 2008).

O “*easy-rsa*” é um dos scripts incluídos no pacote do OpenVPN. Para utilizá-lo no Debian Linux é necessário copiar o conteúdo da pasta “/usr/share/doc/openvpn/examples/easy-rsa” para a pasta “/etc/openvpn/easy-rsa”. Feito isso é necessário editar o arquivo vars com os seguintes comandos:

- `# cd /etc/openvpn/easy-rsa`

- # nano vars

Este arquivo, conforme Quadro 1 abaixo, possui uma série de parâmetros usados para gerar as chaves, por exemplo:

```
export KEY_COUNTRY=BR
export KEY_PROVINCE=MG
export KEY_CITY="Itajubá"
export KEY_ORG="UNIFEI"
export KEY_EMAIL="administrador@unifei.edu.br"
```

Quadro 1 - Script de configuração do OpenVPN
Fonte: Elaboração própria (2010)

Após editar o arquivo é necessário utilizar o comando *“source”* para carregar suas configurações. Em seguida, é preciso executar os scripts *“clean-all”*, que elimina qualquer configuração anterior, e *“build-ca”*, que gera o certificado raiz, usando SSL.

- # source vars
- # ./clean-all
- #./build-ca

Isso criará a pasta *“/etc/openvpn/easy-rsa/keys”*, contendo os arquivos *ca.crt*, *ca.key*, *index.txt* e *serial*. O arquivo *ca.crt* contém o certificado raiz, que é utilizado para gerar os certificados dos clientes. Para gerar o certificado do servidor é utilizado o script *“build-key-server”*, especificando o nome do arquivo que será gerado. Para gerar o certificado dos clientes é utilizado o script *“build-key-pass”*, especificando o nome do cliente e a respectiva senha para acesso.

- # ./build-key-server servidor
- # ./build-key-pass cliente1
- # ./build-key-pass cliente2

Para finalizar a configuração dos certificados é necessário instalar as chaves, tanto no servidor quanto nos clientes. No servidor é necessário criar a pasta *“/etc/openvpn/easy-rsa/keys”* e copiar para ela os arquivos de configuração gerados anteriormente.

- # cd /etc/openvpn/

- # mkdir keys
- # cp -a /etc/openvpn/easy-rsa/keys/ca.crt /etc/openvpn/keys/
- # cp -a /etc/openvpn/easy-rsa/keys/servidor.crt /etc/openvpn/keys/
- # cp -a /etc/openvpn/easy-rsa/keys/servidor.key /etc/openvpn/keys/

4.4 CONFIGURAÇÕES DE ACESSO

Com os certificados já criados deve-se realizar as configurações de acesso no servidor e gerar os arquivos de configuração que serão utilizados pelos clientes para acesso à VPN. As configurações de acesso no servidor são informadas no arquivo “/etc/openvpn/server.conf”. Segue um exemplo, no Quadro 2, de como as opções devem ser configuradas:

```
proto tcp
port 2222
dev tun
server "10.100.10.0 255.255.255.0"
push "route 192.168.0.0 255.255.255.0"
persist-key
persist-tun
max-clients 10
shaper 256000
tls-server
ca /etc/openvpn/keys/ca.crt
cert ca /etc/openvpn/keys/servidor.crt
key /etc/openvpn/keys/servidor.key
```

Quadro 2 - Arquivo de configuração do servidor
Fonte: Elaboração própria (2010)

Neste exemplo o servidor usará o sistema “*tun*”, cujo módulo foi devidamente configurado, além do protocolo TCP e a porta 2222. Os endereços IP disponíveis

para os clientes serão os da rede 10.100.10, máscara de rede 255.255.255.0. A opção `push` permite que o cliente acesse os demais hosts da rede local do servidor, supondo que esta rede seja a 192.168.0.0 máscara de rede 255.255.255.0 (esta opção só deve ser configurada caso necessário). Temos ainda as opções “*max-clients*”, que define o número máximo de usuários permitidos, e “*shaper*”, que define a largura de banda disponível para o cliente. Por fim são indicados os arquivos de certificados gerados anteriormente.

