REVISTA ELETRÔNICA
ACTA SAPIENTIA

GESTÃO DE SEGURANÇA DA INFORMAÇÃO E UTILIZAÇÃO DE FIREWALLS EM EMPRESAS DA INDÚSTRIA TÊXTIL

Carlos Alberto de Sousa Júnior
Faculdade Estácio (FIC)
calberto@fic.br

Eliseu Castelo Branco Júnior
Faculdade Estácio (FIC)
eliseujr@fic.br

Alberto Sampaio Lima
Universidade Federal do Ceará (UFC)
albertosampaio@ufc.br

ABSTRACT

The security technologies, beyond the data protection and secrecy, are important to keep companies reputation. In this work we proceeded a bibliographical revision and a qualitative research, partially based on survey application, in order to understand the relative questions to net security and firewall technology. We presented the evolution of firewall since its sprouting until the current days, studying its description, the net security and firewall perimeters, demonstrating the covering perimeter with firewall, detaching the market trends from UTM use. Results indicated that most evaluated organizations are using information security policies, but still need the employees collaboration to get positive results.

Key-words: Firewall; Network Security; Information Security Management; IT Governance.

RESUMO

As tecnologias de segurança além de protegerem dados, conferirem sigilo, são importantes para manter a reputação das empresas. A partir de uma revisão bibliográfica e pesquisa qualitativa com aplicação de questionário buscou-se identificar como as empresas estão utilizando atualmente os firewalls em suas políticas de segurança da informação. São apresentados aspectos como a evolução dos firewalls desde o surgimento até os dias atuais, com averiguação do aspecto histórico, além de ser avaliada a segurança das redes e os perímetros de uso dos mesmos, bem como as tendências do mercado com o uso do gerenciamento unificado de ameaças. Os resultados indicaram um senso de responsabilidade e preocupação com a política de segurança por parte das empresas avaliadas, apesar da maioria ainda estarem deficitárias em termos do programa de conscientização acerca da política de segurança com seus funcionários.

Palavras-chave: Firewall; Segurança de Redes de Computadores; Gestão de Segurança da Informação; Governança de TI.

1 INTRODUÇÃO

O atual cenário globalizado reflete a realidade de dinamicidade que envolve as organizações contemporâneas, as quais necessitam participar em uma rede complexa de

relações para interligação ao segmento de negócio em que atuam, incluindo os clientes, fornecedores, parceiros ou ainda outras unidades na própria organização. Devido ao crescimento atual no desenvolvimento em tecnologia da informação (TI), essas relações aumentaram a sua abrangência, podendo atingir altos níveis de interconexões. Essas organizações necessitam essencialmente de informações para garantir a sua sobrevivência. De acordo com Netto e Silveira (2009), a partir da utilização dos computadores em diversas organizações, as informações começaram a se concentrar em um único lugar e o grande volume dessas informações passou a ser um problema para a segurança. Houve um aumento dos riscos com o uso dos microcomputadores, a utilização de redes locais e remotas, a abertura comercial da *internet* e a disseminação da informática para diversos setores da sociedade. Dessa forma, as organizações tem se preocupado cada vez mais com a segurança de seus sistemas de informação a partir dos efeitos da globalização nas sociedades, tentando tratar os riscos criados nesses novos mercados surgidos a partir da utilização das vias de comunicação digitais. Existe um desafio crescente para se assegurar a confidencialidade, integridade e disponibilidade da informação resultante do relacionamento com seus fornecedores, parceiros, clientes internos e externos.

