HIRAN CAMARGO DE ARAÚJO

ACESSO REMOTO A SERVIDOR LINUX, VIA TERMINAL WINDOWS, UTILIZANDO VPN

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador: Prof. Emerson Rodrigo Alves Tavares

BARBACENA
2003

HIRAN CAMARGO DE ARAÚJO

ACESSO REMOTO A SERVIDOR LINUX, VIA TERMINAL WINDOWS, UTILIZANDO VPN

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 27 de novembro de 2003.

_____

Prof. Emerson Rodrigo Alves Tavares - Orientador do Trabalho

_____

Prof. Marcelo de Miranda Coelho - Membro da Banca Examinadora

_____

Prof. Eduardo Macedo Bhering - Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço primeiramente a Deus, a meus pais e a minha esposa e filha pela confiança em mim depositada em todos momentos. Agradeço também ao meu orientador pelos sábios conselhos dados a mim, aos meus colegas e a todos que de alguma forma me ajudaram durante o desenvolvimento deste trabalho.

RESUMO

Este trabalho mostra como implementar uma rede VPN (*Virtual Private Network*) ou Rede Privada Virtual por acesso remoto, utilizando a *Internet,* que possui clientes com a plataforma Microsoft Windows acessando um *gateway* de VPN com plataforma Linux. Foi utilizado para isso o protocolo L2TP (*Layer Two Tunneling Protocol*) sobre o protocolo IPSec (*IP Security*)visando um fluxo seguro de dados entre o *gateway* Linux e o cliente Windows. Este fluxo seguro é conseguido através do uso de criptografia nos pacotes de dados, autenticação dos clientes no *gateway* Linux e encapsulamento dos pacotes, formando assim o túnel VPN e possibilitando existir integridade, autenticidade, sigilo e outras premissas desejadas em uma VPN.

Palavras-chave: VPN, Tunelamento, Linux, Criptografia, *Firewall*, IPSec.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AH – *Authentication Header*
CHAP – *Challenge Handshake Authentication Protocol*
DDoS – *Distributed Denial of Service*
DoS – *Denial of Service*
ESP – *Encapsulation Security Payload*
GNU – *General Public License*
GRE – *Generic Routing Encapsulation*
IETF – *Internet Engineering Task Force*
IKE – *Internet Key Exchange Protocol*
IP – *Internet Protocol*
IPSec – *IP Security*
ISAKMP – *Internet Security Association and Key Management Protocol*
ISP – *Internet Service Provider*
ITU – *International Telecommunication Union*
LAC – *L2TP Access Concentrator*
LNS – *L2TP Network Server*
L2F – *Layer Two Tunneling Protocol*
L2TP – *Layer Two Tunneling Protocol*
MMC – *Microsoft Management Console*
NAS – *Network Access Server*
NAT – *Network Address Translation*
PNS – *PPP Network Server*
OSI – *Open Systems Interconnection*
PAC – *Protocol Access Concentrator*
PAP – *Password Authentication Protocol*
PKI – *Public Key Infrastructure*
PPP – *Point-to-Point Protocol*

PPTP – *Point-to-Point Tunneling Protocol*
PSK – *Pré-Shared Key*
RAS – *Remote Access Server*
SA – *Security Association*
SAD – *Security Association Database*
SKEME – *Secure Key Exchange Mechanism*
SPD – *Security Policy Database*
SPI – *Security Parameter Index*
TCP – *Transmission Control Protocol*
TCP/IP – *Transmission Control Protocol/Internet Protocol*
UDP – *User Datagram Protocol*
VPN – *Virtual Private Network*
WAN – *World Area Network*

1 INTRODUÇÃO

Durante a primeira década de sua existência, as redes de computadores foram principalmente usadas por pesquisadores universitários para enviar mensagens de correio eletrônico, por militares e por funcionários de organizações com o objetivo de compartilhar documentos, impressoras entre outros recursos. Sob estas condições de uso restrito a segurança não precisava de maiores cuidados. Mas, atualmente, como milhões de pessoas estão usando as redes para executarem operações bancárias, operações de comércio eletrônico e acesso remoto a informações confidenciais, a segurança das redes está despontando como um problema em potencial. [1]

Nos dias atuais, com a possibilidade de se trocar informações entre vários computadores, espalhados pelos pontos mais remotos do mundo, empresas vêem nesta possibilidade, a oportunidade de compartilhar informações com outras empresas, com filiais ou ainda com seus usuários móveis. Até bem pouco tempo, o compartilhamento de informações era feito através de redes WAN (*World* Area Network) ou rede geograficamente distribuídas, [1] utilizando-se soluções baseadas em linhas dedicadas oferecidas pelas operadoras de telefonia a um alto custo. [2]

As redes VPN surgiram como uma abordagem alternativa, motivada pelo lado financeiro, dado que *links* dedicados são caros se comparados ao acesso discado via provedor local, e também pela grande abrangência da *Internet* que possui um alcance mundial. Uma rede VPN consiste em uma rede privada que permite estabelecer conexões seguras utilizando protocolos de uma rede pública para a transmissão de dados, normalmente esta rede pública é a *Internet*. A rede VPN pode ser estabelecida de várias maneiras: entre dois *hosts*, uma rede e um *host* ou entre duas redes. A VPN utiliza a infra-estrutura da *Internet* exigindo apenas uma conexão (geralmente local) com um provedor de acesso a um custo muito menor que o aluguel de uma linha dedicada.[3]

Uma rede VPN necessita de uma política de segurança muito bem estruturada, de modo a garantir que as informações que transitaram através da rede estejam completamente seguras para atingirem o seu destino. A VPN utiliza os seguintes componentes: protocolos de tunelamento, para gerar um túnel virtual por onde os dados poderão trafegar de forma segura, *firewall*, propiciando uma barreira segura contra acessos indevidos, algoritmos de criptografia, que possibilitam garantir que os dados não serão alterados durante a transmissão entre outros que serão abordados no decorrer deste trabalho.[4]

O sistema operacional Linux é derivado do Unix e foi desenvolvido pelo finlandês Linos Torvalds, um estudante do Curso Ciência da Computação da Universidade de Helsinki. Linos lançou a primeira versão do kernel (núcleo) do sistema em março de 1992. O Linux é um sistema gratuito e é distribuído sobre o abrigo da GNU (*General Public License*) [5], assim não possui qualquer restrição quanto à sua distribuição e utilização.[6]

Como o Linux está crescendo na área de servidores, muitas empresas o estão adotando, pois, além de ser um sistema de baixo custo de aquisição, afinal é um sistema “gratuito”, ele é um sistema que oferece maior segurança se comparado com outros sistemas, sendo assim mais confiável e estável, desde que bem configurado.[7]

O sistema operacional Windows da Microsoft vem se caracterizando há muito tempo, por ser um sistema voltado as necessidades do usuário final, pois possui uma interface gráfica a princípio mais amigável que a do Linux ou Unix, com exceção das versões

2000/2003 *Server*. Desta forma, o Windows se tornou extremamente popular sendo utilizado pela maioria dos usuários comuns.[8]

Uma alternativa interessante, do ponto de vista econômico, para empresas de pequeno e médio porte que possuem muitos usuários móveis acessando sua rede interna, é usar VPN por acesso remoto com a *Internet* como meio de transmissão, Windows nos computadores dos usuários remotos e o Linux no *gateway* da VPN. Desta forma, os gastos com treinamento dos funcionários e licenças serão reduzidos, já que normalmente a grande maioria das pessoas já está familiarizada com o Windows e o sistema Linux usado no *gateway* é gratuito.

1.1 OBJETIVO

O objetivo deste trabalho é propor uma forma de implementação de rede VPN por acesso remoto utilizando-se Windows nos usuários remotos, Linux no *gateway* da VPN e a *Internet* como meio de transmissão de dados, procurando-se assim garantir a segurança dos dados transmitidos pela *Internet* entre o *gateway* e os usuários remotos da VPN.

2 ASPECTOS DE SEGURANÇA

Atualmente muitas empresas possuem informações sigilosas disponíveis em seus computadores, tornando necessário que cuidados especiais com a segurança destas sejam tomados, de forma que sejam protegidas contra acessos indevidos, por parte de pessoas mal intencionadas que não possuem autorização para acessar tais informações, podendo fazer uso destas contra a própria empresa.

Essa preocupação torna-se ainda maior com a popularização da *Internet* nas empresas, aumentando-se assim o risco das informações serem acessadas ou alteradas por pessoas não autorizadas, pois qualquer pessoa conectada à *Internet* pode vir a tomar posse destas informações, caso elas não estejam bem protegidas.

2.1 AMEAÇAS

Para tornar uma rede mais segura e confiável, deve-se estar atento às principais ameaças que podem comprometer a integridade das informações de uma empresa.

As principais ameaças [4] são: *hackers*, antigos funcionários ou funcionários insatisfeitos, parceiros *extranet* [3], usuários curiosos que querem ter posse de determinada informação para uso pessoal ou para benefício próprio, vírus e etc.

2.2 ATAQUES

Pode-se definir ataque como sendo uma técnica específica utilizada pelos *hackers* para explorar as vulnerabilidades existentes em sistemas computadorizados.[9]

Para saber como proteger as informações sigilosas de uma empresa é necessário entender primeiro como os ataques se classificam e quais os tipos mais usados freqüentemente, para que se possa utilizar o método correto de defesa em cada situação.

O fluxo normal da informação é mostrado na Figura 2.1, este é alterado durante a realização de um ataque.

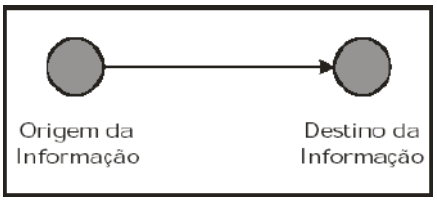

Figura 2.1**: Fluxo normal de uma informação [7].**

2.2.1 INTERRUPÇÃO

Nestes tipos de ataques o objetivo é interromper o serviço oferecido por um servidor ou *host*, ou seja, ataca-se a disponibilidade das informações, este está ilustrado na Figura 2.2.

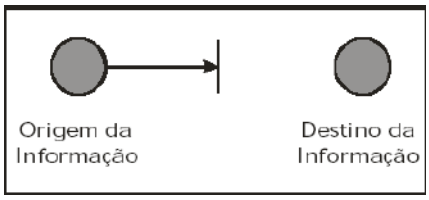

Figura 2.2**: Fluxo interrompido [7].**

O principal tipo de ataque classificado como interrupção é o DoS (*Denial of Service*) ou negação de serviço, que constitui do envio de requisições de serviço, em massa, para um determinado servidor ou *host*, de modo este não consiga responder todas as requisições, ficando assim sobrecarregado, fazendo com que o serviço não esteja disponível para a utilização. Uma evolução do DoS é o ataque DDos (*Distributed Denial of Service*) ou negação de serviço distribuída, neste o atacante amplifica o ataque DoS, engajando máquinas de múltiplas redes que estão conectadas à *Internet* aumentando assim o número de requisições enviadas ao servidor, deixando-o inoperante.

2.2.2 INTERCEPTAÇÃO

Este tipo de ataque tem como objetivo capturar os dados que estão sendo transmitidos sem que o sistema perceba, ou seja, ataca-se a confidencialidade das informações. Este está ilustrado na Figura 2.3.

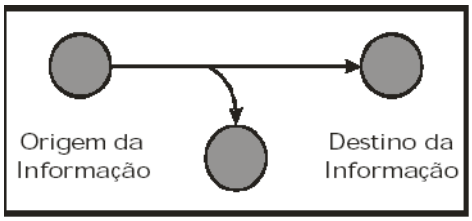

Figura 2.3**: Fluxo interceptado [7]**

Um dos principais ataques desta classificação é o *man-in-the-middle* (homem no meio), onde o invasor simula ser o parceiro de ambas as partes envolvidas na conexão, assumindo a identidade de um usuário válido e interceptando pacotes, passando a fazer parte da comunicação.

2.2.3 MODIFICAÇÃO

Este tipo de ataque acontece quando a informação recebida sofre algum tipo de alteração em relação à informação original. Na Figura 2.4, podemos perceber que uma entidade intercepta a informação após ser transmitida pela entidade de origem, modifica o seu

conteúdo e a envia posteriormente à entidade destino; a entidade interceptadora tenta desta forma fazer-se passar pela entidade remetente. Entende-se por entidade como sendo um *host* ou *gateway* da VPN.

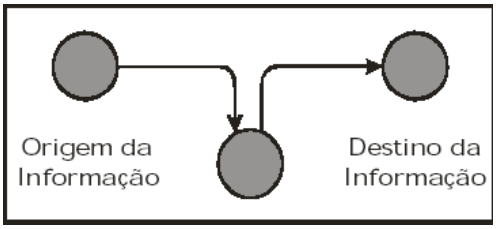

Figura 2.4**: Fluxo modificado [7]**

Um exemplo de ataque desta classificação é o *replay*, onde a totalidade ou parte de uma transmissão da rede é interceptada por um usuário não autorizado, sendo posteriormente retransmitida, simulando um usuário autorizado.

2.2.4 FABRICAÇÃO

Neste tipo de ataque, o atacante, não autorizado no sistema, tenta se passar por um usuário do sistema a fim de obter acesso a rede interna e poder transmitir dados na rede, este ataca a autenticidade da informação, conforme mostra a Figura 2.5.

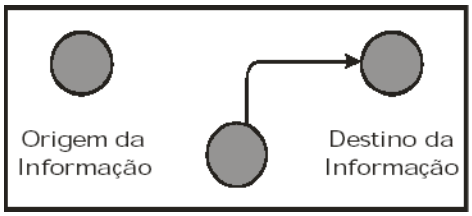

Figura 2.5**: Fluxo fabricado [7]**

O tipo de ataque mais comum de fabricação é o s*poofing*, que consiste na substituição do endereço IP (*Internet Protocol*) do computador do invasor, fazendo com que ele se passe por um usuário autenticado e confiável da rede, podendo assim, ter acesso à rede interna.

2.3 FORMAS DE DEFESA

2.3.1 FIREWALL

Os *Firewall*s são um conjunto de sistemas contendo uma ou mais máquinas/roteadores, situados entre uma rede privada e a *Internet*, com a função principal de interceptar todo o tráfego entre ambos, e com base na política de segurança interna, permitir ou não a passagem deste.[10]

Conforme o nível onde atuam na pilha de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) [1], os *firewalls* podem ser de três tipos diferentes: filtros de pacotes, que atuam no nível de rede e de transporte, inspeção de pacotes, que atuam nas camadas a partir do nível de rede para cima, e os *firewalls* de aplicação que atuam no nível de aplicação.

Os *firewalls* que utilizam filtros de pacotes podem ser implementados em hardware dedicado ou através de software em computadores de uso geral. Estes *firewalls* possuem a capacidade de efetuar a filtragem de pacotes com base nas informações do nível de rede, como endereço IP de origem e destino, protocolo de transporte, portas de origem e destino dos protocolos de transporte entre outros. Possui como vantagens ser mais barato e rápido que os outros tipos de *firewall*, uma vez que não examina o conteúdo dos pacotes, no entanto, justamente por fazer apenas uma filtragem superficial, acaba sendo mais inseguro que os outros.[10]

A inspeção de pacotes, além de desempenhar as funções do filtro de pacotes, analisa também 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. No entanto, possui configuração complexa e não fornece autenticação.[10]

Os *firewalls* de aplicação também chamados comumente de *proxy* são programas para uma aplicação específica, que têm a função de varrer todos os dados que passam por eles, descartando os perigosos ou não autorizados e nunca deixando a rede ficar exposta ao tráfego externo a ela. Possui como vantagens: oferecer a maior segurança dos três tipos de *firewalls*, além de autenticar as atividades dos usuários. Este também é o mais complexo dos três, por isso ele também é mais lento e mais caro que os demais. [10]

2.3.2 CRIPTOGRAFIA

A palavra criptografia tem sua origem no grego e vem das palavras *Kryptos* que significa escondido ou oculto e G*rifo* que significa grafia ou escrita. Então, pode-se definir criptografia como a arte ou ciência da escrita escondida, ou melhor, da escrita de mensagens codificadas ou cifradas com objetivo garantir o sigilo das informações contidas nas mesmas, de forma que apenas pessoas autorizadas a ler as mesmas possam ter acesso ao seu conteúdo. [11]

O processo de criptografia e decriptografia pode ser descrito da seguinte forma: o emissor deseja enviar uma mensagem, chamada de texto plano, utiliza então uma chave (combinação de bits) e um algoritmo de criptografia, combinando-os para gerar uma mensagem criptografada a partir da mensagem original, ou seja, uma mensagem incompreensível para quem não tiver autorização de ter acesso à mesma. Quando chega no receptor, a mensagem criptografada é então decriptografada por este que realiza o processo inverso ao feito pelo emissor, resultando deste processo então o texto plano original. Este processo é ilustrado pela Figura 2.6, onde a mensagem é criptografada na origem e decriptografada no destino.

