UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

CÍCERO ZANELATO

SEGURANÇA EM REDES ADSL UTILIZANDO REDES PRIVADAS VIRTUAIS E O PROTOCOLO IPSEC: ESTUDO DE CASO

CRICIÚMA, DEZEMBRO DE 2011

CÍCERO ZANELATO

SEGURANÇA EM REDES ADSL UTILIZANDO REDES PRIVADAS VIRTUAIS E O PROTOCOLO IPSEC: ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins.

CRICIÚMA, DEZEMBRO DE 2011

CÍCERO ZANELATO

Segurança em Redes ADSL utilizando Redes Privadas Virtuais e o Protocolo IPSec: Estudo de Caso

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. Gilberto Vieira da Silva (UNESC)
Membro Banca

Prof. MSc. Rogério Antônio Casagrande (UNESC)
Membro Banca

A minha mãe Estela pelo total apoio e compreensão durante a realização deste trabalho.

AGRADECIMENTOS

Primeiramente agradeço a Deus por me dar força e criatividade para a realização deste trabalho, não me deixando desanimar com as pedras que apareceram no caminho.

Agradeço a todos os professores da UNESC que proporcionaram um ótimo aprendizado durante minha vida acadêmica.

Ao meu orientador Paulo, por ter empenhado o seu (pouco) tempo livre para que este trabalho fosse possível e para que conseguíssemos atingir as metas propostas.

Aos colegas que fizeram parte de minha vida durante estes quase cinco anos, discutindo, compartilhando experiências e idéias, e também auxiliando muito nesta pesquisa.

Agradeço também a minha mãe Estela que sempre esteve presente, preocupando-se com meu desempenho e não medindo esforços para ajudar sempre que possível ao longo de todos estes anos, dando toda a força e o apoio necessário.

A minha namorada Allessandra Netto Cancellier, por compreender que nestes últimos meses tive que me dedicar bastante à realização desta pesquisa. Por estar sempre me auxiliando no que fosse possível, além de toda a confiança depositada. Sem o seu apoio e carinho nada disto seria possível.

Por fim, a todos que me ajudaram direta ou indiretamente para o cumprimento das metas propostas, finalizando mais esta jornada em minha vida.

“Você não consegue juntar os pontos olhando para o futuro; você só conseguirá conectá-los se olhar para o passado. Então, você tem de confiar que os pontos se conectarão no futuro. Você precisa acreditar em alguma coisa: em sua determinação, destino, vida, dogma ou o que quer que seja. Essa atitude jamais me decepcionou e tem feito a diferença na minha vida.”

(Steve Jobs)

RESUMO

Atualmente as Redes de Computadores estão por toda parte. É por meio delas que se pode realizar pesquisas, trocar informações e arquivos, como imagens. Com toda essa possibilidade de utilização, frequentemente transitam informações sigilosas, que podem cair nas mãos de pessoas mal-intencionadas. Para evitar este tipo de captura, existem ferramentas que auxiliam na segurança do tráfego de informações em redes públicas. A Rede Privada Virtual (VPN), aliada ao protocolo IPSec, configura uma maneira simples, barata e eficiente de transmitir dados em uma rede não segura, como a Internet. É mais utilizada em grandes empresas, mas também é possível aplicar esta solução para usuários comuns ou pequenas empresas, que se conectam através de Internet ADSL. Este trabalho apresenta e discute o conceito de redes VPN, abordando alguns métodos de segurança e tipos de ataques mais comuns. A partir dos conceitos, são realizados testes utilizando o sistema operacional Linux e o software Openswan, que cria túneis IPSec, verificando sua eficiência como alternativa de segurança para conectar usuários por meio da ADSL. Para isto, o cliente, localizado em uma rede com IP dinâmico, se conecta ao servidor realizando consultas HTTP. Os testes realizados com estas ferramentas demonstram a importância da segurança dos dados que trafegam na rede, e propõe uma forma dos usuários se conectarem e compartilharem recursos encontrados em sua rede local, de forma remota.

Palavras-chave: Segurança da Informação; Redes Privadas Virtuais; Internet ADSL; Openswan; IPSec.

ABSTRACT

Currently, Computer Networks are everywhere. It is through them that you can conduct research, exchange information and files, such as images. With all these possibilities, sometimes secret information can pass, and may fall into the hands of bad intentioned people. To avoid this type of capture, there are tools that assist in traffic of safety information on public networks. The Virtual Private Network (VPN), working together with IPSec protocol, show's a simple, cheap and efficient way of data transfer in an unsecured network, as the Internet. It's used in large enterprises, but it is also possible to apply this solution for common users or small businesses, which are connected through ADSL Internet systems. This coursework presents and discusses the concept of VPN networks, the addressing some security methods and the most common types of attacks. Using simple concepts, tests are made with the Linux operational system and Openswan software, which creates IPSec tunnels, checking its efficiency as an security alternative of connecting users through ADSL. For this, the client, located in a network with dynamic IP, connects to the HTTP server by performing queries. Tests made with these tools demonstrate the importance of data security passing to the network, and proposes a way for users to connect and share resources found in your remotely local network.

Keywords: Security of Information; Virtual Private Networks; ADSL Internet; Openswan; IPSec.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3DES	Triple Data Encryption Standard
AC	Autoridade Certificadora
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
APT	Advanced Packaging Tool
AR	Autoridade Registradora
ARPA	Advanced Research Project Agency
CAST	Carlisle Adams and Stafford Tavares
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List
DES	Data Encryption Standard
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICP	Infraestrutura de Chave Pública
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange Protocol

IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX/SPX	Internetwork Packet Exchange / Sequenced Packet Exchange
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MD-5	Message Digest 5
MIT	Massachusetts Institute of Technology
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NAT-T	Network Address Translation – Transversal
NDIS	Network Driver Interface Specification
NetBEUI	Network Basic Input/Output System Extended User Interface
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technologies
OSI	Open Systems Interconnection

PAP	Password Authentication Protocol
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RFC	Request For Comments
RSA	Rivest Shamir Adleman
SA	Security Association
SAD	Security Association Database
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
SMTP	Simple Mail Transfer Protocol
SPD	Security Police Database
SPI	Security Index Parameter
SRI	Stanford Research Institute
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UCLA	University of California Los Angeles
UCSB	University of California Santa Barbara
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

No início, quando as redes surgiram, não existia grande preocupação relacionada à segurança das informações. As primeiras interligavam universidades, algumas empresas e instituições militares.

Atualmente são a base da comunicação. É por meio delas que se pode realizar a troca de informações com pessoas do mundo inteiro, manter-se atualizados com notícias globais e inclusive realizar pesquisas dos mais variados assuntos.

A tecnologia ADSL (em português, Linha Digital Assimétrica para Assinante) surgiu com a finalidade de permitir uma transferência de dados em alta velocidade por meio de linhas telefônicas comuns. Esta forma de conexão em banda larga hoje é a mais utilizada no Brasil e uma das mais conhecidas no mundo. Seu funcionamento é simples, dividindo a linha telefônica em três canais virtuais. Um é utilizado para voz, um para *download* de alta velocidade, e outro para *upload* de média velocidade (FAGUNDES, 2007).

Esta tecnologia de comunicação por meio das redes públicas possibilita que o usuário realize transações bancárias, compre os mais variados produtos em lojas virtuais, assista cursos on-line e também a utilize como forma de entretenimento. Além disso, várias empresas se comunicam com suas filiais por meio deste tipo de rede, expondo seus dados de forma insegura, correndo o risco de serem capturados e interceptados por pessoas mal intencionadas. Elas são consideradas não confiáveis por não terem grande segurança no tráfego de informações (ROSSI; FRANZIN, 2000).

A partir da necessidade de se utilizar as redes públicas de comunicação – como a ADSL – para trafegar informações de forma segura, surgiu o advento das Redes Privadas Virtuais (VPN, ou Virtual Private Network). Ela fornece um canal privado, criptografado e autenticado semelhante a um túnel, porém de forma virtual, utilizando uma rede pública de

comunicação. Permite que um usuário externo participe na rede interna como se estivesse conectado diretamente a ela (NORTHCUTT et al, 2002).

Apesar de sua maior segurança, as VPNs ainda são suscetíveis a falhas. Para fornecer uma maior integridade e sigilo dos dados foram criados alguns protocolos que tornam mais difícil o acesso aos dados privados.

Baseado em padrões desenvolvidos pela Internet Engineering Task Force (IETF, organização que desenvolve os padrões da Internet), o IP Security Protocol (IPSec) é um conjunto de protocolos que buscam garantir a integridade, autenticidade e confidencialidade na comunicação e transporte dos dados em uma rede IP.

Operando sob a camada três (camada de rede) do modelo Open Systems Interconnection (OSI), do International Organization for Standardization (ISO), o IPSec possui por função a tentativa de impedir a perda de integridade dos dados e falsificação de identidade, implementando autenticação e encriptação, e fornecendo uma segurança na comunicação de máquina-a-máquina. Sua vantagem é que pode ser implementado tanto em modems que possuem suporte a este protocolo, quanto no próprio sistema operacional – por meio de softwares específicos –, não sendo necessário realizar alterações nas aplicações para que utilizem o meio de comunicação mais seguro.

Com a finalidade de aplicar e testar o protocolo IPSec como alternativa de segurança às Redes Privadas Virtuais, foi realizado um projeto de rede VPN voltado para clientes ADSL, simulando esta rede entre dois computadores conectados por meio de modems, verificando primeiramente se é possível aplicar esse protocolo para este tipo de cliente e se promove alguns recursos interessantes no que diz respeito à segurança.

1.1 OBJETIVO GERAL

Realizar o projeto de uma Rede Privada Virtual voltada a usuários ADSL, verificando a segurança fornecida a partir do protocolo IPSec.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos seguem abaixo:

a) entender sobre métodos de segurança – *firewall*, certificados digitais e outros – aplicados em redes de computadores e sua importância;
b) descrever os princípios de utilização de uma VPN;
c) utilizar o protocolo de segurança IPSec aplicado às Redes Privadas Virtuais;
d) realizar um experimento em redes VPN para usuários ADSL, simulando uma rede entre dois computadores conectados por meio de Modems e utilizando o software Openswan, que implementa o protocolo IPSec.

1.3 JUSTIFICATIVA

Quando surgiram as redes públicas de dados – e mais tarde a Internet –, muitas empresas optaram por mover seu tráfego de dados (e possivelmente o de voz) para esta, mas sem desistirem da segurança que ela proporciona. Essa demanda logo levou à criação de VPNs, que são sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas de virtuais porque são meramente uma ilusão (TANENBAUM, 1997).

É uma tecnologia que traz enorme redução de custos e grande facilidade de instalação, tornando-se uma grande alternativa para fornecer segurança em redes IP, como a Internet.

Atualmente várias empresas utilizam-na para interligar suas filiais, que podem estar localizadas há vários quilômetros de distância uma da outra, formando uma Rede de Longa Distância (WAN, ou Wide Area Network).

As Redes Privadas Virtuais utilizam a técnica conhecida como *tunneling*, ou tunelamento, que cria um canal de comunicação – chamado de túnel – e utiliza certificação e criptografia para aumentar a privacidade. Este túnel é uma comunicação do tipo ponto-a-ponto, onde é estabelecido rotas seguras para o tráfego das informações, dificultando interferências e possíveis capturas dos dados que transitam na rede.

Para se conectar a uma VPN, primeiramente é realizada uma autenticação entre dois pontos, permitindo ao sistema verificar se a origem e o destino estão autorizados a acessar a rede. Em seguida o servidor VPN verifica os serviços a qual os usuários têm permissão para acessar. Após a formação do túnel, os pacotes recebem um cabeçalho especial, que permitem a autenticação da informação, e são endereçados ao outro ponto do túnel. Finalmente, os pacotes são criptografados e encapsulados em novos pacotes IP.

Como alternativa de segurança em uma rede VPN pode ser utilizado o IPSec Protocol Suíte, que visa oferecer integridade, confidencialidade e autenticidade. Internamente ele possui vários protocolos implementados, incluindo Internet Key Exchange (IKE), Encapsulating Security Payload (ESP) e Authentication Header (AH). Esses protocolos permitem a troca segura de informações fornecendo sigilo e impedindo que elas sejam modificadas.

As Redes Privadas Virtuais configuram uma maneira simples, eficiente e barata para garantir o tráfego de dados de forma segura. Além de empresas e outras organizações,

elas podem ser utilizadas também em redes residenciais, como as ADSLs, dificultando o acesso e captura dos dados transferidos entre dois ou mais computadores conectados por meio de VPN por pessoas que não tenham permissão para tal.

A sua utilização por usuários ADSL se justifica na necessidade de haver uma conexão segura também para o acesso remoto a dados privados contidos tanto em residências quanto em empresas que fazem uso desta tecnologia para a transmissão e troca de informações. Para isto, é necessária a criação de uma Rede Privada Virtual, utilizando como meio a ADSL, verificando primeiramente se esta tecnologia suporta as técnicas de tunelamento e algoritmos da VPN e se é uma alternativa interessante, principalmente quando não se dispõe de grandes recursos financeiros.

1.4 ESTRUTURA DO TRABALHO

O início desta pesquisa apresenta a definição do problema, bem como objetivos gerais e específicos a serem abordados. Apresenta a justificativa com que ilustra um problema a ser resolvido, apontando a importância das Redes Privadas Virtuais e o benefício que elas podem trazer para a comunicação.

O tema redes de computadores, seus principais conceitos, classificação e tipos mais comuns também estão descritos. Além disso, fala-se sobre a forma com que os dispositivos conectados em rede podem se comunicar, por meio dos chamados Protocolos de Comunicação. Ainda, é abordada a segurança, sua importância, formas, tipos de ameaças e ataques mais comuns, além dos métodos de defesa mais utilizados.

Sobre a tecnologia ADSL, é descrito em que consiste, como funciona, qual a sua finalidade e os principais equipamentos utilizados por esta tecnologia.

Em Redes Privadas Virtuais, fala-se sobre seu conceito, utilização e importância deste tipo de rede, principalmente para organizações que necessitam manter sigilo em seus

dados trafegados. São citados alguns protocolos bem comuns, dando ênfase ao IPSec, no seu modo de funcionamento, forma de transmissão e segurança, apontando suas vantagens e desvantagens e fazendo uma comparação entre outros protocolos de tunelamento.

Nos trabalhos correlatos tem-se a abordagem sobre Segurança, Redes Privadas Virtuais e IPSec, com algumas implementações de VPN. Fala-se também sobre a utilização do protocolo IPSec, que, baseado na segurança em redes de computadores, foram realizadas as etapas de implementação e configuração de uma VPN voltada a usuários ADSL, com testes de segurança deste protocolo.

Por fim tem-se a bibliografia utilizada para o trabalho, contendo livros, dissertações e monografias, bem como nos anexos e apêndices, onde são descritas etapas complementares, que serviram de base para a implementação.

2 REDES DE COMPUTADORES

Segundo Tanenbaum (1997), rede de computadores é um conjunto de computadores autônomos interconectados, que podem trocar informações entre si, por meio de um fio de cobre, fibras ópticas, ondas de infravermelho, micro-ondas, satélites de comunicação, entre outros.

As redes foram criadas com o objetivo de compartilhar recursos aos usuários, como dados, aplicações e equipamentos, independente da localização física tanto do usuário como do recurso (ASSIS, 2003; LIMA, 2009). Ainda, conforme Torres (2001, p. 5), “as redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante de você.”

Itens como escalabilidade [1], confiabilidade [2], e economia de custos [3] foram fundamentais para o desenvolvimento das redes (COMER, 2007).

Como exemplo de rede pode-se citar a Internet. Nela existem milhares de computadores interconectados trocando as mais diversas informações, como arquivos, e-mails, páginas pessoais e corporativas (LIMA, 2009; VASQUES; SCHUBER, 2002).

2.1 CLASSIFICAÇÃO

As redes de computadores possuem diversos tamanhos e classificações. As mais comuns são: Redes Locais (Local Area Network - LAN), Redes Metropolitanas (Metropolitan

[1] Possibilidade de aumentar os recursos à medida que for necessário
[2] Várias fontes alternativas fornecendo o mesmo dado
[3] Troca de computadores de grande porte por computadores pessoais

Area Network - MAN) e Redes de Longa Distância (Wide Area Network - WAN) (VASQUES; SCHUBER, 2002).

LANs são as que conectam computadores, estações de trabalho e instalações industriais de empresas em um único edifício ou campus universitário com até alguns quilômetros de extensão, permitindo o compartilhamento de recursos (como impressoras, por exemplo) e a troca de informações. Possui um tamanho restrito, o que significa que o pior tempo de transmissão é limitado e conhecido com antecedência. O conhecimento desse limite permite a utilização de determinados tipos de projetos que em outras circunstâncias não seriam possíveis, além de simplificar o gerenciamento da rede (TANENBAUM, 1997).

De acordo com Assis (2003), uma Rede Metropolitana utiliza a mesma tecnologia da LAN, sendo, na verdade, uma versão ampliada das Redes Locais. Ela pode abranger um grupo de edifícios vizinhos ou uma cidade toda, podendo ser privada ou pública.

As Redes Geograficamente Distribuídas, ou de Longa Distância, são formadas pela ligação de sistemas de computadores localizados em regiões fisicamente distantes, abrangendo uma grande área geográfica como um país ou continente (ASSIS, 2003; VASQUES; SCHUBER, 2002). A Figura 1 demonstra como funciona essa interligação.

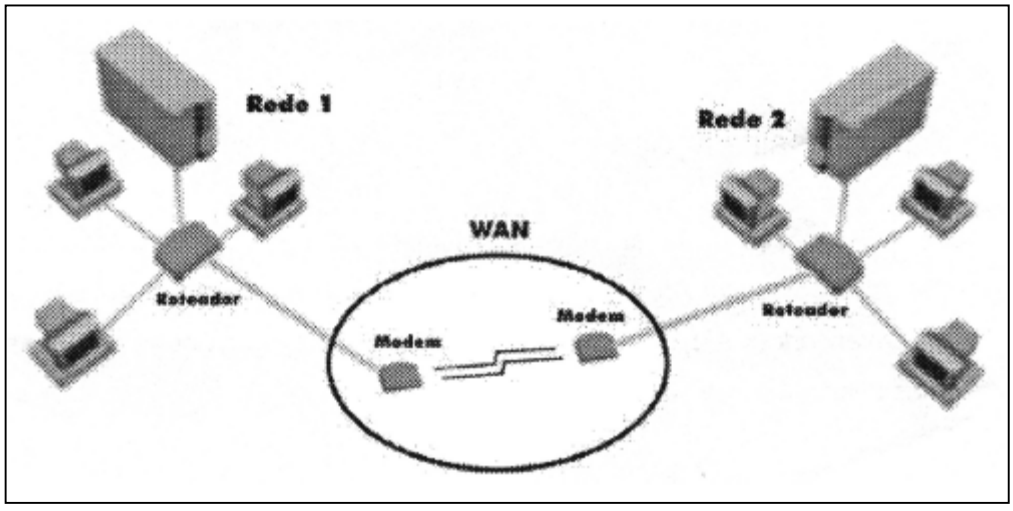


Figura 1. Rede WAN
Fonte: ASSIS, J. M. (2003, p. 5)

Tanto a Rede 1 quanto a Rede 2 são consideradas LANs. Possuem um roteador central que liga algumas estações de trabalho. Ligada nestes roteadores existe o modem, que faz a ligação com a rede externa. Estes dois modems, juntos, formam uma WAN, que nada mais é que duas ou mais LANs/MANs interligadas entre si por meio de modems.

2.2 PROTOCOLOS DE COMUNICAÇÃO

Para Assis (2003) e Vasques e Schuber (2002), protocolo de comunicação é a forma com que os dispositivos conectados em rede podem se comunicar. Para isto, eles devem estar utilizando o mesmo protocolo. Com essa necessidade, vários protocolos foram criados e são utilizados para transmissão de dados. Destacam-se TCP/IP, Network Basic Input/Output System (NetBIOS), Network Basic Input/Output System Extended User Interface (NetBEUI), Interwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) e UDP.

2.2.1 TCP/IP

A Internet teve início quando o departamento de defesa dos Estados Unidos da América (Department of Defense – DoD) criou Advanced Research Project Agency (ARPA), no final da década de 50. No início da década de 60 foi criada a ARPANET, uma rede que tinha por objetivo proteger e transferir informações vitais, tendo em vista a possibilidade de um ataque nuclear por parte da antiga União Soviética. A rede interligava os vários centros de pesquisas: University of Califórnia Los Angeles (UCLA), Stanford Research Institute (SRI), University of Califórnia Santa Barbara (UCSB) e Utah University, e em caso de uma guerra,

se um dos centros fosse destruído, a rede continuaria funcionando (ASSIS, 2003; TEIXEIRA et al, 1999; VASQUES; SCHUBER, 2002).

Aos poucos a ARPANET difundiu-se para centenas de universidades, repartições públicas e outros institutos, como o National Aeronautics and Space Administration (NASA) (TANENBAUM, 1995; VASQUES; SCHUBER, 2002).

Segundo Tanenbaum (1997), no momento em que as redes de rádio e satélite foram criadas começaram a surgir problemas com os protocolos existentes, forçando a criação de uma nova arquitetura de referência. Foi então que, na década de 70, surgiu o conjunto de protocolos que até hoje é a base da Internet, o Transmission Control Protocol/Internet Protocol (TCP/IP), também conhecido como Protocolo de Internet. O nome é derivado dos dois principais protocolos da arquitetura, o TCP e o IP (ASSIS, 2003).

O Protocolo de Internet foi criado pensando em redes grandes e de longa distância, onde a informação pode percorrer diferentes caminhos para chegar ao computador receptor (TORRES, 2001). Para Teixeira et al (1999), este protocolo fornece um sistema aberto, pois muitas de suas implementações e especificações são disponíveis publicamente, fazendo dele a forma mais usada atualmente para comunicar computadores remotos. Ele serve de base para a Internet, que é uma rede de longa distância com nós interligados pelo mundo todo.

Assim como no modelo de referência OSI, a arquitetura do TCP/IP pode ser organizada em camadas. Para este protocolo é utilizado o modelo com quatro camadas, sendo elas: Aplicação, Transporte, Rede e Interface de Rede. A Figura 2 faz relação entre as camadas do modelo OSI/ISO e TCP/IP (TEIXEIRA et al, 1999).

Figura 2. OSI versus TCP/IP
Fonte: TEIXEIRA, J. H. et al (1999, p. 107)

A camada de Aplicação contém todos os protocolos de nível mais alto, faz a comunicação entre os aplicativos e o protocolo de transporte, fornecendo a interface do usuário da rede na forma de aplicativos e serviços de rede. Dentre eles estão: o protocolo de terminal virtual (TELNET), que permite que o usuário de um computador se conecte a uma máquina distante e trabalhe nela; o de transferência de arquivos (FTP), onde se pode mover dados com eficiência de uma máquina para outra; o de correio eletrônico (SMTP), especializado para transferência de arquivos (e-mails, por exemplo); o de serviços de nomes e diretórios (DNS), que mapeia os nomes de *hosts* (computadores) para seus respectivos endereços de rede; e outros (TANENBAUM, 1997; TEIXEIRA et al, 1999; TORRES, 2001).

A Figura 3 mostra o funcionamento da camada de Aplicação, a forma como ela se comunica com as camadas superiores e inferiores e quais as portas padrão para cada serviço.

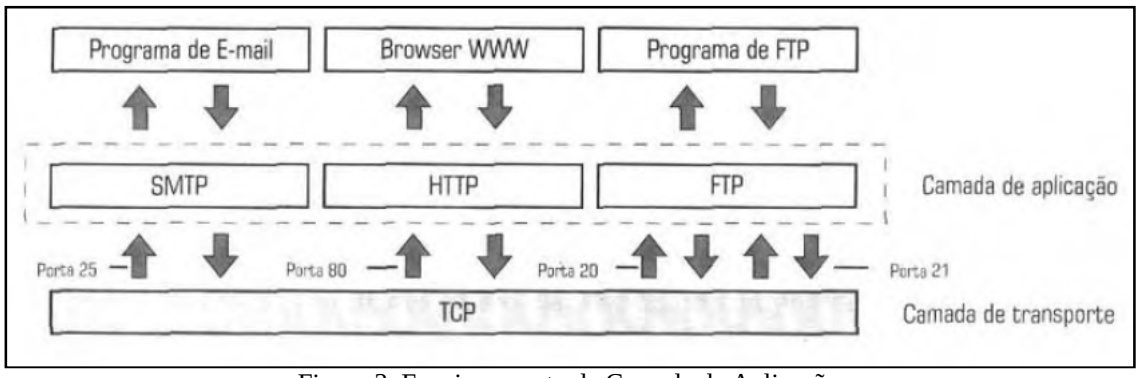


Figura 3. Funcionamento da Camada de Aplicação
Fonte: TORRES, G. (2001, p. 66)

Assis (2003) e Torres (2001) explicam que a camada de Transporte tem a finalidade de permitir que pares de *hosts* mantenham uma comunicação fim a fim confiável. Ela é responsável por transformar os dados enviados pela camada de aplicação em pacotes e repassá-los à camada de rede.

A camada de Transporte possui dois protocolos que são considerados os mais importantes: User Datagram Protocol (UDP) e Transmission Control Protocol (TCP). Por meio do TCP é realizado o controle de fluxo – impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens maior do que este pode manipular –, controle de erro, multiplexação e sequenciamento do acesso à camada de Rede. O UDP tem a função de realizar apenas a multiplexação, para que várias aplicações possam acessar o sistema de comunicação de forma coerente (ASSIS, 2003; TANENBAUM, 1997).

A camada de Rede, também conhecida como camada de Internet, tem a função de permitir que os *hosts* enviem pacotes em diferentes tipos de rede, garantindo que estes trafeguem independentemente até o destino (possivelmente em uma rede diferente) (TANENBAUM, 1997; COMER, 2007). De acordo com Assis (2003), quando ocorre uma transmissão de pacotes entre redes diferentes, o IP é quem garante que eles sejam transmitidos, independente do destino.

Tanenbaum (1997) explica que os pacotes podem ser entregues fora da ordem que foram enviados, devido à possibilidade deles assumirem rotas diferentes para alcançar o destinatário. Caso a entrega em ordem seja desejável, as camadas superiores – aplicação ou transporte – devem reorganizá-los.