Vários motivos podem levar uma organização a buscar a proteção de suas informações. A perda de informações resulta em um prejuízo para o negócio, pelo fato de que sua criação, busca e armazenamento possui um custo e agrega valor ao negócio. A informação possui alta importância no processo de concorrência empresarial, devido ao seu valor relacionado ao fato de estar integrada com os processos, pessoas e tecnologias. A informação muitas vezes é o alvo preferido para *hackers*, sabotadores, espiões, golpistas, entre vários tipos de criminosos que atuam no meio virtual. Dessa forma, informação, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida (NBR 17999, 2003). "Atualmente, mesmo sistemas industriais críticos, como usinas de energia elétrica, fornecedoras de gás e água, refinarias de petróleo e indústrias químicas, fazem uso de tecnologias *internet* em seus sistemas de controle e suas informações estão cada vez mais vulneráveis a problemas de segurança (interna e externa), tal como, roubo de informações e ataques cibernéticos" (NAEDELE, 2007 *apud* ROQUE et al., 2010).

As tecnologias de segurança além de protegerem dados e conferir sigilo às informações do negócio, ainda são importantes no sentido de manter a reputação de uma organização. Existe um crescimento na pesquisa sobre técnicas que possam facilitar a segurança da informação e proteger essa informação contra acessos indevidos.

Liu e Gouda (2009) afirmaram que os *firewalls* consistem em elementos importantes na segurança de redes, tendo sido utilizados em larga escala na maioria dos negócios e instituições visando a segurança nas redes privadas. A função de um *firewall* consiste no exame de cada pacote que chega e que sai para decidir quando aceitar ou descartar um pacote, de acordo com sua política. Ao analisar a segurança de redes, Al-Haj e Al-Shaer (2011) afirmam que os *firewalls* possuem um papel crítico no provimento do nível desejado de proteção a uma rede de computadores, pelo controle do tráfego de chegada e saída entre sub-redes. O comportamento de um *firewall* depende da política escrita para uma tarefa específica na política geral de redes. Para se avaliar o nível de defesa de uma rede, é necessário que se avalie os *firewalls* da rede e sua interação com outros *firewalls* para se atingir o nível de segurança requerido.

Objetivando proceder uma avaliação sobre como as organizações utilizam os *firewalls* em suas políticas de segurança, o presente trabalho abordou os temas relativos à segurança da informação, segurança em redes de computadores e tecnologia *firewall*.

Foi estudada a evolução dos *firewalls* desde o surgimento até os dias atuais, com averiguação do aspecto histórico. Através de uma revisão bibliográfica sobre segurança de redes e os perímetros de uso de um *firewall*, buscou-se a demonstração das necessidades para um perímetro de cobertura. Analisou-se ainda as tendências do mercado, com a utilização do gerenciamento unificado de ameaças (UTM). Para pesquisar sobre a utilização real dos *firewalls* pelas empresas, realizou-se um estudo com três empresas do segmento têxtil. A metodologia utilizada consiste em uma combinação entre a revisão bibliográfica e pesquisa qualitativa, por meio de estudo de caso.

2 REVISÃO BIBLIOGRÁFICA E TRABALHOS RELACIONADOS

De acordo com Beal (2005), segurança da informação é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Netto e Silveira (2009) definiram segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos. Os autores afirmaram que a integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental. A disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário. Enfim, a confidencialidade da informação consiste na garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do seu conteúdo.

Visando a garantia de um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores necessitam possuir uma visão clara das informações que estão tentando salvaguardar, das ameaças existentes e suas razões, antes de poder passar a seleção de soluções específicas de segurança (BEAL, 2005). A autora ainda afirma que as organizações necessitam da adoção de controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos, levando-se em conta os riscos reais a que estão sujeitos esses ativos. Para Fontes (2006), deve-se existir um alerta para o crescimento de incidentes de segurança da informação, principalmente no Brasil. As organizações estão cada vez mais expostas a novas formas de ataques, independentemente do porte ou do tipo de negócio.

Os princípios de governança de tecnologia da informação (TI) sugerem a existência de um forte alinhamento da gestão de segurança da informação com as necessidades de negócio. O guia de melhores práticas ITIL (OGC, 2007) afirma que todos os processos de TI de uma organização devem incluir considerações de segurança. A principal referência para o gerenciamento de segurança da informação no guia ITIL é sua publicação "Desenho de Serviços", entretanto a segurança da informação é abordada no contexto de todo o ciclo de vida de um serviço de TI. Ao se melhorar os aspectos da segurança da informação nos serviços de TI, aumenta-se o valor entregue por esses serviços ao negócio. O principal requisito do gerenciamento de segurança da informação consiste em garantir os aspectos presentes e futuros, bem como um bom gerenciamento dos riscos.

