

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

Análise e Comparativo de Soluções, para o tráfego de informações utilizando Redes Privadas Virtuais (VPN).

Análise e Comparativo de Protocolos para o tráfego de informações utilizando Redes Privadas Virtuais (VPN)

Trabalho de Conclusão de Curso apresentado ao curso Bacharelado em Sistemas de Informação da Faculdade Natalense para o desenvolvimento do Rio Grande do Norte, como requisito básico para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador

Prof. Ricardo Kleber M. Galvão

José Gilberto Avelino Rodríguez

**NATAL / RN
DEZEMBRO / 2005**

JOSÉ GILBERTO AVELINO RODRÍGUEZ

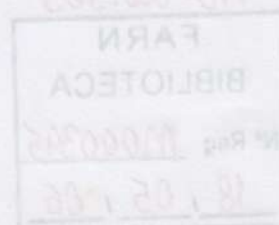
Análise e Comparativo de Soluções, para o tráfego de informações utilizando Redes Privadas Virtuais (VPN).

Monografia apresentada ao curso Bacharelado em Sistemas de Informação da Faculdade Natalense para o desenvolvimento do Rio Grande do Norte, como requisito básico para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador:

Prof. Ricardo Kleber M. Galvão

**NATAL / RN
2005**



JOSE GILBERTO VALLINO RODRIGUES

Análise e Comparação de Soluções para o Tratamento de Informações Utilizando Redes
Tributárias Virtuais (TVN)

Trabalho apresentado ao curso Bacharelado em
Sistemas de Informação da Faculdade Nacional
para o desenvolvimento do Rio Grande do Norte,
nos dias 18/05/06 para obtenção do grau de
Bacharel em Sistemas de Informação.

Orientador

Prof. Ricardo Krieger M. Galvão

RB-26.365

FARN
BIBLIOTECA
Nº Reg <u>M000345</u>
<u>18 / 05 / 06</u>

M

004.7

R 658a

2005

NATAL RN
2005

Rodríguez, José Gilberto Avelino

Análise e Comparativo de Protocolos para o tráfego
de informações utilizando Redes Privadas Virtuais / José
Gilberto Avelino Rodríguez _____ Natal: FARN, 2005.

69p.

Orientador: Ricardo Kleber

Monografia (Graduação em sistemas de informação) –
Faculdade Natalense Para o Desenvolvimento do Rio Grande
do Norte.

1.

RN/FARN/BC

CDU

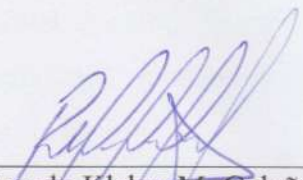


**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

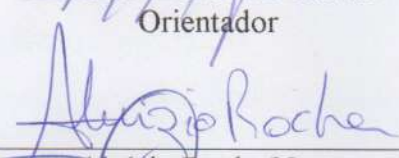
Análise e Comparativo de Soluções, para o trafego de informações utilizando Redes Privadas Virtuais (VPN).

JOSÉ GILBERTO AVELINO RODRÍGUEZ

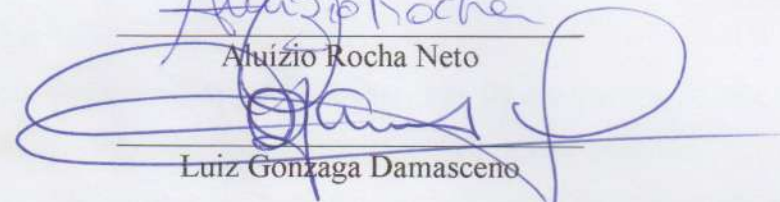
Monografia apresentada e aprovada em 19 de 12 de 2006 pela banca examinadora composta pelos seguintes membros.



Ricardo Kleber M. Galvão
Orientador



Aluizio Rocha Neto



Luiz Gonzaga Damasceno

DEDICO a realização deste trabalho
aos meus pais, Thelma Maria Bezerra
Avelino Rodrigues e Plácido Rodrigues
Rodrigues. Assim como minha grande
irmã Andreia Maria, e minha amada
Gerclaus Peixoto, aos familiares que
me apoiaram e aos verdadeiros amigos
que sempre acreditaram no meu
potencial e que sempre me apoiaram
durante a minha trajetória de vida.

Muito Obrigado a todos!

Natal/RN, ____ de ____ de ____.

DEDICATÓRIA

AGRADEÇO primeiramente a DEUS, criador desse universo misterioso, infinitamente perfeito e maravilhoso, por ter me mantido saudável e em paz durante a elaboração deste trabalho, aos meus pais Plácido Rodríguez Rodríguez e Themis Maria Bezerra Avelino por terem investido na minha educação, não apenas financeiramente, mas acima de tudo um investimento de amor, carinho, compreensão e amizade, que consequentemente refletiu para uma ótima formação acadêmica e profissional, nos dias difíceis não sendo a oportunidade de desfrutar desses momentos tão felizes e importantes.

A irmã da minha vida, Andreza Maria Bezerra Avelino que sempre esteve comigo, dando apoio e atenção em todos os aspectos.

Ao minhas tias Violeta Cabral Avelino, Gracilde Cabral Avelino e Maria Cabral Avelino, por sempre me ajudarem nos momentos mais difíceis, que que também compartilharam amor nos momentos de alegria.

A Minha amada Gerciana Peixoto de Melo que também sempre esteve comigo nos momentos mais difíceis me ajudando a superá-los.

Aos meus primos Fernando, Augusto, André e a todos os familiares que contribuíram para esta minha vitória.

Ao meu orientador o prof. Ricardo Kleber, por ter compartilhado seu conhecimento, para que este trabalho fosse formulado da maneira mais coerente possível.

A FARN, por ser atualmente a melhor a instituição de ensino do Nordeste e ter contribuído diretamente com a expansão do meu conhecimento.

E a todas as pessoas que de uma forma ou de outra contribuíram para esta minha vitória.

DEDICO a realização deste trabalho aos meus pais, Themis Maria Bezerra Avelino Rodríguez e Plácido Rodríguez Rodríguez. Assim como minha grande irmã Andreza Maria, e minha amada Gerciana Peixoto, aos familiares que me apoiaram e aos verdadeiros amigos que sempre acreditaram no meu potencial e que sempre me apoiaram durante a minha trajetória de vida.

Muito Obrigado a todos!

AGRADECIMENTOS

SUMÁRIO

AGRADEÇO primeiramente a DEUS, criador deste universo misterioso, infinitamente perfeito e maravilhoso, por ter me mantido saudável e em paz durante a elaboração deste trabalho, aos meus pais Plácido Rodríguez Rodríguez e Themis Maria Bezerra Avelino por terem investido na minha educação, não apenas financeiramente, mas acima de tudo um investimento de amor, carinho, compreensão e amizade, que conseqüentemente refletiu para uma ótima formação acadêmica e profissional, sem eles dificilmente estaria tendo a oportunidade de desfrutar deste momento tão solene e importante.

A irmã da minha vida, Andrezza Maria Bezerra Avelino que sempre esteve comigo, dando apoio e atenção em todos os aspectos.

As minhas tias Violeta Cabral Avelino, Gracilde Cabral Avelino e Maria Cabral Avelino, por sempre me ajudarem nos momentos mais difíceis, mas que também compartilharam amor nos momentos de alegria.

A Minha amada Gerciana Peixoto de Melo que também sempre esteve comigo nos momentos mais difíceis me ajudando a superá-los.

Aos meus primos Fernando, Augusto, André e a todos os familiares que contribuíram para esta minha vitória.

Ao meu orientador o prof. Ricardo Kleber, por ter compartilhado seu conhecimento, para que este trabalho fosse formulado da maneira mais coerente possível.

A FARN, por ser atualmente a melhor a instituição de ensino do Nordeste e ter contribuído diretamente com a expansão do meu conhecimento acadêmico.

E a todas as pessoas que de uma forma ou de outra contribuíram para essa conclusão.

3. VIR	
3.1 CONCEITO DE VPN	26
3.2 VPN NO MERCADO BRASILEIRO	28
3.3 CARACTERÍSTICAS BÁSICAS DE UMA VPN	30
3.4 PRINCIPAIS APLICAÇÕES PARA VPN	40
3.5 ELEMENTOS DE UMA VPN	41
3.6 PROTOCOLOS DE TUNELAMENTO	44
3.6.1 PPTP	45
3.6.1.1 Conceito	45
3.6.1.2 Aplicações PPTP	46
3.6.1.3 Mecanismos de Segurança do PPTP	47
3.6.1.4 Formato dos Dados	47
3.6.1.2P	48
3.6.2 L2TP	48
3.6.2.1 Conceito	48

SUMÁRIO

1. INTRODUÇÃO	14
2. REFERENCIAL TEÓRICO	16
2.1 REDES DE COMPUTADORES.....	16
2.1.1 Principais Tipos de Redes	17
2.1.2 Classificações	19
2.1.2.1 LAN – <i>Local Area Network</i>	19
2.1.2.2 WAN – <i>Wide Area Network</i>	20
2.1.3 Arquitetura de Modelo RM-OSI	21
2.1.4 Propriedades de Rede	22
2.1.4.1 Redes Privadas	22
2.1.4.2 Redes Públicas	22
2.1.5 Histórico da Internet	23
2.1.6 Protocolos	24
2.1.6.1 Protocolos TCP/IP	24
2.2 SEGURANÇA DA INFORMAÇÃO.....	27
2.2.1 Métodos de Ataques	28
2.2.1.1 Interrupção	28
2.2.1.2 Interceptação	28
2.2.1.3 Modificação	29
2.2.1.4 Fabricação	29
2.2.2 Métodos de Defesas	30
2.2.2.1 <i>Firewall</i>	30
2.2.2.2 <i>Firewall</i> e VPN	31
2.3. CRIPTOGRAFIA.....	33
2.3.1 Criptografia Simétrica	33
2.3.2 Criptografia Assimétrica	34
2.3.3 Função Hash	35
2.3.4 Assinatura Digital	36
2.3.5 Certificado Digital	37
3. VIRTUAL PRIVATE NETWORK (VPN)	38
3.1 CONCEITO DE VPN	38
3.2 VPN NO MERCADO BRASILEIRO	38
3.3 CARACTERÍSTICAS BÁSICAS DE UMA VPN	39
3.4 PRINCIPAIS APLICAÇÕES PARA VPN	40
3.5 ELEMENTOS DE UMA VPN	41
3.6 PROTOCOLOS DE TUNELAMENTO	44
3.6.1 PPTP	45
3.6.1.1 Conexão	45
3.6.1.2 Arquitetura PPTP	46
3.6.1.3 Mecanismos de Segurança do PPTP	47
3.6.1.4 Formato dos Datagramas	47
3.6.2 L2F	48
3.6.2.1 Conexão	48

3.6.2.2 Formato do Datagrama	49
3.6.3 L2TP	49
3.6.3.1 Conexão	50
3.6.3.2 Autenticação	50
3.6.3.3 Formato do Datagrama	50
3.6.4 IPSEC	52
3.6.4.1 Modos de Operação	52
3.6.4.2 Elementos de Segurança do IPSEC	54
3.6.5 SSL/TSL	56

4. ANÁLISE DE RESULTADOS 57

4.1 PPTP: POINT-TO-POINT TUNNELING PROTOCOL..... 57

4.2 L2F: LAYER 2 FORWARDING 57

4.3 L2TP: LAYER 2 TRANSPORT PROTOCOL..... 58

4.4 IPSEC: IP SECURITY PROTOCOL..... 58

4.5 OPENVPN: SSL / TSL..... 59

4.5.1 OPENVPN (SSL/TSL) X IPSEC 59

5. CONCLUSÃO 60

6. REFERÊNCIAS BIBLIOGRÁFICAS..... 61

7. ANEXOS 63

7.1 IMPLEMENTAÇÃO DE UMA VPN EM LINUX USANDO OPENVPN 63

7.1.1 Instalação 63

NetBUI – NetBIOS Extended User Interface
 NIST – National Institute of Standards and Technologies
 NSF – National Science Foundation
 PFS – Perfect Forward Secrecy
 RNP – Rede Nacional de Pesquisa
 RPM – Red Hat Packet Manager
 RSA – Rivest Shamir Adleman
 S/WAN – Secure Wide Area Network
 SA – Security Association
 SAD – Security Association Database
 SHA-1 – Secure Hash Algorithm 1
 SHA-2 – Secure Hash Algorithm 2
 SPD – Security Policy Database
 SPI – Security Parameters Index
 SRI – Stanford Research Institute
 UCLA – University of California Los Angeles
 UCSB – University of California Santa Barbara
 UDP – User Datagram Protocol
 WAN – Wide Area Network

LISTA DE SIGLAS

3DES – Triple Data Encryption Standard	16
AC – Autoridade Certificadora	17
AES – Advanced Encryption Standard	18
AH – Authentication Header	19
ARPA – Advanced Research Project Agency	20
CAST – Carlisle Adams and Stafford Tavares	24
DES – Data Encryption Standard	25
DoS – Denial of Service	28
ESP – Encapsulating Security Payload	28
GRE – Generic Routing Encapsulation	29
GRUB – Grand Unified Bootloader	29
ICMP – Internet Control Message Protocol	29
IETF – Internet Engineering Task Force	30
IKE – Internet Key Exchange Protocol	32
IPX / SPX – Interwork Packet Exchange / Sequenced Packet Exchange	33
ISAKMP – Internet Security Association and Key Management Protocol	37
ITU-T – International Telecommunication Union-Telecommunication Standardization sector	38
KLIPS – Kernel IPSEC Support	38
LAN – Local Area Network	38
LILO – Linux Loader	38
MAN – Metropolitan Area Network	40
MD-5 – Message Digest 5	41
MIT – Massachusetts Institute of Technology	42
MPPE – Microsoft Point-to-Point Encryption	47
MS-CHAP – Microsoft-Challenge Handshake Authentication Protocol	48
NAT – Network Address Translation	49
NetBEUI – NetBIOS Extended User Interface	51
NIST – National Institute of Standards and Technologies	52
NSF – National Science Foundation	52
PFS – Perfect Forward Secrecy	53
RNP – Rede Nacional de Pesquisa	53
RPM – Red Hat Packet Manager	53
RSA – Rivest Shamir Adleman	64
S/WAN – Secure Wide Area Network	65
SA – Security Association	65
SAD – Security Association Database	66
SHA-1 – Secure Hash Algorithm 1	67
SHA-2 – Secure Hash Algorithm 2	68
SPD – Security Policy Database	
SPI – Security Parameters Index	
SRI – Stanford Research Institute	
UCLA – University of California Los Angeles	
UCSB – University of California Santa Barbara	
UDP – User Datagram Protocol	
WAN – Wide Area Network	

LISTA DE TABELAS

Tabela 1 Arquitetura de Modelo RM-OSI	21
Tabela 2 Portas e Serviços.....	26

RESUMO

A VPN – Rede Privada Virtual – é uma das soluções mais viáveis presentes no atual mercado da informática. Neste trabalho, serão mostrados os principais itens desta tecnologia, fazendo uma análise e um comparativo em cima dos principais e mais usados protocolos de tunelamento, sendo implementada no sistema operacional Linux, utilizando o software OPENVPN, juntamente com o protocolo SSL/TSL a fim de posicioná-la como uma alternativa segura e economicamente atrativa para organizações privadas e estatais.

ABSTRACT

1. INTRODUÇÃO

The VPN – Virtual Private Network – is one of the most viable solutions found in the computer market nowadays. At this work, the main features of this technology will be shown, implementing it in the Linux operational system, using the software OPENVPN and protocol SSL/TSL, in order to place it as a safe and economically attractive alternative for private and governmental organizations.

Diversos tipos de métodos e aplicativos, capazes de enviar dados, através de computadores interligados, transmitindo cada vez mais praticidade e rapidez, porém sempre se deparam com o problema da segurança durante a transmissão das informações, o que pode permitir que pessoas não autorizadas tenham acesso aos dados transferidos.

Os dados transmitidos através da internet seguem por um caminho totalmente inseguro e, portanto, devem ser protegidos de forma a não permitir sua modificação ou interceptação, desse modo serão mostrados os serviços de conexão entre corporações (exemplos) através da internet de um modo seguro, o que possibilita conexões criptografadas que podem ser úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

Neste cenário, as Redes Privadas Virtuais (Virtual Private Network - VPN) representam uma alternativa eficiente e segura para essa comunicação, pois possibilitam a economia dos custos de manutenção das redes corporativas ao permitir que as conexões dedicadas existentes de custo mais elevado, sejam substituídas por conexões públicas mais seguras a partir do momento que estas utilizam criptografia e métodos de autenticação de máquina e usuário para a transmissão de dados por meio de um túnel virtual, proporcionando assim um parâmetro de custo e benefício bastante satisfatório.

Para o funcionamento das redes privadas virtuais (VPNs) é necessária a presença de um protocolo de tunelamento que seja responsável pela forma com que os dados ou informações irão trafegar nas redes computacionais através da Internet. Tendo em vista que existem diversos protocolos para desempenhar essa função, a presente pesquisa tem como objetivo geral fazer um comparativo entre as principais tecnologias de protocolos de tunelamento, dando ênfase aos aspectos relacionados com a segurança do tráfego de dados, expondo as vantagens e desvantagens de cada protocolo.

