UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA DE MEDIÇÃO DE FATURAMENTO NO SETOR ELÉTRICO

WILSON MIRANDA JÚNIOR

ORIENTADOR: PAULO ROBERTO DE LIRA GONDIM

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELETRICA

PUBLICAÇÃO: PPGENE.DM - 348/2008

BRASÍLIA/DF: JULHO – 2008

FICHA CATALOGRÁFICA

MIRANDA JR, WILSON

Segurança da Informação para o Sistema de Medição de Faturamento no Setor Elétrico [Distrito Federal] 2008.

Xiv, 82p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2008).

Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia. Departamento de Engenharia Elétrica, 2008.

1. Segurança da Informação
2. Setor Elétrico
3. Sistema de Medição de Faturamento
4. NAT sobre NAT
5. VPN sobre VPN

REFERÊNCIA BIBLIOGRÁFICA

MIRANDA JR., W. (2008). Segurança da Informação Para o Sistema de Medição de Faturamento no Setor Elétrico. Dissertação de Mestrado em Engenharia Elétrica, Publicação: PPGENE.DM - 348/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 82p.

CESSÃO DE DIREITOS

AUTOR: Wilson Miranda Júnior.

TÍTULO: Segurança da Informação para o Sistema de Medição de Faturamento no Setor Elétrico.

GRAU: Mestre ANO: 2008

_____

Wilson Miranda Júnior
SHCES 805 bloco A apt°. 106, Cruzeiro Novo.
70655-851 Brasília – DF – Brasil.

Agradeço

Ao professor Gondim, que alem de orientador foi um grande amigo.

E a toda a minha família.

Dedico

Aos meus pais (*in memorian*).

“Não sou jovem o suficiente para saber tudo”.

Oscar Wilde

RESUMO

A Segurança da Informação hoje é de extrema relevância a todos os pontos em que os dados necessitam ser transitados, dentro de uma corporação ou entre empresas. Os mecanismos de segurança adotados devem prever toda e qualquer necessidade de autenticidade, confiabilidade, disponibilidade e possibilidade de rastreamento da informação. O setor elétrico brasileiro atualmente funciona com seu sistema interligado de norte a sul do país. A CCEE - Câmara de Comercialização de Energia Elétrica é responsável por receber todas as informações dos pontos de medição de faturamento. A ANEEL - Agente Nacional de Energia Elétrica aprovou uma resolução no qual contempla somente uma porção segura na tramitação das informações oriundas do SMF - Sistema de Medição de Faturamento.

Esta pesquisa parte da identificação das empresas que têm a necessidade de receber as informações do SMF, avalia os riscos que comprometem a tramitação da informação e propõe melhorias nos pontos falhos de segurança da informação. São utilizadas técnicas de tecnologias diferenciadas, tais como, o conjunto de padrões IPSec disponibilizando o tunelamento de uma rede virtual privada - VPN sobre VPN e a tradução de endereços de rede - NAT sobre NAT. Para que essa proposta seja avaliada, foi desenvolvido um estudo de caso vivenciado em um agente do setor elétrico brasileiro. Como resultado deste trabalho, uma série de melhorias na segurança da informação do SMF é apresentada.

ABSTRACT

Today, the Security of Information is of extreme importance to all points where data need to be transmitted within the corporation or between companies. The security mechanisms adopted must provide all and any need for authenticity, reliability, availability and traceability of information. The Brazilian electric sector currently works with an interconnected grid from north to south of the country. The CCEE - Electric Energy Marketing Chamber is responsible for receiving all the information from the billing points. The ANEEL - National Electric Energy Agency adopted a resolution which covers only a safe portion in handling of information from the SMF - Billing Measurement System.

This research identifies all companies that need to receive information from the SMF, assesses the risks that compromise the handling of information and proposes improvements in information security failure points. Different techniques from various technologies were used, such as IPSec standards which provide the tunneling of a Virtual Private Network – VPN over VPN and the Network Address Translation – NAT over NAT. A case study was created regarding an experience of a Brazilian electrical sector agent. A series of improvements in the information security of SMF are presented as a result of this study.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3DES – *Triple Data Encryption Standard*

AH – *Authentication Header*

ANEEL – Agência Nacional de Energia Elétrica

CCEE – Câmara de Comercialização de Energia Elétrica

DARPA – *Defense Advanced Research Projects Agency*

DDoS – *Distributed Denial-of-Service*

DES – *Data Encryption Standard*

DMZ – *Demilitarized Zone*

EDI – *Eletronic Data Interchange*

ESP – *Encapsulating Security Payload*

IBM – *International Business Machines*

ICV – *Integrity Check Value*

IETF – Internet *Engineering Task Force*

IKE - Internet *Key Exchange*

IP – Security Protocol

IPSec - *IP Security Protocol*

KBS – *knowledge-Based Systems*

MD5 – *Message-Digest algorithm 5*

NAT – *Network Address Translation*

ONS – Operador Nacional de Energia

OSI – *Open Systems Interconnection*

PIN – *Personal Identification Numbers*

PVC – *Permanent Virtual Circuit*

RAM – *Random Access Memory*

RDSI – *Integrated Services Digital Network*

RSA – algoritmo de ciframento de dados baseado em chave pública (corresponde às iniciais dos sobrenomes dos seus inventores, Rivest, Shamir e Adleman)

SCDE – Sistema de Coleta de Dados de Energia Elétrica

SGSI – Sistema de Gestão de Segurança da Informação

SIN – Sistema Interligado Nacional

SMF – Sistema de Medição de Faturamento

SSL – *Secure Sockets Layer*

TCP – *Transmission Control Protocol*

TI – Tecnologia da Informação

TLS – *Transport Layer Security*

UDP – *User Datagram Protocol*

UTM – *Unified Threat Management*

VPN – *Virtual Private Network*

1 INTRODUÇÃO

A Segurança da Informação hoje é de extrema relevância a todos os pontos que os dados necessitam ser transitados, dentro da corporação ou entre empresas. Os mecanismos de segurança adotados devem prever toda e qualquer necessidade de disposição, identificação, confiança e rastreamento da informação.

Independentemente da forma apresentada pela informação ou o meio através do qual é compartilhada ou armazenada, recomenda-se que ela seja sempre protegida adequadamente. A segurança da informação é obtida a partir da implementação de uma série de controles que podem ser políticos, práticos, de procedimentos e de estruturas organizacionais.

O setor elétrico brasileiro hoje atua com o seu sistema interligado. Para compreendermos essa interligação observamos que a energia produzida no sul pode ser consumida no norte do Brasil e vice-versa. Neste ponto, passa a existir a necessidade da tramitação da informação para comercialização.

Diversos problemas ligados à segurança da informação atingem as atividades do setor elétrico. Tais problemas podem ser verificados nos diferentes agentes envolvidos na geração, transmissão, distribuição, regulação e comercialização de energia.

Uma das atividades de grande relevância para os citados agentes do setor elétrico se refere à utilização do Sistema de Medição de Faturamento – SMF das empresas.

Na atualidade existe uma resolução normativa da ANEEL que contempla somente uma porção segura na tramitação das informações oriundas do SMF no setor elétrico.

Essa pesquisa identifica os pontos vulneráveis na tramitação das informações do SMF e se dispõe a, por meios tecnológicos, avaliar, propor e demonstrar o trâmite seguro das informações entre os agentes do setor elétrico, bem como delimitar suas fronteiras, tais como, a Câmara de Comercialização de Energia Elétrica – CCEE, Operador Nacional de Energia – ONS e as que necessitam da disponibilização da informação do Sistema de Medição de Faturamento – SMF. Dentre tais empresas incluem-se tanto as que realizam produção e distribuição de energia elétrica quanto as que a comercializam.

Para coleta dos dados do SMF é preciso considerar uma série de aspectos relevantes à segurança da informação das empresas envolvidas, tais como:

- Compartilhamento da informação oriunda de medidores de faturamento comuns entre as empresas envolvidas.

- Segregação de perímetro, provendo permissão de acesso lógico de outras empresas dentro das corporações no qual detém o medidor de faturamento.

- Área de abrangência e posicionamento geográfico das empresas envolvidas no processo.

- Assegurar a disponibilidade, integridade, autenticidade, confidencialidade e o não - repúdio da informação.

Conforme será tratado neste trabalho, fazem-se necessárias melhorias de segurança no ambiente como um todo, de sua origem até o destino, tanto dos dados providos da rede externa quanto os trafegados na rede interna, considerando análise da informação trafegada. Esta pesquisa também visa propor a implementação de um dispositivo de monitoramento para assegurar a funcionalidade dos ativos.

Revelando também algumas das definições de melhores práticas, metodologias e tecnologias atuais, este trabalho busca o desenvolvimento de uma sistemática envolvendo ferramentas e ações para atender os requisitos necessários da informação segura no SMF do setor elétrico.

Os meios tecnológicos tratados nessa pesquisa incluem o *firewall* baseado em estado de conexões, o conjunto de padrões IPSec disponibilizando o tunelamento de uma VPN entre empresas distintas que se comunicam pela internet sobre outra VPN dedicada à segurança interna da corporação até o ponto de medição; e NAT sobre NAT entre os perímetros externos e internos até o medidor. Arquiteturas de segurança cooperativa auxiliam na composição desta sistemática integrada para garantir a segurança da informação.

1.1 Motivação

Inicialmente, destaca-se o fato de a segurança da informação ter deixado de ser um assunto restrito aos porões dos quartéis e órgãos diplomáticos, chegando às salas de reunião de diretoria, auditores, administradores das mais diversas empresas, bem como aos próprios indivíduos.

A segurança da informação de um sistema corporativo com ênfase no setor elétrico tem como um de seus produtos finais a coleta de dados de medição de energia para mensurar a valorização do negócio. Verificou-se a necessidade de melhorias no sistema de segurança dessa informação coletada. A abrangência destes dados engloba empresas geradoras, transmissoras e comercializadoras de energia elétrica.

Com o crescimento do setor elétrico brasileiro, a CCEE identificou falta de confiabilidade, integridade, disponibilidade e precisão das informações de controle no SMF. Verificou-se a necessidade de convergência do modelo antigo onde a medição de faturamento era feita localmente, diretamente nos medidores de energia, dependendo do entendimento de leitura dos operadores, sem devidos métodos eficazes em conformidade com o Sistema Interligado Nacional – SIN.

A CCEE e ONS, para cumprimento da Resolução Normativa do Agente Nacional de Energia Elétrica – ANEEL nº 115, de 29 de novembro de 2004, requerem a aprovação de projetos de comunicação ao Sistema de Coleta de Dados de Energia.

Além das proposições estipuladas em cumprimento de normas, os agentes do setor elétrico, as empresas e os consumidores têm a necessidade de se comunicarem, em prol de tramitar, verificar, armazenar, auditar e publicar os dados pertinentes ao SMF com responsabilidade e segurança na informação.

1.2 Objetivos

1.2.1 Geral

- Pesquisar e dissertar sobre um conjunto de ações em interligação entre as empresas relacionadas ao setor elétrico, que supra a necessidade de coleta, tramitação e acesso de modo seguro, de informações relevantes ao faturamento e a sua medição.

1.2.2 Específicos

- Dissertar sobre tecnologia e segurança da informação;
- Apontar os riscos para segurança da informação;

- Abordar a segurança organizacional;
- Pesquisar, desenvolver e dissertar acerca de um estudo de caso a ser vivenciado no setor elétrico brasileiro, especialmente em uma concessionária de serviços de energia elétrica, à qual atribuiremos o codinome de Empresa “A”.

1.3 Metodologia

A pesquisa terá como fundamentação metodológica um caráter descritivo, no qual os fatos serão observados, analisados, registrados, classificados e por fim interpretados de forma concisa e embasados em referências bibliográficas, com base em métodos comparativos, levantamento de dados e estudo de casos.

A metodologia utilizada para as análises e pareceres desenvolvidos na dissertação baseou-se no método indutivo de análise qualitativa, classificando-a como qualitativa e bibliográfica, apresentado por Marconi e Lakatos (2003) e teve por meta buscar por meio desta, elementos que subsidiassem de forma qualitativa os pressupostos básicos e essenciais, a interpretação e a reflexão do problema objeto da pesquisa.

A pesquisa é também quantitativa na medida em que apresenta um estudo de caso cujos dados são oriundos de trabalhos de campo e de medições realizadas em ambiente informatizado de empresa do setor elétrico.

1.4 Organização do trabalho

Além desta Introdução, esta pesquisa abordará ainda as seguintes partes: o capítulo 2 disserta sobre tecnologia e segurança da informação. O capítulo 3 aponta os riscos para a segurança da informação. O capítulo 4 desenvolve um estudo de caso vivenciado no setor elétrico brasileiro em uma empresa específica. Após o capitulo 4, são apresentadas as conclusões e alguns dos possíveis trabalhos futuros.

2 TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta aspectos tecnológicos que devem coexistir para melhor atender às necessidades de prover segurança da informação. O conjunto de padrões estabelecidos para criação de VPN com IPSec e arquitetura de rede com utilização de *firewall* cooperativo são contemplados para demonstrar métodos diferenciados na aplicabilidade da segurança da informação integrada, tanto em diversidade aos meios externos e profundidade aos meios internos.

A informação necessita ser devidamente protegida, pois além de ser um ativo como qualquer outro ativo importante, é também um conjunto de fatos organizados que adquire um valor a mais do que o valor do fato para a organização.

A tecnologia da informação é o modo de gerar e processar informação que seja útil às atividades humanas. É, pois, um conjunto de técnicas que possibilitam lidar com dados, informes, comunicação, representação gráfica, sinais e códigos, desde as formas mais primitivas até os sofisticados processos e imagens de satélite. Atualmente, todas as técnicas da informação convergem para um modo predominante de efetivação: a eletrônica digital. Ao longo dos tempos, a capacidade intelectual dos homens tem se dirigido para o controle e aumento das possibilidades de aperfeiçoamento das técnicas, capazes de ampliar os sistemas de informação. A evolução dos Sistemas de Informação abriu caminho às redes, utilizando modernas técnicas de conexão via satélite e fibras óticas [57].

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas os principais patrimônios de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se ponto crucial para a sobrevivência das organizações. Na época em que as informações eram armazenadas em papel, a segurança era relativamente simples, pela falta de conhecimento quanto ao valor da informação. Com as mudanças tecnológicas, a estrutura de segurança ficou mais sofisticada, possuindo controles centralizados.

Informações contidas em sistemas informatizados são consideradas recursos críticos para concretização de negócios e tomada de decisões. O que pode acontecer se as informações de sua organização caírem nas mãos da concorrência (perda da confidencialidade), se forem corrompidas/apagadas (perda da integridade) ou não puderem ser acessadas para o fechamento de um grande negócio (perda da disponibilidade). Hoje em dia, é muito fácil

atacar os sistemas informatizados, visto que os sistemas de informação estão conectados em redes externas [28].

A constante evolução das técnicas de informação e o constante aperfeiçoamento dos computadores introduziram linguagens e terminologias específicas tanto em relação às novas máquinas, como em relação ao processamento da informação e ao modo pelo qual essa é retratada em termos de linguagem genética.

Um marco importante na evolução da tecnologia da informação foi a instalação pelo *Defense Advanced Research Projects Agency* - DARPA dos Estados Unidos de um nova rede eletrônica de comunicação, que deu origem à Internet.

A Internet *Engineering Task Force* – IETF é uma comunidade internacional voltada à evolução da arquitetura e do perfeito funcionamento da internet e tem como missão identificar e propor soluções para as questões, problemas e interoperabilidade entre diversos padrões e suas aplicações.

Atualmente, a grande maioria das empresas utiliza, direta ou indiretamente, protocolos criados a partir da iniciativa das citadas DARPA e IETF, inclusive para área do segurança da informação.

2.1 Segurança da Informação

Neste tópico são inseridos pontos relevantes para elucidar o grau de importância da segurança da informação.

Segurança de Informação está relacionada com métodos de proteção aplicados sobre um conjunto de dados no sentido de preservar o valor que possui para um indivíduo ou uma organização. São características básicas da segurança da informação os aspectos de confidencialidade, integridade e disponibilidade, não estando restritos somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. Desta forma a Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais.

A segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades.

Atualmente, o conceito é padronizado pela norma ISO/IEC 17799/2005, influenciado pelo padrão inglês (*British Standard*) BS 7799. A série de normas ISO/IEC 27000 foi reservada para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002/2005 continua sendo considerada formalmente como 17799/2005 para fins históricos.

Podem ser estabelecidas métricas (com ou sem o uso de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria da situação de segurança existente.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

Conforme as normas citatas, a segurança da informação está calcada em três objetos de segurança, a saber:

- Confidencialidade: Toda Informação dever ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas por pessoas a quem elas são destinadas;

- Integridade: Evitar que os dados sejam apagados ou de alguma forma alterados, quando toda informação deve ser mantida nas mesmas condições deixadas pelo seu proprietário, protegendo contra alterações indevidas, intencionais ou acidentais;

- Disponibilidade: Proteger o serviços de informática de tal forma que toda informação gerada ou adquirida esteja disponível aos seus usuários.

Conforme a figura 1, a autenticidade e o não - repúdio também podem ser importantes e junto com a integridade, a disponibilidade e a confiabilidade formam as propriedades mais relevantes para a segurança. Isso significa que toda informação deve chegar aos usuários de

uma forma segura. Para que isso aconteça, todos os elementos de rede por onde a informação trafega de sua origem até chegar ao seu destino devem estar assegurados.

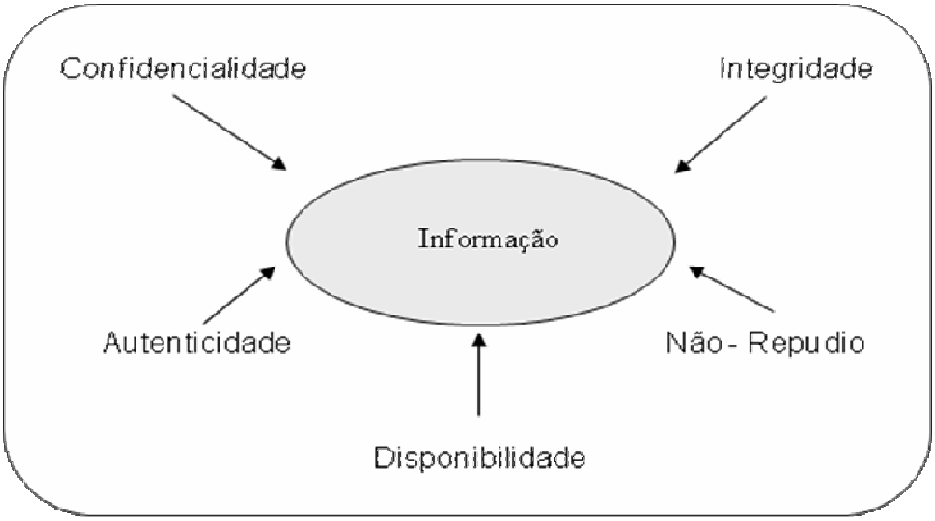

Figura 1 – As propriedades mais relevantes da segurança

- Autenticidade: garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta a informação;
- Não-repúdio: impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação. Garantir que quem originou a menssagem é realmente quem diz ser.

Antes de apresentar um programa de segurança de informações são feitas as seguintes indagações [28]:

- O que devemos proteger?
- Contra que ou quem?
- Quais as ameaças mais prováveis?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos humanos e financeiros pretendemos gastar para atingirmos os objetivos de segurança desejados?
- Quais as expectativas dos usuários e clientes em relação à segurança das informações?
- Quais as conseqüências para a organização se os sistemas e informações forem corrompidos ou roubados?

A figura 2 mostra os aspectos que devem ser considerados na proteção da informação, os quais incluem ainda os aspectos jurídicos e de negócios que direcionam efetivamente a estratégia de segurança de cada tipo e organização.

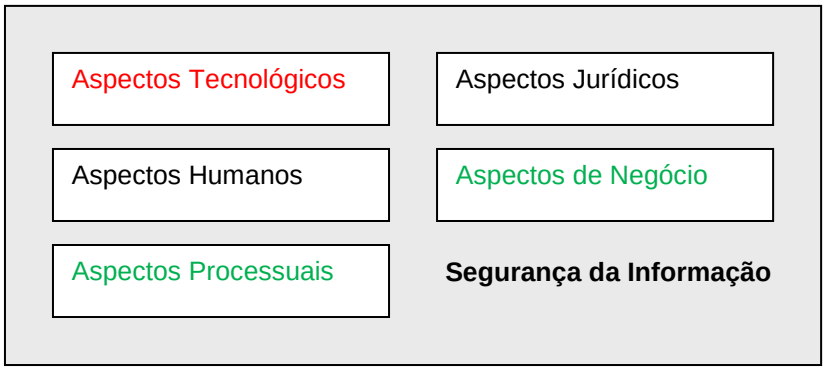

Figura 2 – Os aspectos envolvidos na proteção da informação [40]

Alcançando as respostas para os aspectos envolvidos na proteção da informação será possível definir os objetivos e requisitos de segurança da informação que uma organização tem que desenvolver para apoiar suas operações dentro de um patamar de segurança.

Nesta pesquisa, ao se tratar de segurança da informação, será enfatizado os aspectos tecnológicos. Assim, a segurança de redes pode prover grande parte da manutenção da disponibilidade, integridade, confiabilidade, autenticidade e não - repudio das informações, significando, na verdade, mais que uma proteção contra os *hackers*, maus funcionáros ou vírus. Adicionalmente, os aspectos tecnológicos poderão influenciar algumas outras naturezas de aspectos processuais ou natureza de negócios.

Os pontos tecnológicos, tais como, criptografia, *firewall*, VPN e o conjunto de padrões IPSec são mencionados a seguir para composição de uma segurança cooperativa que constitui uma sistemática para a segurança dos dados tramitados tanto na rede externa, quanto na rede interna.

2.2 Criptografia

O processo criptográfico permite contribuir para o sigilo da informação, pode-se verificar neste tópico a utilização dos métodos criptográficos para contribuir na construção de VPN com IPSec, como pode ser visto na Seção 2.5.

Etimologicamente a palavra "criptografia" deriva de *criptologia*, que se origina do grego "*kryptós lógos*", que significa "palavra escondida". Assim, pode-se ter como fundamento que a criptografia é a ciência da transformação de dados de maneira à torná-Ios incompreensíveis sem o conhecimento apropriado para sua tradução [61].

Segundo o conceito acima, a criptografia serviria para tornar determinado conteúdo secreto, a fim de evitar a descoberta da informação por elementos externos. Assim, os dados acabam sendo convertidos em um código que somente poderá ser traduzido por aquele que possuir a "chave" secreta.

Entende-se o processo de tornar a informação inelegível por "encriptar", enquanto "desencriptar" é o processo inverso, ou seja, retornar o código para algo compreensível. A ciência de inventar códigos denomina-se "criptografia", enquanto a ciência de decifrá-los chama-se "criptoanálise" [61].

[39] afirma que o algoritmo de criptografia é uma seqüência de procedimentos que envolve uma matemática capaz de cifrar e decifrar dados sigilosos. O algoritmo pode ser executado por um computador, por um hardware dedicado ou por um humano. Em todas as situações, o que diferencia um de outro é a velocidade de execução e a probabilidade de erros. Existem vários algoritmos de criptografia.

Além do algoritmo, é utilizada uma chave. Na criptografia computadorizada, a chave é um número, ou um conjunto de números, que protege a informação cifrada. Para decifrar o texto cifrado, deve o algoritmo ser alimentado com a chave correta, que é única. Na figura 3, é ilustrado o esquema geral de cifragem utilizando chave.

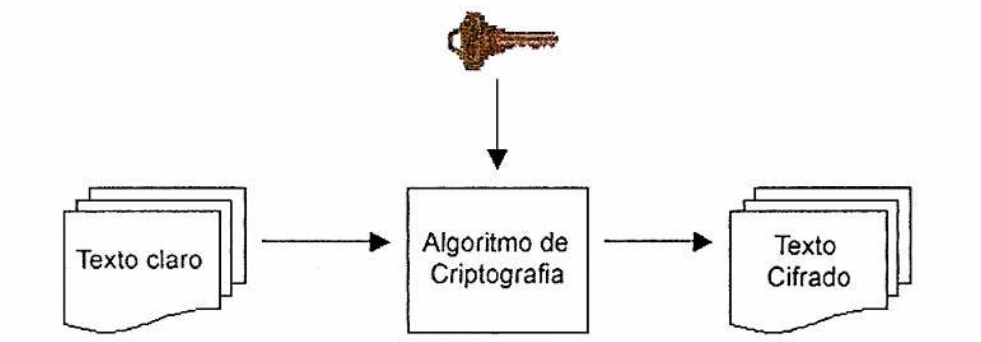

Figura 3 – Esquema geral de cifragem com chave [39]

Segundo [28], “identificação e autenticação são as mais vastas aplicações da criptografia. Identificação é o processo de verificação da identidade de alguém ou de alguma coisa”. Exemplificando, quando se retira dinheiro em um banco, o processo pode ser feito de forma eletrônica, com o uso da criptografia. Todos os cartões de terminais automáticos são associados a uma senha, a qual vincula o proprietário do cartão ao proprietário da conta.