A camada de Interface de Rede é responsável pela transmissão de dados através de um meio físico (cabos metálicos, por exemplo) (TEIXEIRA et al, 1999). Conforme Assis (2003) e Comer (2007), para fazer o envio destes dados ou pacotes (chamados de Pacotes IP) existem alguns protocolos criados com este objetivo e dependendo do *host* e da rede o protocolo muda.

Além disso, realiza também o mapeamento entre um endereço de identificação da camada de Rede para um endereço físico ou lógico do nível de Interface de Rede.

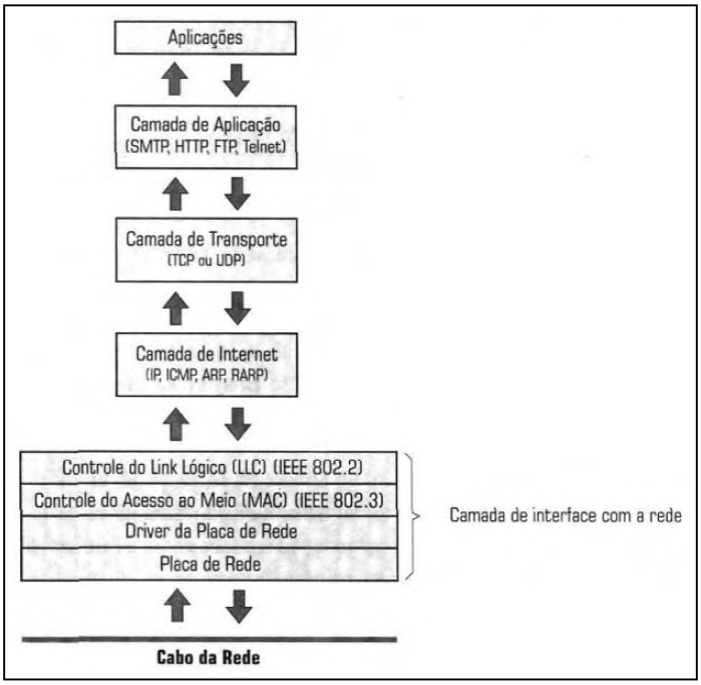


Figura 4. Funcionamento do TCP/IP e suas respectivas camadas
Fonte: TORRES, G. (2001, p. 68)

A Figura 4 mostra um computador operando com o protocolo TCP/IP, com as quatro camadas (Aplicação, Transporte, Rede e Interface de Rede). Segundo Torres (2001),

dependendo do sistema operacional do usuário, o esquema apresentado nesta figura poderá ter mais uma camada no topo da camada de Interface com a Rede, chamada de Network Driver Interface Specification (NDIS), caso o sistema operacional use esse padrão.

2.2.2 IP

O protocolo TCP/IP é roteável, ou seja, permite intercomunicar várias redes por diversos caminhos que interligam o transmissor e o receptor. Para isto, ele utiliza um esquema de endereçamento lógico, chamado de endereçamento IP (TORRES, 2001).

Para Teixeira et al (1999), o IP não possui a função de oferecer um serviço confiável. Ele foi projetado apenas para permitir a interconexão de redes para formar as inter-redes (Internets). Uma inter-rede consiste em *hosts* conectados a redes que são interligadas por meio de *gateways* (computador ou dispositivo responsável pela ligação entre duas redes), e identificados por endereços IP.

Por ser um protocolo sem conexão, cada datagrama IP é tratado como uma unidade independente que não possui ligação com nenhum outro datagrama. Os pacotes que trafegam na rede são independentes, podendo ser fragmentados e enviados por meio de rotas diferentes, chegando fora de ordem no destinatário. O mecanismo de montagem do destinatário se encarrega de reorganizar os pacotes fragmentados à medida que eles forem chegando (FOROUZAN, 2009; TEIXEIRA et al, 1999).

Murhammer et al (2000) afirma que os pacotes podem ser perdidos, mas o IP não se responsabilizará por estas situações. Os protocolos de camada mais alta possuem a função de tratar dessas situações.

Conforme Soares, Lemos e Colcher (1995), um endereço IP não identifica uma máquina individual, e sim uma conexão à inter-rede. Portanto, para ser capaz de identificar um *host* na Internet, cada conexão à inter-rede possui seu próprio endereço IP. Este endereço na sua versão mais utilizada (chamada de IPv4) consiste em números com 32 *bits* escritos em quatro octetos separados por um ponto, e na forma decimal. Por exemplo: 128.31.7.40. Este padrão de endereços é descrito na Request For Comments (RFC) 1166 – Internet Numbers (números da Internet). Uma RFC é um documento que descreve os padrões de cada protocolo da Internet antes de ser considerados um padrão (MURHAMMER et al, 2000).

Para facilitar a distribuição dos endereços IP, foram especificadas cinco classes, ilustradas na Figura 5 (ASSIS, 2003).

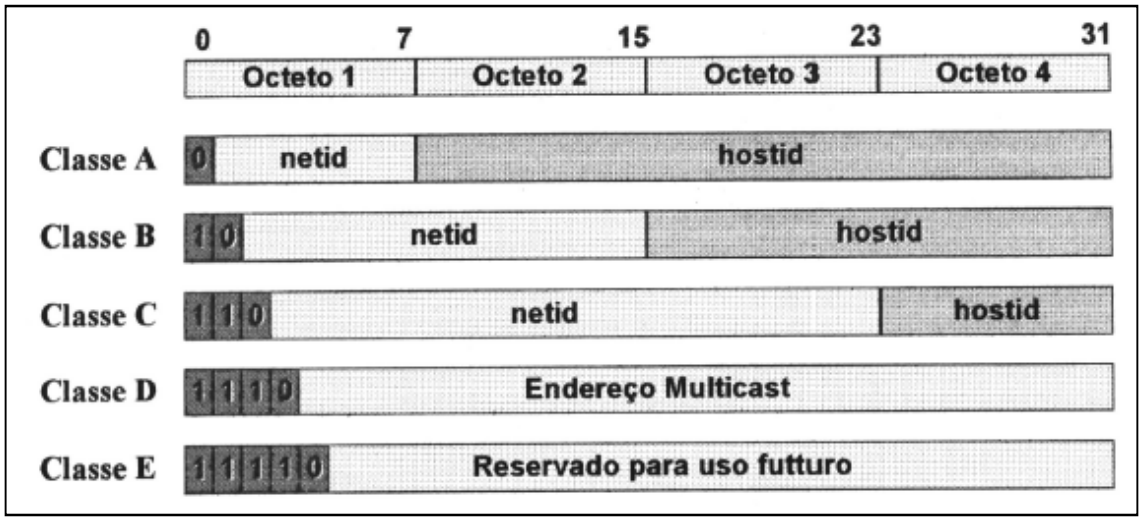


Figura 5. Classes de rede
Fonte: ASSIS, J. M. (2003, p. 14)

A primeira classe de endereços, classe A, é utilizada para redes de grande porte, como a ARPANET, por exemplo. Nela, o *bit* mais significativo é 0, os outros 7 *bits* do primeiro octeto identificam a rede (*netid*) e os 24 restantes definem o endereço local. Com isto, é possível endereçar 16.777.216 máquinas em cada uma das 126 redes disponíveis (TORRES, 2001).

Na classe B é utilizado 14 *bits* para o número de rede e 16 *bits* para endereçar os *hosts*. Cada uma das 16.382 redes pode interligar aproximadamente 65 mil *hosts* (SOARES; LEMOS; COLCHER, 1995).

A classe C utiliza três octetos – ou 21 *bits* – para identificar a rede e 8 *bits* para os *hosts*. Assim é possível criar 2.097.150 redes com 254 *hosts* em cada. É a classe mais utilizada para endereçamento de máquinas, por definir configurações com poucos computadores e muitas redes (MURHAMMER et al, 2000; TEIXEIRA et al, 1999).

Segundo Murhammer et al (2000), os endereços classe D são reservados para *multicasting* – um tipo de transmissão com uma área limitada, apenas para *hosts* que estejam usando o mesmo endereço classe D. Os da classe E são reservados para uso futuro.

Tabela 1. Separação dos bits fixos no início de cada classe de endereço IP

Classe	Endereço mais baixo	Endereço mais alto
A	1.0.0.0	126.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

Fonte: TORRES, G. (2001, p. 71)

A Tabela 1 mostra a separação dos *bits* fixos no início de cada classe de endereços IP. Alguns endereços, como o 127.x.x.x, não aparecem na tabela, pois são de uso reservado, com a finalidade de testar a rede (TORRES, 2001).

Atualmente o número de dispositivos conectados à rede só aumenta. Com isso, o número de endereços IP disponíveis – que pareciam inatingíveis na época da sua invenção – está ficando cada vez mais escasso. Para resolver este impasse foi criada uma nova versão de

endereço IP, chamado de IP versão 6 (IPv6). O IPv6 utiliza um endereço de 128 *bits*, sendo possível alcançar o número de 340.282.366.920.938.463.463.374.607.431.770.000.000 combinações diferentes (TORRES, 2001).

Conforme Assis (2003) e Forouzan (2009), além de aceitar vários *hosts*, o IPv6 reduz o tamanho da tabela de roteamento, simplifica o processo – permitindo que roteadores processem os pacotes com mais rapidez –, oferece mais segurança, permite que um *host* mude de lugar sem mudar o endereço e tem um cabeçalho simplificado, fazendo com que os roteadores processem-no mais rapidamente, melhorando a eficiência da transmissão.

2.2.3 TCP

O Protocolo de Controle de Transmissão (Transmission Control Protocol – TCP), descrito na RFC 793, é orientado à conexão, possuindo a finalidade de fornecer um circuito lógico ou serviço de conexão confiável, o que permite a entrega dos pacotes entre o transmissor e o receptor sem que haja perdas (FOROUZAN, 2009; MURHAMMER et al, 2000). Além disso, segundo Teixeira et al (1999), faz a retransmissão de pacotes perdidos, a eliminação de duplicados, o fornecimento de avisos de recebimento para pacotes recebidos com sucesso, entre outros.

Para que a transferência do fluxo de dados seja efetuada, tanto o transmissor como o receptor criam pontos terminais chamados *socket*. Cada *socket* possui um número que define o endereço IP do *host* agregado a mais um número de 16 *bits* local para este, chamado porta. A porta identifica o acesso a um serviço, que é utilizado quando é criada uma conexão explícita entre o transmissor e o receptor (ASSIS, 2003; FOROUZAN, 2009).

2.2.4 UDP

Descrito na RFC 768, o User Datagram Protocol (UDP) é basicamente uma interface de aplicação para o IP. Segundo Murhammer et al (2000), ele não proporciona confiabilidade, controle de fluxo ou recuperação de erros IP. Serve simplesmente como um multiplexador/demultiplexador para o envio e o recebimento de datagramas, fazendo uso de portas para direcionar os datagramas. Por isso, é utilizado em aplicações que não necessitam de entrega precisa e sim entrega imediata, como voz e imagem (ASSIS, 2003).

Além disso, como em TCP, o UDP emprega campos especiais para identificar os processos emissores e os processos recebedores para cada transação – as portas. Um mecanismo de sumarização de verificações (*checksum*) também é fornecido (TEIXEIRA et al, 1999).

3 SEGURANÇA EM REDES DE COMPUTADORES

Não existe pretensão de abordar todos os aspectos que envolvem segurança em redes de computadores, visto que atualmente existem vários pontos importantes que se deve relevar. Apresenta-se apenas um breve histórico para entendimento acerca do assunto, facilitando a compreensão do que motivou a realização deste trabalho.

O termo segurança é utilizado como significado de minimizar a vulnerabilidade de bens e recursos. Em redes de computadores, está relacionada à necessidade de proteção contra o acesso ou manipulação de informações, confidenciais ou não, por elementos não autorizados (SOARES; LEMOS; COLCHER, 1995; WADLOW, 2000).

A segurança da informação é um conjunto de normas, procedimentos, orientações e demais ações que tem por objetivo proteger a informação. Além disso, para uma organização, ela existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da mesma (FONTES, 2006). Sem a informação, ou conhecimento, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas (FONTES, 2006).

Para Fagundes (2007), quando se fala em segurança da informação presumem-se três premissas que devem ser atendidas: Confidencialidade, Integridade e Autenticidade. Em serviços pela rede, também é necessário garantir a Disponibilidade dos recursos.

A confidencialidade visa assegurar que o conteúdo de um pacote enviado pela rede não será “legível” para intrusos, mas apenas para o real destinatário. Para isso, geralmente é feito o uso de Criptografia (VASQUES; SCHUBER, 2002; WADLOW, 2000).

A Integridade é a garantia de que os dados não serão alterados durante uma transmissão. Já a autenticidade garante que a mensagem foi realmente enviada pelo emissor esperado (AGUIAR, 2005; VASQUES; SCHUBER, 2002).

Disponibilidade é garantir que um serviço esteja disponível quando for solicitado, mesmo em caso de ataques (ASSIS, 2003).

Segundo Soares, Lemos e Colcher (1995), a necessidade de proteção deve ser descrita formalmente nos termos de uma política de segurança, definida por base nas possíveis ameaças e riscos e nos objetivos da organização. Ela consiste em um conjunto de leis, regras e práticas que regulamentam a forma como uma organização distribui, gerencia e protege os recursos de rede e as informações (AGUIAR, 2005; FOROUZAN, 2006).

Uma boa política de segurança deve conter detalhes de como recursos e informações devem ser disponibilizados e utilizados. Eles devem ser tratados de acordo com seu grau de sensibilidade e das formas de acesso suportadas por um sistema (AGUIAR, 2005; SOARES; LEMOS; COLCHER, 1995).

A implementação de uma política de segurança se baseia em aplicar regras que limitam o acesso a informações e recursos, permitindo o acesso conforme o nível de autorização do usuário em relação àquela informação ou recurso. Deste modo, ela define o que é ou não permitido em termos de segurança durante a operação de um determinado sistema (FOROUZAN, 2006; SOARES; LEMOS; COLCHER, 1995). Conforme Aguiar (2005), a sua implantação pode ser feita de forma eficiente com a utilização de vários mecanismos, como criptografia, *firewall*, função *hash*, entre outros.

3.1 AMEAÇAS E ATAQUES

Para se ter uma rede segura e confiável, deve-se estar atento às principais ameaças que podem comprometer a integridade das informações. O ataque ocorre quando uma ameaça tenta levar vantagem sobre uma vulnerabilidade. Os ataques podem ser de duas formas: ativos ou passivos (TEIXEIRA et al, 1999).

Para Soares, Lemos e Colcher (1995), os ataques passivos, quando realizados, não resultam na modificação das informações contidas em um sistema, em sua operação ou em seu estado, apenas observam a informação que trafega. Teixeira et al (1999) aponta que um bom exemplo de ataque passivo é o monitoramento do tráfego em uma rede, que pode permitir a leitura de uma senha de acesso.

Os ataques ativos alteram o sistema e as informações na tentativa de levarem vantagem sobre sua vulnerabilidade. Este tipo é mais difícil de prevenir, sendo possível, na maioria das vezes, apenas detectá-lo (TEIXEIRA et al, 1999).

3.2 TIPOS DE ATAQUES

Para implementar a segurança em uma rede, primeiramente é necessário saber os tipos de ataques mais comuns, para que seja utilizado o método correto de defesa em cada situação.

Conforme Murhammer et al (2000), o ataque por interrupção visa tornar os recursos da rede indisponíveis e não-funcionais. O principal ataque deste tipo é o Denial of Service (DoS), que consiste no envio de requisições em massa para um determinado *host*, de modo que ele fique sobrecarregado e não consiga responder todas elas, fazendo com que o serviço pare de funcionar (VASQUES; SCHUBER, 2002).

O ataque de interceptação tem por objetivo capturar as informações que estão sendo transmitidas pela rede, conseguindo acesso a dados e senhas (MURHAMMER et al, 2000).

De acordo com Soares, Lemos e Colcher (1995), outro ataque convencional é o de modificação, onde o conteúdo das mensagens é alterado. Isto implica em efeitos não autorizados, onde o sistema não consegue detectar alteração.

O ataque de fabricação tem como finalidade se passar por um usuário do sistema. Todas as informações transmitidas em rede são obtidas, atacando a sua autenticidade. O ataque mais comum deste tipo é o IP *Spoofing*, que substitui o endereço IP no computador do invasor e faz com que ele se passe por um computador confiável na rede, obtendo privilégios na comunicação, nos recursos e nas informações (VASQUES; SCHUBER, 2002).

3.3 MÉTODOS DE DEFESA

Conforme Scrimger et al (2002), existem dois aspectos na segurança da rede que deve-se levar em conta: proteger o acesso aos dados e proteger a transmissão dos dados. Sistemas de segurança como *firewalls* tem o objetivo de evitar que ataques sejam feitos contra uma rede ou um sistema específico. Isto pode impedir ou mesmo dificultar que pessoas mal-intencionadas consigam explorar vulnerabilidades, com o objetivo de penetrar no sistema para roubar, inserir ou modificar informações (TORRES, 2001).

Segundo Vasques e Schuber (2002), existem vários métodos de defesas disponíveis para os tipos de ataque existentes. Entretanto, para Redes Privadas Virtuais, os mais importantes são: *Firewall*, *Firewall* e VPN, Criptografia, Assinatura Digital e Certificado Digital.

3.3.1 *Firewall*

De acordo com Murhammer et al (2000), para garantir a segurança da informação em uma organização, os *firewalls* possuem funções significativas. Ele é um sistema – ou grupo de sistemas – que reforça a segurança entre uma rede interna e uma rede não-confiável, como a Internet. Murhammer et al (2000) afirma que os *firewalls* tendem a serem vistos como

uma proteção entre a Internet e a rede privada. Mas em geral, deveriam ser considerados apenas como um meio de dividir o mundo em uma ou mais redes, seguras ou não.

O *firewall* funciona como uma espécie de porteiro em uma rede. É ele quem decide quais pacotes podem entrar ou não, assim como também determina quais podem sair ou não dela. Existem um conjunto de regras específicas implementadas que promovem as ações de bloquear, negar, rejeitar ou aceitar os pacotes (FAGUNDES, 2007). A Figura 6 ilustra o *firewall* funcionando como uma barreira para a entrada e saída dos dados em uma rede interna.

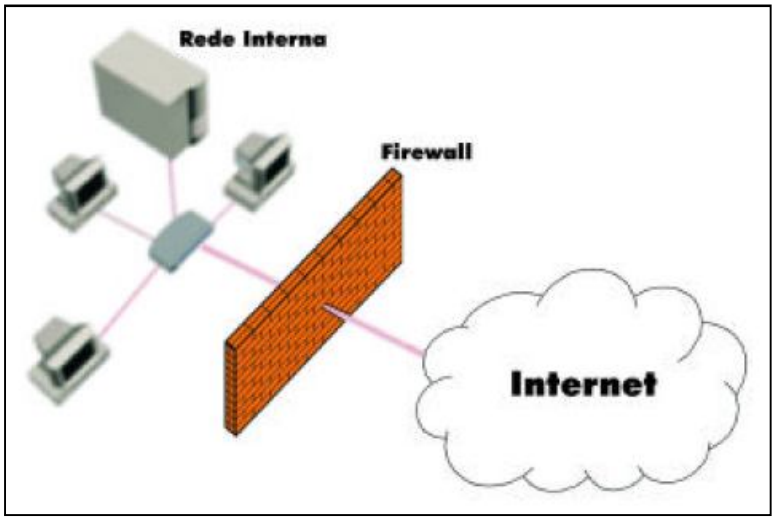


Figura 6. Exemplo de um *Firewall*
Fonte: VASQUES, A. T.; SCHUBER, R. P. (2002, p. 15)

Eles podem ser de três tipos: de filtro de pacotes, de inspeção de pacotes com confirmação de estado e de aplicativos de *Proxy*, que é um software utilizado para permitir o acesso de uma rede à Internet, geralmente por meio de um *firewall*. Conforme Aguiar (2005), na filtragem de pacote, quando ele passa pela interface do *firewall*, este analisa os campos de endereço de IP da origem e do destino e a porta de serviço TCP/IP de origem e destino. Com essa análise é possível permitir, bloquear ou redirecionar o tráfego.

A inspeção de pacotes com informações de estado desempenham as funções do filtro de pacotes e também inspecionam o estado da conexão – apenas conexões previamente estabelecidas e válidas, que cumprem as condições pré-configuradas, têm acesso à rede. Uma das vantagens é não ter a necessidade de configurar cada computador dentro da rede (VASQUES; SCHUBER, 2002).

Ainda, segundo Vasques e Schuber (2002), os aplicativos de *firewall* e de *Proxy* varrem todos os dados que passam por eles, descartando os perigosos ou não autorizados, nunca deixando um computador que se encontra dentro da rede ficar exposto às redes externas.

Com o seu uso, a segurança dos *hosts* e serviços de uma rede ficam concentrados em um ponto central, não sendo necessário configurar todos os computadores e serviços oferecidos para implementar o nível de segurança desejado. Ele permite também o bloqueio do acesso externo às informações do servidor DNS da rede privada. Desse modo, os nomes e endereços IPs das máquinas da rede interna não ficam disponíveis para usuários externos (AGUIAR, 2005). Outra vantagem, segundo Aguiar (2005), é ter acesso a informações da utilização da rede, pois todo o tráfego da mesma passa através dele. Estes acessos podem ser registrados e usados pelo administrador de rede para realizar análises da utilização dos recursos pelos usuários.

3.3.2 *Firewall* e VPN

Para Vasques e Schuber (2002), uma VPN permite interligar duas ou mais redes, fornecendo um canal seguro de comunicação, tornando-se uma ferramenta útil para proteger dados privados. Porém não deve ser a única alternativa de segurança para a rede, pois quanto maior a segurança aplicada, maior dificuldade para acessar os dados.

Aliado a um *firewall*, os *gateways* VPN tornam-se uma boa alternativa para garantir a segurança do tráfego de dados (NORTHCUTT et al, 2002). Segundo Vasques e Schuber (2002), existem três opções de interações: *gateway* VPN dentro, paralelo ou atrás de um *firewall*.

A primeira opção de interação parece a mais simples e rápida, pois a segurança é feita apenas por meio de um computador. Porém, o *firewall* deve ser extremamente seguro, pois qualquer erro na configuração das regras no controle de acesso pode permitir que o tráfego oriundo da Internet penetre na rede utilizando endereços de VPN, sem que seja percebido (NORTHCUTT et al, 2002; VASQUES; SCHUBER, 2002).

A segunda interação existente separa o tráfego de uma VPN do tráfego da Internet em dois ou mais computadores. Assim, devido ao fato de informações transmitidas à Rede Privada Virtual não passarem pelo *firewall*, não se faz necessário nenhuma configuração adicional para permitir a passagem dos pacotes VPN. Entretanto, caso não esteja bem seguro, isso faz com que o *gateway* VPN torne-se vulnerável a ataques externos (VASQUES; SCHUBER, 2002).

A terceira opção faz com que todo o tráfego oriundo da Internet, que trafega na VPN, passe primeiramente pelo *firewall*, deixando a rede mais segura. Em função disso, o mesmo deve possuir uma rota específica para redirecionar o tráfego da Rede Privada Virtual. Uma das desvantagens desta opção é a queda de performance na comunicação (VASQUES; SCHUBER, 2002).

3.3.3 Criptografia

A criptografia surgiu a partir da necessidade de realizar-se o envio de informações sigilosas por meios de comunicação não confiáveis, onde não se tem a possibilidade de garantir que um intruso seja impedido de interceptar o fluxo de dados para leitura ou até mesmo modificação, de modo a detectar se a informação foi ou não alterada ou lida no caminho entre o remetente e o receptor (SOARES; LEMOS; COLCHER, 1995; TEIXEIRA et al, 1999).

Segundo Murhammer et al (2000), o processo de criptografia transforma a mensagem original em uma forma ilegível por meio do algoritmo criptográfico, com o objetivo de ocultar seu significado. Tem como resultado a mensagem cifrada, compreensível apenas para quem tem autorização para lê-la. No receptor, o mesmo algoritmo criptográfico faz a decifragem do código, obtendo a mensagem original (ASSIS, 2003).

Atualmente, nos algoritmos utilizados, a criptografia e a decifração utilizam um parâmetro, a chave. Ela consiste em uma sequencia de *bits* e pode ser escolhida a partir de um conjunto de valores possíveis, chamados de espaço de chaves. Estes espaços são geralmente bem amplos, quanto maior melhor. E, dependendo o tipo de chave utilizada, a criptografia pode se classificar em simétrica e assimétrica (FAGUNDES, 2007; MURHAMMER et al, 2000).

A criptografia de Chave Secreta – ou Simétrica – faz uso da mesma chave para criptografar e decifrar a mensagem, transformando-a novamente em um texto convencional (BRAZIL, 2007; MURHAMMER et al, 2000).

Conforme Aguiar (2005), a cifragem de uma mensagem baseia-se em um algoritmo e uma chave. O algoritmo converte a mensagem original em uma mensagem

cifrada, e vice-versa. A chave é trocada ou combinada entre o receptor e o transmissor antes que a transmissão seja efetuada (FAGUNDES, 2007).

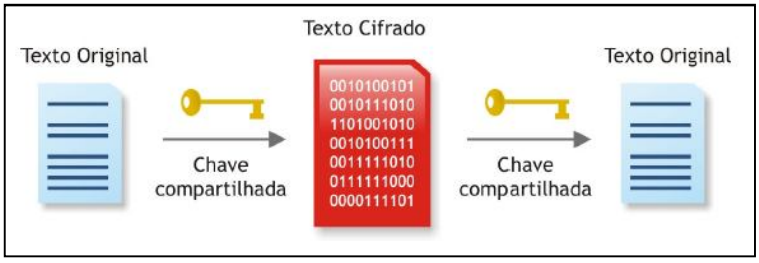


Figura 7. Criptografia Simétrica
Fonte: FAGUNDES, B. A. (2007, p. 15)

A Figura 7 demonstra o processo. A mensagem é cifrada com uma chave compartilhada entre o transmissor e o receptor e então é enviada. O receptor decifra a mensagem com a chave compartilhada, tendo acesso à informação original.