Apesar de não ser o foco principal do trabalho, esta monografia relata alguns conceitos sobre redes de computadores, algumas vantagens das VPNs, mostra em quais tipos de aplicações elas são usadas e suas funções básicas, o funcionamento dos túneis para o fluxo de

1. INTRODUÇÃO

Atualmente, com os grandes avanços tecnológicos, a presença de computadores e o surgimento da Internet, o fluxo das informações e o conhecimento em geral, ficaram ainda mais fáceis de serem disponibilizados e conseqüentemente absorvidos pela humanidade. Durante algum tempo muitos especialistas ou profissionais da informática, vêm criando, desenvolvendo ou aperfeiçoando os mais diversos tipos de métodos e aplicativos, capazes de enviar dados, através de computadores interligados, transmitindo cada vez mais praticidade e rapidez, porém sempre se deparam com o problema da segurança durante a transmissão das informações, o que pode permitir que pessoas não autorizadas tenham acessos aos dados transferidos.

Os dados transmitidos através da internet seguem por um caminho totalmente inseguro e, portanto, devem ser protegidos de forma a não permitir sua modificação ou interceptação, desse modo serão mostrados os serviços de conexão entre corporações (*extranets*) através da internet de um modo seguro, o que possibilita conexões criptografadas que podem ser úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

Neste cenário, as Redes Privadas Virtuais (*Virtual Private Network - VPN*) representam uma alternativa eficiente e sugerida para essa comunicação, pois possibilitam a economia dos custos de manutenção das redes corporativas ao permitirem que as conexões dedicadas existentes de custo mais elevado, sejam substituídas por conexões públicas mais seguras a partir do momento que estas utilizam criptografia e métodos de autenticação de máquina e usuário para a transmissão de dados por meio de um túnel virtual, consolidando assim um parâmetro de custo e benefício bastante satisfatório.

Para o funcionamento das redes privadas virtuais (VPNs) é necessária a presença de um protocolo de tunelamento que será responsável pela forma com que os dados ou informações iram trafegar nas redes computacionais através da internet. Tendo em vista que existem diversos protocolos para desempenhar essa função, a presente pesquisa tem como objetivo geral fazer um comparativo entre as principais tecnologias de protocolos de tunelamento, dando ênfase aos aspectos relacionados com a segurança do tráfego de dados, expondo as vantagens e desvantagens de cada protocolo.

Apesar de não ser o foco principal do trabalho, esta monografia relata alguns conceitos sobre redes de computadores, algumas vantagens das VPNs, mostra em quais tipos de aplicações elas são usadas e suas funções básicas, o funcionamento dos túneis para o fluxo de

informações, os tipos de túneis que podem ser criados, os algoritmos para integridade e criptografia que irão garantir a troca de dados de forma segura e os protocolos implementados para VPNs.

Com o intuito de mostrar como é feita a configuração e instalação de uma VPN em Linux, será demonstrada no final do trabalho, a implementação prática da solução para interligar as redes internas de uma empresa (matriz e filial) localizadas em pontos diferentes e bem distantes, utilizando como software o OPENVPN, por ser uma solução simples e segura, juntamente com protocolo de tunelamento SSL/TSL.

Segundo (TANENBAUM, 1997), as redes de computadores em geral, são elaboradas para "compartilhar recursos" e um de seus objetivos é fazer com que todos os programas, dados e equipamentos estejam disponíveis para qualquer um da rede que solicite, independente da localização física do recurso e do usuário, ou seja, mesmo que o usuário se encontre a uma grande distância dos dados, estes devem ser utilizados como se fossem originados localmente.

O assunto Redes de computadores é muito abrangente, por isso apenas os conceitos básicos e algumas funcionalidades dentro do contexto do trabalho serão expostas.

Um exemplo de rede mundialmente e amplamente difundida é a Internet, que possui milhares de computadores interconectados trocando uma vasta quantidade de informações, através de e-mail, arquivos, etc. A figura 1 mostra uma rede composta por cinco computadores, uma impressora e dois hubs.



Figura 1: Exemplo de uma rede de computadores.
Fonte: 3COM CORPORATION, 2000.

2. REFERENCIAL TEÓRICO

2.1 REDES DE COMPUTADORES

Para uma melhor compreensão do funcionamento das Redes privadas Virtuais (VPNs) que será melhor analisada nos próximos capítulos é de fundamental importância ter uma referência básico sobre Redes de Computadores e alguns conceitos relacionados.

O principal objetivo para se criar uma rede de computadores é compartilhar recursos aos usuários, tais como aplicações, equipamentos e dados, independente da localização física deste recurso ou do próprio usuário.

Segundo (TANENBAUM, 1997), as redes de computadores em geral, são elaboradas para "compartilhar recursos" e um de seus objetivos é fazer com que todos os programas, dados e equipamentos estejam disponíveis para qualquer um da rede que solicite, independente da localização física do recurso e do usuário, ou seja, mesmo que o usuário se encontre a uma grande distância dos dados, estes devem ser utilizados como se fossem originados localmente.

O assunto Redes de computadores é muito abrangente, por isso apenas os conceitos básicos e algumas funcionalidades dentro do contexto do trabalho serão expostas.

Um exemplo de rede mundialmente e amplamente difundida é a Internet, que possui milhares de computadores interconectados trocando uma vasta quantidade de informações, através de e-mail, arquivos, etc. A figura 1 mostra uma rede composta por cinco computadores, uma impressora e dois *hubs*.

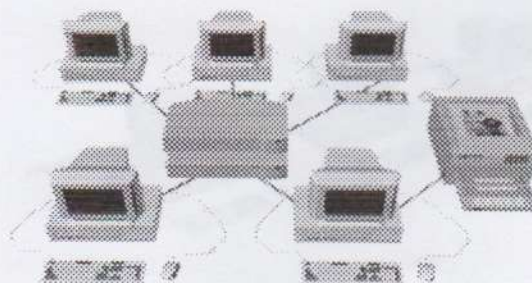


Figura 1: Exemplo de uma rede de computadores.
Fonte: 3COM CORPORATION, 2000.

2.1.1 Principais Tipos de Redes

No aspecto de compartilhamento de dados, existem dois tipos básicos de redes, são elas: ponto-a-ponto e cliente-servidor que iremos abordar superficialmente.

Segundo (TANEMBAUM, 1997), pode se dizer que a principal característica de uma rede ponto-a-ponto é o fato de não estar diretamente conectada a um servidor específico para receber algum tipo de dado ou recurso, sendo assim conhecida como uma rede descentralizada. Os computadores inseridos nesta rede podem assumir tanto o papel de cliente como o de servidor, seja recebendo ou disponibilizando dados e periféricos, como arquivos, unidades de disco, impressoras, scanners, modem, etc.

Um exemplo de rede ponto-a-ponto é exposto na Figura 2, que mostra três computadores compartilhando arquivos entre si.

Elas são de fácil instalação e configuração, porém uma grande desvantagem está relacionada à segurança da rede, devido não ser possível criar uma eficiente política de segurança com este tipo de rede, pois as informações não estão centralizadas em um único computador servidor.

A grande desvantagem que as redes ponto-a-ponto oferecem em relação às redes cliente-servidor é a dificuldade de gerenciar os seus serviços, já que não existe um sistema operacional que centralize a administração da rede. Também não é possível estendê-las excessivamente, já que um número elevado de nós sobrecarregaria o fluxo de dados, tornando-a lenta e conseqüentemente ineficaz. Aos poucos as empresas estão substituindo suas redes ponto-a-ponto por redes cliente-servidor, e o número de redes ponto-a-ponto está diminuindo. [7]

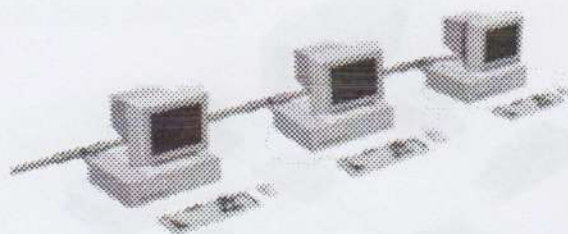


Figura 2: Rede ponto-a-ponto.
Fonte: 3COM CORPORATION, 2000.

As redes do tipo cliente-servidor, também conhecida como centralizada, tem como característica principal possuir pelo menos um computador dedicado a uma ou várias tarefas, sendo este chamado de servidor. Os exemplos mais comuns de servidores são: Arquivos, impressão, aplicações e comunicações (correio eletrônico e páginas *Web*). [8]

A existência de máquinas responsáveis por determinadas tarefas, faz com que o desempenho da rede seja mais eficiente, pois a configuração e manutenção são feitas de forma centralizada, reduzindo os custos para administração, porém a instalação desse tipo de redes é recomendada que seja feita por especialistas.

Segundo (COMER, 2001, pg. 299), “Os aplicativos de rede usam uma forma de comunicação conhecida como paradigma cliente-servidor. Um aplicativo servidor espera passivamente ser contatado, enquanto um aplicativo cliente inicia a comunicação ativamente”.

O termo “Servidor” muitas vezes é usado de forma errônea, principalmente por pessoas que trabalham com a venda de hardware, pois classificam as máquinas com processadores velozes, uma grande quantidade de memória e sistemas operacionais avançados como servidores, mas seguindo a terminologia científica o termo se refere apenas ao programa que está rodando na máquina, não a parte física, esta é chamada de computador da classe servidor, considerado um equipamento poderoso que executa o software servidor. (COMER, 2001).

Umas das grandes vantagens do tipo cliente servidor está relacionada à segurança das informações, pois ficam centralizadas e os acessos a estas são controlados. A figura 3 mostra um exemplo de rede cliente-servidor

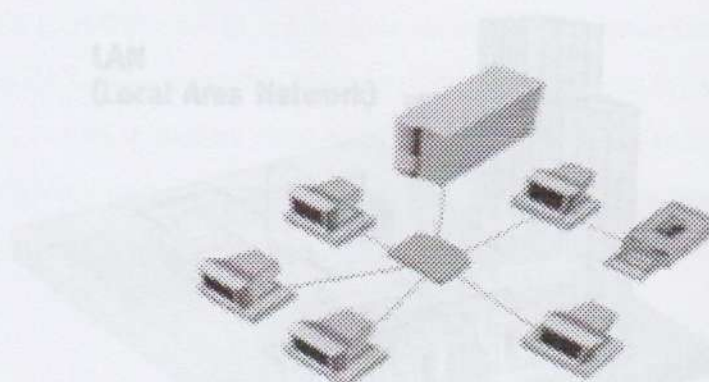


Figura 3: Rede cliente-servidor.
Fonte: 3COM CORPORATION, 2000.

2.1.2 Classificações *Area Network*

Segundo COMER (2001), as redes de computadores possuem diversos tamanhos e tecnologias, entretanto as classificações mais comuns são: *Local Area Network* (LAN), *Wide Area Network* (WAN) e *Metropolitan Area Network* (MAN), *Metropolitan Area Network* ou Rede de Área Metropolitana, abrange uma cidade, porém serão conceituadas apenas as duas primeiras por serem mais usadas.

2.1.2.1 LAN – *Local Area Network*

Segundo TANENBAUM (1997) as LANs são redes locais que conectam servidores, estações, terminais e outros dispositivos em um ou mais edifícios, através de um cabo coaxial que permite transmitir dados em alta velocidade, com baixa taxa de erros e cobre uma área de até 2,5km em prédios separados. Quanto à transmissão de dados, com esse cabo conectado a todas as máquinas, a velocidade de transmissão varia entre 10 e 100 MBPS, tendo um baixo retardo e cometendo poucos erros, os elementos principais que compõe uma LAN são os servidores, que é o principal elemento de processamento, contêm um sistema operativo de rede que se encarrega de administrar todos os processos dentro dela, controla também o acesso aos recursos comuns, como as impressoras e unidades de armazenamento e as estações de trabalho são os computadores pessoais ou qualquer terminal conectado a redes, que trabalham com seus próprios programas ou aproveitam as aplicações existentes no servidor.

A figura 4 mostra uma LAN com 04 computadores, um servidor, uma impressora e um *Hub* para interligar todos dispositivos na rede.

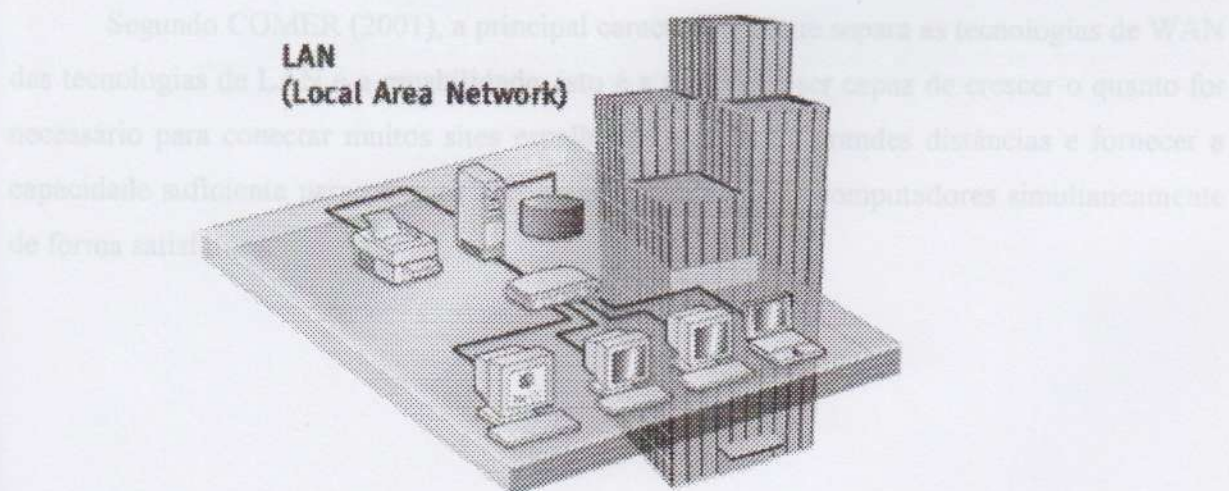


Figura 4: Exemplo de uma LAN

2.1.2.2 WAN – Wide Area Network

Segundo TANENBAUM (1997), são redes remotas geograficamente distribuídas formadas pelas ligações de sistemas de computadores localizados em regiões fisicamente distantes, abrangendo uma grande área geográfica, com frequência um país ou continente. Ela contém um conjunto de máquinas cuja finalidade é executar programas (ou seja, as aplicações) dos usuários, essas máquinas são normalmente chamadas de hosts.

As WANs geralmente utilizam linhas de transmissão de dados oferecidas por empresas de telecomunicações. Segue abaixo como exemplo a Figura 5.

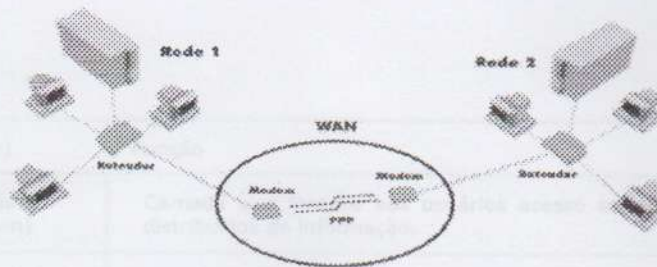


Figura 5: Rede cliente-servidor.

Fonte: 3COM CORPORATION, 2000.

Quando chega a um determinado momento, deixa de ser viável continuar ampliando uma LAN. Muitas vezes isso acontece por limitações físicas, embora tenham formas mais adequadas e econômicas para ampliar uma rede de computadores, como é caso das VPNs que serão abordadas de forma mais detalhada posteriormente.

Segundo COMER (2001), a principal característica que separa as tecnologias de WAN das tecnologias de LAN é a escalabilidade, isto é a rede deve ser capaz de crescer o quanto for necessário para conectar muitos sites espalhados através de grandes distâncias e fornecer a capacidade suficiente para permitir a comunicação de vários computadores simultaneamente de forma satisfatória.

2.1.3 Arquitetura de Modelo RM-OSI

Um estudo superficial da arquitetura de modelo RM-OSI se faz necessária para uma melhor compreensão sobre os 02 níveis de protocolos de tunelamento utilizados em Redes Privadas Virtuais (VPNs).

De acordo com ORTIZ (2002), O RM-OSI (*Reference Model for Open System Interconnection* – Modelo de Referência para o Sistema Aberto de Interconexão) foi desenvolvido pela ISO (*International Standards Organization*) no sentido de padronizar as redes de comunicação, ou seja, é um modelo para arquitetura de um protocolo de comunicação de dados entre dois computadores. Ele é composto por sete níveis, como mostra a tabela abaixo.

Camada (Layer)		Função
7	Aplicação (Application)	Camada que fornece aos usuários acesso ao ambiente OSI e provê sistemas distribuídos de informação.
6	Apresentação (Presentation)	Camada responsável por prover independência aos processos de aplicação das diferenças na representação dos dados (syntaxe).
5	Sessão (Session)	Camada que provê a estrutura de controle para a comunicação entre as aplicações. Estabelece, gerencia e termina conexões (sessões) entre aplicações.
4	Transporte (Transport)	Camada responsável pela transferência de dados entre dois pontos de forma transparente e confiável com funções como controle de fluxo e correção de erro fim a fim.
3	Rede (Network)	Camada que fornece para as camadas superiores independência das tecnologias de transmissão e comutação usadas para conectar os sistemas. Responsável por estabelecer, manter e terminar conexões.
2	Enlace de dados (Data Link)	Camada responsável pela transmissão confiável de informação através do enlace físico. Envia blocos de dados (frames) com o necessário controle de erro e de fluxo.
1	Física (Physical)	Camada responsável pela transmissão de uma sequência de bits em um meio físico. Trata das características mecânicas, elétricas, funcionais e procedurais para acessar o meio físico.