Figura 2.6**: Criptografia e Decriptografia.[11]**

Existem dois tipos diferentes de criptografia, criptografia simétrica e criptografia assimétrica, dependendo diretamente do tipo de chave utilizada na criptografia. Os tipos de criptografia serão tratados a seguir.

2.3.2.1 Criptografia Simétrica

A criptografia simétrica baseia-se na simetria das chaves criptográficas, onde a mesma chave, é utilizada tanto para criptografar quanto para decriptografar a mensagem. Esta chave simétrica é comumente chamada de chave privada ou secreta, pois a força da criptografia simétrica é baseada no sigilo da chave que deve ser conhecida apenas por quem estiver autorizado a ler as mensagens. A chave deve ser previamente trocada entre o emissor e o receptor de forma segura, pois quem possuir a chave, possui também livre e irrestrito acesso ao conteúdo das mensagens. A Figura 2.7 ilustra este tipo de criptografia.

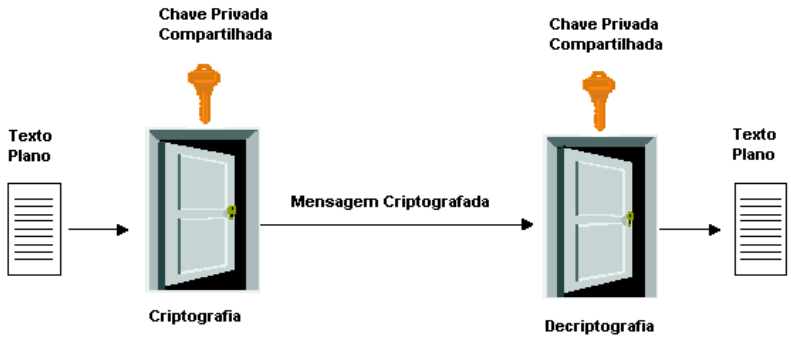

Figura 2.7**: Criptografia Simétrica.[11]**

2.3.2.2 Criptografia Assimétrica

A criptografia assimétrica, diferentemente da criptografia simétrica, utiliza duas chaves criptográficas distintas, uma chave privada e uma chave pública. Como o próprio nome já diz, a chave privada é secreta e a pública não. Assim, ambos emissor e receptor possuem duas chaves, uma privada (apenas ele conhece) e outra pública (com livre acesso).

Desta forma, o emissor utiliza a chave pública do receptor para cifrar a mensagem, e o receptor utiliza a sua chave privada para decifrá-la, este processo é ilustrado na Figura 2.8. [11]

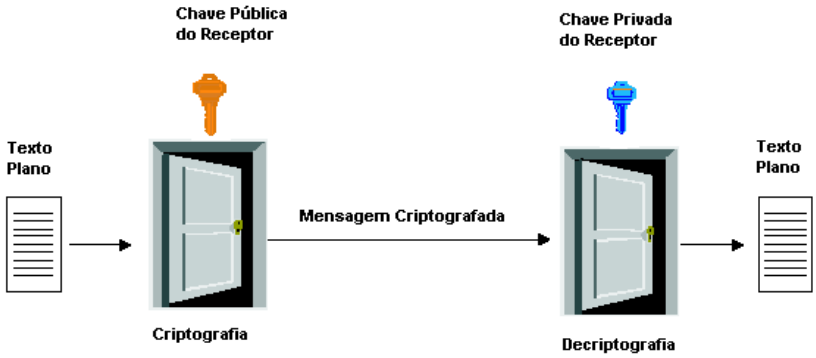

Figura 2.8**: Criptografia Assimétrica.[11]**

2.3.3 FUNÇÃO HASH

A função *hash* aplicada a uma dada mensagem tem como objetivo produzir um número, conhecido como resumo, que consegue representar de forma única esta mensagem. Assim, o emissor, antes de enviar a mensagem, realiza o cálculo da função *hash* e adiciona o resumo à mesma, quando esta chega ao receptor, este verifica o resumo contido na mensagem, através de novo cálculo da função *hash* sobre a mensagem recebida. Se o resumo obtido for igual ao contido na mensagem, esta é então aceita, caso contrário é descartada e um pedido de reenvio pode ser solicitado ao emissor, garantindo assim, a integridade dos dados contidos na mensagem. As funções *hash* funcionam de forma semelhante ao dígito verificador do CPF, assim, se um número qualquer do CPF for modificado, o dígito verificador também sofrerá alteração.[11]

2.3.4 ASSINATURA DIGITAL

A assinatura digital é um código binário que é determinado com base no documento e alguma outra informação, que associa este a uma determinada pessoa ou conjunto de pessoas. Essa associação é conhecida como autenticação e pode ser feita

basicamente de um ou mais dos seguintes três níveis: (1) algo que se sabe como uma senha; (2) algo que se possui como um cartão magnético e (3) algo que se é como uma medida biométrica. A associação considerada mais frágil é a primeira. A segunda é média e a terceira é a mais forte relação entre uma pessoa e a assinatura. Pode-se utilizar mais de uma dessas formas para aumentar o grau de associação.[11]

A assinatura digital utiliza a criptografia assimétrica, sendo a chave privada usada para assinar o documento, enquanto que a chave pública é usada para verificar a assinatura. O processo de geração da assinatura utiliza a função *hash* para a obtenção do resumo da mensagem, e em seguida, esta mensagem é cifrada com a chave privada do emissor que a envia ao receptor, este por sua vez, utiliza a chave pública do emissor para decifrar a mensagem e a função *hash* para recalcular o resumo da mensagem, comparando-o com o resumo anexo e garantindo a integridade da mensagem.[11]

2.3.5 CERTIFICADO DIGITAL

O certificado digital é um arquivo assinado eletronicamente por uma entidade confiável, chamada Autoridade Certificadora [10]. 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 Autoridade Certificadora pode examinar o conteúdo e confirmar a autenticidade de um certificado emitido por esta autoridade, uma vez que a Autoridade Certificadora assina os certificados com a sua chave privada.[11]

As seguintes informações estão presentes em um certificado digital: chave pública do usuário, número de série do certificado, nome da Autoridade Certificadora que emitiu o certificado, a assinatura digital da Autoridade Certificadora, entre outras.

A recomendação mais aceita e utilizada para a produção de certificados digitais é a X.509v3, formulada pela ITU (*International Telecommunication Union*) [12].

O presente capítulo introduziu os conceitos básicos, de segurança em VPNs, muito importantes o para a compreensão dos conceitos de VPN que serão abordados no próximo capítulo.

3 CONCEITOS VPN

Analisando o significado do termo Rede Privada Virtual pode-se dizer que a Rede é a infra-estrutura de comunicação entre computadores, que é Privada por garantir a confidencialidade e segurança dos dados que trafegam por ela e Virtual por unir computadores que estão fisicamente separados.

A VPN baseia-se na tecnologia de tunelamento, onde túneis virtuais são criados entre os pontos da VPN utilizando-se criptografia, com a finalidade de garantir que apenas os participantes da VPN poderão ter acesso aos dados que trafegam pela rede pública. A seguir serão analisados vários aspectos das VPNs.

3.1 TUNELAMENTO

O Tunelamento resume-se basicamente em encapsular pacotes de um protocolo em um pacote de outro protocolo. Esta técnica utiliza protocolos especiais chamados protocolos de tunelamento que utilizam técnicas de encapsulamento de dados para realização do tunelamento.

Os protocolos de tunelamento conhecidos atualmente atuam no nível de enlace ou de rede do modelo OSI (*Open Systems Interconnection*) [1]. Estes operam encapsulando pacotes de dados a serem transmitidos com um cabeçalho adicional, contendo informações de roteamento que serão necessárias para transportá-los através da rede intermediária, rede pública. Neste trabalho é usada a *Internet* como rede intermediária.

A *Internet* utiliza a pilha de protocolos TCP/IP [1] para a comunicação entre computadores. Porém antes desta ficar tão em evidência como hoje, algumas empresas utilizaram outros protocolos na rede interna. Para redes que não utilizam o protocolo IP, é necessário colocar ou encapsular o pacote da rede em questão dentro de um pacote-padrão TCP/IP [1]. Pode-se encapsular também o próprio IP dentro de outro IP, neste caso o objetivo é esconder o endereço IP de origem, podendo ser um IP válido ou não para a *Internet*. Um pacote IP é composto de cabeçalho (ou *header*) e os dados (*payload*). O encapsulamento consiste então, em gerar um novo cabeçalho IP com o datagrama original como *payload*, ou seja, o pacote original é considerado dado para o novo cabeçalho.[4]

Após o encapsulamento com IP os pacotes são transmitidos da rede origem, até à rede destino através da *Internet*, assim que os pacotes chegam ao destino, estes são desencapsulados, ou seja, é removido o cabeçalho IP adicional que foi utilizado para o roteamento e após isso, os pacotes são encaminhados à rede interna.

O tunelamento é ilustrado na Figura 3.1, onde um pacote é transmitido da empresa A até a empresa B, a este é adicionado um cabeçalho de roteamento contendo todas as informações de roteamento necessárias para o pacote trafegar pela *Internet*, estas informações são o endereço IP do pacote tanto de origem quanto de destino, tamanho do pacote, entre

outras. Após isso, o pacote é transmitido pela *Internet* até a empresa B. Assim que o pacote chegar na empresa B, é retirado o cabeçalho adicional e o pacote é enviado para a rede interna da empresa B.

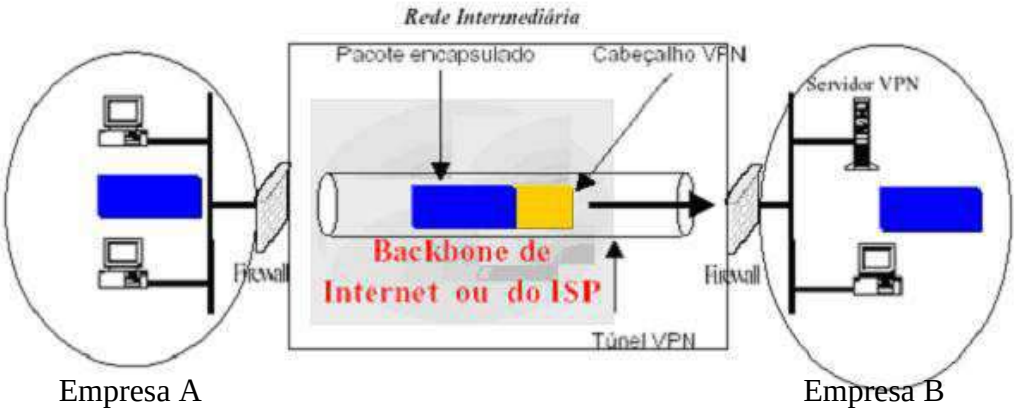

Figura 3.1 **– Tunelamento [2]**

3.1.1 TÚNEIS

Um túnel de VPN é a conexão ou o caminho lógico percorrido pelo pacote através da rede intermediária desde a rede de origem até a rede de destino.

A criação de um túnel VPN é tecnicamente conhecida como abertura de sessão de túnel. Para o estabelecimento de um túnel é necessário que nas extremidades da rede intermediária seja utilizado o mesmo protocolo de tunelamento. Entre os participantes da rede VPN os dados trafegam de forma segura dentro do túnel, impossibilitando assim qualquer acesso não autorizado. A segurança é garantida através do uso de algoritmos de criptografia de dados, impedindo desta forma que mesmo que o pacote seja interceptado, a leitura dos dados contidos nele, garantindo assim a privacidade na transmissão dos dados.[2]

Existem dois tipos de túneis: o túnel compulsório e o voluntário. O primeiro é automaticamente criado, sendo sempre iniciado pelo servidor de acesso remoto, quando for utilizando a VPN por acesso remoto, o segundo é iniciado pelo computador remoto sendo mais flexível para os usuários em trânsito ou móveis.

3.2 TOPOLOGIAS DE VPN

3.2.1 HOST – HOST

Esta topologia é usada para se conectar dois *hosts* com a finalidade de trocarem dados via *Internet* de forma segura, sendo que os *hosts* podem ou não estar presentes em uma rede. Um *host* é um computador que possui uma conexão com a *Internet*. Na Figura 3.2 é apresentada a conexão de dois *hosts* via *Internet*, utilizando roteadores e um túnel VPN para a troca de pacotes.[4]

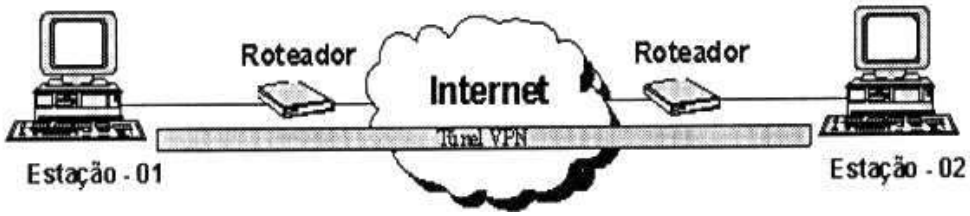

Figura 3.2 **- Topologia VPN Host-Host [4]**

3.2.2 HOST - REDE

A VPN por acesso remoto pode ser utilizada para conectar usuários móveis à rede local de uma empresa. Utilizar a *Internet* como meio de transmissão, através da conexão com um ISP (*Internet Service Provider*) ou provedor de acesso a *Internet*, livra a empresa da necessidade de manter bancos de modem para a conexão dos usuários móveis e diminui assim o gerenciamento destas conexões que acabam ficando centralizadas apenas no *gateway* da VPN. Um usuário remoto pode realizar uma conexão com um ISP recebendo deste um endereço IP, válido e dinâmico, possibilitando a ele trafegar pela *Internet*. Assim, por meio

desta conexão, o usuário remoto pode solicitar a autorização para estabelecer um túnel VPN com o *gateway*. Para efetuar a conexão o usuário remoto deve ter instalado e configurado em seu computador um protocolo de tunelamento que possua suporte à criptografia e autenticação de dados, e seja este protocolo o mesmo utilizado pelo *gateway* da VNP que ele deseja estabelecer o túnel.[4]

Após o usuário remoto ter se conectado ao ISP, ele pode se autenticar no *gateway* da VPN que verifica a sua autenticidade e permite ou não estabelecer o túnel VPN. Se a resposta for positiva o túnel VPN é criado, possibilitando ao usuário e ao *gateway* trocar pacotes criptografados e autenticados através da *Internet*.[4]

A Figura 3.3 exemplifica uma VPN por acesso remoto, onde o usuário Remoto – 01 se conecta a um ISP e solicita a criação de um túnel ao *gateway* VPN da Filial. O *gateway* então autentica o usuário, autorizando a criação do túnel. Após a criação do túnel o usuário está apto a enviar e receber pacotes do *gateway*.[4]