Apesar de este método ser simples, Aguiar (2005) e Assis (2003) apontam que ele possui alguns problemas. Um deles é que a chave é utilizada para cada par emissor-receptor, portanto, se o número de pares for grande será necessário um grande número de chaves, dificultando a gerência das mesmas e acarretando no comprometimento da segurança, visto que nem sempre é possível o seu armazenamento de forma segura. Outro problema decorrente deste tipo de criptografia é que não é possível garantir a identidade de quem enviou ou recebeu a mensagem (AGUIAR, 2005; BRAZIL, 2007).

Existem alguns algoritmos simétricos que produzem chaves de diversos tamanhos. Pode-se citar o Data Encryption Standard (DES), que, segundo Fagundes (2007), é um algoritmo de bloco com diferentes modos de operação, a serem escolhidos baseados na finalidade com que serão usados. Cria chaves de 56 *bits*. Já o Triple Data Encryption Standard (3DES) surgiu para substituir o DES, tornando-o pelo menos duas vezes mais seguro, utilizando o algoritmo de criptografia três vezes, com três chaves diferentes e consegue gerar

chaves de até 112 *bits*. Por ser mais rápido, o algoritmo Advanced Encryption Standard (AES) substituiu o 3DES. Possui chaves de 128, 192 e 256 *bits* (FAGUNDES, 2007; VASQUES; SCHUBER, 2002).

Segundo Assis (2003), Vasques e Schuber (2002), existem outros algoritmos, como o Blowfish (448 *bits*), o Twofish (128, 192 ou 256 *bits*), o Carlisle Adams and Stafford Tavares (CAST), de 128 ou 256 *bits*, o Serpent (128, 192 ou 256 *bits*), entre outros.

Outro tipo de criptografia, a Assimétrica ou de Chave Pública, baseia-se na utilização de chaves distintas – uma para a codificação e outra para a decodificação (SOARES; LEMOS; COLCHER, 1995). Murhammer et al (2000) aponta que nesta forma de criptografia existem dois tipos de chaves, a pública e a privada. Um texto criptografado com chave pública só pode ser decifrado com a chave privada correspondente, e vice-versa, sendo uma chave complementar da outra.

O usuário remetente utiliza a chave pública do destinatário para enviar uma mensagem e o usuário destinatário usa uma privada para decodificar a mensagem. Como somente o destinatário possui a chave secreta, a mensagem pode ser enviada confidencialmente (TEIXEIRA et al, 1999).

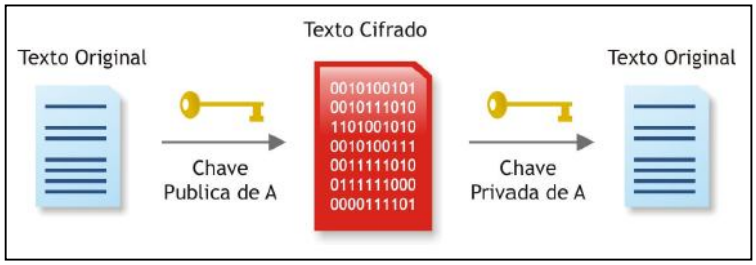


Figura 8. Criptografia Assimétrica
Fonte: FAGUNDES, B. A. (2007, p. 18)

A Figura 8 mostra o processo de cifragem e decifragem pelo método de Criptografia Assimétrica. A mensagem é cifrada com uma chave pública e então é enviada. O

receptor decifra a mensagem com sua chave privada, tendo acesso à mensagem original. Como as chaves são complementares, se a mensagem foi cifrada por uma delas, somente a outra correspondente poderá decifrá-la.

Diferentemente da criptografia simétrica, na assimétrica, cada usuário deve apenas se preocupar com a segurança de sua chave privada, não sendo necessário o envio das mesmas (FAGUNDES, 2007). Além disso, conforme Teixeira et al (1999), a criptografia assimétrica também é utilizada para realização do processo de assinatura digital, que consiste em conduzir informações adicionais para assegurar ao destinatário a identidade do remetente.

Como exemplo de algoritmo deste tipo de criptografia, pode-se citar o Rivest Shamir Adleman (RSA). Composto por chaves de 512, 768, 1024 ou 2048 *bits*, é a base da maioria das aplicações de criptografia assimétrica utilizadas atualmente, pois seus mecanismos dificultam a obtenção da chave utilizada (VASQUES; SCHUBER, 2002). Outro algoritmo assimétrico, segundo Fagundes (2007), é o Elliptic Curve Cryptography (ECC). Ele possui segurança comparável ao RSA, com a vantagem de trabalhar com chaves menores, tornando-se ideal para aplicações onde processador, memória e tráfego de rede são recursos críticos. Ele pode atuar com chaves de 160, 224, 256, 384 ou 512 *bits*.

Tanto o ECC quanto o RSA utilizam criptografia em blocos e possuem forte segurança, devido ao alto poder computacional necessário para se quebrar uma chave. Podem ser usados tanto para cifrar informações como para servir de base para um sistema de assinatura digital. Este tipo de algoritmo é amplamente utilizado na implementação com IPSec (FAGUNDES, 2007).

3.3.4 Função *Hash*

A função *Hash* leva os dados de entrada de tamanho variável e produz dados de saída com tamanho fixo, conhecidos como Resumo. Além disso, uma propriedade desta função diz que elas devem ser de mão única, ou seja, devem ser fáceis de calcular, mas impossíveis de reverter, não sendo possível obter uma mensagem original por meio de um resumo, garantindo a integridade da mesma (MURHAMMER et al, 2000; VASQUES; SCHUBER, 2002).

Segundo Assis (2003, p. 23), "os algoritmos que implementam a função *hash* tem como objetivo fazer com que o resumo sofra uma grande modificação se algum caractere do conteúdo da mensagem for alterado." Dentre os principais, pode-se citar o Message Digest 5 (MD-5), que retorna um resumo de 128 *bits* – o que é mais rápido –, o Secure Hash Algorithm 1 (SHA-1), que retorna um resumo de 160 *bits* (mais lento, porém mais seguro) e o Secure Hash Algorithm 2 (SHA-2) que retorna um resumo que pode ter 256, 384 e 512 *bits*.

Este tipo de função é geralmente mais rápida que algoritmos de criptografia, portanto é comum computar a assinatura digital de um documento ou mensagem cifrando apenas o valor *hash* do documento o qual, normalmente, é muito menor quando comparado com o documento todo. Adicionalmente, este valor pode ser publicado sem revelar o conteúdo do documento com o qual foi gerado (BRAZIL, 2007).

3.3.5 Assinatura Digital

Uma assinatura digital visa garantir ao receptor da mensagem a autenticidade de quem a envia, associada à integridade do seu conteúdo. Para fornecer ainda mais a autenticidade faz uso da criptografia assimétrica, que possui um par de chaves – uma privada

e outra pública – onde o receptor tem a garantia de que a assinatura foi criada sem possibilidade de alteração, por meio de uma chave privada (AGUIAR, 2005; BRAZIL, 2007).

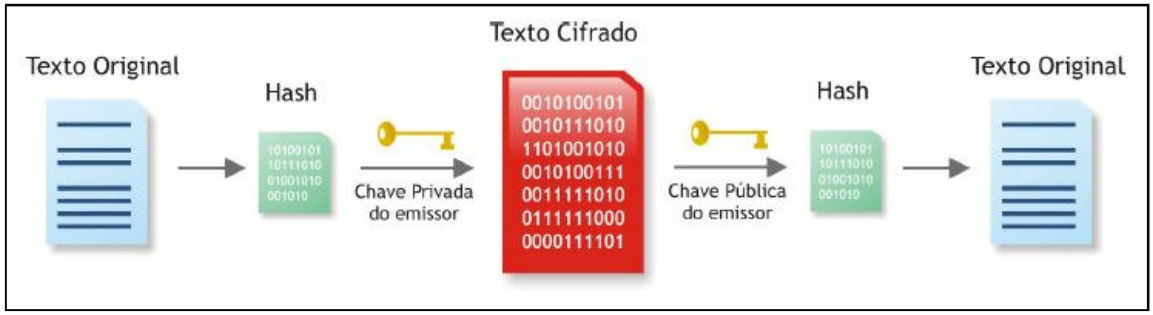


Figura 9. Assinatura Digital
Fonte: FAGUNDES, B. A. (2007, p. 22)

Para geração da assinatura utiliza a função *hash*, que obtém o resumo do documento, em seguida o emissor assina o documento com sua chave privada e envia-o ao receptor, com seu valor criptografado, conforme a Figura 9 (FAGUNDES, 2007). Quando o receptor recebe a mensagem ou documento, decifra o *hash* utilizando a chave pública do emissor, tendo assim a garantia de que a mensagem foi realmente enviada pelo dono da chave privada (BRAZIL, 2007).

3.3.6 Certificado Digital

Certificado digital é um arquivo assinado digitalmente, equivalentes a provas físicas de identificação, como passaporte e cédulas de identidade. Utiliza um par de chaves (privada e pública) que são usadas em conjunto e auxiliam na identificação de usuários em redes de comunicações, comprovando sua identidade (AGUIAR, 2005; BRAZIL, 2007).

De acordo com Brazil (2007), o certificado digital pode estar armazenado em uma estação, um disco, um dispositivo de segurança como um *smart-card* ou um *token*. São elementos essenciais em uma Infraestrutura de Chaves Públicas (ICP). Todo e qualquer

certificado digital é assinado por uma entidade confiável, chamada de Autoridade Certificadora (AC). Uma AC também possui a responsabilidade de manter e divulgar listas com os certificados revogados (Certificate Revocation List – CRL). Os certificados que estão nesta lista podem ter sido roubados, perdidos ou simplesmente estar sem utilidade (AGUIAR, 2005).

Um certificado digital associa a chave pública a uma pessoa ou entidade. Qualquer entidade que conheça a chave pública da AC pode examinar o conteúdo e confirmar a autenticidade de um certificado emitido por esta autoridade, uma vez que a Autoridade Certificadora assina os certificados com sua chave privada (VASQUES; SCHUBER, 2002).

Dentre os seus dados, devem estar contidas as seguintes informações: sobre o objeto que é certificado – caso seja uma pessoa, deve conter dados pessoais como nome, organização, departamento, entre outros –, chave pública do usuário, número de série do certificado, nome da AC que emitiu o certificado, assinatura digital da AC, entre outras informações (AGUIAR, 2005; VASQUES; SCHUBER, 2002).

Segundo Aguiar (2005), existem diversos tipos de certificados. São eles: certificados de AC, que são utilizados para validar outros certificados, sendo auto-assinados ou assinados por outra AC; certificados de servidor, que são utilizados para identificar um servidor seguro, onde tem-se o nome da organização e o nome DNS do servidor; certificados pessoais, que contém nome do portador e informações como endereço eletrônico, endereço postal, entre outros; e certificados de desenvolvedores de software, que são utilizados para validar assinaturas associadas a programas.

Versão
Número Serial
Algoritmo de Assinatura
CA Emitente
Período de Validade
Nome X.500 do Proprietário
Algoritmo de Identificação da chave pública
Chave Pública
Identificação do Emitente
Identificador do Proprietário
Extensão
Assinatura Digital da CA

Figura 10. Certificado padrão X.509
Fonte: BRAZIL, W. G. (2007, p. 28)

Nos dias atuais o uso do certificado digital é bastante difundido, pois dá maior segurança no processo de autenticação, permitindo que ela seja feita baseada no certificado e em uma senha. A recomendação mais aceita e utilizada para a produção de certificados é a X.509, ilustrada na Figura 10, formulada pela International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)[4]. Foi publicado em 1988, passando por revisões até chegar, em 1999, na sua versão final, sendo publicado oficialmente pela IETF (OLIVEIRA, 2010).

[4] Agência intergovernamental responsável por coordenar padronizações relacionadas a telecomunicações.

4 REDES ADSL

Asymmetric Digital Subscriber Line (ADSL) é uma tecnologia de comunicação que consiste em transmitir dados em alta velocidade por uma rede de telefone convencional. Para isto é necessário a utilização de um modem, que converte o sinal padrão do fio de telefone em um canal digital. Os modems são chamados “assimétricos” porque transmitem dados de um local a outro em uma velocidade menor do que recebem. Isto também é considerada uma característica do ADSL (TORRES, 2001).

Esta tecnologia é utilizada principalmente em residências, onde há transmissão de textos, voz e imagens e possui a vantagem de não precisar de cabeamento extra, já que o sinal vem por meio da linha telefônica. Para estas, a forma de atribuição de endereço IP é feita de forma automática e dinâmica, ou seja, é alterado a cada conexão efetuada (MURHAMMER et al, 2000).

4.1 FUNCIONAMENTO DA TECNOLOGIA

Segundo Murhammer et al (2000), o ADSL funciona a partir do modem. Ele se conecta com o modem da operadora telefônica correspondente ao telefone que está instalado no local, sendo responsável pela divisão digital da linha telefônica em três canais separados.

O primeiro é utilizado para transmissão de voz. O segundo para o fluxo de informações do usuário em direção a rede externa (chamado de *upstream*, ou *upload*) e o terceiro canal para o fluxo de dados no sentido da rede para o usuário (conhecido como *downstream,* ou *download*). Desta forma é possível maior velocidade, pois raramente as pessoas fazem o mesmo número de *uploads* e *downloads*. Isto significa que o canal de *downstream* pode ser mais largo sem afetar a velocidade de transmissão de dados. Assim, é

possível uma maior velocidade de transmissão, pois há mais banda disponível (MURHAMMER et al, 2000).

Os modems ADSL, ao criarem canais múltiplos, dividem a largura de banda disponível de uma linha telefônica em uma das suas duas formas: Multiplexação por Divisão de Frequencia (FDM) e Cancelamento de Eco (ESTÁCIO, 2002).

No FDM é determinada uma faixa inferior de dados e outra faixa superior. Na inferior há a divisão através de multiplexação por divisão de tempo em um ou mais canais de alta velocidade ou em um ou mais canais de baixa velocidade. A faixa superior é multiplexada em canais correspondentes de baixa velocidade (ESTÁCIO, 2002).

O Cancelamento de Eco é uma técnica bem conhecida, onde a faixa superior é sobreposta na inferior, separando os dois por meio de cancelamento de eco local. Em ambas, o ADSL divide uma faixa de 4 kHz da linha comum até o final da banda (ESTÁCIO, 2002; TORRES, 2001).

A Figura 11 mostra o FDM e o Cancelamento de Eco.

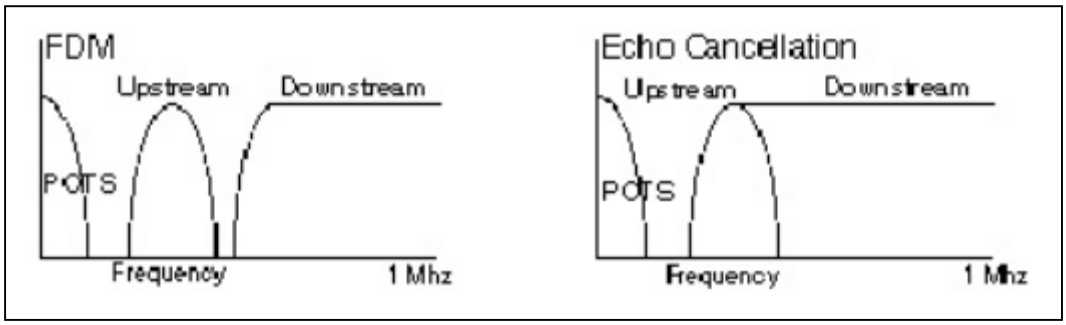


Figura 11. FDM e Cancelamento de Eco
Fonte: ESTÁCIO (2002, p. 6)

O modem de ADSL realiza a organização do fluxo de dados, criado por multiplexação de canais, canais duplex, e manutenção de canais agregados em blocos, prendendo a cada bloco um código de correção de erro. Então, os receptores corrigem erros que acontecem durante a transmissão até os limites indicados pelo código e extensão do

bloco. Isto permite a transmissão efetiva de dados e vídeo com sinais semelhantes (ESTÁCIO, 2002).

4.2 PRINCIPAIS EQUIPAMENTOS UTILIZADOS

O modem ADSL é um dos principais equipamentos utilizados. É ele quem faz o processamento de dados referente à alocação das informações de *dowstream*, *upstream* e voz em seus respectivos canais. Outro muito utilizado é o Digital Subscriber Line Access Multiplexer, ou multiplexador de acesso DSL (DSLAM) (MURHAMMER et al, 2000).

Na estação, cada par telefônico é conectado a um DSLAM. A sua função é concentrar o tráfego de dados das várias linhas com modem DSL existentes e conectá-lo com a rede de dados. Possui suporte a diversos protocolos e a vantagem de estar dedicada apenas a um usuário (TORRES, 2001).

Há também a rede de dados, onde o DSLAM é conectado. Essa poderá ser a rede do provedor de conexão a Internet ou qualquer outro tipo de rede de dados (TORRES, 2001). A Figura 12 mostra a divisão entre a transmissão de dados e voz.

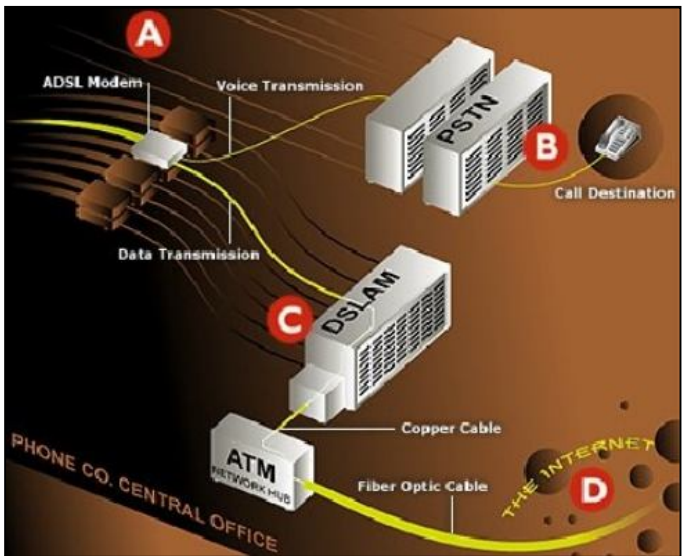


Figura 12. Multiplexador DSLAM
Fonte: ESTÁCIO (2002, p. 4)

A letra “C” na figura corresponde ao multiplexador DSLAM.

Na utilização residencial da tecnologia ADSL, é possível também trafegar dados de forma segura. Com o uso das Redes Privadas Virtuais, um usuário distante pode acessar os dados contidos no computador de sua casa ou escritório com um menor risco de interceptação de informações.

5 REDES PRIVADAS VIRTUAIS

Quando as redes de computadores surgiram não se tinha tanta preocupação com a segurança como atualmente. Comunicações de longa distância são cada vez mais necessárias entre empresas, filiais, parceiros, entre outros. Em um ambiente corporativo, a interconexão de várias redes locais ou acesso a dados fora da empresa é necessária, e para que isso aconteça de forma eficiente a alternativa é utilizar uma rede pública como meio de comunicação: a Internet (AGUIAR, 2005; NORTHCUTT et al, 2002).

As redes públicas são consideradas não confiáveis, pois os dados que nela trafegam estão sujeitos à interceptação e captura, sendo necessário criar algo que garantisse a integridade de informações confidenciais que trafegam pela Internet (THOMAS, 2007).

As Redes Privadas Virtuais (Virtual Private Network – VPN) surgiram com o propósito de fornecer integridade, confidencialidade, autenticidade e controle de acesso às informações trafegadas, reduzindo o risco de ataques externos (ASSIS, 2003; GUIMARÃES; LINS; CORRÊA, 2006). Ela funciona a partir da idéia de se utilizar a rede pública para transmitir dados criptografados de forma segura (NORTHCUTT et al, 2002).

De acordo com Tanenbaum (1997, p. 584), “elas são chamadas “virtuais” porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real.” Algumas implementações VPN utilizam um software cliente instalado nos computadores que se conectam a rede, que é responsável por estabelecer o canal de comunicação entre as duas pontas (ASSIS, 2003).

Outra forma de implementação VPN, segundo Aguiar (2005), é utilizar um *gateway* VPN para criptografar e descriptografar os dados transmitidos, não sendo necessária a intervenção do usuário. Assis (2003) afirma que, muitas vezes, o usuário nem sabe que está utilizando a rede privada. Esta transparência permite que aplicações, usuários e computadores

acessem recursos remotamente como se estivessem em uma rede local, sendo amplamente utilizada para conectar empresas matriz e filial. A Figura 13 ilustra o funcionamento de uma VPN, onde o Túnel é criado utilizando uma rede comum, no caso a Internet.

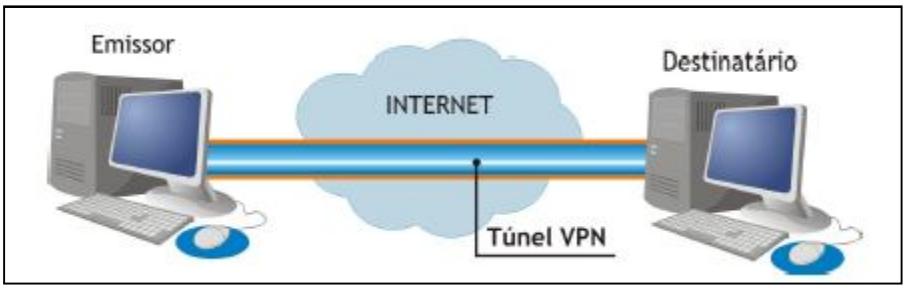


Figura 13. Túnel VPN
Fonte: FAGUNDES, B. A. (2007, p. 37)

As redes privadas virtuais possuem seus próprios protocolos de tunelamento responsáveis por “criar” o canal virtual, que trabalham em conjunto com o TCP/IP. Os mais conhecidos e utilizados são o Point-to-point Tunneling Protocol (PPTP), o Layer Two Tunneling Protocol (L2TP) e o Internet Protocol Security (IPSec). Além disso, existem três topologias comuns utilizadas para VPNs: *Host-Host*, *Host-Gateway* e *Gateway-Gateway* (VASQUES; SCHUBER, 2002).

5.1 TOPOLOGIAS

A topologia *Host-Host* estabelece a comunicação entre dois computadores com acesso à Internet, separados fisicamente, podendo ou não estar na mesma rede (FAGUNDES, 2007). A Figura 14 ilustra um exemplo de dois *hosts* interconectados.

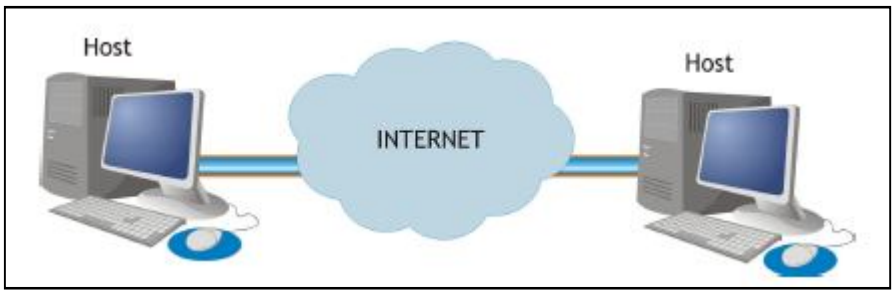


Figura 14. Topologia Host-Host
Fonte: FAGUNDES, B. A. (2007, p. 39)

Esse tipo de topologia tem a finalidade de sincronizar informações entre as máquinas (FAGUNDES, 2007).

A *Host-Gateway* consiste em um *host* conectado a uma rede fisicamente distante. Para isto, segundo Vasques e Schuber (2002), basta o usuário ter um software para conexões remotas VPN instalado no seu computador. Esta opção pode ser utilizada para funcionários que constantemente estão fora da empresa ou viajam e necessitam manter o contato por algum motivo.

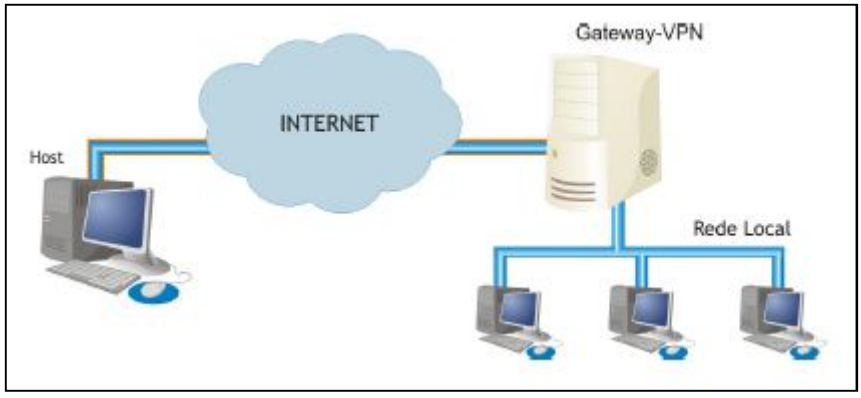


Figura 15. Topologia Host-*Gateway*
Fonte: FAGUNDES, B. A. (2007, p. 39)

A Figura 15 mostra um usuário estabelecendo conexão com o *gateway* VPN da empresa onde trabalha, acessando as informações daquela rede local de modo seguro.

Na topologia *Gateway-Gateway* existem dois *gateways* VPN conectados entre si, dando a possibilidade de duas empresas distantes uma da outra se conectarem e compartilharem os mesmos recursos de rede com um custo muito reduzido (FAGUNDES, 2007).

5.2 POINT-TO-POINT TUNNELING PROTOCOL

O Point-to-Point Tunneling Protocol (PPTP), criado pelo fórum PPTP – um grupo de empresas que incluía 3com, Microsoft, Ascend e ECI Telematics, US Robotics e outras –, tem por objetivo facilitar o acesso de computadores remotos a uma rede privada por meio da Internet ou outra rede baseada em IP, sendo um dos primeiros protocolos VPN que surgiram (FAGUNDES, 2007). É um protocolo de camada dois que utiliza por base de comunicação o Point-to-point Protocol (PPP) para fazer conexões e, em seguida, encapsula e define a rota dos dados utilizando o Generic Routing Encapsulation (GRE) (ASSIS, 2003; NORTHCUTT et al, 2002).

