UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

DANIEL AUGUSTO SIMÕES

IMPLEMENTANDO SEGURANÇA NAS REDES DE COMUNICAÇÃO ATRAVÉS DE VPN NA INTERNET: UM ESTUDO DE VIABILIDADE

MONOGRAFIA DE ESPECIALIZAÇAO

Curitiba – PR

2013

DANIEL AUGUSTO SIMÕES

IMPLEMENTANDO SEGURANÇA NAS REDES DE COMUNICAÇÃO ATRAVÉS DE VPN NA INTERNET: UM ESTUDO DE VIABILIDADE

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Teleinformática e Redes de Computadores, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Armando Rech Filho

Curitiba – PR

2013

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

IMPLEMENTANDO SEGURANÇA NAS REDES DE COMUNICAÇÃO ATRAVÉS DE VPN NA INTERNET: UM ESTUDO DE VIABILIDADE

por

Daniel Augusto Simões

Esta monografia foi apresentada às 20:00h do dia 12. de novembro de 2013 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 8,5 (OITO INTEIROS E CINCO DÉCIMOS).

Prof. Dr. Armando Rech Filho
(UTFPR)

Prof. Dr. Walter Godoy Júnior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

“Quero dedicar esse trabalho a minha esposa Ana e minhas filhas Eduarda e Manuela”

“Agradeço ao Prof. Dr. Armando Rech Filho que mesmo já atarefado aceitou ser orientador desta monografia e que com sua orientação e supervisão foi possível desenvolvê-la”

RESUMO

Este estudo tendo como objetivo mostrar a viabilidade da implementação de segurança nas redes de comunicação através de VPN, empenhou-se através de pesquisa bibliográfica e concluiu que a VPN apresenta grandes benefícios econômicos e técnicos aplicados aos dias de hoje. Sua parcela de contribuição no desenvolvimento de novas tecnologias e melhoramento do desempenho quanto à segurança na utilização da Internet para gerenciar organizações é fator primordial, sendo inúmeros os serviços oferecidos por ela. Quanto à segurança obtida pode-se constatar que os algoritmos de criptografia bem como os protocolos específicos geram grandes obstáculos aos invasores. A VPN atende as condições de segurança quanto à integridade, à confidencialidade das informações transmitidas, assim como a autenticação e o controle de acesso, permitindo maior confiança por parte das empresas que adotam esta solução. São, portanto, cada vez mais pesquisadas e incorporadas às organizações, sejam privadas ou governamentais, em diversos sistemas e ambientes computacionais.

Palavras chaves: criptografia, segurança, redes, VPN.

ABSTRACT

With the objective of demonstrating the feasibility of implementing VPN security in communication networks, this study used bibliographic research and concluded that VPN presents major economic and technical benefits applied nowadays. The share of its contributions in the development of new technologies and performance enhancement regarding security over the Internet as organization management tool with its innumerous services offered is a key factor. As for the security achieved, it was verified that the encryption algorithms as well as specific protocols generate major obstacle to invaders. VPN meets the criteria of security in relation to the integrity, confidentiality of information transmitted, as well as, authentication and access control, allowing greater trust on the part of companies that adopt this solution. They are therefore increasingly researched and adopted by corporations, whether private or governmental, in several systems and computing environments.

Words keys: encryption, security, network, VPN.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE SIGLAS

AC - *Autoridade Certificadora*

ACT - *Autoridade Certificadora do Tempo*

AES - *Advanced Encryption Standard*

AH - *Authentication Header*

AR - *Autoridade de Registro*

AS - *Security Association*

BGP - *Border Gateway Protocol*

BSoD - *Blue Screen of Death*

CBR - *Constraint-Based Routing*

CERT - *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança*

CHAP - *Challenge Handshake Authentication Protocol*

CIR - *Committed Information Rate*

CoS - *Class of Service*

CR-LDP - *Constrained-based Label Distribution Protocol*

DDoS - *Distributed Denial of Service Attack*

DES - *Data Encryption Standard*

DLP - *Discrete Logarithm Problem*

DMZ - *Demilitarized Zone*

DoS - *Denial of Service*

ECC - *Elliptic Curve Cryptography*

ECDLP - *Elliptic-Curve Discrete Logarithm Problem*

ESP - *Encapsulating Security Payload*

FIPS - *Federal Information Processing Standards Publication*

FTP - *File Transfer Protocol*

HTTP - *Hypertext Transfer Protocol*

ICMP - *Internet Control Message Protocol*

ICP - *Infraestrutura de Chaves Públicas*

IETF - *Internet Engineering Task Force*

IFP - *Integer Factorization Problem*

IP - *Internet Protocol*

CPE - *Customer-Provided Equipment*

IPSec - *Internet Protocol Security*

IPX - *Internetwork Packet Exchange*

ISDN - *Integrated Services Digital Network*

ISP - *Internet Service Provider*

ITI - *Instituto Nacional de Tecnologia da Informação*

L2F - *Layer 2 Forwarding*

L2TP - *Layer 2 Tunneling Protocol*

LAN - *Local Area Network*

LER - *Label Edge Router*

LSP - *Label Switch Path*

MAN - *Metropolitan Area Network*

MIT - *Massachusetts Institute of Technology*

MP- iBGP - *Multi-Protocol internal* BGP

MPLS - *Multi Protocol Label Switching*

MS-CHAP - *Microsoft Challenge Handshake Authentication Protocol*

MS-CHAPv2 - *Microsoft Challenge Handshake Authentication Protocol version 2*

NAT - *Network Address Translation*

NOS - *Network Operating System*

NSA - *National Security Agency*

OC - *Optical Carrier*

OSI - *International Organization for Standardization*

PC - *Personal Computer*

PPP - *Point-to-Point Protocol*

PPTP - *Point-to-Point Tunneling Protocol*

PVC - *Permanent Virtual Circuit*

QoS - *Quality of Service*

RADIUS - *Remote Authentication Dial-in User Service*

RSVP - TE - *Resource Reservation Protocol with Tunneling Extensions*

SLA - *Service Level Agreement*

SMTP - *Simple Mail Transfer Protocol*

SNA - Systems *Network* Architecture

SPI - *Security Parameter Index*

SVC - *Switched Virtual Circuit*

TCP - *Transmission Control Protocol*

TCP/IP - *Transmission Control Protocol / Internet Protocol*

TDM - *Time Division Multiplexing*

UDP - *User Datagrama Protocol*

VC - *Virtual Circuit*

VPN - *Virtual Private Network*

VRF - *Virtual Routing and Forwarding*

WAN - W*ide Area Network*

SUMÁRIO

1. INTRODUÇÃO

Atualmente, em função da necessidade crescente de estruturação dos sistemas existentes, conta-se com a possibilidade de administrar as organizações através das redes de computadores, uma vez que muitas Instituições possuem filiais em diferentes localizações, dificultando, portanto a propagação de dados e informações primordiais ao bom funcionamento das mesmas.

Neste cenário destaca-se que as redes de computadores apareceram da necessidade da troca de informações, onde se torna possível acessar dados que estão fisicamente distantes, porém, existe a necessidade de trocar informações de modo seguro, pois as informações são, em geral, consideradas confidenciais e sigilosas.

Assim, a Rede Virtual Privada ou Virtual Private Network (VPN) é uma das formas de interligar as redes das organizações, da qual pode-se usar a rede Internet[1] como *backbone*, tendo como característica principal a criação do que se denomina “túnel virtual” de comunicação, possibilitando a interligação das redes, de modo que os dados possam trafegar de modo seguro, o que significa utilizar a criptografia através dos túneis, aumentando a segurança na recepção de dados.

Logo se entendem relevantes três fatores fundamentais para a implantação da VPN: confidencialidade, integridade e autenticação. A confidencialidade refere-se a limitar o acesso a informações, geralmente através do uso de criptografia, já a integridade assegura que os dados não serão alterados durante uma transmissão, e por fim a autenticidade verifica se a pessoa com quem se está trocando informações sigilosas é realmente quem deveria ser.

No caso da utilização da rede pública Internet a motivação principal para a implementação de VPNs é financeira, de modo a despertar cada vez mais interesse nas organizações com filiais diversas, das quais necessitam de um meio econômico para troca de dados, incentivando-as a adotarem esta tecnologia, de maneira que a VPN apresenta a vantagem de expansão com um impacto financeiro menor sobre os

[1] O uso da Internet é uma motivação, mas a VPN pode ser implantada em qualquer tipo de rede onde se queira confidencialidade, integridade e autenticação dos usuários envolvidos na comunicação.

investimentos em infraestrutura extra, permitindo até mesmo suporte a usuários móveis, sem uso de modem ou servidores de acesso remoto, ajudando no tocante a flexibilidade com equipamentos periféricos.

Assim, este estudo objetiva efetuar uma análise bibliográfica acerca da implantação de Redes Virtuais Privadas, as chamadas redes VPN - Virtual Private Network, focando destacar sua viabilidade e segurança. Justificando-se na tentativa de levar tanto aos leitores desse estudo quanto a esse pesquisador mais esclarecimentos sobre a implantação da VPN e a segurança nas redes de comunicação.

Este trabalho tem como objetivo discutir a viabilidade da implementação de segurança nas redes de comunicação através de VPN.

Em relação aos objetivos específicos tem-se:

- Conceituar e analisar o contexto das redes privadas através da literatura cientifica;
- Destacar as vantagens e desvantagens de uma Rede VPN;
- Enumerar as possibilidades de viabilidade da implantação de segurança nas redes de comunicação através de VPN.

Em relação à metodologia este estudo não apresenta estudo de caso, resumindo-se a pesquisas bibliográficas que, no entanto, são mais vastas e aprofundadas possíveis, gerando um bom panorama para a discussão dos resultados coletados nesses estudos e assim alcançar o objetivo da presente pesquisa. A pesquisa pode ser caracterizada como exploratória porque visa entender o fenômeno das VPNs e como elas podem ser usadas para garantir a segurança na comunicação das redes corporativas.

O estudo divide-se em: introdução, com os parâmetros iniciais do trabalho; o segundo capítulo, teórico, versa um breve histórico sobre a origem das redes e da Internet; o terceiro capítulo aborda segurança de redes, o quarto capítulo dispõe sobre as VPNs; o quinto capítulo aborda certificação digital; o sexto capítulo discute as vantagens e desvantagens das VPNs; o sétimo capítulo trás uma análise das

principais tecnologias VPNs do mercado e o capítulo oito expõe alguns estudos práticos que demonstram as vantagens das VPNs.

2. BREVE HISTÓRICO SOBRE REDES E INTERNET

Inicia-se este trabalho com um breve histórico sobre o surgimento das redes de computadores e a Internet.

2.1 AS ORIGENS DAS REDES MODERNAS DE COMPUTADORES

Segundo Ciccarelli et al (2009), as redes modernas de computadores surgiram a partir do que foi chamado de “tradição dos computadores de grande porte” (mainframes). Muitos dos primeiros projetistas e desenvolvedores estavam acostumados com mainframes. Em um ambiente computacional tradicional de mainframes, como o mostrado na figura 1, terminais “burros” se conectam a um mainframe central. Um terminal burro é simplesmente um monitor e um teclado, de modo que todo o armazenamento, processamento e controle de dados acontecem no mainframe.

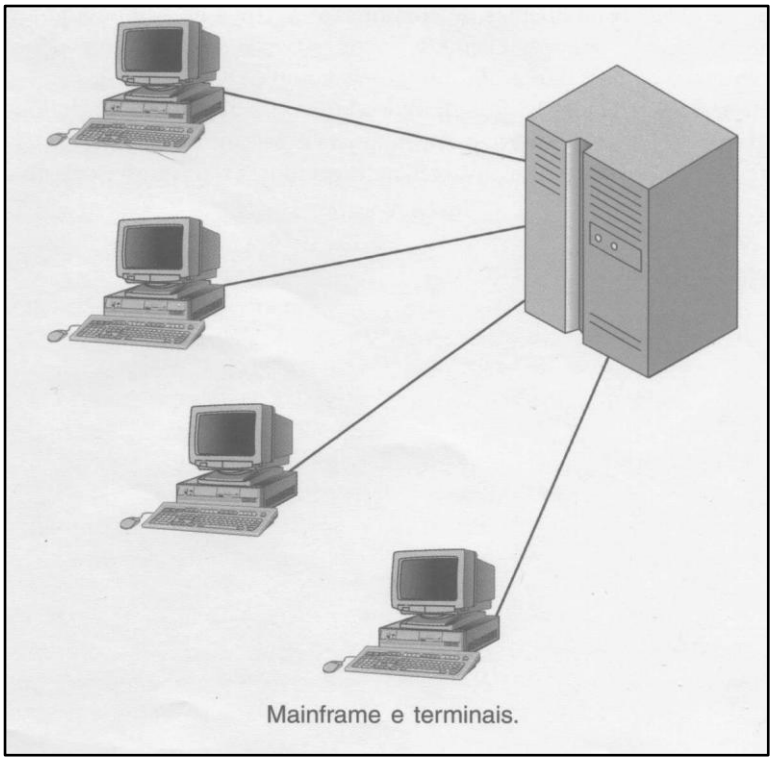

Figura 1 – Mainframe e Terminais
Fonte: Ciccarelli et al (2009).

Uma rede de computadores pessoais parece uma instalação mainframe com os computadores conectados eletronicamente. A maioria das redes tem um ou mais computadores especializados chamados servidores que oferecem recursos para a

rede, atuando mais ou menos como o mainframe central. A principal diferença é que os computadores são terminais inteligentes, com memória e processador integrados.

Os mainframes permitiram que os computadores deixassem de ser exclusividade dos governos, tornando-os acessíveis às empresas, embora só as maiores pudessem fazer uso deles.

O lançamento do PC causou uma revolução nas empresas e, mais tarde, nos domicílios. Os computadores se tornaram acessíveis às pequenas empresas e aos usuários individuais. Entretanto, profissionais da tecnologia da informação (TI) acostumados com mainframes identificaram alguns problemas. Os PCs (Personal Computers) representavam bolsões isolados de dados, dificultando o compartilhamento de dados por parte dos usuários. Também eram vistos como um possível risco de segurança, porque todos que tinham acesso físico a um computador tinham acesso aos dados.

As primeiras redes de PCs surgiram do desejo de resolver esses problemas, possibilitando o armazenamento compartilhado e, na maioria dos casos, centralizado, permitindo o compartilhamento de informações. A maioria também tinha segurança centralizada para limitar o acesso somente a pessoal autorizado.

Outro fator decisivo para a criação das redes foi que, antes das redes de PCs, qualquer solicitação de mudança, relatório, informação ou qualquer outra coisa relacionada a dados passava pelo centro de dados de TI. Frequentemente, os centros de dados demoravam em responder, não tinham os recursos necessários ou não estavam interessados em fazer mudanças para atender às solicitações dos usuários finais. Os PCs e as redes de PCs levaram os aplicativos para a mesa de trabalho e para o usuário individual e permitiram um grau de controle muito maior sobre os dados.

2.2 A ORIGEM DA INTERNET

A Internet desempenha um papel fundamental em muitas configurações de redes modernas. É considerada uma das invenções mais importantes da história dos sistemas de informações e de comunicações. É também um solo fértil para o projeto

e desenvolvimento de novas tecnologias de informações e comunicações; muitas inovações em redes de PCs surgiram diretamente da Internet.

A Internet foi criada pelo Departamento de Defesa dos EUA em 1969 como uma rede de quatro computadores chamada ARPANET. Em 1987, a Internet americana, junto com a equivalente canadense, era composta por cerca de 11.000 servidores. Medidas foram tomadas tanto nos EUA em 1988 quanto no Canadá em 1989 para implementar uma infraestrutura de alta velocidade para solucionar problemas de desempenho, e a Internet combinada dos EUA e Canadá alcançou a marca de 200.000 servidores no fim de 1989.

No inicio da década de 1990 quase todas as redes nacionais estavam conectadas entre si para formar uma rede global de redes. Cada uma dessas redes nacionais era diferente, com nomes, regras de acesso e tarifas próprias, mas todas usavam as mesmas normas que a Internet americana. Gradualmente, as distinções entre as redes nacionais começaram a desaparecer e o nome americano, Internet, começou a ser usado para denominar toda a rede global de redes conectadas à Internet americana. No fim de 1992, havia mais de um milhão de servidores na Internet.

Originalmente o tráfego comercial era proibido na Internet. No início da década de 1990 surgiram as redes comerciais, e novos serviços comerciais online começaram a oferecer acesso a qualquer pessoa disposta a pagar. A conexão à Internet global tornou-se um importante instrumento de marketing. O crescimento comercial rapidamente superou o uso tradicional da Internet pelo governo e pelas universidades. Em 1994, com mais de quatro milhões de servidores na Internet (a maioria deles comerciais), os governos norte-americano e canadense pararam de financiar os poucos circuitos que ainda estavam sob sua responsabilidade e os repassaram para firmas comerciais. A maioria dos outros países fez o mesmo pouco depois. Ninguém sabe exatamente que tamanho a Internet alcançou, mas as estimativas sugerem que mais de quinhentos milhões de computadores e um bilhão de pessoas têm acesso à Internet.

3. SEGURANÇA DE REDES

São discutidos nesta seção alguns aspectos que envolvem a segurança de redes, fundamentais para a construção de WANs VPNs seguras.

3.1 PRINCIPAIS METAS EM SEGURANÇA DE REDES

Para muitas pessoas, segurança significa evitar acessos não autorizados, como a invasão de um computador por um *hacker.* Segurança, porém, é muito mais que isso.

São três as principais metas para oferecer segurança em redes:

- Confidencialidade: é a proteção dos dados mantidos por uma organização para impedir a divulgação não autorizada de informações pessoais a respeito de clientes ou dados protegidos por lei;
- Integridade: é a garantia de que os dados não foram alterados nem apagados;
- Disponibilidade: é o funcionamento contínuo dos hardwares e softwares da organização para que empregados, clientes e fornecedores possam contar com um serviço sem interrupções.

Em geral as metas em relação a ameaças à segurança são garantir a continuidade dos negócios e evitar acessos não autorizados.

O plano de continuidade de negócios se refere principalmente a garantir disponibilidade, com alguns aspectos de integridade de dados. Um dos problemas são os contratempos, que são perdas ou reduções dos serviços da rede.

As interrupções podem ser breves e temporárias, afetando apenas alguns usuários. Podem ser causadas por falhas em dispositivos de rede, ou podem ser causadas devido à perda de dados. Um vírus, por exemplo, pode apagar arquivos indispensáveis.

Acessos não-autorizados estão relacionados principalmente à

confidencialidade, mas também têm a ver com a integridade, já que uma pessoa com acesso não autorizado pode alterar dados importantes.

Alguns acessos não-autorizados podem ser relativamente inócuos. Um intruso curioso pode explorar o sistema, descobrir coisas de pouco valor e talvez deixar um cartão de visitas. Um invasor mais grave pode ser um concorrente envolvido em espionagem industrial que tenta obter acesso a informações sobre produtos em desenvolvimento ou detalhes de uma proposta para um grande contrato. No pior dos cenários, um intruso pode alterar arquivos para cometer fraudes ou roubos ou apagar informações para lesar a organização.