Com a utilização de cartões magnéticos, estando a senha correta, a máquina infere que aquela pessoa seja o proprietário da conta e libera o acesso. Uma outra aplicação que pode-se destacar na criptografia é a autenticação. A autenticação é similar à identificação, uma vez que ambos processos permitem a uma entidade o acesso a determinados recursos. Porém, a autenticação é mais abrangente, dado que ela não envolve necessariamente a identificação da pessoa ou entidade [28].

A autenticação meramente determina se dada pessoa ou entidade é autorizada para aquilo em questão, reconhecendo-a por meio de códigos tidos como pessoais e intransferíveis.

É importante ressaltar que o segredo da criptografia não está no algoritmo empregado, e sim na chave de criptografia. Os melhores sistemas criptográficos são aqueles de domínio público, podendo, portanto, ser extensamente analisados pelos cientistas e validados quanto a possíveis falhas ou fraquezas, sendo posteriormente revistos num processo permanente de melhoria [53].

Afirma-se que a criptografia não é a única ferramenta necessária para assegurar a segurança de dados, nem irá resolver todos os problemas de segurança. É um instrumento entre vários outros. Além disso, a criptografia não é à prova de falhas. Toda criptografia pode ser quebrada e, sobretudo, se for implementada incorretamente, ela não agrega nenhuma segurança real.

Pode-se dizer que a criptografia está presente no dia-a-dia de forma intensa, mesmo que não se tenha esta percepção. De fato, esta técnica é uma poderosa ferramenta no mundo da informática e das transações digitais das quais todos dependem. No entanto, esta pode não ser a última palavra, visto que, a criptografia está condicionada à evolução tecnológica e científica, pois o sucesso da criptografia reside na inviabilidade da reversão do seu processo, com a utilização das tecnologias e conhecimentos que se dispõe. Com o avanço da tecnologia podem surgir novas implementações, tanto de hardware como de software, que facilitem a reversão dos processos criptográficos dos algoritmos atuais.

A partir da evolução dos meios de criptografia, podem ser encontrados dois diferentes processos de cifragem: a criptografia simétrica (convencional) e a criptografia assimétrica (chave pública).

2.2.1 Criptografia Simétrica (Convencional)

A criptografia simétrica é utilizada em um criptossistema em que a criptografia e a decriptografia são realizadas usando a mesma chave. Ela também é conhecida como criptografia convencional. É importante ressaltar que a criptografia simétrica transforma o texto claro em texto cifrado, usando uma chave secreta e um algoritmo de criptografia. Usando a mesma chave e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado [58].

[58] afirma que é impraticável decriptografar uma mensagem com base no texto cifrado mais o conhecimento do algoritmo de criptografia/decriptografia, ou seja, não há necessidade de se manter o algoritmo secreto, conforme pode ser observado na figura 4.

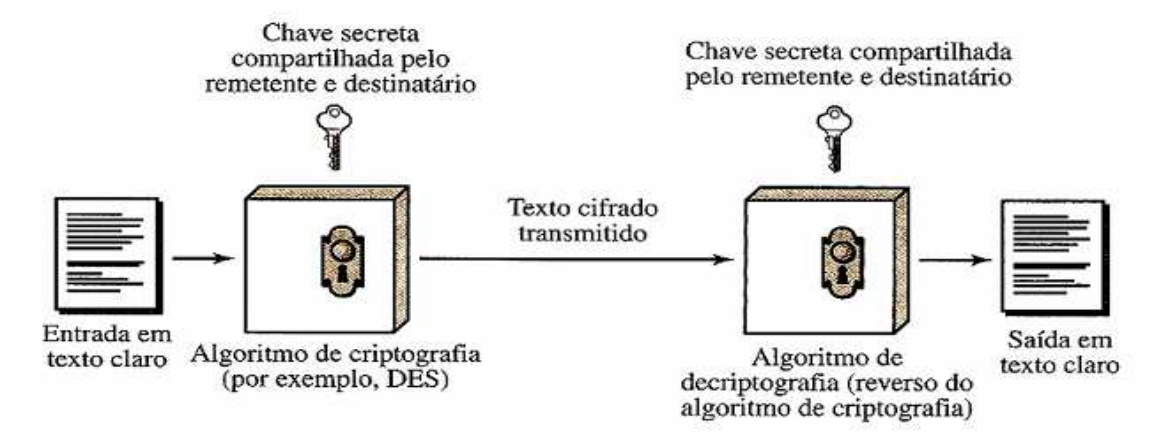

Figura 4 – Modelo simplificado da criptografia convencional [58]

Para uma pessoa se comunicar com outra com segurança, ela deve passar primeiramente a chave utilizada para cifrar a mensagem. Este processo é chamado de "distribuição de chaves", e como a chave é o principal elemento de segurança para o algoritmo, ela deve ser transmitida por um meio seguro.

Uma das tentativas de solucionar o problema da distribuição das chaves secretas foi a criação de um centro de distribuição de chaves (*Key Distribution Center* - KDC), que seria responsável pela comunicação entre pessoas aos pares. Para isto, o KDC deve ter consigo

todas as chaves secretas dos usuários que utilizam seus serviços. Por exemplo, imagine a situação descrita pela figura 4, onde A quer mandar uma mensagem secreta para B. Para isto, ele manda a mensagem para o KDC usando sua chave secreta. O KDC recebe esta mensagem, decifrando com a chave secreta de A, depois o KDC a cifra novamente usando agora a chave secreta de B, e a envia para o mesmo. O maior problema em torno do KDC, é que este constitui um componente centralizado, além de ser gerenciado por pessoas que podem, casualmente, ser corrompidas [59].

Uma vez que a mesma chave é utilizada para cifrar e decifrar, este método é mais rápido e fácil de implementar do que a criptografia assimétrica. Considerando também que as chaves dos algoritmos simétricos são menores do que as chaves dos assimétricos, se tomada como base de comparação a resistência aos ataques de força bruta.

[40] afirma que os algoritmos de chave simétrica têm como característica a rapidez na execução, porém eles não permitem a assinatura e a certificação digitais. Além disso, existe o problema da necessidade de distribuição das chaves secretas a serem utilizadas pelos usuários, que deve ser feita de maneira segura. O problema está na dificuldade de enviar a chave gerada para o usuário, pois o canal de comunicação ainda não é seguro. Outro problema é o uso de chaves secretas diferentes para cada tipo de comunicação e também para cada mensagem, o que faz com que seu gerenciamento se torne muito complexo. Um exemplo dessa complexidade pode ser visto em um ambiente no qual três usuários se comunicam entre si, onde cada um deles deve armazenar e gerenciar três chaves diferentes. A figura 5 mostra que Maria precisa de três chaves secretas diferentes para se comunicar com João, Pedro e Luís

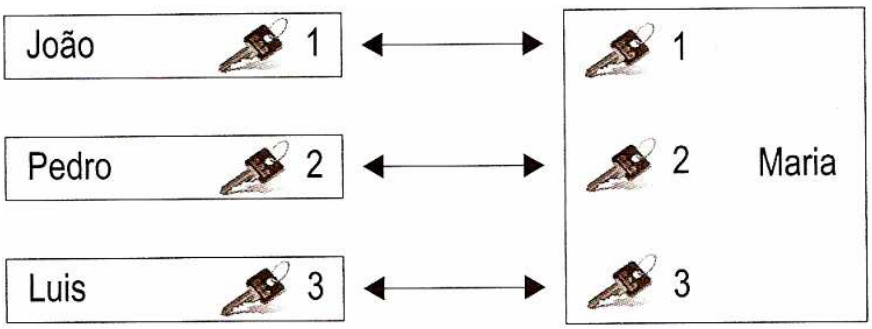

Figura 5 – As chaves secretas necessárias na criptografia simétrica [40]

Observa-se que a grande vantagem da chave simétrica é sua velocidade em relação à chave assimétrica. A desvantagem de compartilhar a chave simétrica é a necessidade de uma cópia em cada extremidade. A chave simétrica não pode ser usada para finalidades de

autenticação, então, seu algoritmo é raramente usado sozinho. Um exemplo é o *Data Encryption Standard* (DES), conforme se verifica adiante é utilizado com uma função *hash* para autenticação.

2.2.1.1 DES e 3DES

O algoritmo de criptografia DES foi desenvolvido na década de 70 pelo *National Bureau of Standarts* com ajuda da *National Security Agency*. O propósito era criar um método padrão para proteção de dados. A International Business Machines – (IBM) criou o primeiro rascunho do algoritmo, chamando-o de LUCIFER. O DES tornou-se oficialmente norma federal americana em novembro de 1976.

Conforme [48], o algoritmo DES trabalha com 64 bits de dados a cada vez. Cada bloco de 64 bits de dados sofre de 1 a 16 iterações (16 é o padrão DES). Para cada iteração um pedaço de 48 bits da chave de 56 bits entra no bloco de ciframento. O deciframento é o processo inverso. O DES pode ser quebrado por ataque de força bruta.

Desenvolveu-se então o 3DES, que cifra a informação mais de uma vez; no 3DES, a mensagem é cifrada com uma chave, seus resultados decifrados com outra, então é cifrada novamente com a chave original, para ser enviada ao destinatário, que realiza as mesmas operações de forma inversa; apenas ao fim das três operações é que teremos a mensagem original. Essa técnica faz com que o tamanho efetivo da chave de 56 bits aumente para 168 bits.

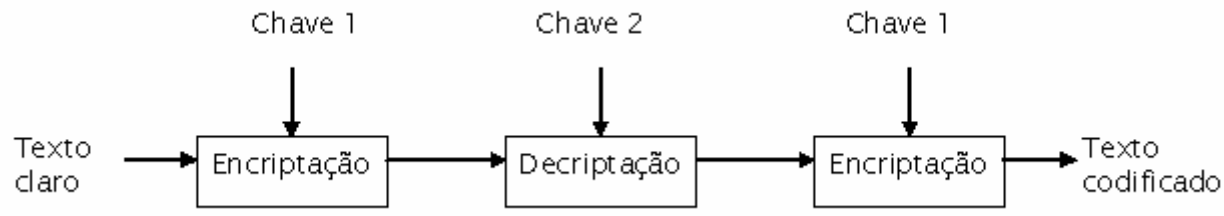

Figura 6 - Ciframento utilizando 3DES

A variante mais simples do 3DES opera da seguinte forma: DES (k3;DES(k2;DES(k1;M))), onde M é o bloco de mensagem a ser criptografado e k1, k2 e k3 são chaves DES.

O 3DES usa 3 chaves de 64 bits (o tamanho máximo da chave é de 192 bits, embora o comprimento atual seja de 56 bits). Os dados cifrados com a primeira chave, decifrados com a segunda chave e finalmente cifrado com a terceira chave, faz do 3DES ser mais lento que o DES original, mas oferece maior segurança.

2.2.1.2 Criptografia com Chave Secreta

Na criptografia com chave secreta, a mensagem, ou texto, é criptografada aplicando-se uma função à mensagem com uma chave secreta. A decodificação é feita aplicando-se a função inversa ao texto criptografado, utilizando a mesma chave, para produzir a mensagem original. Como a chave é mantida em segredo, as funções de codificação e decodificação não precisam ser secretas.

Ambas as partes envolvidas na comunicação (emissor e receptor) devem possuir a função de criptografia e uma chave secreta. Antes que a comunicação comece, a chave secreta deve ser adquirida por ambos através de um canal seguro.

Na criptografia com chave secreta é necessário que haja confiança entre o emissor e o receptor, pois ambos devem ter a posse da chave secreta.

Na criptografia com chave privada, também chamada de *secret-key* ou *symmetric-key encryption*, onde uma chave é usada tanto para cifrar quanto para decifrar. O DES é um exemplo de um sistema de criptografia com chave privada.

2.2.2 Criptografia Assimétrica (Chave Pública)

As chaves assimétricas apesar de serem mais fáceis de gerenciar são um pouco mais complicadas, elas permitem cifrar a informação por uma chave e decifrar por outra. As duas chaves utilizadas nesse cenário são chamadas de chave pública, que é distribuída, e chave privada, que deve ser mantida em segredo. Com chaves assimétricas, os parceiros no negócio trocam suas chaves públicas para se comunicar, mas mantém suas chaves privadas em segredo.

Afirma [58] que os algoritmos assimétricos contam com uma chave para criptografia e uma chave diferente, porém relacionada para decriptografia.

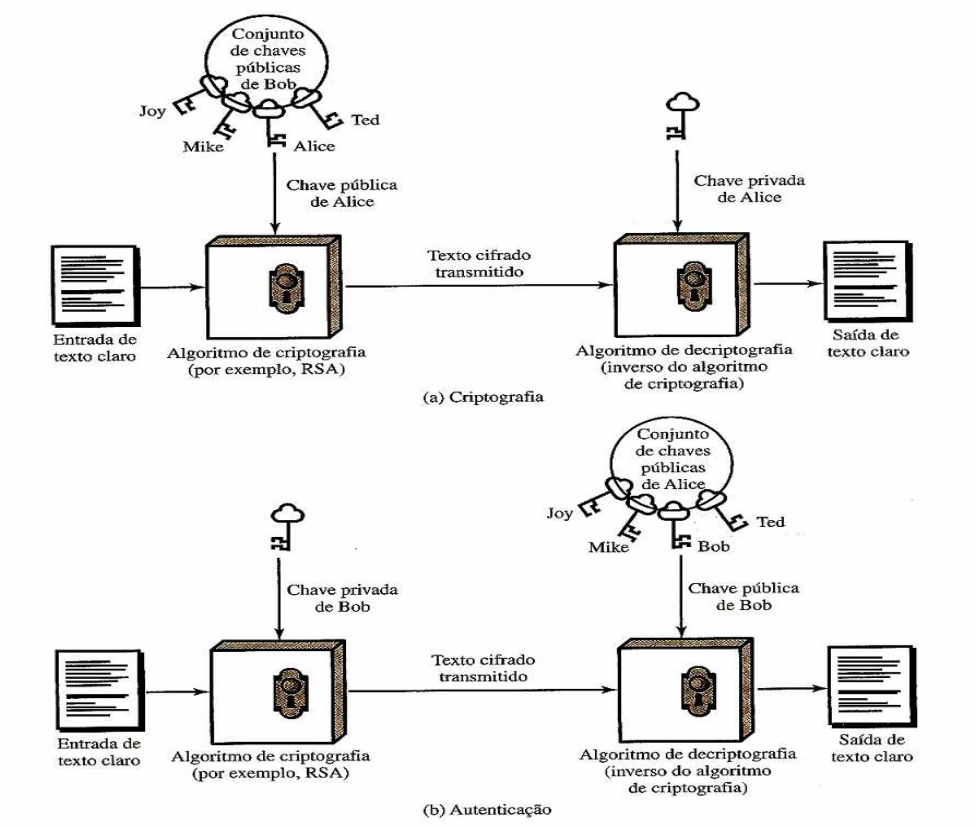

Figura 7 – Criptografia de chave pública [58]

Conforme figura 7, a criptografia com chave pública é um esquema assimétrico que usa um par de chaves para ciframento: uma chave pública, que encripta dados, e uma chave secreta e privada correspondente (as duas chaves são relacionadas entre si) para deciframento. Diz-se que a sua chave pública é para todos enquanto mantém sua chave privada em segredo. Qualquer um com uma cópia de sua chave pública pode, então, encriptar informação que só você pode ler. É computacionalmente quase impossível deduzir a chave privada a partir da chave pública.

Conforme a tabela 1, o benefício primário de criptografia com chave pública, é que, permite as pessoas que não têm nenhum arranjo de segurança, possam trocar mensagens com segurança. A necessidade do transmissor e receptor para compartilhar chaves secretas por algum canal seguro é eliminado, todas as comunicações só envolvem chaves públicas, e nenhuma chave privada é transmitida ou é compartilhada. Um exemplo de sistema de criptografia com chave pública é o RSA[1].

[1] RSA corresponde às iniciais dos sobrenomes dos inventores do código de criptografia, Rivest, Shamir e Adleman.

Criptografia convencional	Criptografia de chave pública
Necessário para funcionar: 1. O mesmo algoritmo com a mesma chave é usado para criptografia e decriptografia. 2. O emissor e o receptor precisam compartilhar o algoritmo e a chave **Necessário para a segurança:** 1. A chave precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais amostra do texto cifrado precisam ser insuficientes para determinar a chave.	**Necessário para funcionar:** 1. Um algoritmo é usado para criptografar e decriptografar com um par de chaves, uma para criptografia e outra para decriptografia. 2. O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não é a mesma chave). **Necessário para a segurança:** 1. Uma das duas chaves precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Tabela 1 - Criptografia convencional e de chave pública [58]

2.2.2.1 RSA

É o mais conhecido dos métodos de criptografia de chave pública. Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no *Massachussets Institute of Technology* - M.I.T. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em diversas aplicações.

A criptografia assimétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando diferentes chaves – uma chave pública e uma chave privada. Ela também é conhecida como criptografia de chave pública. De acordo com [58], a criptografia assimétrica transforma o texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. A criptografia assimétrica pode ser usada para confidencialidade, autenticação ou ambos.

Quanto maiores os números primos utilizados para a criação da chave, maior é a segurança proporcionada por esse algoritmo. Os números primos que são utilizados têm geralmente 512 bits de comprimento e combinados formam chaves de 1.024 bits. Em algumas aplicações, como por exemplo, bancárias, que exigem o máximo de segurança, a chave chega

a ser de 2.048 bits. Os algoritmos para a geração das chaves públicas e privadas usadas para cifrar e decifrar as mensagens são simples [39].

O criptossistema de chave pública mais utilizada é o RSA. A dificuldade de atacar o RSA está no desafio de encontrar os fatores primos de um número composto [58].

2.2.2.2 Diffie-Hellman

Um conceito relacionado à criptografia de chave pública é a troca de chave exponencial, às vezes denominada algoritmo de *Diffie-Hellman*. O *Diffie-Hellman* é um método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976.

De acordo com [15], a troca de chave exponencial fornece um mecanismo para configurar uma conexão secreta, porém não-autenticada, entre duas partes. Isto é, as duas partes podem negociar uma chave de sessão secreta, sem recear bisbilhoteiros. Todavia, nenhuma das partes tem alguma maneira forte de saber o que realmente está na outra extremidade do circuito.

A finalidade do algoritmo é permitir que dois usuários negociem uma chave com segurança, a qual pode então ser usada para a subseqüente criptografia das mensagens. O próprio algoritmo é limitado ao acordo de valores secretos [58].

2.2.3 Função Hash

Uma função *hash* mapeia uma mensagem de tamanho variável em um valor de *hash* de tamanho fixo, ou um resumo de mensagem. Para autenticação da mensagem, uma função de *hash* segura precisa ser combinada de alguma forma com uma chave secreta [58].

A função *hash* tem como objetivo maior embaralhar de maneira irreversível a informação antes de ser encaminhada ao seu destino final.

2.2.3.1 MD5

Para garantir a integridade da informação é utilizado um método criptográfico da função hash.

O *Message-Digest Algorithm* 5 - MD5 é um algoritmo de função *hash* de 128 bits unidirecional desenvolvido, em 1991, por Ronald Rivest, para suceder o MD4 que tinha alguns problemas de segurança. Por ser um algoritmo unidirecional, uma *hash* MD5 não pode ser transformada novamente no texto que lhe deu origem. O método de verificação é, então, feito pela comparação das duas *hash* (uma da base de dados, e a outra da tentativa de *login*). É descrito na *Request for Comments* - RFC 1321 e muito utilizado por softwares com protocolo ponto-a-ponto (P2P, ou *Peer-to-Peer*), verificação de integridade e *logins*.

No algoritmo MD5, a entrada pode ser de comprimento arbitrário, o processamento ocorre em blocos de 512 bits e a saída é de 128 bits.

Segundo [48], o MD5 é o último de uma linha de algoritmos usados para criar assinaturas digitais para uma mensagem, de forma a provar a autoria. Após a mensagem ser comprimida pelo algoritmo, também conhecido como o cálculo do *hash* da mensagem, o resultado é assinado com a chave privada do emissor, utilizando criptografia de chave pública.

O MD5, de acordo com [48], também é usado para verificar a integridade de um ficheiro através, por exemplo, do programa MD5, que cria a *hash* de um ficheiro. Isto pode tornar-se muito útil para downloads de ficheiros grandes, para programas P2P que constroem o ficheiro através de pedaços e estão sujeitos à corrupção dos mesmos. Como autenticação de *login* o MD5 é utilizado em vários sistemas operacionais.

Uma função *hash* de 128 bits, como MD5, não é inadequada para o HMAC, pois para atacar o MD5 o atacante pode escolher qualquer conjunto de mensagens e trabalhar nelas *off-line*, em uma instalação de computação dedicada para encontrar uma colisão. Se a velocidade for um problema, é totalmente aceitável usar MD5 em vez de SHA-1 como função de *hash* embutida para *Hashed Message Autentication Code* - HMAC [58].

2.2.3.2 SHA-1

O algoritmo SHA-1 foi desenvolvido pelo NIST em 1993. A entrada pode ser de comprimento arbitrário e deve ser completada para que o comprimento se torne múltiplo de 512 bits (como ocorre com o MD5) [39].

A saída desse algoritmo é de 160 bits e blocos de 512 bits são processados a cada passo. Este algoritmo possui menor probabilidade de colisão quando comparado com o

algoritmo MD5, e no algoritmo SHA-1 existe a probabilidade de ocorrer colisões após 2^{80} aplicações, contra 2^{64} aplicações do MD5 [7].

A estrutura do algoritmo SHA-1 é semelhante à do algoritmo MD5. O algoritmo SHA-1, a exemplo do algoritmo MD5, possui um buffer que é atualizado a cada operação e que será o resultado final da *hash*. Neste caso, como a saída é de 160 bits, o buffer é composto de 5 partes de 32 bits. O algoritmo SHA-1 utiliza também um segundo buffer de 5 partes de 32 bits [39].

Uma função de *hash* como SHA não foi projetada para uso como um MAC e não pode ser usada diretamente para essa finalidade, pois não depende de uma chave secreta. Tem havido diversas propostas para a incorporação de uma chave secreta em um algoritmo de *hash* existente. A técnica que obteve o maior suporte é HMAC, que foi publicado como a RFC 2104, escolhido como MAC de implementação obrigatória para segurança IP.

Ao invés de utilizar o método convencional do *checksum*, desenhado para detectar erros na transmissão sem prover real segurança, o HMAC é um *framework* que trabalha com padrões de criptografia *hash* para associação do cabeçalho, no qual incorpora um valor secreto para criação do *Integrity Check Value* – ICV na autenticação do cabeçalho. No decorrer dessa pesquisa será utilizada a função *hash* MD5 encapsulado junto ao HMAC para garantir a integridade na autenticação.

2.3 Firewall

Uma das ferramentas de maior importância para a segurança da informação, o *Firewall* tem como sua principal característica a proteção e segregação de redes distintas, sendo para internet, rede interna ou entre empresas. Pode ser considerado um conjunto de funcionalidades, arquitetura e tecnologia. Podemos citar sua tecnologia voltada a filtro de pacotes baseado em estado ou *Proxy* (nível de aplicação).

[15] afirma que um *firewall* é qualquer dispositivo, *software*, arranjo ou equipamento que limita o acesso à rede. Ele pode ser uma caixa comprada ou construída, ou uma camada de *software* em alguma outra coisa. Atualmente, os *firewalls* vêm “gratuitamente” dentro de muitos dispositivos: roteadores, *modems*, estações de base sem fio e *switches* de IP, para citar alguns. Os *firewalls* de *software* estão disponíveis para (ou são incluídas com) todos os sistemas operacionais populares. Eles podem ser um calço de cliente (uma camada de

software) dentro de um PC executando Windows, ou um conjunto de regras de filtragem implementado em um *kernel* Unix.

O foco deste tópico é apresentar e analisar as principais tecnologias e funcionalidades do *firewall* na segurança de qualquer organização. As arquiteturas de um *firewall*, que têm como evolução natural o *firewall* cooperativo, também são apresentadas, passando pelas questões de desempenho e funções de segurança cooperativa da corporação.