Para realizar a autenticação dos dados, os protocolos utilizados são: Password Authentication Protocol (PAP), onde os dados são transmitidos sem nenhuma forma de criptografia; Challenge Handshake Authentication Protocol (CHAP), que é um protocolo de autenticação por desafio de resposta (é considerado a melhoria do PAP) – onde nele a senha é usada para criar uma *string hash* de desafio, o servidor que sabe a senha duplica a operação e compara os resultados; e o Microsoft Challenge/Reply Handshake Protocol (MSCHAP), onde o servidor de acesso remoto exige só a *string* de *hash* da senha para validar a resposta do desafio (FAGUNDES, 2007; NORTHCUTT et al 2002). A maior parte dos problemas relacionados à segurança do PPTP foi devido à insegurança do protocolo de autenticação MSCHAP (NORTHCUTT et al 2002).

De acordo com Vasques e Schuber (2002), uma vantagens de se implementar VPN utilizando o protocolo PPTP é o suporte a outros protocolos diferentes do IP, como o NetBEUI e o IPX. Porém uma de suas principais desvantagens é relativa à sua segurança, pois esse fornece suas chaves de encriptação utilizando a senha do usuário como base. Portanto, se a senha for fraca, como palavras encontradas em dicionários ou números de telefones, a chave também será.

Para estabelecer a conexão de controle, o PPTP utiliza a porta 1723. Essa conexão fica entre o IP dinâmico do cliente da VPN e o endereço IP fixo do servidor. Após o estabelecimento da conexão, inicia a troca de mensagens entre o controle de conexão e o gerenciamento de mensagens PPTP. Os pacotes de controle de desta conexão são compostos por um cabeçalho IP, um cabeçalho TCP e o controle de mensagens PPTP (ASSIS, 2003; NORTHCUTT et al, 2002).

Segundo Assis (2003), o protocolo utiliza três níveis de encapsulamento para fazer o tunelamento dos dados. No tipo *Frame* PPP o pacote é encapsulado e criptografado com um cabeçalho PPP, originando um *frame*. Esse frame recebe um cabeçalho GRE, que é utilizado para repassar informações de roteamento, para trafegar em redes IP.

No pacote GRE, o mesmo é encapsulado por um cabeçalho IP, onde estão os endereços IP de origem e destino do pacote. Para que o pacote possa ir para uma LAN ou WAN, as informações de cabeçalho da camada *Data-Link* são necessárias, pois são utilizadas para o envio desse pacote para a interface física (ASSIS, 2003; FAGUNDES, 2007).

5.3 LAYER TWO TUNNELING PROTOCOL

O Layer Two Tunneling Protocol (L2TP) é definido pela RFC 2661 e consiste em uma solução de tunelamento da camada dois. É uma mistura de dois protocolos de tunelamento anteriores (o Layer Two Forwarding – L2F) da Cisco e o PPTP, combinando os melhores atributos dos dois. É homologado pela Internet Engineering Task Force (IETF), comunidade internacional que trata da evolução da arquitetura da Internet e seu correto funcionamento (NORTHCUTT et al, 2002).

Diferentemente do PPTP, no L2TP a autenticação é feita em duas etapas, sendo que o usuário é autenticado antes do tunelamento ser estabelecido e no momento em que a conexão é estabelecida entre os *gateways*. No L2TP, para que os dados sejam criptografados antes da conexão ser estabelecida, ele utiliza o Data Encryption Standard (ASSIS, 2003). Fagundes (2007) afirma que também é realizado o encapsulamento de pacotes PPP, podendo então fazer uso dos mecanismos de autenticação do mesmo. Também provê suporte para autenticação do túnel, permitindo que seus extremos sejam autenticados.

Conforme Vasques e Schuber (2002), por ser um protocolo padrão, qualquer fabricante pode criar produtos que utilizem o L2TP, de forma que provedores de acesso e consumidores em geral não dependam de produtos fornecidos por uma única empresa.

Este protocolo foi desenvolvido para suportar dois modos de tunelamento: o tunelamento voluntário e o compulsório. O voluntário é mais flexível para usuários em trânsito, pois é iniciado pelo computador remoto, dando a possibilidade de discar para qualquer provedor de acesso, porque o provedor não participa da criação dos túneis, percorrendo vários servidores sem precisar de uma configuração explícita (FAGUNDES, 2007).

De acordo com Fagundes (2007), o tunelamento compulsório é criado automaticamente e iniciado pelo servidor de acesso à rede através de uma conexão discada. Para isto, é necessário que o servidor de acesso à rede seja pré-configurado para saber a terminação de cada túnel baseado nas informações de autenticação de usuário.

O protocolo L2TP possui alguns níveis de tunelamento/encapsulamento, sendo eles: L2TP, onde o pacote é encapsulado, recebendo um cabeçalho PPP, em seguida um cabeçalho L2TP; Encapsulamento UDP, onde o pacote é encapsulado pelo protocolo UDP e enviado à porta 1701; IPSec, que é a fase em que o pacote ganha segurança e também onde os dados são criptografados e autenticados; IP, onde ganha uma etiqueta com informações referentes ao destino e origem; e o de camada de transporte, que é onde ele recebe um cabeçalho que representa os padrões utilizados pela rede na camada de transporte (ASSIS, 2003).

Vasques e Schuber (2002) afirmam que a maior deficiência do L2TP é o encapsulamento dos datagramas. Ele não possui nenhum mecanismo de proteção do tunelamento definido – ao contrário do PPTP, que utiliza o protocolo GRE. Para isso ele depende de outro protocolo mais complexo, o IPSec, tornando a comunicação entre as redes interligadas mais segura, porém, bem mais lenta.

5.4 INTERNET PROTOCOL SECURITY

Como resposta as carências de segurança existentes no protocolo IP, a IETF desenvolveu um conjunto de padrões voltados à segurança sobre o IP, denominado IP Security Protocol (IPSec), com o intuito de ser o protocolo padrão de endereçamento tanto para o IPv4 quanto para a próxima versão do IP, o IPv6 (FAGUNDES, 2007; SILVA, 2003). Localizado na terceira camada do modelo de referência OSI (camada de rede), este conjunto

de padrões ou protocolos fornece principalmente serviços de criptografia (autenticidade, privacidade e integridade), garantindo segurança na camada de rede (GODINHO; BOGO, 2004).

De acordo com Veríssimo (2002), uma das principais vantagens é o fato de que ele é transparente para a camada de aplicação e para o usuário, fazendo com que, desta forma, não haja necessidade de alterar o código de aplicações e nem de treinamento extra para funcionários de uma organização, por exemplo.

5.4.1 Modos de Funcionamento

Segundo Thomas (2007), o IPSec possui dois modos de envio de dados criptografados entre os pontos de comunicação: modo de Transporte e modo Túnel, onde cada modo difere em sua aplicação e na quantidade de carga adicionada ao pacote passageiro.

O modo nativo é o de Transporte. A transmissão do pacote protegido por ele é feita entre os *hosts*, onde o responsável pelo encapsulamento é o próprio *host*. Nos pacotes criados neste modo são adicionados cabeçalhos de autenticação e conteúdo de segurança encapsulador (AH[5] e ESP[6]) logo após o cabeçalho IP original, de modo que apenas os protocolos superiores podem ser cifrados/autenticados (FAGUNDES, 2007; GODINHO et al, 2005).

[5] Authentication Header, possui a função de garantir que o pacote não foi alterado durante a transmissão.
[6] Encapsulating Security Payload, utilizado para prover a checagem de integridade, autenticação e criptografia dos datagramas IP.

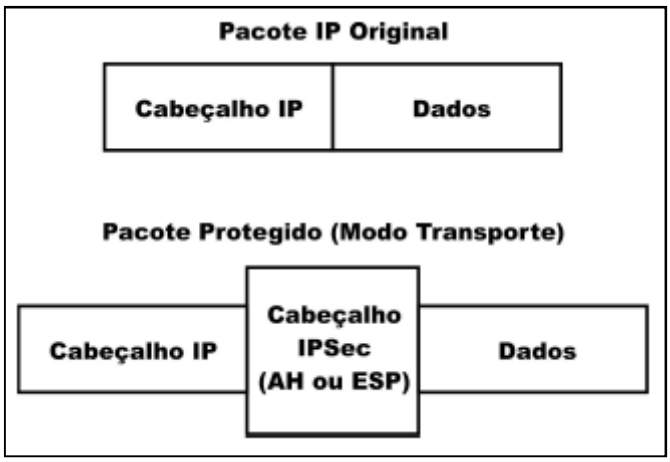


Figura 16. Modo de Transporte
Fonte: Adaptada de KOLENISKOV, O.; HATCH, B. (2002, p.138)

A Figura 16 ilustra os cabeçalhos IPSec adicionados entre o cabeçalho IP original e os dados.

O modo Túnel, segundo Fagundes (2007), é mais utilizado por *gateways* que manipulam o tráfego de *hosts* que não têm suporte ao IPSec, onde o pacote original – que é tratado como um dado só – é encapsulado em um novo pacote com a criptografia do IPSec (incluindo o cabeçalho original), e então é enviado para o outro *gateway* que desencapsula e o encaminha ao destinatário. A Figura 17 demonstra um pacote protegido por este modo.

Figura 17. Modo Túnel
Fonte: Adaptada de KOLENISKOV, O.; HATCH, B. (2002, p.138)

Para Godinho et al (2005), este encapsulamento permite que o endereço IP de origem e destino originais fiquem “escondidos”, impedindo a alteração ou conhecimento do atacante das partes envolvidas, sendo mais seguro que o modo de transporte (ASSIS, 2003).

5.4.2 Security Association

Uma Associação de Segurança (AS, ou Security Association – SA) estabelece um acordo de confiança entre entidades, definindo regras e parâmetros sobre como elas transmitirão informações com segurança utilizando IPSec. Uma AS contém informações como algoritmos de criptografia, funções *hash*, modo de funcionamento (túnel ou transporte), chaves secretas, porta de comunicação, entre outros (NORTHCUTT et al, 2002; THOMAS, 2007).

Segundo Fagundes (2007), a identificação de uma AS é feita por três parâmetros: endereço IP, protocolo de segurança (AH ou ESP) e o Security Parameter Index (SPI) que é definido na fase de negociação, fase que ocorre antes da criação da AS.

Todos os dados de uma Associação de Segurança são armazenados dentro de um banco de dados chamado Security Association Database (SAD), onde o acesso ao seu conteúdo é restrito a pessoas autorizadas. O número que identifica uma AS, juntamente com o endereço IP de destino e os protocolos de segurança, é chamado de Security Parameters Index (SPI). O SPI é composto por índices de 32 *bits* embutido aos cabeçalhos dos pacotes e é definido durante a negociação que antecede o estabelecimento da Associação. Além disso, todos os membros de uma AS também devem conhecer o SPI (THOMAS, 2007; VASQUES; SCHUBER, 2002).

Para o funcionamento do IPSec são definidas algumas estruturas de dados armazenadas em cada nó da rede que execute-o. Um deles é o Security Policy Database

(SPD), composto por um conjunto de regras que definem como processar os pacotes que chegam a uma interface, como por exemplo, determinar se ele seguirá em frente, seguirá após aplicar o protocolo IPSec, ou será descartado (VERÍSSMO, 2002).

Assis (2003) afirma que, enquanto o SAD apenas referencia as políticas a serem usadas por meio de parâmetros, o SPD força a utilização de uma política de segurança sobre os pacotes. Segundo ele, o tratamento de pacotes recebidos e enviados é diferente. No tráfego que entra, a identidade do emissor e a integridade do pacote serão verificados pelo SAD, que depois envia a regra SPD correspondente. No tráfego de saída, as regras são verificadas pelo SPD e é determinada a ação que será aplicada ao pacote. Dependendo da política de segurança, se for necessário, o IPSec consultará o SAD.

5.4.3 Internet Key Exchange

O gerenciamento das Associações de Segurança no IPSec pode ser feito de maneira automática ou de maneira manual, sendo que para redes de grande porte torna-se inviável gerenciar todas manualmente. Para realizar o gerenciamento destas de forma automática e também a atualização das chaves criptográficas, existem vários protocolos considerados satisfatórios, porém o Internet Key Change (IKE) é o principal e mais utilizado (FAGUNDES, 2007; MURHAMMER et al, 2000). No IKE, além das ASs serem negociadas automaticamente, se for habilitado o Perfect Forward Secrecy (PFS) é garantido que, se uma das chaves secretas estiver comprometida, apenas os dados encriptados por ela estarão (VASQUES; SCHUBER, 2002).

Ele é a combinação entre o Internet Security Association and Key Management Protocol (ISAKMP) – que trata das negociações se segurança, definindo o método de distribuição de chaves – com o Oakley – que é responsável pela troca das chaves. Sendo

assim, o IKE é responsável por fornecer a negociação, autenticação, gerenciamento e troca de chaves (NORTHCUTT et al, 2002).

Este protocolo funciona em duas etapas. A primeira estabelece um canal de comunicação seguro entre as duas extremidades que desejam trocar dados. Para isto ser possível, é preciso verificar os protocolos criptográficos e os parâmetros que serão utilizados para escolher os algoritmos de autenticação e de encriptação. Baseado nestas informações é realizada a troca de dados – parâmetros das chaves e um valor randômico que previne contra alguns tipos de ataques – e em seguida feita uma associação segura ISAKMP, para então criar o canal (FAGUNDES, 2007; NORTHCUTT et al, 2002).

A segunda etapa consiste em utilizar o canal criado para transmitir dados, garantindo que os mesmos já estejam protegidos. Para realizar a transmissão e a proteção das trocas de informações desta fase, uma nova associação segura ISAKMP é estabelecida e, posteriormente, são negociados protocolos ou combinação de protocolos que serão armazenados nas SADs de cada extremidade (FAGUNDES, 2007; VASQUES; SCHUBER, 2002).

De acordo com Fagundes (2007), existe uma alternativa para aumentar ainda mais a segurança nesta etapa, o PFS. Ele faz com que a chave seja derivada do algoritmo de Diffie-Hellman (método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman), aumentando a segurança, mas reduzindo o desempenho.

5.4.4 Authentication Header

Utilizado para prover integridade e autenticação para datagramas IP, o Authentication Header (AH, ou cabeçalho de autenticação) possui a função de garantir que o pacote não foi alterado durante a transmissão (MURHAMMER et al, 2000). Porém, segundo

Northcutt et al (2002), sua eficácia é limitada como único método de segurança para a maioria das implementações de VPN, pois não oferece confidencialidade para o pacote. Faz uso de algoritmos simétricos para tornar difícil a modificação e a geração de funções *hash* para a interceptação de pacotes protegidos pelo AH. Porém, mesmo assim, os dados trafegam na rede sem uma proteção e podem ser capturados (ASSIS, 2003).

Apesar de seu uso ser opcional, Murhammer et al (2000) afirma que o serviço de proteção de resposta deve ser implementado por qualquer sistema compatível com IPSec.

Como forma de proteger o pacote é inserido um cabeçalho dentro do mesmo, negociado uma associação segura que utiliza um número sequencial (zerado a cada estabelecimento de uma associação segura) e adicionado funções *hash* MD-5 ou SHA-1/SHA-2 ao AH, para que, baseado no conteúdo do pacote, um novo código de autenticação seja criado. Após isto é feita apenas a divisão do pacote protegido, se necessário (FAGUNDES, 2007). A Figura 18 mostra o cabeçalho AH montado.

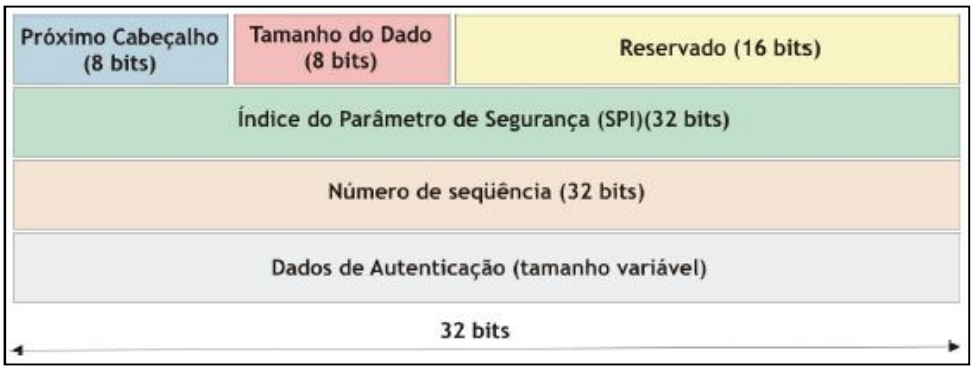


Figura 18. Cabeçalho AH
Fonte: FAGUNDES, B. A. (2007, p. 51)

O protocolo AH não suporta o Network Address Translation (NAT), pois este "mascara" o endereço IP original, perdendo com isso o verdadeiro emissor. O NAT, bastante utilizado em redes IPv4 – principalmente em redes internas –, possui a finalidade de reduzir a

utilização de endereço IP válidos, sendo uma alternativa para o problema da escassez de endereços IPv4 (GODINHO; BOGO, 2004; SILVA, 2003).

O AH pode ser utilizado sozinho ou em conjunto com o Encapsulating Security Payload (ESP) (THOMAS, 2007).

5.4.5 Encapsulating Security Payload

Além de fornecer as características do AH, este protocolo também oferece a confidencialidade, sendo utilizado para prover a checagem de integridade, autenticação e criptografia dos datagramas IP. Ele adiciona seu próprio cabeçalho (o cabeçalho ESP) logo após o cabeçalho AH, caso este esteja sendo utilizado, e criptografa toda a parte correspondente aos dados com um algoritmo que foi negociado durante o estabelecimento da Associação de Segurança, por exemplo, o 3DES (FAGUNDES, 2007; MURHAMMER et al, 2000).

O ESP assegura que, mesmo que se monitore ou intercepte um pacote IP, os dados contidos nele não poderão ser lidos. Diferentemente do AH – que apesar de adicionar um cabeçalho aos pacotes IP, não encapsula todo o conteúdo do datagrama – o ESP empacota os dados dentro de sua estrutura (GODINHO; BOGO, 2004).

Figura 19. Pacote ESP
Fonte: FAGUNDES, B. A. (2007, p. 52)

Para a utilização deste protocolo é necessário primeiramente inserir os campos relativos ao seu cabeçalho no pacote, encriptar os dados inseridos no pacote com o algoritmo e os parâmetros especificados na AS correspondente, e incrementar um valor a uma sequencia de números da mesma forma que o AH. Caso ele não esteja sendo usado, deve-se calcular um valor para autenticação e, por fim dividir o pacote caso haja necessidade (VASQUES; SCHUBER, 2002). A Figura 19 ilustra um pacote ESP montado.

5.4.6 Arquitetura do IPSec

A arquitetura do protocolo IPSec funciona tanto para pacotes IPs enviados (tráfego que sai) ou para pacotes IPs recebidos (tráfego que entra). No tráfego que sai, o pacote IP que se deseja enviar é analisado pelo IPSec a fim de verificar se o mesmo irá prosseguir para seu destino, aplicando ou não a proteção do protocolo. Para que isto seja determinado, o SPD verifica a origem, o destino e o tipo do pacote, e então, dependendo destas características, determina a melhor opção (KOLENISKOV; HATCH, 2002, tradução nossa).

A Tabela 2 mostra um exemplo onde os pacotes IPs originados de qualquer porta da rede 192.168.1.1, com destino a porta 80 da rede 192.168.2.1, precisarão passar pela regra número 1. Esta informa que é necessário o IPSec utilizar o modo túnel, um cabeçalho de autenticação (AH) e o parâmetro 400 da Associação de Segurança.

Tabela 2. Exemplo de um SPD

Regra #	IP Origem	IP Destino	Porta Origem	Porta Destino	Ação	Proto-colo IPSec*	Modo*	Índice da AS que Sai
1	192.168.1.1	192.168.2.1	Qualquer	80	IPSec	AH	Túnel	400
2	192.168.1.23	192.168.2.5	Qualquer	22	Aceitar	-----	----	8500
3	192.168.1.99	192.168.2.1	Qualquer	Qualquer	IPSec	ESP	Transporte	6025

Fonte: Adaptada de KOLENISKOV, O.; HATCH, B. (2002, p. 134)

Os campos marcados com asterisco podem ser omitidos, pois estão presentes na AS a qual este SPD se refere.

De acordo com Vasques e Schuber (2002), o tráfego que entra, ao contrário do que sai, primeiramente analisa o pacote no SAD, utilizando o SPI, o AH e o ESP. Isto se dá, pois é necessário verificar o índice que será referenciado no banco de dados da AS e também a identidade do emissor do pacote, e extrair o dado do pacote encapsulado – este poderá conter um cabeçalho TCP encriptado, com, por exemplo, um número de porta de comunicação, que será necessário quando se for fazer a referência ao SPD. Após esta primeira parte, é referenciada a regra apropriada ao SPD que então irá checar, a partir das informações do pacote, o que fazer com o mesmo (VASQUES; SCHUBER, 2002).

Tabela 3. Exemplo de um SAD

SPI	IP Origem	IP Destino	Porta Origem	Porta Destino	Tipo	Ponteiro para Entrada SPD
1	192.168.2.1	192.168.1.1	Qualquer	Qualquer	Que entra	4
3	192.168.1.1	192.168.2.1	Qualquer	80	Que sai	7

Fonte: Adaptada de KOLENISKOV, O.; HATCH, B. (2002, p. 142)

A Tabela 3 mostra o funcionamento de um SAD. Este posteriormente referenciará a um SPD para tratar um pacote recebido.

5.4.7 Vantagens e Desvantagens

O IPSec foi desenvolvido para fornecer segurança à redes VPN, porém pode se tornar inseguro na utilização em sistemas já comprometidos em relação a segurança dos dados. Isto significa que se deve primeiramente garantir a segurança nas máquinas que implementam os *gateways* IPSec (VASQUES; SCHUBER, 2002). Este comprometimento com a segurança se dá porque sua implementação é complexa e requer alto grau de esforço computacional, por utilizar algoritmos de criptografia muito pesados. Além disso, a fragmentação dos pacotes no IPSec tende a aumentar, pois haverá adição de cabeçalhos maiores do que no IP (KOLENISKOV; HATCH, 2002, tradução nossa).

Outra desvantagem, segundo Vasques e Schuber (2002), é não proteger contra ataques do tipo DoS. Porém a utilização em conjunto com um *firewall* fornecerá a proteção contra este tipo de ataque. Além disto, pode-se citar que o IPSec autentica endereços IP, mas não usuários. Ou seja, pode garantir apenas que a comunicação entre as máquinas transcorra de forma segura e quais delas conectam ao servidor (NORTHCUTT et al, 2002).

Entretanto esta tecnologia apresenta bons resultados, fazendo dela uma grande arma contra vários tipos de ataques e invasões. Se for utilizada de forma correta, combinando bem os recursos de protocolos como o AH e o ESP, ou sabendo quando tirar os melhores proveitos do modo Transporte e do modo Túnel, ou ainda, compartilhando seguramente as chaves secretas por meio do protocolo IKE, dificilmente um invasor descobrirá algum ponto falho na conexão (MURHAMMER et al, 2000; VASQUES; SCHUBER, 2002).

Além disso, segundo Northcutt et al (2002), ele possui mais algumas vantagens: é de fácil manutenção, pois além de ter a possibilidade de ser implementado apenas nos roteadores, *firewalls* e *gateway*, a sua aplicação em determinados pontos da rede pode facilitar o esforço e a manutenção de uma política de segurança consistente dentro da empresa; é transparente a sub-rede, sendo necessária a implementação de seus serviços apenas nos locais de origem e destino, ou seja, não é necessário implementar na sub-rede; e não há necessidade de configurar as estações ou aplicações para trabalhar com ele.

5.5 COMPARAÇÃO ENTRE PROTOCOLOS DE TUNELAMENTO

A Tabela 4 faz a comparação entre os protocolos de tunelamento PPTP (utilizado por alguns softwares mais antigos que implementam VPNs), L2TP, L2TP/IPSec e IPSec.

Tabela 4. Comparação entre protocolos de tunelamento

Propriedades	Descrição	PPTP	L2TP	L2TP/IPSec	IPSec
Autenticação de usuário	Autentica os usuários que queiram estabelecer uma conexão	SIM	SIM	SIM	SIM
Autenticação de Computadores	Autentica computadores envolvidos na conexão	SIM	SIM	SIM	SIM
Suporte a NAT	Passa por meio de um NAT para esconder os pontos finais da conexão	SIM	SIM	NÃO	NÃO
Suporte a Multi-protocolo	Define um método padrão para o tráfego IP e não IP	SIM	SIM	SIM	SIM
Atribuição Dinâmica de Endereço IP	Define uma negociação de endereçamento IP entre o servidor VPN e seus clientes. Isso elimina configurações manuais do protocolo IP	SIM	SIM	SIM	Implementação em andamento pelo grupo de trabalho IPSec da IETF
Encriptação	Pode criptografar o tráfego corrente	SIM	SIM	SIM	SIM
Uso de PKI	Usa infraestrutura de chave pública para implementar a criptografia e a autenticação	SIM	SIM	SIM	SIM
Autenticação de Pacotes	Provê um método de autenticação que garante que os pacotes não foram alterados durante a transmissão	NÃO	NÃO	SIM	SIM
Suporte a Multicast	Pode efetuar tráfego em multicast	SIM	SIM	SIM	NÃO

Fonte: Adaptada de ASSIS, J. M. (2003, p. 36)

A Atribuição Dinâmica de Endereços IP, que faz a definição de uma negociação de endereçamento IP entre o servidor VPN e os clientes, eliminando configurações manuais do protocolo IP, ainda estava em desenvolvimento pelo grupo de trabalho IPSec da IETF no ano de 2003. Pesquisas foram realizadas em diversas fontes, porém informações mais atualizadas sobre o assunto não foram encontradas. Os trabalhos correlatos devem fazer alguma referência a este assunto, podendo ser consultados para informações complementares.

6 TRABALHOS CORRELATOS

Neste capítulo são apresentados alguns trabalhos que serviram de base para esta pesquisa, com o objetivo de transmitir melhor entendimento das propostas apresentadas.

6.1 UMA IMPLEMENTAÇÃO DE VPN

Monografia de Graduação apresentada ao Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis, desenvolvida por Bruno Alves em 2007.