Para que se possa gerenciar a segurança da informação, deve-se definir e recomendar métricas de segurança de acordo com os requisitos de cada organização

(CLINCH, 2009). Ao se avaliar o gerenciamento de segurança da informação ao nível estratégico organizacional, torna-se necessário conhecer alguns aspectos relacionados ao gerenciamento de segurança, tais como a situação atual em relação à segurança da informação, quais processos devem ser melhorados de acordo com as estratégias organizacionais, quais as prioridades em relação aos investimentos em segurança, quais os resultados esperados com a priorização e ações de investimento, resultados de testes comparativos com organizações do mesmo segmento de negócio e o nível de conformidade em relação às normas que tratam do gerenciamento de serviços (ISO 27001, ISO 27002 e ISO 20000). Conforme a ISO/IEC 27004 (2009), um programa de medição de segurança da informação deve incluir as métricas e o desenvolvimento da medição, a operacionalização da medição, a comunicação da análise dos dados e resultados da medição, bem como a avaliação e melhoria do programa de medição.

Conforme citado em Fraser et al. (1997) *apud* Letter to Editor (2012), a implementação de políticas técnicas de segurança são criadas a partir das políticas de alto nível. Essas políticas descrevem o como fazer e são utilizadas para reforçar a política de segurança. O termo *política* é utilizado na literatura para descrever tanto as políticas de alto nível quanto as regras implementadas de baixo nível.

Os processos de criação e implementação de políticas de segurança de redes são mostrados na Figura 1. Muitas empresas utilizam os *frameworks* de melhores práticas reconhecidos pela indústria, tais como o COBIT (*Control Objectives for Information and Related Technology*), o ITIL (OGC, 2007) e a ISO 27002, código de práticas para gerenciamento de segurança da informação utilizado na criação de suas políticas de segurança. Esses guias fornecem às organizações os padrões detalhados para o gerenciamento de segurança em tecnologia da informação e orientações para se manter em conformidade com requisitos de possíveis auditorias (BHAIJI, 2008 *apud* LETTER TO EDITOR, 2012).

Netto e Silveira (2007) afirmaram que em uma política de segurança da informação, a camada física consiste no ambiente onde está instalado fisicamente o *hardware* – computadores, servidores, meio de comunicação – podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis. Para Adachi (2004) *apud* Netto e Silveira (2007), “a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs”. Os autores afirmaram que o controle de acesso aos recursos de TI, equipamentos para fornecimento ininterrupto de energia e *firewalls* são algumas das formas de se gerir a segurança desta camada.

A parte da política de segurança que trata do **controle de acesso** deve garantir que os indivíduos somente possam executar atividades às quais estejam autorizados. O **controle de acesso** garante que as requisições para um recurso específico estejam de acordo com a definição da política de segurança. Em termos de redes, o mecanismo mais comum utilizado para o **controle de acesso** são os *firewalls* e os roteadores de filtro.

Um *firewall* consiste em uma parte implementada por *software* ou *hardware* que filtra todo o tráfego de rede entre o computador, rede doméstica, ou rede da empresa e a *internet*. Todos que usam a *internet* precisam de algum tipo de proteção por *firewall* (O’Reilly, 1999). Conforme Damasceno (2005), um *firewall* deve rastrear e controlar o fluxo das comunicações que passam através dele. Para controlar as decisões, baseadas em serviços da pilha do protocolo TCP/IP, o *firewall* deve obter, armazenar, retornar e manipular as informações derivadas de todas as camadas de comunicação para todos os aplicativos (Figura 1).