2.3.1 Tecnologia de firewall

Dentro das tecnologias que envolvem o *firewall* podemos mencionar:

- **Filtro de Pacote:** Exerce sua funcionalidade de análise na camada de rede e transportes da pilha TCP/IP, para realizar as decisões de filtragem com base na informação do cabeçalho dos pacotes, endereços de origem e destino, portas de origem e destino.
    - Os campos que podem ser utilizados pelo *firewall* são as *flags* (em que o sentido da conexão é verificado com base SYN, SYN-ACK e ACK), protocolo, endereço de origem e endereço de destino.
    - Não é possível filtrar os pacotes provindos do protocolo *User Datagram Protocol* - UDP, pois o UDP não é orientado à conexão.
    - Simples, fáceis, baratos de ser implementado, assim os roteadores que trabalham com *gateway* têm essa facilidade.
    - Menor grau de segurança, pois os pacotes podem ser facilmente ser falsificados ou criados para que passem pelas regras de filtragem específica.
    - Limitados com relação à fragmentação, validação apenas do primeiro pacote fragmentado

Regra	End ORI; Port ORI	End Dest; Port DEST	Ação
1	IP rede Int; Port Alta	QQuer End:80(http)	P
2	QQuer End:80(http)	IP rede Int;Port Alta	P
3	QQuer End; QQuer Port	QQuer End; QQuer Port	N

Tabela 2: Regras de Filtragem do filtro de pacotes

Na tabela de regras acima a regra 1 permite aos usuários da rede interna a requisição de uma página web. Uma porta alta, portas acima do número 1024, é usada pelo cliente de forma aleatória, para iniciar a requisição na porta 80 de um servidor de páginas. Uma vez a conexão estabelecida, a resposta da requisição é recebida pelo cliente, passando pela regra 2 do filtro de pacotes. A regra 3, como qualquer última regra no *firewall* deve ser uma regra padrão, negar qualquer tentativa de requisição, a não ser as expressamente liberadas anteriormente. O canal aberto pela regra 2 pode ser explorado para que o ataque de *backdoor* (porta dos fundos) seja utilizado. Neste caso o atacante inicia uma conexão usando a porta 80, tendo como destino a porta alta aberta, o retorno da regra 1.

Para que seja apresentada uma solução completa e elegante para o *firewall* de filtro de pacotes, pode-se mencionar o *firewall* de filtragem de pacotes baseados em estado.

- **Filtro de Pacote Baseado em Estado:** Pode ser chamado de dinâmico, toma decisões de filtragem tendo como referência 2 elementos:
  - Uma tabela de estados, que armazena os estados de todas as conexões.
  - Filtragem das informações dos cabeçalhos dos pacotes de dados.

Os *firewalls* de inspeção com estado (S*tateful Inspection Firewalls*) tomam as decisões de filtragem tendo como referência dois elementos: as informações dos cabeçalhos dos pacotes de dados, como no filtro de pacotes; e uma tabela de estados, que guarda os estados de todas as conexões. O *firewall* trabalha verificando somente o primeiro pacote de cada conexão, de acordo com as regras de filtragem. A tabela de conexões que contém informações sobre os estados das mesmas ganha uma entrada quando o pacote inicial é aceito, e os demais pacotes são filtrados utilizando-se as informações da tabela de estados [58].

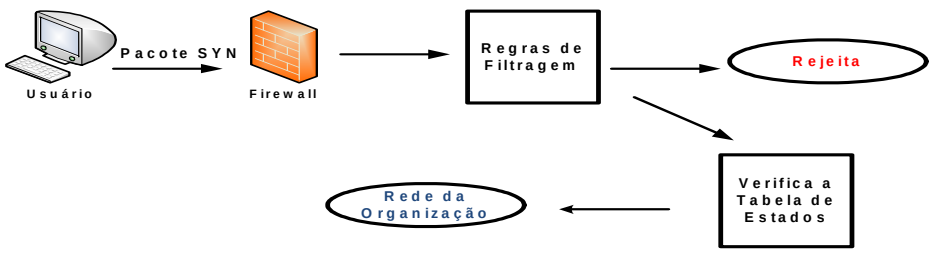

Figura 8: Entrada do pacote SYN pelo *firewall* baseado em estado

Na figura 8 o pacote de sincronismo SYN é verificado no *firewall* primeiramente na regra de filtragem, se o pacote tiver permissão para o acesso, ele é direcionado para a tabela de estados, verifica se já existe entrada do pacote, em caso negativo o pacote é registrado na tabela de estados e encaminhado para seu destino, caso afirmativo ele é atualizado na tabela de estados e segue seu curso até o destino. Se o pacote não tiver permissão na regra de filtragem ele é descartado.

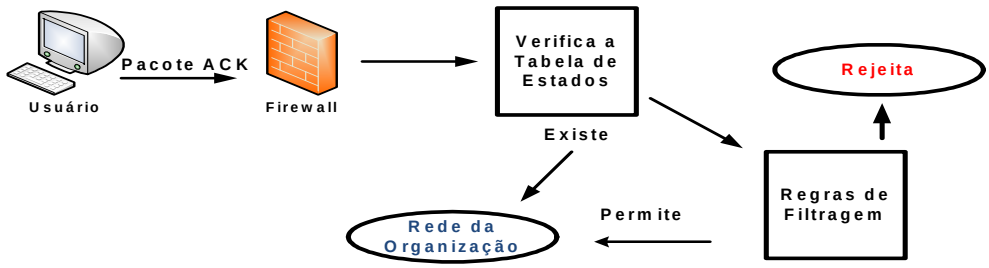

Figura 9: Entrada do pacote ACK pelo *firewall* baseado em estado

A figura 9 identifica-se o pacote *acknowledge* – ACK passando pelo *firewall*. Ao contrário dos pacotes SYN o pacote ACK conforme figura 9, passa pela tabela de estados em primeiro lugar para verificar se já existe uma entrada, caso negativo o pacote é cadastrado na tabela de estado e encaminhado para as regras de filtragem para identificar suas possibilidades, em caso de bloqueio ou inexistência da regra o pacote é descartado, ao contrário o pacote é encaminhado ao seu destino. Caso o pacote tiver uma entrada ele é registrado e encaminhado para seu destino.

No caso do *firewall* filtro de pacote baseado em estado, não é necessário criar a regra de retorno, na qual é fornecida a abertura da porta dos fundos, pois a filtragem baseada em estado armazena em sua tabela tanto a origem quanto o destino do pacote facilitando o sentido reverso da conexão.

- ***Proxy* –** Os *firewall* baseados na tecnologia *proxy* trabalham até a camada de aplicação para filtragem específica de conteúdo de página, palavra ou categoria além da filtragem de pacotes para as portas específicas. Sua principal característica é seu funcionamento como *relay*, um agente permitindo que todo o acesso da rede interna para a rede externa passe em seu *firewall*. Pode-se assim, esconder os verdadeiros endereços privados.

- ***Firewall* e suas Funcionalidades –** As quatro primeiras funcionalidades (filtros, *proxies*, *bastion hosts*, zonas desmilitarizadas) fazem parte do *firewall* clássico e as três funcionalidades restantes (*Network Address Translation* - NAT, *Virtual Private Network* - VPN, autenticação/certificação) foram inseridas no contexto, devido à evolução natural das necessidades de segurança. O balanceamento de cargas e a alta disponibilidade também possuem uma grande importância, principalmente porque todo o tráfego entre as redes deve passar pelo *firewall* [40].

  Dentre diversas funcionalidades de um *firewall* podemos mencionar (adaptado de [40]):

  - Filtros – filtragem de pacotes de sua origem e destino, permitindo ou negando acesso em portas específicas e registrando todas as conexões que por ele trafega.

  - *Proxies* – É um sistema que atua como *gateway*, atendendo às requisições de uma rede interna e analisando a possibilidade de conectividade dependendo das políticas de acesso a ele implementadas.

  - *Bastion hosts* – São equipamentos (servidores), onde são instalados os serviços a serem oferecidos para a internet ou empresas externas a corporação. É importante ressaltar que as configurações exercidas nesse equipamento devem predestinar as portas específicas de acesso, para minimizar o comprometimento com a segurança no acesso a esse equipamento. Como os serviços são oferecidos para fora da corporação, estes equipamentos devem ser alocados em uma DMZ.

  - DMZ – Zona desmilitarizada é um perímetro dentro da corporação que deve ficar disponível para acessos externos, isolado do acesso interno. Essa segmentação faz com que, caso algum equipamento dessa rede desmilitarizada (um *bastion host*) seja comprometido, a rede interna continue intacta e segura.

  - NAT – Faz a tradução de endereços públicos (válidos na internet) para endereços privados ou vice versa. Apesar de sua principal existência ser em relação à escassez de endereços IP no mundo da Internet, a NAT tem um papel importante na segurança da informação, que é esconder os endereços da rede

interna e conseqüentemente sua topologia, dificultando eventuais ataques externos.

- VPN – No qual veremos com maiores detalhes a frente, ela faz uma virtualização privada entre as redes de interesse de acesso. Utiliza mecanismos de criptografia para garantir a sigilo e a integridade na tramitação da informação.

- Autenticação – No *firewall* a autenticação é o processo de provar uma identidade e a decisão sobre quais privilégios resultam essa identidade. A autenticação dos usuários pode ser baseada nos endereço IP, senhas, certificados digitais, *token*, *smartcards* ou biometria.

Com a necessidade cada vez maior de segurança da informação, decorrente dos tipos de ataques são inseridos no *firewall* outras funcionalidades conforme mencionado abaixo:

- QoS – Qualidade de Serviço prioriza uma banda no canal de comunicação para um determinado serviço trafegar sem interrupção e filas concorrentes com outros pacotes.

- IDS / IPS – São sistemas de detecção e prevenção de intrusos. A detecção provê uma segurança ativa identificando e alertando. Já a prevenção atua de maneira proativa, identificando e tomando ações conforme o que for pré-configurado.

2.3.3 Arquiteturas de Firewall

O *firewall* pode ser introduzido dependendo da necessidade da organização. A arquitetura depende da topologia da rede existente para compor a usabilidade de suas diversas funcionalidades e atender a política de acesso da corporação.

Os perímetros devem ser devidamente conhecidos para prover uma segmentação ideal. Dentre algumas arquiteturas vamos mencionar a arquitetura do *firewall* cooperativo. Pode-se identificar o conjunto de necessidades de uma organização com matriz e filiais com aplicabilidade de um domínio único. A exposição do *firewall* cooperativo aplica-se com base

ao conjunto de arquiteturas embutidas para tratar a segurança da informação em diversos aspectos.

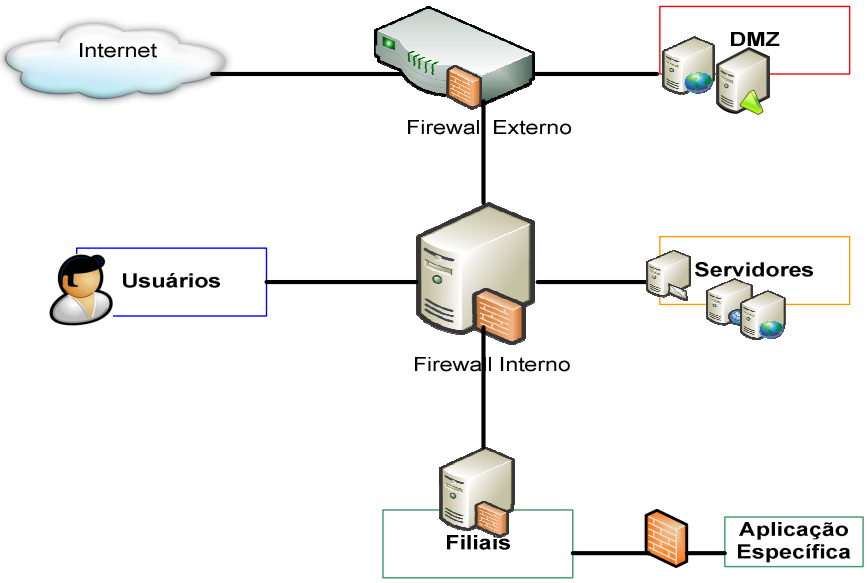

Figura 10 - *Firewall* Cooperativo

Observa-se na figura 10, o *firewall* externo, no qual se pode mencionar *firewall* de borda, utilizando da tecnologia de filtragem de pacotes baseado em estado. Nesse segmento o *firewall* de borda delimita o acesso para Internet, da DMZ e da rede interna. A partir da segregação dos perímetros da rede externa e da rede interna, verifica-se a defesa de adversidade e profundidade. Na rede interna aplica-se o *firewall proxy* para atuar como um *gateway* aos usuários e segmentar as filiais da matriz e dos servidores, onde somente as portas específicas das aplicações da rede interna poderão ser acessadas nesses servidores. Na filial utiliza-se o *firewall proxy* para replicar o cache, minimizar requisições no meio e segregar a segurança das localidades. Por fim observa-se um *firewall* para tratar de aplicações específicas dentro das filiais, podendo este atribuir uma DMZ de uma aplicação que necessite ser compartilhada com outra empresa da localidade em um canal dedicado a isto.

[17] afirma que se uma organização possui múltiplas conexões de Internet, um *firewall* precisa ser colocado em cada uma delas, e todos os *firewalls* da organização precisam estar configurados para fortalecer a política de segurança da corporação. Além do mais, o *firewall* deve ele próprio ser protegido. Isto é:

- Todo o tráfego que entrar na organização precisa passar pelo *firewall*.

- Todo o tráfego que sair da organização precisa passar pelo *firewall*.
- O *firewall* implementa uma política de segurança e rejeita qualquer tráfego que não aderir à política.
- O *firewall*, por si próprio, é imune a ataques de segurança.

Em relação ao desempenho é importante que o equipamento seja devidamente dimensionado para suas funcionalidades em seu processador, memória RAM, placas de rede, barramento.

Dentre diversas aplicabilidades, o *firewall* é uma ferramenta imprescindível à segurança digital, tanto sendo aplicado na borda com a internet, quanto nos perímetros internos das corporações. Atualmente pode-se considerar o *firewall* de borda como um mecanismo de segurança multifuncional. Dentre suas diversas atividades, que podem ser atribuídas conforme mencionado acima, outras podem ser mencionadas: antivírus, analisador de tráfego, identificação de *logs* e repórteres. O *firewall* da atualidade pode ser considerado como um dispositivo de *Unified Threat Management* - UTM que combina em uma única solução diversas atribuições de segurança, possibilitando administrações de políticas corporativas através de um único console, oferecendo assim controle e visibilidade completos em toda a empresa.

Diante deste cenário, nota-se que o *firewall* não pode mais ser considerado apenas um muro, mas sim uma parte da defesa ativa de qualquer organização, que é a idéia principal do *firewall* cooperativo, ou seja, mais uma forma de defesa, mas não a única e infalível.

2.4 VPN

Considera-se uma VPN a conexão de uma rede privada para uma rede pública ou vice-versa utilizando métodos criptográficos para garantir autenticidade e integridade no canal de comunicação e para atribuir confidencialidade na informação trafegada. O túnel VPN agrega um canal virtual para assegurar o sigilo da informação.

Explica [54] que com a rede privada X rede pública surgiu um novo paradigma: o uso da rede pública como se fosse uma rede privada com segurança, criando-se, assim, rede privada virtual. O termo virtual entra, porque depende de uma conexão virtual, temporária, sem presença física no meio. Essa conexão virtual consiste em troca de pacotes, sendo roteados entre vários equipamentos. Essa conexão pode ser observada na figura abaixo:

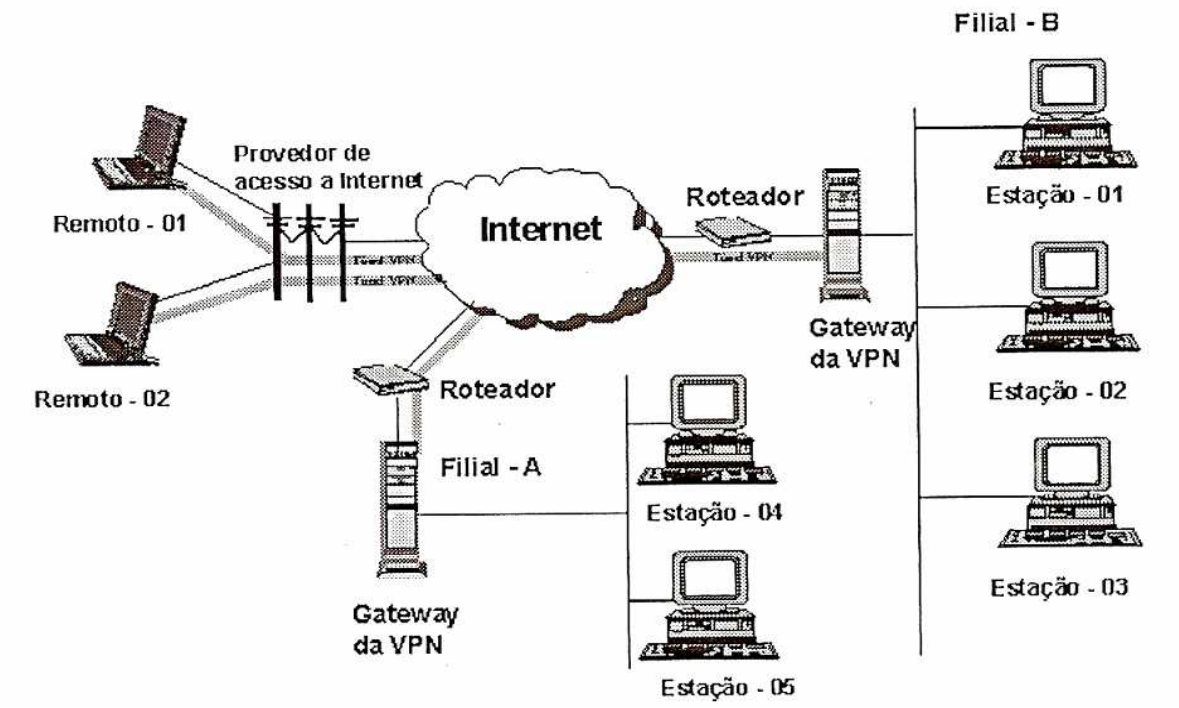

Figura 11 – VPN – Situações Mistas [54]

A figura 11 demonstra que a topologia aplicada às empresas maiores, com duas ou mais filiais, ou entre empresas permite acesso de usuários remotos a determinados sites ou filiais.

Os usuários remotos fazem uma conexão discada para um provedor de acesso à Internet, assim é possível estabelecer uma VPN entre os *gateways* da VPN que protegem uma filial. Cabe ao *gateway* estabelecer a permissão ou negação dos usuários remotos ou de outra filial. Cabe ao *gateway* estabelecer a permissão ou negação dos usuários remotos ou de outra filial para dentro da rede protegida por esse *gateway*.

Neste exemplo, o usuário Remoto-01 pode fechar uma rede virtual com o *gateway* da Filial-B, mas não poderá acessar dados protegidos pelo *gateway* da Filial-A. Por outro lado, o usuário Remoto-02 só poderá estabelecer uma rede com a Filial-A e não com a Filial-B. Pode-se permitir, por exemplo, que a Filial-A tenha uma rede com a Filial-B ou que o usuário Remoto-02 posse estabelecer um túnel entre a Filial-B.

De acordo com [48], o termo VPN esteve associado no passado a serviços remotos de conectividade, como a rede de telefonia pública comutada (RTPC) ou os PVCs (*Permanent Virtual Circuits/Channel*) do *Frame Relay*, mas hoje já está associado ao uso de infra-estruturas públicas de comunicação para simular redes privadas IP. Antes da utilização deste

novo conceito de VPN, as corporações gastavam grandes quantias de recursos para montar complexas redes privadas, chamadas *Intranets*, entre suas diversas unidades. Essas redes utilizavam serviços caros, como linhas privadas, *Frame Relay* e ATM para incorporar filiais à rede interna da companhia. Para escritórios ou usuários móveis, eram utilizados servidores de acesso remoto (com modems e linhas de discagem gratuita como o 0800) ou conexões RDSI (Rede Digital de Serviços Integrados). Ao mesmo tempo, empresas pequenas ou médias, que não têm recursos para manter conexões dedicadas tão caras, utilizavam serviços de comutação de circuito de baixa velocidade.

Nesse contexto, as VPN aparecem para superar o problema de segurança. Usando protocolos de tunelamento e procedimentos de ciframento, a integridade e autenticidade dos dados são garantidas. Como as operações ocorrem sobre uma rede pública, a implementação e manutenção de uma VPN custa significativamente menos do que os serviços dedicados descritos no primeiro parágrafo.

De acordo com [15], uma VPN poderia ser definida como um conjunto de computadores protegidos da Internet via um *firewall*, se eles estivessem realmente conectados. Essas máquinas eram mais seguras contra ataques externos, porque o dinheiro, a perícia e a paranóia estavam todos concentrados na manutenção do *gateway* seguro. Dessa forma, os sites com múltiplas localizações tinham de ser interligados de forma privada, uma vez que a Internet não oferecia serviços suficientemente seguros para interligar localizações. Cada site era protegido por um *firewall*, mas não havia maneira alguma para máquinas em diferentes locais se comunicarem com segurança. Devido ao *firewall*, era improvável que elas pudessem se comunicar de qualquer maneira.

As redes privadas virtuais ampliam os limites de um domínio protegido por meio da criptografia. Há três tipos de VPNs. O primeiro permite a filiais remotas compartilhar um perímetro de segurança e até mesmo um espaço de endereçamento. O segundo é utilizado porque não querem abrir suas redes inteiras umas para as outras, mas desejam ter alguns serviços dos compartilhados - essas VPNs implementam uma DMZ. O terceiro tipo permite que os remotos se conectem a seus locais de trabalho a partir de casa, do hotel ou café-bar [15].

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das

comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Em 1992, foi criado um subgrupo dentro do IETF composto de engenheiros de segurança do mesmo, representante de várias empresas como: Checkpoint, Cisco, IRE, Microsoft, Netrex, IBM, entre outros. Esse subgrupo propôs o conceito do IPSec, que é um padrão para se estabelecer uma VPN entre dois pontos independentemente do fabricante ou da aplicação envolvida.

Deve ser notado que a escolha, implementação e uso destes protocolos não é algo trivial, e várias soluções de VPN inseguras são distribuídas no mercado. Advertem-se os usuários para que investiguem com cuidado os produtos que fornecem VPNs. Por si só, o rótulo VPN é apenas uma ferramenta de marketing.

Um problema enfrentado na VPN pelos provedores de acesso à Internet está na quantidade de endereços IPs que ele pode disponibilizar para seus clientes. Com o crescimento da Internet, a escassez de endereços na versão IPv4 ocorre a necessidade de prover um método no qual os endereços podem ser traduzidos para ser representados um a um ou de um conjunto de endereços por um. Caso o cliente queira um link dedicado entre a sua rede e o provedor de acesso, o provedor necessita de algo que permita com que ele economize endereços IPs e que atenda às necessidades dos seus clientes. Já numa pequena empresa tentando compartilhar o modem e a linha telefônica, o problema é um pouco mais complicado; nesse caso o único meio de acesso à Internet é uma conta em um provedor de acesso. Essas contas de acesso dão direito a apenas um endereço IP, que o computador recebe quando disca para o provedor, e o pior, este endereço IP muda a cada conexão que for feita, assim sendo, será necessário fazer com que este endereço IP seja compartilhado por todas as máquinas da rede local.

Estes IPs são endereços de Classe A, B ou C. Para resolver esses problemas, a saída se baseia numa técnica chamada NAT - tradução de endereço de rede. O NAT é apenas uma série de tarefas que um *gateway* ou equipamento equivalente deve realizar para converter endereços entre redes distintas. O NAT estático faz a tradução de endereços IP de um a um conforme figura 12.