Apresenta alguns conceitos de segurança que servem como base para o entendimento do funcionamento de uma Rede Privada Virtual e realização do objetivo do trabalho, que é apresentar as principais características da mesma, assim como os principais protocolos disponíveis e descrever uma implementação em Linux utilizando o Secure Socket Layer (SSL).

São abordadas as principais formas de criptografia no meio computacional, assim como também serão levados em consideração outras formas de segurança como *firewall*, por exemplo. Apresentam-se conceitos de segurança e algumas formas de ataque, descrevendo o que é um *firewall* e as principais arquiteturas existentes, e também os conceitos de VPN e os protocolos mais utilizados, tendo por finalidade apresentar os principais protocolos utilizados para criar e gerenciar os túneis, apresentando seus pontos positivos e negativos.

Por fim, tem-se a implementação desta rede em Linux utilizando o software OpenVPN, que cria túneis SSL, fazendo uma avaliação sobre este software aplicado em Redes Privadas Virtuais.

6.2 IMPLEMENTANDO VPN EM LINUX

Este trabalho, Monografia de Pós-Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, realizado por João Mário de Assis em 2003, tem como objetivo apresentar a implementação de VPN em Linux utilizando o IPSec, visando analisar a funcionalidade e a segurança desta tecnologia na interligação de computadores usando um meio não seguro de transmissão.

Inicialmente é descrito sobre redes de computadores, suas classes, tamanhos, topologia e protocolos de comunicação, servindo como fundamentação para a abordagem da criptografia (mais utilizadas e funcionamento desta tecnologia). Além disso, é descrito sobre os protocolos e processos de tunelamento, e conceitos de VPN.

A implementação de uma Rede Privada Virtual é realizada por meio do software livre FreeS/Wan, onde é realizada uma avaliação sobre a segurança e são expostos os objetivos alcançados. Este estudo é importante, pois faz a análise da funcionalidade e da segurança desta tecnologia para a interligação de computadores utilizando um sistema operacional específico, o Linux, que é considerado relativamente seguro.

6.3 IMPLEMENTAÇÃO DE UMA VPN EM LINUX UTILIZANDO O PROTOCOLO IPSEC

Trabalho de Conclusão de Curso apresentado à Coordenação do curso de Bacharelado em Ciência da Computação do Centro Universitário do Estado do Pará – CESUPA, por Alan Tamer Vasques e Rafael Priante Schuber no ano de 2002.

Mostra os principais itens das Redes Privadas Virtuais, implementado-a no sistema operacional Linux utilizando o protocolo IPSec, visando analisar a funcionalidade e a segurança desta tecnologia na interligação de redes de computadores.

Para isto, são abordados conceitos e meios de utilização de uma VPN, realizando a introdução sobre os conceitos fundamentais como tipos de redes, classificações e protocolos, destacando o TCP/IP. Além disso, contém informações relevantes a respeito da segurança em VPNs, onde são destacados os principais tipos de ataques e defesas, as ameaças existentes, os métodos de criptografia, assinaturas e certificados digitais, entre outras.

São retomados também as principais características de uma Rede Privada Virtual, como vantagens e desvantagens de sua implementação, além dos principais protocolos, onde é dado ênfase ao IPSec. Após, é mostrada a implementação de uma VPN em caráter experimental, explicando cada uma de suas fases e detalhando aspectos da configuração desta tecnologia, a fim de posicioná-la como uma alternativa segura e economicamente atrativa, principalmente para organizações.

6.4 ANÁLISE DA UTILIZAÇÃO DO IPSEC COMO GARANTIA DE SEGURANÇA NA COMUNICAÇÃO EM REDES TCP/IP

Artigo publicado no VI Encontro de Estudantes de Informática do Estado do Tocantins, curso de Sistemas de Informação do Centro Universitário Luterano de Palmas (CEULP/ULBRA), por Luis Godinho Junior e Madianita Bogo, no ano de 2004.

O objetivo é apresentar os resultados de estudos e de testes práticos, sobre a plataforma Windows 2000, para verificar a vulnerabilidade de redes não protegidas e a segurança oferecida pelo IPSec com o IPv4, que é o protocolo usado atualmente na grande maioria das redes.

Inicialmente é tratado sobre a importância da troca de informações entre dispositivos e sua segurança, além de considerações acerca da segurança em redes de computadores, falando sobre ataques mais comuns e os meios de resolver estes problemas. Também são abordados os sistemas de criptografia e o protocolo IPSec – que integra mecanismos que fornecem ao pacote IP serviços providos pelos sistemas de criptografia – falando sobre os tipos de cabeçalhos e protocolos do IPSec.

Com a finalidade de testar este protocolo como garantia de segurança para redes, é realizada uma implementação do mesmo no sistema operacional Windows, bem como realização de testes para demonstrar a vulnerabilidade das redes TCP/IP não protegidas, verificando a eficiência do IPSec. Além disso, é abordado a importância de procurar alguma forma de fornecer segurança na comunicação em rede, colocando este protocolo de segurança como boa alternativa para integridade, confidencialidade e autenticidade na troca de informações.

Com a aplicação do teste prático de comunicação entre máquinas sem configuração de diretivas de segurança e entre máquinas com diferentes configurações dessas diretivas, foram obtidos e apresentados resultados que comprovam a eficiência do IPSec (GODINHO; BOGO, 2004).

6.5 SEGURANÇA EM REDES WI-FI

Este trabalho é um Projeto Final de Graduação apresentado ao Centro de Ciências Exatas e Tecnológicas – Departamento de Ciência da Computação da Universidade Estadual de Montes Claros – UNIMONTES, por Paulo Américo Freire Aguiar, no ano de 2005.

Aborda a segurança em redes sem fio, descrevendo as redes wireless e wi-fi, sua estrutura e modo de funcionamento, além da comparação entre padrões wi-fi.

É abordado também sobre segurança nestes tipos de rede, falando sobre os métodos de segurança que podem ser utilizados neste padrão, além de descrever as redes VPN, seu conceito, funcionamento e importância, bem como suas desvantagens.

Como conclusão do trabalho proposto, é destacada a importância da segurança da informação e os métodos de segurança utilizados.

6.6 CONCENTRADOR DE VPN COM OPENSWAN PARA CONEXÕES EM TOPOLOGIA “ROAD WARRIOR”

Monografia de Pós-Graduação “Lato Sensu” apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras para obtenção do título de Especialista em “Administração em Redes Linux”, por Emerson Luis Galeli de Oliveira, no ano de 2010.

Apresenta a utilização do IPSec por meio da ferramenta Openswan para a criação de conexões seguras utilizando certificados X.509 em equipamentos com Linux, onde os clientes não precisarão de endereços IPs permanentes ou DNS dinâmico para identificação.

O trabalho foi motivado pelo desafio de atender usuários que possuem conexões do tipo “Road Warrior” – ou seja, com IPs dinâmicos – e criar uma VPN com a empresa em que trabalham, passando a ter outros computadores compartilhando da mesma conexão de Internet para atividades extras, onde muitos optaram em colocar um roteador com NAT em seus escritórios. Mas com a exigência do IP dedicado e válido, a solução tradicional de VPN com IPSec passou a ser um entrave na vida dos usuários, porém com o uso de certificados X.509 junto ao IPSec tornou possível as conexões sem endereços IPs fixos ou IPs reservados ao estabelecerem túneis com segurança.

Foram descritos alguns dos principais métodos de criptografia existentes no mercado para construção de Túneis VPN, e também algoritmos de criptografia que são usados em chaves de autenticação de túneis ou de cifragem dos pacotes de dados transferidos por meio dos túneis.

Outros protocolos além do IPSec foram apresentados para mostrar algumas das características de outras soluções existentes no mercado, com o intuito de enfatizar as vantagens do IPSec.

O maior ganho obtido neste trabalho foi a unificação de uma solução por meio do protocolo IPSec e do aplicativo Openswan, que permite a conexão de Redes Virtuais Privadas com *gateways* CISCO, Linux, Unix ou estações de trabalho Linux ou Windows, com segurança e sem restrições para as formas de acesso dos usuários.

7 UTILIZAÇÃO DO PROTOCOLO IPSEC PARA POSSIBILITAR MAIOR SEGURANÇA EM REDES PRIVADAS VIRTUAIS

Com a finalidade de aplicar e testar o protocolo IPSec como alternativa de segurança para Redes Privadas Virtuais foi realizado um projeto de rede voltado para clientes ADSL. Para isso, é simulada uma rede entre dois computadores conectados por meio de modems, verificando se este protocolo provê o mínimo de segurança necessária para o tráfego de dados em uma rede de Internet.

Portanto, a ênfase se dá na aplicação e teste do protocolo de segurança IPSec, por meio de uma solução que atenda aqueles usuários que se conectam por meio de redes com IP dinâmico ou sem um ponto permanente de acesso à Internet, e necessitam realizar acessos à rede de sua casa ou escritório. Com isso, é possível acessar qualquer dado armazenado no computador remoto e até manter um banco de dados com várias informações, podendo consultá-las de forma mais segura e com menor possibilidade de interceptação dos dados.

Primeiramente é necessária a escolha do sistema operacional a ser utilizado, bem como a ferramenta para implementar o protocolo IPSec. Optou-se pelo sistema operacional Linux, versão Ubuntu 11.04, por possuir grande flexibilidade e recursos que provêem maior segurança da rede. Além disso é gratuito, não sendo necessário adquirir licenças para obtê-lo.

Para a configuração da VPN foi escolhida a ferramenta Openswan, que implementa o protocolo IPSec para proteger o tráfego da rede baseado no IP. É uma continuação do extinto projeto FreeS/WAN, ou seja, é uma implementação *open source* – de código aberto – do IPSec. Sua versão 1.x é baseada na última do Super FreeS/WAN (1.99.8.2), com poucos recursos adicionais, e apenas correções aplicadas. Trabalha com o *kernel* 2.0, 2.2 e 2.4 do Linux.

A partir de 01 de janeiro de 2006 a versão 1.x foi descontinuada, sendo necessário atualizar-se para a versão mais recente, a 2.x. Ela oferece suporte ao *kernel* 2.0, 2.2, 2.4 e 2.6 do Linux, e também a diversas outras plataformas, incluindo x86_64, x86, ia64, MIPS e ARM. Atualmente está na distribuição 2.6.36, de 05 de setembro de 2011, sendo que a 2.x é a única que suporta o *kernel* 2.6 do Linux.

A sua utilização neste trabalho deve-se à necessidade de um software que implemente o serviço IPSec. Com isso, para ser possível a conexão da Rede Privada Virtual teve-se que descartar o mais comum, OpenVPN, que não implementa este recurso. Nele o tunelamento é feito por meio do protocolo SSL.

A instalação e configuração da ferramenta Openswan é descrita nas próximas etapas.

7.1 METODOLOGIA

A primeira etapa deste trabalho compreendeu o levantamento bibliográfico, onde pesquisou-se as obras necessárias para a elaboração do trabalho de conclusão de curso. Ao longo do tempo, algumas referências complementares foram adicionadas, finalizando esta etapa.

Foi realizado o estudo sobre alguns métodos de segurança utilizados em redes de computadores, demonstrando as ameaças e ataques mais comuns e como esses métodos de defesa reagem, visando garantir integridade, confidencialidade e autenticidade dos dados que trafegam na rede. Abordou-se também a importância da informação para as organizações e a necessidade de sigilo das mesmas ao trafegar em redes não seguras.

Baseado na importância da segurança nas redes de computadores levantou-se uma pesquisa sobre as Redes Privadas Virtuais, tratando do que consistem e no seu funcionamento.

Ao verificar as diferenças entre Redes Privadas Virtuais e Redes Públicas, notou-se que o tráfego de dados, em teoria, é muito mais seguro. Além disso, o custo de implementação é consideravelmente baixo, pois ela utiliza a infraestrutura da Rede Pública para trafegar os dados, criando um túnel virtual seguro, que é por onde os dados passam.

A avaliação e descrição do protocolo de segurança IPSec, que é utilizado para a transmissão dos dados em uma VPN, mostrou que ele é o mais indicado para este tipo de rede, pois corrige as carências de segurança dos outros protocolos existentes. Destacou-se também que ele é transparente ao usuário, onde este não necessita saber que está utilizando o mesmo, não havendo também a necessidade de alterar o código de aplicações. Outra vantagem é ter endereçamento padrão tanto para o IPv4 quanto para IPv6.

Foi realizada a implementação de uma rede VPN utilizando o protocolo IPSec baseado em um cenário de aplicação, onde tem-se os equipamentos necessários para que esta rede possa ser criada, bem como a documentação dos resultados obtidos com esta implementação.

7.1.1 Cenário de Aplicação

Com base na Figura 20, o ambiente de aplicação consiste em duas redes distintas, denominadas Rede A e Rede B. Na Rede A existe um *gateway* VPN, formado pelo roteador D-Link DSL-2640B, que possui suporte a IPSec, e um *host* conectado a ele. Este faz o papel de Servidor e será acessado pelo usuário. Possui instalado o sistema operacional Linux

Ubuntu 11.04. Na Rede B tem-se outro *host*, que faz a conexão através de um modem ADSL com endereço IP Dinâmico (automático).

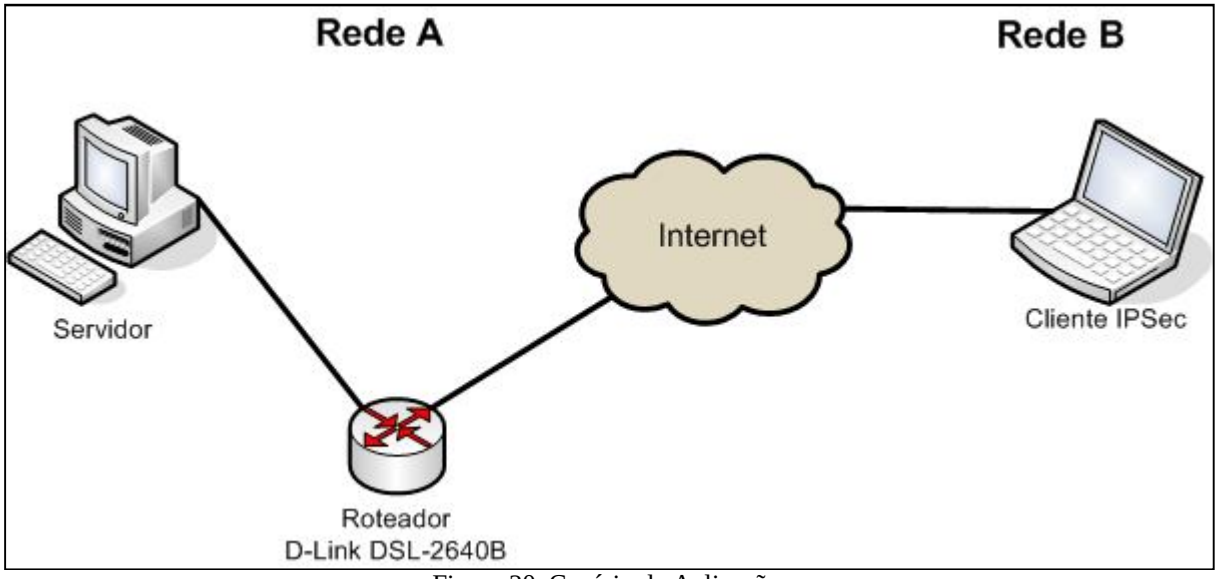


Figura 20. Cenário de Aplicação

Este cenário tem por finalidade atender pessoas que desejam acessar um servidor de dados – este podendo estar localizado em casa ou no trabalho – a partir de uma Internet ADSL comum. Exemplo de aplicação: um médico possui consultórios em três cidades e deseja manter um banco de dados centralizado com informações de todos os seus pacientes, como data da consulta, medicação, dados de exames, entre outros. Para isto, basta ter um computador conectado à Internet e o software VPN instalado, configurado como servidor. De qualquer lugar, por meio de uma conexão ADSL, o médico pode conectar-se ao seu computador principal (servidor) por meio do Túnel e inserir, consultar e alterar dados, sem se preocupar com possíveis capturas de informações.

Os recursos necessários para a realização desta implementação foram os seguintes:

a) três computadores com sistema operacional Linux Ubuntu 11.04 (*kernel* 2.6);

b) softwares Openswan, Wireshark (para captura de pacotes) e Apache;

c) modem D-Link DSL-2640B conectado ao servidor;

d) modem ADSL;

e) conexão com a Internet.

7.1.2 Implementação de VPN com IPSec

Após a definição dos softwares e do cenário a ser implementado, foi necessária a escolha de uma solução que atenda os clientes ADSL, que possuem IPs dinâmicos. Para atender a este requisito foi combinado este aplicativo aos certificados digitais X.509, que são utilizados na identificação dos usuários sem aplicação de DNS dinâmico ou IPs estáticos.

Para a utilização de modem ADSL é necessário realizar algumas alterações, principalmente no lado onde ficará o servidor. Existem duas formas:

a) utilizando NAT Transversal (NAT-T): segundo a RFC 3947 – *Negotiation of NAT-Transversal in the IKE* –, sua função é de verificar se os dois equipamentos que estão estabelecendo a conexão possuem suporte para NAT Traversal, em seguida os equipamentos detectam se existe ou não a tradução de endereços. Por fim, negocia-se os parâmetros do protocolo e inicia-se a transmissão de dados utilizando pacotes encapsulados;

b) utilizando o modo *bridge* do modem ADSL: este modo, quando utilizado, faz com que o IP válido fique referenciado (atrelado) na interface física, sendo necessário efetuar a discagem do mesmo por meio do sistema operacional.

Como a finalidade deste trabalho é testar o protocolo IPSec, será utilizada a opção descrita na alínea B, onde é necessário configurar o modem apenas no lado servidor. No cliente é desnecessário que o IP esteja referenciado na interface, ou seja, pode-se acessar a

Internet por meio de um roteador, *firewall* ou outros dispositivos na frente do *host*. A configuração será descrita no Apêndice A.

O guia para instalação da ferramenta, bem como a criação dos certificados X.509, encontram-se no apêndice B e C respectivamente.

7.1.3 Configuração das Chaves RSA

Antes de iniciar a configuração principal, pode-se primeiramente configurar a chave para a autenticação dos *gateways*. Ela é criada automaticamente ao instalar o Openswan, sendo necessário apenas indicar o caminho no arquivo *ipsec.secrets*. Este processo deve ser refeito no outro *host* que estabelecerá o túnel VPN com este *gateway*. A Figura 21 mostra a configuração do Servidor e do Cliente.

```
Arquivo ipsec.secrets para o Servidor:
%any : RSA /etc/ipsec.d/private/nome-servidor.pem

Arquivo ipsec.secrets para o Cliente:
: RSA /etc/ipsec.d/private/nome-cliente.pem
```

Figura 21. Configuração do arquivo *ipsec.secrets*

O valor *%any* permite que um cliente com qualquer endereço IP faça autenticação fornecendo a respectiva chave pública. Para obter o mesmo efeito, pode-se utilizar o valor 0.0.0.0 ou também deixá-lo sem preenchimento, como é feito na configuração do Cliente. Além disso, outros valores, como endereços IPs dos hosts, são aceitos e fazem igualmente a autenticação com chaves ao servidor.

O valor “RSA” indica o tipo de chave que será utilizada, podendo ser definido também como PSK (menos seguro).

7.1.4 Configuração do Openswan

A configuração básica do Openswan no servidor e no cliente Linux, ambos com a distribuição Ubuntu 11.04, serão apresentadas nesta seção. A correção de possíveis erros está descrita no Apêndice D.

Tanto para o cliente quanto para o servidor, os primeiros arquivos a serem alterados dizem respeito à necessidade de habilitar o Encaminhamento de pacotes IP (IP *Forwarding*) e desabilitar o filtro de caminho inverso (*Reverse Path Filter*). Este filtro é uma característica de segurança que previne ataques do tipo DoS no Linux. Para habilitá-lo, pode-se editar o arquivo */etc/rc.d/rc.local* e adicionar as linhas: *echo 1 /proc/sys/net/ipv4/ip_forward* e *echo 0 /proc/sys/net/ipv4/conf/eth0/rp_filter*.

Por padrão, todas as distribuições Linux modernas têm desabilitado o Encaminhamento IP. Isto normalmente é uma boa idéia, pois a maioria das pessoas não necessita deste encaminhamento. Porém, no caso de uma implementação de VPN com IPSec, é necessário habilitá-lo, editando o arquivo *sysctl.conf* localizado na pasta */etc*. Na linha *net.ipv4.ip_forward = 0* é preciso trocar o número 0 por 1. Já na linha *net.ipv4.conf.default.rp_filter = 1* deve-se alterar o valor para 0.

Após estas configurações serem concluídas, é possível iniciar a configuração do Servidor e posteriormente a do Cliente IPSec.

O uso de um *firewall* na rede pode dificultar ou mesmo impossibilitar a conexão e troca de pacotes. Caso exista, é necessário permitir todo tráfego que transita pela porta UDP 500. Ela é utilizada pelo IKE para negociar as chaves, e permitir os protocolos 50 (ESP) e o 51 (AH). E, caso faz-se uso do NAT-T, também deve-se liberar o tráfego pela porta 4500. A Figura 22 mostra os comandos a serem executados para permitir o acesso VPN através do *firewall* do sistema operacional.

```
Permite Negociação IKE:
# iptables -A OUTPUT -p udp --sport 500 -j ACCEPT
# iptables -A INPUT -p udp --dport 500 -j ACCEPT

Permite Autenticação e Criptografia (ESP):
# iptables -A INPUT -p 50 -j ACCEPT
# iptables -A OUTPUT -p 50 -j ACCEPT

Permite Autenticação de Cabeçalho (AH):
# iptables -A INPUT -p 51 -j ACCEPT
# iptables -A OUTPUT -p 51 -j ACCEPT

Usado para o NAT-T (aplicado quando o IPSec está atrás do NAT):
# iptables -A OUTPUT -p udp --sport 4500 -j ACCEPT
# iptables -A INPUT -p udp --dport 4500 -j ACCEPT
```

Figura 22. Comandos *iptables*

Algumas das referências usadas na elaboração desta configuração podem ser encontradas em OPENSWAN (2011).

7.1.4.1 Configuração do Servidor IPSec

O principal arquivo do Openswan, onde são descritas as configurações do IPSec e das conexões, como IPs, modo de envio de dados, certificados e outros, é o *ipsec.conf*, localizado na pasta */etc* e ilustrado na Figura 23.

```
config setup
        interfaces=%defaultroute
        nat_transversal=no
        virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
        keyingtries=2
        compress=no
        authby=rsasig
        leftrsasigkey=%cert
        rightrsasigkey=%cert

conn vpntcc
        auto=add
        type=tunnel
        pfs=no
        left=189.31.124.90
        leftcert=/etc/ipsec.d/certs/nome-servidor.pem
        right=%any
        rightsubnet=vhost:%priv,%no
```

Figura 23. Arquivo *ipsec.conf* do Servidor

A Figura contém os parâmetros *config setup* e *conn vpntcc*. Na primeira seção, *config setup*, define as configurações básicas utilizadas na inicialização. São elas:

a) *interfaces*: este parâmetro define as interfaces tanto físicas quanto virtuais que o IPSec vai utilizar. O valor *%defaultroute* faz com que o programa procure pela interface ligada ao roteador padrão;

b) *nat_traversal*: é utilizado para contornar a falha do IPSec de não trabalhar com mascaramento de IPs ou NAT. Para desativar este recurso no servidor, utiliza-se o valor “no”;

c) *virtual_private*: é usado para definir subredes virtuais, onde máquinas cliente por detrás no NAT poderão ter endereços dentro de uma faixa de IPs descrita no parâmetro;

d) *keyingtries*: número de tentativas para realizar a conexão;

e) *compress*: se ativo (“yes”), este parâmetro permite que o servidor recomende a compressão dos dados, que ocorre antes da criptografia. Se o valor for “no”,

ele estará inativo, ou seja, o protocolo não vai propor o uso da compressão, mas poderá aceitar se for sugerido pela outra ponta;

f) *authby*: define como o servidor e o cliente se autenticarão. Caso o valor configurado for “rsasig” (mais utilizado), faz uso de chaves RSA para autenticação; o “secret” funciona para chaves pré-compartilhadas; e o valor “never” faz com que não seja possível realizar tentativas de conexão ou que elas nunca sejam aceitas;

g) *leftrsasigkey*: este parâmetro indica a chave RSA para o equipamento ou *host* definido como lado esquerdo da conexão;

h) *rightrsasigkey*: este parâmetro indica chave RSA para o equipamento ou *host* definido como lado direito da conexão.

O segundo, *conn vpntcc* – onde “vpntcc” refere-se ao nome da conexão, escolhido pelo usuário – é referente à seção que define a conexão VPN que será criadas pelo IPSec e utilizada pelos clientes IPSec, contendo parâmetros à seguir:

a) *auto*: define que deve ser feito com esta conexão durante o carregamento do serviço do Openswan. Os valores aceitos são “start” e “add”. Utiliza-se “start”, para a conexão que será iniciada assim que o IPSec for carregado e para conexões fixas, como ocorre entre dois *gateways*. O valor “add” serve para que a conexão seja adicionada no IPSec, mas deve ser iniciada manualmente. É utilizada nas conexões com IP dinâmico e quando o cliente não permanece todo tempo conectado. Ele possui o valor “start”, portanto é responsável pelo estabelecimento da conexão;

b) *type*: refere-se ao modo de envio de dados entre os pontos de comunicação. O modo *tunnel* é mais utilizado por *gateways* que manipulam o tráfego de *hosts* que não têm suporte ao IPSec, e também opção padrão do Openswan;

c) *pfs*: é utilizado em conexões com chaves pré-compartilhadas, portanto exige um sigilo no controle das chaves. O valor padrão desse parâmetro é “yes”;

d) *left*: local onde é definido o endereço IP do host do lado esquerdo da conexão;

e) *leftcert*: indica o nome e o caminho do arquivo com o certificado X.509 gerado para o servidor IPSec;

f) *right*: local onde é definido o endereço IP do host do lado esquerdo da conexão. O valor “%any” representa qualquer endereço de Internet;

g) *rightsubnet*: define qual subrede o cliente deve ter. O uso do valor *vhost:%no,%priv* realiza a permissão de IPs reservados, definidos no parâmetro *virtual_private*, ou endereços privados;

h) *rightcert*: indica o nome e o caminho do arquivo com o certificado X.509 gerado para o *host* IPSec.