3.2 IDENTIFICAÇÃO DE AMEAÇAS

Conforme Ciccarelli et al (2009) uma ameaça a uma rede de comunicação de dados é qualquer ocorrência potencialmente adversa que pode causar estragos, interromper os sistemas que usam a rede ou causar prejuízo monetário à organização. Uma vez identificadas as ameaças, elas podem ser classificadas de acordo com a probabilidade de ocorrência e os custos estimados.

As ameaças a um sistema de segurança computacional podem ser classificadas como ativas ou passivas. Conforme Torres (2001), ameaças ativas causam uma mudança não autorizada do estado de um sistema e as passivas não alteram o estado de um sistema. Inclui-se nesta categoria a escuta (*eavesdropping*), que envolve a escuta de mensagens trocadas. Uma contramedida para isso é a encriptação.

São apresentados a seguir alguns tipos de ameaças ativas:

- Mascaramento: personificação de um usuário autorizado de um sistema de modo a fazer uso não autorizado do mesmo;
- Modificação: modificação não autorizada de informação detida por um sistema ou trocada entre sistemas;
- Replay: a exata repetição de uma transação prévia, para uso não autorizado;

- Repúdio: um usuário autorizado negando envolvimento em uma transação prévia atribuída a este usuário;

- Negação de serviço: indisponibilidade de um serviço a um usuário autorizado.

Para Duffles e Moreira (2005) essas ameaças podem se manifestar na forma de ataques, fazendo-se necessário a utilização de mecanismos de segurança que forneçam ao sistema um ou mais serviços de segurança. Tais conceitos são apresentados a seguir:

- Ataque – qualquer ação que compromete a segurança da informação detida por uma organização;

- Mecanismo de segurança – mecanismo criado para detectar, prevenir ou remediar um ataque;

- Serviço de segurança – serviço que provê a segurança no processamento dos dados e na transferência de informações em uma organização. Os serviços devem combater ataques e fazem uso de um ou mais mecanismos de segurança.

Ferreira (2003) cita alguns serviços de segurança:

- Confidencialidade (privacidade ou sigilo): assegura que a informação armazenada ou transmitida está acessível apenas a partes autorizadas;

- Autenticidade: assegura que a origem de uma mensagem ou documento está corretamente identificada, sendo a identidade verdadeira;

- Integridade: assegura que qualquer modificação na informação pode ser feita apenas pelas partes autorizadas;

- Não-repúdio: previne que nem o remetente nem o destinatário da mensagem possam negar uma transmissão efetivamente realizada;

- Controle de acesso: requer que o acesso aos recursos de informação seja controlado pelo ou para o sistema;

- Disponibilidade: requer que os recursos estejam disponíveis às partes autorizadas quando necessário.

Segurança física provavelmente é o mecanismo de segurança em uso mais comum hoje. Compreendido por mecanismos de segurança que controlam acesso físico a sistemas reais. Por exemplo, fechaduras em portas, ou acesso restrito somente ao pessoal autorizado em salas de computadores. Porém, enquanto segurança física é um mecanismo essencial para a proteção de ativos físicos, tem aplicação limitada nas comunicações. Dutos de cabo lacrados podem estender segurança física para fora do ambiente da sala dos computadores, mas assim que haja uma necessidade de comunicação fora do perímetro protegido pela segurança física, outros mecanismos são necessários.

Funcionalidade de confiança é essencial em tais situações. Aqui são referidas as funções que restringem acesso à operação de um sistema a usuários autorizados, para tarefas autorizadas, e que são provados (através de avaliação) a executar esta tarefa (FERREIRA, 2003).

Funcionalidade de confiança é o mecanismo que impede atacantes de ganhar acesso e fazer uso de um sistema por enlaces de comunicação que são desprotegidos por medidas de segurança física. Isto requer mecanismos para identificar e autenticar usuários autorizados e proteger a integridade e confidencialidade de dados enquanto transitam sobre tais enlaces de comunicação.

Senhas podem prover meio de autenticar usuários autorizados. Porém, são facilmente registradas e reenviadas oferecendo assim só um impedimento limitado. Geralmente mecanismos de criptografia são aplicados. Estes podem prover confidencialidade, integridade, autenticação e são os únicos mecanismos que podem proteger dados em trânsito em enlaces de comunicação desprotegidos (DUFFLES; MOREIRA, 2005).

Nas páginas seguintes são apresentados dois gráficos que mostram dados recentes quanto ao numero de incidentes em redes no Brasil relatados ao CERT

(CERT, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) no período de abril a junho de 2013. O gráfico 1 mostra o total de incidentes e o gráfico 2 mostra um comparativo por tipos de ataque (CERT, 2013).

Descrição dos ataques mencionados pelo CERT:

- Dos (DoS, Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede;

- Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede;

- Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet;

- *Scan*: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;

- Fraude: esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem;

- Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

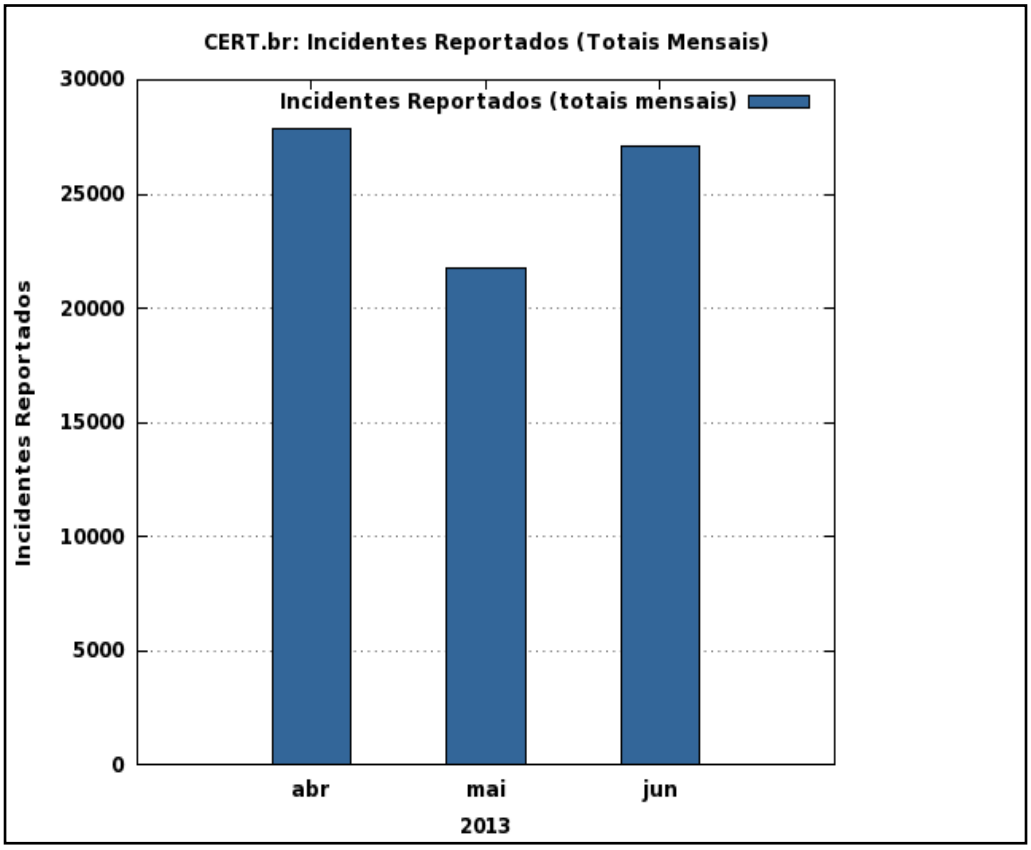

Gráfico 1 – Número de incidentes em redes de abril a junho de 2013

Fonte: CERT (2013).

O número total de notificações de incidentes no segundo trimestre de 2013 foi um pouco maior que 83 mil, o que corresponde a uma queda de 8% em relação ao trimestre anterior e a uma queda de 27% em relação ao mesmo trimestre de 2012 (CERT, 2013).

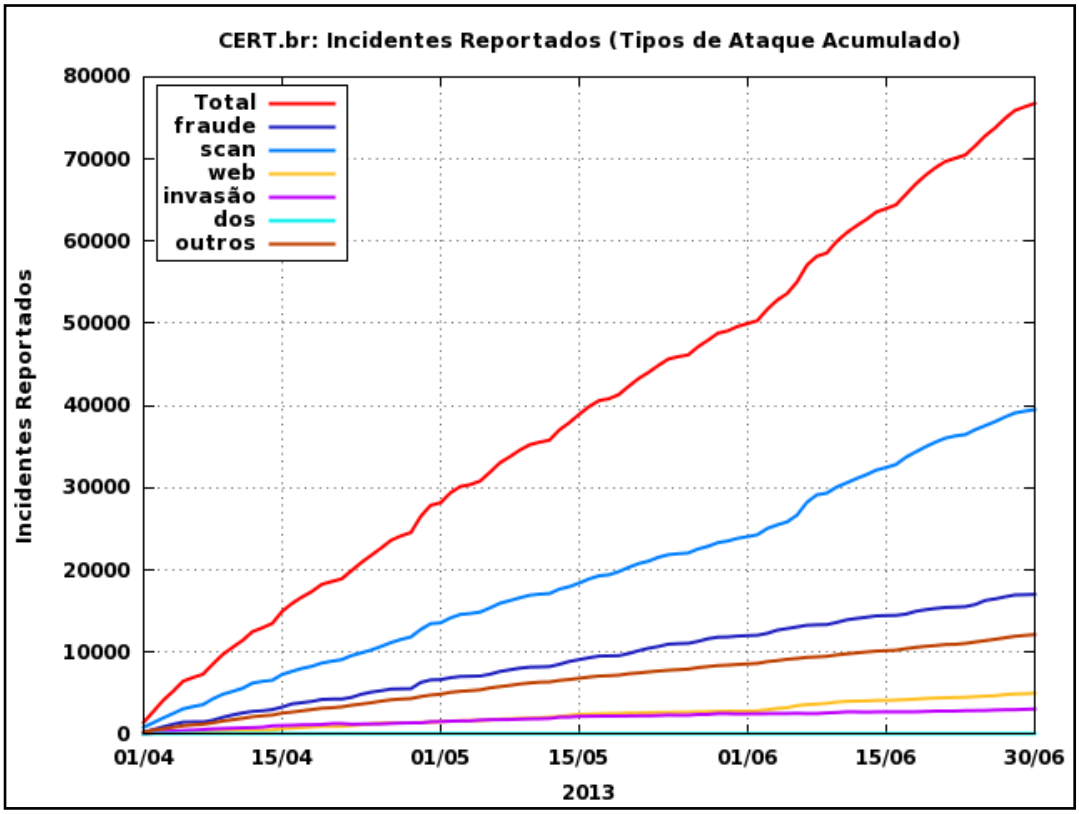

Gráfico 2 – Tipos de ataque em redes de abril a junho de 2013

Fonte: CERT (2013).

Abaixo segue uma análise de alguns fatos observados no período de abril a junho de 2013, agrupados em categorias distintas (CERT, 2013):

➢ Tentativas de Fraude:

- As notificações relacionadas a tentativas de fraudes totalizaram 17.014, praticamente o mesmo número de notificações do trimestre anterior 17.079. Com relação ao segundo trimestre de 2012, o número de notificações apresentou uma queda de 23%;

- Em relação ao primeiro trimestre de 2013, houve um aumento de quase 10% no número de notificações de páginas falsas de bancos e sites de comércio eletrônico (*phishing* clássico). Já em relação ao mesmo período de 2012, a queda foi de quase 13%. O *phishing* clássico continua representando mais da metade das notificações desta categoria;

- As notificações sobre Cavalos de Tróia, utilizados para furtar informações e credenciais, que representam quase 30% das notificações de tentativas de

fraudes, diminuíram 15% em relação ao primeiro trimestre de 2013 e 28% em relação ao segundo trimestre de 2012;

- No segundo trimestre, observa-se um crescimento de 3% no número de notificações de páginas falsas que não envolvem bancos ou comércio eletrônico, em relação ao primeiro trimestre de 2013. Já em comparação com o segundo trimestre de 2012 o número de notificações recebidas foi 74% menor.

➢ Varreduras e propagação de códigos maliciosos:

- As notificações referentes a varreduras reduziram 13% em relação ao trimestre anterior, mas o número de notificações foi praticamente idêntico ao do segundo trimestre de 2012;

- As notificações de varreduras SMTP (25/TCP) continuam em destaque, atingindo 34,5% do total, no trimestre anterior elas atingiram 46,8% do total. A maior parte das reclamações foram referentes a computadores de pequenas e médias empresas, possivelmente infectados, que tentaram identificar *relays* abertos fora do Brasil, com o intuito de posteriormente enviar spam;

- Os serviços que podem sofrer ataques de força bruta continuam sendo visados. RDP (3389/tcp) correspondeu a 19% das notificações de varreduras do segundo trimestre de 2013. O serviço SSH (22/TCP) ainda tem sido visado e correspondeu a 16% das notificações de varreduras. As varreduras visando os serviços TELNET (23/TCP) e FTP (21/TCP) apresentaram queda e corresponderam, respectivamente, a 1,75% e a menos de 1% das notificações de varreduras do segundo trimestre de 2013.

➢ Computadores comprometidos:

- No segundo trimestre de 2013 foram recebidos mais de 3.000 notificações de máquinas comprometidas. Este total foi 39% menor do que o número de notificações recebidas no primeiro trimestre de 2013, mas 172% maior que o número de notificações recebidas no segundo trimestre de 2012;

- A grande maioria das notificações de computadores comprometidos foi referente a servidores Web que tiveram suas páginas desfiguradas (*defacement*).

Analisando os dados fornecidos pelo CERT fica claro a importância da implementação de segurança em redes.

3.3 CONFIGURAÇÃO DE SEGURANÇA DE REDES

A segurança de uma rede envolve duas grandes áreas: a proteção da rede e a proteção dos computadores da rede. Essas duas áreas estão intimamente ligadas.

A primeira precaução é controlar o acesso à rede através de autenticação do usuário, permissões de acesso e atribuição de direitos. Outra precaução é controlar os computadores da rede para garantir que são seguros, o que às vezes significa adicionar programas especiais de segurança. Esse processo de tornar a rede e os computadores mais seguros é chamado de blindagem.

As medidas adotadas para tornar uma rede segura dependem das prioridades. O mais importante é manter a rede funcionando com eficiência? Nesse caso, pode ser aconselhável dividi-la em sub-redes ou configurar domínios de colisão. A preocupação principal é controlar a entrada ou saída de informações? Então, nesse caso convém instalar *firewalls*, que filtram o tráfego de rede com base em vários critérios. Existe um grande risco de que alguém intercepte os dados que trafegam pela rede? Já neste caso, então, pode ser necessário criptografar os dados.

3.4 TIPOS DE ATAQUES A REDES

Segue descrição de algumas técnicas utilizadas em invasões a redes. Os ataques descritos nesta seção têm como proposito levar ao leitor uma noção do funcionamento do mecanismo das técnicas de invasão. Porém, cabe pontuar, que técnicas já existentes são por vezes aperfeiçoadas e que novos métodos constantemente são criados.

Os ataques à rede realizados por um *hacker* são chamados de ataques diretos. Uma das primeiras “ferramentas” de ataque conhecidas foi o WinNuke**,** um programa de Windows que envia pacotes TCP/IP especiais com um cabeçalho TCP inválido. Computadores rodando Windows 95/98 e Windows NT/2000 travavam quando recebiam um desses pacotes por causa da forma como lidavam com dados inválidos no cabeçalho TCP. Em vez de retornar um código de erro ou rejeitar os dados inválidos (chamados de dados fora de faixa pela Microsoft), mandavam o computador para a tela azul da morte (BSoD, Blue Screen of Death), uma falha irrecuperável. Em sentido figurado, o *hacker* fazia o computador explodir (to *nuke* significa atacar com armas nucleares). *Patches* e pacotes de serviços para os produtos Microsoft suscetíveis combateram há muito tempo a ameaça que eram os dados fora de faixa, mas os *hackers* continuaram a refinar os ataques.

Falsificação de IP (IP, Internet Protocol) é o processo de enviar um pacote com um falso endereço de origem, fingindo que o pacote vem de dentro da rede que o *hacker* está tentando atacar. O endereço pode ser roubado da rede atacada pelo *hacker*. Um roteador (mesmo do tipo que filtra pacotes) trata o pacote como se viesse da rede e o deixa passar; um *firewall*, porém, pode evitar que este tipo de pacote entre na rede. A Figura 2 mostra um *hacker* tentando falsificar um IP. Note-se que o *hacker* com o endereço de IP falso tem o acesso à rede negado pelo *firewall*.

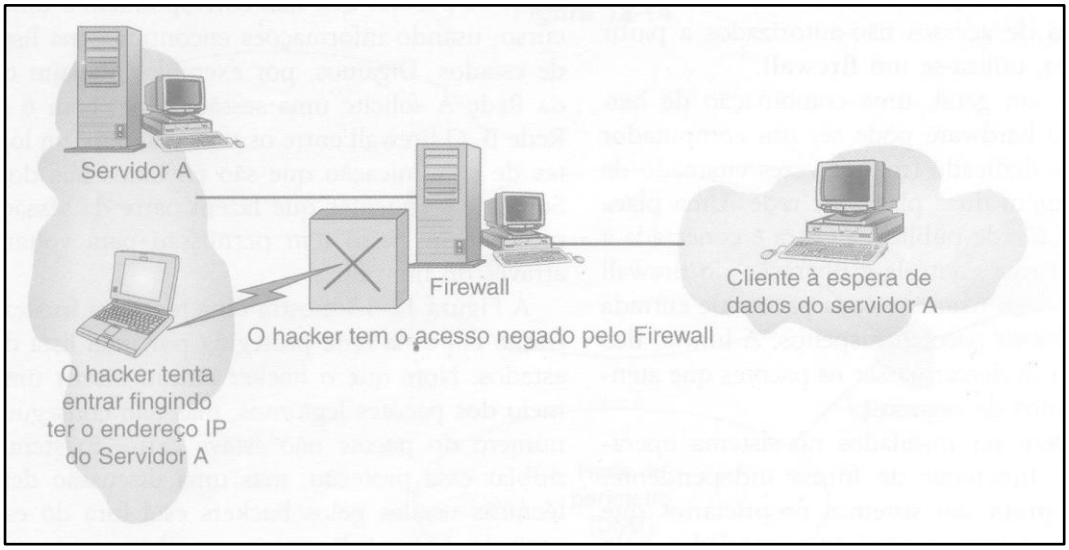

Figura 2 – Falsificação de IP

Fonte: Ciccarelli et al (2009).

O *ping* da morte é um tipo de ataque de negação de serviço (DoS, Denial of Service*).* Um ataque DoS impede que qualquer usuário, mesmo que legítimo, use o sistema. Geralmente, quando se faz um *ping* em um *host* remoto, quatro pacotes de protocolo de mensagens de controle da Internet (ICMP, Internet Control Message Protocol) de tamanho normal são enviados ao host remoto para verificar se está disponível. Em um ataque de *ping* da morte, um pacote ICMP muito grande é enviado para o *host* remoto, o que causa o estouro do buffer. Isso costuma causar uma reinicialização ou travamento do sistema. A maioria dos sistemas operacionais dispõe de *patches* que impedem que o *ping* da morte funcione.