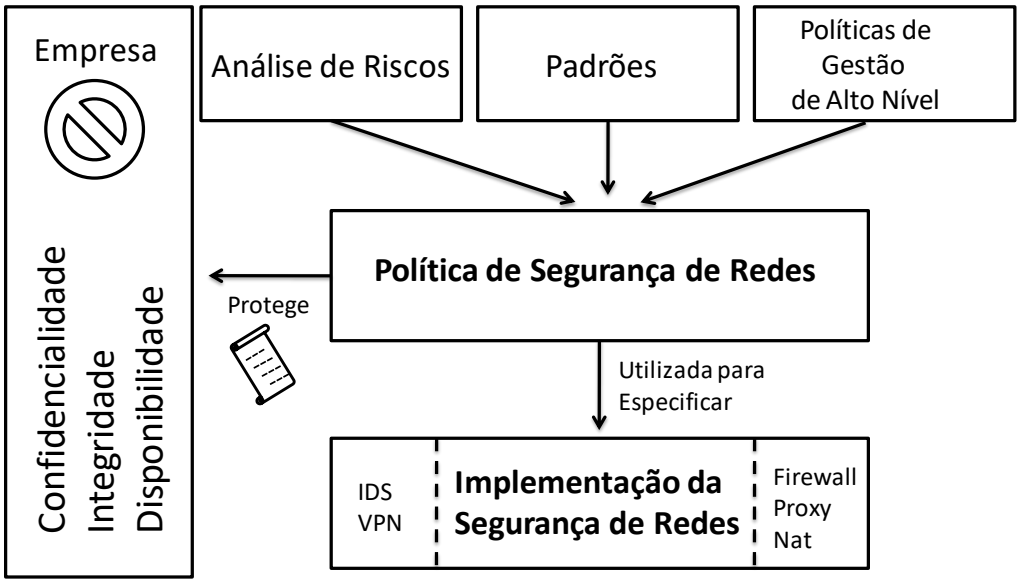

Figura 1 - Política de Segurança de Redes. Fonte: Editor Letter (2012).

Al-Shaer e Hamed (2003b) afirmam que a segurança em *firewalls*, como em qualquer outra tecnologia, requer um gerenciamento próprio para prover um serviço de segurança adequado. Possuir um *firewall* na rede não necessariamente faz essa rede segura. Um dos motivos para esse fato consiste na complexidade das regras de gerenciamento e na vulnerabilidade potencial da rede, devido a conflitos de configuração. O trabalho apresentado pelos autores mostrou técnicas para melhoria e proteção da política de filtragem de anomalias, que podem ser utilizadas na gestão de políticas de filtragem sem uma análise *a prior* dessas regras. Os autores continuaram o trabalho de pesquisa em Al-Shaer e Hamed (2004), onde foi mostrado que o gerenciamento de regras de *firewall*, especialmente para redes de empresas, tem se tornado uma atividade complexa e um ambiente propício para ocorrência de erros. As regras de filtragem dos *firewalls* devem ser escritas cuidadosamente e organizadas de forma a implementar de forma correta a política de segurança. A inserção ou modificação de regras de filtragem requer a análise dos relacionamentos entre a regra que será mudada e as demais regras, de forma a se determinar a ordem apropriada dessa regra e implantar as modificações. Na pesquisa dos autores, foi apresentado um conjunto de técnicas de algoritmos para descoberta automática de anomalias na política de *firewall*, revelando conflitos de regras e problemas potenciais em *firewalls* legados, bem como edição de política para inserção, remoção e modificação de regras livres de anomalias. A implementação foi feita por meio de uma ferramenta denominada "*Firewall Policy Advisor*", minimizando assim a ocorrência de vulnerabilidades por conta de erros na configuração do *firewall*. Liu e Gouda (2009) afirmaram que o entendimento e a análise da função de um *firewall* são muito difíceis, pelo fato do mesmo possuir um grande número de regras e essas regras muitas vezes são conflitantes. Segundo os autores, um modo efetivo para ajudar aos administradores de *firewalls* no entendimento e análise da função dos mesmos consiste na definição de consultas.