Tabela 1: Arquitetura de modelo RM-OSI

2.1.4 Propriedades de Rede

Para um melhor entendimento do trabalho em questão é de fundamental importância que os conceitos de redes privadas e públicas sejam discriminados.

2.1.4.1 Redes Privadas

Segundo COMER (2001, pg. 179), “as redes que pertencem a e são usadas por uma única empresa ou indivíduo são ditas como *privadas*”.

2.1.4.2 Redes Públicas

Segundo COMER (2001, pg. 179), “e as redes que pertencem a concessionárias comuns são chamados de redes públicas”.

Em diferença a uma rede privada, uma rede pública depende de um sistema telefônico, ou seja, qualquer um pode assinar o serviço e conectar um computador. O sistema público permite que qualquer computador da rede se comunique com outro computador de assinante sem precisar de algum tipo de autorização. Para tornar esse tipo de serviço atraente é fundamental que esteja disponível para muitos assinantes em diversas localizações, por isso a maior parte das redes públicas são WANs.

De acordo com COMER (2001), as LANs são mais usadas para redes privadas, pois estas têm uma ou mais LAN's privadas que conectam os computadores em único edifício ou local, a corporação necessita apenas comprar o equipamento e o software adequado pra cada LAN, fazer a instalação do cabeamento e colocar a rede pra funcionar.

O termo público nesse contexto se refere à disponibilidade do serviço e não dos dados transferidos entre os assinantes, basta pagar para se ter o acesso, funciona como num sistema telefônico, onde o diálogo entre duas pessoas é feito de forma privada, a não ser que os assinantes solicitem uma conferência será permitida a entrada de outras pessoas na conversa, ou seja, dois computadores podem trocar mensagens entre eles numa rede pública, usando uma conexão privada e na teoria apenas esses terão acesso aos dados. (COMER, 2001)

2.1.5 Histórico da Internet

A tão conhecida Internet teve início no final da década de 50, nos Estados Unidos, no auge da Guerra Fria, com o objetivo de proteger e transferir informações confidenciais na eventualidade de acontecer um ataque nuclear vindo da antiga União Soviética. [3]

No ano de 1957, foi criada a *Advanced Research Project Agency* (ARPA) pelo Departamento de Defesa dos Estados Unidos, que, no início dos anos 60, criou a ARPANET, conectando vários centros de pesquisa: *University of California Los Angeles* (UCLA), *Stanford Research Institute* (SRI), *University of California Santa Bárbara* (UCSB) e *Utah University*.

A primeira mensagem trocada entre as redes partiu da UCLA para o SRI em outubro de 1969. Em 1971, já haviam 23 computadores conectados, entre eles a *Massachusetts Institute of Technology* (MIT) e a *National Aeronautics and Space Administration* (NASA). Em 1973, a ARPANET já estava presente em Londres, na *University College* e na Noruega, no *Royal Radar Establishment*.

Em virtude da rápida expansão da ARPANET, o protocolo de comunicação utilizado já não estava mais suprimindo as necessidades desta rede. Foi então que, após intensa atividade de pesquisa na década de 70, surgiu o conjunto de protocolos que até hoje é a base da Internet, conhecido como TCP/IP.

No ano de 1985, a *National Science Foundation* (NSF) interligou os seus supercomputadores, formando a NSFNET, que, no ano seguinte, interligou-se à ARPANET. A união dessas redes passou a ser conhecida oficialmente como Internet.

Em 1988, finalmente a Internet chegou ao Brasil, através das comunidades acadêmicas de São Paulo e do Rio de Janeiro. No ano de 1989, foi criada a Rede Nacional de Pesquisa (RNP), uma instituição com o objetivo de coordenar os serviços de acesso à Internet no Brasil. [3]

Acesso a Rede

Figura 4: Modelo de Referência TCP/IP

Segundo ORTIZ (2002), O TCP/IP é um conjunto de protocolos de interconexão de sistemas, executado em ambiente aberto, organizado em 05 camadas conceituais, definidas como:

2.1.6 Protocolos

Os protocolos permitem que os dispositivos de redes possam se comunicar entre si, mas para isso é necessário que eles sejam compatíveis, ou seja, utilizem o mesmo protocolo de comunicação. Para que isso ocorra, vários protocolos foram criados e são utilizados para transmissão de dados em uma rede. Os protocolos mais comuns e utilizados são o TCP/IP, que são os dois protocolos base para o funcionamento da internet, *Net Bios Extend User Interface* (NETBUI) e o *Interwork Packet Exchange / Sequenced Packet Exchange* (IPX/SPX). [13]

2.1.6.1 Protocolos TCP/IP

Segundo COMER (2001) A Sigla TCP / IP refere-se a dois protocolos de rede utilizados na internet: *Transmission Control Protocol* and *Internet Protocol*. O TCP / IP tinha duas vantagens principais sobre outros protocolos: era leve e podia ser implementado com custo mais baixo do que outras escolhas então disponíveis. Com base nesses fatores, o TCP/IP tornou-se amplamente popular. O modelo de Referência TCP / IP, como mostrado na figura 6, possui um número reduzido de níveis em comparação ao modelo RM-OSI.

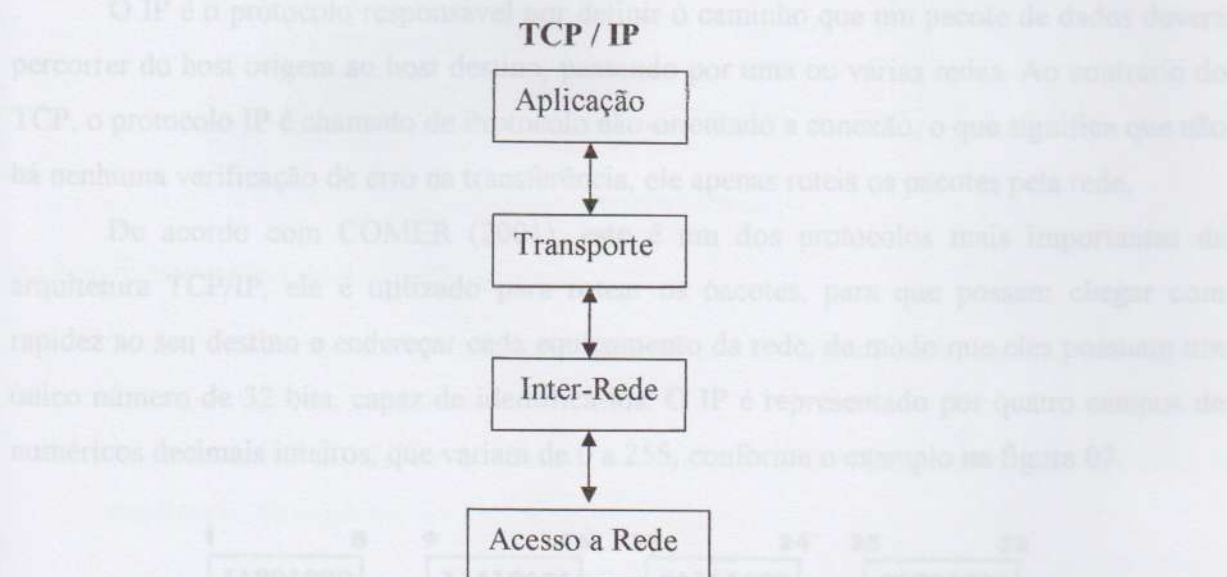


Figura 6: Modelo de Referência TCP/IP

Segundo ORTIZ (2002), O TCP/IP é um conjunto de protocolos de interconexão de sistemas, executado em ambiente aberto, organizado em 05 camadas conceituais, definidas como:

Camada de Aplicação: fornece a interface do usuário de rede na forma de aplicativos e serviços de rede. Exemplos de protocolo: FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*) DNS (*Domain Name System*) e TELNET.

Camada de Transporte: responsável por organizar as mensagens recebidas de camadas mais altas nos segmentos, por controlar os erros e por controlar o fluxo. Exemplos de protocolo: TCP e *User Datagram Protocol* (UDP);

Camada de Inter-Rede: responsável pelo endereçamento dos equipamentos e, pela transmissão (ou roteamento) dos dados em redes diferentes. Exemplos de protocolo: Internet *Control Message Protocol* (ICMP), ARP (*Address Resolution Protocol*) e RARP (*Reverse Address Resolution Protocol*);

Camada de host / rede: responsáveis por controlar o fluxo de dados e organizar os bits da camada física entre redes conectadas a internet, nessa camada empregam gateways e roteadores.

IP – Internet Protocol

O protocolo IP, atualmente encontra-se nas versões 4 e 6 (IPV4 e IPV6).

O IP é o protocolo responsável por definir o caminho que um pacote de dados deverá percorrer do host origem ao host destino, passando por uma ou várias redes. Ao contrário do TCP, o protocolo IP é chamado de Protocolo não-orientado a conexão, o que significa que não há nenhuma verificação de erro na transferência, ele apenas roteia os pacotes pela rede.

De acordo com COMER (2001), este é um dos protocolos mais importantes da arquitetura TCP/IP, ele é utilizado para rotear os pacotes, para que possam chegar com rapidez ao seu destino e endereçar cada equipamento da rede, de modo que eles possuam um único número de 32 bits, capaz de identificá-los. O IP é representado por quatro campos de numéricos decimais inteiros, que variam de 0 a 255, conforme o exemplo na figura 07.

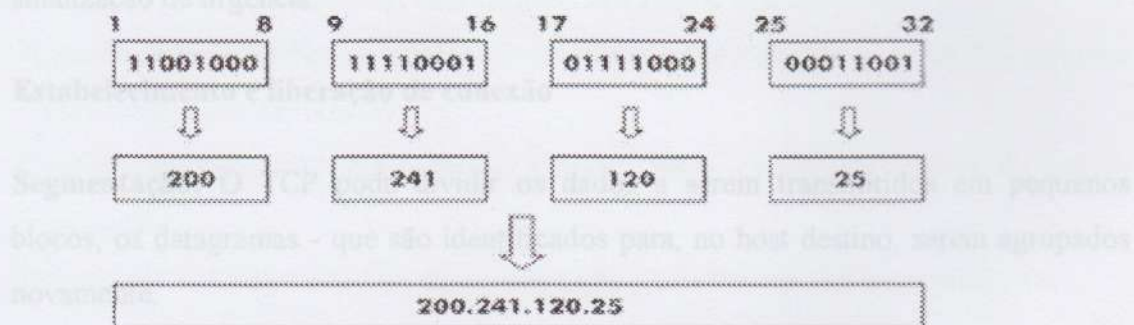


Figura 7: Representação de um IP

TCP - Transmission Control Protocol

O protocolo TCP é utilizado na comunicação entre computadores de uma rede Internet. Através dele pode-se obter um serviço confiável, ou seja, que os dados sejam transmitidos integralmente para os destinos corretos.

As informações transmitidas entre os computadores podem originar de diversas aplicações diferentes, como um E-mail, um acesso a HTTP ou uma transferência de arquivos (FTP).

Para que seja possível identificar a que serviço um determinado datagrama pertence, o TCP utiliza o conceito de *portas*. Determinada a porta, toda a comunicação com a aplicação é realizada e endereçada através dela.

Uma porta é a representação numérica de um serviço Internet. Alguns serviços têm números de porta padrão, como podemos ver na tabela 2 abaixo:

Serviço (Server)	Porta
HTTP (WWW)	80
HTTPS (WWW seguro)	443
IRC (Chat, ou bate-papo)	6667
FTP (Transferência de arquivos)	21
TELNET (Emulação de terminal)	23
SMTP (Transferência de E-Mail entre MTAs)	25

Tabela 2: Portas e Serviços

As principais funções do TCP são:

- **Transferência de dados:** transmissão de dados em blocos (datagramas) e em modo full-duplex (envio e recebimento simultâneos)
- **Transferência de dados urgentes:** transmite primeiro datagramas que contenham sinalização de urgência
- **Estabelecimento e liberação de conexão**
- **Segmentação:** O TCP pode dividir os dados a serem transmitidos em pequenos blocos, os datagramas - que são identificados para, no host destino, serem agrupados novamente.

- **Controle de fluxo:** o TCP é capaz de adaptar a transmissão dos datagramas às condições de transmissões (velocidade, tráfego) entre os sistemas envolvidos.
- **Controle de erros:** como vimos na segmentação, os datagramas são identificados antes de serem transmitidos. Além disso, é adicionado o checksum, um número utilizado para verificar e corrigir erros na transmissão.

UDP – User Datagram Protocol

O UDP é um protocolo mais rápido que o TCP para o transporte de dados entre hosts TCP/IP. [3]

Estes conceitos servirão como base para um melhor entendimento do funcionamento de uma VPN, pois como o próprio nome deixa explícito, esta tecnologia é considerada uma rede, mesmo que virtual.

2.2 SEGURANÇA DA INFORMAÇÃO

Com o avanço da tecnologia em constante crescimento as empresas armazenam informações sigilosas em seus computadores, e a necessidade de proteger esses dados é fundamental. A segurança da informação tem como função principal limitar o acesso físico e lógico aos computadores, através de ferramentas de segurança.

Com a popularização da internet nas empresas, onde o risco das informações serem acessadas ou até mesmo alteradas é relativamente maior por ser uma rede pública, usuários mal intencionados podem tomar posse destas informações, caso elas não estejam bem protegidas. A presença das funções abaixo em um sistema, obviamente irá proporcionar um acréscimo de segurança.

De acordo com a MODULO Security, as principais funções de segurança são:

- **Autenticidade** – Verifica se a pessoa com quem está se trocando informações sigilosas é realmente quem deveria ser;
- **Confidencialidade** – Limita o acesso a informações, geralmente através do uso de criptografia;
- **Integridade** – Assegura que os dados não serão alterados durante uma transmissão;
- **Controle de acesso** – Limita o acesso e a utilização de recursos apenas a pessoas autorizadas;

- Disponibilidade – Mantém os recursos disponíveis, mesmo em caso de ataques;
- Não -repúdio – Impede que uma entidade (computador, pessoa, etc.) envolvida em uma transação negue a sua participação no evento.

2.2.1 Métodos de Ataques

De acordo com BATISTA (2002), para saber como proteger as informações sigilosas de uma empresa é necessário entender primeiro como os ataques se classificam e quais os tipos mais frequentes, para que se possa utilizar o método correto de defesa em uma determinada situação.

Baseados na Figura 8, os ataques se classificam em:

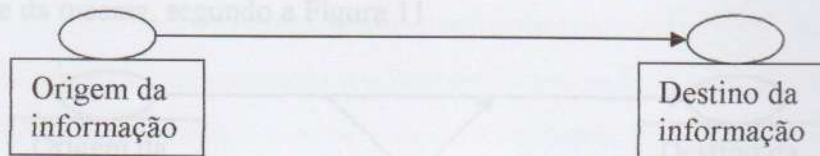


Figura 8: Fluxo normal de uma informação

2.2.1.1 Interrupção

Visa interromper o serviço oferecido, ou seja, ataca-se a disponibilidade das informações, conforme a Figura 9.

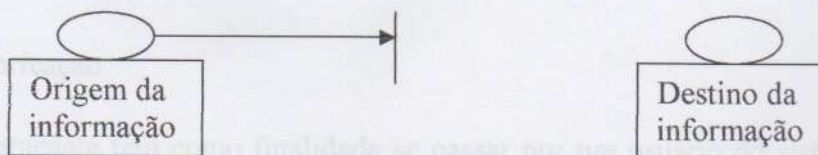


Figura 9: Fluxo interrompido

Segundo BATISTA (2002), o principal tipo de ataque classificado como interrupção é o *Denial of Service* (DoS), que é o envio de requisições em massa para um determinado computador, de modo que o mesmo não consegue responder todas elas, ficando sobrecarregado, fazendo com que o serviço pare de funcionar.

2.2.1.2 Interceptação

Esse tipo de ataque tem como objetivo capturar o que está sendo transmitido sem que o sistema perceba, ou seja, ataca-se a confidencialidade das informações, de acordo com a Figura 10.

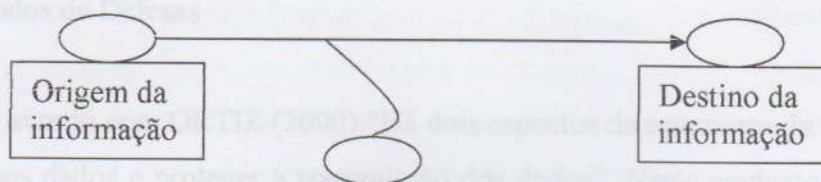


Figura 10: Fluxo interceptado

Um dos principais tipos de ataque desta classificação é o *man-in-the-middle*, onde o invasor simula ser o parceiro de ambas as partes envolvidas na conexão, sumindo a identidade de um usuário válido.

2.2.1.3 Modificação

É quando há alteração da informação que está sendo transmitida, ou seja, ataca-se a integridade da mesma, segundo a Figura 11.