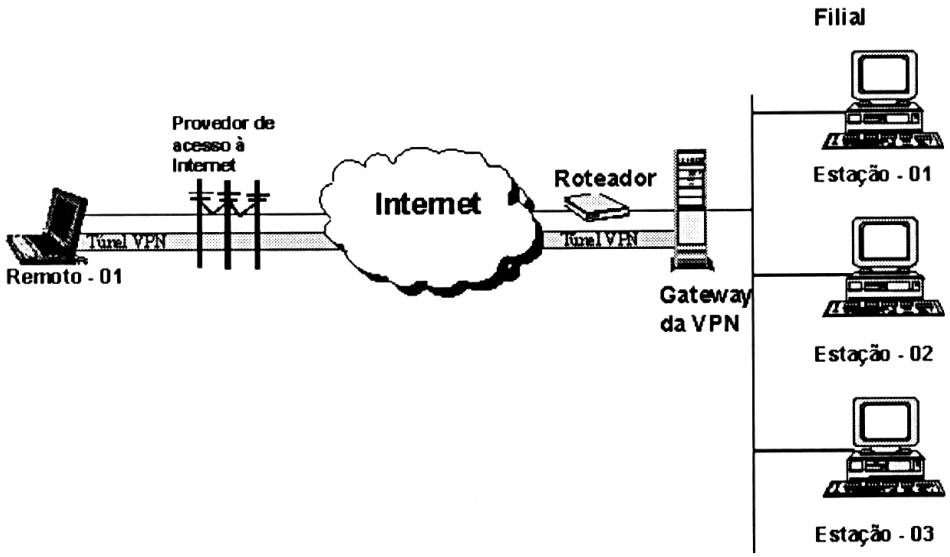

Figura 3.3 **- Topologia VPN Host – Rede [4]**

3.2.3 REDE - REDE

Esta VPN é utilizada na comunicação entre duas redes. O *gateway* da VPN é responsável por decidir, neste caso, que usuários poderão navegar na *Internet* e quais vão se

inscrever no túnel VPN. Diferente do que acontece na VPN por acesso remoto, a criação do túnel é completamente transparente ao usuário. Neste tipo de VPN, os dados só são transmitidos com segurança através do túnel VPN, ou seja, os pacotes de dados que não forem da VPN e trafegam de dentro da rede interna para a *Internet* e da *Internet* para a rede interna não estão protegidos pela VPN.[4]

A Figura 3.4 ilustra uma VPN interligando as redes de duas filiais de uma empresa, a filial – A comunica-se com a filial – B através do túnel VPN criado entre os dois *gateways*, onde estes são responsáveis pela criação do túnel VPN utilizando protocolos de tunelamento.

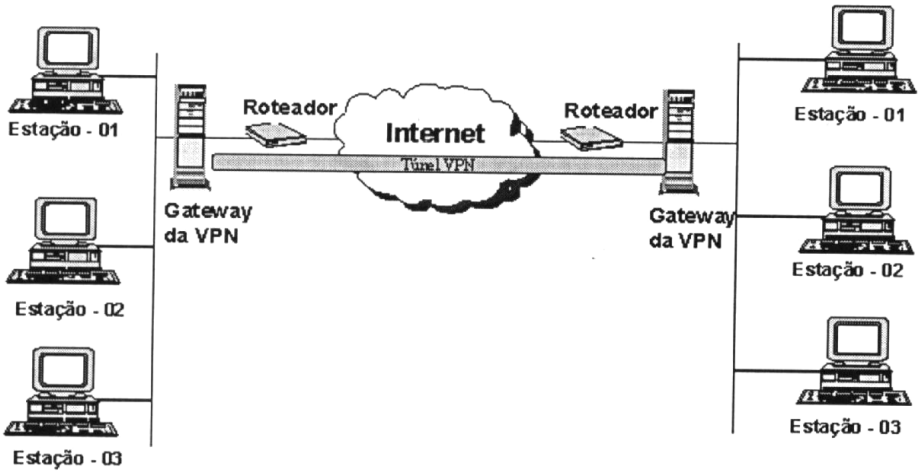

Figura 3.4 **- Topologia VPN Rede - Rede [4]**

3.3 RISCOS PROTEGIDOS PELA VPN

Quando falamos em segurança de dados e informações, é muito importante que se especifique de forma clara quais dados e informações necessitam ser realmente protegidos e quais não precisam de proteção. Uma pergunta muito importante é: Como valorizar o que estamos protegendo? A resposta a esta pergunta não é uma tarefa das mais fáceis. É importante nesse caso usar o bom senso pois, não se pode ser extremista a ponto de que seja necessário um cartão magnético para usar o elevador da empresa. O bom senso ensina a olhar a empresa como um conjunto maior e a separá-la em subconjuntos, ou seja, os grupos de

pessoas dentro da empresa que trocam determinados tipos de informações. Uma vez divididos os grupos, é necessário analisar o fluxo da informação, ou seja, de onde vai e para onde vai, quem pode ter acesso a esta informação e quanto esta informação é importante para a empresa. Desta forma pode-se estabelecer uma VPN entre os grupos, separados anteriormente, e cada membro pode se inscrever em uma ou mais VPNs se for o caso. Desta forma se pode concluir que algumas premissas em uma VPN devem ser consideradas.[4]

3.3.1 PREMISSAS DA VPN

3.3.1.1 Privacidade

O conceito de privacidade em VPN é bem parecido com o que se tem na vida cotidiana. Esta premissa visa garantir que dados trafegando pelo túnel VPN apenas possam ser visualizados e manipulados por participantes da VPN devidamente autenticados. Assim mesmo que os dados sejam interceptados por um usuário não autorizado, estes não poderão ser vistos ou utilizados. A privacidade em uma VPN é garantida através da implementação de criptografia. Esta é usada para criptografar o dado antes do envio, e para decriptografar quando o dado atinge o outro extremo do túnel VPN.[4]

3.3.1.2 Integridade

A integridade quando implementada, visa garantir que um dado enviado através do túnel VPN chega na outra extremidade do túnel sem sofrer nenhum tipo de alteração. Sendo assim, o dado que foi recebido é idêntico ao que foi enviado. A integridade do dado é obtida por meio da utilização de funções *hash*.[4]

3.3.1.3 Autenticidade

A autenticidade visa garantir que o remetente da mensagem é realmente quem disse ter enviado, ou seja, quando um pacote é recebido tem-se certeza de quem foi que o enviou. A autenticidade é obtida por meio de assinaturas digitais.[4]

3.3.1.4 Não – repúdio

O não-repúdio visa garantir que um usuário que enviou uma mensagem não possa dizer que não seja ele o remetente da mensagem em questão. O não-repudio é uma etapa executada após a autenticação (ou um atributo opcional da autenticidade) que só pode ser implementada via criptografia assimétrica.[4]

3.3.1.5 Controle de Acesso

O controle de acesso tem por finalidade limitar o acesso e a utilização de recursos disponíveis. Apenas a pessoas autorizadas e com privilégios de acessar determinado recurso do sistema.[4]

3.3.1.6 Disponibilidade

Visa manter os recursos disponíveis mesmo em caso de ataques ou panes no sistema. [4]

3.4 VPN E *FIREWALL*

A VPN é uma tecnologia que possibilita conectar várias redes, sendo muito útil na proteção dos dados, porém, a segurança não se limita a uma única tecnologia, mas a uma integração de várias tecnologias com políticas de gestão e fornecendo uma combinação equilibrada de proteções e riscos aceitáveis. Desta forma, a utilização da VPN juntamente com o *firewall* torna-se atraente para garantir um nível maior de segurança a VPN. Desta forma, é necessário um planejamento prévio cuidadoso antes de escolher a melhor opção para ser implementada, podendo ser as seguintes:

3.4.1 *GATEWAY* VPN INTEGRADO AO *FIREWALL*

Esta é a situação ideal e está ilustrada na Figura 3.6, pois pode atender a todos os requerimentos de segurança, tais como:

- Proteção de ataques vindos da *Internet* por parte *firewall;*

- Controle de acesso de todo o tráfego, como o *firewall* e o *gateway* compartilham informações de usuários. Pode-se definir quais serviços cada usuário pode acessar e todo o tráfego pode ser analisado, após decriptografado pelo *firewall*;

- Gerência centralizada simplificando a gerência, principalmente se houver muitos *firewalls* e *gateways*;

- *Logs* consolidados. Apenas nesta opção rede, objetos, usuários, serviços entre outros, podem ser compartilhados com o *gateway* e o *firewall* mantendo-se um registro em log de todos os acessos;

- Arquiteturas escaláveis, uma solução integrada pode ser aplicada à uma rede VPN sem muito esforço;

- Roteamento simplificado elimina a necessidade em se manter uma tabela de rotamento para cada um *gateway* e *firewall* da VPN;

- Performance, uma solução integrada pode se tornar pouco eficiente, porém no mercado existem soluções que aceitam hardware com acelerador de criptografia e gerência de banda integrada, desta forma o tráfego VPN pode ser priorizado ou não, dependendo da situação.

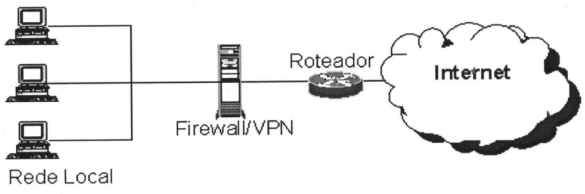

Figura 3.6 **– *Gateway* VPN integrado com *Firewall* [4]**

3.4.2 *GATEWAY* VPN EM FRENTE AO *FIREWALL*

Esta opção tem como sua idéia principal permitir que o tráfego VPN seja analisado pelo *firewall* somente depois que sai da VPN, ilustrada na Figura 3.7. Entretanto, o *gateway* fica exposto, ou seja, sujeito a qualquer tipo de ataque, sendo assim, caso falhe, todo o tráfego pode parar, tornando toda a VPN indisponível. Nesta opção ainda, não existe controle de acesso, um usuário pode se conectar ao *gateway* que decriptografa os dados e repassa-os para o *firewall* sem qualquer tipo de análise dos serviços ou portas que o usuário pode acessar. Para que o *firewall* analise o perfil do usuário é necessário que o usuário seja autenticado duas vezes, uma no *gateway* e outra no *firewall*, pois o *gateway* não compartilha informações de usuários.[4]

Outro ponto a se analisar é que o *firewall* e o *gateway* podem vir a ser de fabricantes diferentes, tornando mais difícil, a gerência e configuração da VPN.[4]

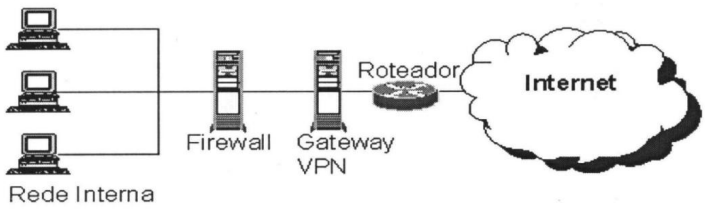

Figura 3.7 - ***Gateway* VPN em frente ao *Firewall* [4]**

3.4.3 *GATEWAY* ATRÁS DO *FIREWALL*

Esta opção trata o problema do *gateway* ficar exposto a ataques vindos da *Internet*, pois o *firewall* o protegerá dos ataques que possam ocorrer e é ilustrada na Figura 3.8.

Como o *firewall* está antes do *gateway*, este deve deixar passar todo o tráfego da VPN, este tráfego não é analisado pelo *firewall*, mas sim pelo *gateway* depois de passar pelo *firewall*. Desta forma, o *gateway* fica vulnerável a ataques. A gerência do *firewall* e do

gateway pode se tornar penosa se os equipamentos forem de fabricantes diferentes, tornando mais difícil, a gerência e configuração da VPN.[4]

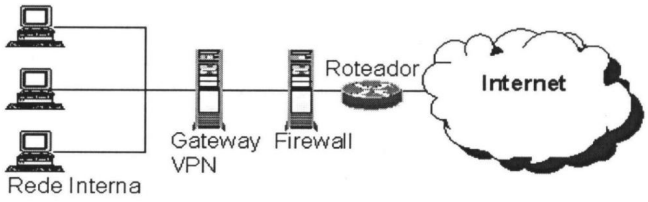

Figura 3.8 **– *Gateway* VPN atrás do *Firewall* [4]**

3.4.4 *GATEWAY* VPN EM PARALELO AO *FIREWALL*

O objetivo desta opção é separar o tráfego da VPN do tráfego comum vindo da *Internet*. Sendo assim, o tráfego VPN não passa pelo *firewall* e nem o *gateway* trata outro tráfego que não seja o da VPN. Novamente, o *gateway* está exposto a ataques, não existe controle de acesso e o usuário tem que se autenticar duas vezes, pois o *gateway* não compartilha informações dos usuários. Esta opção é ilustrada na Figura 3.9.[4]

Para que esta opção seja viável é necessário que o *gateway* VPN tenha funcionalidades de NAT (*Network Address Translation*) [4], bem como suporte a um conjunto de endereços IP distribuídos aos usuários. Esta opção requer um esquema de roteamento complicado, causando aborrecimentos ao administrador da rede.

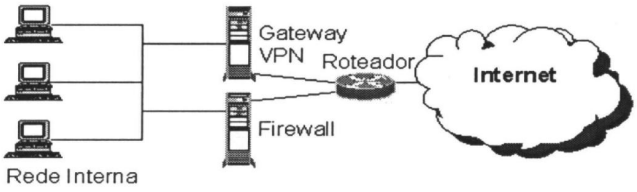

Figura 3.9 **– *Gateway* VPN em paralelo ao *Firewall* [4]**

3.4.5 *GATEWAY* VPN NUMA INTERFACE DO *FIREWALL*

Nesta opção, todo o tráfego que entra ou que sai pela *Internet* obrigatoriamente é analisado pelo *firewall.* Este recebe e envia dados ao *gateway.* O *gateway* é responsável por tratar o tráfego da VPN. Esta opção possui a vantagem de o *gateway* estar protegido contra ataques pelo *firewall*, mas em contrapartida possui as seguintes desvantagens: possibilidade dos equipamentos serem de fabricantes diferentes, dificuldade na auditoria, sendo difícil rastrear o acesso feitos por usuários, queda de performance, pois, toda comunicação passa duas vezes pelo *firewall* e a re-autenticação de usuário, forçando este se autenticar duas vezes. A Figura 3.10 ilustra esta opção.[4]

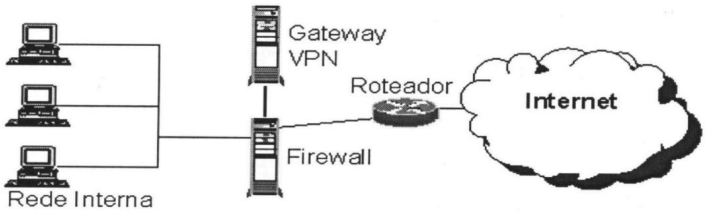

Figura 3.10 **– *Gateway* VPN numa interface do *firewall* [4]**

3.5 PROTOCOLOS DE VPN

Os protocolos de VPN são comumente chamados de protocolos de tunelamento e têm a função de garantir a segurança dos dados que trafegam pela VPN.

Existem dois conjuntos de protocolos de tunelamento: os orientados a pacotes, que trabalham nas camadas enlace, rede e transporte do modelo OSI [1] e os protocolos orientados a aplicação, que operam nas camadas da sessão, apresentação e aplicação do mesmo. Os protocolos orientados a aplicação são mais eficientes em matéria de privacidade e autenticidade, mas não fazem encapsulamento dos pacotes. Já os protocolos orientados a pacotes, são naturalmente a melhor opção, porque trabalham nas camadas de enlace e rede, onde os pacotes são montados e desmontados para recebimento e envio respectivamente. A questão da privacidade e autenticidade é mais explorada dentro do protocolo IPSec, este é

orientado a pacotes, mas agrega funcionalidades específicas para resolver problemas antes solucionados apenas nos protocolos orientados à aplicação.[4]

Na Figura 3.11 são apresentados os protocolos distribuídos nas camadas do modelo OSI [1].