Para os clientes também há um arquivo semelhante de configuração que possui a linha “*remote*”, que indica o endereço IP do servidor e a porta de conexão. Para configuração do cliente no sistema operacional Windows, este arquivo, representado no Quadro 3, tem o nome de “*client.ovpn*”.

```
remote 201.7.178.45 2222
proto tcp
port 2222
dev tun
client
pull
persist-key
persist-tun
tls-client
ca /etc/openvpn/keys/ca.crt
cert ca /etc/openvpn/keys/servidor.crt
key /etc/openvpn/keys/servidor.key
```

Quadro 3 - Arquivo de configuração do cliente
Fonte: Elaboração própria (2010)

Há casos em que é necessário revogar os certificados para não permitir que o usuário continue acessando a VPN. Nesses casos deve-se revogar o certificado do respectivo usuário. Este processo consiste em criar um arquivo que contém a lista dos certificados revogados e configurar o servidor para utilizá-la. Para isso são necessários os seguintes comandos:

- `# cd /etc/openvpn/easy-rsa`
- `# source vars`

- # ./revoke-full cliente1

Será gerado o arquivo “*crl.pem*” que deve ser copiado para a pasta “/etc/openvpn/keys”, a mesma dos arquivos de certificados. Para que esse arquivo seja verificado é necessário adicionar ao arquivo “/etc/openvpn/server.conf” a seguinte linha: `crl-verify /etc/openvpn/keys/crl.pem`.

4.5 CONFIGURAÇÃO DO CLIENTE

Para realizar a conexão com a VPN, o cliente necessita de um aplicativo específico. Além do OpenVPN Server, existe também o OpenVPN Client, que também é um aplicativo gratuito e pode ser obtido no site <http://openvpn.net/index.php/open-source/downloads.html>. Após sua instalação no Microsoft Windows XP, deve-se copiar os arquivos de configuração para a pasta “C:\Arquivos de programas\OpenVPN\config”, conforme a Figura 14:

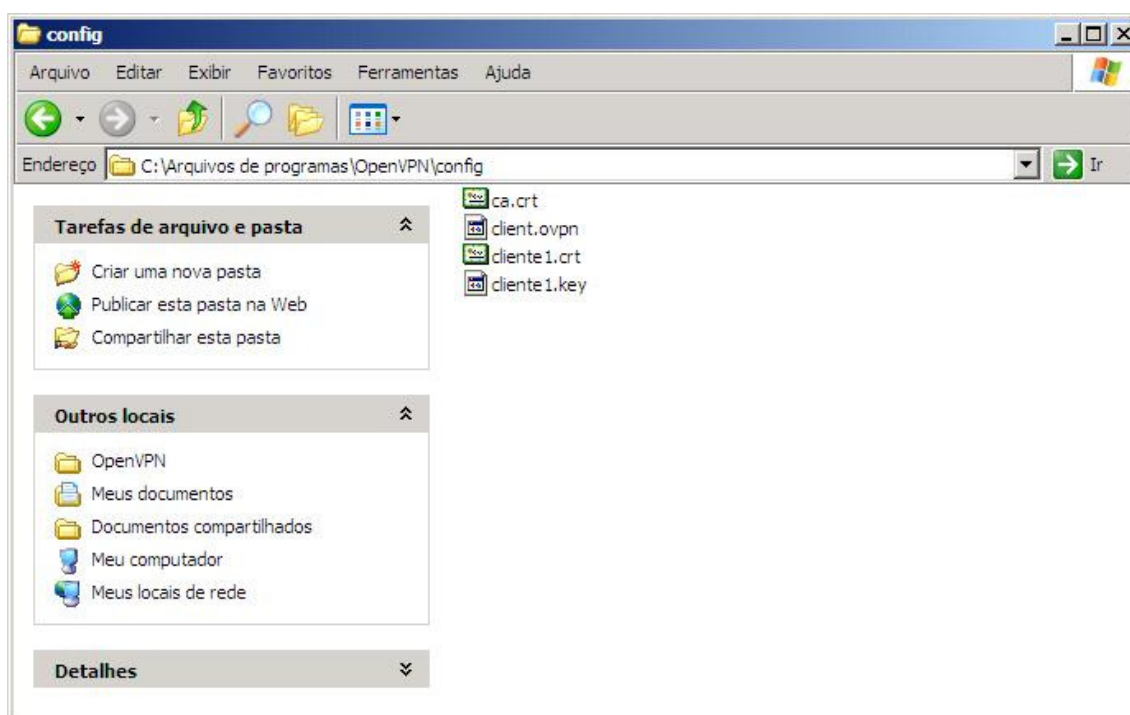


Figura 14 - Configuração do cliente OpenVPN
Fonte: Elaboração própria (2010)

Ao abrir o aplicativo OpenVPN Client será realizada a conexão conforme as configurações do arquivo “*client.ovpn*” e os respectivos certificados .