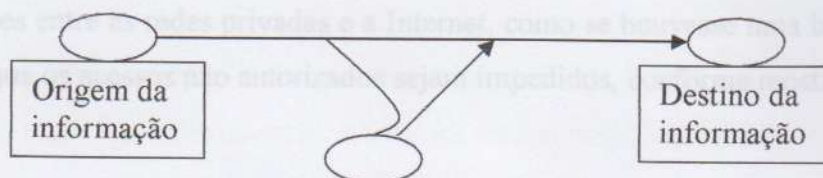


Figura 11: Fluxo modificado

Um exemplo de ataque desta classificação é o Replay, onde parte de uma transmissão da rede é copiada e reproduzida posteriormente, simulando um usuário autorizado.

2.2.1.4 Fabricação

O atacante tem como finalidade se passar por um usuário do sistema, a fim de obter informações para transmitir dados na rede, ou seja, ataca-se a autenticidade das informações, conforme a Figura 12.

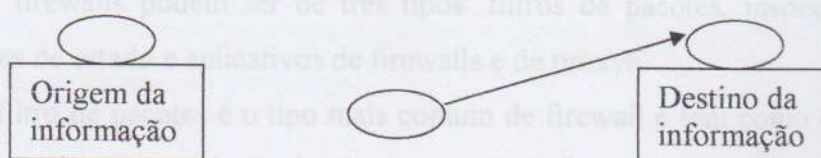


Figura 12: Fluxo fabricado

De acordo com BATISTA (2002) O tipo de ataque mais comum de fabricação é o *IP Spoofing*, que consiste na substituição do endereço IP do computador do invasor, fazendo com que ele se passe por um computador confiável da rede, podendo assim obter privilégios na comunicação.

2.2.2 Métodos de Defesas

De acordo com ORTIZ (2000) “Há dois aspectos da segurança de uma rede – proteger o acesso aos dados e proteger a transmissão dos dados”. Neste contexto, a autenticação dos usuários e a criptografia das informações destacam-se, servindo como base para a segurança de uma VPN.

Existem outros métodos de defesas disponíveis para os mais variados tipos de ataque. Entretanto, o objetivo deste trabalho limita-se à explicação daqueles que são úteis à implementação de uma VPN, os quais serão explicados a seguir.

2.2.2.1 Firewall

É uma combinação de hardware e software, cujo objetivo é controlar o trânsito de informações entre as redes privadas e a Internet, como se houvesse uma barreira entre ambas, de modo que os acessos não autorizados sejam impedidos, conforme mostra a Figura 13.

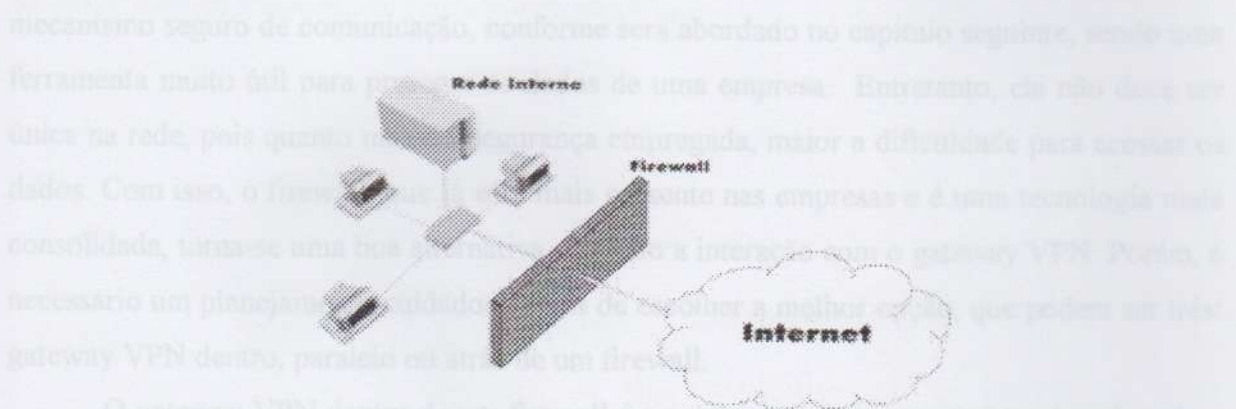


Figura 13: Exemplo de um firewall

Os firewalls podem ser de três tipos: filtros de pacotes, inspeção de pacotes com informações de estado e aplicativos de firewalls e de proxy⁶.

O filtro de pacotes é o tipo mais comum de firewall e tem como objetivo permitir ou negar a entrada de um determinado pacote de informações em uma rede, levando em consideração o endereço IP ou a porta de origem e de destino. Possui como vantagens ser mais barato e rápido que os outros tipos de firewall, uma vez que ele não se importa com o conteúdo dos pacotes. Entretanto, por fazer apenas uma filtragem superficial, sua principal desvantagem é ser mais inseguro que os demais.

A inspeção de pacotes com informações de estado, além de desempenhar as funções do filtro de pacotes, inspecionam o estado da conexão, ou seja, apenas aquelas conexões previamente estabelecidas e válidas, que cumprem as condições configuradas pelo firewall, têm acesso à rede. Uma de suas vantagens é não ter a necessidade de configurar cada computador dentro da rede, reduzindo os encargos administrativos. Todavia, suas configurações são complicadas e não fornecem autenticação de usuário.

Os aplicativos de firewall e de Proxy são os mais complexos, pois varrem todos os dados que passam por eles, descartando os perigosos ou não autorizados e nunca deixando um computador de dentro da rede ficar exposto às redes externas. Possui como vantagens oferecer a maior segurança dos três tipos de firewalls, além de autenticar as atividades dos usuários. Devido ser mais complexo, ele também é mais lento e mais caro que os demais.

2.2.2.2 Firewall e VPN

Uma VPN permite interligar duas ou mais redes de computadores, provendo um mecanismo seguro de comunicação, conforme será abordado no capítulo seguinte, sendo uma ferramenta muito útil para proteger os dados de uma empresa. Entretanto, ela não deve ser única na rede, pois quanto maior a segurança empregada, maior a dificuldade para acessar os dados. Com isso, o firewall, que já está mais presente nas empresas e é uma tecnologia mais consolidada, torna-se uma boa alternativa, fazendo a interação com o gateway VPN. Porém, é necessário um planejamento cuidadoso antes de escolher a melhor opção, que podem ser três: gateway VPN dentro, paralelo ou atrás de um firewall.

O gateway VPN dentro de um firewall é a opção que parece mais natural, pois toda a segurança de sua rede é feita em apenas um computador, de acordo com a Figura 14. Todavia, o mesmo deve ser extremamente seguro, uma vez que qualquer configuração imprópria nas regras do firewall pode permitir que o tráfego vindo da Internet penetre a sua rede utilizando endereços de VPN, sem ser percebido.

O gateway VPN atrás de um firewall faz com que todo o tráfego vindo da Internet passe primeiramente pelo firewall, conforme a Figura 16, deixando a rede mais segura. Em função disso, o mesmo deve possuir uma porta específica para redirecionar o tráfego da VPN. Esta topologia possui como uma de suas vantagens a queda de desempenho na comunicação, em razão de todo o conteúdo de uma VPN passar antes pelo firewall.

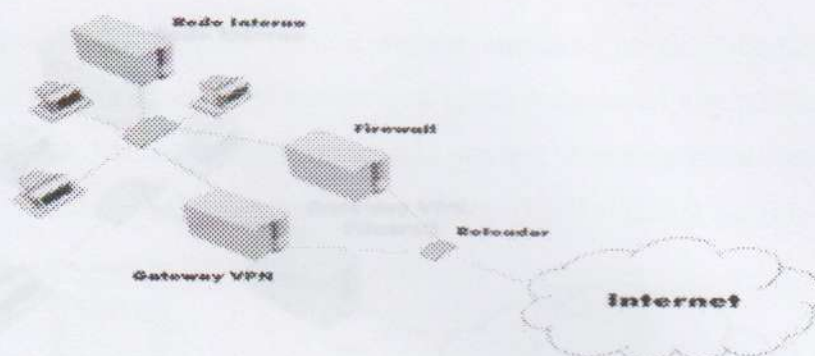


Figura 14: Gateway VPN dentro de um firewall.

O gateway VPN paralelo ao firewall, por sua vez, separa o tráfego de uma VPN do tráfego da Internet em dois ou mais computadores, segundo a Figura 15. Uma das vantagens em separá-los é que, devido o fluxo das informações transmitidas à VPN não passar pelo firewall, nenhuma configuração extra é necessária no mesmo para permitir a passagem de pacotes VPN. Entretanto, isso faz com que o gateway VPN torne-se vulnerável a ataques externos, caso os mesmos não estejam bem seguros.

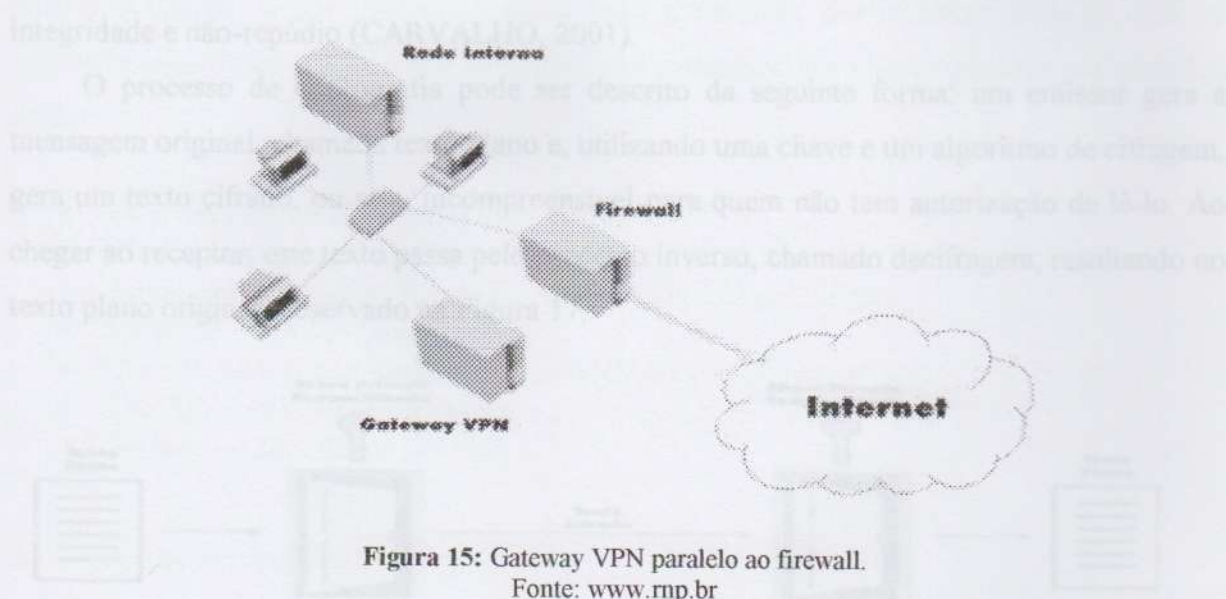


Figura 15: Gateway VPN paralelo ao firewall.
Fonte: www.rnp.br

O gateway VPN atrás de um firewall faz com que todo o tráfego vindo da Internet passe primeiramente pelo firewall, conforme a Figura 16, deixando a rede mais segura. Em função disso, o mesmo deve possuir uma rota específica para redirecionar o tráfego da VPN. Esta topologia possui como uma de suas desvantagens a queda de desempenho na comunicação, em razão de todo o conteúdo de uma VPN passar antes pelo firewall.

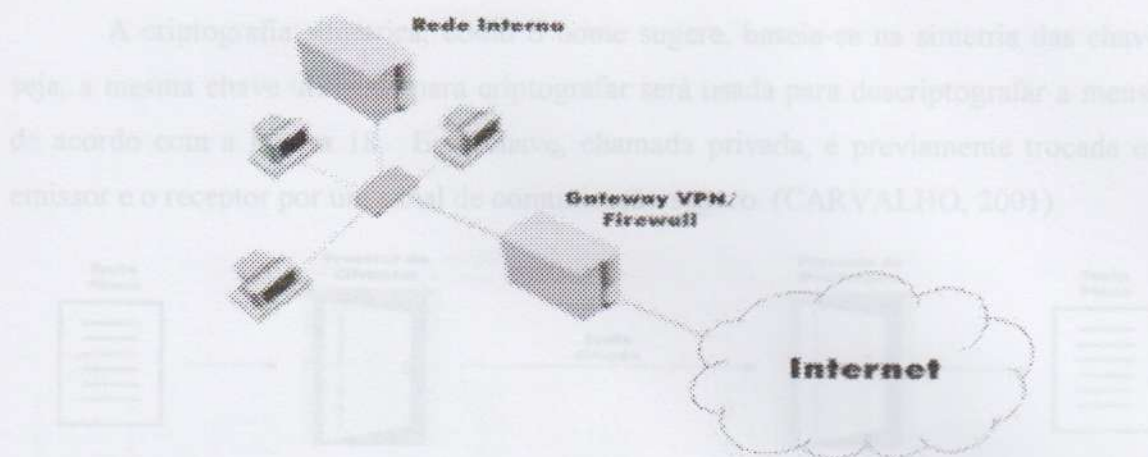


Figura 16: Gateway VPN atrás de um firewall.

2.3. CRIPTOGRAFIA

A palavra criptografia vem do grego (Kryptos = escondido, oculto e Grafia = Escrita) e pode ser definida como a arte ou ciência de garantir a segurança de mensagens, de forma que apenas pessoas autorizadas a leiam. Ela garante confidencialidade, autenticidade, integridade e não-repúdio (CARVALHO, 2001).

O processo de criptografia pode ser descrito da seguinte forma: um emissor gera a mensagem original, chamada texto plano e, utilizando uma chave e um algoritmo de cifragem, gera um texto cifrado, ou seja, incompreensível para quem não tem autorização de lê-lo. Ao chegar ao receptor, este texto passa pelo processo inverso, chamado decifragem, resultando no texto plano original, observado na Figura 17.

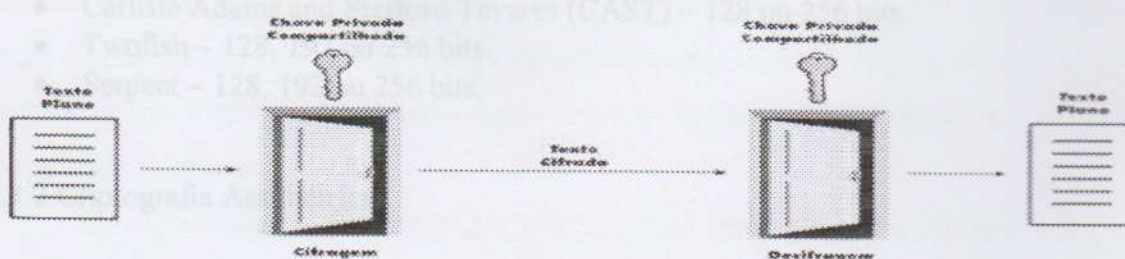


Figura 17: Processo de cifragem e decifragem.

Uma chave é uma combinação de bits e, quanto maior for esta combinação, maior será a segurança obtida. Dependendo do tipo de chave utilizada, a criptografia classifica-se em: Criptografia Simétrica e Criptografia Assimétrica. (CARVALHO, 2001).

2.3.1 Criptografia Simétrica

A criptografia simétrica, como o nome sugere, baseia-se na simetria das chaves, ou seja, a mesma chave utilizada para criptografar será usada para descriptografar a mensagem, de acordo com a Figura 18. Essa chave, chamada privada, é previamente trocada entre o emissor e o receptor por um canal de comunicação seguro. (CARVALHO, 2001)

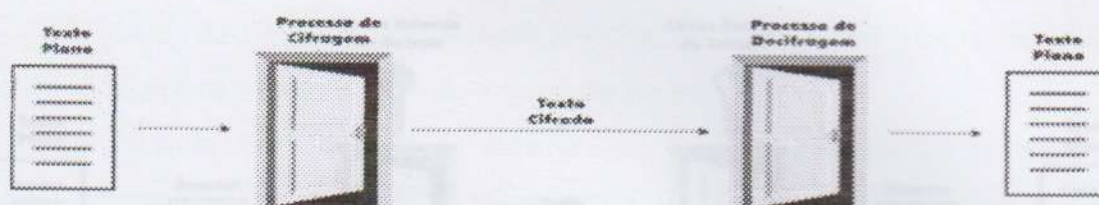


Figura 18: Processo de criptografia simétrica.

As desvantagens deste processo devem-se ao fato de que como apenas uma chave é utilizada para cada par de pessoas, a segurança em cima dela deve ser rígida e, se o número de pessoas que queiram comunicar-se de forma segura for muito grande, serão necessárias inúmeras chaves, o que dificultará ainda mais a gerência das mesmas. Pode-se citar os seguintes algoritmos simétricos e os respectivos tamanhos das chaves geradas por cada um deles:

- Data Encryption Standard (DES) – 56 bits.
- Triple Data Encryption Standard (3DES) – 112 bits.
- Advanced Encryption Standard (AES) – 128, 192 ou 256 bits.
- Blowfish – até 448 bits.
- Carlisle Adams and Stafford Tavares (CAST) – 128 ou 256 bits.
- Twofish – 128, 192 ou 256 bits.
- Serpent – 128, 192 ou 256 bits.