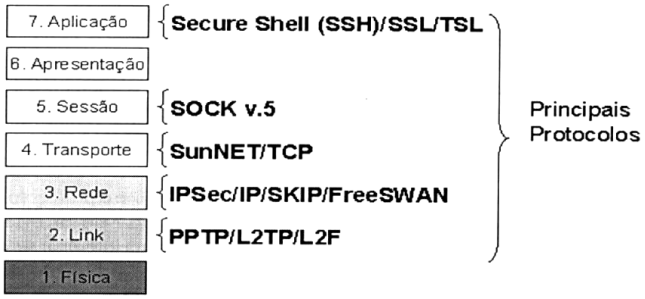

Figura 3.11 **– Distribuição dos protocolos por camadas [4]**

3.5.1 PPP (*Point-To-Point Protocol*)

Este protocolo constitui a forma mais popular de conectar computadores, sob linha serial ou discada. Para estabelecer uma conexão VPN, um usuário remoto deve configurar uma conexão PPP entre o computador remoto e o RAS (*Remote Access Server*) ou servidor de acesso remoto. Estabelecida a conexão, o computador remoto se torna capaz de enviar pacotes IP dentro de *frames* PPP ao RAS. Este por sua vez recebe os *frames* PPP vindos da *Internet*, retira o cabeçalho PPP e envia o pacote IP para a rede interna, a Figura 3.12 ilustra como é conexão PPP.[4]

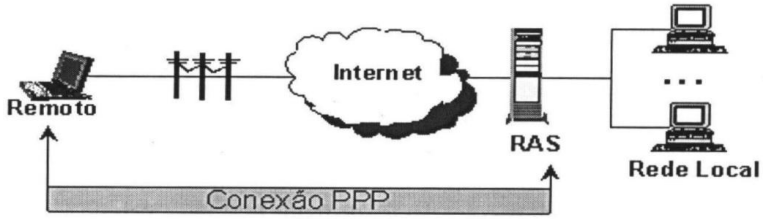

Figura 3.12 **– Conexão PPP [4]**

O protocolo PPP exige que empresa que o utiliza possua um conjunto de modems para acesso discado em quantidade suficiente para atender a todos os usuários remotos. Desta forma o usuário para realizar a conexão deve fazer ligação telefônica para o RAS. Neste caso o túnel criado entre o usuário remoto e o RAS é chamado túnel voluntário, porque o túnel só é estabelecido a pedido do usuário remoto quando este quiser acessar a rede interna.

A Figura 3.13 mostra um modelo padrão PPP, onde o protocolo de tunelamento é dividido em duas partes, uma que fica no cliente chamada PAC (*Protocol Access Concentrator*) com a função de encapsular os pacotes IP em *frames* PPP e estes dentro de algum protocolo que seja roteável na *Internet*, como o IP, já no servidor PPP da rede interna o PNS (PPP *Network Server*), possui a função de retirar dos *frames* PPP os pacotes IP e enviar à rede interna. [4]

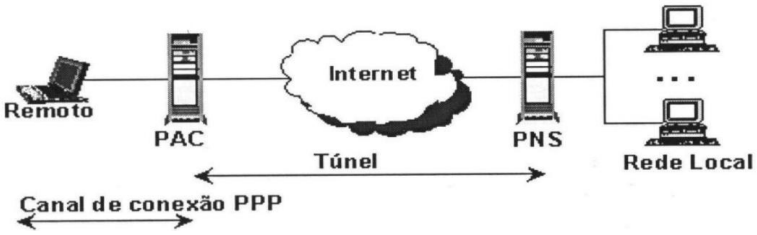

Figura 3.13 **– Modelo – padrão do PPP [4]**

3.5.2 PPTP (*Point-to-Point Tunneling Protocol*)

Este protocolo foi desenvolvido pelo fórum PPTP que incluiu empresas como a *Microsoft*, *Ascend Communication*, *US Robotics* e *ECI Telematics*. Esse fórum tinha por objetivo facilitar o acesso de computadores remotos a numa rede privada utilizando a *Internet* ou outra rede baseada no protocolo IP. Por se tratar de uma extensão do PPP o PPTP, só funciona em conjunto com o servidor de acesso remoto da Microsoft [4].

O PPTP encapsula pacotes PPP utilizando uma versão modificada do GRE (*Generic Routing Encapsulation*) ou protocolo de encapsulamento genérico [9], que suporta outros tipos de protocolos além do IP.

O protocolo PPTP não inclui privacidade e nem gerencia chaves de criptografia, sendo recomendado a utilização do IPSec para esta finalidade. Já a autenticação fica por conta do próprio RAS que suporta vários protocolos de autenticação.

A Figura 3.14 apresenta uma conexão PPTP, onde existem três entidades envolvidas: o cliente PAC, o NAS (*Network Access Server*) e o servidor PPTP. O usuário remoto conecta-se primeiramente a um NAS por meio de uma ligação discada a um ISP, usando o protocolo PPP nesta conexão os usuários enviam pacotes IP encapsulados em

frames PPP, que recebem ainda um cabeçalho GRE. Outro cabeçalho IP é adicionado e por último todo o pacote é encapsulado novamente dentro de um *frame* PPP até o NAS; em seguida uma segunda conexão é estabelecida sobre a conexão PPP, interligando o servidor PPTP ao usuário remoto; nesta é retirado o último cabeçalho PPP e os pacotes com cabeçalho IP são enviados do usuário até o servidor PPTP.

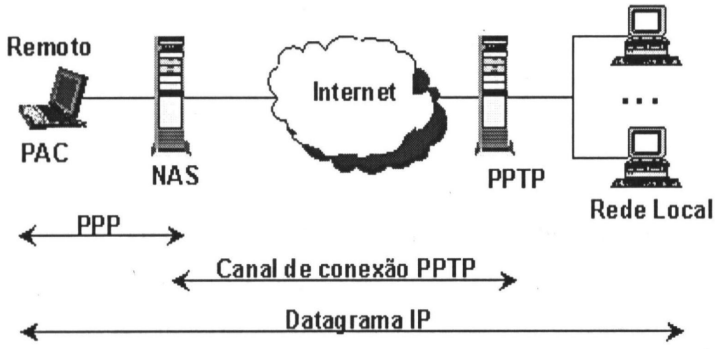

Figura 3.14 **– Conexão PPTP [4]**

3.5.3 L2F (*Layer Two Forwarding Protocol*)

O protocolo L2F foi lançado em 1996 pelas empresas, *Cisco, Northern, ECI Telecom* , 3Com e a *Shiva Corporation*, com a finalidade de possibilitar aos provedores de acesso ou empresas de telecomunicações oferecerem acesso remoto discado à redes privadas de empresas. Assim, as empresas não precisariam possuir um conjunto de modems e equipamentos para o acesso remoto, mas sim pagar pelo serviço [4] [13].

A Figura 3.15 ilustra o funcionamento do L2F, que é bem parecido com o do PPTP. A grande diferença entre os dois é que no L2F o término do túnel sempre possui um *gateway* ou f*irewall* antes da rede interna. No L2F, o usuário remoto conecta-se a um ISP através de uma ligação discada local e o NAS autentica este usuário utilizando o CHAP (*Challenge Handshake Authentication Protocol*) ou PAP (*Password Authentication Protocol*) [14]. Durante a autenticação, o NAS cria o túnel com o *gateway*, possibilitando ao usuário remoto enviar a receber datagramas IP. Neste caso, como o túnel é criado pelo próprio provedor e não pelo computador remoto, este é um túnel compulsório.

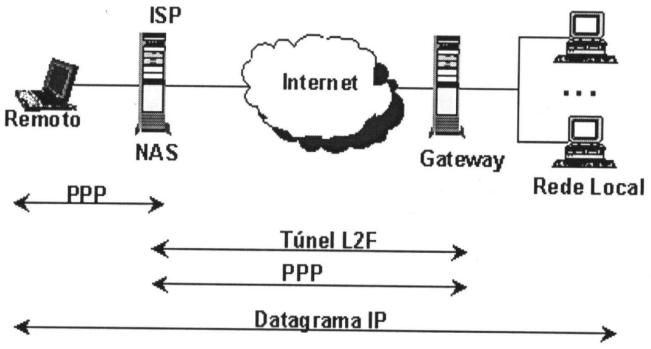

Figura 3.15 **– Conexão L2F [4]**

O L2F usa qualquer protocolo orientado a pacotes que suporte conexão ponto-a-ponto. A grande desvantagem do L2F, como no PPTP, é a ausência de criptografia e encapsulamento de dados.

3.5.4 L2TP (*Layer Two Tunneling Protocol*)

Este protocolo foi criado com o intuito de unir o que há de melhor no L2F e PPTP.

O IETF (*Internet Engineering Task Force*) [15] em conjunto com os criadores do L2F foi o órgão que ficou encarregado desta tarefa, propondo o L2TP como protocolo padrão para acesso remoto para VPN.

A Figura 3.16 mostra o funcionamento do L2TP, sendo bem similar ao PPTP, possuindo um LAC (*L2TP Access Concentrator*) que faz o papel do PAC no PPTP e o LNS (*L2TP Network Server*) que realiza o mesmo papel do servidor PPTP. Por outro lado, diferentemente do PPTP, o L2TP não usa conexão TCP (*Transmission Control Protocol*) [1] separada para o controle de canal, utilizando para isso o mesmo pacote L2TP. Finalmente o PPTP usa o GRE para encapsulamento e o L2TP o protocolo UDP (*User Datagram Protocol*) [1] (porta 1701).

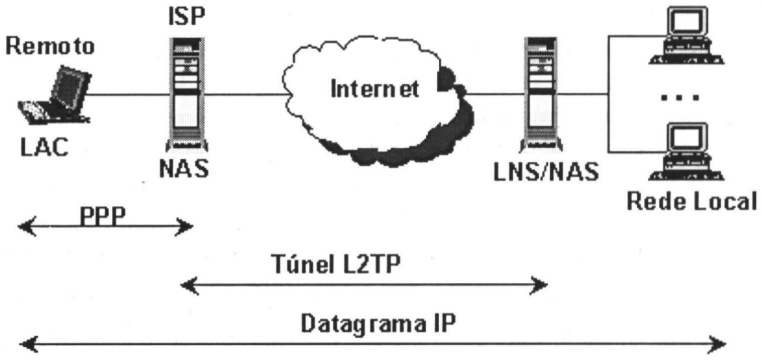

Figura 3.16 **– Conexão L2TP [4]**

O L2TP foi desenvolvido para utilizar os dois modos de túnel, tanto o compulsório quanto o voluntário. Este último possui a vantagem de ser mais flexível para usuários em trânsito pois, podem discar para qualquer provedor de acesso local. No túnel compulsório, devido ao fato do túnel ser completamente gerenciado pelo NAS, não há necessidade de existirem softwares específicos no computador remoto sendo o processo de tunelamento completamente transparente ao usuário remoto [4].

O protocolo L2TP, bem como PPTP e L2F, não possuem mecanismos sólidos de proteção ao túnel. O L2TP encapsula *frames* PPP, porém não possui um mecanismo de gerência de chaves criptográficas e autenticação. Assim, para minimizar esta deficiência, o L2TP faz o uso do IPSec para criptografia e gerenciamento de chaves. Esta opção é usada na implementação de VPN proposta neste trabalho [4].

3.5.5 IPSEC (*IP Security*)

O IPSec é um conjunto de protocolos desenvolvidos pela IETF [15], que define a arquitetura e especificações para prover serviços de segurança ao protocolo IP. O IPSec foi padronizado para garantir interoperabilidade, mecanismos de criptografia para IPv4 e para a próxima geração do protocolo IP o IPv6. O IPSec também define um conjunto de serviços de segurança, incluindo integridade de dados, autenticação, confidencialidade e limite de fluxo de tráfego. O IPSec oferece todos estes serviços independentemente do algoritmo de

criptografia usado, desta forma o IPSec se torna mais flexível sendo possível a inclusão de outros algoritmos de autenticidade e criptografia.

3.5.5.1 Protocolos do IPSec

O IPSec utiliza dois protocolos para prover todos os seus serviços de segurança: o *Authentication Header* e o *Encapsulation Security Payload*.

3.5.5.1.1 Authentication Header

O protocolo *Authentication Header* ou AH é utilizado pelo IPSec para garantir autenticidade e integridade aos dados durante a transmissão. Este oferece proteção para ataques do tipo *replay*, *spoofing* e *man-in-the-middle*. A Figura 3.17 descreve os campos utilizados pelo AH na autenticação.[4]

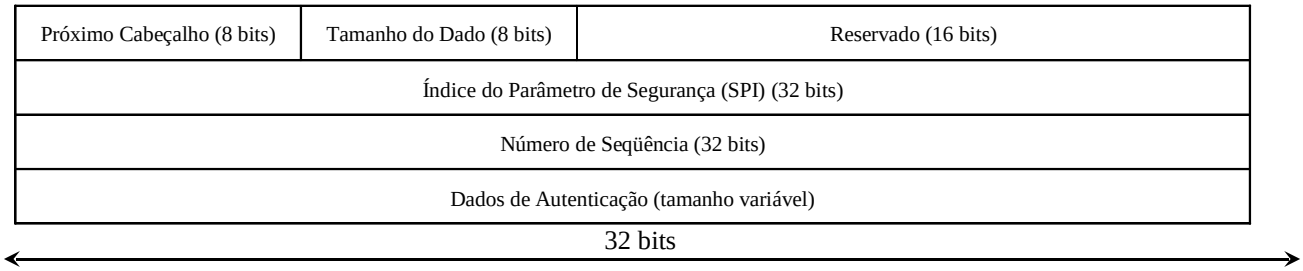

Figura 3.17 **– Formato do protocolo AH [4]**

A autenticação é realizada utilizando-se a função *hash* juntamente com a chave negociada durante o processo de estabelecimento da SA. O resultado da função *hash* nada mais é do que um *checksum* do conteúdo de alguns campos do cabeçalho IP e do *payload*.

Embora a autenticação seja realizada sobre o pacote IP, nem todos os campos deste podem ser autenticados, pois alguns campos alteram seus valores durante a transmissão e são chamados de mutantes ou variáveis, recebendo valor zero para o cálculo do *checksum*.

No outro extremo do túnel VPN a entidade que receber o pacote calcula o *hash* novamente e compara o resultado com o recebido. Se os dois forem idênticos, a autenticação está funcionando corretamente, caso contrário existe alguém ou algum equipamento

interferindo na comunicação. Este processo de verificação só pode ocorrer se o pacote não estiver fragmentado. Caso esteja, é necessário desfragmentá-lo antes do cálculo do *hash*.

Modo Transporte AH

Neste modo, o cabeçalho original do pacote é mantido no novo pacote IP gerado e um cabeçalho de autenticação é inserido entre o cabeçalho original e a parte de dados. A Figura 3.18 ilustra este processo.

No cabeçalho original apenas o campo protocolo é alterado, recebendo o valor 51 referente ao protocolo AH e o valor original do campo protocolo é colocado dentro do cabeçalho de autenticação, com o intuito de restabelecer o valor original do campo protocolo quando o pacote chegar ao seu destino final. Como o cabeçalho original é utilizado na transmissão, os equipamentos que possuírem o endereço IP de origem e destino devem utilizar o modo transporte do protocolo AH.