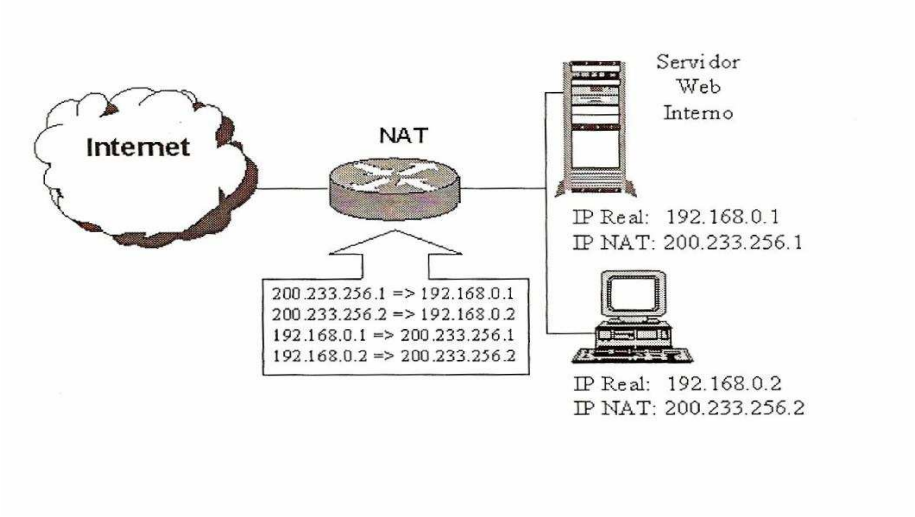

Figura 12 – NAT Estático [54]

O NAT *Hide* conforme figura 13 faz a tradução de vários endereços para um endereço.

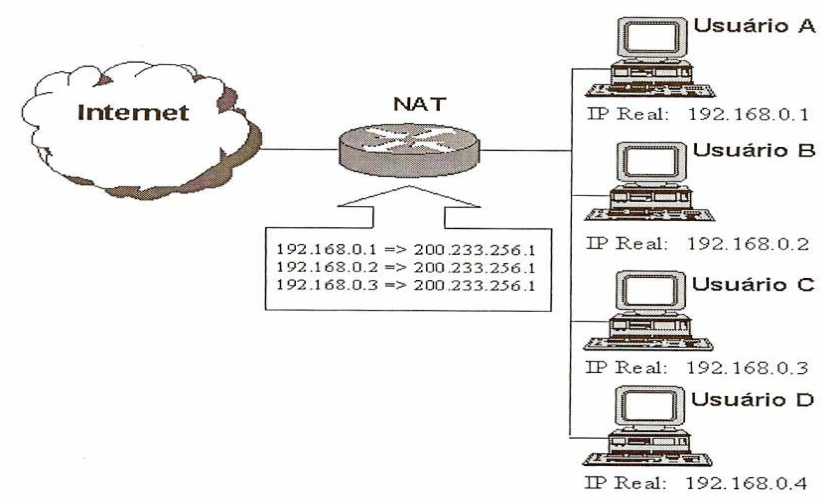

Figura 13 – NAT *Hide* [54]

Um aspecto que se pode mencionar em relação a NAT é a composição de NAT sobre NAT ou a fusão da utilização da NAT *Hide* com a NAT estática. A variação dos métodos de aplicabilidade da NAT é utilizada quando há necessidade de esconder o endereço da rede privada de 2 pontos distintos dentro da mesma rede ou quando há uma aplicação específica atrás de um segundo *firewall* dentro da mesma organização, conforme figura 14 abaixo.

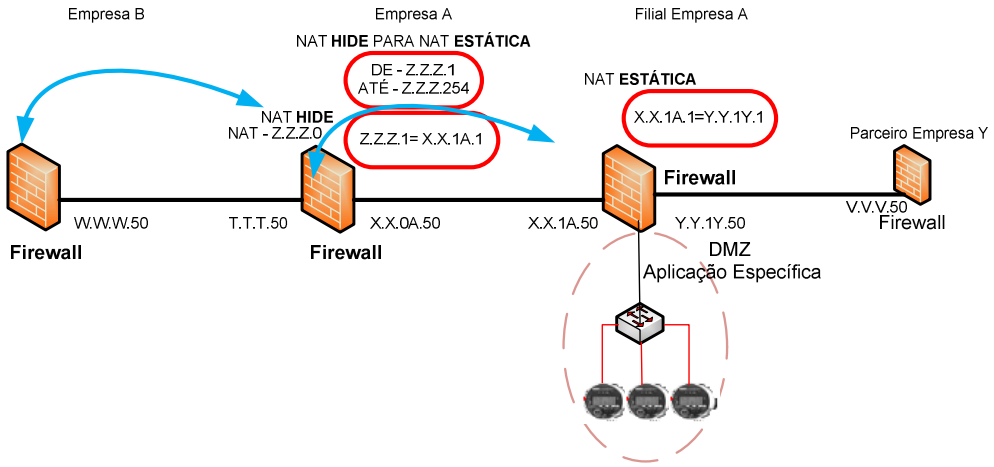

Figura 14 - NAT sobre NAT

Observa-se na figura 14 uma filial da Empresa A com suas aplicações específicas. Tanto a Empresa B quanto o parceiro Empresa Y necessitam acessar a aplicação específica. Conforme apresentado o endereçamento interno da Empresa A e de sua filial não aparecem para nenhuma das empresas externas. O acesso provindo da Empresa B, conhece somente o endereço de NAT *Hide*, rede Z.Z.Z.0, com a máscara 255.255.255.0, que indica 254 possibilidades de *hosts*, que posteriormente é transformado em NAT estática para os endereços internos de *host* X.X.1A.1 até X.X.1A.254. Sua próxima tradução refere-se de NAT estática X.X.1A.1 para Y.Y.1Y.1 o destino. Por outro lado a Empresa Y vai conhecer somente os endereços de sua própria rede, os endereços V e os endereços da DMZ Y.Y.1Y.1, mantendo a salvaguarda dos endereços da rede X.X.0.0.

Outro aspecto que podemos considerar é a necessidade de proteção na tramitação da informação de uma aplicação específica na rede interna dos seus próprios usuários. A topologia e a disponibilidade geográfica de cada organização devem ser avaliadas antes de qualquer definição em relação à segurança da informação. Para proteger a informação a ser trafegada de um ponto distinto da rede interna até uma organização externa, pode-se utilizar o método de VPN sobre VPN conforme figura 15.

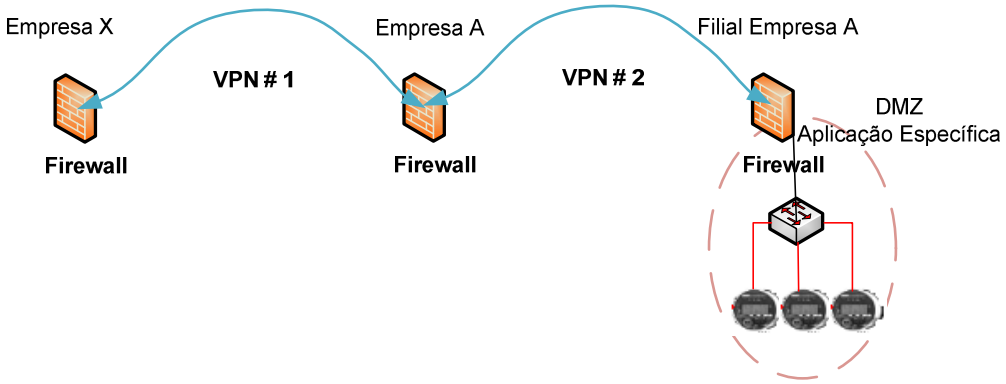

Figura 15 - VPN sobre VPN

Observa-se na figura 15 a constituição da VPN entre a Empresa X e a Empresa A. Se existir somente a VPN entre as Empresas X e A, os usuários da empresa A podem atacar os dados trafegados dentro da organização. Com a inserção da VPN 2 os dados podem tramitar dentro da organização com maior segurança garantindo a integridade, autenticidade e confidencialidade desde sua origem até seu destino. Os dados de uma VPN 1 são inseridos na VPN 2. Para compatibilidade em seu funcionamento é importante que as VPN 1 e 2 tenham os mesmos parâmetros de configuração, fazendo assim o reconhecimento dos padrões adotados desde sua origem até seu destino.

Dentro da abordagem de VPN, a segurança é a sua mais importante função, leva-se em consideração o meio, os pontos autorizados para criação do túnel entre a internet, e as redes públicas ou privadas para transferência da informação. A VPN baseia-se no método de tecnologia de tunelamento, processo de encapsular um protocolo dentro de outro. A VPN utiliza técnicas de criptografia antes de encapsular o pacote de modo a tornar ilegível a informação. Dentre os protocolos de tunelamento que podem ser utilizados, faz-se atribuição aos padrões IPSec que trabalham na camada de rede e permitem que os pacotes IP sejam cifrados e encapsulados com o cabeçalho adicional.

2.5 IPSec

O IPSec foi desenvolvido para atender as demandas do IPv6, mas foi adaptado para poder suprir as deficiências de segurança do IPv4. Surgiu em 1995, como uma resposta à necessidade de segurança e o controle do tráfego não autorizados da rede; é um padrão da

IETF. Vem se tornando o verdadeiro padrão utilizado pelos túneis VPN. Para sua utilização é necessário que os equipamentos cliente ou *gateway* tenham implementado o protocolo na pilha TCP/IP.

Os serviços de segurança do IPSec são oferecidos por meio de dois protocolos de segurança, o *Authentication Header* (Cabeçalho de Autenticação - AH) e o *Encapsulation Security Payload* (Encapsulamento Seguro do Dado - ESP). Os protocolos AH e ESP fazem parte da arquitetura básica IPSec e, por questões de garantia de interoperabilidade, estabelecem que todas as implementações IPSec suportem alguns algoritmos predefinidos [53], tais como:

- Criptografia

- DES, Blowfish, 3-DES, CAST, AES, SERPENT, TWOFISH etc.

- Autenticação

- HMAC, MD5, SHA-1, SHA-2.

Dessa forma, o IPSec “implementa ciframento e autenticação na camada de rede, fornecendo uma solução de segurança fim-a-fim”. Ele pode ser implementado tanto nos roteadores, quanto no sistema operacional, assim os dispositivos não precisam sofrer alterações para tornarem-se seguros.

Destacam-se alguns aspectos dos protocolos citados ESP e AH:

- O ESP provê autenticação, confidencialidade dos dados e integridade da mensagem. O campo de autenticação do ESP contém um ICV que é acrescido à assinatura digital calculada sobre a parte restante do ESP. O ICV tem tamanho variável dependendo do algoritmo de autenticação utilizado. A autenticação é calculada no pacote ESP depois da ciframento estar concluído. O padrão atual do IPSec utiliza a HMAC (assinatura assimétrica) que é validada por algoritmos SHA-1 e MD5. O ICV aceita exclusivamente a assinatura assimétrica. O equipamento de origem encripta o controle dos dados do usuário e insere o resultado no campo de autenticação do ESP e o equipamento de destino confere se o dado foi alterado e se o endereço de origem é válido.

- O AH provê a autenticação e integridade dos pacotes entre origem e destino, mas não a confidencialidade. O AH é utilizado para serviços de autenticação. O AH pode operar isolado, em conjunto com o ESP ou embutido quando o modo de tunelamento é usado. A autenticação suprida pela AH difere da ofertada pelo ESP na medida em que este não protege os endereços de IP de origem e destino. Os serviços do AH mantém a privacidade de todo o pacote, inclusive do endereço IP de origem. O AH não protege todas as informações do *header* externo do IP porque os endereços podem variar durante a propagação do pacote pela rede e não há uma forma de antecipar qual o comportamento dos *routers* de trânsito. O AH protege tudo o que não pode ser modificado durante o transporte do pacote entre origem e destino [32].

[48] informa que o IPSec combina diferentes e diversas tecnologias para prover uma melhor segurança, como um mecanismo de criptografia de chave pública para assinar as trocas de chave de *Diffie-Hellman*, garantindo assim a identidade das duas partes e evitando ataques do tipo *man-in-the-middle* (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação); algoritmos de ciframento para grandes volumes de dados, como o DES; algoritmos para cálculo de *hash* com utilização de chaves, como o HMAC, combinado com os algoritmos de *hash* tradicionais como o MD5 ou SHA, autenticando os pacotes e certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

O IPSec fornece dois modos de operação, que são, segundo [40]:

- Modo de transporte – modo nativo, no qual há a transmissão direta dos dados protegidos pelo IPSec entre os *hosts*. A codificação e a autenticação são realizadas no *payload* do pacote IP, e não no cabeçalho IP, conforme demonstra a figura 16. É utilizado em dispositivos que incorporam o IPSec na implementação do TCP/IP, como no caso de *software*-cliente IPSec. Algumas modalidades que utilizam o modo de transporte são o *gateway-to-gateway* VPN, *client-to-gateway* VPN e o *remote-acess* VPN.

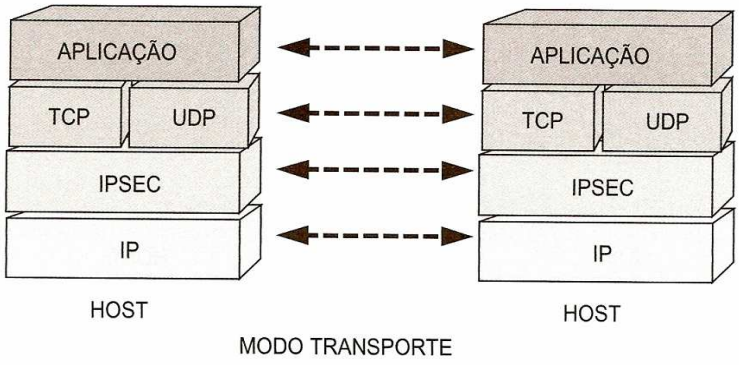

Figura 16 – No modo transporte, o IPSec é incorporado na pilha TCP/IP [40]

- Modo de tunelamento – é geralmente utilizado pelos *gateways* IPSec, que manipulam o tráfego IP gerado por *hosts* que não aceitam o IPSec, como na modalidade que pode ser observada na figura 17. O *gateway* encapsula o pacote IP com a criptografia do IPSec, incluindo o cabeçalho de IP original. Ele, então, adiciona um novo cabeçalho IP no pacote de dados e o envia por meio da rede pública para o segundo *gateway*, no qual a informação é decifrada e enviada ao *host* do destinatário, em sua forma original.

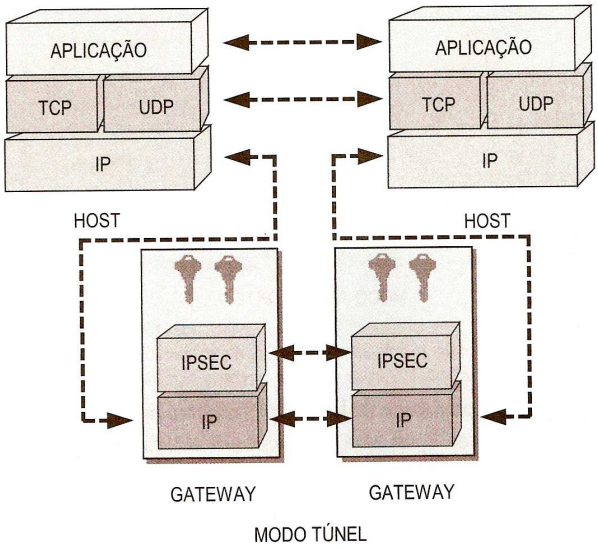

Figura 17 – No modo 'túnel', o IPSec é implementado no *gateway* [40]

A diferença da utilização do modo de tunelamento é a aplicabilidade em empresas, pois todo o pacote original é colocado dentro de um novo pacote, sendo gerados dois novos cabeçalhos, um IP e outro ESP. Conforme figura 18 o túnel sendo feito entre *gateway*s, como roteadores ou *firewall*, os endereços de origem e de destino do novo cabeçalho serão os dos *gateway*s e os endereços dentro do pacote criptográficos serão os dos hosts atrás dos *gateway*s.

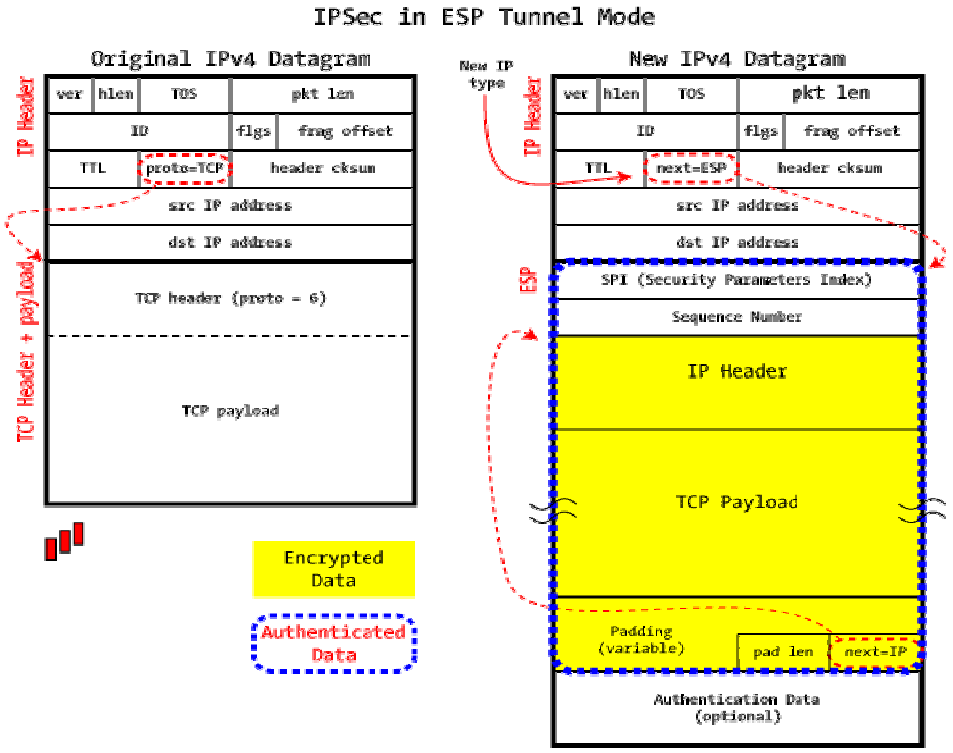

Figura 18 – Modo túnel IPSec sobre ESP [59]

De acordo com [53], um dos mais importantes conceitos do IPSec é o de *Security Association* (Associação de Segurança - SA). Uma SA define os tipos de medidas de segurança que devem ser aplicadas aos pacotes baseados em quem está enviando os pacotes, para onde eles estão indo e que tipo de dados eles estão conduzindo. O conjunto de serviços de segurança oferecidos pela SA depende do protocolo de segurança, de suas opções escolhidas e do modo no qual a SA irá trabalhar.

Uma SA é identificada por três parâmetros: endereço IP de destino, identificação do protocolo de segurança (valor 51 para AH e o valor 50 para ESP) e o índice de parâmetro de segurança (*Security Parameter Index* - SPI). O SPI é um número que identifica uma SA, sendo definido durante a negociação que antecede o estabelecimento desta. Assim, todos os membros de uma SA devem conhecer o SPI correspondente e usá-lo durante a comunicação [53].

O gerenciamento de chaves definido pelo IPSec é realizado pelo IKE, que tem por base o protocolo ISAKMP (Internet *Security Association and Key Management Protocol*) e parte da implementação Oakley e SKEME (*Secure Key Exchange Mechanism*) como métodos de troca de chave, a qual se negocia dinamicamente uma SA [40].

Uma SA pode ser configurada manualmente por um administrador de segurança em cada *gateway* podendo ser negociada dinamicamente por meio de um protocolo de gerência de chaves como o IKE. Essa negociação dinâmica é necessária por várias razões: primeiro, porque não se sabe a priori quando será preciso negociar uma SA para estabelecer o túnel VPN e, segundo, porque uma associação de segurança não deve ter um tempo de vida infinito, ou seja, é recomendável que se troque a SA de tempos em tempos e, conseqüentemente, as chaves de criptografia. Quanto mais tempo se utilizar a mesma chave de criptografia, maiores serão as chances de algum invasor descobri-la [54].

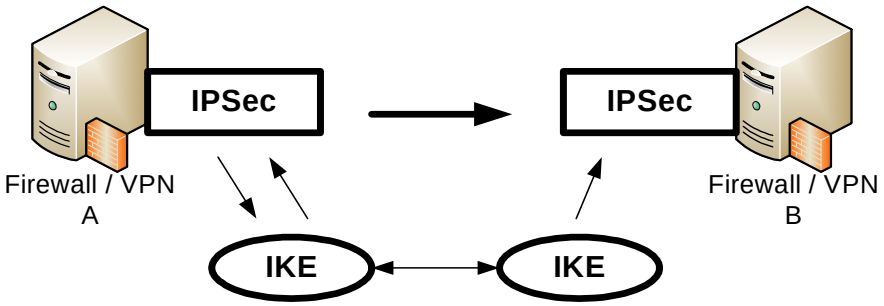

Figura 19 – Negociação de Chaves

A figura 19 demonstra que o ISAKMP define duas fases na negociação da associação de segurança. A 1ª etapa é entre as duas entidades IKE. Nessa fase, as duas entidades concordam em como proteger a comunicação. A 2ª etapa uma associação segura para o IPSec, é negociada entre as entidades. Como o canal entre as entidades já foi estabelecido na fase 1, essa etapa é mais rápida.

Segundo Rappaport [48] a autenticação e a troca de chaves criam a SA entre os IKEs, um túnel seguro entre os dois dispositivos. Um dos lados do túnel oferece um conjunto de algoritmos, e o outro deve aceitar uma das ofertas ou rejeitar a conexão. Quando os dois lados concordam com os algoritmos que serão utilizados, eles devem produzir as chaves que serão utilizadas pelo IPSec no AH ou ESP, ou os dois. A chave compartilhada pelo IPSec é diferente da compartilhada pelos IKEs; ela pode ser obtida pelo método de Diffie-Hellman novamente, para garantir o sigilo, ou atualizando a criada pela troca original para gerar a SA IKE, fazendo o *hash* com outro número aleatório. O primeiro método, apesar de fornecer maior segurança, é mais lento. Após esse passos, a SA IPSec é estabelecida.

[40] afirma que o IKE fornece três modos de troca de informações e estabelecimentos de SA:

- *Main Mode*: corresponde à fase do IKE e estabelece o canal seguro para a fase seguinte, gerando o IKE SA.

- *Aggressive Mode*: corresponde também à fase 1 do IKE, porém é mais simples e rápido que o *main mode*, pois não fornece a proteção das identidades das entidades que estão se comunicando. Isso ocorre porque as identidades são transmitidas juntamente com as solicitações de negociação, sem que um canal seguro seja criado antes, estando, assim, susceptíveis a ataques do tipo *man-in-the-middle.*

- *Quick Mode*: corresponde à fase 2 do IKE e é a comunicação estabelecida para a negociação do SA.

ISAKMP define como as duas entidades instituirão um canal de comunicação seguro entre si, fazendo com que os participantes se autentiquem entre si, trocando informações de chaves e negociando serviços de segurança. Entretanto, não especifica como a autenticação é feita ou quais as chaves serão geradas, ou seja, é definido um caminho seguro, ou veículo de transporte, deixando o conteúdo para que outro processo especifique. Uma mensagem ISAKMP contém um cabeçalho e um ou mais dados ISAKMP, formando pacotes UDP (porta 500), como mostra a figura 20.

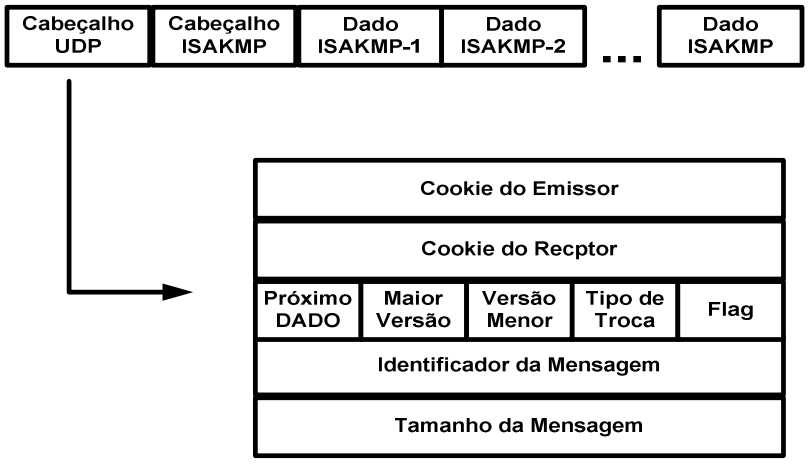

Figura 20 - Formato da mensagem ISAKMP [54]

Desse modo, no Protocolo de gerenciamento de chaves (Internet *Key Management Protocol* - IKMP), o IPSec assume que as SAs já existem para ser utilizadas, mas não especifica como elas serão criadas. O IETF decidiu dividir o processo em duas partes: o IPSec

fornece o processamento dos pacotes, enquanto o IKMP negocia as associações de segurança. Após analisar as alternativas disponíveis, o IETF escolheu o IKE como o método padrão para configuração das SAs para o IPSec.