2.3.2 Criptografia Assimétrica

A criptografia assimétrica, por sua vez, envolve o uso de duas chaves distintas, uma privada e outra pública. Pode-se utilizar qualquer uma das chaves para cifrar a mensagem. Entretanto, somente a chave inversa deve ser utilizada para decifrá-la. Por exemplo, se um emissor utiliza a chave pública do receptor para cifrar a mensagem, o receptor deve utilizar a sua chave privada para decifrá-la, conforme a Figura 19. Dessa forma, garante-se autenticidade e confidencialidade.

Contudo, se o emissor utilizar a chave privada para cifrar a mensagem, qualquer pessoa poderá decifrá-la, uma vez que a chave pública é de conhecimento de todos, o que garantirá apenas a autenticidade da mensagem.

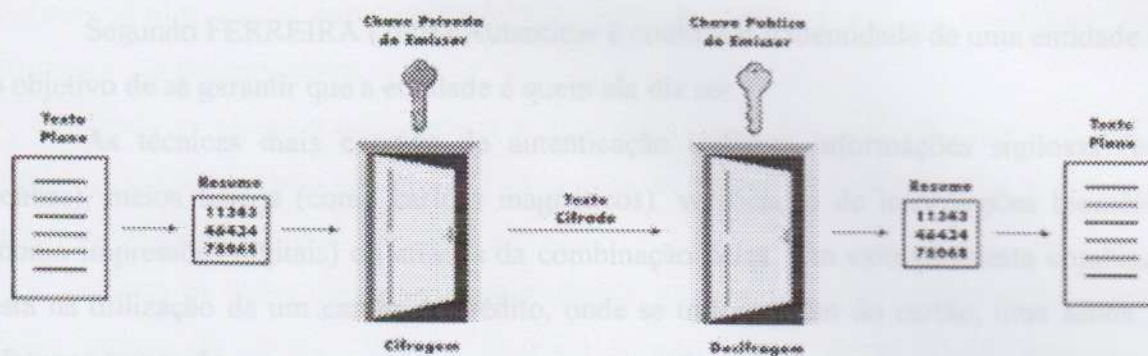


Figura 19: Processo de criptografia assimétrica.

Como exemplo de algoritmo assimétrico, pode-se citar o *Rivest Shamir Adleman* (RSA), composto por chaves de 512, 768, 1024 ou 2048 bits. Este algoritmo é à base da maioria das aplicações de criptografia assimétrica utilizadas atualmente, pois seus mecanismos dificultam a obtenção da chave utilizada. (CARVALHO, 2001)

2.3.3 Função Hash

Dada uma mensagem original, a função hash tem como objetivo produzir um número, conhecido como resumo, que representa de forma única esta mensagem. Uma propriedade desta função diz que o caminho inverso deverá ser computacionalmente inviável, ou seja, não poderá ser possível obter uma mensagem original através de um resumo, o que garante a integridade da mesma.

Os algoritmos que implementam a função hash têm como objetivo fazer com que o resumo sofra uma grande modificação caso algum caractere do conteúdo da mensagem seja alterado. Dentre os principais, podemos destacar o *Message Digest 5* (MD-5) e o *Secure Hash Algorithm 1* (SHA-1). A principal diferença entre os dois é que o primeiro é mais rápido, pois retorna um resumo de 128 bits, enquanto que o segundo retorna um número de 160 bits e, por isso, é mais seguro. Em 01 de Janeiro de 2003, o *Secure Hash Algorithm 2* (SHA-2) será o mais novo algoritmo hash a ser padronizado pelo *National Institute of Standards and Technology* (NIST), tendo como principal característica o retorno de um resumo de 256, 384 ou 512 bits.

2.3.4 Assinatura Digital

Uma assinatura digital é um código binário baseado em 2 aspectos: o documento em si e alguma informação que o ligue a uma certa pessoa ou conjunto de pessoas. Essa ligação é denominada autenticação.

Segundo FERREIRA (2001) Autenticar é confirmar a identidade de uma entidade com o objetivo de se garantir que a entidade é quem ela diz ser.

As técnicas mais comuns de autenticação utilizam informações sigilosas (como senhas), meios físicos (como cartões magnéticos), verificação de informações biométricas (como impressões digitais) ou através da combinação delas. Um exemplo desta combinação está na utilização de um cartão de crédito, onde se utiliza, além do cartão, uma senha para efetuar a transação.

A assinatura digital faz uso da criptografia assimétrica, pois utiliza um par de chaves, uma privada e outra pública. A chave privada serve para assinar o documento, enquanto que a pública serve para verificar a assinatura.

O processo de geração da assinatura utiliza a função hash para a obtenção do resumo do documento, que, em seguida, cifra-o com a chave privada do emissor e envia-o ao receptor. Este utilizará a chave pública do emissor para decifrar a mensagem e a função hash para recalculer o resumo do documento, comparando-o com o resumo recebido, segundo a Figura 20. Isto garante a integridade do documento.

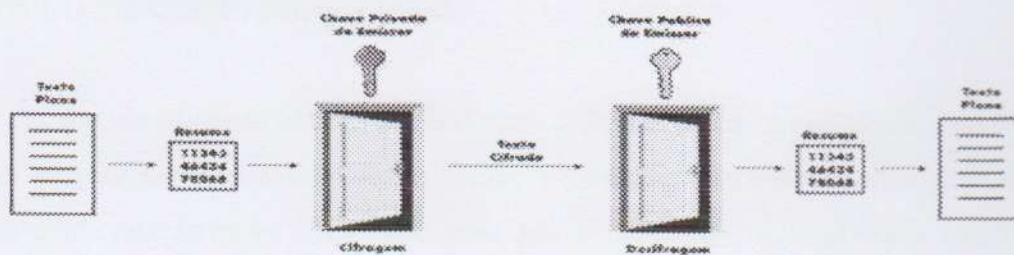


Figura 20: Processo de assinatura digital.

2.3.5 Certificado Digital

O certificado digital é um arquivo assinado eletronicamente por uma entidade confiável, chamada Autoridade Certificadora (AC). Um certificado tem o objetivo de associar a chave pública a uma pessoa ou entidade, servindo, assim, como um mecanismo para a divulgação da chave pública.

Qualquer entidade que conheça a chave pública da AC pode examinar o conteúdo e confirmar a autenticidade de um certificado emitido por esta autoridade, uma vez que a AC assina os certificados com a sua chave privada.

Dentre os dados de um certificado digital, as seguintes informações estão presentes: chave pública do usuário, número de série do certificado, nome da AC que emitiu o certificado, a assinatura digital da AC, entre outras.

A recomendação mais aceita e utilizada para a produção de certificados digitais é a X.509v3, formulada pela *International Telecommunication Union – Telecommunication Standardization Sector* (ITU-T).

O próximo capítulo abordará os principais conceitos de uma VPN, explicando cada uma de suas características, citando alguns protocolos utilizados, dando ênfase ao IPSEC.

3.2 VPN NO MERCADO BRASILEIRO

Apesar de algumas empresas brasileiras desconhecerem a existência desta modalidade de solução que serve para estender redes locais, através de uma rede pública proporcionando uma excelente relação custo x benefício, esse tipo de tecnologia no Brasil vem sendo utilizada vez mais, principalmente no setor de pequenas e médias empresas.

De acordo com ORTIZ (2002, pg. 25), "No final do ano 2001, 44% das empresas que se interessam em implementar uma solução VPN, tinham em mente em fazê-lo em até um ano".

O mercado brasileiro no final do ano 2001 estava dividido da seguinte forma, o que mostra que o mercado para implementação de VPN atualmente está bastante desenvolvida, o que caracteriza a viabilidade da solução.

De acordo com ORTIZ (2002) o mercado de Grandes empresas é representado por 0,12% do total de empresas brasileiras e os produtos consumidos era: Serviço de voz, rede de

3. VIRTUAL PRIVATE NETWORK (VPN)

3.1 CONCEITO DE VPN

As redes privadas virtuais foram desenvolvidas, com o intuito de criar um método confiável para transmitir informações de forma privada, utilizando um túnel criptografado através de redes públicas, como a internet, que é classificada como uma rede não confiável para o tráfego de dados, pois estes podem ser interceptados e copiados sem o usuário perceber.

De acordo com **Comer (2001)**, Uma Rede Privada Virtual combina as vantagens de redes públicas e privadas permitindo que uma empresa com múltiplas localizações tenha a ilusão de uma rede completamente privada, enquanto está usando uma rede pública para transportar tráfego entre seus centros.

Nesse contexto observa-se que a *Virtual Private Networking* ou VPN é uma forma de estender uma rede interna até aos sistemas clientes ligados através da Internet. Uma vez ligados através de VPN, um sistema remoto é virtualmente transportado para dentro da instituição, dando a impressão de estar localmente ligado à rede local e obviamente tendo acesso a todos os recursos aí existentes.

3.2 VPN NO MERCADO BRASILEIRO

Apesar de algumas empresas brasileiras desconhecerem a existência dessa excelente solução que serve para estender redes locais, através de uma rede pública proporcionando uma excelente relação custo x benefício, esse tipo de tecnologia no Brasil vem crescendo cada vez mais, principalmente no setor de pequenas e médias empresas.

De acordo com **ORTIZ (2002, pg. 25)**, “No final do ano 2001, 44% das empresas que se interessam em implementar uma solução VPN, tinham em mente em fazê-lo em até um ano”.

O mercado brasileiro no final do ano 2001 estava dividido da seguinte forma, o que mostra que o mercado para implementação de VPN atualmente esta bastante desenvolvida, o que caracteriza a viabilidade da solução.

De acordo com **ORTIZ (2002)** o mercado de Grandes empresas é representado por 0,12% do total de empresas brasileiras e os produtos consumidos era: Serviço de voz, rede de

dados, *data hosting*, *value added services* e *asp*. Mercado de Médias empresas é representado por 0,64% do total, com os mesmos serviços descritos acima. Mercado de pequenas empresas é representado por 8,15% das empresas brasileiras, serviços de voz, internet banda larga, *web hosting* simples e *value added services*. Mercado de microempresas que engloba a maior fatia do mercado brasileiro, 91% das empresas, utiliza VPN pra serviço de voz, internet banda larga, e *web hosting* simples.

De acordo com os dados levantados por ORTIZ (2002), as Micro, pequenas e médias empresas são as que mais procuram implantar VPN como solução aqui no Brasil.

3.3 CARACTERÍSTICAS BÁSICAS DE UMA VPN

Segundo FERREIRA (2003), para a criação de uma VPN de forma segura e confiável é recomendado que esta rede apresente alguns elementos básicos que serão abordados logo em seguida.

Autenticidade de usuários

Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados por um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

Gerenciamento de endereço

A distribuição de endereços deve assegurar que os endereços estão sendo entregues às redes privadas, os quais continuarão sendo privados.

Criptografia de Dados

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

Gerenciamento de Chaves

Essa característica é responsável pela constante atualização das chaves de criptografia nas pontas do túnel, apenas através dessas chaves é que o cliente e o servidor conseguem descriptografar as mensagens que trafegam na VPN.

Suporte Multi-Protocolo

Com o suporte a Multi-Protocolo a solução de VPN fica mais flexível. No mínimo os protocolos que devem ser suportados são IP e IPX.

3.4 PRINCIPAIS APLICAÇÕES PARA VPN

Segundo FERREIRA (2003), as principais aplicações para VPN, são:

Acesso Remoto Via Internet

O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso (*Internet Service Provider - ISP*). A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

Basicamente o tunelamento em uma VPN pode ser feito de duas formas.

A primeira forma é um simples *host* em trânsito, conecta em um provedor Internet e através dessa conexão, estabelece um túnel com a rede remota. A figura 21 abaixo demonstra essa forma.

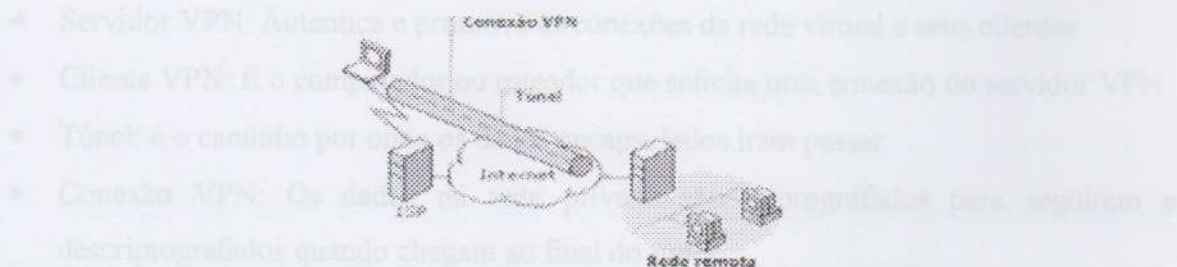


Figura 21: Conexão VPN de um simples *host*

Conexão de LANs Via Internet

Uma solução que substitui as conexões entre *LANs* através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a *WAN* corporativa.

A depender das aplicações também, pode-se optar pela utilização de circuitos discados em uma das pontas, devendo a *LAN* corporativa estar, preferencialmente, conectada à Internet via circuito dedicado local ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.

Nessa segunda forma de fazer uma VPN, duas redes se interligam através de *hosts* com link dedicado ou discado via internet, formando assim um túnel entre as duas redes. A figura 22 ilustra essa forma.

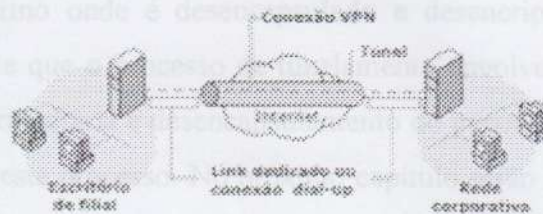


Figura 22: Conexão VPN entre 02 redes interligadas

3.5 ELEMENTOS DE UMA VPN

Para um melhor entendimento do trabalho é de fundamental importância conhecer os elementos que compõem uma VPN e analisar seus conceitos, de acordo com **ORTIZ (2002)** são eles:

- Servidor VPN: Autentica e promove as conexões da rede virtual e seus clientes
- Cliente VPN: É o computador ou roteador que solicita uma conexão do servidor VPN
- Túnel: É o caminho por onde os dados encapsulados irão passar.
- Conexão VPN: Os dados da rede privada são criptografados para seguirem e descriptografados quando chegam ao final do túnel.
- Protocolos de tunelamento: Gerenciam os túneis e encapsulam os dados.
- Dados tunelados: Dados que trafegam através dos túneis criados
- Rede Pública: Na grande maioria das vezes, é a internet.

Uma VPN tem como principais elementos: a criação de um túnel virtual encriptado (tunelamento), a autenticação das extremidades e o transporte subjacente.

Tunelamento

De acordo com SILVA (2002), Tunelamento pode ser definido como sendo o processo de encapsular um protocolo dentro de outro. O uso de tunelamento nas VPNs insere uma nova característica a essa técnica, conhecida como criptografia, já estudada de uma forma mais detalhada no capítulo anterior. A criptografia tem a função de tornar o pacote de informações ilegível, garantindo que se a informação for capturada, será muito difícil entendê-la, a não ser que a chave utilizada seja descoberta.

O pacote criptografado e encapsulado viaja pela Internet, através de um túnel virtual até alcançar seu destino onde é desencapsulado e descriptografado, retornando ao seu formato original. Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote. Os protocolos de tunelamento são responsáveis por este processo. No próximo capítulo serão abordados de uma forma mais detalhada os principais protocolos tunelamento responsáveis pelo processo de tunelamento.

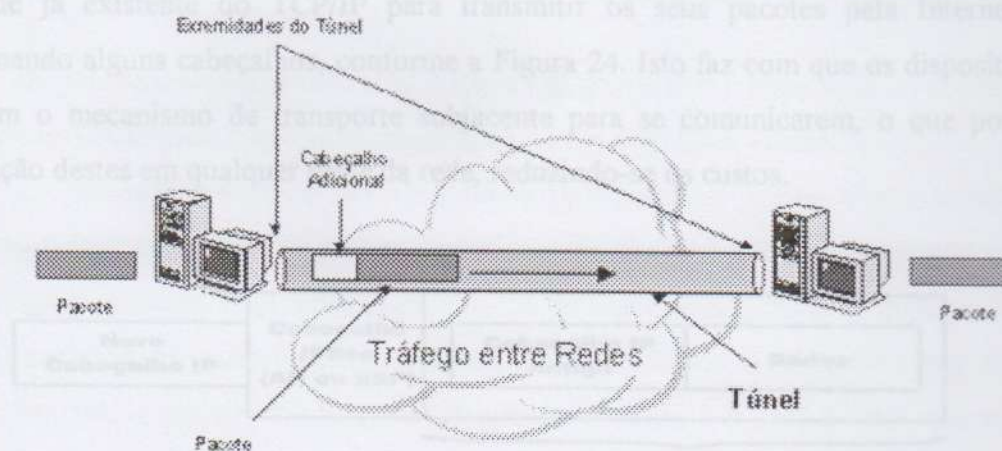


Figura 23: Túnel virtual entre 02 redes
Fonte: LINXWALL

Existem dois tipos de tunelamento para efetuar o processo de encapsulamento, transmissão de pacotes ao longo da rede intermediária e desencapsulamento do pacote, sendo assim os túneis podem ser criados de 02 diferentes formas – voluntárias e compulsórias.

Túnel Voluntário - um cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel.