A inundação SYN é outro ataque de DoS especializado. Nas comunicações normais, uma estação de trabalho que quer abrir uma comunicação TCP/IP com um servidor envia um pacote TCP/IP com a *flag* SYN ligada. O servidor responde automaticamente à solicitação, indicando que está pronto para iniciar as comunicações. Somente comunicações novas usam *flags* SYN, e um novo pacote SYN é usado somente se um usuário perde a conexão e precisa restabelecer as comunicações. Para iniciar uma inundação SYN, um *hacker* envia uma grande quantidade de pacotes SYN e o computador que os recebe tenta responder a cada solicitação SYN até que a máquina não consegue responder a nenhuma solicitação adicional porque os buffers estão cheios. A partir desse instante, passa a rejeitar todos os pacotes, incluindo as solicitações legítimas para uma conexão. Existem *patches* para vários NOSs que ajudam a resolver esse problema.

Existem também outros tipos de ataques DoS, nos quais um invasor tenta interromper a rede inundando-a de mensagens. A maioria dos invasores usa ferramentas que permitem adicionar endereços IP falsos às mensagens recebidas para que seja impossível descobrir rapidamente se a mensagem é real ou é uma mensagem DoS, o que dificulta a prevenção dos ataques.

O ataque de negação de serviço distribuído (DDoS, Distributed Denial of Service Attack) é ainda mais perigoso que um ataque DoS comum. Em um ataque DDoS, o agressor assume o controle de muitos computadores (milhares, às vezes) através da Internet e instala neles programas conhecidos como agentes DDoS. O invasor usa um software chamado manipulador DDoS para controlar os agentes, o manipulador dá instruções aos computadores controlados pelo invasor, que

começam a enviar mensagens simultaneamente para o alvo do ataque. Assim, o alvo é inundado por mensagens de muitas origens diferentes, o que dificulta a identificação das mensagens DoS e aumenta enormemente o número de mensagens que atingem o alvo.

É importante notar que um dos melhores meios de prevenir ataques a uma rede é saber o máximo possível a respeito dos ataques que podem ser desferidos contra essa rede em particular e seu sistema operacional. A pesquisa de vulnerabilidade, um termo que se refere ao processo de atualização para proteção contra ataques à rede, é uma tarefa permanente. Um *site* que pode ajudar é o SearchSecurity.com que dispõe de referências online e bancos de dados pesquisáveis com links para informações de segurança e utilitários. O *site* permite o acesso a ferramentas que ajudam a detectar, prevenir ataques dirigidos à rede e mesmo corrigir os danos produzidos por um ataque.

4. REDES PRIVADAS (VPN)

A ideia de empregar uma rede pública (Internet) em vez de linhas consideradas privativas para gerenciar redes corporativas é denominada de Virtual Private Network (VPN) ou ainda Rede Privada Virtual (ABREU, 2006).

4.1 DEFINIÇÕES

VPN denota, em português, Redes Privadas Virtuais, de forma que desmembrando este termo, pode-se destacar que Redes é uma infraestrutura por onde os computadores se comunicam; Privadas, devido essas redes empregarem recursos de criptografia para afiançar a segurança das informações navegadas pelo meio de comunicação e; Virtuais, porque depende de uma conexão virtual, temporária, sem presença física no meio. Essa conexão consiste na troca de pacotes, sendo roteados entre vários equipamentos.

Em outros termos VPNs são redes de computadores separadas fisicamente e, que através de um meio público de comunicação – ordinariamente a Internet – comunicam-se de modo seguro, através do emprego de criptografia.

Northcutt (2002) conceitua VPN como “uma sessão de rede protegida formada através de canais desprotegidos, como a Internet”.

Conforme Nakamura e Geus (2007 apud SANTOS, 2008) as redes virtuais privadas têm uma importância fundamental para as organizações, principalmente no seu aspecto econômico, ao permitirem que as conexões dedicadas sejam substituídas pelas conexões públicas. Além do que ocorre com as conexões privadas, também é possível obter economia com a substituição das estruturas de conexões remotas, que podem ser eliminadas em função da utilização dos clientes e provedores VPN.

Usando uma técnica chamada "tunelamento" (*tunneling*), os pacotes de dados são transmitidos através de uma rede pública roteada, Internet, em um túnel privado que simula uma conexão ponto-a-ponto. Um túnel pode ser começado, por exemplo, pelo notebook de um usuário final equipado com uma interface de comunicação para PC e o software Dial-Up de habilitação para VPN (CHIN, 2006).

Também pode ser inicializado em uma rede local (LAN) a partir de uma filial ou de casa (*home office*), através de um roteador extranet devidamente configurado para VPN, ou ainda através de um concentrador de acesso devidamente habilitado para VPN a contar de um ponto de presença (POP) de um provedor de serviços de rede. Um túnel pode ser finalizado por um terminador ou interruptor de túnel ou através de um *gateway* VPN em um roteador *extranet* de um provedor de serviços de rede (MORAES, 2004).

> As redes privadas virtuais ampliam os limites de um domínio protegido por meio da criptografia. Há três tipos de VPNs. O primeiro permite à filiais remotas compartilhar um perímetro de segurança e até mesmo um espaço de endereçamento. O segundo é utilizado por aquele que não quer abrir suas redes inteiras umas para as outras, mas desejam ter alguns serviços compartilhados - essas VPNs implementam uma DMZ. O terceiro tipo permite aos usuários remotos se conectarem a seu local de trabalho a partir de casa, do hotel ou café-bar. (CHESWICK 2003 apud SANTOS, 2008, p. 42).

As facilidades de VPN podem ser adicionadas a equipamentos de rede existentes através de software. Uma vez instaladas, as facilidades podem ser usadas para múltiplas aplicações VPN, cada qual implicando em significativa redução da relação custo/benefício (ABREU, 2006).

Um aspecto primordial que deve ser levado em consideração para o desenvolvimento de VPNs sobre a estrutura de rede pública já existente é a segurança.

Os protocolos TCP/IP (Transmission Control Protocol / Internet Protocol) e a própria Internet, não foram originalmente projetados tendo a segurança como prioridade, porque o número de usuários e os tipos de aplicações não requeriam maiores esforços para a garantia da mesma. Mas, se as VPNs são substitutos confiáveis para as linhas dedicadas e outros links de WAN, tecnologias capazes de garantir segurança e desempenho tiveram que ser acrescentadas à Internet. Os padrões para segurança de dados sobre redes IPs evoluíram de tal forma que permitiram a criação das VPNs.

As tecnologias que possibilitaram a criação de um meio seguro de comunicação dentro da Internet asseguram que uma VPN seja capaz de:

- Proteger a comunicação de escutas clandestinas - a privacidade ou proteção dos dados é conseguida pela criptografia que, através de transformações matemáticas complexas, codifica os pacotes originais, para depois, decodificá-los no final do túnel. Esta codificação é o aspecto mais difícil e crítico em sistemas que implementam a criptografia;

- Proteger os dados de alterações - esta proteção é alcançada através de transformações matemáticas chamadas de "*hashing functions*", as quais criam "impressões digitais" utilizadas para reconhecer os pacotes alterados;

- Proteger a rede contra intrusos - a autenticação dos usuários previne a entrada de elementos não autorizados. Vários sistemas baseados em senhas ou desafio de resposta, como o protocolo CHAP (Challenge Handshake Authentication Protocol) e o RADIUS (Remote Dial-in Service Protocol), assim como *tokens* baseados em hardware e certificados digitais, podem ser usados para a autenticação de usuários e para controlar o acesso dentro da rede.

Os aspectos mencionados nesta seção são discutidos nas próximas seções do trabalho.

4.2 CONSTITUIÇÃO DE UMA VPN

Uma VPN é constituída basicamente pelos seguintes elementos:

- Servidor VPN – responsável por aceitar as conexões dos clientes VPN. Esse servidor é o responsável por autenticar e prover as conexões da rede virtual aos clientes;

- Cliente VPN – é aquele que solicita ao servidor VPN uma conexão. Esse cliente pode ser um computador ou mesmo um roteador;

- Túnel – é o caminho por onde os dados passam pela rede pública. Comparando com as tecnologias orientadas à camada 2 (Enlace) do modelo OSI, um túnel é similar a uma sessão, onde as duas extremidades negociam

a configuração dos parâmetros para o estabelecimento do túnel, como endereçamento, criptografia e parâmetros de compressão;

- Protocolos de Tunelamento – São os responsáveis pelo gerenciamento e encapsulamento dos túneis criados na rede pública;
- Rede Pública – Efetua as conexões da VPN. Normalmente trata-se da rede de uma prestadora de serviços de telecomunicações.

4.3 TIPOS DE VPN

As VPNs são classificadas como sendo de quatro tipos, são elas:

4.3.1 VPN formada por circuitos virtuais discados

A implementação de um acesso discado VPN é semelhante a uma conexão *dial-up* entre dois computadores em localidades diferentes. A diferença é que os pacotes são transferidos por um túnel e não através da simples conexão discada convencional. Por exemplo, um usuário em trânsito conecta-se com um provedor Internet através da rede pública de telefonia (RTPC) e através dessa conexão estabelece um túnel com a rede remota, podendo transferir dados com segurança.

4.3.2 VPN formada por circuitos virtuais dedicados

O acesso por link dedicado, interligando dois pontos de uma rede, é conhecido como LAN-to-LAN. No link dedicado as redes são interligadas por túneis que passam pelo *backbone* da rede pública. Por exemplo, duas redes se interligam através de hosts com link dedicado, formando assim um túnel entre elas.

4.3.3 VPN utilizando a Internet

O acesso é proporcionado por um provedor de acesso à Internet (ISP, Internet Service Provider) conectado à rede pública. A partir de túneis que passam pela Internet, os pacotes são direcionados até o terminador do túnel em um nó da rede corporativa. Atualmente a maneira mais eficiente de conectar redes por meio da Internet é através de um link dedicado de acesso como o ADSL. Basta que as redes

disponham de uma conexão dedicada como esta para que a VPN possa ser montada.

4.3.4 VPN IP fornecida por um provedor com *backbone* IP

Existem alguns tipos de VPN IP disponibilizadas pelas próprias operadoras de serviços de telecomunicações. A diferença entre uma e outra está nos tipos de serviços disponibilizados para o usuário:

- VPN IP baseada na rede da operadora (network-based IP VPN): totalmente gerenciada pelo provedor de serviços. A tecnologia fica sob-responsabilidade da operadora. No cliente é instalado apenas um roteador e configurado o serviço;

- VPN IP com gestão de CPEs[2] (Managed CPE-based IP VPN): o provedor de serviços instala e gerencia os CPEs (Customer Premises Equipments) que são os elementos de rede que ficam nas instalações do cliente, além de todos os outros dispositivos de conectividade;

- VPN IP solução *in-house*: nesse caso a empresa adquire equipamentos de um fabricante e o link para a conectividade com a operadora, sendo de sua responsabilidade a implantação e o gerenciamento da VPN.

4.4 APLICAÇÔES VPN

Entre as aplicações VPNs, destacam-se três principais: Intranet VPN, Extranet VPN e Acesso Remoto VPN.

---

[2]CPE (Customer Premises Equipment) é um termo técnico muito utilizado por operadoras de telecomunicações e fornecedores de serviços de comunicação. Significa "equipamento dentro das instalações do cliente”. Qualquer equipamento que seja necessário para um cliente receber um serviço de comunicação é um CPE.

4.4.1 Intranet VPN

Uma *intranet* é uma rede privada (LAN) que se utiliza do modelo da Internet. Contudo, o acesso aos recursos fica limitado aos usuários internos a uma organização. A rede usa programas aplicativos definidos para a Internet global, tal como o HTTP (HTTP, Hypertext Transfer Protocol*)* e hospeda servidores Web, servidores de impressão, servidores de arquivos e assim por diante (Forouzan, 2006).

4.4.2 Extranet VPN

Uma *extranet* é essencialmente a mesma coisa que uma *intranet*, exceto pelo fato de que alguns recursos podem ser acessados por grupos específicos de usuários externos a uma organização, sob o controle do administrador da rede. Por exemplo, uma organização pode permitir aos consumidores acessarem as tabelas de produtos e realizarem pedidos de compra. Uma universidade ou faculdade pode permitir que estudantes localizados em outras cidades acessem o servidor de aplicações tornando possível o ambiente de educação a distância.

4.4.3 Acesso remoto VPN

Uma VPN de acesso remoto conecta uma empresa a seus empregados que estejam distantes fisicamente da rede. Neste caso, o usuário faz uma conexão discada para um provedor de serviços de Internet (ISP) ou um provedor de acesso à Internet, recebe autorização para utilizar a rede por esse provedor e recebe um endereço IP, válido e dinâmico, para trafegar. Por meio deste canal com a Internet é possível estabelecer uma VPN entre o usuário remoto e o *gateway* da VPN que protege uma filial ou empresa.

4.5 MODOS DE IMPLEMENTAÇÃO DE VPN

As VPNs podem ser implementadas das seguintes formas:

4.5.1 Modo transmissão

Somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes

específicos de hardware e software que trabalham em conjunto e que não oferecem flexibilidade para a escolha dos componentes (CUNHA, 2008);

4.5.2 Modo transporte

Somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes. É uma solução de segurança adequada, para implementações onde os dados trafegam somente entre dois nós da comunicação;

4.5.3 Modo túnel criptografado

Tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino;

4.5.4 Modo túnel não criptografado

Tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino. No entanto, cabeçalho e dados são mantidos tal como gerados na origem, não garantindo a privacidade;

4.5.5 VPN através da camada de enlace

As VPNs criadas através desta camada são uma analogia bastante próxima das redes privadas convencionais, pois os clientes da rede privada virtual têm a impressão de estarem conectados através de enlaces dedicados, quando na verdade são utilizados circuitos virtuais (ATM e Frame Relay) ou LSPs (MPLS).

4.6 ELEMENTOS COMPONENTES

Uma VPN tem como principais elementos: a encriptação dos dados, a integridade da mensagem, a autenticação das extremidades e o transporte subjacente (GOLDANI, 2004).

4.6.1 Confidencialidade dos dados

As informações trafegam em modo encriptado, gerando a ideia da criação de um túnel virtual, como mostra a Figura 3, onde os dados que estiverem trafegando pelo mesmo permanecem ininteligíveis para quem não fizer parte dele. Isto garante que, se a informação for capturada, será muito difícil entendê-la, a não ser que se descubra o método criptográfico e a chave utilizada (MORAES, 2004).

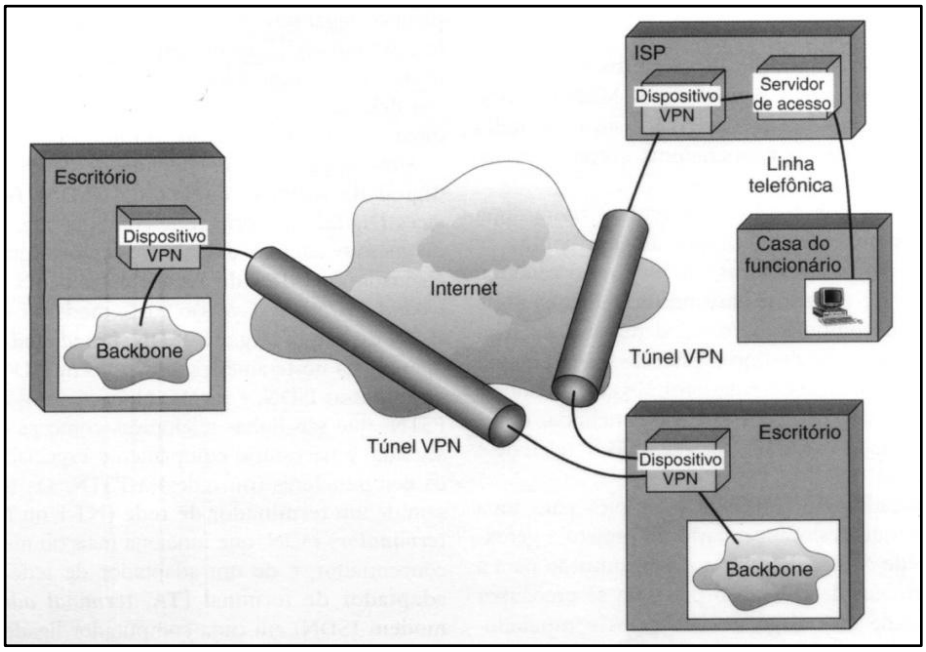

Figura 3 – Túnel Virtual
Fonte: Ciccarelli et al (2009).

4.6.2 Autenticação dos dados

Para verificar se os pacotes de dados chegaram inalterados, os sistemas VPN utilizam a função de *hash*. Esta função cria uma espécie de impressão digital do dado original, calculando um único número para a mensagem em questão, chamado de *hash*, formado por uma cadeia fixa ou variável de bits (MORAES, 2004). Desta forma, se alguma parte da mensagem for alterada durante a transmissão, o pacote é descartado (GOLDANI, 2004).

A autenticação dos usuários de uma VPN é baseada no IPSec (Internet Protocol Security), sendo que a autenticação do cliente e do servidor e a integridade e confidencialidade dos dados são providos por este protocolo e por algoritmos criptográficos agenciados pelo mesmo. Contudo, não se deve esquecer que o caso

de um protocolo ser devidamente seguro não afiança a segurança do sistema, já que esta segurança depende da implementação correta do protocolo. Muitos casos de erros em implementação que afetavam a segurança foram descobertos, especialmente em algoritmos criptográficos. Assim, uma falha na implementação do IPSec pode afetar o sistema, e deve ser examinado por meio de insistentes testes e análises de todas as probabilidades de conexões possíveis.

Destaca-se ainda que mesmo a implementação e o projeto do usuário VPN podem ainda ter problemas que comprometem a segurança.

4.7 PROTOCOLOS DE TUNELAMENTO

Para se estabelecer um túnel é necessário que as extremidades de uma conexão utilizem o mesmo protocolo de tunelamento. O tunelamento pode ocorrer na camada 2 ou 3 (respectivamente enlace e rede) do modelo de referência OSI (Open Systems Interconnection). São protocolos de tunelamento nível 2: o Protocolo ponto a ponto (PPTP, Point-to-Point Tunneling Protocol), o Protocolo de encaminhamento de camada 2 (L2F, Layer 2 Forwarding) e o Protocolo de tunelamento da camada 2 (L2TP, Layer 2 Tunneling Protocol). O IPSec (IPSec, Internet Protocol Security*)* é um protocolo de tunelamento de nível 3.

4.7.1 Protocolo de tunelamento PPTP

O PPTP é um protocolo criado pela Microsoft baseado em PPP, usado para criar conexões virtuais através da Internet usando TCP/IP e PPP.

Para usar PPTP, configura-se uma sessão PPP entre o cliente e o servidor, tipicamente através da Internet. Uma vez estabelecida a sessão, é criada uma sessão que se conecta através da sessão PPP existente usando PPTP. A sessão PPTP tunela através da conexão PPP existente, criando uma sessão segura.

Uma vantagem do PPTP é que ele é compatível com dispositivos NAT (NAT, Network Address Translation*),* e as principais desvantagens são:

- O processo de negociação dos parâmetros de conexão é feito com criptografia muito fraca;

- As mensagens do canal de controle são transmitidas sem qualquer forma de autenticação ou proteção de integridade;
- Não existe autenticação no período de negociação dos parâmetros da conexão;
- O PPTP não está disponível em todos os tipos de servidores;
- Não é uma norma totalmente aceita;
- Suporta somente autenticação do usuário (não suporta autenticação de máquina);
- O tunelamento pode reduzir a taxa de transferência.