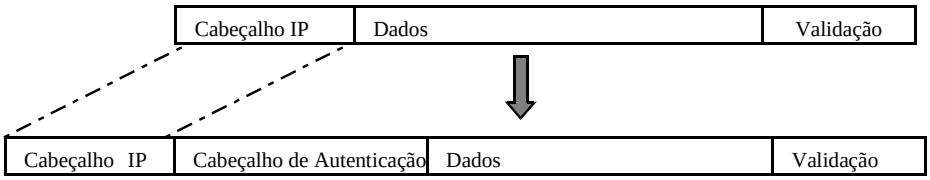

Figura 3.18 **– Modo Transporte no protocolo AH [4]**

Modo Túnel AH

Neste modo, um novo cabeçalho é criado para o da VPN e o cabeçalho de autenticação é inserido entre o cabeçalho original e o novo cabeçalho. A Figura 3.19 exemplifica este processo. Neste caso, o pacote IP original permanece intacto sendo encapsulado em um novo pacote IP, autenticando-se assim todo pacote IP original. Como o pacote original não é alterado, os endereços de origem e destino, permanecem também inalterados. Assim, os endereços origem e destino passam a ser os do dispositivo IPSec (*gateway* da VPN). A desvantagem neste modo é que existe mais processamento envolvido para se construir o pacote e voltá-lo para a sua forma normal.

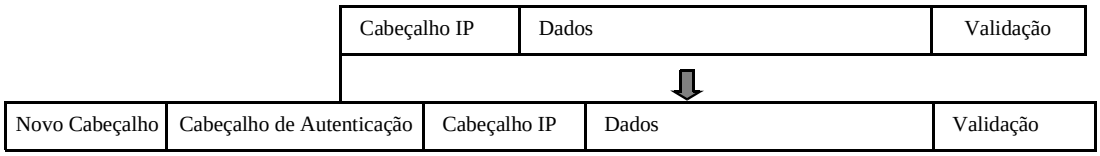

Figura 3.19 **– Modo Túnel no protocolo AH [4]**

O protocolo AH adiciona autenticação, porém não se preocupa com a confidencialidade. Sendo assim, os dados trafegam pela rede desprotegidos podendo ser capaturados por pessoas não autorizadas.

3.5.5.1.2 Encapsulation Security Payload

Este protocolo *Encapsulation Security Payload* ou ESP prove autenticação, protegendo contra ataques de *replay* e confidencialidade.

Como o pacote IP é um datagrama, é necessário que cada pacote contenha informações de criptografia com a finalidade de garantir o sincronismo da mesma, permitindo que a descriptografia possa ocorrer na entidade de destino, caso ocorra fragmentação de pacotes.

No protocolo ESP, como no AH, alguns campos são inseridos no pacote IP com o intuito de adicionar os serviços de autenticidade e confidencialidade. Alguns campos estão no Cabeçalho ESP, outros estão no final do pacote no ESP Trailer e ESP Autenticação, como mostra a Figura 3.20. Os campos SPI (*Security Parameter Index*) ou Índice de Parâmetro de Segurança, Número de Seqüência, Próximo Cabeçalho e Dados de Autenticação são definidos como se fossem do protocolo AH, o campo Complemento é usado para fazer com que o campo Dados da Autenticação seja sempre múltiplo de 4 bytes ou exercer outra complementação pertinente ao algoritmo de criptografia utilizado, já o campo Tamanho do Complemento é utilizado para indicar quantos bytes foram inseridos no complemento e retirá-los no momento da decriptografia.

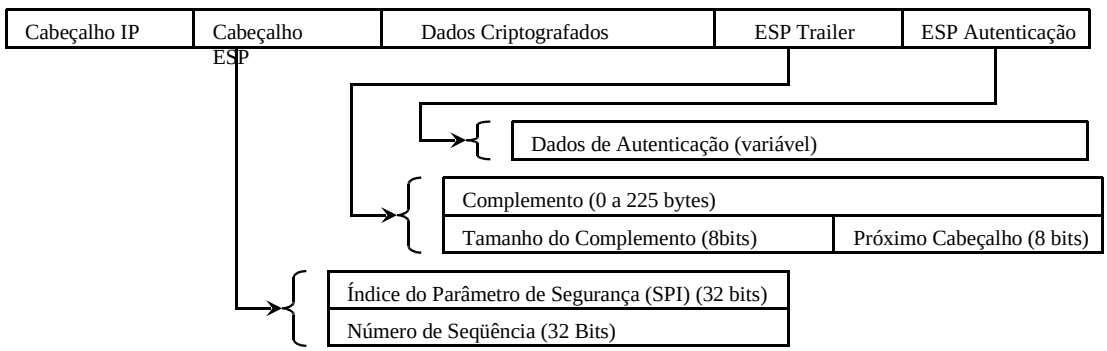

Figura 3.20 **– Campos do protocolo ESP [4]**

O pacote resultante, após o emprego do ESP, é maior que o pacote original, podendo até superar o tamanho máximo permitido que está por volta de 1.500 bytes (*Maximum Transmission Unit* do protocolo de enlace *Ethernet*) [1], desta forma, caso o tamanho exceda o máximo permitido, o pacote é fragmentado durante a transmissão. Assim, o *gateway* deve desfragmentar os pacotes e depois decriptografar os dados contidos nestes, remontando-os em seguida e encaminhado-os à rede interna.

Como acontece com o protocolo AH, o ESP também possui dois modos de operação, um modo de transporte e um modo túnel.

Modo Transporte ESP

Neste modo o cabeçalho ESP é inserido entre o cabeçalho IP e o campo de dados, preservando se assim o cabeçalho original, adicionando também os campos dados da autenticação e segmentação da autenticação (dentro do ESP Trailer). Se o pacote já possuir algum cabeçalho de segurança IPSec, o novo cabeçalho é inserido antes do cabeçalho IPSec já existente. Como o cabeçalho original é mantido, da mesma forma que no AH, o modo transporte só pode ocorrer entre *hosts* ou servidores, os quais possuam os endereços IP de origem e destino. A Figura 3.21 exemplifica o processo.

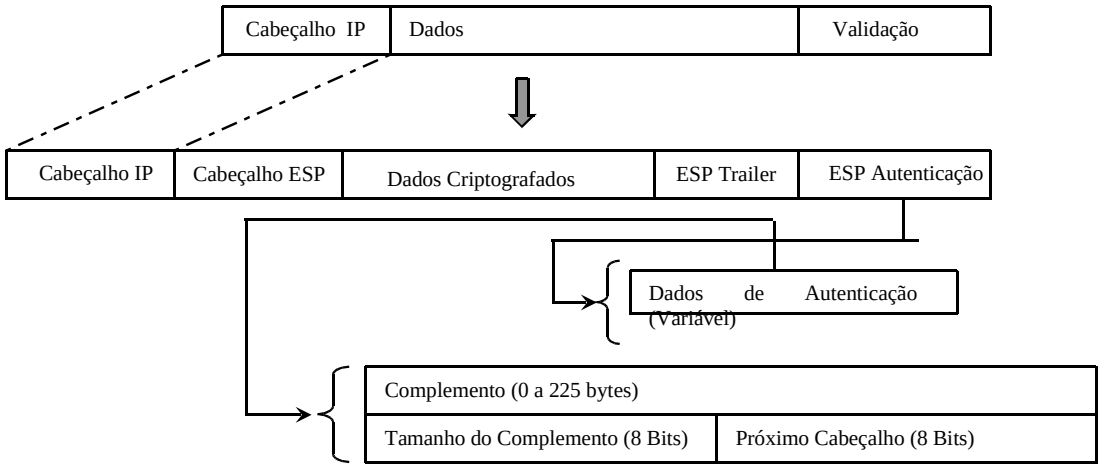

Figura 3.21 **– Modo Transporte no protocolo ESP [4]**

Modo Túnel ESP

Neste modo, todo o pacote IP original é colocado dentro de um novo pacote sendo gerado um novo cabeçalho IP e o cabeçalho ESP, bem como adiciona também os campos de autenticação e segmentação de autenticação, a Figura 3.22 representa este processo. Se o túnel for estabelecido entre dois servidores ou *hosts*, os endereços de origem e destino do novo cabeçalho são os mesmos do cabeçalho original. Mas se o túnel for feito entre dois *gateways*, como roteadores ou *firewall*, os endereços de origem e destino do novo cabeçalho são os dos *gateways* e os endereços do cabeçalho original dentro do pacote criptografado serão os dos *hosts* ou servidores da rede interna atrás do *gateway*.

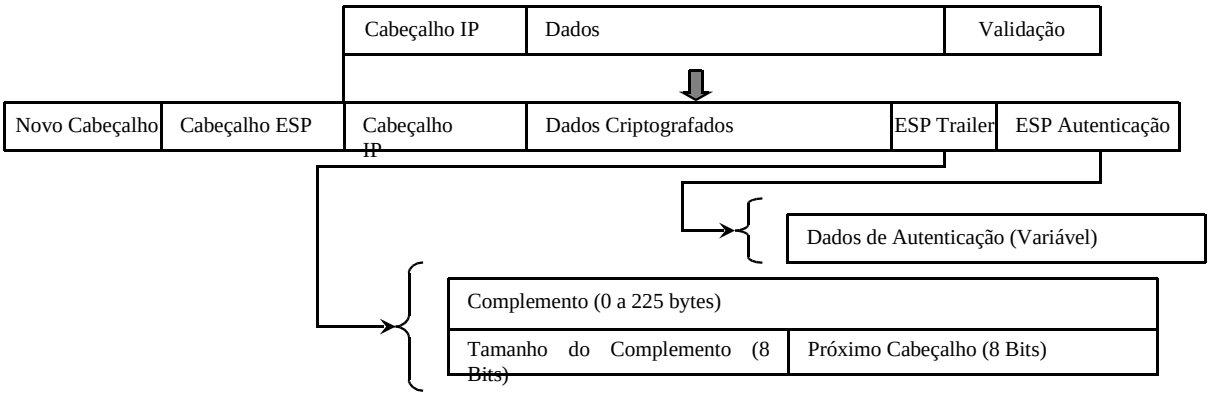

Figura 3.22 **– Modo Túnel no protocolo ESP [4]**

3.5.5.1.3 Associação de Segurança

Uma SA (*Security Association*) ou Associação de Segurança define que medidas de segurança devem ser aplicadas aos pacotes baseando-se em quem está enviando, para onde esta indo e que tipo de dados o pacote contém. O conjunto de serviços de segurança oferecidos pela SA depende do protocolo de segurança utilizado, das opções do protocolo escolhidas e do modo no qual a SA deve trabalhar, se em modo de transporte ou túnel.

As informações da SA servirão para constituir o túnel VPN e podem ser trocadas dinamicamente entre as entidades da VPN no momento do estabelecimento do túnel. Uma outra opção, um pouco menos usada, é estabelecer SAs fixas para cada entidade da VPN.

As SAs são identificadas por três parâmetros: endereço IP de destino, identificação do protocolo de segurança (valor 51 para AH e o valor 50 para ESP) e o SPI que identifica unicamente uma SA, sendo definido durante a negociação da SA entre as entidades. Todos os participantes da VPN devem conhecer o SPI correspondente e usá-lo durante a comunicação.

A SA define apenas o endereço IP de destino, pois esta é acordada entre duas entidades para a transmissão de dados numa única direção. Se houver a necessidade de duas entidades trocarem informações entre si, é então necessário a criação de duas SAs.

Durante o processo de negociação da SA são definidos as chaves criptográficas, os algoritmos de criptografia e autenticação e os parâmetros que serão usados por estes algoritmos. Além disso, as SAs podem ser estabelecidas de dois modos diferentes, no modo transporte ou no modo túnel.

No modo de transporte, a SA é estabelecida entre dois *hosts*. No caso da SA usar o ESP, este prove serviços de segurança somente para os protocolos de mais alto nível, como TCP ou UDP, não incluindo o cabeçalho IP ou os cabeçalhos de extensão que precedem o ESP. Já no caso da SA utilizar o AH, este estende a proteção aos cabeçalhos não protegidos pelo ESP, isso acontece pelo fato de o ESP criptografar os dados que o sucedem no pacote, além de autenticar apenas a “porção ESP” do pacote, enquanto o AH autentica todo o pacote.

Quando pelo menos um dos participantes da VPN é um *gateway* que implementa o IPSec, a SA deve ser estabelecida em modo túnel. Em uma SA em modo túnel, o cabeçalho IP externo indica o destino no contexto do IPSec, ou seja, o endereço do dispositivo VPN que pode ser um *gateway* ou *host*, e o cabeçalho IP interno indica o destino real do pacote, ou seja, o endereço da máquina que deve recebê-lo dentro da rede interna. Assim, os cabeçalhos dos protocolos de segurança são inseridos depois do cabeçalho IP externo e antes do cabeçalho IP interno. Semelhante à análise no modo de transporte, o AH provê segurança para o cabeçalho IP externo e, conseqüentemente, para os protocolos de mais alto nível, assim como para o pacote IP que já se encontra no túnel. Já quando o ESP é usado em modo túnel, apenas a segurança do pacote IP é assegurada.

As Figuras 3.23 e 3.24 apresentam a organização dos modos túnel e transporte descritos acima.

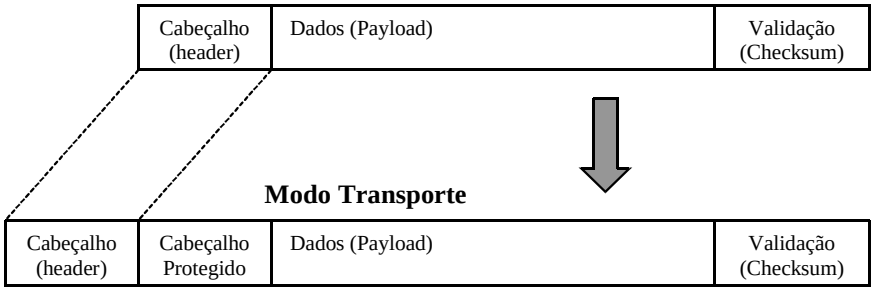

Figura 3.23 – **Modo Transporte da Associação de Segurança [4]**

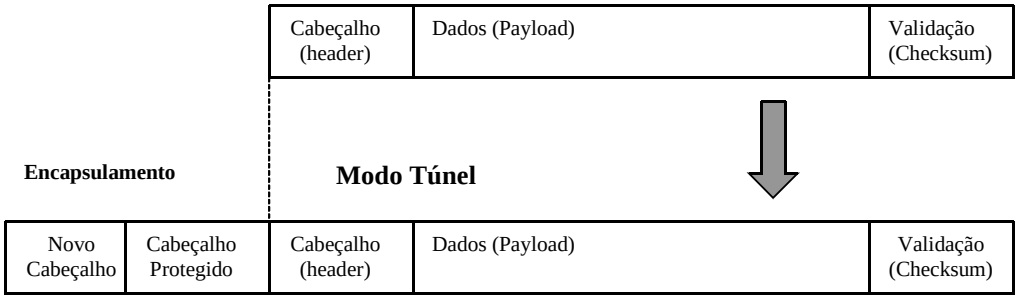

Figura 3.24 **– Modos Túnel da Associação de Segurança [4]**

3.5.5.1.4 Banco de Dados de Segurança

O IPSec utiliza dois bancos de dados diferentes: um contendo todas as políticas de segurança o SPD (*Security Policy Database*), mantidas pelo SPD para serem usadas

quando for necessário durante o processamento dos pacotes IP e na construção das SAs; outro banco, o SAD (*Security Association Database*) contém o conjunto de parâmetros associados a cada SA, onde cada SA tem uma entrada neste banco especificando todas as informações necessárias ao processamento do IPSec para os pacotes pertencentes à SA .

As informações contidas em uma SA são:

- SPI é o número que identifica a SA dentro do SAD;
- O protocolo utilizado na SA pode ser ESP ou AH;
- O modo de funcionamento da SA, túnel ou transporte;
- Contador de seqüência do pacote IP dentro da SA;
- Número máximo de unidades de transmissão;
- Endereço de origem da SA;
- Endereço de destino da SA;
- Algoritmo de autenticação e sua chave de autenticação;
- Algoritmo de criptografia e sua chave de criptografia;
- Tempo de vida das chaves;
- Tempo de vida da SA.

Quando um pacote está chegando a um *host* ou *gateway* com IPSec, a SA é identificada por meio do endereço IP de destino, do tipo do protocolo e do SPI. Destes, o endereço IP de destino e o tipo do protocolo são localizados no cabeçalho IP e o SPI no cabeçalho AH ou ESP. Se uma SA for localizada, são aplicados ao pacote todos os serviços de segurança acordados para esta SA, e em seguida, o processamento do pacote segue para o SPD.