Túnel Compulsório - um servidor de acesso discado VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

Autenticação das Extremidades

As mensagens são autenticadas para assegurar que elas vieram de usuários válidos, através da utilização de protocolos de autenticação, que geralmente implementam algoritmos *hash*. Desta forma, se alguma parte da mensagem for alterada durante a transmissão, o pacote é descartado. Mesmo a mensagem estando encriptada, a razão de se autenticá-la deve-se ao fato da prevenção de ataques do tipo Replay.

Transporte Subjacente

De acordo com SILVA (2002), o protocolo TCP/IP ser à base da Internet, ele é amplamente utilizado para a comunicação entre redes. Entretanto, ele é muito inseguro, devido não ter sido projetado para esta finalidade. Por isso, uma VPN utiliza a infra-estrutura de rede já existente do TCP/IP para transmitir os seus pacotes pela Internet, apenas adicionando alguns cabeçalhos, conforme a Figura 24. Isto faz com que os dispositivos VPN utilizem o mecanismo de transporte subjacente para se comunicarem, o que possibilita a instalação destes em qualquer parte da rede, reduzindo-se os custos.

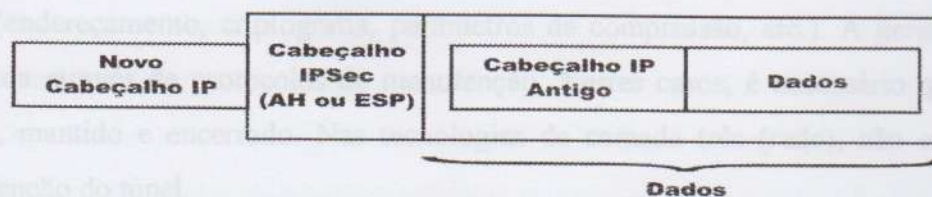


Figura 24: Funcionamento do transporte adjacente

- IPSEC (IP Security Protocol) da IETF (Internet Engineering Task Force)
- SSL / TLS (Secure Socket Layer / Transport Layer Security)

3.6 PROTOCOLOS DE TUNELAMENTO

3.6.1 PPTP

Os protocolos de tunelamento utilizados em VPNs são responsáveis pela transmissão dos dados de uma rede a outra, de forma segura e confiável. Eles são responsáveis pelo gerenciamento de tráfego, controle de erros, segurança e ainda criam os túneis dentro da rede pública para o tráfego de dados. Estes protocolos são divididos em dois grupos, os protocolos da camada 2 e protocolos da camada 3 (respectivamente enlace e rede) do modelo de referência OSI (*Open Systems Interconnection*).

Vale salientar que para se estabelecer um túnel é necessário que suas extremidades utilizem sempre o mesmo protocolo de tunelamento.

Os protocolos de camada dois – Enlace (PPP sobre IP): transporta protocolos de camada três, utilizando quadros como unidade de troca. Os pacotes são encapsulados em quadros PPP, os protocolos da camada 2 abordados neste trabalho são:

- PPTP (*Point-to-Point Tunneling Protocol*) da Microsoft.
- L2TP (*Layer 2 Tunneling Protocol*) da IETF (*Internet Engineering Task Force*)
- L2F (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.

Os protocolos de camada três – Rede (IP sobre IP): encapsulam os pacotes IP com cabeçalhos deste mesmo protocolo antes de enviá-los pelo túnel virtual.

Em túneis orientados à camada 2 (enlace), um túnel é similar a uma sessão, onde as duas extremidades do túnel negociam a configuração dos parâmetros para estabelecimento do túnel (endereçamento, criptografia, parâmetros de compressão, etc.). A gerência do túnel é realizada através de protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada três (rede), não existe a fase de manutenção do túnel.

Os protocolos da camada 03 abordados neste trabalho são:

- IPSEC (*IP Security Protocol*) da IETF (*Internet Engineering Task Force*)
- SSL / TLS (*Secure Socket Layer / Transport Layer Security*)

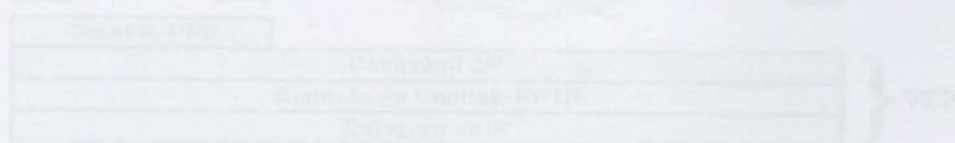


Figura 25: Encapsulamento de um pacote IP em um túnel PPTP

3.6.1 PPTP

O protocolo point-to-Point-Tunneling (PPTP) da Microsoft é um protocolo de camada dois, que utiliza os mesmos mecanismos de autenticação nas conexões dos sistemas PPP. Ele possui uma série de ferramentas que o auxilia na autenticação de dados. Utiliza para fazer a criptografia o MPPE (Criptografia ponto a ponto a Microsoft).

As chaves de criptografia são geradas pelos protocolos de autenticação MS-CHAP ou pelo EAT-PLS. Vale salientar que o PPTP encapsula pacotes PPP utilizando uma versão modificada do GRE e os envia até a outra ponta da VPN, o que torna o PPTP um *multiprotocol* capaz de lidar com outros tipos de pacotes além do IP, como o IPX (*Internet Packet Exchange*) e o NETBEUI (*Network Basic Input/Output System Extended User Interface*), pois é um protocolo baseado na camada 2 do modelo OSI (enlace).

3.6.1.1 Conexão

Em uma conexão que utiliza o protocolo PPTP, existem três elementos envolvidos: o Cliente PPTP, o Servidor de Acesso a Rede (NAS - *Network Access Server*) e o Servidor PPTP. O cliente se conecta a um NAS, através de um POP em um ISP local. O cliente depois de conectado pode enviar e receber pacotes via Internet. O NAS utiliza TCP/IP para todo o tráfego de Internet.

Depois de o cliente ter estabelecido a conexão PPP inicial com o ISP, uma segunda chamada dial-up é efetuada sobre a conexão PPP existente. Os dados desta segunda conexão são enviados na forma de datagramas IP que contém pacotes PPP encapsulados. É esta segunda conexão que cria o túnel com o servidor PPTP nas imediações da LAN corporativa privada. A figura 25 abaixo mostra o esquema de conexão com o protocolo PPTP.

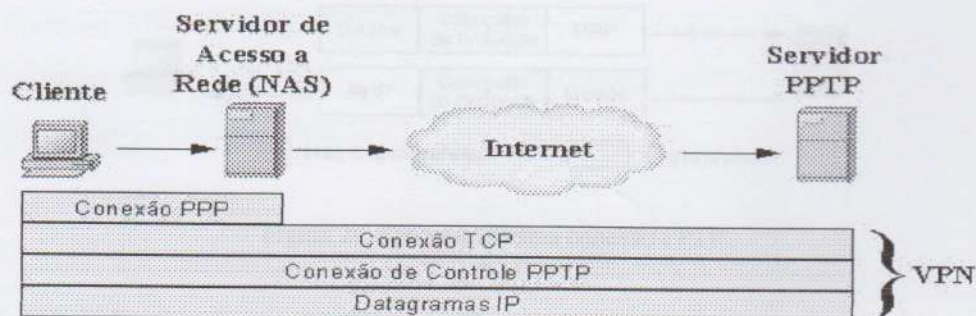


Figura 25: Esquema de um túnel PPTP

3.6.1.2 Arquitetura PPTP

Uma comunicação segura criada pelo PPTP geralmente é composta por três processos, cada um deles exigindo que os anteriores sejam satisfeitos. Esses três processos são:

- **Conexão e Comunicação PPP:** o cliente PPTP usa o PPP para se conectar ao ISP utilizando uma linha telefônica ou ISDN padrão. O PPP é utilizado aqui para estabelecer a conexão e criptografar os dados;
- **Conexão de Controle PPTP:** Utilizando a conexão estabelecida pelo PPP, o PPTP cria um controle de conexão desde o cliente até o servidor PPTP na Internet. Esta conexão utiliza o TCP e é chamada de túnel PPTP;
- **Tunelamento de Dados PPTP:** O PPTP cria os datagramas IP contendo os pacotes PPP criptografados e os envia através do túnel até o servidor PPTP. Neste servidor, os datagramas são então desmontados e os pacotes PPP descriptografados para que finalmente sejam enviados até a rede privada corporativa.

No primeiro processo, o PPP, protocolo que permite enviar dados multi-protocolares encapsulados através de redes TCP/IP, é utilizado para desempenhar três funções: iniciar e terminar conexões físicas, autenticar usuários e criar datagramas PPP contendo pacotes criptografados.

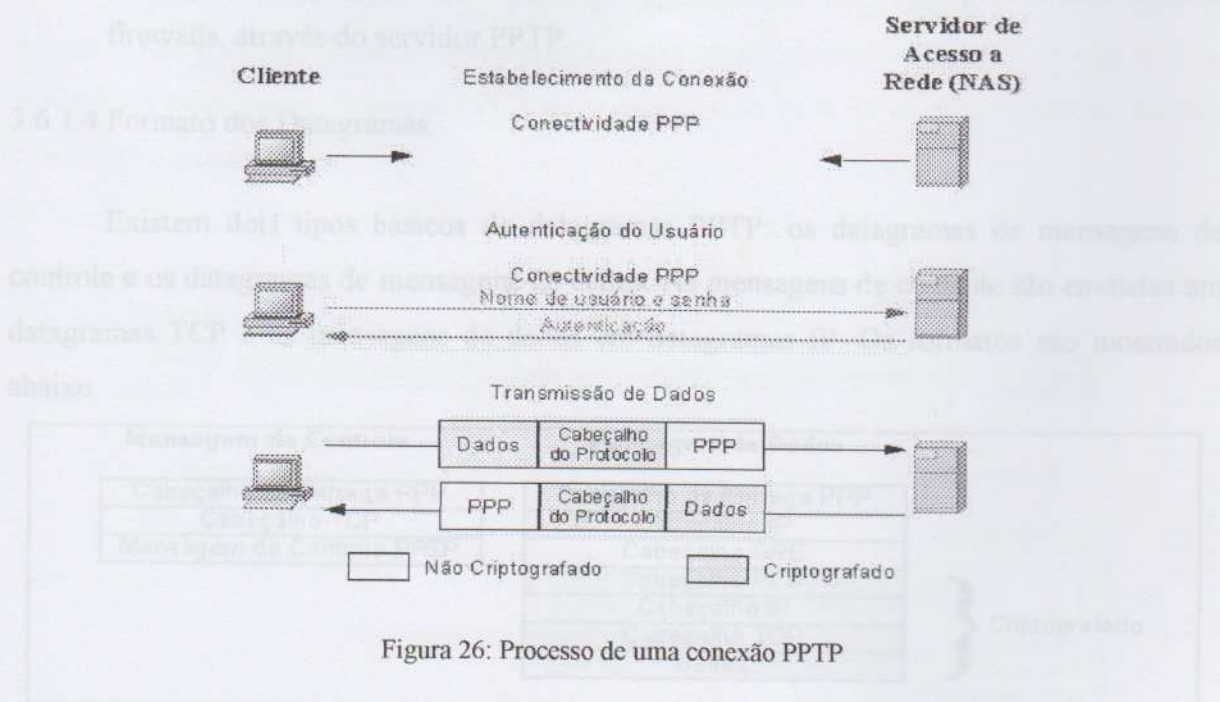


Figura 26: Processo de uma conexão PPTP

No segundo processo, o PPTP especifica uma série de mensagens de controle a serem trocadas entre o cliente PPTP e o servidor PPTP. Estas mensagens estabelecem, mantêm e

terminam os túneis PPTP. Elas são enviadas em pacotes de controle dentro de um datagrama TCP através de uma conexão TCP especialmente criada para trocar mensagens de controle.

Após o túnel PPTP ter sido estabelecido, os dados do usuário são finalmente transmitidos entre o cliente PPTP e o servidor PPTP. É importante frisar que o cliente PPTP não necessariamente identifica o usuário numa extremidade da comunicação. Podem haver usuários utilizando máquinas sem suporte ao PPTP e nestes casos, a comunicação PPTP começa a partir do NAS.

3.6.1.3 Mecanismos de Segurança do PPTP

Para garantir a segurança na transmissão, o PPTP utiliza os seguintes mecanismos:

- **Controle de acesso e autenticação:** a autenticação de usuários remotos é feita utilizando os mesmos métodos do PPP - através dos protocolos PAP, CHAP ou de uma versão da Microsoft, o MS-CHAP;
- **Criptografia de dados:** o PPTP utiliza os métodos de criptografia e compressão do PPP;
- **Filtragem de pacotes PPTP:** este recurso do PPTP permite que apenas os pacotes PPTP dos usuários autenticados entrem no servidor PPTP da rede privada;
- **Utilização de firewalls:** o PPTP também oferece recursos para trabalhar com firewalls, através do servidor PPTP.

3.6.1.4 Formato dos Datagramas

Existem dois tipos básicos de datagramas PPTP: os datagramas de mensagens de controle e os datagramas de mensagens de dados. As mensagens de controle são enviadas em datagramas TCP e as mensagens de dados em datagramas IP. Os formatos são mostrados abaixo.

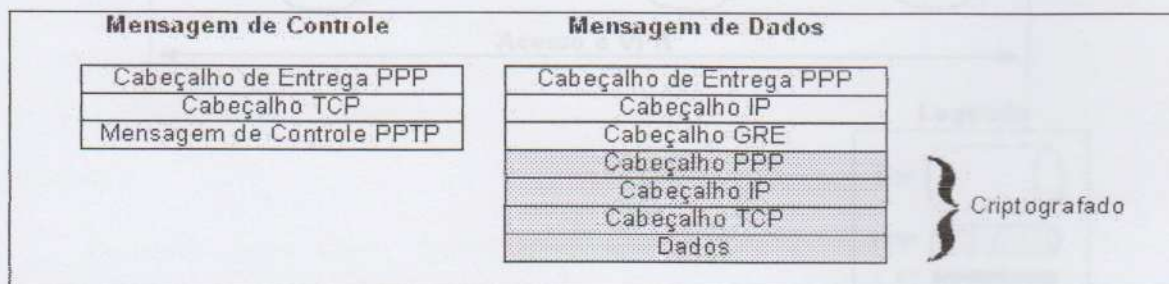


Figura 27: Datagrama PPTP

3.6.2 L2F

O protocolo *Layer 2 Forwarding* (L2F) da Cisco é utilizada para VPNs discadas. Foi um dos primeiros protocolos utilizado por VPNs. Como o PPTP, o L2F foi projetado como um protocolo de tunelamento entre usuários remotos e corporações. Uma grande diferença entre o PPTP e o L2F, é o fato do mesmo não depender de IP e, por isso, é capaz de interagir diretamente com outros meios como *FRAME RELAY* ou ATM.

3.6.2.1 Conexão

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

Quando um usuário deseja se conectar ao gateway da Intranet corporativa, ele primeiro estabelece uma conexão PPP com o NAS do ISP. A partir daí, o NAS estabelece um túnel L2F com o gateway. Finalmente, o gateway autentica o nome de usuário e senha do cliente, e estabelece a conexão PPP com o cliente.

A figura a seguir mostra como funciona o tunelamento com L2F. O NAS (Servidor de Acesso a Rede) do ISP local e o gateway da Intranet estabelecem um túnel L2F que o NAS utiliza para encaminhar os pacotes PPP até o gateway. A VPN de acesso se estende desde o cliente até o gateway.

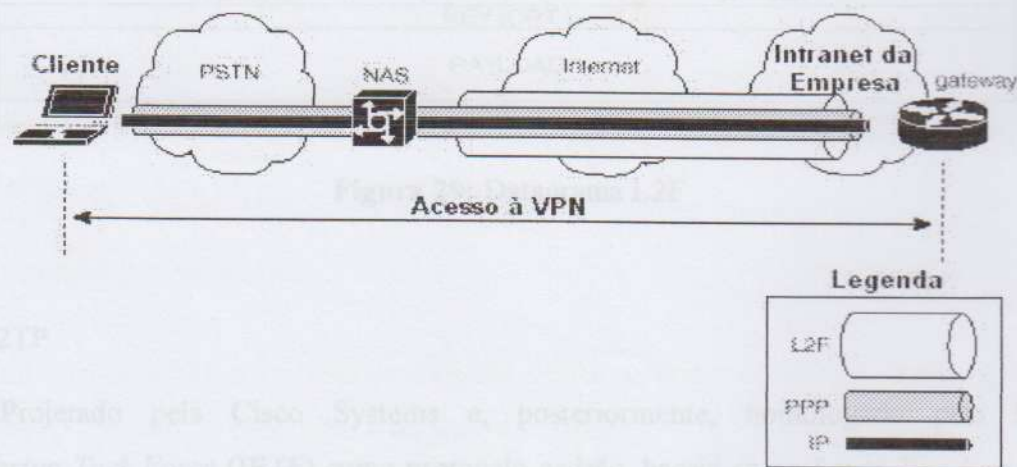


Figura 28: Tunelamento usando o protocolo L2F

3.6.2.2 Formato do Datagrama

Os seguintes campos compõe o cabeçalho:

- **Ver:** versão do L2F;
- **Protocol:** protocolo carregado dentro do pacote L2F;
- **Sequence Number:** quando o bit "S" (bit 3) for igual a 1, este campo identifica o número do pacote numa sequência;
- **Multiplex ID:** identifica uma conexão dentro de um túnel;
- **Client ID:** campo utilizado para auxiliar a demultiplexação em túneis;
- **Length:** indica o tamanho do pacote em octetos, sem levar em conta o campo de checksum;
- **Offset:** quando o bit "F" (bit 0) for igual a 1, este campo identifica aonde começa a área de dados do pacote indicando o número de bytes após o cabeçalho.
- **Key:** o campo de chave está presente se o bit "K" (bit 1) for igual a 1. Serve como chave durante toda a sessão para resistir a ataques de "spoofing".
- **Checksum:** o campo de checksum está presente se o bit "C" (bit 12) for igual a 1.