CONCLUSÃO

Este trabalho se propôs a demonstrar como implementar uma VPN em um ambiente de software livre, utilizando o OpenVPN, detalhando aspectos de suas configurações, além de analisar sua funcionalidade e segurança. Para isso foram estudadas diversas características relacionadas às redes de computadores como topologias, protocolos e segurança.

Como citado anteriormente, a implementação proposta neste trabalho é utilizada atualmente na Universidade Federal de Itajubá, para prover recursos aos técnicos, professores e alunos. Exemplos destes recursos utilizados são o acesso ao portal de periódicos da CAPES e o acesso ao sistema acadêmico utilizado na instituição.

Com este trabalho podemos concluir que uma solução VPN é uma forma segura e econômica de se conectar redes através de um meio público, como a Internet. Optou-se por utilizar o OpenVPN por ser um software livre, possui fácil implementação e utiliza túneis SSL, que são amplamente utilizados para transações seguras pela Internet e está em constante atualização.

O sistema operacional Debian Linux mostrou-se eficaz, sendo uma ótima solução para as organizações que necessitam de servidores para os mais variados serviços como compartilhamento de arquivos, firewall e a própria VPN.

REFERÊNCIAS

- CIOTTI, Alex. **Projeto de infra-estrutura de um laboratório de redes de computadores em uma instituição de ensino superior**. Universidade Luterana do Brasil. Canoas: 2003. Disponível em: <www.garcia.pro.br/orientacoes/TCC%20Alex%20Ciotti.pdf>. Acesso em: 12 jun. 2010.
- FOROUZAN, Behrouz A.. **Comunicação de dados e redes de computadores**. 3 ed. reimpr. Porto Alegre: Bookman, 2008.
- KIRCH, Olaf. **Guia do administrador de redes Linux**. Curitiba: Conectiva, 1999.
- MENDES, Douglas Rocha. **Redes de computadores: teoria e prática**. São Paulo: Novatec, 2007.
- MIRANDA, Anibal D. A.. **Introdução às redes de computadores**. Vila Velha: ESAB, 2008
- MORIMOTO, Carlos Eduardo. **Servidores Linux: guia prático**. Porto Alegre: Sul Editores, 2008.
- ODOM, Wendell. **CISCO CCNA: guia de certificação do exame #640-607**. Rio de Janeiro: Alta Books, 2003.
- SENA, Jansen Carlo. **Um modelo para proteção do tráfego de serviços baseados em níveis de segurança**. 2002. Dissertação (Mestrado em Ciencia da Computação). Instituto de Computação, Universidade Estadual de Campinas, Campinas, 2002. Disponível em: <<http://libdigi.unicamp.br/document/?code=vtls000249045> >. Acesso em: 10 jun. 2010.
- SILVA, Lino Sarlo da. **VIRTUAL PRIVATE NETWORK: VPN**. São Paulo: Novatec, 2002.
- SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sergio. **Redes de computadores: das Lans, Mans e Wans às redes ATM**. Rio de Janeiro: Campus, 1995.
- STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. São Paulo : Pearson Prentice Hall , 2008.
- TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Campus, 2003.

TORRES, Gabriel. **Redes de Computadores**: curso completo. Rio de Janeiro: AXCEL Books do Brasil, 2001.

VASQUES, Alan Temer; SHUBER, Rafael Priante. **Implementação de uma VPN em Linux Utilizando o Protocolo IPSec**. Monografia (Bacharelado em Ciência da Computação). Centro Universitário do Estado do Pará, Belém, 2002. Disponível em: <<http://www.abusar.org.br/manuais/VPN-alan-rafael.pdf>>. Acesso em: 19 jun. 2010.