A figura 4 mostra um exemplo de uma estação de trabalho configurada para se conectar à Internet através de um provedor de acesso usando o protocolo PPTP.

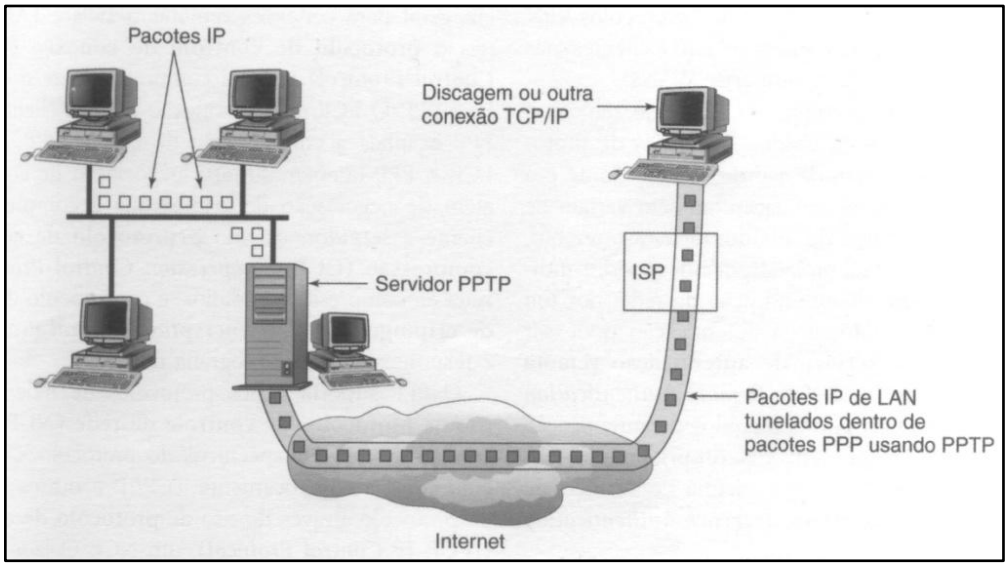

Figura 4 – Conexão usando PPTP
Fonte: Ciccarelli et al (2009).

4.7.2 Protocolo de tunelamento L2F

O Protocolo de Encaminhamento de Camada 2 (L2F), surgiu nos primeiros estágios da criação da tecnologia VPN e foi desenvolvido pela Cisco Systems. O L2F foi desenvolvido para criação de túneis, assim como foi o PPTP. O L2F usa o PPP para autenticação de usuários remotos, tal qual o PPTP. Uma grande diferença entre o PPTP e o L2F é a de que o L2F não possui tunelamento dependente do IP, sendo capaz de trabalhar diretamente com outros protocolos. Outra diferença com o

PPTP é a de que o L2F permite que os túneis possam dar conta de mais de uma conexão.

No L2F existem dois níveis de autenticação do usuário: uma antes do estabelecimento do túnel e outra quando a conexão é efetuada no *gateway* da corporação. Por ser o L2F um protocolo de camada 2, ele oferece, aos usuários, a mesma flexibilidade que o PPTP em lidar com outros protocolos diferentes do IP.Quando um usuário deseja se conectar ao *gateway* da corporação, ele primeiro estabelece uma conexão PPP com o NAS. A partir daí, o NAS estabelece um túnel L2F com o *gateway*. Finalmente, o *gateway* autentica o nome de usuário e senha do cliente, e estabelece a conexão PPP com o cliente.

4.7.3 Protocolo de tunelamento L2TP

Este é uma combinação das tecnologias Microsoft PPTP e Cisco encaminhamento de camada 2 (L2F, Layer 2 Forwarding*).* Suporta vários protocolos, entre eles IPX (IPX, Internetwork Packet Exchange*)* e AppleTalk. Isso lhe dá a vantagem de permitir que se conectem clientes não-TCP/IP em redes que rodam outros protocolos que não TCP/IP.

Este protocolo foi desenvolvido para suportar dois modos de tunelamento:

- Voluntário – é iniciado pelo computador remoto, sendo mais flexível para usuários em trânsito que podem discar para qualquer provedor de acesso, como o provedor não participa da criação dos túneis, este pode percorrer vários servidores sem precisar de uma configuração explicita;

- Compulsório – é criado automaticamente e iniciado pelo servidor de acesso a rede sob a conexão discada. Isto necessita que o servidor de acesso à rede seja pré-configurado para saber a terminação de cada túnel baseado nas informações de autenticação de usuário.

Algumas vantagens do L2TP:

- É um protocolo padrão da indústria, o que significa que tem amplo suporte;

- Pode autenticar tanto o servidor quanto o cliente usando certificados (um método de definir segurança compartilhada) ou uma chave pré-compartilhada (um valor conhecido pelo servidor e pelo cliente);
- Suporta métodos de autenticação mais rigorosos que o PPTP.

Algumas desvantagens do L2TP:

- Não é compatível com alguns dispositivos NAT (NAT, Network Address Translation*).* O NAT do Windows Server 2003, porém, é suportado;
- O tunelamento pode reduzir a taxa de transferência.

A segurança para o L2TP é fornecida através da segurança do protocolo Internet (IPsec, Internet Protocol Security).

4.7.4 Protocolo IPSec

O IP Security (IPSec) é uma coleção de protocolos desenvolvidos pelo IETF (IETF, Internet Engineering Task Force), RFCs 4301, 4302 e 4303, para fornecer segurança para um pacote de camada IP. O IPSec não define o uso de nenhuma técnica de cifragem ou método de autenticação. Na verdade, ele fornece uma estrutura e um mecanismo; ele deixa a escolha do tipo de cifragem, autenticação e métodos de *hashing* para o usuário (FOROUZAN, 2006).

O IPSec requer uma conexão lógica entre dois *hosts* usando um protocolo de sinalização, chamado Security Association (AS). Em outras palavras, o IPSec precisa que o protocolo sem conexão IP seja modificado para um protocolo orientado à conexão antes da segurança ser implementada afetivamente.

Uma conexão AS é uma conexão *simplex* (unidirecional) entre a fonte e o destino. Assim, se houver necessidade de estabelecer conexão *full-duplex* (bidirecional) serão necessárias duas conexões AS, uma em cada direção.

Uma conexão AS é definida unicamente através de três elementos:

1. Um SPI (Security Parameter Index) de 32 bits age como um identificador de circuito virtual em protocolos orientados à conexão, como o Frame Relay e o ATM;

2. O tipo de protocolo usado para a segurança. O IPSec define dois protocolos alternativos: AH e ESP;

3. A origem do endereço IP.

O IPSec opera em dois modos diferentes, a saber: modo de transporte e modo de tunelamento. O modo define onde o cabeçalho IPSec será adicionado ao pacote IP.

- Modo de Transporte:

Neste modo, o cabeçalho IPSec é adicionado entre o cabeçalho IP e o restante do pacote, conforme a figura 5.

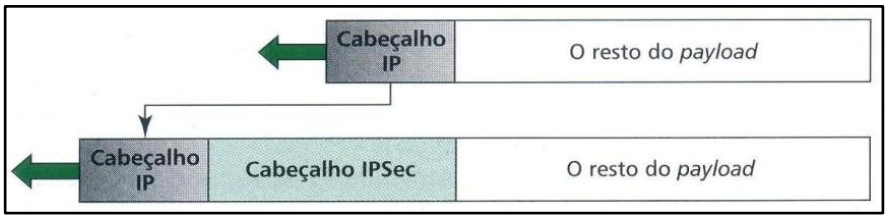

Figura 5 – Modo de transporte
Fonte: Forouzan (2006).

- Modo de Tunelamento:

Neste modo, o cabeçalho IPSec é colocado logo à frente do cabeçalho IP original. Um novo cabeçalho IP é adicionado na frente do cabeçalho IPSec. O cabeçalho IP original e o restante do pacote são tratados como *payload* no modo de tunelamento. A figura 6 mostra o pacote IP original e o novo pacote IP.

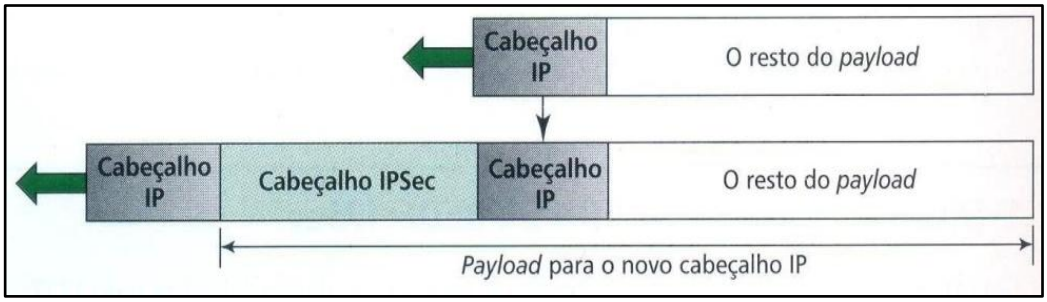

Figura 6 – Modo de tunelamento
Fonte: Forouzan (2006).

O IPSec define dois protocolos de segurança: Authentication Header (AH) e Encapsulating Security Payload (ESP). Analisam-se estes a seguir:

- AH – (Authentication Header):

O protocolo AH foi desenvolvido para autenticar o *host* de origem e assegurar a integridade do *payload* transportado pelo pacote IP dele. O protocolo calcula a síntese da mensagem, usando uma função de *hashing* e uma chave simétrica, e insere a síntese no cabeçalho do protocolo AH. O AH é colocado na posição correta no datagrama IP baseado no modo de operação (transporte ou tunelamento). A figura 7 ilustra os campos e a posição do protocolo AH no modo de transporte.

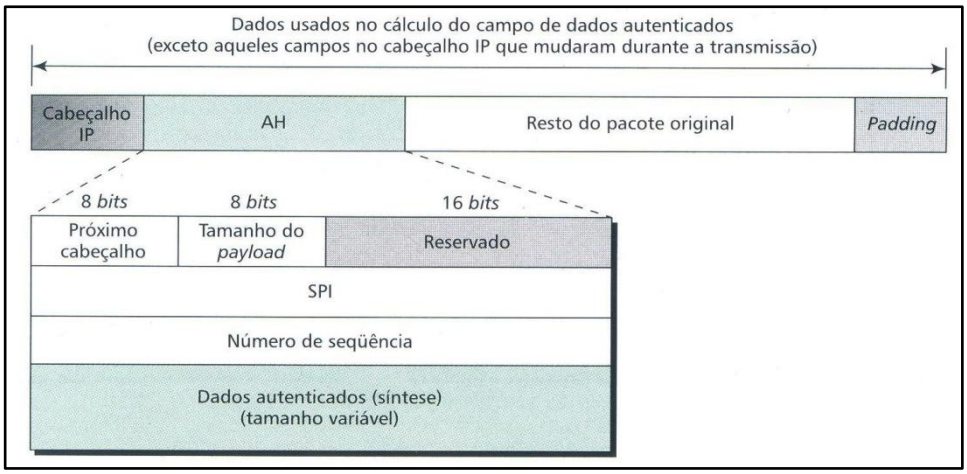

Figura 7 – Authentication Header
Fonte: Forouzan (2006).

Quando um datagrama IP transporta um AH, o valor original no campo protocolo do cabeçalho IP é substituído pelo valor 51. Um campo interno ao

protocolo AH (campo próximo cabeçalho) define o valor original do campo protocolo (o tipo de *payload* sendo transportado pelo datagrama IP).

Para agregar o protocolo AH ao datagrama IP é necessário seguir as seguintes etapas:

1. O protocolo AH é adicionado ao campo *payload* juntamente com o campo de dados autenticando todo configurado em zero;

2. Pode ser necessário adicionar *padding* (bits de enchimento) para tornar o tamanho total do pacote par, caso algum algoritmo de *hashing* particular exija isto;

3. A função de *hashing* é baseada no tamanho do pacote total. Entretanto, somente os campos do cabeçalho IP que não sofreram modificações durante a transmissão serão incluídos no calculo da síntese da mensagem (autenticação dos dados);

4. A autenticação dos dados está incluída no protocolo AH;

5. O cabeçalho IP é adicionado ao pacote após a troca do valor do campo protocolo para 51.

O protocolo AH é uma fonte de autenticação e integridade de dados, mas não oferece privacidade.

- ESP – (Encapsulating Security Payload*):*

O protocolo AH não suporta privacidade. A versão IPSec posterior definiu um protocolo ESP (Encapsulating Security Payload) alternativo fornecendo autenticação, integridade e privacidade da informação. O ESP adicionou um cabeçalho e um rótulo (*trailer*) ao datagrama IP original. Observe que os dados autenticados via ESP são adicionados ao final do pacote, o que torna o seu cálculo mais simples. A figura 8 mostra a localização do cabeçalho e *trailer* ESP.

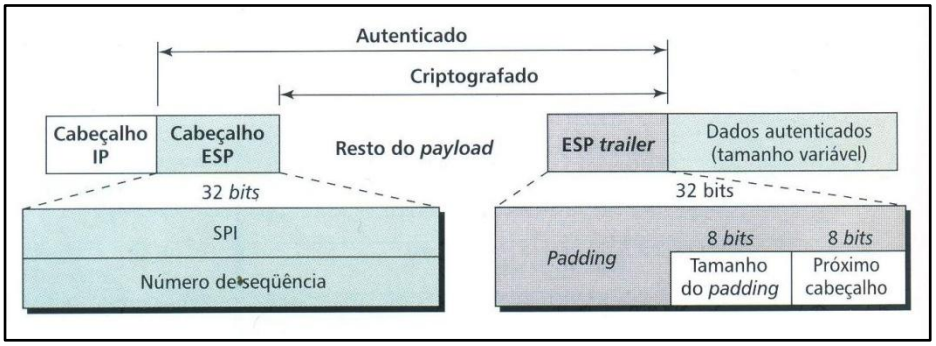

Figura 8 – Cabeçalho *e Trailer* ESP
Fonte: Forouzan (2006).

O procedimento ESP segue as seguintes etapas:

1. Um *trailer* ESP é adicionado ao *payload*;
2. O *payload* e o *trailer* são criptografados;
3. O cabeçalho ESP é adicionado ao *payload*;
4. O cabeçalho ESP, o *payload* restante e um trailer ESP são usados para gerar dados autenticados;
5. Os dados autenticados são agregados ao final do *trailer* ESP;
6. O cabeçalho IP é adicionado após a mudança do valor do protocolo para 50.

O protocolo ESP fornece autenticação, integridade e privacidade à informação.

O IPSec suporta tanto a versão IPv4 quanto a versão IPv6. Entretanto, na versão IPv6 ambos protocolos (AH e ESP) são parte do cabeçalho estendido.

O protocolo ESP foi desenvolvido depois do protocolo AH estar em pleno uso, o ESP tem tudo que o protocolo AH incorpora, agregando mais uma funcionalidade: a privacidade. Então, a questão é: por que é necessário o protocolo AH? A resposta é que apesar do ESP ter como adicional a função de privacidade o AH é ainda uma opção válida, pois pode-se querer integridade e autenticação mas não necessariamente privacidade.

4.8 SEGURANÇA DA INFORMAÇÃO EM REDES VPN

São apresentados nesta seção alguns aspectos relacionados com segurança da informação em redes VPN.

4.8.1 *Firewalls*

Quando uma rede privada, na qual somente usuários autorizados têm acesso aos dados, é conectada a uma rede pública, na qual todos que estão conectados têm acesso aos dados, a possibilidade de invasão aumenta. Para proteger a rede privada de acessos não autorizados a partir de uma rede pública, utiliza-se um *firewall*.

Os *firewalls* são, em geral, uma combinação de hardware e software. O hardware pode ser um computador ou um equipamento dedicado (muitas vezes chamado de caixa-preta) que contém duas placas de rede. Uma placa de rede é conectada à rede pública; a outra é conectada à rede privada. O software controla a operação do *firewall* e protege a rede privada. Examina cada pacote de entrada e saída e rejeita todos os pacotes suspeitos. A função dos *firewalls*, em geral, é só deixar passar os pacotes que atendem a certos requisitos de segurança.

Os *firewalls* podem ser instalados no sistema operacional existente ou funcionar de forma independente. Os sistemas caixa-preta são sistemas proprietários que possuem controles externos e não são controlados pelo sistema operacional.

Uma característica importante dos *firewalls* é a filtragem de pacotes, que é a capacidade de um roteador ou de um *firewall* de descartar pacotes que não atendem a certos critérios. Outra é a filtragem de portas, que envolve o bloqueio ou a liberação da passagem de pacotes com base no endereço de porta.

Muitos *firewalls* usam a filtragem dinâmica de pacotes para garantir que os pacotes encaminhados pertencem a sessões iniciadas no lado privado. Uma lista dinâmica de estados (também chamada de tabela de estados) mantida no *firewall* contém um registro de todas as sessões de comunicações entre estações de trabalho dentro e fora do *firewall*. Essa lista é alterada sempre que uma sessão de

comunicação é iniciada ou terminada. As listas dinâmicas de estados permitem que um *firewall* filtre pacotes dinamicamente. Na filtragem dinâmica de pacotes, somente pacotes associados a sessões de comunicações em curso (e válidas) recebem permissão para passar.

Os *firewalls* frequentemente são configurados como parte de uma zona desmilitarizada (DMZ, Demilitarized Zone*),* também chamada de rede de perímetro, que é uma área protegida por um ou dois *firewalls*. Quando usado na *intranet* para isolar um segmento, essa área é chamada de sub-rede filtrada.

O quadro 1 descreve três tipos comuns de *firewalls,* suas vantagens e desvantagens.

Método	**Descrição**	**Vantagens**	**Desvantagens**
Nat	Tradução do endereço da rede (*Network Address Translation*) insere sub-redes IP privadas atrás de um ou um pequeno grupo de endereços IP públicos, mascarando todos os pedidos para uma fonte ao invés de várias.	Pode ser configurado transparentemente para máquinas em uma LAN. A proteção de muitas máquinas e serviços por trás de um ou mais endereços IP externos simplifica as tarefas de administração. A restrição de acesso do usuário de e para uma LAN pode ser configurada abrindo e fechando portas no firewall/gateway do NAT.	Não pode evitar atividades mal intencionadas depois de usuários se conectarem a um serviço fora do firewall.
Filtro de Pacotes	Lê cada pacote de dados que passa por dentro e por fora de uma LAN. Pode ler e processar pacotes pela informação do cabeçalho e filtrar o pacote baseado em conjuntos de regras programáveis implementadas pelo administrador do firewall.	Não requer nenhuma personalização no lado do cliente, já que todas as atividades da rede são filtradas no nível do roteador ao invés do nível da aplicação. Como os pacotes não são transmitidos através de um proxy, o desempenho da rede é mais rápido devido à conexão direta do cliente para host remoto.	Não é possível filtrar pacotes para *firewalls* de proxy de conteúdo. Processa pacotes na camada de protocolos, mas não pode filtrar pacotes na camada do aplicativo. Arquiteturas de rede complexas podem dificultar o estabelecimento de regras de filtragem de pacotes, especialmente se for usado com o mascaramento do IP ou sub-redes locais e redes DMZ.