A figura x mostra o formato do datagrama para o protocolo L2F

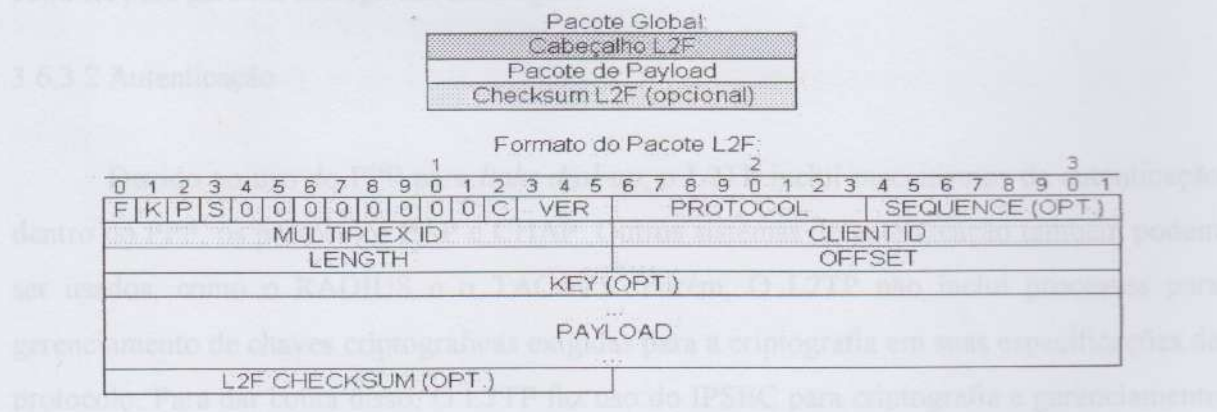


Figura 29: Datagrama L2F

3.6.3 L2TP

Projetado pela Cisco Systems e, posteriormente, homologado pela Internet Engineering Task Force (IETF) como protocolo padrão, baseia-se no *Layer Two Forwarding* (L2F) para solucionar os problemas do PPTP, sendo considerado o seu herdeiro. 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.

3.6.3.1 Conexão

O L2TP funciona de forma similar ao protocolo L2F. Um Concentrador de Acesso L2TP (LAC) localizado no PoP do ISP troca mensagens PPP com usuários remotos e se comunica por meio de solicitações e respostas L2TP com o Servidor de Rede L2TP (LNS) para criação de túneis. O L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão ponto-a-ponto. Os quadros enviados pelo usuário são aceitos pelo PoP do 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 a interface apropriada.

O L2TP utiliza dois tipos de mensagem: mensagens de controle e mensagens de dados. As mensagens de controle são usadas para gerenciar, manter e excluir túneis e chamadas. As mensagens de dados são usadas para encapsular os pacotes PPP a serem transmitidos dentro do túnel. As mensagens de controle utilizam um confiável canal de controle para garantir entrega das mensagens.

3.6.3.2 Autenticação

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 usados, como o RADIUS e o TACACS. Porém, O L2TP não inclui processos para gerenciamento de chaves criptográficas exigidas para a criptografia em suas especificações de protocolo. Para dar conta disso, O L2TP faz uso do IPSEC para criptografia e gerenciamento de chaves em ambiente IP.

3.6.3.3 Formato do Datagrama

Os pacotes L2TP para canal de controle e canal de dados utilizam o mesmo formato de cabeçalho. O formato do cabeçalho é mostrado a seguir:

1										2										3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
T	L	x	x	S	X	O	P	x	x	x	x	VER					LENGTH (OPT.)														
TUNNEL ID												SESSION ID																			
NS (OPT)												NR (OPT)																			
OFFSET SIZE (OPT.)																															

Figura 30: Datagrama L2TP

O cabeçalho possui os seguintes campos:

- **Type (bit 0):** identifica o tipo de mensagem. Se o bit for igual a 1 é uma mensagem de controle, se for igual a 0 é uma mensagem de dados;
- **Ver:** identifica o número da versão do protocolo;
- **Length:** identifica o tamanho do pacote em octetos se o bit "L" (bit 1) for igual a 1;
- **Tunnel ID:** indica o identificador do Túnel para controle de conexão;
- **Session ID:** indica o identificador de uma sessão dentro de um túnel;
- **Ns:** indica o número de sequência para o atual pacote (mensagem ou controle). Sua presença é definida pelo bit "S" (bit 4);
- **Nr:** indica o número de sequência esperado para o próximo pacote de mensagem de controle. Sua presença também é definida pelo bit "S";
- **Offset Size:** determina o tamanho do offset (espaço entre o cabeçalho e a área de dados). Sua presença é definida pelo bit "O" (bit 6);
- **Priority (bit 7):** se for igual a 1, o pacote deve receber tratamento preferencial com relação aos outros;
- **Bits X:** reservados para extensões futuras.

3.6.4.1 Modos de Operação

Segundo ORFIZ (2012) existem 03 modos de pacotes criados através do IPSEC para o envio de dados. Nos pacotes criados no modo transporte são adicionados cabeçalhos IPSEC entre o cabeçalho IP original e os dados, conforme a Figura 31.

3.6.4 IPSEC

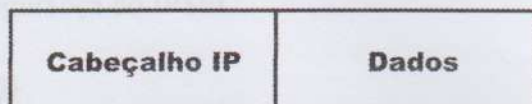
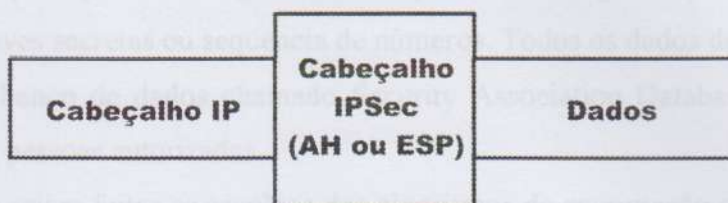
Segundo ORTIZ (2002), IPSEC é um conjunto de protocolos desenvolvido para proteger o tráfego dos pacotes IP. Sua principal característica é garantir a segurança da comunicação. Para isto, ele utiliza os conceitos de autenticação, proteção à integridade, proteção a ataques do tipo Replay e confidencialidade, todos dependendo do conjunto de protocolos a serem utilizados.

O IPSEC foi desenvolvido pelo Grupo de Trabalho de Segurança do IP da IETF com o intuito de ser o protocolo padrão de endereçamento para a próxima versão do IP, chamada IPv6, que está em fase de testes em diversas instituições no mundo inteiro. No Brasil, um dos órgãos que está testando o IPv6 é a RNP. Por enquanto, o IPSEC é apenas opcional para o IPv4.

O IPSEC é uma estrutura de padrões abertos que garante comunicação privativa segura em redes de protocolo de Internet em nível de camada de rede. O IPSEC faz a criptografia de camada de rede do protocolo de Internet. O padrão define vários formatos de novos pacotes: o cabeçalho de autenticação (AH) para fornecimento da integridade dos dados, e a carga de segurança encapsuladora (ESP - *Encapsulating Security Payload*), para garantir a privacidade e a integridade destes dados. A associação entre gerenciamento de chaves e segurança e os parâmetros IPSEC entre duas máquinas são controlados com a Troca de Chaves de Internet (IKE - *Internet Key Exchange*). A IKE pode usar os certificados digitais para a autenticação de aparelhos, a fim de permitir a criação de grandes redes de criptografia. Sem suporte aos certificados digitais, as soluções IPSEC não poderão ser redimensionadas para se ajustar a internet.

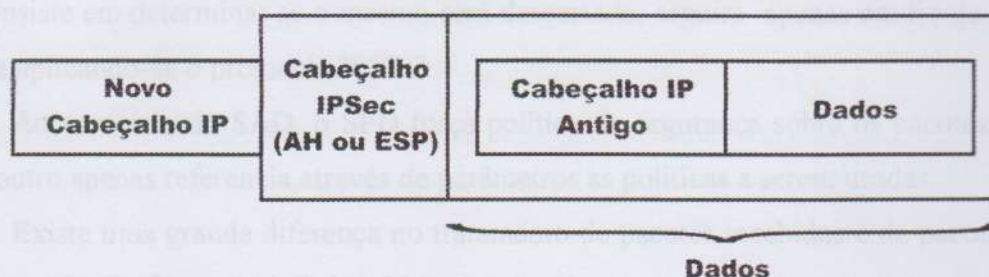
3.6.4.1 Modos de Operação

Segundo ORTIZ (2002) Existem 02 modos de pacotes criados através do IPSEC para o envio de dados. Nos pacotes criados no modo transporte são adicionados cabeçalhos IPSEC entre o cabeçalho IP original e os dados, conforme a Figura 31.

Pacote IP Original**Pacote Protegido (Modo Transporte)****Figura 31: Modo transporte**

Este modo é muito utilizado para computadores em diferentes redes, comunicando-se diretamente entre si, e que desejam proteger o seu tráfego IP por encapsulamento, autenticação ou ambos.

No modo túnel, um cabeçalho IPSEC também é adicionado, porém a diferença para o modo transporte é que será adicionado um novo cabeçalho IP e o pacote original será tratado como se fosse um dado só, sendo todo ele encriptado pelo cabeçalho IPSEC na parte referente ao dado do novo cabeçalho, de acordo com a Figura 32.

Pacote Protegido (Modo Túnel)**Figura 32: Modo Túnel**

O modo túnel é comumente utilizado na comunicação entre *gateways*, pois fornece maior segurança aos dados originais encriptados dentro do novo pacote.

3.6.4.2 Elementos de Segurança do IPSEC

Security Association (SA)

As associações seguras chamadas de SAs são responsáveis por alocar informações sigilosas para a proteção do tráfego entre computadores ou gateways, como algoritmos de criptografia, chaves secretas ou sequência de números. Todos os dados das SAs são guardados dentro de um banco de dados chamado Security Association Database (SAD), tendo seu acesso restrito à pessoas autorizadas.

Para que sejam feitas as escolhas dos algoritmos de encriptação ou das funções hash a serem utilizadas para assegurar os pacotes, as chaves ou as sequências de números, são definidos parâmetros para cada SA. Os exemplos mais utilizados são: endereços IPs de origem ou destino; números de origem ou destino das portas de comunicação; protocolos de segurança; assinaturas ou certificados digitais; modo transporte ou modo túnel; ou os *Security Parameters Index* (SPI) – índices de 32 bits incorporados aos cabeçalhos dos pacotes que juntamente com o endereço IP de destino e com os protocolos de segurança, identificam a melhor SA para usar no pacote.

Security Policy Database (SPD)

É o banco de dados responsável pela ação mais importante a ser feita sobre o pacote, que consiste em determinar se o mesmo será descartado, seguirá apenas em frente ou seguirá adiante aplicando-se o protocolo IPSEC.

Ao contrário do SAD, o SPD força política de segurança sobre os pacotes, enquanto que o outro apenas referencia através de parâmetros as políticas a serem usadas.

Existe uma grande diferença no tratamento de pacotes recebidos e de pacotes a serem enviados. No Tráfego recebido, o SAD é aplicado antes do SPD, pois serão verificadas a identidade do emissor e a integridade dos pacotes, para depois enviá-los à regra SPD correspondente. No Tráfego enviado, o SPD é executado para verificar qual ação será aplicada ao pacote e, se necessário, dependendo da política de segurança, o IPSEC poderá pesquisar o SAD.

Gerenciamento de Chaves

Em redes com poucos computadores pode-se configurar as SAs e os SPDs manualmente. Todavia, se a rede for grande, o recomendado é configurá-los automaticamente, o que acarretará no uso de um gerenciamento de chaves automático.

Alguns protocolos implementam de forma satisfatória este gerenciamento, porém o principal deles é o Internet Key Exchange Protocol (IKE), que combina os protocolos Internet Security Association and Key Management Protocol (ISAKMP), SKEME e *Oakley Key Determination Protocol*.

O IKE negocia automaticamente as SAs, permitindo maior proteção contra ataques e, se habilitado o *Perfect Forward Secrecy (PFS)*, garante que se uma das chaves secretas estiver comprometida, apenas os dados encriptados por esta chave estarão. Caso contrário, todas as outras chaves e SAs podem ser afetadas.

Este protocolo funciona em duas fases: a primeira estabelece um canal de comunicação seguro entre as duas extremidades que desejam trocar dados. Para que isto seja possível é necessária a seguinte seqüência de operações: verificar os protocolos criptográficos e os parâmetros que serão utilizados para escolher os algoritmos de autenticação e de encriptação e, baseado nestas informações, as chaves secretas entre estas extremidades serão trocadas e, em seguida, uma associação segura ISAKMP é feita para então criar o canal; a segunda fase fornece as melhores associações seguras para proteger o tráfego IP pelo canal de comunicação criado na primeira fase. Isto é feito através dos seguintes passos: uma nova associação segura ISAKMP é estabelecida para a proteção das trocas de informações desta fase e, posteriormente, são negociados protocolos ou combinação de protocolos que posteriormente serão armazenados nas SADs de cada extremidade.

3.6.5 SSL/TSL

Uma tecnologia usada em VPN que esta crescendo na popularidade é a camada segura dos soquetes (SSL) VPN. Uma grande vantagem de SSL VPNS é que você não necessita de software de cliente especial de VPN. Isso acontece porque o SSL VPN usa o *web browser* como a aplicação do cliente. Assim, o SSL VPNs é inteligente como soluções "clientless".

Isto significa também que os protocolos que podem ser segurados por uma SSL VPN sejam mais limitados. Entretanto, esta pode também ser uma vantagem de segurança. Com SSL VPNS, em vez de dar aos clientes de VPN o alcance à rede ou ao subnet inteira como no IPSEC, você pode restringi-los às aplicações específicas. Se as aplicações que você quer dar acesso pelo browser não forem baseadas e for necessária fazer uma programação feita sob encomenda para criar uma interação Java ou Activex com o browser. Ocorre uma desvantagem neste momento, pois a fim de usar Java ou activex, os ajustes do browser do cliente terão que ser abertos até permitirem o índice ativo - assim expor o browser aos *applets* maliciosos a menos que você o ajuste para obstruir índice ativo não assinado e para se assegurar de que os de encaixe estejam com assinatura digital.

4. ANÁLISE DE RESULTADOS

4.1 PPTP: POINT-TO-POINT TUNNELING PROTOCOL

- Amplamente utilizado para dial-up VPNs
- Presença de suporte (servidor) no RRAS do Windows NT 4.0
- Presença de suporte (cliente) no Windows 9x
- Protocolo da camada 2 (enlace), pode carregar outros protocolos além do IP

No aspecto de segurança este protocolo não apresenta grande credibilidade, pois é baseado no PPP, usando PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*), considerados não muito robustos, para a identificação/autenticação de clientes, porém pode ser usado o MS-CHAP, mais robusto para autenticar em domínios NT, segundo a Microsoft.

4.2 L2F: LAYER 2 FORWARDING

É semelhante ao PPTP, acrescentando:

- Suporte a outros protocolos para o túnel (*Frame Relay*, ATM).
- Suporte a TACACS e RADIUS para autenticação (além de PAP)
- Suporte a mais de uma conexão por túnel

Exige dois níveis de enlace:

- Cliente ⇔ ISP
- ISP ⇔ Rede Corporativa

Usa protocolo próprio no enlace ISP ⇔ Rede Corporativa

4.3 L2TP: LAYER 2 TRANSPORT PROTOCOL

No entanto, uma diferença visível em relação a seu predecessor (L2F) é quanto à forma de autenticação, pois ela é feita em dois níveis. No primeiro, o usuário é autenticado pelo provedor de acesso antes do túnel ser instalado e, no segundo, quando a conexão é estabelecida entre os gateways.

Sendo um protocolo padrão, qualquer fabricante pode criar produtos que utilizem o L2TP, de forma que provedores de acesso e consumidores em geral não dependam de produtos fornecidos por uma única empresa.

Apesar de ser atual, o L2TP apresenta como desvantagem não possuir um mecanismo eficiente de encapsulamento, ou seja, para executar esta tarefa, ele necessita do protocolo IPSEC, que será explicado posteriormente, para que juntos possam garantir a segurança da VPN.

- É o primeiro protocolo proposto por uma força tarefa da Internet (IETF)
- É semelhante ao PPTP e L2F para uma fácil adaptação da base instalada
- Usa PPP para o enlace cliente ↔ ISP
- Usa protocolo próprio (semelhante ao L2F) no enlace ISP ↔ Rede Corporativa
- Para tornar mais robusta a proteção aos dados, usa técnicas de criptografia baseadas no protocolo IPSEC.