Releva-se a importância do IPSec em atendimento a deficiência de segurança no IPv4 e para o fornecimento de autenticação, integridade e privacidade das informações transitadas através de redes IP. Conforme o IPSec volta-se para ciframento da camada de rede é definido em seu formato o cabeçalho de autenticação para fornecer a integridade entre a origem e destino do pacote e o encapsulamento seguro da informação. O IPSec tem como objetivo tratar as ameaças na camada de rede. Utiliza-se o IKE para criar um túnel seguro entre duas entidades, que pode ser obtido pelo método *Diffie-Hellman*, que garante o sigilo para depois negociar as SA. Entretanto pode-se considerar o IPSec como um conjunto de padrões para compor um sistema de tramitação segura em redes IP.

2.6 Auditoria

Segundo [12], a auditoria pode ser definida como sendo o levantamento, estudo e avaliação sistemática das transações, procedimentos, operações, rotinas e demonstrações contábeis de uma entidade por meio de testes regulares nos controles internos específicos de cada organização. Ou ainda pode ser vista como atividade de exame e avaliação de procedimentos, processos, sistemas, registros e documentos, com o objetivo de aferir o cumprimento dos planos, metas, objetivos e políticas da organização. É utilizada também como atividade de análise e emissão de parecer sobre a conformidade de dados contábeis, financeiros e operacionais.

Quanto ao vínculo com a empresa, a auditoria pode ser externa ou interna; quanto aos objetivos do exame pode ser operacional, de sistemas, contábil e financeira ou de gestão, dentre outras, e quanto ao campo de atuação pode ser de natureza governamental ou privada.

A auditoria é importante para as empresas no atendimento de suas metas proporcionadas por uma política sólida e estrutura de maior aproveitamento de suas potencialidades. Na medida em que é uma ferramenta de constatação de irregularidades e padronização de procedimentos, torna-se também ferramenta de segurança [12].

A auditoria em ambiente de tecnologia de informação não muda a formação exigida para a profissão de auditor, apenas percebe que as informações até então disponíveis em

forma de papel são agora guardadas em forma eletrônica e que o enfoque da auditoria teria que mudar para se assegurar de que essas informações em forma eletrônica sejam confiáveis antes de emitir sua opinião [35].

A filosofia de auditoria em tecnologia de informação está calcada em confiança nos controles internos que visam confirmar se os controles internos foram implementados e, caso existam, se são efetivos.

As atividades de auditoria de tecnologia de informações, além de tentarem utilizar recursos de informática para auditar o próprio computador, também visam automatizar todos os processos de auditoria. Como em qualquer outra atividade, as empresas de auditoria também buscam um diferencial competitivo. Entre outros objetivos, consideram-se [35]:

a. Melhorar a eficiência e reduzir os custos;
b. Melhorar a qualidade do trabalho de auditoria, reduzindo, assim, os níveis de risco de auditoria;
c. Atender às expectativas dos clientes, que esperam de seus auditores o mesmo grau de automatização que utilizam em seu próprio negócio;
d. Preparar-se para a globalização dos negócios, que vem exigindo uma globalização dos auditores;
e. Manter-se entre as maiores e mais reconhecidas pelo mercado

Os benefícios da automação compreendem, entre outros:

- Treinamento de pessoal e superação de resistências à tecnologia;
- Decisão sobre quais tarefas devem ser automatizadas primeiro;
- Avaliação, escolha e implantação de softwares e hardwares;
- Gerenciamento dos arquivos eletrônicos: dispositivos de segurança e *backup*;
- Disponibilização de equipamentos para toda a equipe de auditores, podendo trabalhar em redes;
- Instalação e manutenção de uma malha de comunicações;
- Maior transferência de conhecimento entre os membros da equipe e entre trabalhos de equipes diferentes;
- Independência das limitações impostas pelos arquivos de auditoria em papel;
- Economia de tempo das atualizações; melhor qualidade na apresentação;

- Liberação de funcionários mais experientes para que se dediquem a áreas mais técnicas e de maior risco;
- Agregação de valor ao trabalho de auditoria;
- Formação de equipes virtuais (*groupware*), maximizando a especialização;
- Fluxo de informações mais rápido;
- Maior satisfação profissional;
- Maior respeito pelo auditado;
- Maior produtividade; e
- Realização das tarefas sem a automatização pelos profissionais menos experientes. Antes somente poderiam ser executadas por profissionais mais experientes.

Para auditar as informações em ambiente de tecnologia de informação, o auditor poderá desenhar as abordagens que lhe convêm. As abordagens mais comuns são: abordagens ao redor do computador; através do computador; e com o computador.

A auditoria sempre foi conhecida por sua responsabilidade nos testes de confiabilidade dos registros de acordo com os documentos-fonte (os documentos que geram todas as transações econômicas, financeiras e contábeis) disponíveis através de quaisquer dados intermediários que possam existir e para os quais são produzidos relatórios para a tomada de decisões gerenciais. Porém, devido à evolução da tecnologia de informação, que interfere nas tecnologias gerenciais, geração a geração, é necessário guardar as informações para que sejam acessíveis para auditoria quando forem requisitadas. Sabe-se que, devido à complexidade dos ambientes e expansão dos negócios que atingiram implementações em ambiente de intranet e internet, há grandes problemas quanto à vulnerabilidade de computadores e alguns casos comuns de fraudes.

2.7 Conclusão

Neste capitulo foram apresentadas as principais tecnologias que serão abordadas. Cabe ressaltar as funcionalidades e os padrões das tecnologias bem como a arquitetura cooperativa de firewall a ser utilizada para criar uma sistemática uniforme que será aplicada na solução da comunicação segura entre as empresas do setor elétrico.

3 AMEAÇAS E ATAQUES EM SEGURANÇA DA INFORMAÇÃO

Neste capitulo é abordado as ameaças e alguns tipos de ataques de maior importância que podem expor os riscos ao sistema de medição de faturamento e as empresas envolvidas na tramitação da informação.

As ameaças sempre vão estar ligadas a um “agente”, que é o autor do ataque, a um “mecanismo”, que é a ferramenta ou método que o agente utilizou para fazer o ataque e a um “ativo”, que é o alvo do agente.

Para que o agente tenha sucesso em um ataque é fundamental que ele tenha um bom conhecimento do sistema e disponha de mecanismos que explorem as suas vulnerabilidades. Alguns dos mecanismos de ataque podem ser:

- Abuso de poder: usuário, administrador ou programador utiliza acesso legal sobre o sistema para realizar um ataque;
- Força bruta: usado para quebrar senhas e criptografia, por tentativa e erro;
- Exploração de vulnerabilidade conhecida: muitos sistemas prontos possuem lista de vulnerabilidade conhecida e publicada na Internet, algumas com exemplos de como explorá-las;
- Repúdio de origem ou de recebimento: negação de envio ou recebimento de mensagens;
- Interceptação: acesso por pessoa, programa ou sistema computacional não autorizado;
- Interrupção: destruição de um dispositivo de *hardware*, remoção de um programa ou arquivo de dados e mau funcionamento de um sistema de arquivos;
- Modificação: ocupação por pessoa, programa ou sistema computacional não autorizado;
- Fabricação: transações falsificadas em uma rede de comunicação ou adicionar registros a um banco de dados existente.

Afirma-se que uma aplicação que consiga se proteger de um número grande de ameaças muito provavelmente estará dificultando uma série de outras ameaças que não foram percebidas, isto porque muitas delas utilizam o mesmo modo de ataque.

3.1 Ameaças

Entende-se ameaça como uma possível violação de segurança de um sistema, sendo difícil apontar todas as ameaças a que um sistema está exposto. Surgiram muitas ameaças nos últimos tempos em virtude da evolução da tecnologia e até mesmo de alterações feitas em aplicações utilizadas nos sistemas.

Uma das duas ameaças à segurança que ganha mais publicidade é a do intruso, geralmente conhecido como *hacker* ou *cracker* [58].

Com o advento da Internet, vislumbrava-se como potenciais invasores de rede os hackers e espiões industriais, ou mesmo ameaças de governos estrangeiros. Não se dava muita atenção ao pessoal interno das organizações, acreditava-se que, se estes tivessem um bom *Firewall* entre a sua rede e o mundo exterior, eles estariam seguros. Entretanto, esse *firewall* não poderá proteger uma organização contra certos problemas, como os citados por [28]:

- Se um Diretor escolher o nome de seu filho, ou outro parente próximo, como senha de acesso a um determinado sistema, e não a modifica por cinco anos, qualquer bom invasor será capaz de tentar invadi-lo;
- Um funcionário descontente pode realizar cópias das informações confidenciais em disquetes ou CD's e os vender à concorrência. Não fará diferença se o *Firewall* utilizado é o melhor de mercado;
- Se alguém dentro da empresa acidentalmente (ou propositadamente) insere um disquete com vírus em um computador da rede, e este começa a formatar os discos de todos os servidores, não há nada que um *Firewall* possa fazer.

Em uma rede corporativa de computadores, são os funcionários ou também prestadores de serviços e consultores externos que trabalham na rede, que conhecem a localização das informações mais importantes e, muito freqüentemente, têm acesso ao CPD. Isso significa que um segurança na entrada do prédio não é suficiente. Para garantir a segurança é necessário vigilância também nos corredores que levam às salas onde são guardados os bens mais valiosos. Também se deve colocar os dados dentro da rede de

computadores de forma a proteger os dados mais valiosos: financeiros, legais, pessoais, estratégicos e outros.

Buscando proteger informações, as organizações devem se proteger de investidas externas e internas devendo “configurar vários *Firewalls*, ou seja, um para proteger-se dos invasores da Internet e outros, em vários pontos da *Intranet*, para minimizar as oportunidades dos funcionários obterem informações não autorizadas” [28].

3.2 Tipos de Ataques

A democratização da tecnologia possibilita o incremento diário de aperfeiçoamentos, melhorias e etc., mas, da mesma forma que os benefícios evoluem, os malefícios também, com o advento de novas formas de ataques e de quebra de segurança de informações.

Ataques são violações a sistemas de computação que podem envolver alguma forma de exploração de senhas, exploração de sistema, exploração de informações, acesso confiável do computador [5].

Para [49] os ataques são eventos que pegam as pessoas de surpresa, que são ‘notícia’ em sua definição real. Eles são rompimentos do contrato social da sociedade e interrompem as vidas normais das vítimas. Desse modo, as ameaças no mundo digital espelham as ameaças no mundo físico.

Para que a continuidade dos negócios das organizações não seja afetada, busca-se, contra esses riscos, todos os níveis de segurança, desde o físico até o de aplicação, que as organizações têm de lutar, principalmente por meio das técnicas, tecnologias e conceitos [40].

3.2.1 Furto de Senhas

Uma das maneiras mais comuns e fáceis de entrar em um computador é normalmente pela porta da frente, isto é pelo comando *login*. Em quase todos os sistemas, um *login* bem-sucedido está baseado no fornecimento de uma senha correta, dentro de um número razoável de tentativas [15].

Essa estratégia de força bruta tem sucesso, por exemplo, em muitos tipos de sistemas UNIX que não bloqueiam tentativas de login após um determinado número de insucessos.

Essa fraqueza inerente em termos de segurança permite que o intruso dê início a um grande número de tentativas de *login* que não são impedidas. Às vezes, os violadores descobrem as senhas da seguinte forma: acessando mensagens de correio eletrônico que contenham senhas; ou decifrando-as como a ferramenta que permite localizar e obter informações sobre senhas vulneráveis em sistemas UNIX. Na verdade, alguns crackers utilizam TFTP ou FTP para tentar obter de forma remota o arquivo de senhas (/etc/passwd) disponível publicamente para leitura em alguns sistemas UNIX [5].

[17] afirma que um mecanismo de controle de acesso, controla quais usuários ou programas de computador podem acessar os dados. Por exemplo, alguns sistemas implementam uma Lista de Controle de Acesso (*Access Control List , ACL*) para cada objeto, determinando quem tem permissão para acessar o objeto. Em outros sistemas, atribui-se uma senha (*password*) para cada usuário. Quando um usuário precisa acessar um recurso protegido, pede-se a ele que entre com a senha.

Quando se estendem listas de controle de acesso e senhas através de redes, os passos precisam ser tomados de maneira a prevenir acessos não intencionais. Por exemplo, se um usuário em um local envia uma senha decodificada através de uma rede para um computador em outro local, qualquer um que grampeie a rede pode obter uma cópia da senha. Os grampos são especialmente fáceis quando os pacotes viajam através de uma LAN sem fio, pois uma conexão física não é necessária – qualquer um no alcance da transmissão pode capturar uma cópia de cada pacote.

3.2.2 Engenharia Social

Ao invés de explorar a tecnologia, a engenharia social é a técnica que explora as fraquezas humanas e sociais. Ela tem como objetivo ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização. Essa técnica de enganar explora o fato da disposição dos usuários a ajudar e a colaborar com os serviços da organização.

Preceitua-se [15] que normalmente o que ocorre não é má fé e sim desinformação, o que em parte é culpa da própria organização, e isto acaba por tornar estas pessoas despreparadas ou desatualizadas em responsáveis por propagar ataques de engenharia social.

O engenheiro social é capaz de convencer a pessoa que está do outro lado da porta a abri-la, independentemente do tamanho do cadeado. Ele manipula as pessoas para que elas entreguem as chaves ou abram o cadeado, explorando características humanas como reciprocidade, consistência, busca por aprovação social, simpatia, autoridade e medo [40].

Para evitar tipos de ataques de engenharia social dentro de empresas, é importante que os usuários sejam orientados a não repassar sua senha em nenhum momento e uma metodologia de identificação pessoal seja aplicada antes de repasse de informações corporativas.

3.2.3 Bugs e Portas dos Fundos

Os desenvolvedores de *software* por si só são um dos maiores responsáveis pelos *bugs* de sistemas ou ataques de negação de serviços. Diversas falhas no desenvolvimento, na implementação dos aplicativos, protocolos e sistemas operacionais abrem brechas que podem ser exploradas em ataques contra a organização. Alguns tipos de falhas que oferecem condições de *buffer overflow* podem ser utilizados para que códigos prejudiciais e arbitrários sejam inseridos e executados, o que pode resultar em vulnerabilidades ou abertura de portas indesejadas.

Segundo [15] esse estouro de *buffer* é chamado colisão de pilha e é a maneira mais comum como os invasores subvertem programas. Faz-se necessário um pouco de cuidado para escrever o código, pois os caracteres sobrescritos são códigos de máquina para o *host* alvo, mas muitas pessoas fizeram isso. A história e a literatura da computação estão repletas de projetos para evitar ou frustrar estouros de *buffer*. Isso nem mesmo é possível em muitas linguagens de computação. Alguns *hardwares* (como as antigas máquinas *Burroughs*) não executariam o código na pilha. Além disso, alguns compiladores e bibliotecas utilizam diversas abordagens para frustrar ou detectar tentativas de colisão de pilha atuando de forma preventiva.

São muitas as formas de ataque, sendo uma delas, que como o verme da Internet se espalhou, foi enviar um novo código ao *daemon* de *finger*. Naturalmente, o *daemon* não esperava receber tal coisa, e não havia provisão alguma no protocolo para receber esse código. Entretanto, o programa emitiu uma chamada *gets*, que não especifica o comprimento máximo de um *buffer*. O verme preencheu o *buffer* de leitura e algo mais com seu próprio

código e prosseguiu até sobrescrever o endereço de retorno no quadro da pilha do *gets*. Assim sendo, quando a sub-rotina por fim retomou, ela foi desviada para esse *buffer* e executou o código do invasor, quebrando a segurança [15].

Um exemplo de *bug* pode ser visto na descoberta de uma falha conceitual no UNIX, tornando-o vulnerável. Essa falha que atinge todos os tipos de sistemas UNIX, até mesmo Linux, com exceção do BSD, ocorre quando diversas conexões são feitas, porém sem pedidos de requisição. Assim, os diversos serviços (*daemons*) não podem responder às conexões e a tabela de processos do sistema, que pode trabalhar com um número entre 600 e 1.500 processos simultâneos, fica cheia e causa a parada do servidor [40].

3.2.4 Vazamento de Informações

A maioria dos protocolos revela algumas informações. Freqüentemente, essa é a intenção de uma pessoa que deseja coletar informações contidas nos protocolos da organização, numa linha de espionagem. As informações por si só poderiam ser o alvo de agentes de espionagem comercial, ser desejadas como uma motivação para uma invasão e vazamento de informações.

Outra forma de vazamento de informações pode se basear no *packet sniffing*, que consiste na captura de pacotes que circulam na rede, podendo conter informações importantes e, portanto, confidenciais para a empresa, tais como segredos de negócio e senhas de sistemas de software. Os serviços de FTP e *Telnet* são vulneráveis a esse tipo de ataque, pois é possível obter facilmente as senhas dos usuários que utilizam esses serviços. De fácil execução, o ataque de *packet sniffing* pode ser usado por qualquer pessoa que possua conhecimentos mínimos em computação, pois existem *softwares*, que são de utilização simples e produzem bons resultados, específicos para esse fim [9].

3.2.5 Ataques Exponenciais – Vírus e Vermes

Os chamados ataques exponenciais utilizam programas para espalhar a si mesmos, multiplicando seus números rapidamente. Quando os programas viajam sozinhos, eles são vermes. Quando se anexam a outros programas, são vírus. A matemática da sua multiplicação é similar, e a distinção não tão importante. A epidemiologia de tais programas é bem semelhante a agentes infecciosos biológicos, se espalhando e ‘contaminando’ [15].

Os vírus de computador são programas que podem infectar outros programas de computador através da modificação destes, de forma a incluir uma cópia de si mesmo. A denominação de programa-vírus vem de uma analogia com o vírus biológico, que transforma a célula numa fábrica de cópias dele. Para o público em geral, qualquer programa que apague dados, ou atrapalhe o trabalho, pode levar a denominação de vírus. No ponto de vista de um programador, o vírus de computador é algo bastante interessante. Sendo o vírus um programa de computador sofisticado, ainda que use técnicas de inteligência artificial, ele obedece a um conjunto de instruções contidas no seu código. Portanto, é possível se prevenir contra o seu funcionamento, conhecendo seus hábitos [60].

O verme (*worm*) é um programa que pode se replicar e enviar cópias de um computador para outro através de conexões de rede. Na chegada, o verme pode ser ativado para replicar-se e propagar-se novamente. Além da propagação, o verme normalmente realiza alguma função indesejada. Um vírus de e-mail tem algumas das características de um verme, pois se propaga de um sistema para outro. Porém, ainda podemos classificá-lo como um vírus, pois exige um humano para movê-lo adiante. Um verme busca ativamente mais máquinas para infectar e cada máquina infectada serve como uma plataforma de lançamento automatizada para ataques em outras máquinas [58].

3.2.6 Ataques de Negação de Serviço

Esses ataques contam com fraquezas de protocolos de segurança, *bugs* de programação nos servidores e mesmo pessoas impropriamente úteis. O ataque de negação de serviço (DOS) é diferente, uma vez que constituem a simples super utilização de um serviço levando *software*, *hardware* e enlaces de rede além da capacidade para eles concebida. A intenção é desativar ou degradar a qualidade de um serviço, e, geralmente, esse é um objetivo modesto, podendo apresentar objetivos muito mais amplos e prejudiciais à organização, ou mesmo à sociedade, em face de qual seja a organização vítima do ataque [15].

A negação de serviço impede ou inibe o uso ou gerenciamento normal das instalações de comunicação. Esse ataque pode ter um alvo específico; por exemplo, uma entidade pode suprimir todas as mensagens dirigidas a determinado destino. Outra forma de negação de serviço é a interrupção de uma rede inteira, seja desativando a rede ou sobrecarregando-a com mensagens, a fim de prejudicar o desempenho [58].

Os ataques de negação de serviço funcionam porque as redes de computador existem para se comunicar. Algum ataque simples como dizer “alô”, pode ser automatizado até que se torne um ataque de negação de serviço. Isso é basicamente o ataque de inundação SYN que paralisou vários provedores em 1996 [49].

3.2.7 Ataques Ativos e Passivos

Os ataques ativos atribuem alguma modificação do fluxo de dados ou a criação de um fluxo falso e podem ser subdivididos em quatro categorias: disfarce, que ocorre quando uma entidade finge ser uma entidade diferente; repetição, que envolve a captura passiva de uma unidade de dados e sua subseqüente retransmissão para produzir um efeito não autorizado; a modificação de mensagens significa que alguma parte de uma mensagem legítima foi alterada ou que as mensagens foram adiadas ou reordenadas para produzir um efeito não autorizado; e a negação de serviço, que impede ou inibe o uso ou gerenciamento normal das instalações de comunicação [58].

Os ataques passivos possuem a natureza de bisbilhotar ou monitorar transmissões. O objetivo é obter informações que estão sendo transmitidas. Eles são muito difíceis de detectar, pois não envolvem alteração de dados. Normalmente, o tráfego de mensagens ocorre em um padrão aparentemente normal, e nem o emissor nem o receptor estão cientes de que um terceiro leu as mensagens ou observou o padrão de tráfego. Porém, normalmente, é viável impedir o sucesso desses ataques por meio da criptografia. Assim, a ênfase em lidar com ataques passivos está na prevenção, em vez da detecção [58].

No que se refere à criptografia, há dois tipos de invasor. O primeiro é um invasor passivo, que pode espionar toda a comunicação de rede, com o objetivo de descobrir o maior número de informações confidenciais possível.

O outro é um invasor ativo, que pode modificar mensagens à vontade, introduzir pacotes no fluxo de mensagens ou excluí-Ias. Muitos artigos teóricos modelam um sistema como uma rede em estrela, com um invasor no meio. Cada mensagem (pacote) vai ao invasor, que pode registrá-Ia em *log*, modificá-Ia, duplicá-Ia, descartá-Ia, e assim por diante. Esse invasor pode também produzir mensagens e enviá-Ias como se estivessem vindo de outra pessoa qualquer [15].

[9] destaca que uma das formas de ataque passivo é o *packet sniffing*, já mencionado anteriormente no item 3.2.4.

3.2.8 Falsificação de endereços IP

Conhecido como *Spoofing* onde o intruso transmite pacotes externos com um campo de endereço IP de origem contendo o endereço de um host interno. O atacante espera que o uso de um endereço falsificado permita a penetração de sistemas que empregam segurança simples do endereço de origem, em que os pacotes de hosts internos confiáveis específicos são aceitos. A contramedida é descartar pacotes com um endereço de origem interno se o pacote chegar por uma interface externa.

3.3 Potenciais Atacantes

Dá-se o nome de atacante à pessoa que realiza um ataque (tentativa de comprometimento ou invasão) a um sistema computacional, obtendo êxito ou não. Essa terminologia é utilizada apenas didaticamente, pois o termo mais conhecido é hacker, amplamente usado pela mídia. Embora este último seja o mais empregado, ele é menos genérico do que o primeiro, já que existem ramificações do termo hacker: *Script Kiddies, Crackers, Carders, Cyberpunks, Insiders, Coders, White hats, Black hats e Preacker* .

Os *hackers*, por sua definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como um desafio às suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar sua capacidade e depois compartilham suas proezas com seus colegas. Eles não têm a intenção de prejudicar, mas sim de apenas demonstrar que conhecimento é poder. Exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores, eles geralmente não gostam de ser confundidos com *crackers.*

Os *crackers* são elementos que invadem sistemas com intenção maléfica de roubar informações e causar danos às vítimas. O termo *crackers* também é uma denominação utilizada para aqueles que decifram códigos e destroem proteções de *software*.

Ressalta-se, porém, que não são apenas os *hackers* que causam problemas de segurança nos sistemas. Os usuários, autorizados ou não, mesmo sem intenções malévolas,

também podem causar danos ou negar serviços de redes, por meio de seus erros e de sua própria ignorância.

A grande maioria dos atacantes é jovem. São pessoas que trabalham em projetos de computadores e técnicos altamente especializados. O que os motiva a desempenhar suas atividades é o status que adquirem ao conseguir quebrar algum sistema de segurança, ganhando com isto mais respeito dos seus 'colegas de profissão', vingança de alguém que os prejudicou ou obtenção de vantagens lucrativas. Qualquer que seja o motivo, o verdadeiro *hacker* é sempre difícil de ser localizado, pois para manter-se no anonimato, ele consegue apagar todas as pistas deixadas após uma invasão [54].

De fato, sem uma política de segurança adequada, essas organizações sempre apresentam alguma brecha de segurança pronta para ser explorada, principalmente as que são geradas pela falta de atualização de um *patch* do servidor. Isso é o suficiente para que os *script kiddies* executem as ferramentas encontradas na internet contra seus servidores e causem estragos consideráveis. [40].