Proxy	Filtram todos os pedidos de um determinado protocolo ou tipo de clientes LAN para uma máquina proxy, que então faz estes pedidos à Internet representando o cliente local. Uma máquina proxy age como um buffer entre os usuários remotos mal-intencionados e as máquinas clientes de redes internas.	Fornece aos administradores controle sobre quais aplicativos e protocolos funcionam fora da LAN. Alguns servidores proxy podem armazenar dados frequentemente acessados no cache localmente, ao invés de ter que usar a conexão Internet para solicitá-los, o que é conveniente para reduzir o consumo de banda larga. Os serviços proxy podem ser autenticados e monitorados de, permitindo um controle maior do uso de recursos na rede.	Proxies são frequentemente específicos às aplicações (HTTP, Telnet, etc.) ou restritos a protocolos (a maioria dos proxies funciona com serviços conectados por TCP). Serviços de aplicação não podem rodar por trás de um proxy, portanto seus servidores de aplicações devem usar uma forma separada de segurança de rede. Proxies podem se tornar um gargalo na rede, já que todos os pedidos e transmissões passam através de uma mesma fonte ao invés de passar diretamente do cliente para um serviço remoto.

Quadro 1 – **Comparativo entre tipos de *firewalls***

Fonte: Red Hat (2013).

Existem dois métodos de utilização de um *firewall* com um servidor VPN (Microsoft, 2013). São eles:

- Servidor VPN à frente do *firewall* – neste o servidor VPN está conectado à Internet e o *firewall* fica situado entre o servidor VPN e a *intranet*.

- Servidor VPN atrás do *firewall* – neste o *firewall* está conectado à Internet e o servidor VPN fica situado entre o *firewall* e a *intranet*.

Estes dois métodos são descritos a seguir:

- Servidor VPN à frente do *firewall* - quando o servidor VPN estiver situado à frente do *firewall* e conectado à Internet, será preciso adicionar filtros de pacotes à interface da Internet que permitam somente a passagem do tráfego VPN de ida e volta do endereço IP da interface da Internet do servidor VPN. No caso do tráfego de entrada, quando os dados encapsulados são descriptografados pelo servidor VPN, eles são encaminhados para o *firewall*. Com o uso de filtros, o *firewall* permite que o tráfego seja encaminhado para recursos da intranet. Como o único tráfego

que atravessa o servidor VPN é gerado por clientes VPN autenticados, nessa situação, a filtragem do *firewall* pode ser utilizada para impedir que usuários VPN acessem recursos específicos da intranet. Como o único tráfego de Internet permitido na *intranet* deve passar pelo servidor VPN, esse método também impede o compartilhamento de FTP (FTP, File Transfer Protocol) e de recursos da Web na intranet com usuários da Internet de fora da VPN. A figura 9 mostra o servidor VPN à frente do firewall.

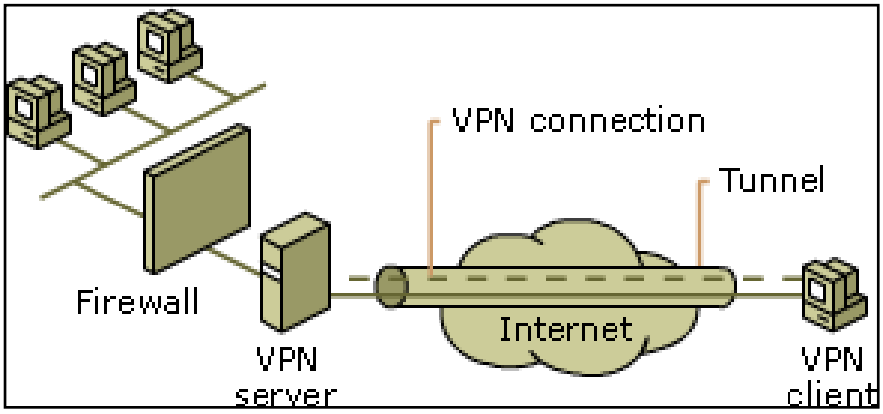

Figura 9 – Servidor VPN à frente do firewall
Fonte: Microsoft (2013).

- Servidor VPN atrás do *firewall* - Em uma configuração mais comum, o *firewall* fica conectado à Internet, e o servidor VPN é um recurso da *intranet* conectado à Rede de Perímetro. O servidor VPN dispõe de uma interface tanto na rede de perímetro quanto na *intranet*. Nessa situação, o *firewall* deve ser configurado com filtros de entrada e saída na interface da Internet que permitam a passagem do tráfego de manutenção de encapsulamento e dos dados encapsulados para o servidor VPN. Filtros adicionais podem permitir a passagem do tráfego para servidores Web, FTP e de outros tipos na rede de perímetro. Para obter uma camada de segurança adicional, o servidor VPN também poderá ser configurado com filtros de pacotes PPTP ou L2TP/IPSec na interface da rede de perímetro.Como o *firewall* não dispõe das chaves de criptografia para cada conexão VPN, ele só poderá filtrar os cabeçalhos em texto simples dos dados encapsulados. Em outras palavras, todos os dados encapsulados passam pelo *firewall*. Isso, entretanto, não representa um risco de segurança, pois a conexão VPN exige um processo

de autenticação que impede o acesso não autorizado posterior ao servidor VPN. A figura 10 mostra o servidor VPN atrás do *firewall* na rede de perímetro.

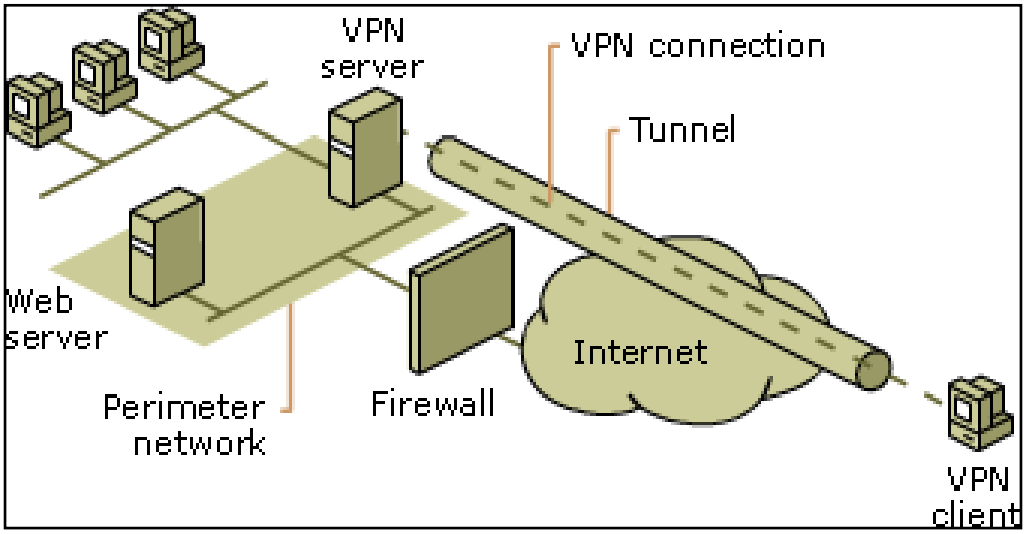

Figura 10 – servidor VPN atrás do firewall

Fonte: Microsoft (2013).

4.8.2 Criptografia

Criptografia é o processo de codificar dados, e descriptografia é o processo de decodificar dados criptografados. Dados criptografados são enviados através de uma rede e descriptografados pelo destinatário. Em termos gerais, a criptografia consiste em aplicar aos dados (representados como números) uma fórmula ou algoritmo de criptografia (que utiliza um parâmetro conhecido como chave), usado para criptografar e descriptografar os dados. Como a NSA (NSA, National Security Agency*)* classifica as ferramentas e fórmulas de criptografia como armas de guerra desde 1979, é responsável por sua regulamentação. A NSA não quer que países hostis, terroristas e criminosos usem comunicações em código para planejar crimes sem serem descobertos.

Um meio de avaliar um algoritmo de criptografia é por meio da força de criptografia (ou seja, pelo tamanho da chave). Até 1998, o governo dos Estados Unidos só permitia a exportação de softwares com criptografia de 40 bits ou menos, esse limite foi aumentado para criptografia de 56 bits e depois criptografia de 128 bits com permissão especial do Departamento de Comércio dos EUA.

Em redes internas, alguma criptografia é necessária, como, por exemplo, quando há necessidade de acessar um servidor seguro. Isso pode ser feito automaticamente por muitos NOSs e usada por muitos sistemas de e-mail, o que proporciona aos usuários a opção de criptografar algumas ou todas as suas mensagens de e-mail. Pacotes de programas de outros fabricantes podem ser usados para criptografar as mensagens de sistemas de e-mail que não oferecem essa opção. A criptografia também costuma ser usada para transmitir dados por VPN para manter o sigilo dos dados ao usar a Internet para conectar de forma segura usuários remotos a redes internas. Finalmente, a criptografia ganhou importância com o uso da Internet para compras, transações bancárias e investimentos. Comprar produtos e realizar operações financeiras online não seria possível se os dados trocados pelos participantes através da Internet não fossem criptografados.

O processo de criptografia envolve a comparação de cada caractere dos dados com uma chave. Assim, por exemplo, é possível criptografar de muitas formas diferentes a seguinte frase: Quem Cala Consente.

Para fins ilustrativos, é usado um código simples de substituição. Nesse método, cada letra do alfabeto corresponde a um número diferente. Usando uma correspondência direta entre letras e números (A=l, B=2, C = 3 e assim por diante, por exemplo), obtemos a seguinte sequência numérica: {16 20 5 12 3 1 11 1 3 14 13 18 5 13 19 5}. Essa série de números pode ser transmitida através de uma rede, e o destinatário pode descriptografar a mensagem usando a mesma chave no sentido inverso. Da esquerda para a direita, o número 16 se transforma na letra Q, o 20 em U, o 5 em E e assim por diante. No fim do processo, o destinatário recupera a mensagem inteira: Quem Cala Consente.

A maioria dos métodos de criptografia usa fórmulas e métodos muito mais complexos que esse. A chave usada como exemplo tem cerca de 8 bits; algumas chaves são extremamente complexas, podendo chegar até 256 bits quando fazendo uso de chave simétrica com algoritmo AES *(*Advanced Encryption Standard*) e* 1024 bits ou ainda maiores quando utilizando-se de chave assimétrica com algoritmo RSA (Rivest Shamir Adleman). Quanto maior a chave (em bits), mais complexa é a criptografia e mais difícil é quebrar o código.

Para codificar uma mensagem e decodificar uma mensagem criptografada, é preciso dispor da chave ou chaves de criptografia apropriadas. Uma chave de criptografia é a tabela ou fórmula que define que caractere dos dados é transformado em que caractere criptografado. As chaves de criptografia se dividem em duas categorias: pública (assimétrica) e privada (simétrica).

- Criptografia de chave privada:

Na criptografia de chave privada, também conhecida como criptografia de chave simétrica ou criptografia de chave compartilhada, o remetente e o destinatário possuem a mesma chave e a utilizam para codificar e decifrar todas as mensagens.

Esta chave deve ser conhecida apenas pelo remetente e pelo destinatário das mensagens, o que implica na existência de um canal seguro para que a chave seja trocada sem que um atacante possa descobri-la (TRAPPE; WASHINGTON 2002).

A vantagem deste método é sua simplicidade, o que se traduz em tempo de execução menor dos algoritmos. Além disso, o tamanho da chave necessária para obter um bom nível de segurança é da ordem de meia centena de bits. Por estas razões ela é adequada para encriptação em massa, de longas mensagens.

A IBM desenvolveu um dos sistemas mais usados de chave privada, a chamada norma de criptografia de dados (DES, Data Encryption Standard*).* Em 1977, os Estados Unidos adotaram a DES como norma oficial, definida na publicação de normas de processamento de informações federais 46-2 (FIPS *[*Federal Information Processing Standards Publication*]* 46-2).

A DES usa funções de consulta a tabelas e é muito mais rápida que os sistemas de chave pública. A chave tem 56 bits. Em um desafio para quebrar a DES, vários usuários da Internet trabalharam em equipe, cada um atacando uma parte dos 72 quatrilhões de combinações possíveis (CICCARELLI et al, 2009). A chave usada no desafio foi quebrada em junho de 1997, depois de uma busca de 18 quatrilhões de chaves dos 72 quatrilhões possíveis. A mensagem em texto claro era a seguinte: “*Strong cryptography makes the world a safer place*” (Uma criptografia forte torna o mundo mais seguro).

Os algoritmos de chave privada (simétrica) são (CISCO, 2013):

- DES (Data Encryption Standard) - chave de 56 bits;
- 3DES (Triple Data Encrytpion Standard) - aplicação de 3 chaves de 56 bits (168 bit);
- AES (Advanced Encryption Standard) algoritmo mais eficiente com chaves de 128, 192 ou 256 bits.

➢ Criptografia de chave pública:

A criptografia de chave pública, também conhecida como criptografia de chaves assimétricas, usa duas chaves para criptografar e descriptografar dados: uma chave pública e uma chave privada (Figura 11). A chave pública do destinatário é usada para criptografar uma mensagem. A mensagem é enviada ao destinatário, que pode descriptografar a mensagem usando sua chave privada. Essa é uma comunicação de mão única. Se o destinatário quer enviar uma mensagem de retorno, o mesmo princípio é usado. A mensagem é criptografada com a chave pública do primeiro remetente (o primeiro remetente passa a ser o destinatário da nova mensagem) e só pode ser descriptografada com a chave privada.

No modelo clássico de criptografia (criptografia simétrica), A e B tinham que escolher secretamente uma chave K, que dava origem a uma regra para cifrar e_k e uma regra para decifrar d_k. Nos sistemas criptográficos que seguem este modelo d_k, é igual a e_k, ou então é facilmente obtido a partir de e_k.

Um grande inconveniente da criptografia simétrica é a necessidade de haver a prévia troca da chave K entre A e B, através de um canal seguro. Isto pode representar um sério impedimento em diversas situações onde não é possível estabelecer um canal seguro (PFLEEGER; PFLEEGER, 2000).

Em 1976, Diffie e Hellman propuseram a ideia de um sistema criptográfico de chave pública. No ano seguinte, Rivest, Shamir e Adleman, três cientistas do Instituto de Tecnologia de Massachusetts (MIT, Massachusetts Institute of

Technology) inventaram o conhecido sistema RSA, que deve seu nome a seus criadores.

O software de criptografia criado por eles é usado em vários produtos de redes. Posteriormente, outros sistemas foram propostos, alguns dos quais são descritos na próxima seção.

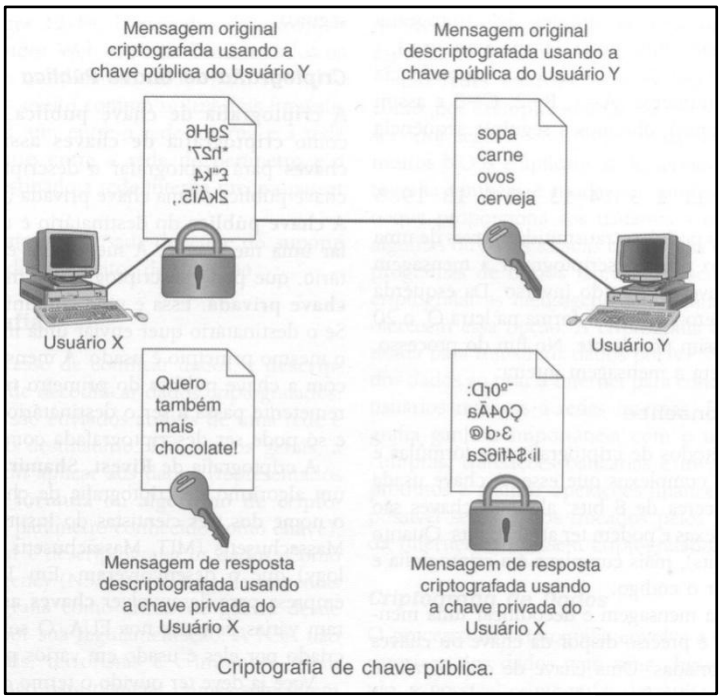

Figura 11 – Criptografia de chave pública

Fonte: Ciccarelli et al (2009).

O algoritmo RSA é capaz de criar chaves públicas com 1024 bits ou ainda maiores (CISCO, 2013).

Sistemas de chaves públicas podem ser construídos usando um certo tipo de função chamada *trapdoor one-way function*. Estas funções são chamadas *one-way* por serem fáceis de calcular, mas difíceis de inverter (PFLEEGER; PFLEEGER, 2000).

A criptografia de chave pública é utilizada na certificação digital para autenticação de assinaturas digitais. A certificação digital é discutida na seção 6.

4.8.3 Sistemas criptográficos atuais

Existem três problemas ditos matematicamente complexos, nos quais se baseiam diversos dos sistemas de criptografia de chave pública em uso hoje (AERONAUTICAL, 1998):

• Problema de fatoração de inteiros (Integer Factorization Problem – IFP), em que se baseia, por exemplo, o RSA;

• Problema de logaritmos discretos (Discrete Logarithm Problem – DLP), tendo como exemplo DSA;

• Problema de logaritmos discretos em curvas elípticas (Elliptic-Curve Discrete Logarithm Problem – ECDLP), no qual é baseado o ECC (Elliptic Curve Cryptography*)*;

Um problema é dito matematicamente difícil se o algoritmo mais rápido para resolvê-lo leva um tempo longo relativamente ao tamanho de suas entradas. Algoritmos de tempo polinomial rodam em um tempo curto em relação a suas entradas, e um exemplo é o algoritmo de soma: assim como é trivial adicionar números pequenos, existe um algoritmo que soma números enormes em um tempo curto. O mesmo não acontece com algoritmos de tempo exponencial, como algoritmos de fatoração. Apesar de ser simples fatorar números pequenos, o mesmo não acontece para números grandes. Assim, fatoração é um problema matematicamente complexo, ao passo que soma é um problema simples.

Ao projetar um sistema criptográfico, procuram-se problemas cujos algoritmos possuem tempo de execução exponencial. Em termos gerais, quanto mais tempo leva o algoritmo de resolução de um problema, mais seguro será o sistema criptográfico baseado neste problema.

Os três tipos sistemas de criptografia de chave pública citados acima são considerados hoje seguros e eficientes.

4.8.4 Assinatura digital

As assinaturas digitais garantem autenticidade, ou seja, funcionam como uma prova da origem de uma mensagem, da mesma forma que as assinaturas reais.

A assinatura digital é enviada junto com a mensagem, e é um *hash* da mesma, cifrado com a chave privada do remetente. Ao recebê-la, o receptor computa o *hash* da mensagem, decifra o *hash* anexado à mensagem usando a chave pública do suposto remetente e compara os dois. Se forem iguais, a autenticidade está garantida.

As assinaturas digitais geradas através de algoritmos de criptografia assimétrica são não-repudiáveis, uma característica muito importante. Isso acontece porque uma pessoa que deseja enviar uma mensagem gera a assinatura digital usando a sua chave secreta e a autenticação é feita na recepção usando a chave pública. Como apenas a pessoa que enviou a mensagem conhece sua chave privada, somente ela poderia ter gerado a mensagem. Em compensação qualquer um pode autenticar a mensagem, pois a chave pública é conhecida de todos (DUFFLES E MOREIRA, 2005).