De forma complementar, Al-Haj e Al-Shaer (2011) propuseram um conjunto de métricas para a avaliação objetiva e comparação das dificuldades e semelhanças das políticas de acesso de *firewalls* isolados, com base no uso de regras, distribuição do

tráfego permitido e requisitos de segurança. A contribuição desse trabalho consistiu na identificação da conformidade e fraquezas de segurança visando otimizar a política e engenharia de segurança.

2.1 EVOLUÇÃO DOS *FIREWALLS*

O papel de um *firewall* em uma rede de computadores é muito semelhante ao de um *firewall* em um edifício. Assim como um *firewall* feito de concreto protege uma parte de um edifício, um *firewall* em uma rede garante que se algo de ruim acontece em um lado desse *firewall*, os computadores do outro lado não serão afetados. Ao contrário de um edifício de *firewall*, que protege contra uma ameaça muito específica (fogo), um *firewall* de rede tem o objetivo de proteger a rede contra muitos tipos diferentes de ameaças (O'REILLY, 1999).

Quando um ou mais computadores estão interligados através de uma rede, a comunicação efetuada entre eles é feita através de fragmentos de dados chamados pacotes. Um *firewall* atua diretamente sobre esses fragmentos de dados, analisando seu conteúdo e assim tomando decisões com base no conteúdo analisado, por isso são conhecidos, muitas vezes, como filtro de pacotes (BARTH, 2007, P. 15).

Pode-se afirmar que um *firewall* consiste basicamente em um dispositivo de proteção, servindo especialmente para proteção de riscos referentes aos:

- ✓ Dados: a **informação** mantida nos computadores (sigilo, integridade da informação e disponibilidade);
- ✓ Recursos: os próprios computadores; e
- ✓ Reputação.

As ameaças abrangidas pela atuação dos *firewalls* incluem vírus, *worms*, ataques de negação de serviço (*DoS*), outros tipos de ataques, *hackers* e invasões. *Hackers* estão perambulando pelas amplas extensões da internet. Qualquer bom *firewall* impede o tráfego de rede que passa entre a *internet* e a rede interna de uma empresa, organização ou mesmo residência (O'REILLY, 1999).

Damasceno (2005) afirma que não é suficiente somente o exame dos pacotes de forma isolada. O estado da informação (*State Information*) derivado de comunicações anteriores e de outros aplicativos é um fator essencial para fazer o controle de decisões para novas tentativas de comunicação. Dependendo da tentativa de conexão, o estado da comunicação (derivada de comunicações anteriores) e o estado da aplicação (derivado de outras aplicações) podem ser críticos no controle de decisões.

Existe uma necessidade frequente de se conhecer o nível de proteção oferecido por um *firewall*, bem como suas deficiências. *Firewalls* não são *softwares* ou equipamentos que podem simplesmente ser retirados da caixa, conectados na rede e utilizados instantaneamente. Precisam ser configurados adequadamente, geralmente seguindo uma política de segurança da informação corporativa, para que possam atender necessidades específicas de cada rede. Além disso, essa configuração é dinâmica e precisa ser revista periodicamente, seja quando novas vulnerabilidades são descobertas, quando são efetuadas alterações na arquitetura da rede ou ainda quando existe modificação na política de segurança da informação corporativa (BARBOSA, 2006, p. 1).