O fato mais marcante é que os próprios funcionários das empresas conhecem as operações, a cultura e os detalhes da organização, o que facilita muito a espionagem. A conseqüência disto é que eles sabem onde estão os segredos, quem são os concorrentes e, principalmente, como apagar seus rastros. Esses fatos fazem com que os *insiders* sejam difíceis de ser identificados e punidos [21].

Pode-se verificar que a segurança é, muitas vezes, um problema social, e não apenas um problema tecnológico. Assim, estes problemas demonstram também que os aspectos humanos, sociais e pessoais não podem ser esquecidos na definição da estratégia de segurança.

Portanto, as invasões não autorizadas que resultam no vazamento de informações confidenciais, podem resultar em graves conseqüências, principalmente quando essas informações envolvem a segurança nacional.

3.4 Violação da Segurança de Informação em Banco de Dados

A segurança de dados começa com a forma como eles serão armazenados. Tipicamente é necessário armazenar dados de acesso a bancos de dados, senhas para acesso a

outros sistemas e talvez uma senha mestre para administração do site. É muito comum que desenvolvedores armazenem no mesmo diretório todos os arquivos do site, ou seja, armazenem em um só lugar os arquivos .html, os com extensão .php e vários arquivos de figuras. Não é incomum que desenvolvedores com o intuito de proteger senhas de acesso armazenem informações confidenciais em arquivos com a extensão.inc e guardem esses arquivos junto com todos os demais [46].

Um assunto que merece maior atenção diz respeito à violação da segurança e integridade. O mau uso dos dados pode ser definido como intencional (com má intenção) ou acidental [52]. A perda acidental de dados pode ocorrer de diversas formas: por queda de energia elétrica durante o processamento de transações, anomalias por acesso simultâneo ao banco de dados; anomalias pela distribuição de informações em diversos computadores e por erro lógico que viola a suposição de transações que devam preservar as restrições de consistência do banco de dados.

Portanto, é mais fácil proteger o Banco de Dados contra perda acidental das informações do que contra acesso intencional. São inúmeras as maneiras de acesso intencional. Tais como: leitura não-autorizada de dados (furto de informação); modificação não-autorizada de dados e destruição não-autorizada das informações.

A proteção absoluta do Banco de Dados contra ações intencionais é impossível. Mas o custo e a penalidade ao contraventor podem ser aumentados para deter seus ataques. Para proteger os bancos de dados podem ser adotadas medidas de segurança em diferentes níveis: no físico, no humano, no sistema operacional e no sistema de banco de dados.

O nível físico consiste em dotar o local, ou locais, onde estão os sistemas computadorizados de segurança contra entrada armada ou clandestina de estranhos; o segundo, o humano, prevê o critério cuidadoso de autorização a usuários para evitar que pessoas estranhas possam ter acesso aos dados, usando de suborno ou troca de favores.

O terceiro nível, o de sistema operacional, a segurança consiste em evitar qualquer falha que permita a entrada de pessoas estranhas aos serviços. Dessa forma, o nível de segurança do software dentro do sistema operacional é tão importante quanto a segurança física. Já o sistema de banco de dados pode prever a segurança restringindo as informações para alguns usuários e habilitando-as para outros. É responsabilidade do sistema de banco de dados assegurar que essas restrições não sejam violadas.

A segurança dentro do sistema operacional é implementada em diversos níveis, desde códigos para acesso ao sistema até o isolamento de outros processamentos em curso. O sistema de arquivo também permite certo grau de proteção aos dados. É possível obter segurança usando mecanismos que restrinjam a capacidade de visões ou de ocultação de dados aos usuários. A segurança do sistema de banco de dados relacionais pode ser aplicada em dois níveis: relação, que permite ou nega o acesso direto do usuário a uma relação; visão, que impede ou permite o acesso a dados que apareçam em uma visão. Assim, o usuário pode acessar parte das informações por meio de uma visão. Uma combinação de segurança em níveis relacionais e de visão pode ser utilizada para limitar o acesso do usuário apenas aos dados necessários a ele.

3.5 Conclusão

Neste capítulo observaram-se alguns tipos de ameaças e tipos de ataques, bem com os potenciais atacantes. As vulnerabilidades existem no sistema ou nas pessoas dependendo como cada caso é abordado e explorado. Para que os pontos falhos sejam minimizados deve-se compreender o comportamento do sistema no qual se pretende contemplar a proteção, tanto contra os ataques externos, quanto contra os ataques internos.

4. ESTUDO DE CASO: Segurança da Informação no Sistema de Medição de Faturamento no Setor Elétrico

4.1 Descrição do Problema

O modelo apresentado na figura 21 é descrito no sub-módulo 12.2, Instalações do Sistema de Medição para Faturamento promovido pela ONS, motivado pela criação do Operador Nacional do Sistema Elétrico, aprovado pela ANEEL, resolução nº 140/02 de 25/03/2002, figura 7.1. Os demais casos tratados na resolução podem ser mapeados com pequenas modificações no caso aqui considerado, para os efeitos das melhorias pretendidas nesse trabalho, conforme ANEXO 1. O modelo atualmente adotado para coleta, tramitação e auditoria dos dados caracteriza uma conexão que não é totalmente segura e isolada a um conjunto de medidores, sendo a segurança aplicada somente para CCEE. É utilizada nessa conexão a *internet*, com a utilização de VPN entre a CCEE (Câmera de Comercialização de Energia Elétrica) e os pontos de medição das empresas, para inspeção lógica e aquisição de energia, conforme apresentado na figura abaixo:

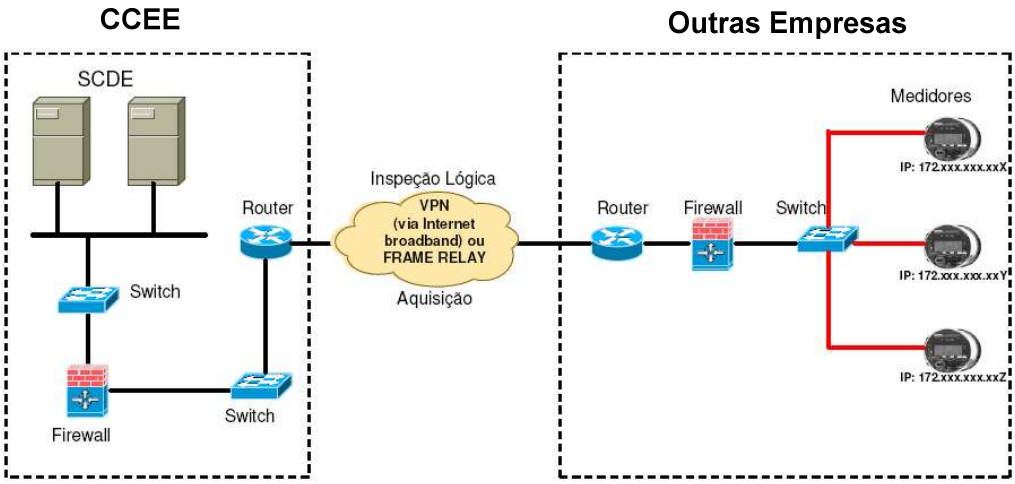

Figura 21 - Coleta de Dados de Medição via Canais Dedicados pela CCEE [44]

Verifica-se na figura 21 o modelo de comunicação via VPN entre a CCEE e outras empresas. No campo da CCEE identifica-se o SCDE – Sistema de Coleta de Dados Elétricos, que recebe as informações oriundas do SMF e o firewall, utilizado para segurança e o estabelecimento da VPN com os agentes do setor elétrico. No campo de outras empresas demonstra-se a existência um firewall para fechar a conexão VPN junto a CCEE e um

conjunto de medidores. Essa comunicação é apresentada na resolução acima mencionada para fazer acesso e inspeção lógica nos medidores.

O problema identificado nessa solução envolvendo as empresas que necessitam da mesma informação é a falta de segurança nas empresas para fazer acesso ao medidor de faturamento de diversos pontos e o monitoramento desses ativos.

Para permitir uma melhor constatação dessa falta de segurança empresarial considere-se que:

- Empresas distintas para comercialização de energia, que tenham a necessidade das informações de medição de energia, harmônicos, qualidade de energia sejam interligadas. Para essa medição os medidores podem estar alocados tanto na empresa provedora de energia, quanto na empresa receptora de energia, ou em ambas as empresas. As empresas provedora e receptora de energia têm a necessidade de medir a energia produzida, vendida e consumida. A empresa provedora de energia deve repassar as informações de energia coletadas para o órgão gestor, a CCEE. A CCEE, por sua vez, tem a prerrogativa de auditar as informações recebidas, fazendo acesso diretamente aos medidores de faturamento, quando achar necessário. Então, verifica-se aqui uma necessidade de acesso em conjunto de empresas distintas a um mesmo medidor. Essas empresas distintas têm seus próprios domínios e informações. Logo deve-se verificar o ponto de acesso ao medidor, mais o conjunto de empresas para prover a devida segurança, permitindo somente o acesso ao que é necessário e autorizado.

- A empresa provedora de energia pode estar distribuída em diversos pontos geográficos. Além dessas informações pertinentes ao medidor de faturamento de energia deverem estar concentradas em um ponto único de coleta para ser encaminhadas à CCEE, temos também uma diversidade de pontos de atuação e mapeamento distinto por localidade para prover a comunicação ao ponto de acesso do medidor, entre empresas provedora e compradora de energia, devendo ser observados os padrões de segurança. Os esforços para prover segurança ao acesso diretamente à internet devem ser considerados, pois, além das dificuldades de certas localidades isoladas em relação à comunicação,

também deve-se ater para o quantitativo administrativo para prover controle de acesso.

- A VPN seja configurada somente entre a CCEE e a empresa provedora de energia. A empresa provedora de energia, além dos pontos de medição de faturamento, tem toda uma rede corporativa dividindo o mesmo segmento e endereçamento dos ativos. Tanto os usuários quanto sistemas automatizados de coletas de dados da empresa provedora de energia necessitam por sua vez fazer acesso ao mesmo medidor de faturamento no qual a CCEE tem a prerrogativa de fazer auditoria. Como a empresa provedora de energia está no mesmo segmento dos medidores de faturamento, se torna improvável prover segurança a esses medidores pela rede interna.

- A CCEE tenha a prerrogativa de auditar diretamente os medidores da empresa provedora de energia. Caso seja identificado algum ponto de medição inoperante no momento da inspeção lógica, a empresa provedora de energia pode ser penalizada com multa.

Dessa forma pode-se identificar alguns dos ataques iminentes que podem sofrer a medição de faturamento:

- Ataques do tipo *Insiders*, que se referem ao nível interno das organizações. Os próprios funcionários são as maiores ameaças, pois têm a liberdade necessária para procurar algo de seu interesse. O fato mais marcante é que essas pessoas conhecem as operações, a cultura e os detalhes da organização, podendo capturar as informações, disponibilizá-las manipulá-las ou até mesmo comercializá-las.

- Ataques do tipo DoS *Deny of Service*, ocorrem quando há um excesso de tentativas de acesso, requisições maiores que o equipamento ou *software* pode suportar, com a finalidade de degradar e até mesmo paralisar seu funcionamento.

- Ataques do tipo passivo, com o objetivo de espionar toda comunicação e descobrir as informações confidenciais.

- Ataque do tipo ativo, com a intenção de modificar, capturar ou excluir mensagens ou mesmo outras informações.

- Ataque do tipo exponencial – Vírus e Vermes são programas injetáveis intencionalmente ou por propagação aleatória com intenção de infectar o sistema.

- Ataque do tipo falsificação de endereço IP, conhecido como *spoofing*, com o objetivo de penetrar no sistema com endereços internos provindo da rede externa.

O conjunto de exemplos acima caracteriza a significância desta pesquisa. Para que haja a possibilidade de desenvolver uma sistemática de melhorias necessárias ao acesso seguro do sistema de medição de faturamento do setor elétrico apresenta-se a seguir a proposta de solução.

4.2 Proposta de Solução

Para que se possa promover a comunicação, verificação e validação com a devida segurança no âmbito do sistema de medição de faturamento apresenta-se aqui uma proposta a fim de atender de forma satisfatória à entidade reguladora (ANEEL) e às empresas envolvidas no setor elétrico.

Será descrita uma sistemática de coleta, envio e auditoria segura dos dados do SMF para a CCEE. Tal sistemática envolve ações promovidas pela utilização de NAT sobre NAT, VPN sobre VPN, monitoramento dos ativos e controle de acesso aos pontos de medição, permitindo uma fronteira segura entre as empresas, com possibilidades de rastrear e auditar os dados trafegados.

O desenvolvimento dessa pesquisa propõe solucionar as deficiências de segurança física e lógica e resolver o problema de comunicação segura entre as empresas envolvidas que necessitam da mesma informação dos medidores de faturamento, conforme figura 22.

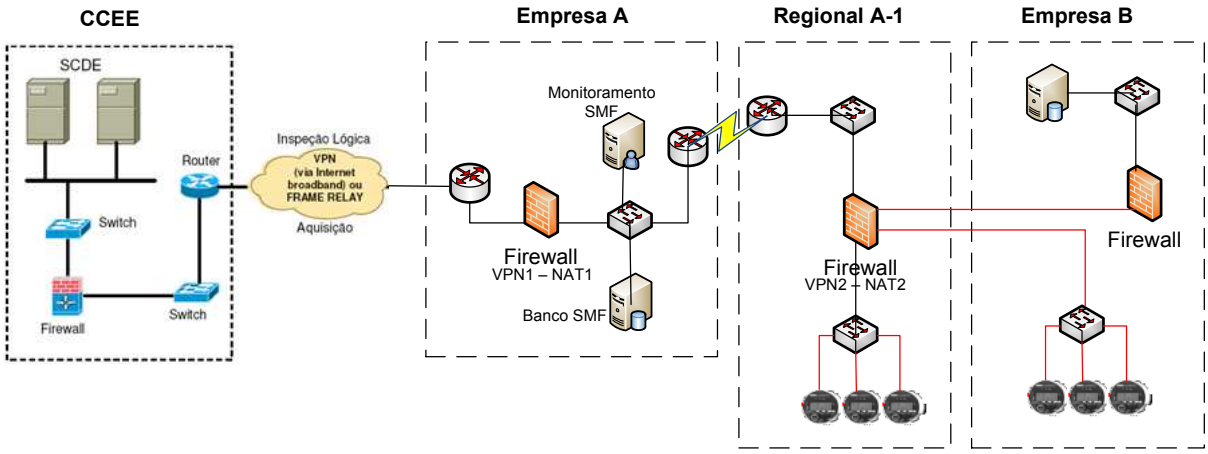

Figura 22 – Proposta para comunicação Segura SMF

Nessa figura, têm-se como possíveis agentes a CCEE, Empresa A, Regional da Empresa A e a Empresa B. Demonstra-se a comunicação da CCEE constituindo a primeira VPN/NAT até a Empresa A e a segunda VPN/NAT da Empresa A até a Regional da Empresa A. Verifica-se a inserção de um banco de dados na Empresa A, onde são armazenadas as informações dos medidores da Empresa A para o envio posterior dos dados a CCEE. Identifica-se um servidor de monitoramento para validar o funcionamento dos ativos do SMF, entre eles *firewalls*, roteadores, *switches* e medidores.

A solução a ser apresentada deve resolver os problemas de segurança dentro das corporações, fazendo interligação com outras empresas, que necessitam das informações do medidor de faturamento. Para iniciar a apresentação é demonstrada, na figura abaixo, a abrangência do sistema no qual foi contemplada a pesquisa para atender a resolução do problema entre diversas interligações físicas, considerando inclusive quantitativo de medidores, *firewalls*, empresas distintas e estudo para proteção com o mesmo modelo de segurança para outros ativos.

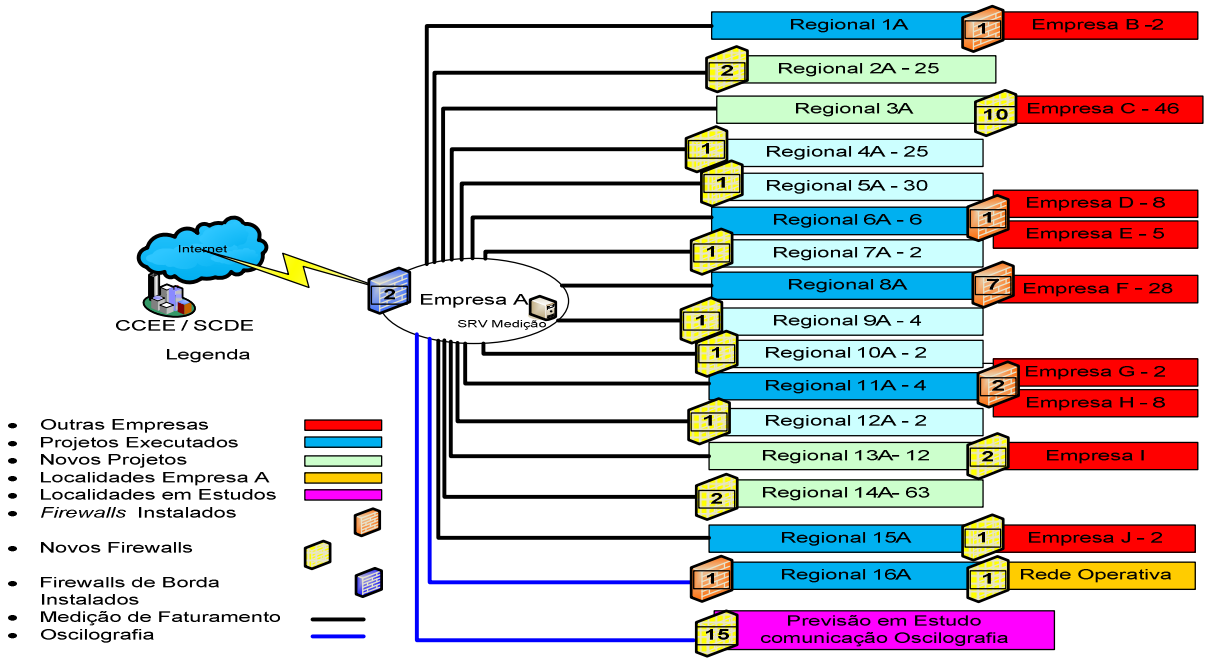

Figura 23 – Abrangência do sistema de medição de faturamento Empresa A

Demonstra-se na figura 23 a abrangência dessa pesquisa de segurança da informação no SMF, na Empresa A e seus parceiros. Verifica-se o quantitativo de *firewalls* instalados e a ser instalado, o quantitativo de medidores a serem monitorados e um novo estudo para segurança na comunicação da rede de oscilografia.

4.2.1 Segurança de comunicação entre as empresas para o acesso ao medidor

Com a abrangência do sistema de medição de faturamento dimensionado, inicia-se a descrição da sistemática de coleta, envio e auditoria segura dos dados do SMF para a CCEE e empresas interligadas.

Após a coleta e armazenamento no banco de dados das informações de todos os pontos de medição de faturamento via sistema, os dados do SMF são encaminhados para a CCEE com segurança. Ocorre uma comunicação VPN cliente/servidor direta do Banco SMF da Empresa A com a CCEE periodicamente. Após o recebimento dessa informação a CCEE detém a prerrogativa de conectar-se diretamente ao medidor para auditar as informações recebidas. Definiu-se a utilização de uma VPN modo túnel, que é uma VPN *site-to-site* que auxilia na conectividade entre *gateways*, CCEE e Empresa A por se tratar de empresas distintas que possuem um *firewall* em sua saída de internet.

Foi utilizada a configuração de VPN nativa do *firewall* Check Point versão RS65 por ser a ferramenta utilizada pela empresa provedora de energia, para proteção da VPN, controle de acesso do tráfego, gerência centralizada, *logs* consolidados, roteamento simplificado, melhor desempenho, bloqueio a ataques e atendimento às especificações técnicas conforme solicitadas pela CCEE.

Dentro dos padrões IPsec utilizados na VPN a mesma configuração para a VPN 1 foi atribuída para a VPN 2. Conforme pesquisa, para que o acesso seja estabelecido da CCEE, passado pela Empresa A, até chegar aos medidores, as características de criptografia da VPN devem ser a mesma tanto para a VPN1, quanto para a VPN2 para que se feche o túnel desde sua origem até o destino conforme figura 24.

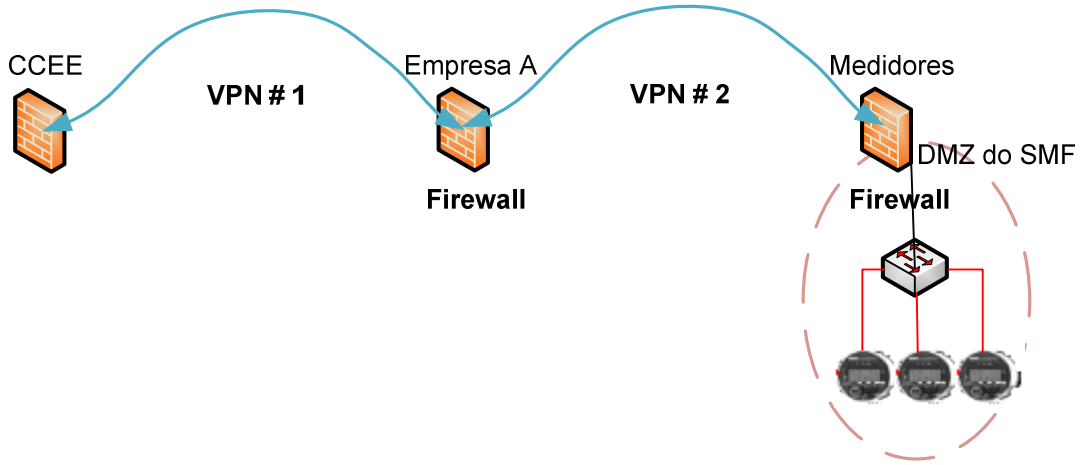

Figura 24 – Aplicabilidade de VPN sobre VPN

Conforme configuração proposta pela CCEE, apresentam-se abaixo os parâmetros utilizados para criação da VPN sobre VPN, modo túnel, envolvendo técnicas de segurança com o IPSec:

- **Protocolo de Túnel VPN:** A VPN foi utilizada nos padrões IPSec Protocolo de Segurança IP, um mecanismo padrão de segurança para redes IPs que visa o fornecimento de privacidade na comunicação entre entidades. A configuração IPSec foi dividida em 2 fases: parâmetros IKE (*Internet Key Exchange*) e parâmetros do túnel IPSec.

Na associação segura de chaves que indica a fase 1, utilizou-se a seguinte configuração conforme abaixo:

- **Parâmetros IKE (Fase 1):**

Criptografia: 3DES
Autenticação: HMAC-MD5
Diffie-hellman: Grupo 2
Lifetime: 1440 minutos
Pre-shared Secret:xxxx

Para criação do túnel seguro na fase 2 utilizou-se a seguinte configuração conforme abaixo:

- **Parâmetros do Túnel IPSec (Fase 2) :**

Modo: Túnel
Criptografia: esp-3des
Autenticação: esp-hmac-md5
Diffie-hellman: Grupo 2
Lifetime: 3600 segundos
Use Perfect Forward Secrecy: SIM

As telas abaixo demonstram as configurações aplicadas:

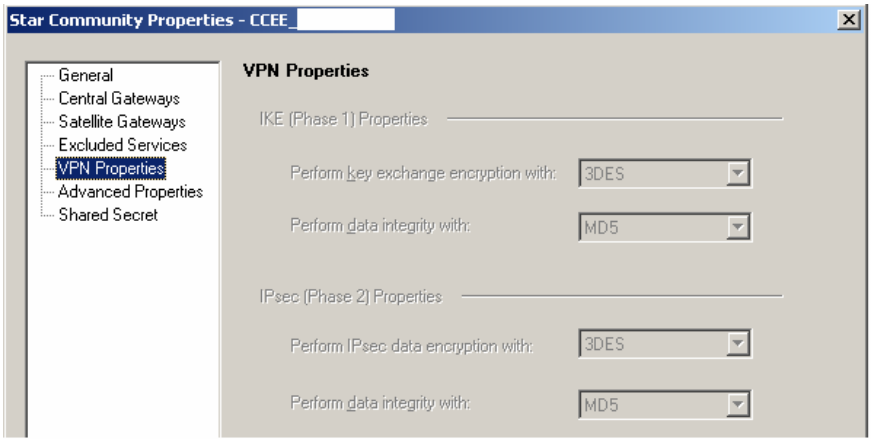

Figura 25 – VPN Fase 1 e Fase 2

Identifica-se na figura 25 uma tela do *firewall* Check Point, de propriedades da VPN onde atribui na fase 1 o tipo de ciframento para troca de chaves, conforme selecionado o 3DES e a integridade dos dados com a função *hash* MD5. São configurados, na fase 2, os parâmetros de ciframento IPSec, conforme selecionado o 3DES e a integridade dos dados com a função *hash* MD5.