No entanto, existe um problema ligado à distribuição das chaves públicas. Como são amplamente distribuídas, é difícil garantir que uma chave pública é genuína. Um atacante pode substituir a chave de uma pessoa por uma falsa, e assim, personificá-la.

Uma solução encontrada para este problema é emissão de certificados emitidos por Autoridades de Certificação (AC). Este certificado garante que uma chave pública pertence de fato à pessoa para a qual ele é emitido. A certificação digital é discutida no próximo capitulo.

5. CERTIFICAÇÃO DIGITAL

5.1 O QUE É CERTIFICAÇÃO DIGITAL

A Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. Utilizando-se da Certificação Digital, é possível, por exemplo, evitar que *hackers* interceptem ou adulterem as comunicações realizadas via Internet. Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas. Embora seja baseada em conceitos matemáticos altamente sofisticados, ela pode ser utilizada facilmente.

A maioria dos sistemas de correios eletrônicos e navegadores estão preparados para orientar os usuários, de forma didática, a realizar as principais operações com Certificação Digital.

A Certificação Digital baseia-se na existência de Certificados Digitais, que são “documentos de identificação" eletrônicos. Eles são emitidos por uma Autoridade Certificadora, que é uma entidade considerada confiável pelas partes envolvidas numa comunicação e/ou negociação. Esses certificados podem ser emitidos para pessoas físicas ou jurídicas, equipamentos ou aplicações, chamados de "titulares de certificados".

Basicamente, um certificado é concedido a uma empresa, computador ou pessoa para garantir sua autenticidade. No próprio sistema operacional Windows, por exemplo, é possível gerar certificados para uso interno ou para testar comunicações.

5.2 VANTAGENS DA CERTIFICAÇÃO DIGITAL

- Garantia de sigilo e privacidade – Quando visita-se um site "seguro" da Web, o computador recebe o certificado contendo a chave pública desse site, o que é suficiente para criar um túnel criptográfico, tornando os dados incompreensíveis durante o tráfego, sendo possível apenas ao servidor Web recuperar a informação original (ITI, 2013a);

- Controle de acesso a aplicativos – O servidor Web pode solicitar ao usuário que apresente um certificado digital, em vez de digitar usuário e senha. Os usuários não poderão colocar em perigo a aplicação pela falta de cuidado no uso e armazenamento da senha (ITI, 2013a);

- Assinatura de formulários e impossibilidade de repúdio – Os usuários poderão assinar os formulários que submetem preenchidos pela Web da mesma maneira que fariam pessoalmente em um balcão de atendimento (ITI, 2013a);

- Garantia de sigilo e privacidade – O sistema de correio eletrônico utilizado para troca de mensagens através da Internet não possui recursos nativos para impedir a violação da correspondência eletrônica. Com o uso de certificados digitais, pode-se selar uma correspondência em um envelope digital criptográfico e certificar-se de que apenas o destinatário será capaz de compreender seu conteúdo (ITI, 2013a);

- Identificação do remetente – Não existirá mais dúvidas sobre a origem de uma mensagem, pois será possível certificar-se da identidade do emissor (ITI, 2013a);

- Assinatura de mensagens e impossibilidade de repúdio – As mensagens de correio eletrônico, ou qualquer documento digital passam a valer como documento assinado, com validade jurídica, dispensando-se o uso de papel (ITI, 2013a).

5.3 CERTIFICAÇÃO DIGITAL NO BRASIL

Como visto as assinaturas digitais utilizam-se das chaves públicas para autenticar mensagens. Para garantir autenticidade a essas chaves existe o que se denomina de Infraestrutura de Chaves Públicas (ICP). Esta infraestrutura é um orgão de iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais. A principal função da ICP é definir um conjunto de

técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública. A seguir é apresentada a infraestrutura de chaves públicas brasileira.

5.3.1 Infraestrutura de chaves públicas brasileira

A infra-estrutura de chaves públicas do Brasil, definida pela Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001, é denominada Infra-Estrutura de Chaves Públicas Brasileira ou ICP-Brasil.

A Certificação Digital permite que informações transitem pela Internet com maior segurança. Utilizando-se da Certificação Digital, é possível, por exemplo, evitar que hackers interceptem ou adulterem as comunicações realizadas via Internet. Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas.

As diversas Infraestruturas de Chaves Públicas existentes hoje no mundo conseguem assegurar a autenticidade de assinaturas digitais utilizadas atualmente na rede mundial de computadores de modo a possibilitar, com elevadíssimo grau de segurança, de que um usuário de e-mail, por exemplo, seja realmente o emissor da mensagem e de que o receptor seja realmente quem ele diz ser.

No caso brasileiro a ICP-Brasil se caracteriza pela presença de um sistema hierárquico ou vertical, onde há a presença de uma AC-raiz (papel realizado pelo Instituto Nacional de Tecnologia da Informação), que credencia e audita as ACs pertencentes ao sistema.

5.3.2 Como fazer parte

Qualquer pessoa física ou jurídica pode obter uma certificação, através de uma Autoridade de Registro (AR), portando documentos necessários. É importante salientar que é indispensável a identificação pessoal do futuro titular do certificado, uma vez que este documento eletrônico será a sua "carteira de identidade" no mundo virtual. Assim, para a emissão do certificado tanto o interessado pode ir à AR como a AR pode ir ao cliente identificá-lo.

5.3.3 Aspectos legais

Conforme a Medida provisória 2.200-2, a lei brasileira determina que qualquer documento digital tem validade legal se for certificado pela ICP-Brasil (a ICP oficial brasileira). A medida provisória também prevê a utilização de certificados emitidos por outras infraestruturas de chaves públicas, desde que as partes que assinam reconheçam previamente a validade destes.

O que a MP 2.200-2 portanto outorga à ICP-Brasil é a fé pública, considerando que com o certificado emitido pela ICP-Brasil qualquer documento digital assinado pode de fato ser considerado assinado pela própria pessoa.

Resultado igual pode ser obtido se o usuário de um certificado emitido por outra ICP qualquer, depositar em cartório de registro o reconhecimento da mesma como sua identidade digital. O que se quer preservar é o princípio da irrefutabilidade do documento assinado, assim sendo, o registro em cartório de um documento no qual o usuário reconhece como sendo seu um determinado certificado digital é prova mais que suficiente para vincular a ele qualquer documento eletrônico assinado com aquele certificado.

Atualmente, estão cadastradas as seguintes entidades como Autoridades Certificadoras na ICP-Brasil (ITI, 2013b):

- CAIXA ECONÔMICA FEDERAL;
- CERTISIGN;
- PRESIDÊNCIA DA REPÚBLICA;
- SECRETARIA DA RECEITA FEDERAL;
- SERASA EXPERIAN;
- IMPRENSA OFICIAL DO ESTADO DE SÃO PAULO;
- AC JUS;
- AC PR;
- CASA DA MOEDA DO BRASIL;
- VALID CERTIFICADORA DIGITAL;
- SOLUTI CERTIFICAÇÂO DIGITAL;
- SERPRO.

5.4 HIERARQUIZAÇÃO DA ICP-BRASIL

A Infraestrutura de Chaves Públicas Brasileira é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI (Instituto Nacional de Tecnologia da Informação), além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

5.4.1 Composição da ICP-Brasil

A estrutura hierárquica da ICP-Brasil está composta da seguinte forma:

1. AC – Raiz

A Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

2. AC - Autoridade Certificadora

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o

certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

3. AR - Autoridade de Registro

Uma Autoridade de Registro (AR) é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

4. ACT – Autoridade Certificado do Tempo

Autoridade Certificadora do Tempo (ACT) é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir Carimbos do Tempo. A ACT tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo, conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período. Na prática, um documento é produzido e seu conteúdo é criptografado. Em seguida, ele recebe os atributos ano, mês, dia, hora, minuto e segundo, atestado na forma da assinatura realizada com certificado digital servindo assim para comprovar sua autenticidade. A ACT atesta não apenas a questão temporal de uma transação, mas também seu conteúdo.

6. VANTAGENS E DESVANTAGENS DE UMA REDE VPN

São apresentadas nesta seção algumas vantagens e desvantagens das VPNs.

6.1 VANTAGENS DE VPN

Existem várias vantagens quanto ao uso de VPNs. Segue-se agora a enumeração de algumas vantagens:

- Através da implantação de uma VPN permite-se a comunicação entre redes de pontos distintos, de, por exemplo, duas filiais de determinada empresa, de forma transparente e segura, formando uma única rede virtual (PINHEIRO, 2007);

- Pode-se fazer uma chamada local para a companhia telefônica ou o provedor de serviços de Internet, que se conecta a um servidor de acesso remoto e à rede corporativa. A companhia telefônica ou o provedor gerencia os *modems* e as linhas telefônicas necessárias para o acesso *dial-up*. Como o provedor oferece suporte a configurações complexas de hardware de comunicação, um administrador de rede pode gerenciar contas de usuário de maneira centralizada no servidor de acesso remoto (MICROSOFT, 2013);

- A conexão pela Internet é criptografada e segura. A autenticação e a criptografia são reforçadas pelo servidor VPN. Os dados confidenciais estão ocultos para os usuários não autorizados, mas estão acessíveis aos usuários autorizados através da conexão (MICROSOFT, 2013);

- Como as informações enviadas por uma VPN são criptografadas, os endereços especificados são protegidos e a Internet apenas verifica o endereço IP externo. Para organizações com endereços privados, essa é uma vantagem substancial, porque não há custos administrativos decorrentes da troca de endereços IP para um acesso remoto através da Internet (MICROSOFT, 2013);

- Interconexão de *intranets* localizadas distantes, sem necessidade de links dedicados, como no caso de uma empresa possuir uma matriz e duas filiais distantes geograficamente uma da outra, sendo que em cada uma delas existe uma *intranet* assim como existe a necessidade de unificação das redes para procedimentos, intervenções e consultas, tanto no aspecto da produção quanto na segurança da própria empresa (PINHEIRO, 2007);

- Outra grande vantagem a se considerar no emprego do uso de VPNs é no tocante a possibilidade de interligar a rede da empresa com fornecedores e clientes de forma mais direta permitindo que uma empresa acesse diretamente o banco de dados da outra (PINHEIRO, 2007);

- As soluções VPN permitem que as empresas possam: 1. Eliminar linhas alugadas de longas distâncias, pois como a infraestrutura utilizada é a Internet, não há necessidade de se manter WANs com linhas dedicadas. 2. Eliminar chamadas de longa distância para modems analógicos e equipamentos de acesso ISDN (ISDN, Integrated Services Digital Network*)*. 3. Pagar apenas pela banda utilizada, sem o inconveniente ou a preocupação de se desperdiçar largura de banda em linhas dedicadas de alta capacidade. Além disso, se a banda se tornar insuficiente, basta uma simples requisição de aumento ao provedor para melhorar a capacidade do acesso. 4. Utilizar um número menor de equipamentos, pois uma única solução VPN pode prover tanto acesso VPN como acesso a Internet, o que elimina o uso de bancos de *modems* separados, adaptadores de terminais, servidores de acesso remoto, etc. 5. Diminuir a estrutura de rede na extremidade do usuário e as responsabilidades de gerenciamento (ZANAROLI et al, 2000);

- Além dos benefícios econômicos, as VPNs também oferecem vantagens técnicas, por prover seus serviços com a robustez inerente à infraestrutura da Internet. Entre estas vantagens estão: 1. Facilidade de acesso devida à presença de ISPs em qualquer localidade, criando uma cobertura de rede a nível mundial. 2. Simplificação de treinamento devida à familiaridade com o

usuário. 3. Usuários remotos têm maior facilidade de acesso a um custo reduzido (ZANAROLI et al, 2000).

6.2 DESVANTAGENS DE VPN

Apesar das vantagens serem inúmeras, o uso de VPNs também tem suas desvantagens, segue agora algumas desvantagens:

- Segundo Chin (2010) como as VPNs dependem da rede pública para realização de suas conexões, esta rede deve estar quase que sempre disponível, porém isto é praticamente impossível, pois podem ocorrer falhas nas mesmas; como falhas de seguranças, ataques externos, etc;

- A Internet não foi projetada inicialmente para garantir níveis confiáveis e consistentes de tempo de resposta. Na verdade, a Internet é um meio de comunicação "Best-Effort", ou seja, realiza o máximo de esforço para prestar o serviço a qual é destinada: a transmissão de dados da origem ao destino (CATRAMBY, 2013);

- A criptografia e o processo de tunelamento podem influir bastante na velocidade de transmissão dos dados pela Internet. Contudo, muitas redes corporativas, não podem ficar a mercê dessas flutuações de desempenho e acesso da Internet (CATRAMBY, 2013);

- Aplicações onde o tempo de transmissão é crítico, o uso de VPNs através de redes externas ainda deve ser analisado com muito cuidado, pois podem ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos (CHIN, 2010).

7. ANÁLISE DAS TECNOLOGIAS VPN

É apresentada nesta seção uma análise das características que envolvem as principais tecnologias VPN existentes. São analisadas as tecnologias Frame Relay, VPN IP (VPN IPSec) e VPN MPLS. A tecnologia X.25 não é analisada devido a estar completamente fora de mercado. A tecnologia ATM também não é analisada devido a ser uma tecnologia que teve pouca aceitação no mercado brasileiro devido a sua complexidade de implantação e aos altos custos de equipamentos, ficando restrita ao uso por operadoras de telecomunicações para fornecimento de seus serviços de rede.

Primeiramente antes das análises nas seções seguintes, é apresentado no quadro 2 um comparativo entre as três tecnologias VPNs mencionadas.

Características	**Frame Relay**	**VPN IP (IPSec)**	**MPLS**
Isolamento de Tráfego (VPN)	Sim	Sim	Sim
Voz c/ QoS IP	Não	Não	Sim
Fornecimento de CPE	Sim	Sim	Sim
Gerência Pró-ativa	Sim	Sim	Sim
Endereçamento Privado	Sim	Sim	Sim
Conexão Internacional	Sim	Sim	Sim
Utilização de VC/Tunel	Sim	Sim	Não
Criptografia de dados	Não	Sim	Não
Utilização de TAGs	Não	Não	Sim

Quadro 2 – Comparativo entre Frame Relay, IPSec e MPLS

Fonte: Silva (2002).

Analisando a tabela, pode-se observar que a criptografia dos dados não é um fator relevante para MPLS nem Frame Relay, porque o tráfego da informação é controlado nos circuitos e roteadores, sendo garantida a privacidade na comunicação isolando o tráfego de cada empresa por VPN.

7.1 TECNOLOGIA FRAME RELAY

Frame Relay é uma WAN baseada em circuito virtual desenvolvida no final dos anos 80, início dos anos 90, para responder às demandas de novos tipos de serviços em redes WAN. É orientado a conexões sem controle de erros e nenhum controle de fluxo. Por se tratar de uma rede orientada a conexões, os pacotes são entregues em ordem (quando são entregues). As propriedades de entrega em ordem, nenhum controle de erros e nenhum controle de fluxo tornavam o Frame Relay semelhante a uma LAN de área extensa. Sua aplicação mais importante é a interconexão de LANs instaladas em vários escritórios de uma empresa. O Frame Relay desfrutou de um modesto sucesso, e ainda hoje é utilizado em alguns lugares (TANENBAUM, 2003).

O Frame Relay é um serviço de pacotes ideal para tráfego de dados IP, que organiza as informações em frames de dados com endereço de destino definido, ao invés de colocá-los em *slots* fixos de tempo, como é o caso do TDM (Time Division Multiplexing). Este procedimento permite ao protocolo implementar as características de multiplexação estatística e de compartilhamento de portas.

O Frame Relay é baseado no uso de Circuitos Virtuais (VC, *Virtual Circuit*), um VC é um circuito de dados virtual bidirecional entre duas portas quaisquer da rede, que funciona como se fosse um circuito dedicado.

Existem dois tipos de Circuitos Virtuais: O circuito virtual permanente (PVC, Permanent Virtual Circuit) e o circuito virtual comutado (SVC, Switched Virtual Circuit). O SVC não chegou a ser fornecido pelas operadoras.

O PVC é um circuito virtual permanente configurado pelo operador na rede através de um sistema de gerência de rede, como sendo uma conexão permanente entre 2 pontos. A rota através dos equipamentos de rede pode ser alterada ao passo

que ocorrem falhas ou reconfigurações, mas as portas de cada extremidade são mantidas fixas.

Já o SVC é um circuito virtual comutado, que é disponibilizado na rede de forma automática, conforme a demanda, sendo utilizado principalmente por aplicações de voz que estabelecem novas conexões a cada chamada.

Uma característica interessante do Frame Relay é o CIR (Committed Information Rate). O Frame Relay é um protocolo de redes estatístico, voltado principalmente para o tráfego tipo rajada, em que a sua infraestrutura é compartilhada pela operadora de telefonia e, consequentemente, tem um custo mais acessível do que uma linha privada. Isto significa que quando um usuário de serviços de telecomunicações contrata uma linha Frame Relay com 128 kb/s, não quer dizer que ele tenha alocado na rede da operadora esta banda todo o tempo, pois, já que a infraestrutura é compartilhada, haverá momentos em que ocorrerá congestionamentos.

A rede Frame Relay é sempre representada por uma nuvem, já que ela não é uma simples conexão física entre 2 pontos distintos. A conexão entre esses pontos é feita através de um circuito virtual configurado com uma determinada banda. A alocação de banda física na rede é feita pacote a pacote, quando da transmissão dos dados. A figura 12 apresenta uma rede Frame Relay.

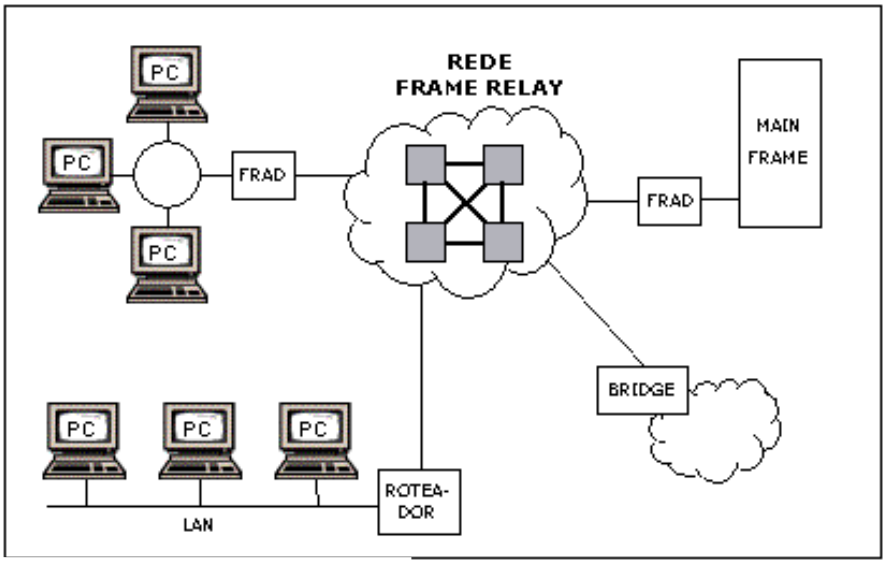

Figura 12 – Rede Frame Relay

Fonte: Teleco (2003).