7.1.4.2 Configuração do Cliente IPSec

A configuração do cliente é muito semelhante à do servidor, feita através da edição do arquivo */etc/ipsec.conf*. Os parâmetros são apresentados na Figura 24.

```
config setup
        interfaces=%defaultroute
        nat_transversal=yes

conn vpntcc
        auto=start
        pfs=no
        left=189.31.124.90
        leftcert=/etc/ipsec.d/certs/nome-servidor.pem
        right=192.168.0.2
        rightsubnet=vhost:%priv,%no
        rightcert=/etc/ipsec.d/certs/nome-cliente.pem
```

Figura 24. Arquivo *ipsec.conf* do Cliente

A diferença da configuração do cliente para o servidor é em apenas dois parâmetros. O primeiro diz respeito à ativação do suporte ao NAT, alterando o valor equivalente ao *nat_traversal* – o novo valor deve ser “yes”. O segundo é referente à indicação do endereço IP do cliente, *right*. Deve ser alterado sempre que o cliente obtiver um novo endereço.

Os parâmetros descritos na seção de configuração do servidor servem para o cliente, portanto não serão descritos novamente.

7.1.4.3 Iniciando o serviço IPSec

Concluído o processo de configuração, o próximo passo é verificar novamente o status do IPSec, por meio do comando *# ipsec verify*, onde todos os campos devem conter a informação “[OK]” em verde, conforme a Figura 25.

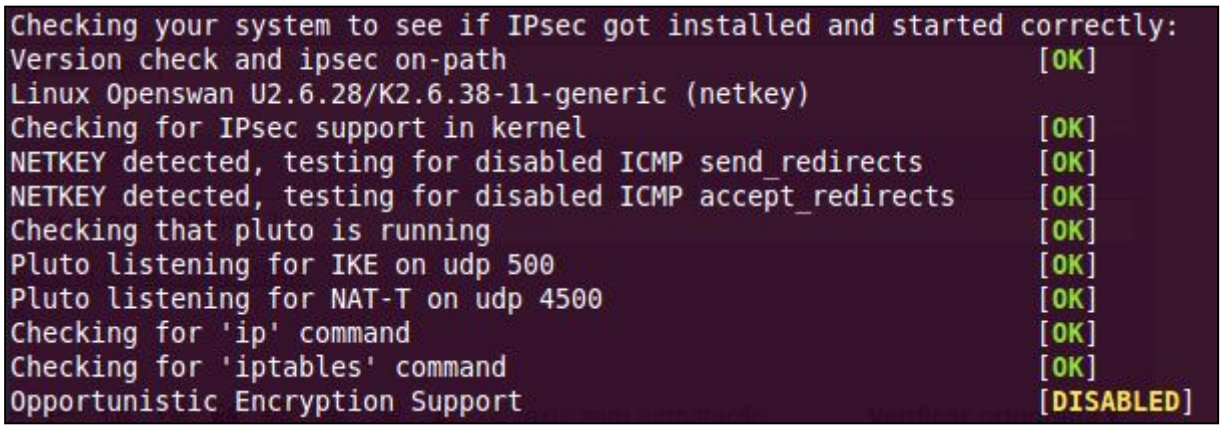


Figura 25. Configuração IPSec Correta

Posteriormente já é possível iniciar o serviço por meio do comando *# ipsec setup start* e estabelecer o túnel por meio do *# ipsec auto --up vpntcc*. A VPN estará criada e funcionando corretamente.

7.2 RESULTADOS OBTIDOS

O uso de VPN com IPSec aliado ao software Openswan permite que um usuário acesse remotamente os dados e recursos da sua rede residencial, conectado por meio de uma Internet ADSL, promovendo a segurança no tráfego de informações.

A Figura 26 apresenta um esquema com os componentes utilizados na configuração do cenário de teste do circuito com Openswan e sistema operacional Linux.

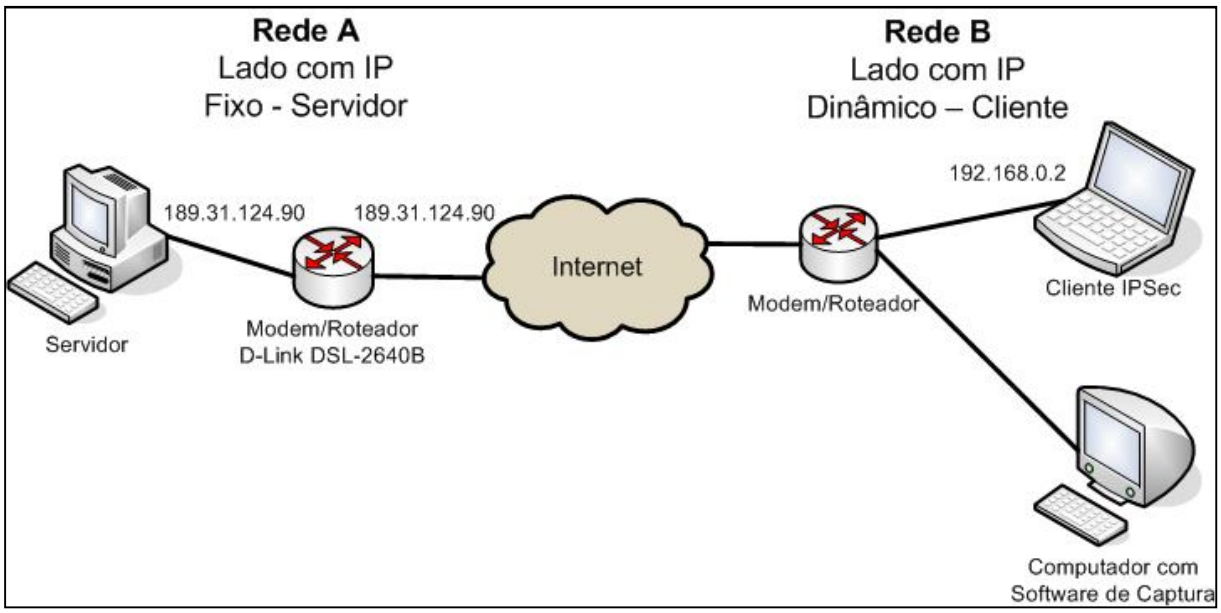


Figura 26. Cenário de Teste

No lado com IP Fixo encontra-se localizado o computador Servidor, rodando um Servidor HTTP Apache[7] com uma página da *web*, onde o cliente irá acessar, realizando a troca de pacotes entre as duas redes e verificando a segurança do protocolo IPSec.

[7] Programa responsável por aceitar pedidos HTTP de clientes e retorná-los com respostas HTTP, podendo incluir dados – geralmente páginas web, como documentos HTML com objetos (imagens, vídeos, entre outros) (APACHE, 2011).

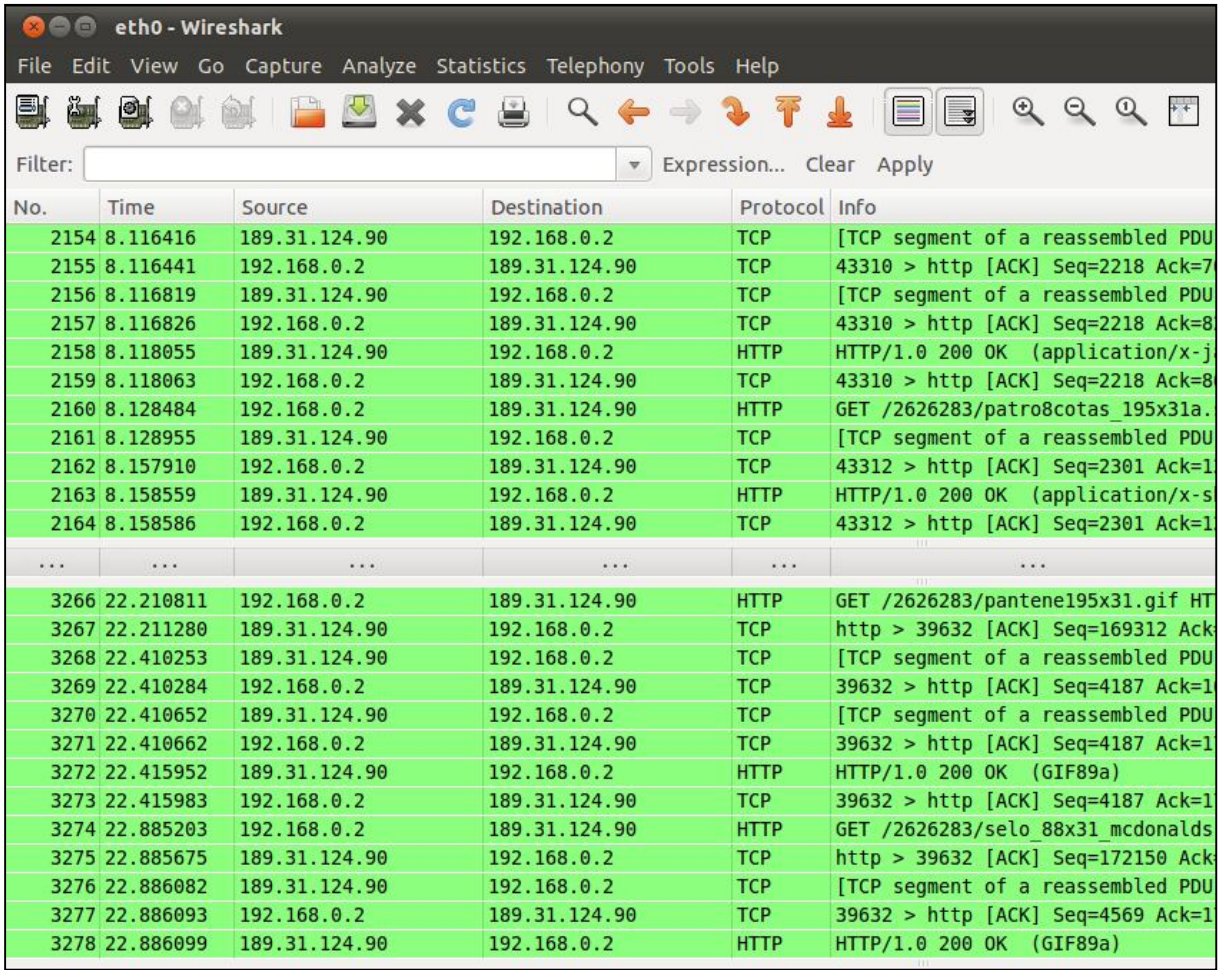
Conectado por meio do roteador D-Link DSL-2640B, que possui suporte à IPSec, o computador da rede A navega na Internet e oferece a possibilidade de receber conexões VPN. Está configurado em modo *bridge*, portanto o endereço IP válido – de saída, neste caso o 189.31.124.90 – é o de sua interface de rede, tornando mais simples a implementação.

Na rede B existe um cliente que se conectará ao servidor e um computador onde está instalado o software de captura de pacotes. Ambas as máquinas encontram-se ligadas à rede por meio de um modem/roteador comum, com funcionamento similar aos de qualquer estabelecimento público, como shoppings, hotéis, entre outros.

A máquina destinada à captura dos pacotes fica "escutando" a rede, tentando capturar primeiramente com a VPN inativa e posteriormente com o Túnel estabelecido, servindo para verificar se o protocolo IPSec aplicado a Redes Privadas Virtuais se mostra eficiente pela sua proposta.

Esta solução representa um baixo custo de implantação, visto que os softwares utilizados são de distribuição livre, tendo apenas a necessidade de se utilizar, no lado do Servidor, um modem/roteador que transmita e receba pacotes IPSec. Traz a facilidade das conexões poderem ser feitas de qualquer ponto onde haja Internet, sem depender do endereço IP do cliente e se há ou não NAT entre as duas pontas, e reduz consideravelmente o tráfego de dados, a partir do uso da compressão de pacotes fornecido pelo IPSec (OLIVEIRA, 2010).

Para verificar se é possível obter certo nível de segurança com esse protocolo, foram capturados os pacotes transitados na rede sem o uso de VPN após uma consulta ao servidor HTTP – localizado na rede A (Figura 26) –, monitorado por meio do software Wireshark. O resultado da análise dos pacotes está representado na Figura 27.



No.	Time	Source	Destination	Protocol	Info
2154	8.116416	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2155	8.116441	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=7
2156	8.116819	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2157	8.116826	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=8
2158	8.118055	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (application/x-j
2159	8.118063	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=8
2160	8.128484	192.168.0.2	189.31.124.90	HTTP	GET /2626283/patro8cotas_195x31a.
2161	8.128955	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2162	8.157910	192.168.0.2	189.31.124.90	TCP	43312 > http [ACK] Seq=2301 Ack=1
2163	8.158559	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (application/x-s
2164	8.158586	192.168.0.2	189.31.124.90	TCP	43312 > http [ACK] Seq=2301 Ack=1
...	...	...	...	...	...
3266	22.210811	192.168.0.2	189.31.124.90	HTTP	GET /2626283/pantene195x31.gif HT
3267	22.211280	189.31.124.90	192.168.0.2	TCP	http > 39632 [ACK] Seq=169312 Ack
3268	22.410253	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3269	22.410284	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3270	22.410652	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3271	22.410662	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3272	22.415952	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (GIF89a)
3273	22.415983	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3274	22.885203	192.168.0.2	189.31.124.90	HTTP	GET /2626283/selo_88x31_mcdonalds
3275	22.885675	189.31.124.90	192.168.0.2	TCP	http > 39632 [ACK] Seq=172150 Ack
3276	22.886082	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3277	22.886093	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4569 Ack=1
3278	22.886099	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (GIF89a)

Figura 27. Pacotes Capturados sem VPN

Com base na Figura – editada com a junção de duas, para que se possa ilustrar um maior número de informações – percebe-se que a quantidade de pacotes capturados é grande, todos trafegando entre o Servidor (189.31.124.90) e o Cliente (192.168.0.2).

A Figura 28 mostra o resultado da mesma consulta, desta vez passando por meio da Rede Privada Virtual, presente entre o Servidor e o Cliente remoto.

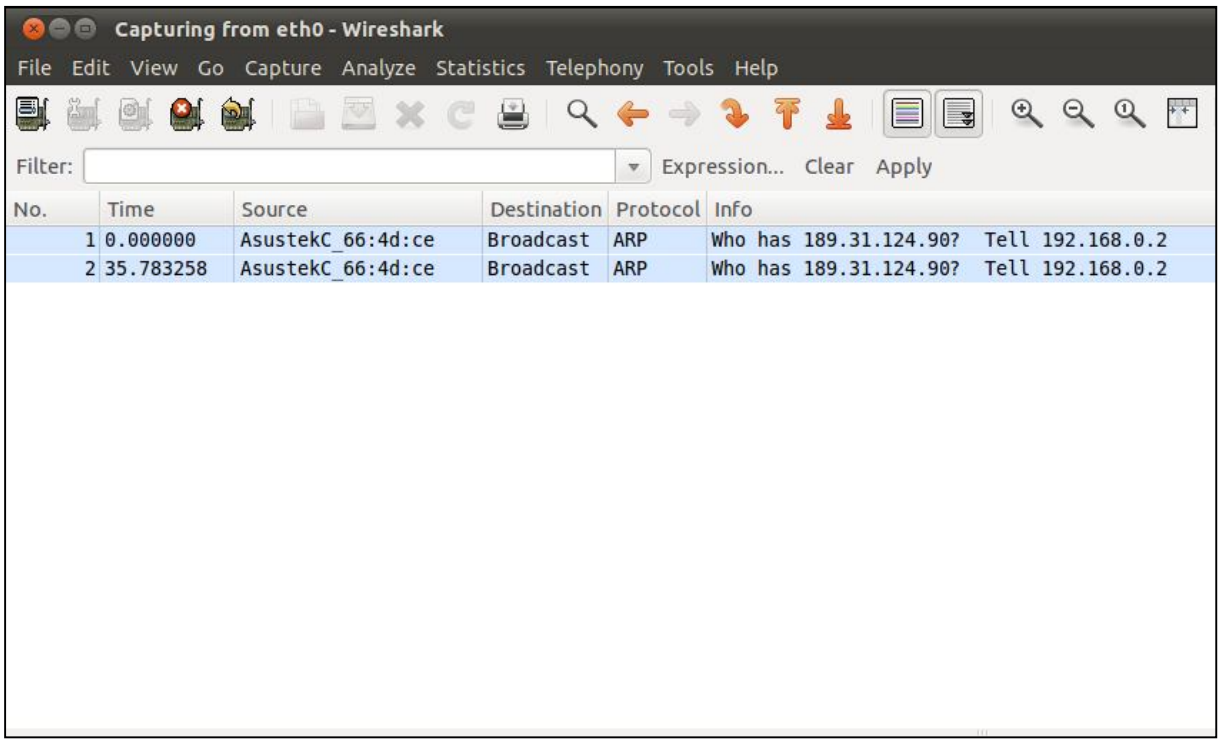


Figura 28. Pacotes Capturados com VPN

Percebe-se que, ao iniciar o túnel, nenhum pacote é capturado através do software – apenas os com destino ao *Broadcast*. Isto mostra que a VPN dificulta que o conteúdo trafegado entre os *hosts* nela conectados seja capturado por *sniffers*[8] ou usuários mal-intencionados, oferecendo a confidencialidade nas informações transmitidas, característica principal de uma Rede Privada Virtual.

[8] Ferramenta capaz de interceptar e registrar o tráfego de dados em uma rede de computadores, capturando, decodificando e analisando o conteúdo de cada pacote.

CONCLUSÃO

De acordo com os estudos realizados, observou-se a importância da Internet na atualidade, principalmente no que diz respeito às redes públicas, utilizadas pela maior parte da população. As informações que nela trafegam correm risco de serem capturadas, analisadas e modificadas por pessoas mal-intencionadas, portanto, quanto maior segurança na transmissão, menor a perda da integridade, da confidencialidade e da autenticidade dos dados.

O objetivo deste foi testar o protocolo de segurança IPSec aplicado à VPN em um ambiente Linux, para interligar usuários ao seu computador residencial por meio de conexões ADSL com NAT ou endereços IPs dinâmicos, detalhando aspectos de configuração e correção de erros. Outros protocolos foram abordados, como o PPTP e L2TP, que se apresentaram como boas alternativas de implementação. Porém, no que diz respeito à segurança o IPSec mostrou maior robustez, apresentando características mais expressivas na proteção do tráfego entre as redes interligadas, podendo-se citar os cabeçalhos de autenticação e conteúdo de segurança encapsulador (AH e ESP) – que visam assegurar a não alteração dos dados, a garantia de que a mensagem foi realmente enviada pelo emissor esperado e também a criptografia dos datagramas IP –, a utilização de Associações de Segurança e o gerenciamento destas AS, feito por meio do Internet Key Exchange.

A partir da aplicação dos testes práticos de comunicação entre máquinas, com e sem configuração de diretivas de segurança, foram obtidos e apresentados resultados que comprovam a eficiência do IPSec. Se utilizado de forma correta, combinando os recursos de protocolos como o AH e o ESP, e outros existentes, dificultará consideravelmente que um invasor descubra algum ponto falho na conexão. Isto faz dele uma grande arma contra os vários tipos de ataques e invasões existentes, fornecendo boa segurança em redes IP, como a Internet.

É importante destacar que somente a VPN e o IPSec não são suficientes para garantir a total segurança de uma rede. É essencial que, além de um planejamento envolvendo políticas rígidas de segurança, exista outras formas de proteção, como *firewalls* por exemplo.

Tanto o sistema operacional Linux quanto o Openswan apresentaram-se eficazes, se mostrando ferramentas atrativas para usuários que não disponibilizam de muitos recursos financeiros ou não pretendem gastar valores altos com tecnologias proprietárias. O Openswan foi capaz de implementar os protocolos do IPSec e fornecer características interessantes de segurança, como métodos de criptografia eficientes, suporte a múltiplos protocolos, suporte para gerenciamento de chaves, gerenciamento de endereços dos clientes e autenticação.

Sua configuração é relativamente complicada, porém a documentação oficial oferece um bom suporte ao usuário, mostrando e explicando todos os arquivos nela contidos. Tem-se apenas que apresentar um pequeno domínio sobre a arquitetura IPSec e uma noção do funcionamento das redes interligadas, a fim de não enfrentar problemas com a configuração desta ferramenta. A maior dificuldade foi aplicá-lo em redes ADSL, pois, com o uso do NAT, tornou-se trabalhoso encontrar a configuração correta, sendo que existe pouca documentação sobre a utilização do software neste tipo de rede. Além disso, se apenas um parâmetro estiver incorreto, já é suficiente para a rede não conectar.

No IPSec alguns ajustes tiveram de ser feitos ao longo do tempo, e no Linux a aplicação Openswan apresentou as melhorias do protocolo frente aos outros existentes. Ganhou recursos para atender as necessidades de usuários que utilizam formas de conexões variadas – geralmente com IPs dinâmicos e utilizando NAT – ou viajam com certa frequencia e não podem depender de um ponto de acesso fixo para ter segurança na transferência de informações.

Os resultados obtidos por esta pesquisa foram satisfatórios, partindo do princípio de que não são necessários equipamentos complexos e caros, fazendo com que esta tecnologia

possa ser empregada até mesmo em redes pequenas, como as residenciais. A tendência atual é que ela seja ainda mais utilizada com o desenvolvimento do acesso à Internet ADSL, tornando-se um atrativo tanto para as organizações pequenas, quanto para usuários comuns, que desejam ter uma base de dados remota e acessá-la de forma segura, independente do local em que esteja.

Em virtude do longo tempo utilizado para encontrar uma configuração correta para o Openswan e usuários ADSL, testes mais exaustivos e com outras ferramentas não puderam ser feitos, bem como testes de estresse, que consiste em testar os limites do software, avaliar seu comportamento e possíveis falhas existentes.

Partindo do princípio que a segurança do IPSec foi testada e comprovada nesta pesquisa, como sugestão para trabalhos futuros e também como forma de aprimorar os conhecimentos nesta tecnologia, pode-se criar uma aplicação que se conecte, por meio de uma VPN, a um banco de dados armazenado em um servidor, ligado à Internet por intermédio de um modem ADSL. Além disso, é possível realizar testes de desempenho[9], avaliando como um banco de dados remoto se comporta com as informações trafegando por meio do túnel, verificando se, além da segurança, o protocolo fornece o desempenho necessário para este tipo de atividade, tomando esse trabalho como subsídio para esta próxima pesquisa.

[9] Para este teste, deve-se levar em conta outros fatores, como por exemplo, a largura de banda.

REFERÊNCIAS

APACHE. The Apache Software Foundation. Disponível em: <http://www.apache.org/>. Acesso em: 8 Out. 2011.

AGUIAR, Paulo Américo Freire. **Segurança em redes wi-fi.** Montes Claros: Universidade Estadual de Montes Claros, 2005.

ASSIS, João Mário de. **Implementando VPN em Linux.** Lavras: Universidade Federal de Lavras, 2003.

BARROS, Aidil da Silveira Barros; LEHFELD, Neide Aparecida de Souza. **Fundamentos de metodologia:** um guia para iniciação científica. 2. ed. São Paulo: Makron Books, 2000.

BRAZIL, Wagner Gaspar. **Protegendo Redes ad hoc com Certificados Digitais e Limite Criptográfico.** Niterói: Universidade Federal Fluminense, 2007.

CERVO, Amado Luiz, BERVIAN Pedro Alcino. **Metodologia cientifica.** 5. ed. São Paulo: Prentice Hall, 2002.

COMER, Douglas E. **Redes de Computadores e Internet.** 4. ed. Porto Alegre: Bookman, 2007.

ESTÁCIO. **ADSL:** Asymmetric Ditigal Subscriber Line. Rio de Janeiro: Universidade Estácio de Sá, 2002. Disponível em: <http://www.micropic.com.br/noronha/Informatica/REDES/ADSL.PDF>. Acesso em: 18 maio 2011.

FAGUNDES, Bruno Alves. **Uma Implementação de VPN.** Petrópolis: Instituto Superior de Tecnologia em Ciências da Computação, 2007.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

FOROUZAN, Behrouz A.. **Comunicação de Dados e Redes de Computadores.** 3. ed. Porto Alegre: Bookman, 2006.

_____. **Protocolo TCP/IP.** 3. ed. São Paulo: Mcgraw-Hill Brasil, 2009.

GODINHO, Luis; BOGO, Madianita. Análise da Utilização do IPSec como Garantia de Segurança na Comunicação em Redes TCP/IP. In: VI ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2004, Palmas. **Anais...** Palmas: CEULP/ULBRA, 2004. Disponível em <http://www.focosecurity.com.br/materiais_academicos_arquivo/luisGodinhoIPSECEncoinfo 2004.pdf>. Acesso em: 22 abr. 2011.

GODINHO, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady; BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: CEULP/ULBRA, 2005. Disponível em <http://lucaszc.homelinux.org/fic-pos/IPV6/IPv6.pdf>. Acesso em: 22 abr. 2011.

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; CORRÊA, Raimundo. **Segurança em Redes Privadas Virtuais – VPNs.** Rio de Janeiro: Brasport, 2006.

LIMA, Almir Wirth. **Redes de Computadores:** Tecnologia e Convergência de redes. Rio de Janeiro: Alta Books, 2009.

MURHAMMER, Martin W.; ATAKAN, Orcun; BRETZ, Stefan; PUGH, Larry R.; NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec, 2007.

NORTHCUTT, Stephen; NOVAK, Judy. **Segurança e Prevenção em Redes.** Tradução: Marcos Vieira. São Paulo: Berkeley, 2001.

NORTHCUTT, Stephen; ZELTSER, Lenny; WINTERS, Scott; FREDERICK, Karen Kent; RITCHEY, Ronald W. **Desvendando Segurança em Redes**: o guia definitivo para fortificação de perímetros de rede usando Firewalls, VPNs, roteadores e sistemas de detecção de invasores. Tradução: Daniel Vieira. Rio de Janeiro: Campus, 2002.

OLIVEIRA, Emerson Luis Galeli de. **Concentrador de VPN com Openswan para conexões em topologia "Road Warrior".** Lavras: Universidade de Lavras, 2010.