Quando um pacote está saindo de um *host* ou *gateway* com IPSec, o SPD é processado primeiramente. Se o pacote atender a todas as políticas de segurança o SAD procura pela SA correspondente. Caso não encontrar uma nova SA é negociada e armazenada no SAD, mas se já existir, o pacote é então processado de acordo com a SA.

3.5.5.1.5 Gerenciamento de Chaves

Os serviços de segurança do IPSec compartilham chaves secretas tanto para a autenticação como para criptografia, deste modo é necessário existir um mecanismo exclusivo para gerenciamento de chaves, suportando a distribuição manual ou automática. Em redes com poucos computadores pode-se configurar as SAs manualmente. Todavia, se a rede for grande, o recomendado é configurá-los automaticamente e também dinamicamente, a negociação dinâmica é necessária pois, não se sabe exatamente quando a SA é negociada para o estabelecimento do túnel e também porque a SA deve ter tempo de vida finito, devendo ser trocada de tempos em tempos. Desta forma faz-se necessário o uso de um gerenciamento de chaves automático. Alguns protocolos implementam de forma satisfatória este gerenciamento, porém o principal deles é o IKE (*Internet Key Exchange Protocol*), que combina os protocolos ISAKMP (*Internet Security Association and Key Management Protocol*), SKEME (*Secure Key Exchange Mechanism*) e o *Oakley Key Determination Protocol*.

O ISAKMP define como duas entidades podem estabelecer um canal de comunicação segura entre si, fazendo com que uma entidade se autentique na outra, através da troca de informações de chaves e negociação de serviços de segurança. Entretanto, não especifica como a autenticação é feita ou quais chaves serão geradas. As mensagens ISAKMP possuem um cabeçalho e um ou mais dados ISAKMP, formando-se assim pacotes UDP como é ilustrado na Figura 3.24.

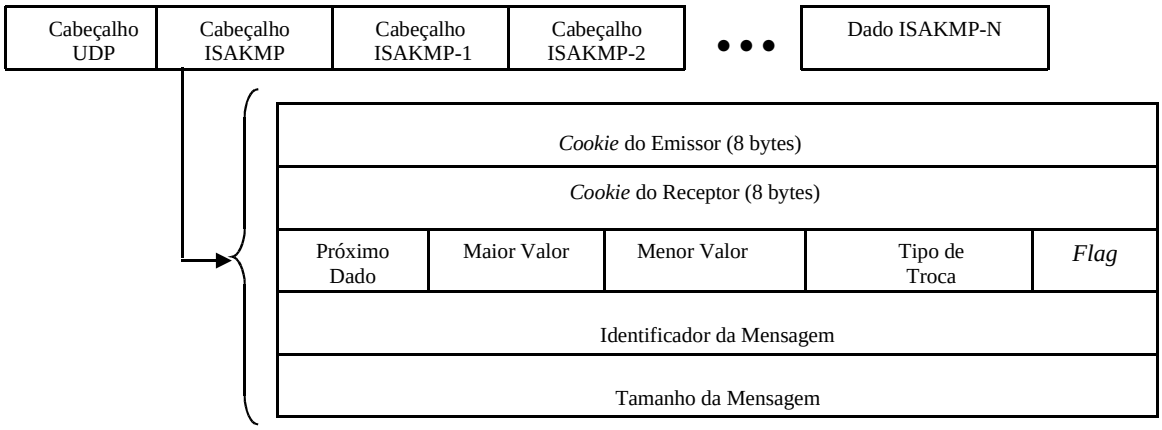

Figura 3.25 **- Formato da mensagem ISAKMP**

Entre os campos da mensagem do ISAKMP, podem ser destacados, o *Cookie* do Emissor e o *Cookie* do Receptor. Estes são valores produzidos pelas entidades e são também utilizados para identificação da SA entre duas entidades depois da conclusão da negociação do canal. Assim, um pacote não esperado pode ser descartado mais rapidamente sem gastar tempo com processamento da mensagem.

O ISAKMP possui duas etapas para a negociação de uma associação de segurança.

Primeira Etapa:

A primeira etapa consiste da negociação entre as entidades ISAKMP pela escolha de uma associação de segurança confiável para negociações futuras. Não se deve confundir a SA do IPSec que é unidirecional com associação de segurança do ISAKMP que é bidirecional e não se aplica ao tráfego do IPSec.

Esta etapa é subdividida em dois modos de negociação, modo principal e modo agressivo.

O modo principal possui três fases. Na primeira, o emissor envia várias propostas de SA para o receptor que por sua vez escolhe uma delas e envia de volta. Na segunda, as entidades trocam os parâmetros das chaves e um valor aleatório, chamado de *nonces*, que serve para evitar ataques do tipo *replay*. Na última fase, todas as informações da SA são trocadas. Estas são autenticadas por algum dos métodos (chave secreta, por assinatura digital ou criptografia de chave pública). Caso a escolha do mecanismo de autenticação seja chave privada, a chave é derivada do segredo e é realizada a função *hash* nesta chave que por sua vez é trocada entre as duas entidades, sendo esta a informação de autenticação. Caso a escolha seja assinatura digital, é necessário pegar o certificado digital que contenha a assinatura de cada entidade na qual a autenticação é baseada. Caso a escolha seja criptografia por chave

pública, as duas entidades trocarão as chaves criptográficas entre si. As fases do modo principal estão ilustradas na Figura 3.25.

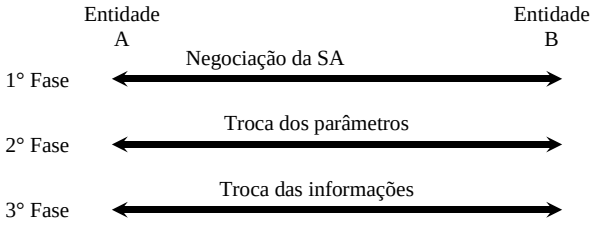

Figura 3.26 **– Primeira Etapa do ISAKMP: Modo principal da negociação da [4]**

O modo agressivo todas as três fases do modo principal acontecem em uma única mensagem enviada entre o emissor e receptor, no entanto as informações de autenticação não são criptografadas. A Figura 3.26 ilustra o modo agressivo.

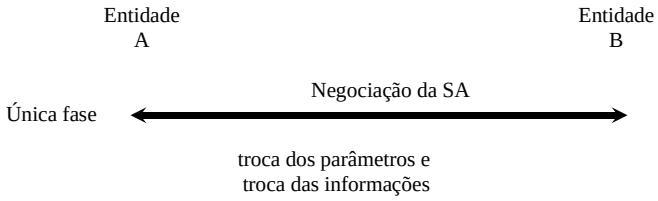

Figura 3.27 **– Primeira Etapa: Modo agressivo da Negociação [4]**

Segunda Etapa:

Na segunda etapa é negociada a SA do IPSec, utilizando o canal criado na primeira etapa. Como o canal já foi estabelecido, esta etapa tende a ser mais rápida, por isso também é chamada de Modo Rápido. A Figura 3.27 mostra a segunda etapa da negociação ISAKMP.

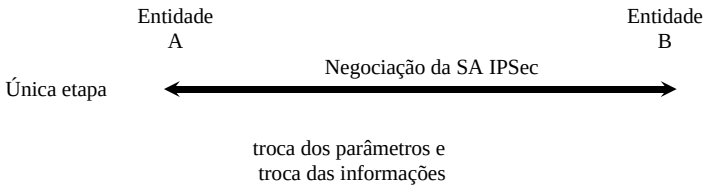

Figura 3.28 **– Segunda Etapa: Modo rápido da Negociação [4]**

Neste capítulo foram abordados vários conceitos relacionados a VPN. Destes, os mais importantes são o tunelamento e os protocolos de tunelamento, sendo os mais importantes para este trabalho, o PPP, L2TP e o IPSec pois, serão úteis para o entendimento do próximo capítulo.

3.6 VANTAGENS E DESVANTAGENS

De acordo com [4], as vantagens em se utilizar uma rede VPN estão diretamente relacionadas com a segurança, transparência, facilidade de administração e redução de custos. A segurança em VPN é garantida através da autenticidade, confidencialidade, integridade e controle de acesso, minimizando-se assim os riscos de ataques levarem a grandes danos no sistema. A transparência contribui facilitando o gerenciamento das redes e diminuindo a necessidade de treinamentos dos administradores, não permitindo que os usuários percebam a localização física dos recursos, e possibilitando o acesso a estes de lugares remotos como se estivessem presentes localmente na máquina do usuário. A redução de custos está entre uma das maiores vantagens em se usar uma VPN, pois a conexão diretamente com um ISP ou provedor de acesso discado é mais barata que o aluguel de linhas dedicadas e o uso de servidores de acesso remoto.

Apesar de todas as vantagens citadas, uma VPN apresenta algumas desvantagens, como, a confiança entre as redes interconectadas e a disponibilidade do ISP em manter o serviço de utilização da *Internet*. A implementação de uma VPN pode consumir bastante tempo caso não haja um planejamento adequado, podendo assim, haver dificuldade na localização de seus defeitos. Assim, é extremamente importante o conhecimento do seu funcionamento pois, uma imperfeição pode resultar em mais tempo gasto para criar a VPN. Como os dados trafegam criptografados na VPN, a localização de defeitos, a não sincronização das chaves, a falha de autenticação, os pacotes perdidos e a sobrecarga do *gateway*, pode se tornar difícil de ser detectada e tratada. A relação de confiança entre as redes é uma necessidade, devendo ser bem planejada anteriormente. Desta maneira, se uma

das redes não possuir uma segurança adequada, perde-se assim em confiabilidade, ficando ambas as redes vulneráveis a ataques por parte de *hackers*.[4]

Em razão de uma VPN depender da *Internet*, é necessário que esta esteja sempre disponível, o que nem sempre é possível devido às falhas existentes nos ISPs. Assim, é muito interessante possuir duas opções de conexão com a *Internet*, caso uma falhe ou fique inoperante, basta trocar para a outra.

4 VPN COM SERVIDOR LINUX FREES/WAN E CLIENTE MICROSOFT L2TP/IPSEC

4.1 CENÁRIO

A proposta de implementação é constituída por um *gateway* VPN que utiliza a plataforma Linux, e este aceita conexões VPN de usuários remotos utilizando a plataforma Microsoft Windows. Para realizar as conexões VPN são utilizados dois protocolos de tunelamento, o IPSec e o L2TP. Estes protocolos trabalham em conjunto, sendo que o L2TP utiliza o IPSec para realizar a conexão. Sendo assim, o usuário remoto inicia a conexão VPN e o IPSec, implementado no Windows, tentará estabelecer o túnel VPN com o IPSec do *gateway* VPN autenticando-se neste. Depois disso, o L2TP utiliza o túnel criado pelo IPSec para estabelecer a sua conexão criando através do protocolo PPP um túnel PPP, ou seja, onde os pacotes IP estão encapsulados em *frames* PPP. O cenário descrito é ilustrado na Figura 4.1.

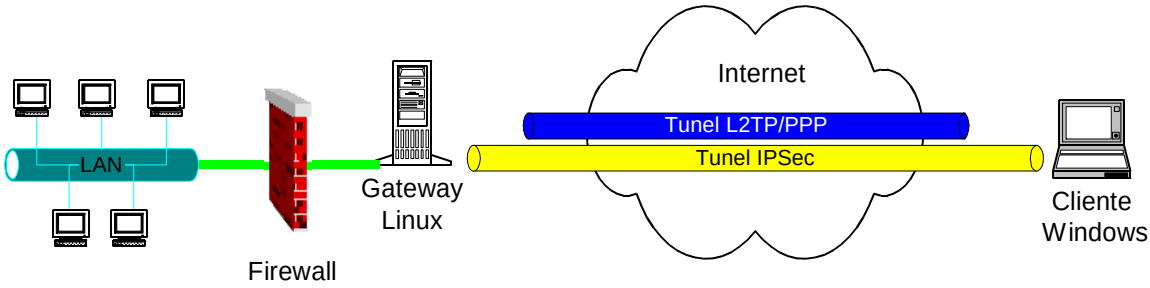

Figura 4.1 – **Cenário**

4.2 GATEWAY VPN

Nesta seção são destacados todos aspectos relevantes ao *gateway* da VPN proposta neste trabalho.

4.2.1 FREES/WAN

O FreeS/WAN é uma implementação para Linux do protocolo IPSec, e foi inicialmente projetado por John Gilmore, em 1996, com o objetivo de ser um pacote aberto de acordo com os padrões do IETF[15] para o protocolo IPSec [4]. O FreeS/WAN é composto por três partes:

- KLIPS: *Kernel* do IPSec integrado ao *Kernel* do *Linux*. Este tem como função tratar os protocolos AH e ESP do IPSec e faz a negociação dos pacotes dentro do *Kernel*.

- Pluto é um *daemon* que faz a negociação de chaves do IKE e trata da negociação da comunicação entre as entidades da VPN. Este interage também com KLIPS quando necessário e pode ser iniciado automaticamente por de um script de inicialização do FreeS/WAN.

- Utilitários e scripts que servem de interface de administração do ambiente FreeS/WAN.

No IPSec padronizado pela IETF[15] há o conceito de Associação de Segurança. No FreeS/WAN não existe este conceito, porém ele utiliza o conceito chamado de criptografia oportunista, o que significa que qualquer entidade que participar da VPN pode criptografar o tráfego de dados antes do envio, em qualquer direção, mesmo sem uma possuir qualquer informação a respeito da outra entidade e sem nenhuma intervenção dos administradores de rede. Este recurso reduz a necessidade administração do IPSec, uma vez que não são necessárias configurações específicas de túneis, apesar de ainda ser permitido configurá-los para casos específicos. Existem dois tipos de criptografia oportunista: parcial e total. Na parcial, apenas é possível iniciar conexões oportunistas, enquanto que na total, é possível tanto iniciá-las quanto aceitá-las.[16]

No entanto, a criptografia oportunista não é considerada um padrão do protocolo IPSec proposto pela IETF[15], mas está sendo proposta para ser uma extensão dele. Portanto, ela só é possível quando, os dois participantes da VPN utilizarem o FreeS/WAN na comunicação. Desta forma, neste trabalho não é utilizada a criptografia oportunista, pois a plataforma Windows não suporta este tipo de criptografia.

A versão atual do FreeS/WAN 2.x garante segurança para versão 4 do IP. Porém a versão que suporta a versão 6 do IP já está sendo desenvolvida. Devido a restrições de exportação de alguns países para programas que utilizam criptografia forte, o FreeS/WAN não está presente no kernel padrão do Linux, sendo necessária a sua instalação.[16]

4.2.2 SOFTWARES NECESSÁRIOS

O servidor de VPN Linux deve rodar uma distribuição do Linux que possua uma versão recente *kernel*, como por exemplo, o *kernel* 2.4.18 (ou superior). Ainda no servidor devem estar instalados os seguintes pacotes:

- O FreeS/WAN na versão 1.99 (ou superior), algumas distribuições do Linux já possuem o FreeS/WAN instalado como padrão. O FreeS/WAN é encontrado na url: http://www.freeswan.org/download.html. Este foi escolhido por ser a mais popular implementação do IPSec disponível

para o Linux, possuir extensa documentação e tender a se tornar um padrão do IPSec para Linux.[16]

- O L2TPD na aversão 0.69 (ou superior). Este é um *daemon*, ou seja, é um software que executa continuamente em segundo plano, que foi criado por Mark Spencer, mas atualmente está sendo desenvolvido por David Skoll, este tornou disponível a última versão a 0.69. O L2TPD foi criado com o intuito de é a de estabelecer conexões L2TP através do Linux. O L2TPD é gratuito de acordo com a GNU [5] e pode ser conseguido na url: http://www.l2tpd.org/download.html . Este foi escolhido por ser uma das mais usadas implementações do L2TP para Linux e possuir também uma boa documentação. [17]

- O PPPD na sua versão 2.4.1(ou superior). Este é um *daemon* que foi criado com o objetivo de suportar conexões PPTP no Linux. A versão atual deste é a 2.4.1. foi escolhido por ser uma implementação do PPP muito usada no Linux e também por já estar disponível em algumas distribuições.