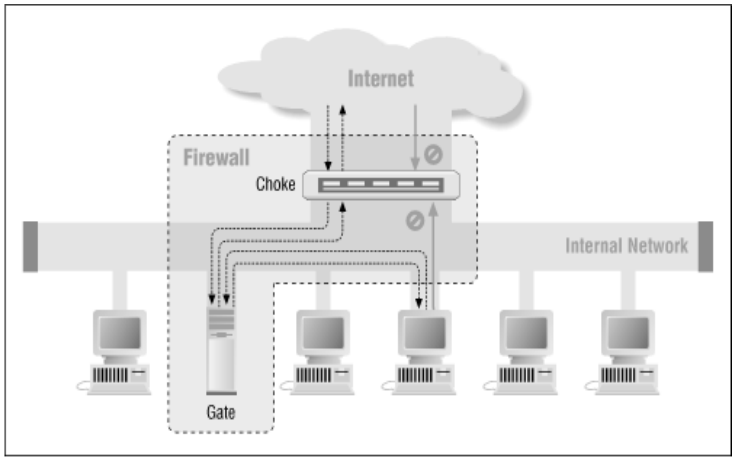

Figura 2 - Firewall tradicional. Fonte: O'Reilly, 1999.

Depois de sua instalação, deve-se alterar os padrões de rede para permitir o tráfego selecionado através do *firewall*. As portas de rede são concebidas para proporcionar uma abertura e ainda garantir a segurança para todos os usuários. Na configuração de um *firewall*, são criadas algumas aberturas controladas que não comprometem a segurança da rede, mas permitem o tráfego de rede selecionado passar, projetando a defesa contra ataques provenientes da *internet*. Entretanto é prudente nunca se confiar em uma única forma de proteção para a rede, o que pode passar uma falsa sensação de segurança. A Figura 2 ilustra o funcionamento de um *firewall* tradicional, enquanto a Figura 3 ilustra um *firewall* porta *dual host.*

A maioria das organizações atualmente possuem uma rede interna que interliga os seus sistemas de computador. Geralmente existe um grau elevado de confiança entre os sistemas informáticos nessa rede, especialmente se a rede é privada. No entanto, muitas organizações necessitam dos benefícios de se conectar à *internet,* que consiste em uma rede inerentemente insegura. Algumas das ameaças inerentes ao fato de se manter uma conexão com a *internet* incluem:

- ✓ Conexão fraca ou sem necessidade de autenticação;
- ✓ *Software* inseguro;
- ✓ Facilidade de *Masquerade* (*Spoofing*);
- ✓ Programas de *Sniffer*; e
- ✓ Programas *Cracker*.

Os *softwares firewalls* podem ser baixados pela *internet* a partir de várias fontes fidedignas ou comprados em qualquer lugar onde se compra um *software* de computador. Provedores de *internet* também são uma boa fonte para *hardware* e *software* de *firewall* que foram testados e certificados. Os *firewalls* de *hardware* (*appliances*) e sofisticados sistemas de detecção de intrusão para grandes organizações, podem ser adquiridos de empresas especializadas em segurança de rede (O'REILLY, 1999).

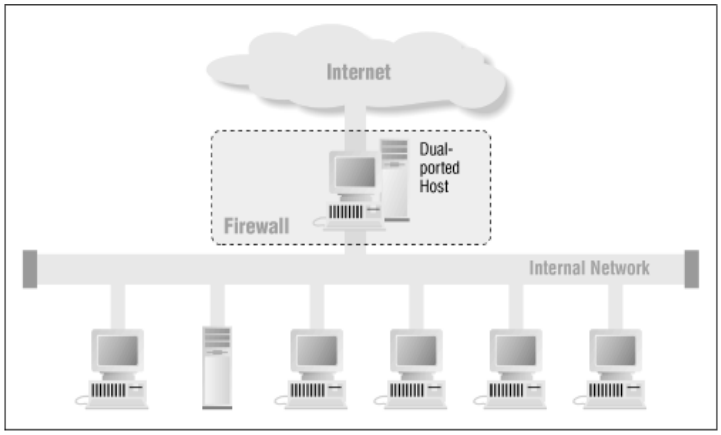

Figura 3 - Firewall porta dual. Fonte: O'Reilly, 1999.