OPENSWAN. **Openswan Documentation**. Disponível em: <http://www.openswan.org/docs/>. Acesso em: 6 Ago. 2011.

SCRIMGER, Rob; LASALLE, Paul; PARIHAR, Mridula; GUPTA, Meeta. **TCP/IP:** A Bíblia. Rio de Janeiro: Campus, 2002.

SILVA, Lino Sarlo da. **Virtual Private Network:** VPN. São Paulo: Novatec, 2003.

SOARES, Luiz Fernando G.; LEMOS, Guido; COLCHER, Sérgio. **Redes de Computadores:** das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 1997.

TEIXEIRA, José Helvécio; SUAVÉ, Jacques Philippe; MOURA, José Antão Beltrão; TEIXEIRA, Suzana de Queiroz Ramos. **Redes de Computadores:** Serviços, Administração e Segurança. São Paulo: Makron Books, 1999.

THOMAS, Thomas M. **Segurança de Redes Primeiros Passos.** Rio de Janeiro: Ciência Moderna, 2007. Tradução: Flavio Morgado. Network Security First-step.

TORRES, Gabriel. **Redes de Computadores:** Curso Completo. Rio de Janeiro: Axcel Books, 2001.

VASQUES, Alan Tamer; SCHUBER, Rafael Priante. **Implementação de uma VPN em Linux utilizando o protocolo IPSec.** Belém: CESUPA, 2002.

VERISSIMO, Fernando. **Segurança em redes sem fio.** Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2002.

WADLOW, Thomas A. **Segurança de redes:** projeto e gerenciamento de redes seguras. Tradução: Fábio Freitas da Silva. Rio de Janeiro: Campus, 2000.

BIBLIOGRAFIA COMPLEMENTAR

ALBUQUERQUE, Fernando. **TCP/IP Internet:** Protocolo e Tecnologias. 3. ed. Rio de Janeiro: Axcel Books, 2001.

CYCLADES do Brasil. **Guia Internet de Conectividade.** 6. ed. São Paulo: SENAC, 2000.

FALBRIARD, Claude; BERNAL, Paulo Sergio Milano. **Redes Banda Larga.** Tatuapé: Érica, 2002.

GALLO, Michael A.; HANCOCK, William M. **Comunicação entre Computadores e Tecnologias de Rede.** São Paulo: Cangage Learning, 2003.

KOLENISKOV, Oleg; HATCH, Brian. **Building Linux Virtual Private Networks (VPNs).** Estados Unidos da América: New Riders, 2002.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

PETERSON, Larry L.; DAVIE, Bruce S. **Redes de Computadores:** uma Abordagem de Sistemas. 3. ed. São Paulo: Campus, 2004.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio:** aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 2. ed. São Paulo: Novatec, 2005.

SILVA, Luiz Hamilton Roberto da. **Tecnologia em Redes de Computadores.** Rio de Janeiro: Ciência Moderna, 2009.

SOUSA, Lindeberg Barros de. **Projetos e Implementação de Redes.** Tatuapé: Érica, 2007.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados.** São Paulo, Campus, 2005.

SUZUKI, Kazunari; WOOD, David H. **TCP/IP:** Tutorial e Técnico. São Paulo: Makron Books, 2000.

APÊNDICE A – CONFIGURAÇÃO DO DISCADOR NO SERVIDOR LINUX

Para realizar a conexão utilizando o modo *bridge* do modem ADSL, onde é necessário efetuar a discagem do mesmo por meio do sistema operacional, primeiramente deve-se configurar o modem ADSL. Isto não será abordado neste trabalho, pois difere para cada fabricante e é disponibilizado na documentação do mesmo.

Após o modem, precisa-se criar a conexão no Linux. Para isto, primeiramente deve-se entrar no Terminal. É necessário ter o pacote PPPoE instalado para que o comando tenha efeito. Este pacote é instalado por padrão, mas pode estar ausente se a configuração foi alterada.

No terminal, digita-se: *# sudo pppoeconf*. A Figura 29 ilustra a tela que é apresentada após o comando anterior.

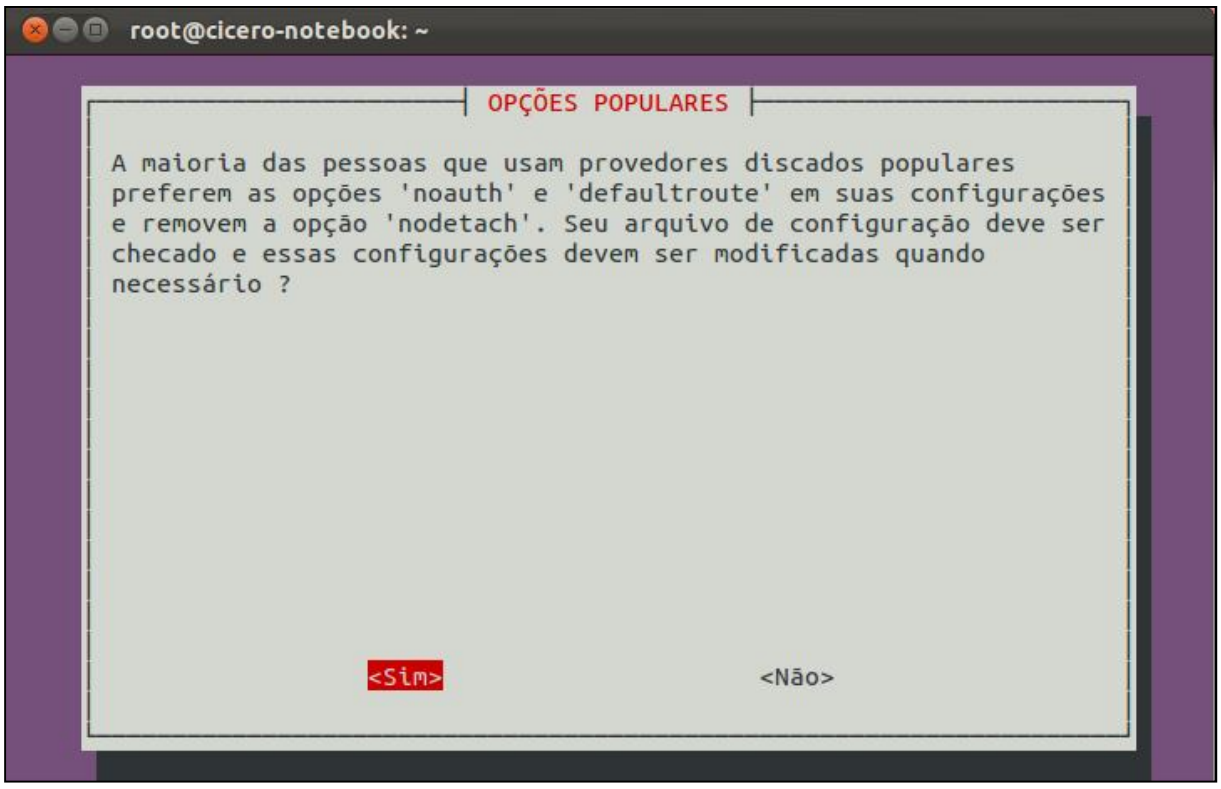


Figura 29. Resultado do Comando *# sudo pppoeconf*

As opções a serem configuradas seguem a ordem das alíneas abaixo:

a) opções populares: será perguntado se o usuário prefere ter as opções “noauth” e “defaultroute” em suas configurações e remover a “nodetach”. Deve-se escolher <Sim>;
b) se já existe uma conexão PPPoE configurada, será perguntado se ele pode ser modificado. Caso isto aconteça, selecionar <Sim>;
c) digitar o nome de usuário;
d) digitar a senha;
e) usar Peer DNS – escolher <Sim>;
f) problema MSS limitado – selecionar <Sim>;
g) optar por iniciar a conexão na inicialização do sistema operacional deve ser escolhida conforme as preferências do usuário;
h) para estabelecer a conexão imediatamente, na tela seguinte coloque <Sim>;
i) por fim, aparecerá a informação de que a conexão foi iniciada, com alguns comandos utilizados para obter diversas informações. Depois de terminado estes passos, a conexão estará funcionando.

Outra configuração que deve ser feita é referente ao servidor DNS. Para isto, é necessário editar o arquivo */etc/resolv.conf*, alterando os números existentes pelos do provedor de Internet.

A partir destes passos a configuração está criada com sucesso.

APÊNDICE B – INSTALAÇÃO DO OPENSWAN

Por meio da ferramenta Advanced Packaging Tool (APT), é possível realizar a instalação de forma simples e rápida.

Tanto no cliente quando no servidor, ela é feita por meio do seguinte comando: # *apt-get install openswan*, informando a senha do administrador (*root*) do sistema.

Caso seja solicitada a confirmação de instalação de novos pacotes para atender aos pré-requisitos do Openswan devem-se aceitar as recomendações, para o funcionamento correto do IPSec no Linux.

Também é necessário criar um certificado X.509, selecionando a opção <Sim> ao surgir a mensagem “Criar um certificado X509 auto-assinado?” e posteriormente usar o certificado criado para o *host.*

Tabela 5. Diretório e arquivos de configuração do IPSec

Diretório/Arquivo	Descrição
/etc/ipsec.d	Contém certificados, configurações e referências do ipsec.conf
/etc/ipsec.conf	Arquivo com a configuração inicial e parâmetro das conexões
/etc/ipsec.secrets	Arquivo com as chaves usadas nas conexões

Fonte: Adaptada de OLIVEIRA, E. L. G. (2010, p. 30)

Ao final da instalação, o diretório e arquivos a serem criados são apresentados na Tabela 5.

O próximo passo consiste na configuração dos certificados.

APÊNDICE C – CRIAÇÃO DE CERTIFICADOS DIGITAIS X.509

Ao instalar o Openswan, o certificado é criado se a opção <Sim> for selecionada ao surgir a mensagem “Criar um certificado X509 auto-assinado?”. Caso não tenha sido criado, é possível fazê-lo através dos comandos ilustrados na Figura 30.

```
Gera Certificado para a CA:
# perl /usr/lib/ssl/misc/CA.pl -newca

Gera certificado para as estações:
# perl /usr/lib/ssl/misc/CA.pl -newreq
# perl /usr/lib/ssl/misc/CA.pl -sign
```

Figura 30. Geração do Certificado X.509

Desta forma eles estarão criados e poderão ser utilizados para a conexão VPN.

APÊNDICE D – CORREÇÃO DE ERROS DO OPENSWAN

Alguns erros podem ser apresentados. Esta seção mostra como resolvê-los, deixando o Openswan prontamente configurado para a utilização.

O primeiro trata do Erro de suporte no *kernel* e pluto. Ao utilizar o comando *# ipsec verify*, que serve para verificar o serviço IPSec, a mensagem apresentada é ilustrada na Figura 31.

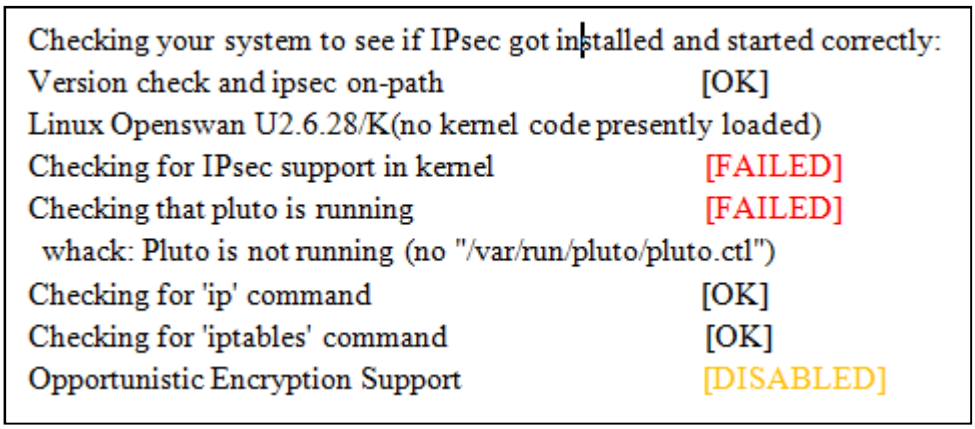


Figura 31. Erro *kernel* e pluto

A resolução dos erros em vermelho é possível simplesmente reiniciando o serviço, por meio do comando *# ipsec setup restart*.

O segundo que pode ocorrer é referente ao NETKEY. Utilizando o comando *# ipsec verify*, ocorre falha na checagem do meso e é solicitado para que o usuário desabilite *send_redirects* e *accept_redirects* (Figura 32).

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.28/K2.6.38-11-generic (netkey)
Checking for IPsec support in kernel                            [OK]
NETKEY detected, testing for disabled ICMP send_redirects       [FAILED]

 Please disable /proc/sys/net/ipv4/conf/*/send_redirects
 or NETKEY will cause the sending of bogus ICMP redirects!

NETKEY detected, testing for disabled ICMP accept_redirects     [FAILED]

 Please disable /proc/sys/net/ipv4/conf/*/accept_redirects
 or NETKEY will accept bogus ICMP redirects!

Checking that pluto is running                                  [OK]
Pluto listening for IKE on udp 500                              [OK]
Pluto listening for NAT-T on udp 4500                           [OK]
Checking for 'ip' command                                       [OK]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

Figura 32. Erro NETKEY

Este problema é resolvido editando/criando o *script* localizado na pasta */Bin*, por meio do comando *# gedit /bin/disable_send_accept_redirects* e inserindo o conteúdo presente na Figura 33.

```
#!/bin/bash

# Disable send redirects
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/default/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth0/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth1/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/lo/send_redirects

# Disable accept redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/default/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth0/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth1/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/lo/accept_redirects
```

Figura 33. *Script* a ser criado

Após inserir o conteúdo é necessário salvar e fechar. Posteriormente, deve-se acessar a pasta por meio do comando *# cd /bin* e executar o arquivo por meio dos comandos *# chmod +x disable_send_accept_redirects* e *# ./disable_send_accept_redirects.*

Para que ele seja iniciado automaticamente, basta adicionar uma linha no *script rc.local*, por meio do comando *# gedit /etc/rc.local*. A linha é a referente à pasta de localização e o arquivo editado: */bin/disable_send_accept_redirects.*

Outros erros podem ser facilmente resolvidos reiniciando o serviço IPSec, por meio do comando *# ipsec setup restart*.

APÊNDICE E - SEGURANÇA EM REDES ADSL UTILIZANDO REDES PRIVADAS VIRTUAIS E O PROTOCOLO IPSEC: ESTUDO DE CASO

Segurança em Redes ADSL utilizando Redes Privadas Virtuais e o Protocolo IPSec

Cícero Zanelato[1], Paulo João Martins[2]

[1] Acadêmico do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – Brasil

[2] Professor MSc. do Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – Brasil

cicerozanelato@gmail.com, pjm@unesc.net

ABSTRACT. *Currently, Computer Networks are everywhere. It is through them that you can conduct research, exchange information and files, such as images. With all these possibilities, sometimes secret information can pass, and may fall into the hands of bad intentioned people. To avoid this type of capture, there are tools that assist in traffic of safety information on public networks. The Virtual Private Network (VPN), working together with IPSec protocol, show's a simple, cheap and efficient way of data transfer in an unsecured network, as the Internet. It's used in large enterprises, but it is also possible to apply this solution for common users or small businesses, which are connected through ADSL Internet systems. This coursework presents and discusses the concept of VPN networks, the addressing some security methods and the most common types of attacks. Using simple concepts, tests are made with the Linux operational system and Openswan software, which creates IPSec tunnels, checking its efficiency as an security alternative of connecting users through ADSL. For this, the client, located in a network with dynamic IP, connects to the HTTP server by performing queries. Tests made with these tools demonstrate the importance of data security passing to the network, and proposes a way for users to connect and share resources found in your remotely local network.*

RESUMO. *Atualmente as Redes de Computadores estão por toda parte. É por meio delas que se pode realizar pesquisas, trocar informações e arquivos, como imagens. Com toda essa possibilidade de utilização, frequentemente transitam informações sigilosas, que podem cair nas mãos de pessoas mal-intencionadas. Para evitar este tipo de captura, existem ferramentas que auxiliam na segurança do tráfego de informações em redes públicas. A Rede Privada Virtual (VPN), aliada ao protocolo IPSec, configura uma maneira simples, barata e eficiente de transmitir dados em uma rede não segura, como a Internet. É mais utilizada em grandes empresas, mas também é possível aplicar esta solução para usuários comuns ou pequenas empresas, que se conectam através de Internet ADSL. Este trabalho apresenta e discute o conceito de redes VPN, abordando alguns métodos de segurança e tipos de ataques mais comuns.*

A partir dos conceitos, são realizados testes utilizando o sistema operacional Linux e o software Openswan, que cria túneis IPSec, verificando sua eficiência como alternativa de segurança para conectar usuários por meio da ADSL. Para isto, o cliente, localizado em uma rede com IP dinâmico, se conecta ao servidor realizando consultas HTTP. Os testes realizados com estas ferramentas demonstram a importância da segurança dos dados que trafegam na rede, e propõe uma forma dos usuários se conectarem e compartilharem recursos encontrados em sua rede local, de forma remota.

1. Introdução

Quando as redes surgiram, não existia grande preocupação relacionada à segurança das informações. As primeiras interligavam universidades, algumas empresas e instituições militares.

Atualmente são a base da comunicação. É por meio delas que se pode realizar a troca de informações com pessoas do mundo inteiro, manter-se atualizados com notícias globais e inclusive realizar pesquisas dos mais variados assuntos.

A tecnologia ADSL (em português, Linha Digital Assimétrica para Assinante) surgiu com a finalidade de permitir uma transferência de dados em alta velocidade por meio de linhas telefônicas comuns. Esta forma de conexão em banda larga hoje é a mais utilizada no Brasil e uma das mais conhecidas no mundo.

Esta tecnologia de comunicação por meio das redes públicas possibilita que o usuário realize transações bancárias, compre os mais variados produtos em lojas virtuais, assista cursos on-line e também a utilize como forma de entretenimento. Além disso, várias empresas se comunicam com suas filiais por meio deste tipo de rede, expondo seus dados de forma insegura, correndo o risco de serem capturados e interceptados por pessoas mal intencionadas. Elas são consideradas não confiáveis por não terem grande segurança no tráfego de informações (ROSSI; FRANZIN, 2000).

A partir da necessidade de se utilizar as redes públicas de comunicação – como a ADSL – para trafegar informações de forma segura, surgiu o advento das Redes Privadas Virtuais (VPN, ou Virtual Private Network). Ela fornece um canal privado, criptografado e autenticado semelhante a um túnel, porém de forma virtual, utilizando uma rede pública de comunicação. Permite que um usuário externo participe na rede interna como se estivesse conectado diretamente a ela (NORTHCUTT et al, 2002).

Apesar de sua maior segurança, as VPNs ainda são suscetíveis a falhas. Para fornecer uma maior integridade e sigilo dos dados foram criados alguns protocolos que tornam mais difícil o acesso aos dados privados.

Baseado em padrões desenvolvidos pela Internet Engineering Task Force (IETF, organização que desenvolve os padrões da Internet), o IP Security Protocol (IPSec) é um conjunto de protocolos que buscam garantir a integridade, autenticidade e confidencialidade na comunicação e transporte dos dados em uma rede IP.

Operando sob a camada três (camada de rede) do modelo Open Systems Interconnection (OSI), do International Organization for Standardization (ISO), o IPSec possui por função a tentativa de impedir a perda de integridade dos dados e falsificação de identidade, implementando autenticação e encriptação, e fornecendo uma segurança na comunicação de máquina-a-máquina.

Com a finalidade de aplicar e testar o protocolo IPSec como alternativa de segurança às Redes Privadas Virtuais, foi realizado um projeto de rede VPN voltado para

clientes ADSL, simulando esta rede entre dois computadores conectados por meio de modems, verificando primeiramente se é possível aplicar esse protocolo para este tipo de cliente e se promove alguns recursos interessantes no que diz respeito à segurança.

A sua utilização por usuários ADSL se justifica na necessidade de haver uma conexão segura também para o acesso remoto a dados privados contidos tanto em residências quanto em empresas que fazem uso desta tecnologia para a transmissão e troca de informações. Para isto, é necessária a criação de uma Rede Privada Virtual, utilizando como meio a ADSL, verificando primeiramente se esta tecnologia suporta as técnicas de tunelamento e algoritmos da VPN e se é uma alternativa interessante, principalmente quando não se dispõe de grandes recursos financeiros.

2. Redes de Computadores

As redes de computadores foram criadas com o objetivo de compartilhar recursos aos usuários, como dados, aplicações e equipamentos, independente da localização física tanto do usuário como do recurso (ASSIS, 2003; LIMA, 2009). Ainda, conforme Torres (2001, p. 5), "as redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante de você."

Elas possuem diversos tamanhos e classificações. As mais comuns são: Redes Locais (Local Area Network - LAN), Redes Metropolitanas (Metropolitan Area Network - MAN) e Redes de Longa Distância (Wide Area Network - WAN) (VASQUES; SCHUBER, 2002).

A forma com que os dispositivos conectados em rede podem se comunicar se chama protocolo de comunicação. Para isto, os dispositivos devem estar utilizando o mesmo protocolo. Com essa necessidade, vários foram criados e são utilizados para transmissão de dados. Destacam-se TCP/IP, Network Basic Input/Output System (NetBIOS), Network Basic Input/Output System Extended User Interface (NetBEUI), Interwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) e UDP.

2.1. TCP/IP

Segundo Tanenbaum (1997), no momento em que as redes de rádio e satélite foram criadas começaram a surgir problemas com os protocolos existentes, forçando a criação de uma nova arquitetura de referência. Foi então que, na década de 70, surgiu o conjunto de protocolos que até hoje é a base da Internet, o Transmission Control Protocol/Internet Protocol (TCP/IP), também conhecido como Protocolo de Internet. O nome é derivado dos dois principais protocolos da arquitetura, o TCP e o IP (ASSIS, 2003).

O Protocolo de Internet foi criado pensando em redes grandes e de longa distância, onde a informação pode percorrer diferentes caminhos para chegar ao computador receptor (TORRES, 2001). Para Teixeira et al (1999), este protocolo fornece um sistema aberto, pois muitas de suas implementações e especificações são disponíveis publicamente, fazendo dele a forma mais usada atualmente para comunicar computadores remotos. Ele serve de base para a Internet, que é uma rede de longa distância com nós interligados pelo mundo todo.

2.2. IP

O protocolo TCP/IP é roteável, ou seja, permite intercomunicar várias redes por diversos caminhos que interligam o transmissor e o receptor. Para isto, ele utiliza um esquema de endereçamento lógico, chamado de endereçamento IP (TORRES, 2001).

Para Teixeira et al (1999), o IP não possui a função de oferecer um serviço confiável. Ele foi projetado apenas para permitir a interconexão de redes para formar as inter-redes (Internets). Uma inter-rede consiste em *hosts* conectados a redes que são interligadas por meio de *gateways* (computador ou dispositivo responsável pela ligação entre duas redes), e identificados por endereços IP.

2.3. TCP

O Protocolo de Controle de Transmissão (Transmission Control Protocol – TCP), descrito na RFC 793, é orientado à conexão, possuindo a finalidade de fornecer um circuito lógico ou serviço de conexão confiável, o que permite a entrega dos pacotes entre o transmissor e o receptor sem que haja perdas (FOROUZAN, 2009; MURHAMMER et al, 2000). Além disso, segundo Teixeira et al (1999), faz a retransmissão de pacotes perdidos, a eliminação de duplicados, o fornecimento de avisos de recebimento para pacotes recebidos com sucesso, entre outros.

Para que a transferência do fluxo de dados seja efetuada, tanto o transmissor como o receptor criam pontos terminais chamados *socket*. Cada *socket* possui um número que define o endereço IP do *host* agregado a mais um número de 16 *bits* local para este, chamado porta. A porta identifica o acesso a um serviço, que é utilizado quando é criada uma conexão explícita entre o transmissor e o receptor (ASSIS, 2003; FOROUZAN, 2009).

2.4. UDP

Descrito na RFC 768, o User Datagram Protocol (UDP) é basicamente uma interface de aplicação para o IP. Segundo Murhammer et al (2000), ele não proporciona confiabilidade, controle de fluxo ou recuperação de erros IP. Serve simplesmente como um multiplexador/demultiplexador para o envio e o recebimento de datagramas, fazendo uso de portas para direcionar os datagramas. Por isso, é utilizado em aplicações que não necessitam de entrega precisa e sim entrega imediata, como voz e imagem (ASSIS, 2003).

Além disso, como em TCP, o UDP emprega campos especiais para identificar os processos emissores e os processos recebedores para cada transação – as portas. Um mecanismo de sumarização de verificações (*checksum*) também é fornecido (TEIXEIRA et al, 1999).

3. Segurança em Redes de Computadores

O termo segurança é utilizado como significado de minimizar a vulnerabilidade de bens e recursos. Em redes de computadores, está relacionada à necessidade de proteção contra o

acesso ou manipulação de informações, confidenciais ou não, por elementos não autorizados (SOARES; LEMOS; COLCHER, 1995; WADLOW, 2000).

A segurança da informação é um conjunto de normas, procedimentos, orientações e demais ações que tem por objetivo proteger a informação. Além disso, para uma organização, ela existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da mesma (FONTES, 2006). Sem a informação, ou conhecimento, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas (FONTES, 2006).

Para Fagundes (2007), quando se fala em segurança da informação presumem-se três premissas que devem ser atendidas: Confidencialidade, Integridade e Autenticidade. Em serviços pela rede, também é necessário garantir a Disponibilidade dos recursos.

A confidencialidade visa assegurar que o conteúdo de um pacote enviado pela rede não será "legível" para intrusos, mas apenas para o real destinatário. Para isso, geralmente é feito o uso de Criptografia (VASQUES; SCHUBER, 2002; WADLOW, 2000).

A Integridade é a garantia de que os dados não serão alterados durante uma transmissão. Já a autenticidade garante que a mensagem foi realmente enviada pelo emissor esperado (AGUIAR, 2005; VASQUES; SCHUBER, 2002).

Disponibilidade é garantir que um serviço esteja disponível quando for solicitado, mesmo em caso de ataques (ASSIS, 2003).