- O patch para suporte a certificados X.509[18] da Strongsec [19] para o FreS/WAN na versão compatível com o mesmo, os procedimentos de instalação podem ser encontrado em [20]. Este foi escolhido por possibilitar o uso de autenticação através de certificado digital no FreeS/WAN.

4.3 CLIENTE VPN MICROSOFT L2TP/IPSEC

O cliente VPN Microsoft L2TP/IPSec é um pacote gratuito criado pela Microsoft em julho de 2002, e está disponível para *donwload* na *web* no *site* da Microsoft na sua versão 1.0 com o nome de MSL2TP.exe. Este pacote permite que computadores rodando Windows98 (todas as versões), Windows ME e Windows NT4.0 usem o protocolo L2TP juntamente com

o protocolo IPSec. A combinação do L2TP e IPSec, é conhecida como L2TP/IPSec, e este é usado para prover segurança para a VPN por acesso remoto através da *Internet*.

Antes do lançamento do pacote MSL2TP tratado acima, L2TP/IPSec podia apenas ser usado com clientes Windows XP ou Windows 2000, pois estes já possuem suporte para o L2TP e IPSec.

Requisitos Básicos de software para se estabelecer a VPN no Windows:

- Windows 98: deve possuir instalado o Internet Explorer 5.01 (ou superior, devido ao tamanho da chave criptográfica) e o adaptador para rede *Dial-up* na sua versão 1.4 (ou superior).
- Windows ME: deve possuir instalado o componente para comunicação para VPN e o Internet Explorer na versão 5.01(ou superior, devido ao tamanho da chave criptográfica).
- Windows NT 4.0: deve possuir instalado o RAS (Serviço de Acesso Remoto), o protocolo PPTP, o *Service Pack 6* e o Internet Explorer 5.01(ou superior, devido ao tamanho da chave criptográfica).
- Windows 2000: deve possuir instalado o *Service Pack 2* (ou superior).
- Windows XP: não necessita de nenhuma instalação extra, porém é sempre bom possuir sempre as últimas atualizações instaladas.

Após todos os pacotes serem instalados, deve-se instalar o MSL2TP.exe no Windows 98, ME e NT. Caso não seja instalado algum dos pacotes citados, o MSL2TP.exe não concluirá a sua instalação e indicará qual pacote está faltando. O Windows 2000 e XP não necessitam da instalação do MSL2TP, pois já possuem suporte ao cliente L2TP/IPSec como padrão.[21]

O processo de instalação dos componentes de software listados acima não é abordado neste trabalho, pois foge completamente do seu escopo, no entanto, pode ser encontrado em [21].

4.4 TIPOS DE AUTENTICAÇÃO POSSÍVEIS:

- **Certificados**

Quando os certificados são usados para autenticação no IPSec, cada entidade valida o certificado da outra entidade. Por exemplo, duas entidades A e B trocam certificados entre si, assim a entidade A valida o certificado da entidade B e a B valida o certificado da A.

Os certificados nos clientes rodando Windows 98, ME e NT são importados através do Internet Explorer e uma vez importados, podem ser utilizados pelo MSL2TP. Já para os clientes usando Windows 2000 e XP, os certificados são importados através do MMC (*Microsoft Management Console*).

- **PSK (*Pré-Shared Key*)**

Uma pré-shared key (chave previamente compartilhada) é uma seqüência de caracteres usada para autenticar a porção IPSec da conexão L2TP/IPSec. Ambos, servidor e cliente devem estar configurados para usar a mesma chave para que a autenticação do IPSec funcione corretamente.

A PSK é configurada como padrão pelo FreeS/WAN, mas já o Windows 2000 não possui suporte a mesma, usando apenas certificados para a autenticação.[21]

4.4.1 CERTIFICADOS X PRÉ-SHARED KEY

PSK’s são mais fáceis de usar, pois todos os clientes possuem a mesma chave. Porém isto acarreta em riscos a segurança, já que esta chave pode ser perdida. Certificados

exigem que se possua uma infraestrutura de PKI (*Public Key Infrastructure*) [4], torna mais complexo o gerenciamento. Porém, aumenta consideravelmente a segurança.[21]

PSK deve ser usada por curto período de tempo, sendo trocada periodicamente. Certificados já possuem uma duração maior, pois são garantidos pela Autoridade Certificadora.[21]

PSK apenas é usada com clientes que possuam endereço IP fixo. Já os certificados podem ser usados clientes que possuam endereço IP variável. Como normalmente os usuários remotos possuem endereço IP variável os certificados são mais indicados para realizar a autenticação.[21]

Assim, se as informações que irão trafegar pela rede não forem muito preciosas, pode-se usar PSK. Mas se as mesmas exigem uma segurança maior, o melhor é usar a autenticação por certificados. [21]

4.5 VISÃO DA IMPLEMENTAÇÃO

O cenário da VPN proposta pode ser implementado utilizando no *gateway* da VPN o FreeS/WAN, para possibilitar a criação do túnel IPSec e o L2TPD para a criação do túnel PPP utilizando o PPPD. Assim como no *gateway*, no lado do cliente Windows deve estar implementado o L2TP/IPSec. Esta implementação é ilustrada na Figura 4.2, onde primeiramente o cliente Windows solicita a criação do túnel IPSec ao FreeS/WAN no *gateway* VPN, e este por sua vez verifica a autenticidade do usuário através de PKS ou certificados digitais e só então autoriza ou não o seu acesso. Criado o túnel IPSec, o cliente Windows solicita o estabelecimento do túnel L2TP, utilizando o túnel criado pelo IPSec. Assim o L2TPD no *gateway* aceita a criação do túnel L2TP, onde na verdade trafegam *frames* PPP enviados e recebidos pelo L2TP.

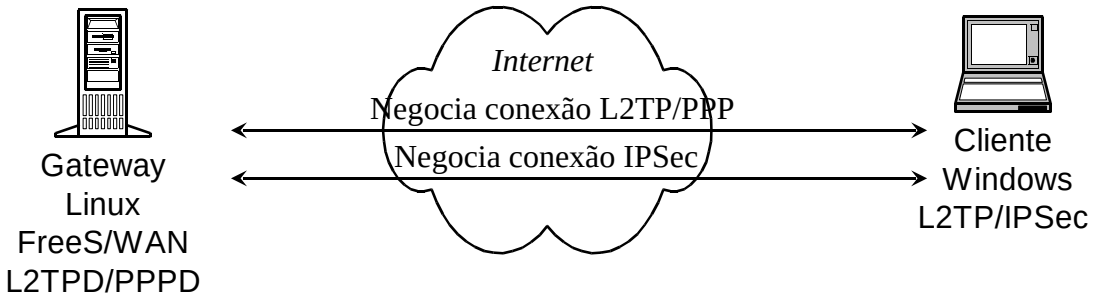

Figura 4.2 - **Implementação proposta**

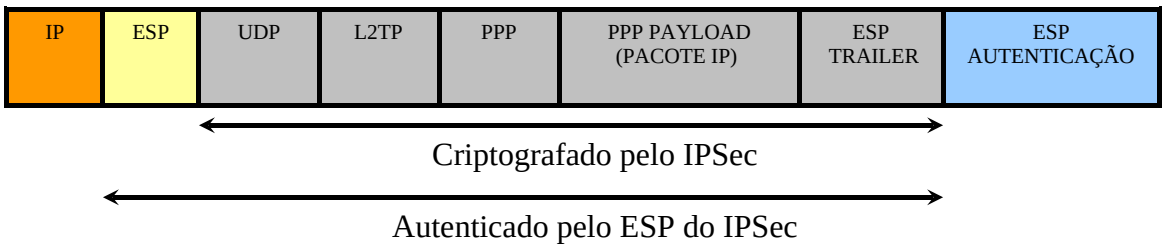

Figura 4.3 - **Pacote da VPN**

Depois de estabelecida a conexão VPN, o tipo do pacote que trafega na VPN será o apresentado na Figura 4.3, onde os dados antes do envio são encapsulados em *frames* PPP, depois é acrescentado o cabeçalho L2TP. Após é colocado o cabeçalho UDP, em seguida todo o pacote é criptografado pelo ESP do IPSec, adicionando o cabeçalho de autenticação e por último é colocado o cabeçalho IP possuindo o endereço do *gateway* e do usuário remoto.

Na implementação proposta, foi utilizada uma combinação dos protocolos L2TP e IPSec, ou seja, L2TP sobre IPSec. Esta foi escolhida, por ser a combinação de protocolos suportada por todas as versões do sistema operacional Windows para estabelecimento de VPN [21]. Sendo assim, é possível ao *gateway* da VPN com sistema operacional Linux e o L2TP sobre IPSec como protocolo de VPN, aceitar conexões solicitadas por usuários remotos que possuam qualquer versão do Windows, desde que devidamente configurados para isso.

5 CONCLUSÃO

Este trabalho se propôs mostrar como implementar uma VPN utilizando clientes Microsoft Windows acessando um servidor Linux através do protocolo L2TP sobre o protocolo IPSec, detalhando aspectos de suas configurações, além de analisar a funcionalidade e a segurança da mesma.

Pode-se constatar, que a VPN vem crescendo como uma tecnologia de rede. Isto pode ser observado através do grande interesse por parte da empresas em garantir a segurança durante a transmissão de dados via *Internet*, pois os serviços oferecidos pelas empresas de telecomunicações vêm crescendo e aprimorando a cada dia atraindo cada vez mais empresas para a utilização de VPN. Os principais motivos do aumento da procura por implementações de VPN estão diretamente ligados à segurança e à economia que se consegue obter na transmissão de dados via VPN.

A cada dia que passa, surgem mais pesquisas sobre redes VPN possibilitando assim surgir diferentes protocolos e maneiras de implementá-los, aprimorando assim a segurança de dados e a flexibilidade em se lidar com VPN. Esta segurança é obtida

principalmente através da utilização de algoritmos de criptografia e protocolos específicos, que geram grandes obstáculos aos invasores.

Os protocolos abordados neste trabalho foram o PPP, o L2TP e o IPSec. Os dois primeiros se mostraram boas alternativas de implementação, porém pecam na segurança, pois não possuem suporte à criptografia. A utilização do IPSec fecha a brecha de segurança deixada, garantindo assim, uma comunicação segura, pois este é um protocolo mais completo em relação ao L2TP e PPP possuindo características mais expressivas de proteção do tráfego da VPN. No entanto, o IPSec é um protocolo complexo, sendo indispensável entender bem o seu funcionamento antes de implementá-lo em uma VPN.

É de suma importância reconhecer que nem o IPSec nem uma VPN sozinhos conseguem garantir a segurança de uma rede. Desta forma, é imprescindível que seja elaborado um planejamento cuidadoso, que envolva políticas rígidas de segurança, permitindo que haja proteção física e lógica dos servidores.

O sistema operacional Linux constitui-se uma solução atrativa para as organizações que não disponibilizam de muitos recursos financeiros ou que pretendem não gastar muito com soluções proprietárias, já que os gastos da implementação proposta restringem-se aos gastos com pessoal e licenças de Windows.

Foi observado também que a ferramenta FreeS/WAN utilizada neste trabalho atende às necessidades exigidas para a implementação da VPN proposta, sendo capaz de implementar o protocolos do IPSec e fornecer suporte a criptografia e autenticação via certificados, características importantes para se estabelecer um nível de segurança adequado as necessidades da VPN proposta.

Conclui-se que os tópicos abordados na implementação da VPN proposta neste trabalho, vieram a contribuir academicamente conceituando os aspectos principais de segurança abordados em redes VPN, além de também analisar as diversas características e elementos existentes nas VPNs. Este trabalho tem como contribuição, de forma prática, uma implementação para VPN que reduz consideravelmente os custos de implantação,

possibilitando indiretamente a um número maior de empresas, que não possuem um grande orçamento para a área de informática utilizarem a VPN por acesso remoto.

Finalmente, para trabalhos futuros pode-se propor a adição de um *firewall* integrado ao *gateway* da VPN, visando uma maior proteção contra ataques vindos da *Internet*.

Pode-se ainda, como trabalhos futuros, implementar a VPN proposta e executar testes sobre suas configurações de modo a verificar o seu comportamento durante a utilização. Um exemplo de teste possível é verificar o número máximo de usuários remotos suportados pelo *gateway* da VPN.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Tanenbaum, Andrew S. Redes de Computadores; tradução da terceira edição do original. Editora Campus, 1997.

[2] Ayub, Ricardo; Forbici, Eduardo Sudol. *Uma Reflexão sobre VNP's* [on line]. Disponível na URL: http://www.presidentekennedy.br/publicacoes/I_encontro/Artigos/artigo16.pdf [acessado em março de 2003].

[3] Almeida, Eduardo Santana; Barros, Maria Fernanda; Garcia, Vinícius Cardoso. Análise e Implementação de VPN em ambiente Linux [on line]. Disponível na URL: http://library.seng.com.br/network/vpn/Anal_implem_VPN_linux.pdf [acessado em março de 2003].

[4] Silva, Lino Sarlo da. *Virtual Private Network* [on line]. Aprenda a Construir Redes Privadas Virtuais em Plataformas Linux e Windows. São Paulo, SP: Editora NOVATEC Ltda, 2003.

[5]GNU [on line] Disponível na URL: http://lie-br.conectiva.com.br/licenca_gnu.html [acessado em novembro de 2003]

[6] DANESH, Arman. Dominando o Linux Red Hat 6.0 "A Bíblia". Makron Books, 2000.

[7] D'ÁVILLA, Márcio H. C. Segurança de Redes [on line]. Disponível na URL: http://www.inet.com.br/~mhavila/aulas/seguranca/material.html [acessado em setembro de 2003]

[8] RSD - Revista da Sociedade Digital. 1° Edição. Disponível na URL: http://www.bibvirt.futuro.usp.br/textos/hemeroteca/rsd/rsd011201/rsd011201.pdf [acessado em setembro de 2003]

[9] Arranhado , Gustavo Jorge Mourato. VPN- Redes Privadas Virtuais [on line] na URL: http://www.ipg.pt/user/~sduarte/rc/trabalhos/VPN/criar_vpn.htm# [acessado em março de 2003].

[10] Pouw, Keesje Duarte. Segurança na arquitetura TCP/IP: de *firewall*s a canais seguros

[on line] na URL: http://www.las.ic.unicamp.br/paulo/teses/Keesje_Duarte_Pouw/ [acessado em maio de 2003].

[11] BROCARDO, Marcelo Luiz: Um Protocolo Criptográfico para Análise Segura de Crédito. [on line] Disponível na URL: http://www.inf.ufsc.br/~custodio/orientacao.html [acessado em outubro de 2003].

[12] *International Telecommunication Union* [on line] na URL: http://www.itu.int/home/ [acessado em novembro de 2003].

[13] *Cisco Systems, Nortel and Shiva Team to Provide New Virtual Dial-Up Service Opportunities. Virtual private dial-up networks become a reality with proposed standards-based functionality* [on line] na URL: http://www.cisco.com/warp/public/146/pressroom/1996/jun96/309.html [acessado em setembro de 2003].

[14] Gast, Matthew: *Inner Authentication Methods* [on line] na URL: www.ilabs.interop.net/WLAN_Sec/Inner_Auth-lv03.pdf [acessado em novembro de 2003].

[15] IETF (*Internet Engineernig Task Force*) [on line] na URL: http://www.ietf.org [acessado em junho de 2003].

[16] Documentação do FreeS/WAN [on line] na URL: http://www.freeswan.org/doc.html [acessado em outubro de 2003].