7.1.1 Vantagens das redes Frame Relay

1. Capacidade para suportar múltiplos protocolos da camada três:

A tecnologia Frame Relay pode suportar qualquer protocolo da camada 3. As empresas que executam aplicativos baseados em protocolos não-IP, tais como IPX, SNA ou Apple Talk, devem considerar fortemente a implementação de uma rede Frame Relay ou permanecer com ela. Para as empresas que executam puramente aplicações baseadas em IP, isso não é um fator-chave de decisão (SPRINT, 2002).

2. Capacidade para lidar com aspectos de segurança da Internet com um único *firewall*:

Várias redes corporativas Frame Relay são construídas numa arquitetura radial (*hub-and-spoke*), com uma única conexão à Internet através de um *hub* central. Esta arquitetura requer que todos os pontos remotos da rede acessem a Internet via um *hub* central. Neste cenário, a empresa é capaz de proteger sua rede de acessos não autorizados utilizando-se apenas de um *firewall* localizado no *hub* central.

No entanto, para as empresas cujos funcionários enviam e recebem uma quantidade considerável de tráfego da Internet devem pensar bem sobre este tipo de configuração. O uso ineficiente de largura de banda, tal como o tráfego de Internet fluindo pela rede até o *hub* central podem acabar custando mais do que a implantação de conexões de Internet e *firewalls* em cada local remoto (SPRINT, 2002).

3. Capacidade de fornecer um desempenho previsível para o tráfego sensível a atrasos:

Uma vez que os quadros que transportam dados em redes Frame Relay são variáveis em comprimento, podem surgir problemas de congestionamento da rede, quando grandes blocos de dados entram na fila antes de tráfego sensível a atrasos, tais como voz. Para ajudar a amenizar este problema, o Fórum de Frame Relay ratificou procedimentos para quebrar quadros maiores em uma série de menores.

Embora tais métodos não sejam protocolos oficiais CoS (CoS, Class of Service) eles podem fornecer padrões de atraso previsíveis e, portanto, manter a integridade do tráfego sensível a atrasos. Empresas preocupadas com a qualidade do tráfego sensível a atrasos enviado através de sua rede podem se sentir mais confortáveis com uma solução Frame Relay do que uma solução VPN IP. No entanto, Frame Relay não garante uma real priorização de tráfego. Isto é importante porque o Frame Relay não pode oferecer um melhor desempenho para tráfego sensível a atrasos como em soluções IP suportados por SLAs (SLA, Service Level Agreement) competitivos (SPRINT, 2002).

7.1.2 Desvantagens das redes Frame Relay

1. Alto custo e complexidade de configurações em malha:

Empresas que querem permitir que suas locações remotas comuniquem-se uma com as outras sem a necessidade de conexão através de um hub *central*, devem ter PVCs entre cada par de locais remotos em questão. Para as empresas com muitas locações, um grande número de PVCs pode ser necessário. Quanto mais PVCs maior a complexidade e o custo. As empresas interessadas em habilitar comunicações diretas entre vários pontos, podem encontrar em uma VPN IP ou VPN MPLS uma alternativa mais viável tanto do ponto de vista técnico como financeiro (SPRINT, 2002).

2. Atraso de rede potencialmente alto:

Dependendo da topologia de rede Frame Relay de uma empresa, os pacotes que percorrem por uma rede Frame Relay podem estar sujeitos à alta latência se comparados aos de uma rede IP. Por exemplo, em uma configuração *hub-and-spoke*, o tráfego deve primeiro viajar para um *hub* central antes de chegar a seu destino final. Esta distância adicionada pode retardar a entrega de dados. Mais uma vez, as empresas que procuram conexões rápidas e diretas entre muitos locais remotos a melhor alternativa poderá ser soluções não Frame Relay, tal como VPN IP ou VPN MPLS (SPRINT, 2002).

3. Interoperabilidade limitada:

Backbones Frame Relay existentes hoje são gerenciados por diferentes operadoras e são limitados em sua capacidade de interagir um com os outros. Enquanto provedores podem interligar suas redes utilizando interfaces rede-a-rede (NNIs, Network-to-Network Interface), PVCs (PVC, Permanent Virtual Circuit*)* através de interfaces rede-a-rede são complexas e podem ser difíceis de gerenciar (SPRINT, 2002).

4. Incapacidade inerente para acesso remoto:

As redes Frame Relay não podem inerentemente suportar usuários móveis que precisam se conectar à rede corporativa enquanto estiverem distantes. Para atender às necessidades desses usuários, as empresas com redes Frame Relay devem implantar uma infraestrutura de acesso remoto separada, tais como serviços de *dial-up*. Embora esta seja uma opção viável e aceitável para muitos, empresas com uma força de trabalho móvel de considerável tamanho e crescimento, devem seriamente considerar soluções de recursos de acesso remoto de uma VPN IP ou VPN MPLS (SPRINT, 2002).

Segue, abaixo, um quadro comparativo entre Frame Relay e VPN IP:

Critérios	**Frame Relay**	**VPN IP (VPN IPSec)**
Custo	Provedores de serviços cobram mais por um circuito virtual permanete que por um VPN IP.	Elimina a necessidade de circuitos virtuais permanentes. Reduz custo da rede e de acessos. Permite a consolidação de dados, voz e tráfego de vídeo.
Escalabilidade	A escalabilidade é um desafio para implantações Frame Relay muito grandes e totalmente entrelaçadas.	É totalmente escalável, especialmente em uma VPN baseada em rede IP. Simplifica operações de WAN
Agilidade de implantação	Tipicamente de 1 a 7 semanas para um novo PVC.	Não é necessaria nenhuma configuração PVC. Menor tempo de instalação.

Flexibilidade	Normalmente implantado para conexão site-a-site entre corporações e filiais. Não permite acesso controlado à parceiros extranet.	Extende a rede para filiais remotes, extranet e trabalhadores móveis. Permite uma extranet segura com parceiros, fornecedores e revendedores.
Suporte para aplicações baseadas em IP	Projetada para camada de transporte (camada 2). Não reconhece tráfego de camada superior e oferece pouco valor acrescentado para camadas superiores.	Fornece a base para implantar serviços avançados baseados em IP que não são viáveis sobre Frame Relay, como a comunicação unificada, vídeo multicast, extranet, acesso remoto e serviços de segurança de rede.
Abrangência geográfica	Limitado a área de serviço do provedor.	Melhora a cobertura geográfica e oferece a estrutura para a conectividade global.
Acesso remoto	Normalmente não oferece acesso remoto.	Estende segurança de rede para trabalhadores móveis.
Segurança de rede	Depende de separação de tráfego para a segurança de transporte de dados.	Fornece segurança equivalente ou melhor do que Frame Relay, dependendo da escolha da tecnologia IPSec, tais como criptografia de dados Triplo Standard (3DES) e Advanced Encryption Standard (AES), faz a VPN mais segura que redes Frame Relay.

Quadro 3 – Comparativo entre Frame Relay e VPN IP (VPN IPSec)

Fonte: Cisco (2003).

7.2 TECNOLOGIA VPN IP

É apresentada nesta seção uma análise das vantagens e desvantagens da tecnologia VPN IP e também alguns estudos que demonstram algumas vantagens em relação ao Frame Relay.

7.2.1 Vantagens das redes VPN IP

1. Conectividade *any-to-any:*

Quando uma empresa conecta suas filiais com a Internet, cada filial pode se comunicar diretamente com qualquer outra filial sem a necessidade de provisão

especial de conexões independentes. Túneis seguros IPSec devem ser estabelecidos entre as filiais (SPRINT, 2002).

2. Variedade e custo-efetividade da opção de largura de banda:

O acesso à Internet está disponível em velocidades de 56 Kbps a 622,08 Mbps (OC-12) e além, enquanto Frame Relay só está disponível em velocidades de cerca de 56 kbps a 44,736 Mbps (DS3). Isso pode não ser de muita importância para empresas onde o envio de tráfego é mínimo entre os seus locais, mas é importante lembrar que, como os requisitos de largura de banda crescem, taxas de transmissão IPs elevadas são mais rentáveis do que taxas Frame Relay de alta velocidade e cargas de circuitos virtuais permanentes (PVCs). Assim, mesmo as empresas em que as atuais taxas de largura de banda são satisfeitas com o uso do Frame Relay, podem encontrar nas VPNs IP a melhor solução a longo prazo caso seus negócios continuem a crescer (SPRINT, 2002).

3. Capacidade inerente para acesso remoto:

Usuários remotos VPN IP podem simplesmente discar para o seu provedor de serviços de Internet (ISP, Internet Service Provider) ou usar conexões de banda larga DSL ou por cabo. Eles, então, usam um software para estabelecer túneis IPSec para qualquer um dos locais habilitados para a VPN IP da empresa. Como resultado, nenhuma infraestrutura de suporte precisa ser implantada ou mantida para suportar recursos de acesso remoto. Isto pode ser extremamente conveniente para as empresas com funcionários móveis ou mesmo com várias filiais com necessidades de largura de banda que podem ser abordadas por soluções de acesso remoto (SPRINT, 2002).

4. Necessidade de apenas uma conexão por site:

Uma VPN IP permite aos funcionários de uma empresa usarem a mesma conexão para Internet e conectividade WAN. Combinando estas duas funções em uma conexão poder-se-a traduzir em custos mais baixos, já que uma única porta IP de alta velocidade é mais rentável do que várias portas de velocidade mais baixas. Além disso, estas economias aumentam com a quantidade de largura de banda

requerida. Isto significa que as empresas que procuram simplificar suas infraestruturas de rede ou proporcionar aos seus empregadoso acesso à Internet, podem obter benefícios significativos através da implementação de uma VPN IP (SPRINT, 2002).

5. Maiores opções de conectividade:

VPNs IP com base em equipamentos utilizados nas instalações do cliente podem ter mais conectividade que aquelas baseadas em operadoras. Isto permite que empresas aproveitem opções de melhor custo-benefício, como DSL de alta velocidade e acesso à Internet a partir de uma ampla variedade de ISPs quando construindo suas VPNs. Significa, também, que as empresas interessadas em implementar uma *extranet* não tem que garantir que cada colaborador irá acessá-la usando o mesmo provedor de serviços (SPRINT, 2002).

7.2.2 Desvantagens das redes VPN IP

1. Altos custos de base para certos tipos de soluções:

VPNs IP baseadas em CPE (CPE, Customer Premises Equipment) são complexas, devido à necessidade de fornecer criptografia em altas velocidades e tunelamento IPSec em conexões *any-to-any*. Com solução VPN IP baseada em CPE clientes que não necessitam de acesso de alta velocidade ou configurações de rede em malha irão pagar por esses recursos. Redes baseadas em VPNs IP transferem a complexidade para a rede da operadora, diminuindo assim os custos dos equipamentos de base do cliente para o mesmo nível de uma Frame Relay. No entanto, clientes que escolherem entre uma solução VPN IP baseada em CPE ou uma solução Frame Relay geralmente irão encontrar um maior custo-efetivo para redes tipo *hub-and-spoke* de baixa velocidade (SPRINT, 2002).

2. Opções de controle de acesso mais complexas:

Conectar cada ponto da empresa na Internet exige que o controle de acesso da e para a Internet seja endereçada para cada um desses pontos. A política empresarial pode ditar que todo o tráfego de Internet atravesse o *backbone* VPN IP e saia

através de um *firewall* único, tal como uma rede Frame Relay. Ou, se aceitável, o acesso a internet pode ser concedido em cada local. No entanto, este cenário exige que *firewalls* com políticas apropriadas sejam implantados em cada conexão. Embora *firewalls* construídos em dispositivos VPN IP muitas vezes possam utilizados, o custo e a complexidade aumentariam muito para tal situação (SPRINT, 2002).

7.2.3 Tecnologia VPN IP x Tecnologia Frame Relay

Alguns estudos encontrados na pesquisa para este trabalho evidenciam algumas vantagens das Redes VPN IP sobre Redes Frame Relay, como tratado a seguir.

Migrar de uma rede corporativa Frame Relay para IP VPN (Rede Privada Virtual sobre Protocolo de Internet) oferece vantagens estratégicas e táticas para empresas de qualquer tamanho, desde multinacionais até pequenas e médias (AVAYA, 2002 apud GOLDANI, 2004).

A implementação de uma rede IP VPN é mais simples e efetiva que uma rede Frame Relay, sendo que as redes IP VPN possuem um alcance geográfico consideravelmente maior, provêm conectividade de redes entre escritórios em diferentes localidades, assim como entre usuários remotos e parceiros de negócio, e representam o primeiro passo para o desdobramento de serviços de valor agregado não disponíveis em redes Frame Relay, tais como comunicação unificada, vídeos de multidifusão e extranets (CISCO, 2004 apud GOLDANI, 2004).

Cisco (2004 apud GOLDANI, 2004) revela que a migração de Frame Relay para redes IP VPN está gerando às empresas reduções significativas no custo de conexão mensal.

Um exemplo dessa tendência é o caso da empresa Lante, líder em consultoria em Tecnologia da Informação. Os custos mensais eram de US$ 34.500 para conexões de rede Frame Relay entre a sede e quatro filiais. Quando a empresa migrou para IP VPN, os custos mensais de conectividade caíram para US$ 13.250, uma economia de 61% (CISCO, 2004 apud GOLDANI, 2004).

7.3 TECNOLOGIA VPN MPLS

Multi Protocol Label Switching (MPLS) é um mecanismo de transporte de dados pertencente à família das redes de comutação de pacotes. O MPLS é padronizado pelo IETF através da RFC-3031 e uma gama de RFCs subsequentes, e opera numa camada OSI intermediária às definições tradicionais do *Layer 2* (Enlace) e *Layer 3* (Rede), pelo que se tornou recorrente ser referido como um protocolo de "*Layer 2,5*".

O MPLS permite que os operadores de uma determinada rede tenham alto desempenho no desvio de tráfego de dados em situações críticas, tais como falhas e congestionamentos.

O MPLS permite assegurar que a transmissão de determinados pacotes tenham perdas ou atrasos imperceptíveis em função da capacidade de uma gestão de tráfego mais eficaz, possibilitando assim maior qualidade dos serviços e consequentemente maior confiabilidade.

O MPLS é uma tecnologia de encaminhamento de pacotes baseada em rótulos (*labels*) que funciona, basicamente, com a adição de um rótulo nos pacotes de tráfego (o MPLS é indiferente ao tipo de dados transportado, pelo que pode ser tráfego IP ou outro qualquer) à entrada do *backbone* (chamados de roteadores de borda) e, a partir daí, todo o encaminhamento pelo *backbone* passa a ser feito com base neste rótulo. Comparativamente ao encaminhamento IP, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de *routing*.

O *label* é um identificador curto, de tamanho fixo e significado local. Todo pacote ao entrar numa rede MPLS recebe um *label*. Este pode ser pensado como uma forma abreviada para o cabeçalho do pacote. Desta forma os roteadores só analisam os *labels* para poder encaminhar o pacote. O cabeçalho MPLS deve ser posicionado depois de qualquer cabeçalho da camada 2 e antes do cabeçalho da camada 3, ele é conhecido como Shim Header e está representado na figura 13.

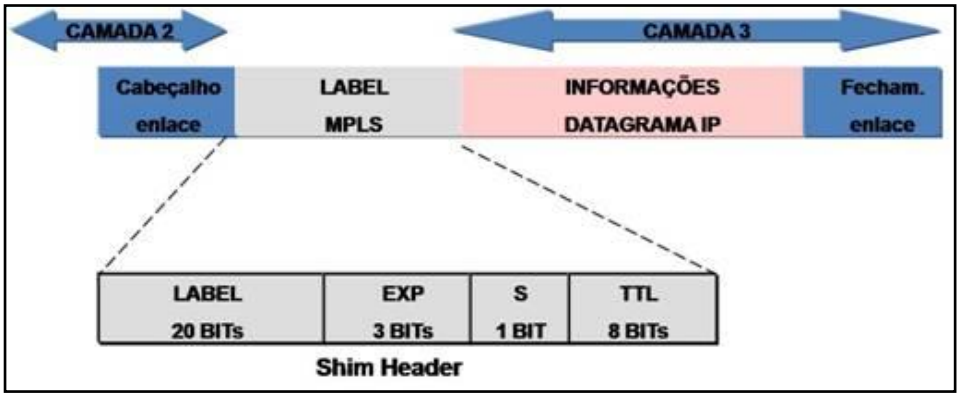

Figura 13 – Cabeçalho MPLS
Fonte: Wikipédia (2013).

Este protocolo permite a criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "*labels*" (usadas para roteamento) exclusivas de cada VPN.

Além disso, é possível realizar QoS (Quality of Service) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo.

Uma falha fundamental nas redes IP, especialmente em redes públicas, é a sua incapacidade de otimizar a utilização dos recursos da rede. Usando o padrão de roteamento IP, todo o tráfego entre dois pontos é enviado através do caminho de menor métrica, embora possam existir vários caminhos. Durante períodos de grande volume de tráfego, isso pode resultar em congestionamento do tráfego em certas rotas, enquanto rotas alternativas estão subutilizadas. Este problema é conhecido como hiperagregação (Figura 14).

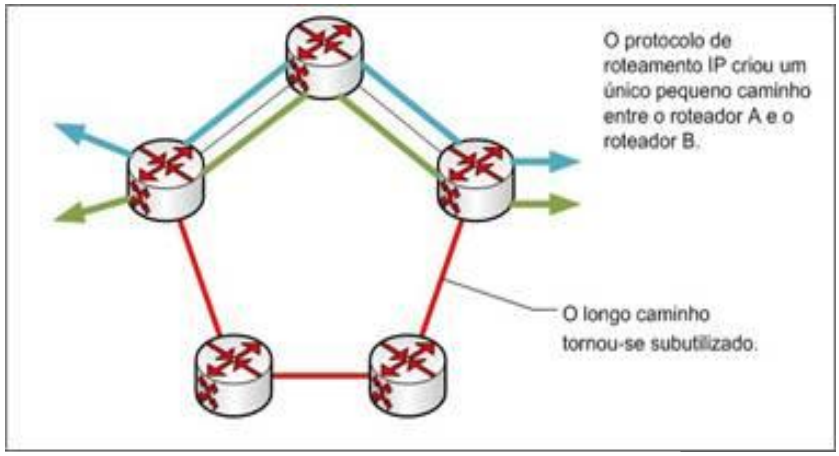

Figura 14 – Hiperagregação em rede IP convencional
Fonte: Teleco (2011).

Em vez de adicionar largura de banda para gerenciar o aumento do tráfego, a engenharia de tráfego MPLS utiliza a largura de banda existente de forma mais eficiente, permitindo que pacotes possam ser encaminhados por rotas explícitas e com uma largura de banda específica garantida. Isto é conhecido como CBR (CBR, Constraint-Based Routing), e é a chave da engenharia de tráfego MPLS. O CBR gere caminhos do tráfego de dados dentro de uma rede MPLS, permitindo que o tráfego seja encaminhado a rotas desejadas.