4. Redes ADSL

Asymmetric Digital Subscriber Line (ADSL) é uma tecnologia de comunicação que consiste em transmitir dados em alta velocidade por uma rede de telefone convencional. Para isto é necessário a utilização de um modem, que converte o sinal padrão do fio de telefone em um canal digital. Os modems são chamados "assimétricos" porque transmitem dados de um local a outro em uma velocidade menor do que recebem. Isto também é considerada uma característica do ADSL (TORRES, 2001).

Segundo Murhammer et al (2000), o ADSL funciona a partir do modem. Ele se conecta com o modem da operadora telefônica correspondente ao telefone que está instalado no local, sendo responsável pela divisão digital da linha telefônica em três canais separados. O primeiro é utilizado para transmissão de voz. O segundo para o fluxo de informações do usuário em direção a rede externa (chamado de *upstream,* ou *upload*) e o terceiro canal para o fluxo de dados no sentido da rede para o usuário (conhecido como *downstream,* ou *download*).

5. Redes Privadas Virtuais

Quando as redes de computadores surgiram não se tinha tanta preocupação com a segurança como atualmente. Comunicações de longa distância são cada vez mais necessárias entre empresas, filiais, parceiros, entre outros.

As Redes Privadas Virtuais (Virtual Private Network – VPN) surgiram com o propósito de fornecer integridade, confidencialidade, autenticidade e controle de acesso às informações trafegadas, reduzindo o risco de ataques externos (ASSIS, 2003; GUIMARÃES; LINS; CORRÊA, 2006). Ela funciona a partir da idéia de se utilizar a rede pública para transmitir dados criptografados de forma segura (NORTHCUTT et al, 2002).

Algumas implementações VPN utilizam um software cliente instalado nos computadores que se conectam a rede, que é responsável por estabelecer o canal de comunicação entre as duas pontas (ASSIS, 2003). Outra forma de implementação VPN, segundo Aguiar (2005), é utilizar um *gateway* VPN para criptografar e descriptografar os dados transmitidos, não sendo necessária a intervenção do usuário. Assis (2003) afirma que, muitas vezes, o usuário nem sabe que está utilizando a rede privada. Esta transparência permite que aplicações, usuários e computadores acessem recursos remotamente como se estivessem em uma rede local, sendo amplamente utilizada para conectar empresas matriz e filial.

5.1. Internet Protocol Security

Como resposta as carências de segurança existentes no protocolo IP, a IETF desenvolveu um conjunto de padrões voltados à segurança sobre o IP, denominado IP Security Protocol (IPSec), com o intuito de ser o protocolo padrão de endereçamento tanto para o IPv4 quanto para a próxima versão do IP, o IPv6 (FAGUNDES, 2007; SILVA, 2003).

5.1.1. Modos de Funcionamento

Segundo Thomas (2007), o IPSec possui dois modos de envio de dados criptografados entre os pontos de comunicação: modo de Transporte e modo Túnel, onde cada modo difere em sua aplicação e na quantidade de carga adicionada ao pacote passageiro.

O modo nativo é o de Transporte. A transmissão do pacote protegido por ele é feita entre os *hosts*, onde o responsável pelo encapsulamento é o próprio *host*. Nos pacotes criados neste modo são adicionados cabeçalhos de autenticação e conteúdo de segurança encapsulador (AH[10] e ESP[11]) logo após o cabeçalho IP original, de modo que apenas os protocolos superiores podem ser cifrados/autenticados (FAGUNDES, 2007; GODINHO et al, 2005).

O modo Túnel, segundo Fagundes (2007), é mais utilizado por *gateways* que manipulam o tráfego de *hosts* que não têm suporte ao IPSec, onde o pacote original – que é tratado como um dado só – é encapsulado em um novo pacote com a criptografia do IPSec (incluindo o cabeçalho original), e então é enviado para o outro *gateway* que desencapsula e o encaminha ao destinatário.

6. Utilização do IPSec para Possibilitar maior Segurança em Redes Privadas Virtuais

Com a finalidade de aplicar e testar o protocolo IPSec como alternativa de segurança para Redes Privadas Virtuais foi realizado um projeto de rede voltado para clientes ADSL. Para

---

[10] Authentication Header, possui a função de garantir que o pacote não foi alterado durante a transmissão.
[11] Encapsulating Security Payload, utilizado para prover a checagem de integridade, autenticação e criptografia dos datagramas IP.

isso, é simulada uma rede entre dois computadores conectados por meio de modems, verificando se este protocolo provê o mínimo de segurança necessária para o tráfego de dados em uma rede de Internet.

O sistema operacional a ser utilizado foi o Linux, versão Ubuntu 11.04, por possuir grande flexibilidade e recursos que provêem maior segurança da rede. Além disso é gratuito, não sendo necessário adquirir licenças para obtê-lo.

Para a configuração da VPN foi escolhida a ferramenta Openswan, que implementa o protocolo IPSec para proteger o tráfego da rede baseado no IP. É uma continuação do extinto projeto FreeS/WAN, ou seja, é uma implementação *open source* – de código aberto – do IPSec.

A sua utilização neste trabalho deve-se à necessidade de um software que implemente o serviço IPSec. Com isso, para ser possível a conexão da Rede Privada Virtual teve-se que descartar o mais comum, OpenVPN, que não implementa este recurso. Nele o tunelamento é feito por meio do protocolo SSL.

6.1. Cenário de Aplicação e Testes

O uso de VPN com IPSec aliado ao software Openswan permite que um usuário acesse remotamente os dados e recursos da sua rede residencial, conectado por meio de uma Internet ADSL, promovendo a segurança no tráfego de informações.

A Figura 1 apresenta um esquema com os componentes utilizados na configuração do cenário de teste do circuito com Openswan e sistema operacional Linux.

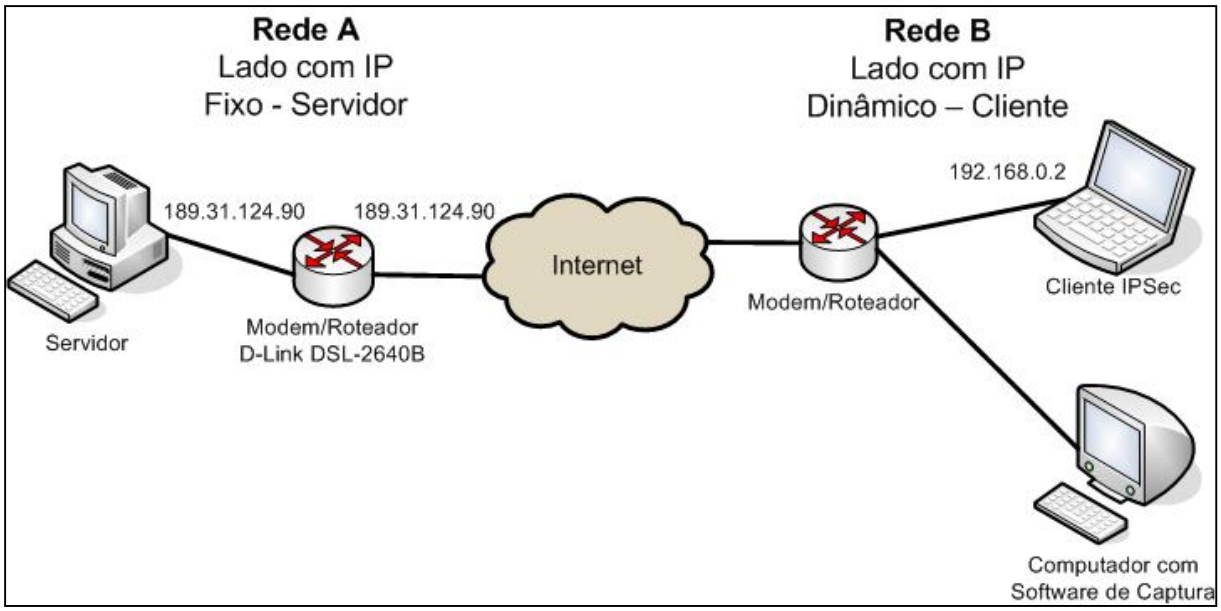


Figura 1. Cenário de Teste

No lado com IP Fixo encontra-se localizado o computador Servidor, rodando um Servidor HTTP Apache[12] com uma página da *web*, onde o cliente irá acessar, realizando a troca de pacotes entre as duas redes e verificando a segurança do protocolo IPSec.

Conectado por meio do roteador D-Link DSL-2640B, que possui suporte à IPSec, o computador da rede A navega na Internet e oferece a possibilidade de receber conexões VPN. Está configurado em modo *bridge*, portanto o endereço IP válido – de saída, neste caso o 189.31.124.90 – é o de sua interface de rede, tornando mais simples a implementação.

Na rede B existe um cliente que se conectará ao servidor e um computador onde está instalado o software de captura de pacotes. Ambas as máquinas encontram-se ligadas à rede por meio de um modem/roteador comum, com funcionamento similar aos de qualquer estabelecimento público, como shoppings, hotéis, entre outros.

A máquina destinada à captura dos pacotes fica "escutando" a rede, tentando capturar primeiramente com a VPN inativa e posteriormente com o Túnel estabelecido, servindo para verificar se o protocolo IPSec aplicado a Redes Privadas Virtuais se mostra eficiente pela sua proposta.

Após a definição dos softwares e do cenário a ser implementado, foi necessária a escolha de uma solução que atenda os clientes ADSL, que possuem IPs dinâmicos. Para atender a este requisito foi combinado este aplicativo aos certificados digitais X.509, que são utilizados na identificação dos usuários sem aplicação de DNS dinâmico ou IPs estáticos.

Para a utilização de modem ADSL é necessário realizar algumas alterações, principalmente no lado onde ficará o servidor. Existem duas formas:

c) utilizando NAT Transversal (NAT-T): segundo a RFC 3947 – *Negotiation of NAT-Transversal in the IKE* –, sua função é de verificar se os dois equipamentos que estão estabelecendo a conexão possuem suporte para NAT Traversal, em seguida os equipamentos detectam se existe ou não a tradução de endereços. Por fim, negocia-se os parâmetros do protocolo e inicia-se a transmissão de dados utilizando pacotes encapsulados;
d) utilizando o modo *bridge* do modem ADSL: este modo, quando utilizado, faz com que o IP válido fique referenciado (atrelado) na interface física, sendo necessário efetuar a discagem do mesmo por meio do sistema operacional.

Com a finalidade de testar a utilização do protocolo IPSec em redes ADSL, será utilizada a opção descrita na alínea B, onde é necessário configurar o modem apenas no lado servidor. No cliente é desnecessário que o IP esteja referenciado na interface, ou seja, pode-se acessar a Internet por meio de um roteador, *firewall* ou outros dispositivos na frente do *host*.

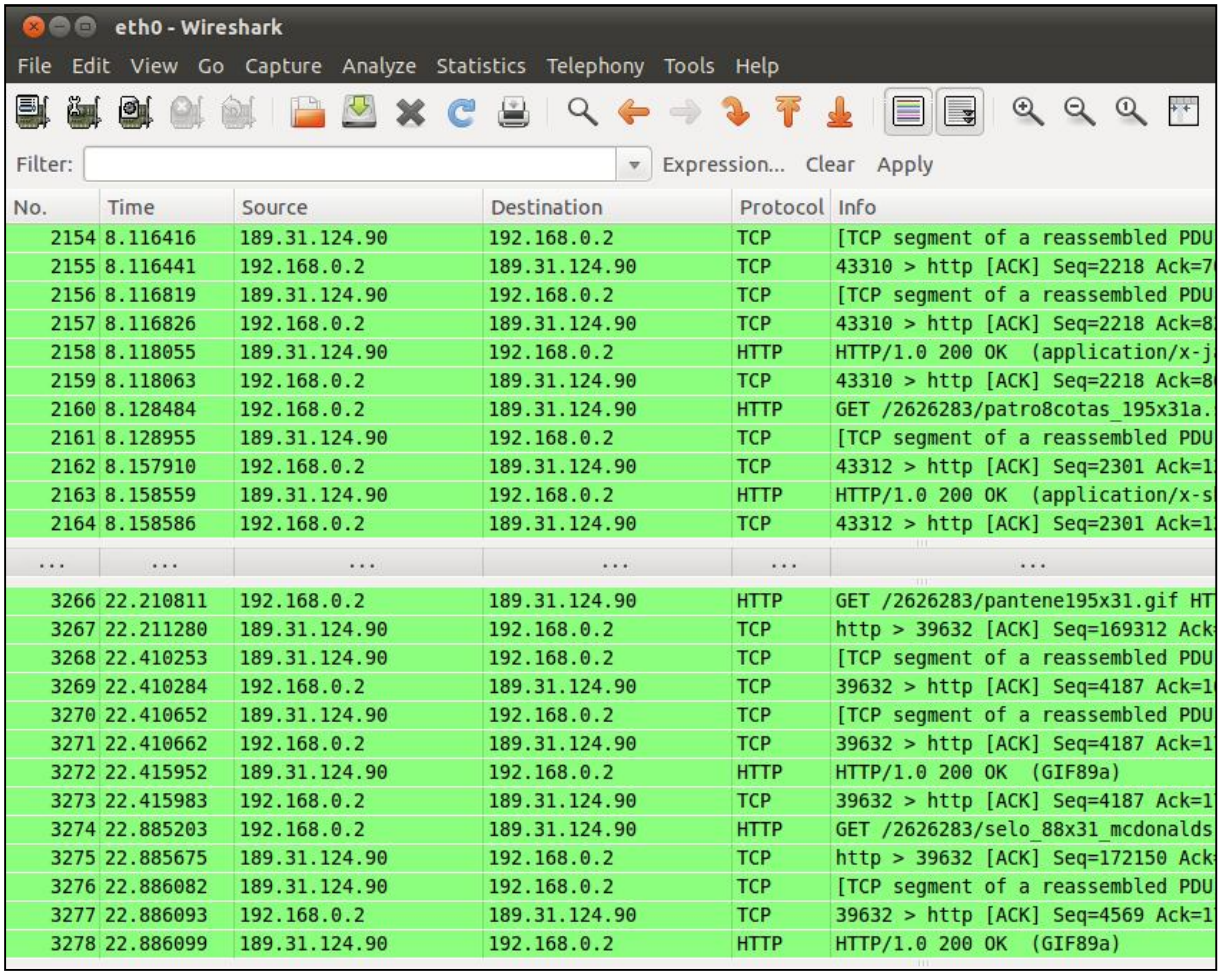
6.2. Resultados Obtidos

O uso de VPN com IPSec aliado ao software Openswan permite que um usuário acesse remotamente os dados e recursos da sua rede residencial, conectado por meio de uma Internet ADSL, promovendo a segurança no tráfego de informações.

Para verificar se é possível obter certo nível de segurança com esse protocolo, foram capturados os pacotes transitados na rede sem o uso de VPN após uma consulta ao

[12] Programa responsável por aceitar pedidos HTTP de clientes e retorná-los com respostas HTTP, podendo incluir dados – geralmente páginas web, como documentos HTML com objetos (imagens, vídeos, entre outros) (APACHE, 2011).

servidor HTTP – localizado na rede A (Figura 26) –, monitorado por meio do software Wireshark. O resultado da análise dos pacotes está representado na Figura 2.



No.	Time	Source	Destination	Protocol	Info
2154	8.116416	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2155	8.116441	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=7
2156	8.116819	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2157	8.116826	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=8
2158	8.118055	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (application/x-j
2159	8.118063	192.168.0.2	189.31.124.90	TCP	43310 > http [ACK] Seq=2218 Ack=8
2160	8.128484	192.168.0.2	189.31.124.90	HTTP	GET /2626283/patro8cotas_195x31a.
2161	8.128955	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
2162	8.157910	192.168.0.2	189.31.124.90	TCP	43312 > http [ACK] Seq=2301 Ack=1
2163	8.158559	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (application/x-s
2164	8.158586	192.168.0.2	189.31.124.90	TCP	43312 > http [ACK] Seq=2301 Ack=1
...	...	...	...	...	...
3266	22.210811	192.168.0.2	189.31.124.90	HTTP	GET /2626283/pantene195x31.gif HT
3267	22.211280	189.31.124.90	192.168.0.2	TCP	http > 39632 [ACK] Seq=169312 Ack
3268	22.410253	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3269	22.410284	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3270	22.410652	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3271	22.410662	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3272	22.415952	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (GIF89a)
3273	22.415983	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4187 Ack=1
3274	22.885203	192.168.0.2	189.31.124.90	HTTP	GET /2626283/selo_88x31_mcdonalds
3275	22.885675	189.31.124.90	192.168.0.2	TCP	http > 39632 [ACK] Seq=172150 Ack
3276	22.886082	189.31.124.90	192.168.0.2	TCP	[TCP segment of a reassembled PDU
3277	22.886093	192.168.0.2	189.31.124.90	TCP	39632 > http [ACK] Seq=4569 Ack=1
3278	22.886099	189.31.124.90	192.168.0.2	HTTP	HTTP/1.0 200 OK (GIF89a)

Figura 2. Pacotes Capturados sem VPN

Com base na Figura – editada com a junção de duas, para que se possa ilustrar um maior número de informações – percebe-se que a quantidade de pacotes capturados é grande, todos trafegando entre o Servidor (189.31.124.90) e o Cliente (192.168.0.2).

A Figura 3 mostra o resultado da mesma consulta, desta vez passando por meio da Rede Privada Virtual, presente entre o Servidor e o Cliente remoto.

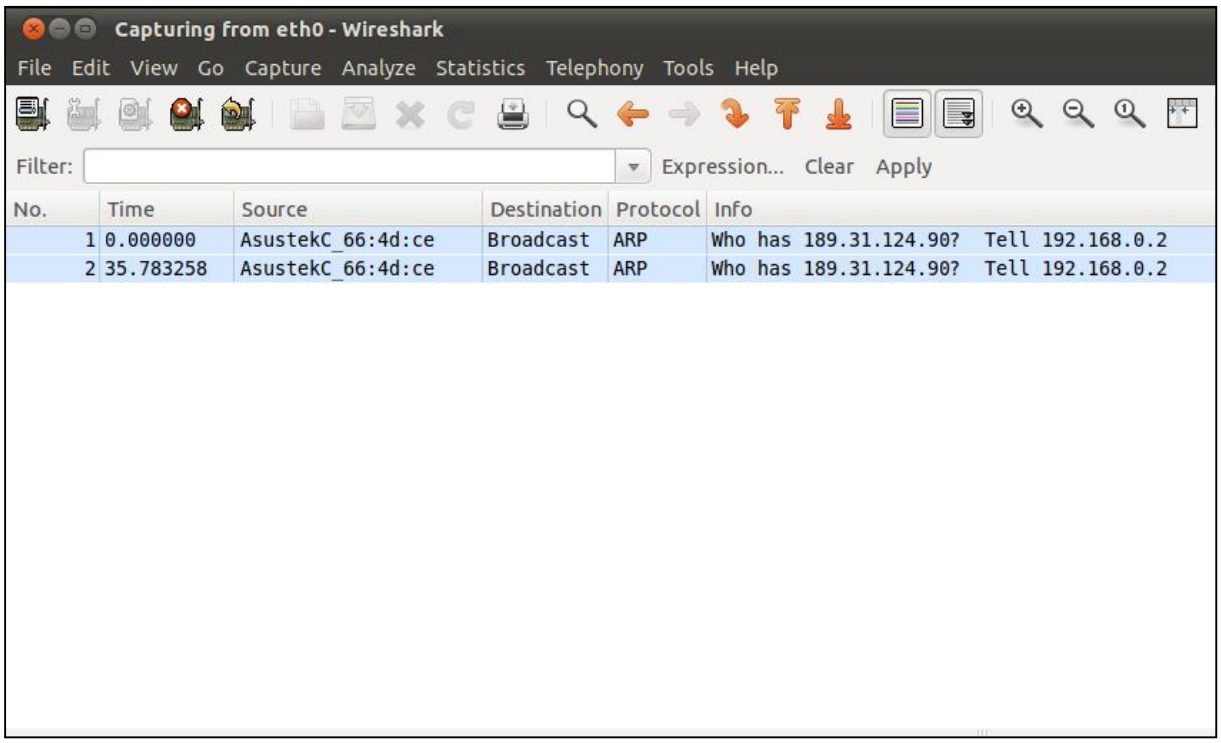


Figura 3. Pacotes Capturados com VPN

Percebe-se que, ao iniciar o túnel, nenhum pacote é capturado através do software – apenas os com destino ao *Broadcast*. Isto mostra que a VPN dificulta que o conteúdo trafegado entre os *hosts* nela conectados seja capturado por *sniffers*[13] ou usuários mal-intencionados, oferecendo a confidencialidade nas informações transmitidas, característica principal de uma Rede Privada Virtual.

7. Conclusão

De acordo com os estudos realizados, observou-se a importância da Internet na atualidade, principalmente no que diz respeito às redes públicas, utilizadas pela maior parte da população. As informações que nela trafegam correm risco de serem capturadas, analisadas e modificadas por pessoas mal-intencionadas, portanto, quanto maior segurança na transmissão, menor a perda da integridade, da confidencialidade e da autenticidade dos dados.

A partir da aplicação dos testes práticos de comunicação entre máquinas, com e sem configuração de diretivas de segurança, foram obtidos e apresentados resultados que comprovam a eficiência do IPSec. Se utilizado de forma correta, combinando os recursos de protocolos como o AH e o ESP, e outros existentes, dificultará consideravelmente que um invasor descubra algum ponto falho na conexão. Isto faz dele uma grande arma contra os vários tipos de ataques e invasões existentes, fornecendo boa segurança em redes IP, como a Internet.

[13] Ferramenta capaz de interceptar e registrar o tráfego de dados em uma rede de computadores, capturando, decodificando e analisando o conteúdo de cada pacote.

É importante destacar que somente a VPN e o IPSec não são suficientes para garantir a total segurança de uma rede. É essencial que, além de um planejamento envolvendo políticas rígidas de segurança, exista outras formas de proteção, como *firewalls* por exemplo.

Tanto o sistema operacional Linux quanto o Openswan apresentaram-se eficazes, se mostrando ferramentas atrativas para usuários que não disponibilizam de muitos recursos financeiros ou não pretendem gastar valores altos com tecnologias proprietárias. O Openswan foi capaz de implementar os protocolos do IPSec e fornecer características interessantes de segurança, como métodos de criptografia eficientes, suporte a múltiplos protocolos, suporte para gerenciamento de chaves, gerenciamento de endereços dos clientes e autenticação.

Os resultados obtidos por esta pesquisa foram satisfatórios, partindo do princípio de que não são necessários equipamentos complexos e caros, fazendo com que esta tecnologia possa ser empregada até mesmo em redes pequenas, como as residenciais. A tendência atual é que ela seja ainda mais utilizada com o desenvolvimento do acesso à Internet ADSL, tornando-se um atrativo tanto para as organizações pequenas, quanto para usuários comuns, que desejam ter uma base de dados remota e acessá-la de forma segura, independente do local em que esteja.

Partindo do princípio que a segurança do IPSec foi testada e comprovada nesta pesquisa, como sugestão para trabalhos futuros e também como forma de aprimorar os conhecimentos nesta tecnologia, pode-se criar uma aplicação que se conecte, por meio de uma VPN, a um banco de dados armazenado em um servidor, ligado à Internet por intermédio de um modem ADSL. Além disso, é possível realizar testes de desempenho[14], avaliando como um banco de dados remoto se comporta com as informações trafegando por meio do túnel, verificando se, além da segurança, o protocolo fornece o desempenho necessário para este tipo de atividade, tomando esse trabalho como subsídio para esta próxima pesquisa.

Referências

AGUIAR, Paulo Américo Freire. **Segurança em redes wi-fi.** Montes Claros: Universidade Estadual de Montes Claros, 2005.

ASSIS, João Mário de. **Implementando VPN em Linux.** Lavras: Universidade Federal de Lavras, 2003.

FAGUNDES, Bruno Alves. **Uma Implementação de VPN.** Petrópolis: Instituto Superior de Tecnologia em Ciências da Computação, 2007.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

FOROUZAN, Behrouz A.. **Protocolo TCP/IP.** 3. ed. São Paulo: Mcgraw-Hill Brasil, 2009.

[14] Para este teste, deve-se levar em conta outros fatores, como por exemplo, a largura de banda.

GODINHO, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady; BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: CEULP/ULBRA, 2005. Disponível em <http://lucaszc.homelinux.org/fic-pos/IPV6/IPv6.pdf>. Acesso em: 22 abr. 2011.

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; CORRÊA, Raimundo. **Segurança em Redes Privadas Virtuais – VPNs.** Rio de Janeiro: Brasport, 2006.

LIMA, Almir Wirth. **Redes de Computadores:** Tecnologia e Convergência de redes. Rio de Janeiro: Alta Books, 2009.

MURHAMMER, Martin W.; ATAKAN, Orcun; BRETZ, Stefan; PUGH, Larry R.; NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec, 2007.

NORTHCUTT, Stephen; ZELTSER, Lenny; WINTERS, Scott; FREDERICK, Karen Kent; RITCHEY, Ronald W. **Desvendando Segurança em Redes**: o guia definitivo para fortificação de perímetros de rede usando Firewalls, VPNs, roteadores e sistemas de detecção de invasores. Tradução: Daniel Vieira. Rio de Janeiro: Campus, 2002.
SILVA, Lino Sarlo da. **Virtual Private Network:** VPN. São Paulo: Novatec, 2003.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 1997.

TEIXEIRA, José Helvécio; SUAVÉ, Jacques Philippe; MOURA, José Antão Beltrão; TEIXEIRA, Suzana de Queiroz Ramos. **Redes de Computadores:** Serviços, Administração e Segurança. São Paulo: Makron Books, 1999.

THOMAS, Thomas M. **Segurança de Redes Primeiros Passos.** Rio de Janeiro: Ciência Moderna, 2007. Tradução: Flavio Morgado. Network Security First-step.

TORRES, Gabriel. **Redes de Computadores:** Curso Completo. Rio de Janeiro: Axcel Books, 2001.

VASQUES, Alan Tamer; SCHUBER, Rafael Priante. **Implementação de uma VPN em Linux utilizando o protocolo IPSec.** Belém: CESUPA, 2002.

WADLOW, Thomas A. **Segurança de redes:** projeto e gerenciamento de redes seguras. Tradução: Fábio Freitas da Silva. Rio de Janeiro: Campus, 2000.