As contribuições do trabalho de Liu e Gouda (2009) incluíram a proposta de uma linguagem do tipo SQL denominada Structured Firewall Query Language, para descrever a consulta em firewalls. Os autores apresentaram um teorema denominado Firewall Query Theorem, como a base para o desenvolvimento de algoritmos para processamento de consultas em firewall. O algoritmo de processamento de consultas que utiliza diagramas de decisão na sua estrutura de dados principal foi considerado eficiente pelos autores. Os resultados obtidos indicaram que o algoritmo de processamento de consultas foi muito eficiente. Também foram apresentados métodos para otimização dos resultados de consultas. Por último, foram apresentados os métodos para execução das operações de união, interseção e subtração nos resultados da consulta em firewall.

2.1.1 Histórico da utilização dos *firewalls* pelas organizações

Nos primórdios da *internet*, um erro de programação fez com que um programa saísse de controle e afetasse cerca de seis mil servidores dos 60 mil existentes na época. Com uma preocupação em relação às conseqüências do '*verme de Morris*', a ARPA criou o CERT (*Computer Emergency Responce Team*), que tinha como objetivo a pesquisa e o aprimoramento da segurança na rede. "O primeiro *firewall* - num sistema de *hardware* e *software* destinado a impedir acesso não autorizado - tinha sido criado pela *Digital Equipment Corporation* dois anos antes" (RANGEL, 2009).

Em 1990 surgiram efetivamente os primeiros *firewalls* para segurança de redes. Eram dispositivos com regras do tipo: "Alguém da rede **A** pode acessar a rede **B**, ou alguém da rede **C** não pode acessar a rede **B**. Esses *firewalls* eram efetivos, mas bastante limitados. Como exemplo, era muito difícil configurar as regras corretamente" (MADEIRA, 2006, p. 1).

Existia uma escolha a ser feita, entre dois tipos de conexões com a *internet*: via um modem *dial-up* com conexão lenta para os indivíduos e as organizações de menor dimensão, ou uma conexão rápida e muito cara para as grandes empresas e instituições. Hoje pode-se escolher entre vários tipos de conexões com a *internet*, cada um deles

fornecendo velocidades de acesso diferentes e os riscos de segurança diferentes. Cada vez mais, essas escolhas estão se tornando disponíveis em muitas partes do mundo (O'REILLY, 1999).

Uma das grandes dificuldades encontradas pelos administradores de redes consiste na validação da configuração dos sistemas de *firewalls* para que operem de maneira satisfatória, seguindo as especificações estabelecidas na política de segurança da informação corporativa que, por sua vez, contempla a política de restrição de comunicação, sendo descrita em linguagem de alto nível (AL-SHAER, 2003a). Os administradores de rede são responsáveis por implementar a política de segurança usando, na maioria das vezes, uma linguagem de baixo nível para configurar as *bases-de-regras* desses equipamentos de proteção de redes de computadores. Além disso, determinadas funcionalidades dos *firewalls* necessitam de regras específicas para habilitá-las, não sendo simples se determinar sua configuração correta ou se alguma funcionalidade de proteção está ativa (BARBOSA, 2006, p. 1).

Um fator importante consiste na **largura de banda** - a quantidade de dados que pode transferir através de uma conexão de rede. A largura de banda é diretamente relacionada à velocidade de conexão. Velocidades de transferência de rede e modem são normalmente medida em bits por segundo (*bps*) (O'REILLY, 1999).

Os computadores mantém o controle de dados usando um sistema binário no qual todos os caracteres são convertidos em zeros e uns. Um *bit* é um único ou um zero. A maioria dos caracteres do alfabeto, incluindo números e caracteres especiais, pode ser expressa usando oito bits, o que é muitas vezes referida como um *byte*. Assim, se uma conexão de rede permite a transferência de dados de 8 *kilobits* por segundo (que é 8.000 bits por segundo), ou 8 *Kbps*, o computador irá transferir cerca de 1.000 caracteres por segundo - menos um pouco por causa da sobrecarga para manter o controle da conexão (O'REILLY, 1999).