A engenharia de tráfego MPLS também permite confiabilidade e escalonabilidade para ser introduzida ao longo da rede, aumentando a disponibilidade e valor da rede para os clientes. Ao utilizá-la, as conexões LSPs (LSP, Label Switch Path*)* podem ser otimizadas e deduzidas. Quando ocorrem falhas, o tráfego pode ser re-roteado automaticamente por outro *link* ao redor da falha. Dois protocolos de sinalização estão atualmente em desenvolvimento pela IETF: o RSVP – TE (Resource Reservation Protocol with Traffic Engineering) e o CR-LDP (Constrained-based Label Distribution Protocol).

O RSVP-TE é um protocolo do tipo *soft-state*, ou seja, os dados devem ser atualizados periodicamente para não serem apagados, e utiliza pacotes UDP (UDP, User Datagrama Protocol*)* como mecanismo de sinalização das configurações de comunicação do LSP, incluindo descoberta de pares, rótulos perdidos, mapeamento e gestão. Ele possui características robustas e provê capacidades significantes para a engenharia de tráfego, tais como:

- QoS e parâmetros de tráfego;
- Notificação de falhas;
- Recuperação de falhas;
- Detecção de *looping*;
- Suporte multi-protocolo;
- Gerenciamento;
- Registro de objetos de rota;
- Dedução de caminho.

A engenharia de tráfego MPLS é tipicamente utilizada no núcleo na rede MPLS, enquanto o QoS é usado nas extremidades. QoS na borda da rede garante

que os pacotes de alta prioridade obtenham um tratamento preferencial, enquanto a engenharia de tráfego evita congestionamentos na rede utilizando adequadamente os recursos disponíveis de banda. Juntos, QoS e engenharia de tráfego permitem que as organizações se movam de múltiplas formas, obtendo redes especializadas de voz, vídeo e dados em uma única rede convergente IP/MPLS, reduzindo significativamente os custos e o trabalho administrativo.

7.3.1 QoS em MPLS

QoS é definido como sendo mecanismos que proporcionam aos administradores de rede a capacidade de gerenciar o tráfego da largura de banda, atraso e congestionamento em toda a rede. O QoS é implementado tipicamente na extremidade da nuvem MPLS, onde o tráfego não rotulado do cliente entra na rede da prestadora de serviço.

Uma ausência fundamental em uma rede IP, em comparação com Frame Relay e ATM, é a inabilidade de prover serviços com garantia de tráfego. Por exemplo, tráfego em tempo real como voz ou vídeo requer um serviço de alta qualidade (baixa latência, baixa interrupção, etc.) para atravessar uma rede com sucesso. Semelhantemente, dados de transações *e-commerce* devem ter prioridade em relação a dados de Web.

O MPLS permite as VPNs fornecerem circuitos com *framework* orientado à conexão, permitindo implementação de transporte VPN sobre infraestruturas de redes IP tradicional.

7.3.2 Tipos de VPN MPLS

As VPNs MPLS dividem-se em dois grandes tipos: as que operam na camada três (L3 VPN) e as que operam na camada dois (L2 VPN). As VPNs baseadas na camada três possuem uma extensão do BGP (BGP, Border Gateway Protocol), especificamente o MP-iBGP (Multi-Protocol internal BGP) para distribuir as informações de roteamento através do *backbone* do provedor de serviço. O mecanismo padrão MPLS é utilizado para encaminhar todo o tráfego da VPN para o *backbone*. Em um L3 VPN assim como em uma rede MPLS comum, o LER (LER,

Label Edge Router) e o roteador do cliente são pares. O roteador do cliente provê ao LER, informações de roteamento referente à rede privada que está por traz dele. O LER armazena estas informações de roteamento em uma tabela virtual de encaminhamento e roteamento (VRF - Virtual Routing and Forwarding); cada VRF representa essencialmente uma rede IP privada. O LER mantém uma tabela VRF separada para cada VPN proporcionando assim, isolamento e segurança adequadamente. Os usuários de uma VPN possuem acesso apenas a sites ou *hosts* dentro de uma mesma VPN. Além das tabelas VRF, o LER também armazena as informações de roteamento necessárias para efetuar o encaminhamento do tráfego ao longo da rede pública.

VPN de camada três utiliza uma pilha de rótulos MPLS contendo dois níveis. O rótulo de nível interno (2º nível na pilha) transporta especificações da VPN (a VRF da VPN), do LER ligado ao equipamento do cliente, até o LER ligado ao destino, passando por todos os LSRs (Label Switch Router*)* que compõem seu caminho. O rótulo externo (1º nível da pilha) carrega as informações de encaminhamento da rede MPLS. Os equipamentos do núcleo da rede MPLS apenas lêem e utilizam as informações contidas no rótulo externo dos pacotes que trafegam pela rede, não havendo interação com rótulo interno.

A abordagem de uma L3 VPN possui várias vantagens. O espaço do endereçamento IP do cliente é gerido pela prestadora de serviços, simplificando significativamente o papel de TI do cliente – novos clientes com sites VPN são facilmente ligados e geridos pela prestadora. L3 VPNs também possuem vantagens no suporte à auto-descoberta para distribuição de rotas VPN, aproveitando as capacidades de roteamento dinâmico do BGP. A maior desvantagem do L3 VPN é suportar apenas o tráfego dos clientes baseados em encapsulamento IP.

A seguir, no quadro 4, é apresentado um comparativo entre VPN MPLS e VPN IP (VPN IPSec).

Característica	VPN MPLS	VPN IP (VPN IPSec)
Confiabilidade	Todos os circuitos MPLS são recebidos através de uma única transportadora, o que contribui com a confiabilidade. Entretanto, algumas operadoras de serviço oferecem VPN em MPLS usando DSL como enlace local, o que pode resultar em menor confiabilidade. Em geral, MPLS será mais confiável do que VPNs IPSec, porque há menos complicações na configuração de tunelamento e *firewall*.	Receber todos os circuitos IPSec VPN através da mesma transportadora vai aumentar a confiabilidade (tolerância a falhas) sobre o uso de múltiplas operadoras de Internet. Mas devido a vários concentradores VPN e configuração de criptografia, uma VPN IPSec pode ser menos confiável do que VPN em MPLS devido a complexidade de gerenciar várias conexões.
Custo	O custo de um projeto MPLS para o fornecimento de VPN é relativamente alto. Porém em VPNs IPsec exige mão de obra especializada para o gerenciamento dos túneis, quanto a confiabilidade e segurança das informações, como também concentradores para agregar *links*. No MPLS VPN esses fatores ficam sobre a responsabilidade da operadora de serviço.	Ao contrário das VPN em MPLS, em VPN IPSec são necessários concentradores VPNs, o que irá aumentar o custo inicial. Depois de ter o hardware, o pessoal necessário para manter o sistema e solucionar problemas dos túneis VPN IPSec, no final os valores podem aumentar, podendo ser o mesmo ou até passar em comparação a VPN em MPLS.
QoS	As QoS podem ser oferecidas como serviço nesse caso. Com MPLS QoS, podem-se priorizar determinados tipos de tráfego ao longo da rede da operadora, provendo QoS fim a fim. Isso é ótimo para aplicações sensíveis à latência, como Voz, Vídeo.	Recursos de QoS em VPN IPSec não existem. Ao trafegarem na rede, os dados são criptografados gerando atraso e pouco pode ser feito quanto a isso.
Segurança	VPN e MPLS são mais seguros do que os túneis VPN IPSec, desde que não permitam que seus circuitos MPLS tenham acesso diretamente à Internet. Para maior segurança, as VPNs MPLS devem ser usadas apenas como redes privadas. Usado como uma rede privada, as VPNs MPLS oferecem um bom nível de segurança, porém tendo em vista que os dados nesse caso não são criptografados.	Elementos que compõem uma rede de túneis VPN IPSec, é uma preocupação que deve ser levada em consideração já que os dados estão sendo transmitidos através de um *link* de internet. Esse circuito Internet está aberto para conexões de todo o mundo. Um *firewall* mal configurado pode abrir uma rede VPN IPSec para a Internet. Segurança é uma preocupação ainda maior se usar a divisão de túnel em concentradores VPN. Porém os dados em VPN IPSec são criptografados.

Quadro 4 - Comparativo entre VPN MPLS e VPN IP (VPN IPSec)

Fonte: Teleco (2010).

8. ESTUDOS PRÁTICOS QUE COMPROVAM AS VANTAGENS DE UMA VPN

Nascimento (2009) realizando estudos teóricos e práticos acerca das vantagens da aplicação de VPN concluiu em uma implantação desse sistema na Unimontes, que o uso de VPN sobre a Internet pode ser visto como alternativa de baixo custo, gerenciável e segura para interligar os Campi da Unimontes. O estudo apresentou técnicas de criptografia, tunelamento e comutação de pacotes, incluindo exemplos e diversos algoritmos na revisão bibliográfica, assim como alternativas para o serviço, vantagens e desvantagens para um completo entendimento do leitor.

Nascimento (2009) concluiu que a utilização da VPN trouxe a possibilidade de desfrutar dos serviços que de forma alternativa seria necessário à contratação de circuitos virtuais pelas operadoras, gerando economia considerável para a instituição, possibilitando a contratação de serviços melhores para o acesso à Internet para os campi da Universidade. O autor mostra ainda na prática que com a VPN é possível suprir as demandas existentes da Universidade, integrando as secretarias e possibilitando que os sistemas do Estado funcionem em vários Campi, admitindo que a rede seja flexível para acompanhar o crescimento da instituição, de forma segura e gerenciável.

Em outro caso prático os estudos de Galvão et al (2012) revelam que após apresentada a realidade atual da topologia de acesso remoto para manutenção da Controladora de Discos da empresa Beta, mostrados os conceitos e o funcionamento de uma VPN, concluiu-se sua total vantagem frente a outras tecnologias.

O estudo de Pires (2010) revelou também no cenário de estudos práticos acerca de VPN a importância de se ter um controle preciso dos projetos executados pela Eletrobrás – Distribuição Acre, através da tecnologia VPN, bem como uma analise pós-implantação dos sistemas, onde se concluiu que VPN é uma tecnologia que se liga à rede de computadores através da Internet de forma a trabalhar como se estivesse presente na central de dados, com isso economiza tempo, gastos com movimentação de pessoal e equipamentos, assim como implantação de sistemas dedicados, que oneram os projetos.

Por fim, nos estudos de Faneli e Marchezini (2007) mostrou-se na aplicação prática de VPN que aplicando essa metodologia em uma empresa possuidora de matriz e duas filiais em conjunto com outras ferramentas de segurança, é possível garantir integridade, confidencialidade, autenticação e controle de acesso, permitindo uma comunicação tão segura quanto o estágio atual da tecnologia possibilita. Entretanto, para usufruir de todos os benefícios hoje disponíveis, Faneli et Marchezini (2007) revelam que a implementação deve ser cuidadosamente planejada, procurando-se ajustar os recursos existentes às diversas situações possíveis do cenário prático real. Isso envolve políticas rígidas de segurança tanto para a parte física quanto lógica da rede, aplicáveis aos diversos elementos que a compõem: servidores, *proxies*, *firewalls*, *gateways*, *gateways* de VPN, estações de trabalho, antivírus, *anti-spyware*, *anti-spam*, etc.

CONCLUSÃO

Através de estudos teóricos e alguns casos práticos foi possível comprovar a hipótese defendida nesse estudo acerca da viabilidade e vantagens do uso de VPN nas empresas atuais.

Tendo como objetivo principal mostrar a viabilidade da implementação de segurança nas redes de comunicação através de VPN, conclui-se através de pesquisa bibliográfica que a VPN apresenta grandes benefícios econômicos e técnicos aplicados aos dias de hoje.

Sua parcela de contribuição no desenvolvimento de novas tecnologias e desempenho quanto à segurança na utilização da Internet para gerenciar organizações é fator primordial, sendo inúmeros os serviços oferecidos por ela.

Quanto à segurança obtida pode-se constatar que os algoritmos de criptografia bem como os protocolos específicos geram grandes obstáculos aos invasores. Atende as condições de segurança quanto à integridade, à confidencialidade das informações transmitidas, assim como à autenticação e o controle de acesso, permitindo maior confiança por parte das empresas que adotam esta solução. São, portanto cada vez mais pesquisadas e incorporadas às organizações, sejam privadas ou governamentais, em diversos sistemas e ambientes computacionais.

Porém, cabe ressaltar, que apesar de inúmeras vantagens, também existem algumas desvantagens. Caberá então às organizações analisarem as características de seus negócios a fim de implementar ou migrar para uma rede VPN, decidindo qual é a melhor tecnologia a ser aplicada às suas necessidades. Apesar das vantagens financeiras obtidas, fazer, por exemplo, uma migração de uma rede Frame Relay para uma VPN IP ou MPLS não custa pouco. Exige empenho financeiro e uma forte mobilização do quadro de colaboradores.

Finalizando este trabalho, propõem-se, futuramente, estudos práticos sobre o tema, analisando empresas que aderiram à VPN, mostrando o cenário antes e

depois da implantação, as etapas de implantação e os resultados obtidos na visão da administração.

BIBLIOGRAFIA

ABREU, L. H. **Arquitetura MPLS para Formação de VPN**. 2006. Disponível em <http://www.si.uniminas.br>. Acessado em julho de 2013.

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL. **Application Security Solution for the Aeronautical Telecommunication Network**. [S.l.: S.n.], 1998.

CATRAMBY, G. F. **Virtual Private Network** Disponível em: <http: //www.gta.ufrj.br/grad/99_1/gabriela/vpn.html>. Acessado em setembro de 2013.

CERT, **Incidentes Reportados ao CERT.br de Abril a Junho de 2013.** Disponível em <http://www.cert.br/stats/incidentes/>. Acessado em outubro de 2013.

CHIN, L. K. 2006. **Rede Privada Virtual – VPN.** Disponível em <http://www.rnp.br/newsgen/9811/vpn.html>. Acessado em junho de 2013.

CICCARELLI, P. et al. **Princípios de Redes**. 1 ed. Rio de Janeiro: LTC, 2009.

CISCO, **From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task**. Disponível em <http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/vpnmi_wp. html>. Cisco Systems, 2003. Acessado em outubro de 2013.

CISCO, **HandsOn-IOS-VPN**. Disponível em: <http://www.academ ias. isep.ipp. pt/ uploads/ Ficheiros/HandsOn-IOS-VPN.pdf>. Acessado em outubro de 2013.

CUNHA, J. C. 2008. **O que é uma VPN e suas características**. Disponível em <http://jeancarloscunha.wordpress.com/2008/11/15/>. Acessado em setembro de 2013.

DUFFLES, M.; MOREIRA, D. **Função Hash e Autenticação em Redes de Computadores**. 2005. Universidade Federal do Rio de Janeiro.

FANELI, A.; MARCHEZINI, V. **OPENVPN: implementação de VPN através de SSL em ambiente de software livre.** Monografia apresentada ao Curso de Pós-graduação em Segurança de Redes de Computadores da Faculdade Salesiana de Vitória, para o curso de Especialista em Segurança de Redes de Computadores. Vitória, 2007.

FERREIRA, F.N.F. **Segurança de informação**. Rio de Janeiro: C. Moderna, 2003.

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

GALVÃO, L. et al. **Uma solução segura de acesso remoto via VPN para manutenção de Controladora de Discos de Mainframe da Empresa Beta baseada na Norma NBR ISO/IEC 17799**. 2012. Disponível em <http://www.lyfreitas.com.br/ant/artigos_mba/artvpn.pdf> acessado em julho de 2013.

GOLDANI, C. A. **IPSec e Redes Virtuais Privadas** – informe técnico. Unicerte, 2004.

ITI. **Certificação Digital.** Disponível em <http://www.iti.gov.br/certificacao-digital>. Acessado em agosto de 2013a.

ITI. **ICP-Brasil.** Disponível em <http://www.iti.gov.br/icp-brasil>. Acessado em agosto de 2013b.

MICROSOFT. **Conexões de VPN**. In TechNet: Disponível em: <http://technet.microsoft.com/pt-br/library/cc775417%28v=ws.10%29.aspx> Acessado em agosto de 2013.

MORAES, A. F. **Reduzindo Custos de Telecom com VPNs**. 2004. Disponível em <www.sucesues.org.br/eventos>. Acessado em agosto de 2013.

NASCIMENTO, R. **Estudo de Caso para implantação de VPN na Unimontes**. Monografia de Pós-Graduação “Lato Sensu” apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em “Administração em Redes Linux”. MG: 2009.

NORTHCUTT, S. et. al. **Desvendando Segurança em Redes**. Rio de Janeiro: Campus, 2002.

PFLEEGER, C. P.; PFLEEGER, S. L. **Security in Computing**. 3 ed. New Jersey: Prentice Hall, 2000.

PINHEIRO, J. M. S. **Redes Privadas Virtuais.** 2007. Disponível em <http://www. projetoderedes.com.br/tutoriais/tutorial_vpn_01.php>. Acessado em setembro de 2013.

PIRES, A. **Uso da tecnologia VPN no gerenciamento a distância de empreendimentos de engenharia**. Dissertação apresentada ao Programa de Mestrado em Engenharia Civil da Universidade Federal Fluminense. Curso de Tecnologia da Construção. UFF, Niterói, 2010.

RED HAT. **Guia de segurança: Um Guia para Proteger o Red Hat Enterprise Linux Ed. 1.5** Disponível em: https://access.redhat.com/site/documentation/pt-BR//Red_Hat_ Enterprise _ Linux/6 /pdf/ Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-pt-BR.pdf> , Red Hat, Inc. 2011. Acessado em setembro de 2013.

SANTOS, J. P. **Ameaças e ataques ao sistema de informação**. UNIFOA, 2008.

SILVA, L. S. Da. **Virtual Private Network**. 1 ed. São Paulo: Novatec, 2002.

SPRINT, **Frame Relay vs. IP VPNs.** 2002, Disponível em <http://www.sprint.com/business/resources/02089.pdf>. Acessado em agosto de 2013.

STALLINGS, W. **Cryptography and networks security: principles and practice**. 2.ed. New Jersey: Prentice Hall, 1999.

STALLINGS, W. **Criptografia e segurança de redes: Princípios e práticas**. 4 ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, A. S. **Redes de Computadores**. 4 ed. Rio de Janeiro: Eselvier, 2003.

TELECO. **Estudo Básico do MPLS**. 2011. Disponível em <http://www.teleco.com.br/tutoriais/tutorialmplseb2/default.asp>. Acessado em agosto de 2013.

TELECO. **Frame Relay.** 2003. Disponível em <http://www.teleco.com.br /tutoriais/ tutorialfr /default.asp>. Acessado em agosto de 2013.

TELECO. **Redes MPLS II: VPN em Camada 3.** 2010. Disponível em <http://www.teleco.com.br/tutoriais/tutorialmplscam2/default.asp>. Acessado em agosto de 2013.

TORRES, G. **Redes de Computadores - Curso Completo**. Axcel Books, 2001.

TRAPPE, W.; WASHINGTON, L. **Introduction to Cryptography with Coding Theory.** New Jersey: Prentice Hall, 2002.

WIKIPEDIA, **MPLS**. Disponível em: http://pt.wikipedia.org/wiki/MPLS. Acessado em agosto de 2013.

ZANAROLI, A. P. et al. **VPN – Virtual Private Network** – Seminário da Disciplina de Redes Locais de Computadores – 9º Período de Engenharia de Telecomunicações, novembro/2000. Disponível em <http://www.abusar.org.br/vpn/vpnport.htm>. Acessado em agosto de 2013 .