[17] Documentação do L2TPD [on line] Disponível na URL: www.l2tpd.org [acessado em outubro de 2003].

[18] Goldani, Carlos Alberto, Sistemas de Certificação Digital X.509 e PKIX [on line] na URL: www.inf.ufsc.br/~kazienko/tec_art/Certificacao.pdf [acessado em outubro de 2003].

[19] *Strogsec web site* [on line] na URL: http://www.strongsec.com [acessado em novembro de 2003].

[20] Guia de instalação do path de certificados X.509 para o FreeS/WAN [on line] na URL: http://www.strongsec.com/freeswan/install.htm [acessado em novembro de 2003].

[21] *Administrator's Guide to Microsoft L2TP/IPSec VPN Client* [on line] Disponível na URL: http://www.microsoft.com/technet/itsolutions/network/maintain/security/vpnclnta.asp [acessado em outubro de 2003].

[22] Leeuw, Jacco: *Using FreeS/WAN with Windows L2TP/IPSe*c [on line] na URL: http://www.jacco2.dds.nl/networking/RPMS/Mandrake9.1/l2tpd-0.69-8jdl.i586.rpm [acessado em novembro de 2003].

ANEXO A – CONFIGURAÇÕES

Configuração do *Gateway* VPN

Configuração do FreeS/WAN
Uma vez instalado o kernel do Linux com suporte ao FreeS/WAN, é necessário configurar a conexão IPSec. Se a versão do FreeS/WAN for a 2.x é necessário desabilitar a criptografia oportunista.
Existe uma diferenciação para usuários remotos que utilizam Windows 2000/XP atualizados e desatualizados (sem nenhuma atualização), sendo esta diferença a porta usada pelo IPSec para a comunicação, assim, deve ser especificada no FreeS/WAN a porta correta para cada um deles.
Para a configuração do FreeS/WAN são utilizados os arquivos /etc/ipsec.conf e /etc/ipsec.secrets, onde devem ser adicionadas as configurações que virão a seguir:

Configuração usando PSK
Especificação da chave PSK:

```
# Exemplo do arquivo /etc/ipsec.secrets para gateway com IP 123.123.123.123

#
123.123.123.123      234.234.234.234:      PSK      "thisismytopsecretkey"
123.123.123.123 111.222.111.222: PSK "keyforanotherclient"
```

Configuração mínima para utilizar usuário Windows 2000/XP sem atualização:

```
      # Habilita o uso de PSK definida em /etc/ipsec.secrets é necessário
desabilitar o PFS.
      authby=secret
      pfs=no
      #
      left=123.123.123.123
      leftnexthop=%defaultroute
```

```
      #
      # Configuração de porta necessária para usuários Windows 2000/XP não
atualizados.
      leftprotoport=17/0
      #
      #IP do usuário remoto e porta utilizada.
      #
      right=234.234.234.234
      rightprotoport=17/1701
      #
      # Habilita a configuração para o usuário.
      #
      auto=add
      keyingtries=3
```

Configuração para usuário com qualquer tipo de cliente windows incluindo o Windows 2000/XP atualizado, mas excluindo não atualizado:

```
      # Habilita o uso de PSK definida em /etc/ipsec.secrets é necessário
desabilitar o PFS.
      #
      authby=secret
      pfs=no
      #
      left=123.123.123.123
      leftnexthop=%defaultroute
      #
      leftprotoport=17/1701
      #
      # IP do usuário remoto e porta utilizada.
      #
      right=234.234.234.234
      rightprotoport=17/1701
      #
      # Habilita a configuração para o usuário.
      #
      auto=add
      keyingtries=3
```

Configuração usando Certificados:

Configuração mínima para utilizar usuário Windows 2000/XP sem atualização:

```
      # Habilita o uso de Certificados é preciso desabilitar o PFS.
      #
      authby=rsasig
      pfs=no
      #
      left=123.123.123.123
      leftnexthop=%defaultroute
      leftrsasigkey=%cert
      leftcert=/etc/ipsec.d/ssl/localCERT.pem
      #
      # Configuração de porta necessária para usuários Windows 2000/XP não
atualizados.
      leftprotoport=17/0
      #
```

```
# IP do usuário remoto, certificado e porta utilizada.
#
right=%any
rightrsasigkey=%cert
rightcert=/etc/ipsec.d/ssl/userCERT.pem
rightprotoport=17/1701
#
# Habilita a configuração para dos usuários.
#
auto=add
keyingtries=3
```

Configuração para usuário com qualquer tipo de cliente windows incluindo o Windows 2000/XP atualizado, mas excluindo não atualizado:

```
# Habilita o uso de Certificados é preciso desabilitar o PFS.
#
authby=rsasig
pfs=no
#
left=123.123.123.123
leftnexthop=%defaultroute
leftrsasigkey=%cert
leftcert=/etc/ipsec.d/ssl/localCERT.pem
#
leftprotoport=17/1701
#
# IP do usuário remoto, certificado e porta utilizada.
#
right=%any
rightrsasigkey=%cert
rightcert=/etc/ipsec.d/ssl/userCERT.pem
rightprotoport=17/1701
#
# Habilita a configuração para dos usuários.
#
auto=add
keyingtries=3
```

Configuração do L2TPD

O L2TPD utiliza o arquivo */etc/l2tpd/l2tpd.conf* para armazenar as suas configurações, sendo que as configurações a seguir devem ser adaptadas e adicionadas a este após a instalação do L2TPD.

Abaixo temos um exemplo do arquivo de configuração do L2TPD. Neste exemplo, a rede interna utiliza os IP’s 192.168.1.0/24 e uma faixa de IP é reservada para os usuários remotos e definida no parâmetro “IP range” de 192.168.1.128 à 192.168.1.254 no exemplo.

O parâmetro “listen-addr” pode ser usado caso seja interessante que o L2TP especifique os endereços IP’s em vez de especificar todas as interfaces de usuários remotos, porém existe uma outra forma é especificar a interface da rede interna colocando um IP em “listen-addr”com 192.168.1.98 que é mostrado no exemplo.

O IP do parâmetro “local ip” é usado pelo L2TP como seu endereço na interface pppd.

As configurações contidas no exemplo abaixo são consideradas mínimas para o estabelecimento da VPN.

```
Exemplo:
[global]
listen-addr = 192.168.1.98

[lns default]
ip range = 192.168.1.128-192.168.1.254
local ip = 192.168.1.99
require chap = yes
refuse pap = yes
require authentication = yes
name = LinuxVPNserver
ppp debug = yes
# Especifica o local do arquivo de configuração do PPPD
pppoptfile = /etc/ppp/options.l2tpd
length bit = yes
```

Configuração do PPPD

O PPPD armazena as configurações em /etc/ppp/options.l2tpd e /etc/ppp/chap-autenticaiton, as configurações a seguir devem ser adicionadas a estes arquivos após a instalação do PPPD.

A seguir temos um exemplo de configuração do PPPD contendo as configurações necessárias para serem utlizadas na VPN:

```
ipcp-accept-local
ipcp-accept-remote
ms-dns  192.168.1.1
ms-wins 192.168.1.2
auth
crtscts
idle 1800
mtu 1400
mru 1400
nodefaultroute
debug
lock
proxyarp
connect-delay 5000
```

As configurações mostradas devem ser adaptadas e adicionadas ao arquivo etc/ppp/options.l2tpd para que o L2TP possa utilizá-lo.

Autenticação no PPP

Este é um exemplo de configuração para se utilizar à autenticação do PPP com o CHAP, esta autenticação é opcional, pois o IPSec já possui autenticação, as seguintes configurações devem ser adaptadas para a implementação e adicionadas ao arquivo /etc/ppp/chap-secrets se esta autenticação adicional for ser usada:

```
# Chaves para autenticação usando o CHAP [14]
# usuário    servidor     chave                    IP
joao           *          "chavesecreta"           192.168.1.128/25
*              joão       "chavesecreta"           192.168.1.128/25
pedro          *          "rumpelstiltskin         192.168.1.5
*              pedro      "rumpelstiltskin         192.168.1.5
```

Todas as configurações apresentadas nesta seção são baseadas em [22].

Configuração dos Clientes Microsoft

Configuração para Clientes Microsoft rodando windows 98/ME/NT 4.0

Como o Windows 98, ME e NT possuem o mesmo clientes rodando as configurações para os mesmos são análogas.
Uma vez instalados todos os pacotes citados anteriormente juntamente com o MSL2TP, devemos agora realizar a outra parte da configuração do cliente.
Importação de certificados
Para importar certificados, deve se seguir os seguintes passos:
Inicie o Internet Explorer, vá até menu ferramentas e clique em opções de *Internet*, em seguida clique na guia conteúdo e depois em certificados, após isso clique em importar o assistente é iniciado clique em avançar, em seguida clique em procurar e selecione o certificado com extensão *.pfx ou *.p12, clicar em avançar novamente, em seguida entre com o *password* do certificado e clique em avançar, e por último selecione a opção selecionar automaticamente o certificado e clique em finalizar.[21]
Após realizar este procedimento o certificado está disponível para ser usado pelo MSL2TP que foi instalado anteriormente.
Usando Certificados ou PSK
Após a instalação do MSL2TP, aparece no menu iniciar uma pasta chamada "Microsoft L2TP/IPSec VPN Client", e nesta pasta existe um atalho para o L2TPConfig.exe chamado de "Microsoft IPSec VPN Configuration".
Para determinar o tipo de autenticação deve se seguir os seguintes passos:
Clique no menu iniciar e depois no "Microsoft IPSec VPN Configuration", se a autenticação utilizada for a PSK selecione esta opção, mas se a autenticação for através de certificados, selecione qual certificado deve ser usado, e selecione a opção selecionar automaticamente o certificado quando for importar, para finalizar o Microsoft IPSec VPN Configuration clique em Ok para salvar as alterações.[21]

Configuração da conexão VPN
Para configurar a conexão VPN deve se seguir os seguintes passos:
Clique no ícone meu computador no *desktop* e em seguida em acesso à rede *Dial-Up* então clique em fazer uma nova conexão, em seguida entre com o nome da conexão, o dispositivo deve ser "Microsoft L2TP/IPSec VPN Adapter 1" para Windows 98/ME e "RASL2TPM" para Windows NT 4.0, clique então em avançar, entre com o nome do *Host* ou endereço IP do servidor VPN Linux e clique em avançar e depois em finalizar. [21]
Após efetuar a configuração acima, entre nas propriedades da conexão criada, na guia geral selecione a guia tipo de servidor, então desabilite os protocolos IPX e NETBEUI após clique em Ok para finalizar.
Para testar a conexão, clique duas vezes sobre ela e entre com o nome do usuário e senha que devem ser os mesmos definidos em /etc/pp/chap-secrets ou /etc/ppp/pap-secrets no servidor VPN Linux.
Configuração para Clientes Microsoft rodando Windows 2000/XP

Importação de Certificados
Primeiramente, para importar certificados no Windows 2000 e XP, deve se possuir privilégios de administrador, logando no sistema como tal.
Para importar um certificado deve se seguir os seguintes passos:
Deve-se executar o "Console de Gerenciamento Microsoft" clicando no menu iniciar, executar, digitando "mmc" e tecle enter. Após isso, deve-se ir até o menu arquivo e clicar em Adicionar/remover snap-in..., em seguida clique em adicionar, selecionar o item certificados e clicar em adicionar, após escolher conta de computador, pois o IPSec apenas autentica computadores e não pessoas, clicar em "Avançar", escolher então a opção "computador local" e clicar em "Ok" para concluir. O próximo passo a ser feito é escolher o certificado para ser importado, na raiz do console, expandir "Certificados (computador local)" e depois expandir também a pasta "Pessoal", clicar com

o botão direito na pasta certificados, e depois em Todas as Tarefas e Importar, assim o “assistente de importação de certificados” é iniciado, clicar agora em “avançar”, localizar o certificado em “Procurar”, após selecionar o certificado desejado com a extensão *.pfx ou *.p12, clicar em “Avançar” e selecionar a opção “Selecionar automaticamente o armazenamento de certificados conforme o tipo do certificado”, assim o L2TP/IPSec pode localizar o certificado automaticamente, após clicar em “Avançar” e depois em “Concluir”.[21]
Após este procedimento estar concluído, os certificados estão prontos para serem usados pelo L2TP/IPSec para realizar a autenticação.

Configuração usando Certificados ou PSK:

PSK

Como o Windows 2000 não possui suporte a PSK este tipo de configuração sé apenas válida para o Windows XP.
Clicar sobre o menu “Iniciar/Programas/Acessórios/Comunicações”, em seguida clicar no “Assistente para novas conexões” e depois em “Avançar”, após isso escolha a opção “Conectar-me a uma rede em meu local de trabalho” e depois clicar em “Avançar”, selecione então a opção “Conexão VPN (rede privada virtual)” e em seguida clicar em “Avançar”, entre com um nome para a conexão e depois clicar em “Avançar”, se o cliente possuir uma conexão direta com a *Internet* deve-se selecionar esta conexão, caso contrário pode optar por não discar uma conexão e escolher manualmente a conexão quando for conectar à VPN, ”, entre com o nome ou endereço IP do servidor VPN Linux e depois clicar “Concluir”.[21]

Depois que a conexão foi criada, é necessário configurá-la adequadamente. Para isto deve se seguir os seguintes passos:
Deve-se entrar nas propriedades da conexão recém criada. Primeiramente, deve-se verificar se todas configurações da guia “Geral” estão corretas. Após isso, deve ir até a guia “Opções” e verificar todas as opções de discagem e rediscagem. Em seguida deve-se selecionar a guia segurança e desabilitar a criptografia do L2TP/PPP desmarcando a opção “Exibir criptografia de dados(desconectar se não houver)”, pois caso contrário estará utilizando criptografia duas vezes, pois o IPSec já possui ciptografia, pode-se também usar criptografia opcional neste caso, selecionado-se a opção “Avançada(configurações personalizadas)”, escolhendo a opção “Criptografia opcional (conecta mesmo sem criptografia)” e habilitar o protocolo CHAP selecionando a sua opção e clicar em “Ok”. Ainda na guia segurança, deve-se configurar o IPSec clicando no em “Configurações do IPSec...”, selecionar a opção “Usar chave pré-compartilhada para autenticação” e entrar com a mesma chave que foi definida no servidor VPN Linux em /etc/ipsec.secrets. Depois disso, deve-se selecionar a guia rede e mudar o tipo de VPN para “L2TP IPSec VPN”. Por último deve-se selecionar a guia “Avançado”, opcionalmente pode-se habilitar a opção “*Firewall* de conexão com a *Internet*” e o ICS (Compartilhamento de conexão com a Internet), usando este último na conexão VPN pode ser pouco produtivo segundo.[21]

Certificados

Uma vez importados os certificados deve-se configurar a conexão L2TP/IPSec para usar estes certificados na autenticação no servidor VPN Linux. Infelizmente não se pode selecionar o certificado manualmente como no MSL2TP, pois o cliente L2TP/IPSec do Windows 2000/XP escolhe o certificado apropriado automaticamente. Uma exigência para os certificados é que os mesmos devem ser assinados pela mesma autoridade certificadora em ambas as entidades para autenticação.[21]

O procedimento para criar a conexão VPN usando certificados é análogo ao para criar a conexão VPN usando PSK, com a diferença de que dentro das propriedades da conexão recém criada na guia “Segurança” as configurações do IPSec na opção “Configurações do IPSec...” deve estar desmarcada a opção “Usar chave pré-compartilhada para autenticação” para o Windows XP. No Windows 2000 não existe a opção “Configurações do IPSec...” na guia “Segurança”, pois o mesmo não possui suporta a PSK, assim os certificados serão sempre usados, simplesmente seguindo os passos para a criar a conexão VPN usando PSK, desconsiderando apenas os passos referentes as configurações do IPSec.[21]

Após estas configurações serem todas realizadas, é esperado que a VPN funcione normalmente sem grandes problemas. Porém, como nada é totalmente perfeito podem ser que alguns problemas ocorram.