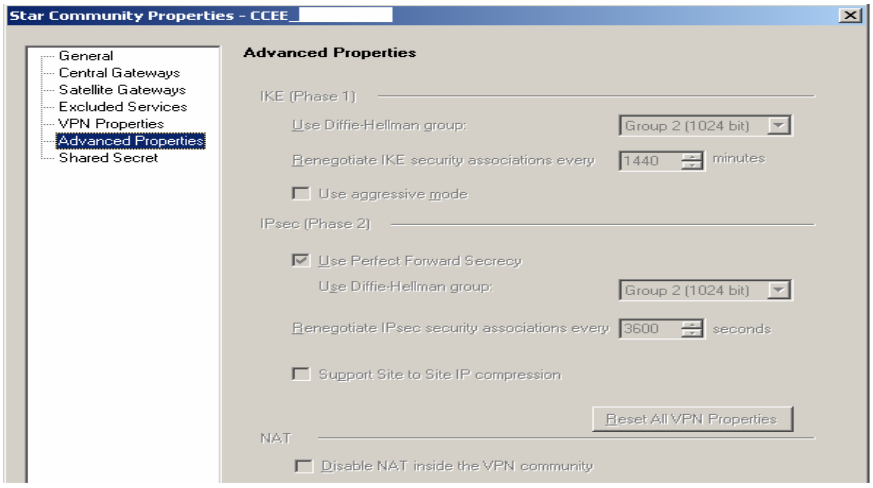

Figura 26 - Negociação da Chave

Verifica-se na figura 26 uma tela do *firewall* Check Point, nas propriedades avançadas da criação da VPN, a fase 1, usando grupo de chave 2 de 1024 bits o ciframento Diffie-Hellman e a associação segura da renegociação de troca de chaves a cada 24 horas. Na fase 2 utiliza-se, para o sigilo do encaminhamento, o grupo 2 de 1024 bits, o algoritmo Diffie-Hellman e a associação segura de renegociação do IPSec a cada 1 hora.

É necessária a identificação dos endereços da origem e do destino, onde é provido o acesso. Identifica-se no decorrer deste trabalho a associação dos endereços W para a CCEE, dos endereços Z a NAT CCEE, dos endereços X para os medidores da Empresa A e dos endereços Y para NAT da rede dos medidores Empresa A _Regional_n.

- **Parâmetros do Gateway VPN para o SCDE:**

Endereço do Peer: W.W.W.50
Endereço host: W.W.W.50

Na a criação da VPN entre os *firewalls* CCEE e Empresa A, ocorre a necessidade de tradução de endereço válido da internet para os endereços privados da Empresa A.

Sendo que a primeira VPN é estabelecida entre a CCEE até a Empresa A, então, existe a possibilidade de capturar o pacote do SMF na rede interna da Empresa A, decifrado. Para solução dessa vulnerabilidade ocorre a necessidade de inserção da segunda VPN, para assegurar sigilo da informação do SMF por todos os meios em que a mesma trafega.

Para estabelecer segurança na Empresa A, envolvendo todo parque computacional mais os medidores de faturamento foi inserido um segundo *firewall*, interno, na Empresa A e

uma segunda VPN que é associada entre o *firewall* de borda da Empresa A e o *firewall* dos medidores. Identifica-se no decorrer da pesquisa que o *firewall* interno executa a segregação entre o parque computacional da Empresa A e os medidores de faturamento. Atribui-se dessa segregação uma DMZ do SMF para cada localidade, uma zona no qual os medidores ficam separados da rede interna. Essa DMZ provê segurança aos medidores do próprio acesso interno da Empresa A, da exposição do parque computacional corporativo da Empresa A e segurança na interseção entre a Empresa A e outras empresas diretamente interligadas conforme figura 24.

Após a inserção do segundo *firewall, a*plica-se a segunda VPN entre o *firewall* de borda da Empresa A e o *firewall* interno das localidades nA dos medidores. A segunda VPN entre os *firewall* tem como sua principal função coibir a captura e a identificação da informação trafegada na rede interna. Verifica-se a seguir a inserção das regras nos *firewalls.*

Figura 27 - Regras no firewall de borda

Na figura 27 as regras no firewall são aplicadas em ordem de sua execução, no campo *Source* indica de onde está provindo o acesso, no caso, provido do endereço w.w.w.50, CCEE. Posteriormente verifica-se o destino, no caso da CCEE_Rede_NAT é aplicado a NAT *Hide* conforme figura 24 e a especificação dos medidores MEDIDOR_X.X.1A.n com uma NAT estática conforme figura 25. No campo VPN observa-se primeiramente a VPN com a CCEE_Empresa A e posteriormente entre Empresa A_Regional nA. No campo *SERVICE* é relacionado a porta de acesso. No campo *ACTION* é aceito a execução da regra. No campo TRACK é permitido o *log* e por fim no campo *INSTALL ON* indica-se onde é aplicada a regra.

Figura 28 - Regras no firewall Empresa A_Regional 1A

Na figura 28 verifica-se a aplicabilidade da regra com a segunda VPN no *firewall* da Empresa A_Regional nA. Esta regra estabelece a VPN com a Empresa A permitindo a

passagem dos específicos endereços para a específica porta autorizada. No *firewall* dos medidores pode-se aplicar também uma VPN diretamente com as outras empresas para estabelecer uma comunicação segura. Deve-se utilizar os mesmos parâmetros de configuração IPSec, com as devidas alterações de endereços conforme cada empresa e regional.

Em uma terceira porta no *firewall* dos medidores, utiliza-se a comunicação segura com a rede operativa, para tramitar informações referentes à qualidade de energia e harmônicos extraídos do medidor.

Com a utilização de um segundo firewall para separação dos ativos computacionais da Empresa A dos medidores de faturamento, identificou-se a necessidade de criação de uma segunda NAT para endereçar a DMZ do SMF. Agora se observa que o acesso lógico aos medidores está separado da rede interna da Empresa A. Os acessos provindos da CCEE terão duas traduções de endereços antes de estabelecer a comunicação com os medidores de faturamento. Entre a CCEE e a Empresa A aplica-se um NAT no modelo *hide,* permitindo que uma rede seja estabelecida em sua formação Z.Z.Z.0. A próxima tradução ocorre para os endereços da rede Z.Z.Z.0, um a um de Z.Z.Z.1 até Z.Z.Z.254 com um NAT estático para a rede interna Z.Z.Z.1 = X.X.1A.1, por se tratar de diversas localidades distintas dentro da Empresa A. A próxima NAT ocorrerá entre o *firewall* Empresa A_Regional nA aos medidores, é aplicado uma nova NAT estática X.X.1A.1= Y.Y.1Y.1 para a tradução de cada endereço da rede dos medidores serem relacionados diretamente com os endereços internos da rede da Empresa A, conforme figura 29.

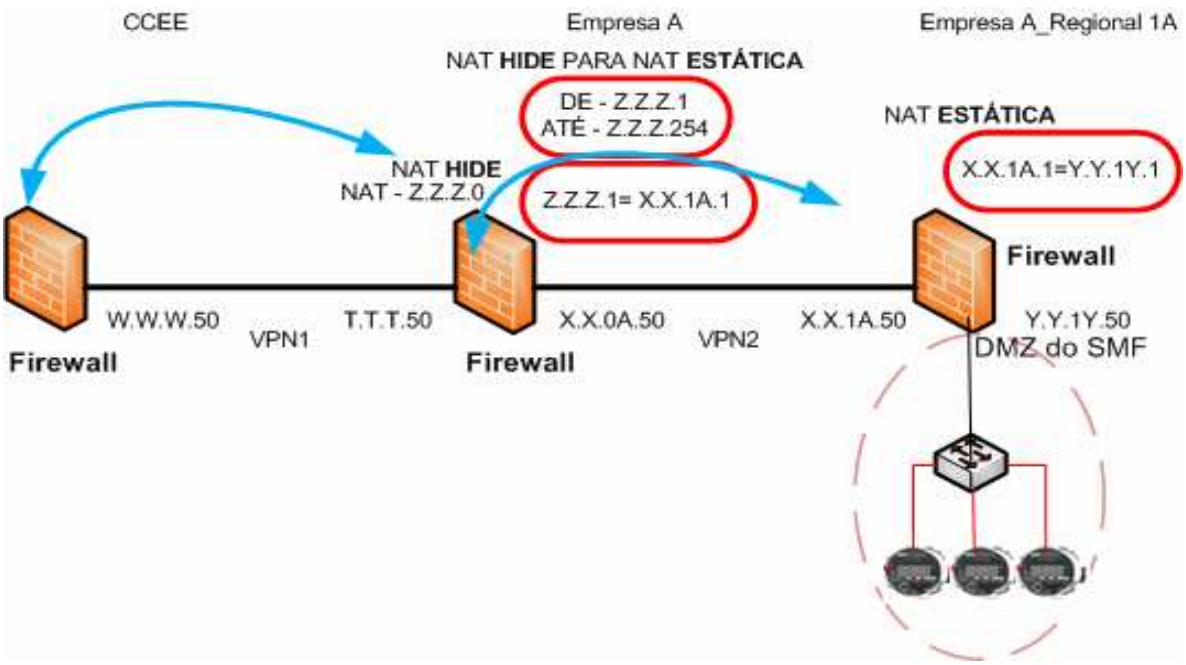

Figura 29– VPN sobre VPN e NAT sobre NAT

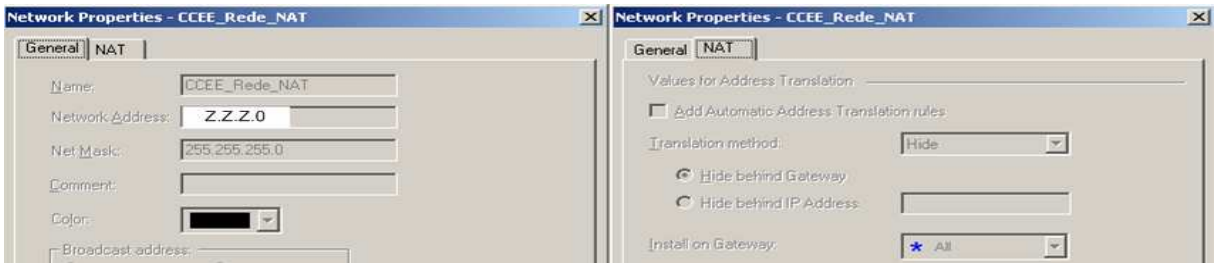

Figura 30 – Formação de NAT *Hide*

Na figura 30 apresenta-se a configuração da NAT *Hide*, uma segmentação de rede é apresentada conforme o campo *Net Mask* indicando o quantitativo de endereços possíveis.

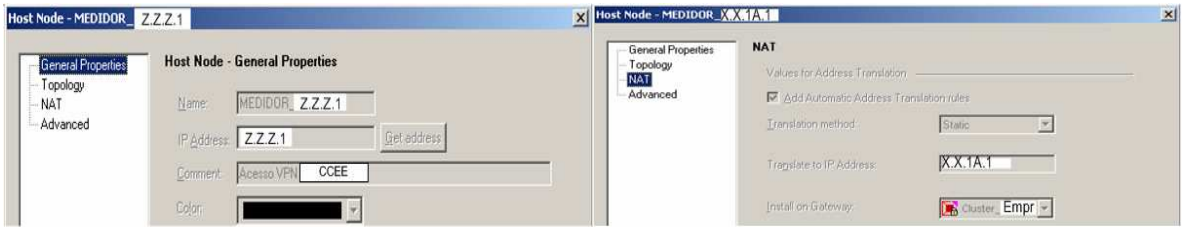

Figura 31 – Formação de NAT Estático

A figura 31 apresenta a tradução dos endereços da NAT *hide* para os endereços internos da organização traduzidos para NAT estática.

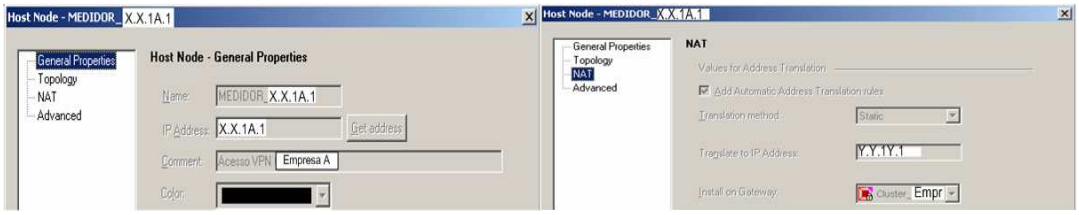

Figura 32 - NAT da rede interna para os medidores

A figura 32 apresenta a NAT estática dos endereços da rede interna para os endereços da rede dos medidores para cada localidade.

Após as VPNs estabelecidas no *firewall* Check Point, observa-se o *log* de acesso, de modo cifrado para estabelecer a tramitação segura das informações do SMF, conforme figura 27.

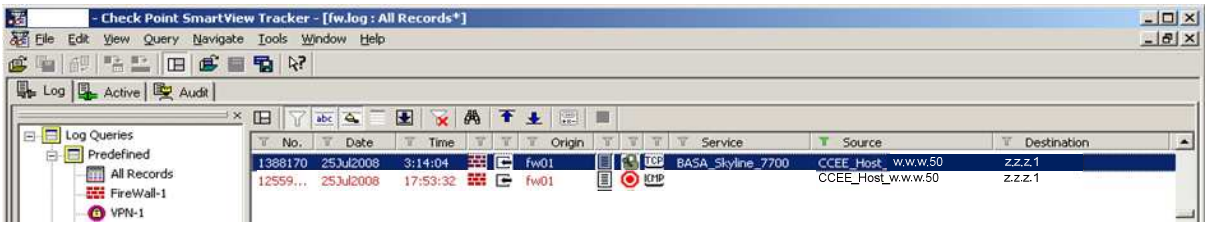

Figura 33 – VPN *Log* de Acesso

Verifica-se na figura acima a tela de *log* do *firewall* Check Point, onde é apresentado no campo de número o registro do acesso, no campo Date o dia, mês e ano em que ocorreu o acesso, o campo Time informa a hora, minutos e segundos do acesso. É demonstrado os dois acessos distintos para o mesmo endereço, o símbolo da chave amarela indica que a conexão VPN foi estabelecida com sucesso e o símbolo de vermelho indica que a conexão não foi estabelecida com sucesso. Maiores detalhes das seções dos *logs* de VPN são apresentados na figura abaixo:

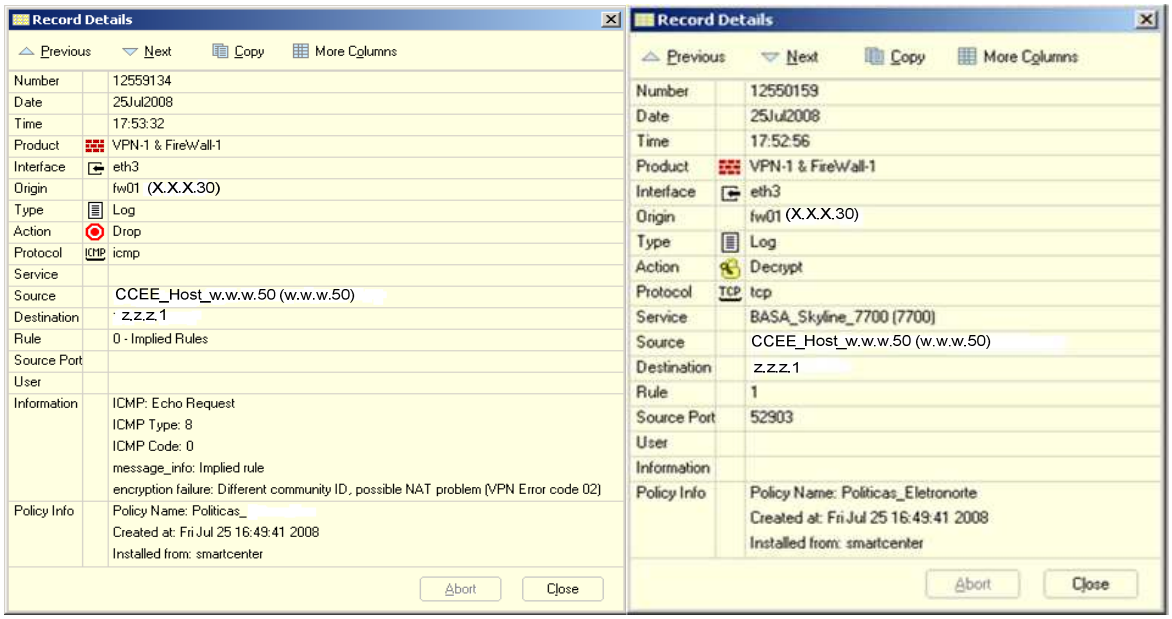

Figura 34 – Detalhes dos *Logs* de Acessos

A figura 34 apresenta detalhes do *log* de acesso. Observa-se na tela da esquerda que a seção de VPN não foi estabelecida, pois a requisição de acesso identificado foi para o protocolo ICMP, cujo serviço não está autorizado para esta requisição, conforme a regra do *firewall* na figura 27. Observa-se na tela da direita o acesso bem sucedido dentro dos parâmetros da VPN estabelecido.

4.2.2 Solução da arquitetura de comunicação segura entre os medidores e as empresas distintas

As soluções de arquitetura foram desenvolvidas para cada localidade com modelos diferenciados dependendo da necessidade de cada ponto de acesso. Os desenhos abaixo apresentados demonstram como são desenvolvidos os levantamentos de requisitos diferenciados:

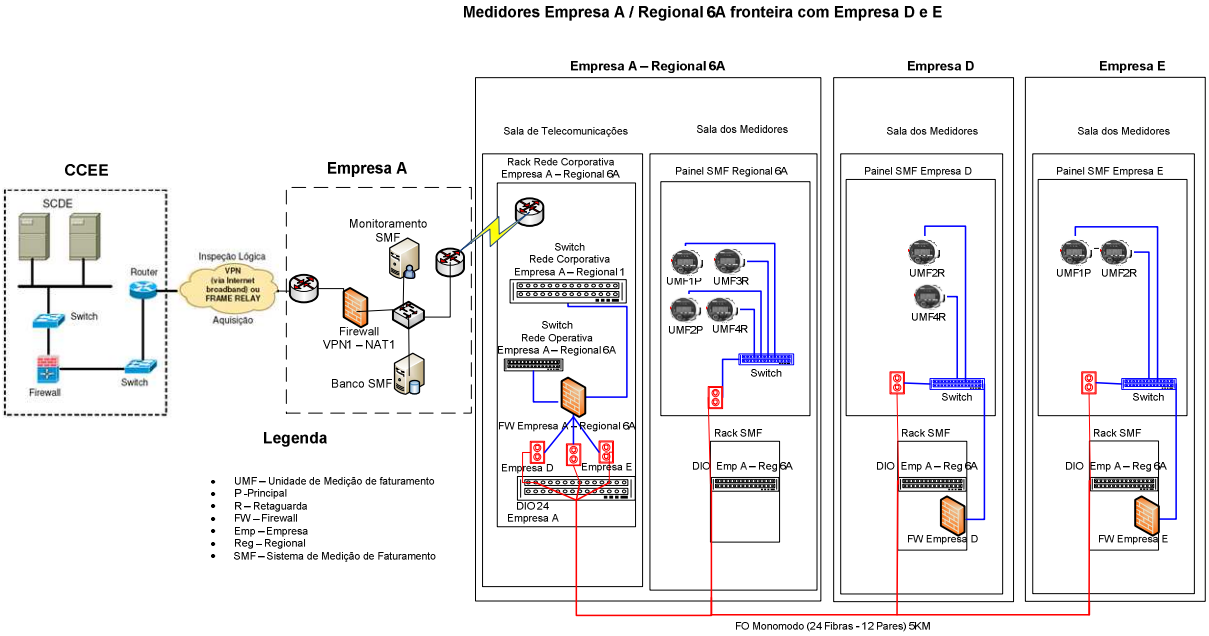

Figura 35 – Modelo de comunicação 1

A figura 35 apresenta empresas distintas com medidores instalados em cada empresa separadamente, podendo qualquer uma das empresas buscar informações dos outros medidores nas outras empresas. Foi passada uma fibra óptica em uma distância de até 5 quilômetros entre as corporações, todas as empresas chegando até o firewall na Empresa A / Regional n. A partir desse ponto todas as empresas podem fazer acesso com devida segurança na porta específica do medidor e com possibilidade de rastreamento. Essas informações, por sua vez, também são coletadas pela Empresa A e encaminhadas para CCEE via VPN externa. A CCEE tem a possibilidade de verificar as informações recebidas dos medidores procedendo um auditoria lógica nos medidores via túneis de VPNs que interligam as empresas aos medidores.

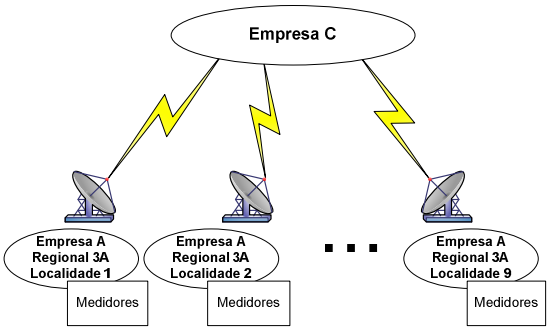

Figura 36 – Disposição de comunicação de vários pontos Empresa A para Empresa C

A figura acima demonstra a interligação de vários pontos de acesso da Empresa A / Regional 3 A / Localidade n para a Empresa C via satélite. A figura abaixo, modelo de comunicação 2, representa o encaminhamento das informações do ponto de coleta dos medidores para Empresa C. Demonstra também a inserção do *firewall* segmentando os medidores. Essa segmentação é apropriada para a Empresa A e as empresas em conexão. Foi concebido um endereçamento diferenciado das redes, onde é permitido o acesso, chamamos de DMZ (Zona desmilitarizada). Para que o acesso ocorra em cada medidor dentro da DMZ com endereços diferenciados, foi promovida a criação de uma NAT tradução de endereços de rede onde os endereços da DMZ x.x.x.x possam ter validades como y.y.y.y na rede das empresas. Sendo assim, conforme a apresentação da proposta, identificou-se que na CCEE para a Empresa A, há uma NAT e da Empresa A para Regional NA Rede Medidores, existe uma segunda NAT.

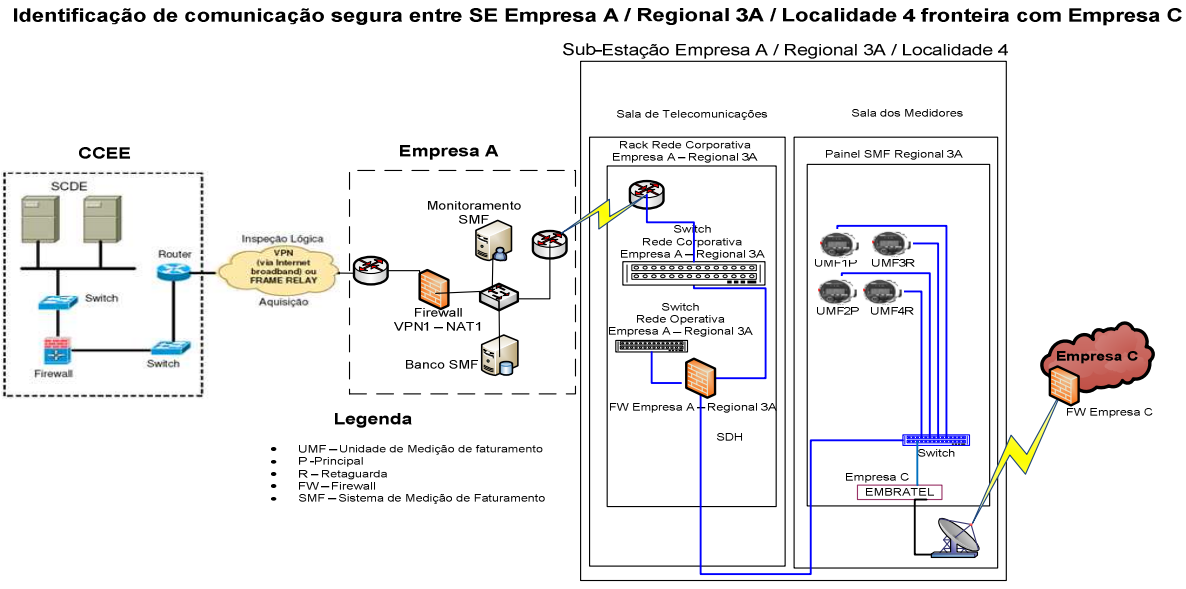

Figura 37 – Modelo de comunicação 2

O próximo modelo de comunicação que é apresentado na figura abaixo representa a comunicação somente dentro da Empresa A, sem a necessidade de interligação com empresas distintas. Podemos observar que continuamos com a existência de um *firewall* para segmentar as redes corporativa, operativa e a DMZ do SMF. Utilizando ainda a técnica de NAT sobre NAT e VPN sobre VPN, até a disponibilização da informação junto ao CCEE.