4.4 IPSEC: IP SECURITY PROTOCOL

- É derivado dos esforços para implementar segurança no nível IP do IPv6
- Permite autenticação/criptação de cada pacote transmitido
- Pode ser usado em dois modos: Transporte: somente o conteúdo transportado por um datagrama IP é autenticado/criptografado e Túnel: todo o datagrama IP é autenticado/criptografado e levado através de um túnel
- Impõe segurança eficiente com: Troca de chaves *Diffie-Hellman* para entrega de chaves secretas entre parceiros através da rede pública, Criptografia de chave pública para sinalizar troca de chaves *Diffie-Hellman*, DES para criptografia de dados, HMAC, MD5 e SHA para autenticação de pacotes, Certificados digitais para validação de chaves públicas.
- Pode usar dois métodos para a troca de chaves (mandatório no IPSEC): Manual e Automático via *Internet Key Exchange* (IKE)

4.5 OPENVPN: SSL / TSL

- Fácil de configurar
- Multiplataforma, funciona em diversos sistemas operacionais, tais como: Linux, Solaris, OpenBSD, Mac OS X Darwin FreeBSD, Windows XP, Windows 2000 e NetBSD
- Open source
- Flexível (TCP ou UDP e suporta Proxy)
- Nat amigável
- *Bridge layer 2 over layer 3*

4.5.1 OPENVPN (SSL/TSL) X IPSEC

O OPENVPN possui excelentes recursos que o atual IPSEC também possui só que de maneira mais simples:

- Utilização de chaves estáticas para a criação de VPNs com rapidez e simplicidade.
- Utilização de VPNs usando SSL/TLS + RSA, permitindo que se usem certificados X.509 para as conexões assim como o IPSEC.
- Permite conexões Gateway-to-Gateway, Host-to-Host e Host-to-Gateway. VPNs Road Warrior são comuns.
- Não necessita de patches como o NAT-Traversal para que a VPN possa ser estabelecida por de trás de um Firewall, como é o caso do IPSEC.
- Atualmente o driver TUN/TAP já vem com o kernel e basta apenas habilitá-lo para que o OPENVPN possa funcionar. No caso do IPSEC, o FreeSwan precisa ser aplicado no kernel 2.4 e o kernel 2.6 vem com um IPSEC que não é mesmo do FreeSwan Team.
- Com o OPENVPN podemos encontrar uma versão deste para Windows XP e Windows 2000 que funciona muito bem e livre de licenças. No caso do IPSEC temos que contar com o IPSEC implementado pela Microsoft ou outros clientes comerciais que em ambos os casos são mais complexos de se implementar que o OPENVPN.
- O arquivo conf do OPENVPN também é bem mais simples de se entender e administrar.

Desvantagem OPENVPN

Não funciona em sistemas operacionais Windows sem Tecnologia NT, ou seja, win 95, win 98 e Me.

5. CONCLUSÃO

Dentre as estratégias de tornar seguro o tráfego de informações em redes inseguras como a Internet, o uso de VPNs é um dos mais eficientes e baratos, podendo ser considerada uma alternativa segura para transmissão de dados através de redes públicas ou privadas. As VPNs possuem diversos protocolos que oferecem recursos de autenticação e criptografia com diferentes níveis de segurança, o que possibilita eliminar os Links dedicados de longa distância, de alto custo, na conexão de redes WANs

As VPNs cada vez mais são pesquisadas e incorporadas às organizações, sejam privadas ou governamentais, em diversos sistemas e ambientes computacionais. Os principais motivos desta crescente procura estão relacionados à segurança e economia no tráfego das informações.

Esta segurança é obtida principalmente através da utilização de algoritmos de criptografia e protocolos específicos, que geram grandes obstáculos aos invasores. Algumas das funções de segurança garantidas por uma VPN é a integridade e a confidencialidade das informações transmitidas, assim como a autenticação.

Alguns dos protocolos abordados neste trabalho foram o PPTP, L2TP e L2F, que se mostraram boas alternativas de implementação, porém pecam na segurança. Por sua vez, o IPSEC mostrou-se um protocolo mais completo em relação a estes, possuindo características mais expressivas no intuito de proteger o tráfego das redes interligadas. Todavia, ele ainda é muito complexo e, por isso, é indispensável entender exatamente o seu funcionamento antes de implementá-lo em uma VPN, já a solução OPENVPN com o protocolo SSL/TSL é o mais aconselhável atualmente, pois possui todos recursos que o atual IPSEC implementa, sendo que de uma forma mais simples, segundo a análise feita nesta monografia.

É importante salientar que nem o OPENVPN SSL/TSL e nem uma VPN sozinhos são garantias de segurança de uma rede. É fundamental que um planejamento seja elaborado, formulando políticas concretas de segurança, permitindo que haja proteção lógica e física dos servidores.

12. JULIO, Anderson. *Modelo de Referência OSI*.

Disponível em: <http://www.jurumweb.com.br/artigos/artigos.php?artigo=000001>

Acesso em: 12 SET. 2005

13. MICROSOFT. *Point-Point Tunneling Protocol (PPTP) FAQ*.

Disponível em: <http://www.microsoft.com/na/server/ProductInfo/faq/PPTPfaq.asp>

em: 18 NOV. 2005.

6. REFERÊNCIAS BIBLIOGRÁFICAS

1. ARTHAS, Kael. **Redes Ponto a Ponto.**

Disponível em: <<http://www.babooforum.com.br/idealbb/view.asp?topicID=219678>> Acesso em: 09 AGO. 2005.

2. BATISTA, Thaís Vasconcelos. **Segurança em Redes de Computadores.** Natal, 2002.

Aula 1. Disponível em: <http://www.dimap.ufrn.br/~thais/Seguranca/home.html>>. Acesso em: 1 SET. 2005.

3. BATISTI, Júlio. **Introdução ao TCP/IP.**

Disponível em: <http://www.juliobattisti.com.br/artigos/windows/tcpip_p11.asp> Acesso em: 25 SET. 2005.

4. BOGO, Kellen Cristina. **A história da Internet – Como tudo começou.**

Disponível em: <<http://kplus.cosmo.com.br/materia.asp?co=11&rv=Vivencia>> Acesso em: 12 OUT. 2005

5. CARVALHO, Balparda Daniel de. **Criptografia: Métodos e Algoritmos.** 2º ed. Rio de Janeiro, Book Express, 2001.

6. CHIN, Liou Kuo. **Rede Privada Virtual (VPN).**

Disponível em: <<http://www.rnp.br/newsgen/9811/vpn.html>> Acesso em: 12 OUT. 2005

7. COMER, Douglas E. **Redes de computadores e Internet.** 2º ed. Trad. Marinho Marcelos. Porto Alegre. Bookman, 2001.

8. FERREIRA, Edwilson Tavares; ORTIZ, Eduardo Bellincanta. **Vpn - Virtual Private Network - Implementando Soluções com Linux.** 1º ed. São Paulo, Erica, 2003.

9. FONTES, Edson. **Política de Segurança da Informação.**

Disponível em: <<http://www.modulo.com.br>> Acesso em: 05 NOV. 2005

10. GASPARINI, Anteu Fabiano L; BARRELA, Francisco Eugênio. **A infra-estrutura de LANs disponibilidade (Cabling) e Performance (Switching e Rounting).** 1º ed. São Paulo, Érica, 1997.

11. JESUS, Marcolino Alexandre. **Criando VPNs entre servidores linux sem mistério**
Disponível em: <<http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=337>>. Acesso em: 09 AGO. 2005.

12. JÚLIO, Anderson Júlio. **Modelo de Referência OSI.**

Disponível em: <http://www.forumweb.com.br/artigos/artigos.php?action=file&id=268>>
Acesso em: 12 SET. 2005

13. MICROSOFT. **Point-Point Tunneling Protocol (PPTP) FAQ.**

Disponível em: <<http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp>> Acesso em: 18 NOV. 2005.

14. ORTIZ, Eduardo Bellincanta. VPN – Virtual Private Network – **Implementando Soluções com Windows 2000 Server**. 1º ed. Erica, 2002.
15. OPENVPN, Howto. Disponível em: <<http://OPENVPN.net/howto.html>> Acesso em: 25 NOV. 2005
16. ROSSI, Marco Antônio, FRANZIM, Oswaldo, **GPR Sistemas / ASP Systems**. <<http://www.gpr.com.br/download/vpn>> Agosto 2000. Acesso em: 10/09/2005
17. SILVA, Lino Sarlo da. **VPN: Virtual Network**. 1º ed. São Paulo, Novatec, 2002.
18. TANENBAUM, Andrew S. **Redes de computadores**. 3º ed. Trad. Insight serviços de Informática. Rio de Janeiro: Campus, 1997.
19. TECHNICAL, root. **Definição de protocolos**. Disponível em: <<http://www.techroot.org/modules/news/article.php?storyid=91>> Acesso em: 10 NOV. 2005.
20. TERADA, Routo. **Segurança de dados criptografia em redes de computadores**. 1º ed. São Paulo. Edgard Blucher, 2000.

7.1.1 Instalação

Pré-instalação:

LZO – biblioteca de compressão e descompressão para ser usado com o OPENVPN e que pode ser baixado deste site: <http://www.oberthur.org/openvpn/dependencies/>

Configurando o kernel:

Como exemplo foi utilizado o kernel 2.6.5, mas o mesmo deve ser feito com o kernel 2.4. É preciso ativar o driver TUN/TAP no kernel para que o OPENVPN funcione. Este é a única dependência dele para o seu funcionamento. Pode ser compilado dentro (incorporado ao kernel) ou como módulo, para ser usado quando necessário.

[*] Network device support

```

[*] Network device support
  < > ARCnet devices --->
  < > Dummy net driver support
  < > bonding driver support
  < > EQL (kernel based) support
  < > Ethernet 10/100/1000 device driver support
  < > Ethernet network tap (OBSOLETE)
  < > General Instruments Serialcard 1000
  < > Intel 82559 (i82559) --->

```

7. ANEXOS

7.1 IMPLEMENTAÇÃO DE UMA VPN EM LINUX USANDO OPENVPN

Esse capítulo tem como objetivo mostrar a implementação de uma VPN baseada em Linux utilizando o OPENVPN como ferramenta. Por ser um projeto *Open Source* este é um software estável, simples de configurar, além de ser um projeto que está sempre em desenvolvimento.

A VPN foi criada com intuito de interligar as redes internas de uma empresa, numa conexão VPN do tipo LAN-LAN (matriz e filial). Isto é, qualquer máquina da rede da matriz se conecta diretamente com qualquer máquina da rede da filial, sendo que ambas se localizam em lugares diferentes e bem distantes. Cada localidade da empresa ADSL rodando Linux como servidor e suas respectivas redes internas. Existem dois tipos de criptografia usadas na implementação OPENVPN, através de chaves estáticas criptográficas e no modo TLS, em que as chaves são trocadas periodicamente. Será demonstrado nesse exemplo OPENVPN SSL/TLS + RSA, por ser considerado o mais seguro. A seguir veremos os passos necessários para a instalação e configuração do software.

7.1.1 Instalação

Pré-instalação:

LZO – biblioteca de compressão e descompressão para ser usado com o OPENVPN e que pode ser baixado deste site: <http://www.oberhumer.com/opensource/lzo/>.

Configurando o kernel:

Como exemplo foi utilizado o kernel 2.6.5, mas o mesmo deve ser feito com o kernel 2.4. É preciso ativar o driver TUN/TAP no kernel para que o OPENVPN funcione. Esta é a única dependência dele para o seu funcionamento. Pode ser compilado *builtin* (incorporado ao kernel) ou como módulo, para ser usado quando necessário.

[*] Network device support

```

ARCnet devices --->
< > Dummy net driver support
< > Bonding driver support
< > EQL (serial line load balancing) support
<*> Universal TUN/TAP device driver support
< > Ethertap network tap (OBSOLETE)
< > General Instruments Surfboard 1000
Ethernet (10 or 100Mbit) --->

```

```

Ethernet (1000 Mbit) --->
[ ] FDDI driver support
[ ] HIPPI driver support (EXPERIMENTAL)
<*> PPP (point-to-point protocol) support
< > SLIP (serial line) support
Wireless LAN (non-hamradio) --->
Token Ring devices --->
[ ] Fibre Channel driver support
< > Red Creek Hardware VPN (EXPERIMENTAL)
< > Traffic Shaper (EXPERIMENTAL)
Wan interfaces --->

```

Nota: Para maiores informações sobre a compilação e configuração do Kernel do linux, acessar o site. <http://www.kernel.org>

A figura 33 mostra a instalação de todo pacote OPENVPN, juntamente com suas dependências, através do comando apt-get install, presente na distribuição *Debian* do Linux.

```

Arquivo Editar Ver Terminal Abas Ajuda
pruonckk@001-admin:/$ su
Password:
001-admin:/# apt-get install openvpn
Lendo Lista de Pacotes... Pronto
Construindo Árvore de Dependências... Pronto
Os NOVOS pacotes a seguir serão instalados:
  openvpn
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
E preciso fazer o download de 302kB de arquivos.
Depois de desempacotamento, 774kB adicionais de espaço em disco serão usados.
Obtendo:1 http://127.0.0.1 stable/main openvpn 2.0-1 [302kB]
Baixados 302kB em 0s (3573kB/s)
Pré-configurando pacotes ...
Selecione o pacote previamente não selecionado openvpn.
(Lendo banco de dados ... 72351 arquivos e diretórios atualmente instalados.)
Descompactando openvpn (de .../openvpn_2.0-1_i386.deb) ...
Instalando openvpn (2.0-1) ...
Restarting virtual private network daemon:.

001-admin:/#

```

Figura 33: apt-get install openvpn

Configurando a VPN no servidor (matriz)

A figura 34 abaixo mostra a criação da chave criptográfica de 2048bit do servidor, através do comando **#openvpn --genkey --secret /etc/openvpn/chave**. Essa chave serve para criptografar e descriptografar os dados que trafegam no túnel VPN.

Figura 34: Configuração do servidor

```

Arquivo  Editar  Ver  Terminal  Abas  Ajuda
001-admin:/# openvpn --genkey --secret /etc/openvpn/chave
001-admin:/#
001-admin:/# cd /etc/open
openoffice openvpn
001-admin:/# cd /etc/open
openoffice openvpn
001-admin:/# cat /etc/openvpn/chave
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
2784313d59d7906dee2d32f0fa46558b
33fff3cd2e3d69760d9a8aefc9025931
47f452012465c79c2b7d483b29e4b375
a05ca709a3b46df4481a95ac4437eb58
8127c859ece005054b09c4747c193b7f
91b7a99ceb017066b848aa3a75eb4ce7
49ffe022783f49950d0143323d9965b5
182f6b6a2864af59ae1f25ef8da9762c
cf765af32d47fe9d4ee198f2bdbbe8ae9
a9a5ad288cf42e432be63aaf8c1ca6de
e1da00c4ccab41b36306821721363d2a
37bce63d5af89867da00c487fa146ec4
047bb4a2dc70f5a1f1a8758978fed8de
4c10a2393da5b6fe410ef29c40732d13
b5fc0750b34777d0e953d6488f9af5b6
b3d3754416ea4fc5cab0f847f153b3ec
-----END OpenVPN Static key V1-----
001-admin:/#

```

Figura 34: Chave criptográfica do servidor

Conforme a figura 35 abaixo é criado o arquivo de configuração do servidor, através do arquivo servidor.conf, os comentários abaixo inseridos na própria figura, explica como tudo funciona.

Servidor.conf

```

# Usar como interface o driver TUN
dev tun
# 10.0.0.1 ip que será assumido na matriz
# 10.0.0.2 ip remoto, ou seja, esse será o ip da filial
ifconfig 10.0.0.1 10.0.0.2
# Entra no diretório onde se encontram os arquivos de configuração
cd /etc/openvpn
# Indica que esse túnel possui uma chave de criptografia
secret chave
# OpenVPN usa a porta 5000/UDP por padrão.
# Cada túnel do OpenVPN deve usar uma porta diferente, o padrão é porta a 5000
port 5000
# Usuário que rodará o daemon do OpenVPN
user nobody
# Grupo que rodará o daemon do OpenVPN
group nobody
Usa a biblioteca Izo
comp-izo
# Envia um ping via UDP para a parte
# remota a cada 15 segundos para manter
# a conexão de pé em firewall statefull
# Muito recomendado, mesmo se você não usa # um firewall baseado em statefull.
ping 15
# Nível de log
verb 3

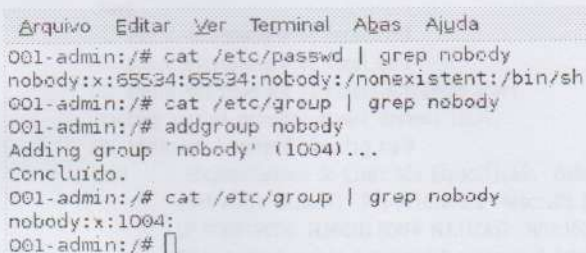
```

Figura: 35 Configuração do servidor

Em seguida será executado o comando abaixo que é responsável por iniciar a conexão do servidor.

```
# openvpn --config /etc/openvpn/matriz.conf--daemon
```

A figura 36 abaixo mostra se no conteúdo do arquivo de senhas (passwd), tem um grupo nobody que será o grupo default para execução da VPN.



```
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
001-admin:/# cat /etc/passwd | grep nobody
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
001-admin:/# cat /etc/group | grep nobody
001-admin:/# addgroup nobody
Adding group 'nobody' (1004)...
Concluido.
001-admin:/# cat /etc/group | grep nobody
nobody:x:1004:
001-admin:/#
```

Figura 36: Grupo nobody