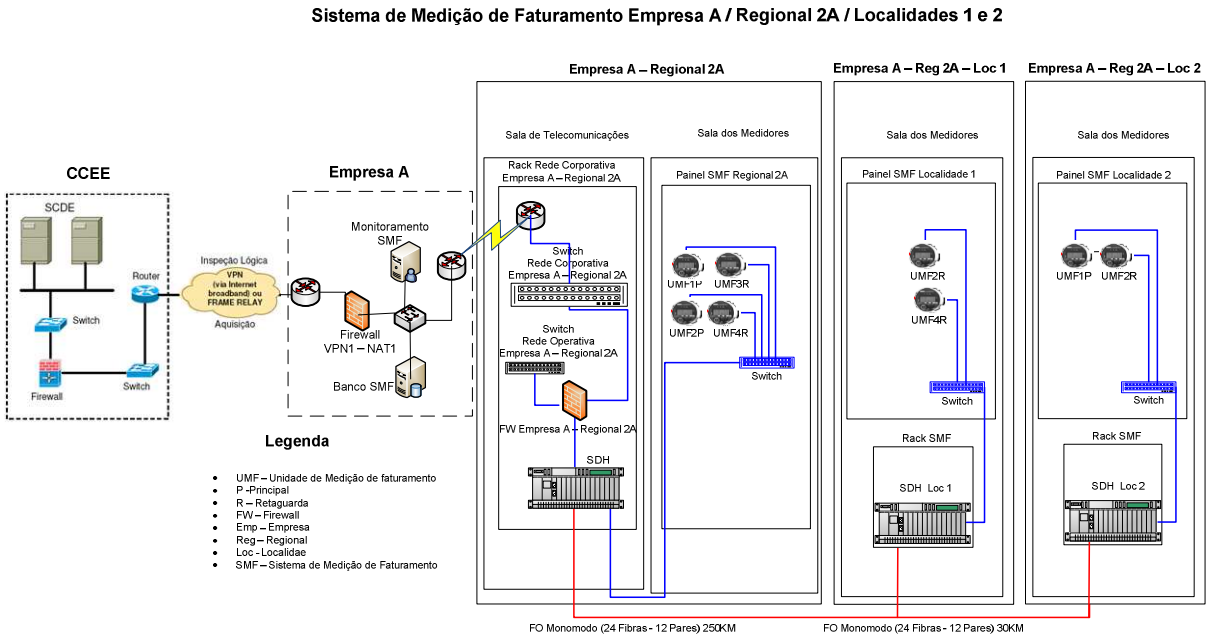

Figura 38 – Modelo de comunicação 3

4.2.3 Solução para Monitoramento do Sistema Implementado

Para identificarmos se o sistema de *firewalls* instalado e os medidores de faturamento estão em funcionamento, respondendo a comunicação física, lógica ou falha em algum ponto da conexão foi desenvolvido um software de monitoramento dos ativos. Esse programa identifica e alerta, por sinais gráficos, os ativos que estão conectados e em operação na rede e quando ocorre uma parada na comunicação. É um aplicativo que permite ao monitor ou analista identificar, a longa distância, em qual localidade ocorreu a parada.

Para construção dessa ferramenta foi utilizado conceitos de gerenciamento de rede, o comando Ping. O comando Ping é utilizado pelo protocolo ICMP *Internet Control Message Protocol*, que é integrante do protocolo IP, no qual faz a verificação de conectividade entre equipamentos. Para obter respostas da conexão, o Ping resolve o TTL - tempo de vida e o tempo de latência entre a comunicação, todos esses tempos são mensurados em milissegundos. A ferramenta de monitoramento foi desenvolvida em PHP versão 5.1.2 e

utilizado o servidor de páginas Apache/2.2.0 (Win32) e para inserção de dados foi utilizado o banco de dados MySQL versão 5.0.11-beta. Apresentamos na figura abaixo Monitoramento de Ativos a ferramenta em execução.

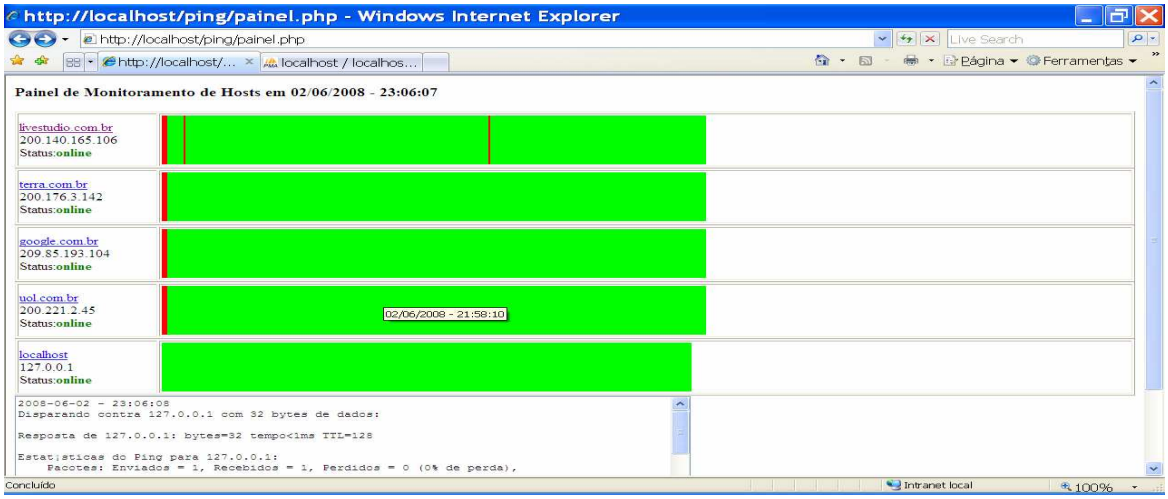

Figura 39 – Monitoramento de Ativos

A figura acima demonstra o programa Monitoramento de Ativos em sua execução. É uma aplicação que ocorre após a abertura do *browser* da internet com a chamada local ou via rede. É apresentado na parte superior o nome do programa com data e hora de cada ocorrência de chamada de execução. Logo após podemos observar uma tabela, onde no lado esquerdo foi atribuído o nome da localidade, o endereço de análise e o status da comunicação. Ao lado direito verifica-se a existência de cores verdes para indicar que o ponto monitorado está ativo e, em vermelho, indica-se falha no ponto monitorado. O programa identifica também o horário da ocorrência da verificação, indiferente do status, ao passar o *mouse* em cima de qualquer ponto monitorado. Na parte inferior da aplicação podemos notar a análise de monitoramento de cada ponto descrito: dia, hora, *host*, status. Todos os dados são armazenados diretamente no banco de dados para construção do histórico conforme figura abaixo:

Figura 40 – Histórico Monitoramento de Ativos

Após clicar no nome da localidade no Monitoramento de Ativos ocorre uma chamada ao histórico das informações coletadas. Conforme a figura 40 mostra, no campo superior, a localidade e data de coleta do histórico. Tanto o nome da localidade quanto a data no campo superior podem ser alterados dependendo da necessidade. É identificado no gráfico o histórico das informações. A barra preta à direita do gráfico indica o ano do histórico. Os números acima no gráfico indicam o quantitativo de verificações procedentes de cada acesso, esse quantitativo é diretamente proporcional ao tempo de uma execução para outra. A cor verde mostra o status que o ponto monitorado ficou ativo e a cor vermelha demonstra as falhas de comunicação por período. Os números abaixo no gráfico indicam as horas de monitoramento por dia.

4.3 Melhorias Apresentadas

Conforme pesquisa desenvolvida, podemos verificar que o conjunto de ações aplicadas para prover a comunicação segura ao sistema de medição de faturamento possibilita melhorias diretas e indiretas nas corporações, tais como:

- Tramitação segura da informação nas fronteiras das empresas do setor elétrico e parceiros em atendimento a comunicação aos medidores de faturamento.
    - Favorece as empresas reguladoras em sua inspeção lógica, mas também as empresas envolvidas no processo de compra e venda de energia, valorizando a confiabilidade, integridade e disponibilidade da informação do sistema de medição de faturamento no setor elétrico.

- Atribui segurança na rede interna, tanto para a corporação, que inibe o acesso aos medidores dentro da mesma rede corporativa, quanto para os medidores de faturamento que estão em segmento separado, que permite fazer somente acessos desejados.

- Gerenciamento integrado e seguro para o SMF
    - Permite que todo o sistema seja unificado no banco de dados do SMF para que possa fazer verificações, identificações precisas da medição de faturamento com segurança na tramitação da informação.
    - Inviabiliza ataques internos e externos dos tipos ativos e passivos.
    - Controla o acesso individualizado por localidade do ponto de medição.
- Gerenciamento de funcionamento dos ativos de segurança corporativo.
    - Provê monitoramento dos ativos e alerta em caso de falha.
    - Facilita identificação de ocorrências via histórico.

Melhorias indiretas:

- Viabilização da comunicação entre os medidores na rede corporativa.
    - Antes da implementação do sistema de medição de faturamento toda coleta de informação era feita manualmente pelo operador verificando a energia consumida. Hoje, após a implementação conforme o modelo da solução apresentada, o sistema é automatizado na coleta de medição de faturamento.
    - Além de toda medição ser automatizada, ocorre também a coleta de qualidade de energia, harmônicos, dentre outros, sem necessidade de intervenção do operador.
- Reestruturação de comunicação da rede corporativa.

- Conforme pesquisa identifica-se que para o funcionamento adequado da comunicação segura aos medidores de faturamento alguns equipamentos tiveram que ser substituídos e alguns *links* redimensionados para as devidas localidades.

- Integração das redes corporativa e operativa.

  - Conforme o modelo do setor elétrico, onde dentro da mesma empresa costuma existir redes diferenciadas, uma somente para a área operacional do sistema elétrico e outra voltada para a corporação, podemos identificar a comunicação entre ambas sem serem invasivas e coexistindo com total segurança dentro da segmentação proposta conforme o modelo apresentado na solução. Informações são distribuídas do mesmo ponto de acesso conforme a necessidade de cada rede em questão.

- Repasse da sistemática de segurança implementada para outros projetos corporativos.

  - Conforme estudo, outras aplicações ou equipamentos podem fazer uso da mesma metodologia de segurança aplicado à medição de faturamento.

- Identificação e análise de qualidade de energia diretamente nos medidores.

  - Com a integração das redes operacional e corporativa, existe a possibilidade de tramitação das informações pertinentes à qualidade de energia para as áreas fins.

  - Possibilidade de verificação de distúrbios pontuais na linha.

CONCLUSÃO

Atualmente, a grande maioria das informações disponíveis nas organizações encontra-se armazenada, sendo trocadas entre os mais variados sistemas automatizados. Dessa forma, inúmeras vezes decisões e ações tomadas decorrem das informações manipuladas por esses sistemas. Dentro deste contexto, toda e qualquer informação deve ser correta e precisa estar disponível, a fim de ser armazenada, recuperada, manipulada ou processada, além de poder ser trocada de forma segura e confiável. A informação constitui uma mercadoria de suma importância para as organizações dos diversos segmentos. Por esta razão, segurança da informação tem sido uma questão de elevada prioridade nas organizações.

A segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses pilares, juntamente com mecanismos de proteção têm por objetivo prover suporte à restauração de sistemas de informações, adicionando-lhes capacidades de detecção, reação e proteção. Os componentes criptográficos da segurança da informação são utilizados para a confidencialidade, integridade, não repúdio e autenticidade.

O envio e o recebimento de informações sigilosas é uma necessidade antiga, que existe há centenas de anos. Com o surgimento da internet e sua facilidade de entregar informações de maneira precisa e extremamente rápida, a criptografia tornou-se uma ferramenta fundamental para permitir que apenas o emissor e o receptor autênticos tenham acesso livre à informação trabalhada.

Dessa forma, vê-se que a segurança da informação possui influência cada vez maior no sucesso dos negócios. Para aplicar a melhor estratégia de defesa é preciso conhecer os principais riscos e ataques realizados por *hackers*, além de entender os principais conceitos de segurança e tecnologias, mecanismos e protocolos disponíveis para proteção.

Este trabalho apresentou a proposição de uma solução prática, hoje já em funcionamento, atendendo os pré-requisitos da CCEE, ONS, ANEEL e empresas interligadas, com a tramitação segura da informação do sistema de medição de faturamento pelos meios de comunicação adequados.

Os modelos de segurança em suas formas diversas buscaram contemplar as necessidades de cada localidade. Após estabelecer a comunicação dos medidores e prover a implementação dos *firewalls* para atendimento de comunicação segura entre o sistema de medição de faturamento e empresas parceiras, verificou-se a importância de uma sistemática que permite atender de forma segura todo o conjunto de acesso e tramitação da informação dos dados do Sistema de Medição de Faturamento.

Verifica-se após o funcionamento da sistemática apresentada, a aplicabilidade do método de segurança adotado, poder ser compartilhado para utilização com qualquer sistema ou equipamento que necessite estar alocado dentro de um nível topológico diferenciado, garantindo os devidos propósitos de acesso seguro conforme apresentados.

Algumas melhorias podem ser verificadas a partir da adoção da proposta apresentada:

- Para o caso de empresas distintas necessitando da mesma informação dos medidores:

- Tramitação segura da informação nas fronteiras das empresas do setor elétrico e parceiros em atendimento a comunicação aos medidores de faturamento.

- Para o caso da empresa provedora de energia estar distribuída em diversos pontos geográficos:

- Gerenciamento integrado e seguro para o SMF.
- Identificação e análise de qualidade de energia direto dos medidores.
- Controle de acesso ao SMF.

- Para o caso da empresa provedora de energia segregar o ponto de medição de faturamento em relação à rede corporativa:

- Viabilização da comunicação entre os medidores na rede corporativa.
- Reestruturação de comunicação da rede corporativa.
- Integração das redes corporativa e operativa.

- Para o caso de auditoria nos pontos ativos dos medidores de faturamento:

- Gerenciamento e histórico de funcionamento dos ativos do SMF.

Trabalhos futuros incluem:

- Inserção de detecção e prevenção de intrusos, para coibir e bloquear ataques de maneira proativa.
- Aferição da qualidade de serviço na área de segurança, para priorizar a tramitação segura da informação.
- Melhoria no sistema de monitoramento para identificação do ponto de parada da comunicação via alerta ou e-mail.
- Verificação do desempenho da rede após a inserção da segunda NAT e VPN.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no desenvolvimento de software: como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408.** Rio de Janeiro: Campus, 2002.

[2] AMARO, George. **CRIPTOGRAFIA SIMÉTRICA E CRIPTOGRAFIA DE CHAVES PÚBLICAS: vantagens e desvantagens.** Disponível em <http://publica.fesppr.br/index.php/rnti/article/viewFile/33/20> Acesso em: 06 fev. 2008.

[3] ANDRADE, M. M. de. **Introdução à metodologia do trabalho científico**. 6. ed. São Paulo: Atlas, 2003.

[4] BEAL, Adriana. **Segurança da Informação**: **Princípios e melhores práticas para a proteção dos ativos de Informação nas organizações.** São Paulo: Atlas, 2005.

[5] BERNSTEIN, Terry; BHIMANI, Anish B.; SIEGEL, Carol A. **Segurança na Internet: Tradução de Insight Serviços de Informática.** Rio de Janeiro: Campus, 1997.

[6] BISSON, J.; SAINT-GERMAIN, R. **Implementando políticas de segurança com padrão BS7799 / ISO17799.** Disponível em: <**www.callio.com.**> Acesso 28 mar. 2006.

[7] BURNETT, Steve; PAINE, Stephen. **Criptografia e Segurança: O Guia Oficial RSA**. Rio de Janeiro: Campus, 2002.

[8] CAMPOS, André L. N. **Sistemas de Segurança da Informação controlando os riscos**. Florianópolis-SC: Visual Books, 2006.

[9] CARVALHO, Luciano Gonçalves de. **Segurança de Redes.** Rio de Janeiro: Editora Ciência Moderna Ltda, 2005.

[10] CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

[11] CAVALCANTI, A. Encontro do Club Lan. Disponível em: <**http://www.nextplay.com.br/?actA=3&areaID=1&artigoID=102**>. Acesso 28 mai. 2007.

[12] CEPALDI, S.A. **Cursos básicos de contabilidade de custos**. São Paulo: Atlas, 2000.

[13] CHEHAB, Mauro. **Gestão da Segurança da Informação – Enfoque ISSO 17799 – apostila MBA especialização em governança de TI**. Brasília, 2006.

[14] CHEN, P. **Gerenciando banco de dados.** São Paulo: Makron Books, 1990.

[15] CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. **Firewalls e segurança na internet** – **repelindo o hacker ardiloso.** 2 ed. Porto Alegre: Bookman, 2005.

[16] COBIT. Framework CobiT 4.0. **Information Technology Governance Institute** – ITGI: ISBN 1-933284-37-4, USA, 2003.

[17] COMER, Douglas E. **Redes de computadores e internet**. 4 ed. Porto Alegre: Artmed, 2007.

[18] COSTA, H. F. D. da *et al*. **Análise de Sistemas para Aplicações e Soluções WEB**. Faculdades Associadas de São Paulo - FASP. São Paulo, 2005.

[19] COUCEIRO, L.A.C.C.; BARRENECHA, H. F. S. **Sistema de gerência de banco de dados distribuídos**. Rio de Janeiro: Livros Técnicos e Científicos, 1984.

[20] DAVENPORT, T. H.; KLAHR, P. **Managing customer support knowledge.** California Management Review. v. 40, n. 3, p. 195-208, Spring 1998.

[21] DENNING, P.J. **Teaching as a social process**. Educom Review, 34 (3), May/June, 1999.

[22] DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axel Books do Brasil, 2001.

[23] Diffie, W.; Hellman, M.E. **New directions in cryptography. IEEE Trans. Inform. Theory, 1976.** Disponível em **http://citeseer.ist.psu.edu/diffie76new.html>.** Acesso em: 15 mar. 2008.

[24] Diretrizes Gerais para **Políticas de Segurança**. Disponível em: <**http://www.proderj.rj.gov.br/**> Acesso 03 maio 2008.

[25] DUTTA, S. **Strategies for implementing knowledge-based systems**. *IEEE Transactions on Engineering Management*, v. 44, n. 1, p. 79-90, Feb.1997.

[26] FERNANDES, Aguinaldo A. **Implementando a governança de TI: da estratégia à gestão dos processos e serviços.** Rio de Janeiro: Brasport, 2006.

[27] FERNANDES, Aguinaldo A; ABREU, Vladimir Ferraz. **Implantando a Governança de TI**. São Paulo: Brasport, 2006.

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

[29] FITZSIMMONS, James A.; FITZSIMMONS, Mona J. **Administração de Serviços: Operações, estratégia e tecnologia de informação**. 2. ed. Porto Alegre: Bookman, 2000.

[30] FOINA, Paulo Rogério. **Tecnologia de informação**: **planejamento e gestão.** 2. ed. – São Paulo: Atlas, 2006.

[31] GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**, 4. ed., São Paulo: Atlas, 2002

[32] GOLDANI, Carlos Alberto. **IPSec e redes virtuais privadas** – informe técnico. Unicerte, 2004.

[33] HAMMER, Michael. **A empresa voltada para processos. HSM Management.** Nº 9, jul./ago. 1998.

[34] HAMMER, Michael. Sob um mesmo guarda-chuva. **HSM Management**, número 34, set./out. 2002.

[35] IMONIANA, Joshua Onone. **Auditoria de Sistemas de Informação**. São Paulo: Atlas, 2005.

[36] LIEBOWITZ, J.; GILES, P.; GALVIN, T.; HLUCK, G. **The role of knowledge-based systems in serving as the integrative mechanism across disciplines**. Computers & Industrial Engineering, v. 34, n. 2, p.559-564, Apr. 1998.

[37] MILTON, N.; SHADBOLT, N.; COTTAN, H.; HAMMERSLEY, M. **Towards a knowledge technology for knowledge management**. International Journal of Human-Computer Studies, v. 51, n. 3, p. 615-641, Sept. 1999.

[38] MOLINARI, Leonardo. **Security & Network Testing: a Fronteira Final de uma Rede**. – Developers'. Ano 5 - n° 56. Abril/2001.

[39] MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware.** São Paulo: Novatec, 2005.

[40] NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

[41] NBR ISO/IEC 17799. Disponível em **https://www.abntnet.com.br/ecommerce/ssl/norma.aspx?Norma=37529,** Acesso em 05.jul.2008

[42] NEKOOGAR, F. **Digital Cryptography: Rijndael encryption and AES applications. TechOnline,** 11 out. 2001. Disponível em: <http://www.techonline.com/community/ed_resource/feature_article/14754>. Acessado em: 24 jun. 2008.

[43] OLIVEIRA, Silvio Luiz de. **Tratado de metodologia científica: projetos de pesquisas, TGI, monografias, dissertações e teses.** São Paulo: Pioneira, 1999.

[44] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. **Instalação do sistema de medição para faturamento.** Disponível em: http://www.ons.org.br.

[45] PATACO, Vera Lucia Paracampos. **Metodologia para trabalhos acadêmicos e normas de apresentação gráfica.** Rio de Janeiro: Ed. Rio, 2004.

[46] PESSOA, Márcio. **Segurança em PHP: Desenvolva programas PHP com alto nível de segurança e aprenda como manter os servidores web livre de ameaças.** São Paulo: Novatec, 2007.

[47] PETERS, Marcos. **Implementando e Gerenciando a Lei Sarbanes Oxlei**: **Governança corporativa agregando valor ao negócio.** São Paulo: Atlas 2007.

[48] RAPPAPORT, Eduardo. Departamento de Engenharia Eletrônica e de Computação (DEL). Escola Politécnica. UFRJ, 2003. Disponível em: **http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/ipsec.html**. Acesso 20 jun. 2008.

[49] SCHNEIER, B. **Applied Cryptography**. 2. ed. New York: John Wiley & Sons, 1996.

[50] **Segurança.com: segredos e mentiras sobre a proteção na vida digital**/ Bruce Schneier; tradução de Daniel Vieira. Rio de Janeiro: Campos, 2001.

[51] SÊMOLA, Marcos. **Gestão da segurança da informação – uma visão executiva.** Rio de Janeiro: Elsevier, 2003.

[52] SILBERSCHATZ, A.; KORTE, H. F.; SUDARSHAN, S. **Sistema de banco de dados.** 3. ed., São Paulo: Makron Books, 1999.

[53] SILVA, Lino Sarlo da**. Public Key Infrastructure – PKI: Conheça a Infra-estrutura de Chaves Públicas e a Certificação Digital.** São Paulo: Novatec, 2004.

[54] SILVA, Lino Sarlo da**. Virtual Private Network**. São Paulo: Novatec, 2003.

[55] SOARES, L. F. G. ; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores das Lan's, Man's e Wan's às redes Atm**. 2. ed. São Paulo: Campus, 1995.

[56] SPEEL, P. H.; ABEN, M. **Preserving conceptual structures in design and implementation of industrial KBS**. International Journal of Human – Computer Studies, v. 49, n. 4, p. 547-575, Oct. 1998.

[57] STAIR, Ralph M. **Princípios de sistemas de informação: uma abordagem gerencial.** 2. ed. Rio de Janeiro: LTC, 1998.

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

[59] STEVE FRIED´L. Disponível em **http://www.unixwiz.net/techtips/iguide-ipsec.html**, Acesso em 25.julh.2008

[60] TRINTA, F.A.M.; MACÊDO, R.C. **Um Estudo sobre Criptografia e Assinatura Digital**. Pernambuco: DI/UFPE, 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 25 abr. 2008.

[61] VASCONCELLOS, Marcio Jose Accioli. **A Internet e os Hackers: ataques e defesas**. 2ª ed. São Paulo: Chantal.

[62] VOLPI, Marlon Marcelo. **Assinatura digital – Aspectos Técnicos, Práticos e Legais.** Rio de Janeiro: Axcel Books, 2001.

ANEXO