A transmissão costumava ser uma medida comum para velocidades de modem. A transmissão é uma medida para o número de sinais elétricos que são enviados por segundo. Em baixas taxas de transferência o número de transmissão é idêntica à taxa de *bps*, mas a taxas superiores a dois diferentes. Ao comparar as velocidades deve-se atentar para os números *bps*. Esses números são fáceis de interpretar e comparar: Quanto maior o número, mais rápida a conexão. Os *quilobits por segundo* (*Kbps*) são de cerca de 1.000 *bps*, e um *megabit por segundo* (*Mbps*) é aproximadamente 1 milhão de *bps* (O'REILLY, 1999).

Esse conceito começou a ser utilizado no final da década de 80, quando roteadores faziam a separação de pequenas redes. Dessa forma, as redes, então separadas, poderiam instalar aplicativos e gerenciar seus recursos de redes da forma que bem entendessem. Caso essas aplicações apresentassem algum problema congestionando a rede, as redes dos demais segmentos não seriam afetadas (MADEIRA, 2006, p. 1).

A maioria das conexões *dial-up* usam um modem para se conectar à *internet*, assim todos os dados entre o computador e o provedor de serviços *internet* (ISP) são transmitidos através POTS (*Plain Old Telephone Service*), também conhecida como rede de telefonia PSTN (*Public Switched*). A tecnologia atual dos *modems* permite uma conexão a velocidades de até 56 *Kbps* considerada rápida se comparada com as velocidades que estavam disponíveis há apenas alguns anos atrás, mas 'dolorosamente' lenta em comparação com a maioria das tecnologias disponíveis. Um modem de 56 *Kbps* pode se conectar a essa velocidade apenas em circunstâncias ideais, o que quase nunca acontece. As condições da linha, centrais telefônicas demais, e as limitações de

regulamentação podem contribuir para limitar a largura de banda real que pode atingir. Depois de conectado, se pode transmitir dados apenas na velocidade máxima da direção a jusante, a partir do ISP para o computador. A tecnologia da época limitava as ligações a montante do computador para o ISP para 33,6 *Kbps*. Ainda assim, por causa de seu baixo custo, os *modems* ainda são usados por uma grande quantidade de pessoas para se conectar à *internet*. Alguns *modems* não operam mesmo a 56 *Kbps*. Os modems e as condições da linha podem ter um efeito sobre a taxa de transferência de dados reais (O'REILLY, 1999).

A segunda geração de *firewalls* foi bem mais elaborada, pois usavam filtros de pacotes e de aplicativos (*proxy*) além de trazer uma *GUI* (*Graphic User Interface* – Interface gráfica) para gerenciar as políticas de *firewall*. Estes dispositivos eram conhecidos como *Bastion Hosts* (computadores que são expostos totalmente a um ataque, sendo colocado no lado da *DMZ - Demilitarized zone*, desprotegido por um *firewall* ou por filtros de roteadores. *Firewalls* ou roteadores que provêm acesso de controle ao perímetro da rede, são considerados *Bastion Hosts*. Provavelmente, o primeiro produto dessa geração, foi o *DEC Firewall*, desenvolvido pela equipe de *Network Systems* da *Digital Equipment Corporation*. O primeiro *DEC firewall* foi configurado e instalado para o primeiro cliente, uma grande empresa química da costa leste americana, em 13 de junho de 1991. Durante os próximos meses, Marcus Ranum da DEC, inventou *proxies* de segurança e re-escreveu muito do código do *firewall*. O *firewall* foi produzido e batizado do *DEC SEAL* (*Security External Acess Link*). O *DEC SEAL* era composto de um elemento externo chamado de *Gatekeeper*, de um *gateway* de filtragem, conhecido como *Gate* e um dispositivo interno chamado *Mail Hub*. No mesmo momento, Cheswick e Bellovin da Bell Labs, experimentavam um *firewall* baseado em comutação de circuito. O produto originado desse experimento foi chamado de *Raptor Eagle*, que chegou depois de seis meses depois do *DEC SEAL*. Em seguida foi lançado o *ANS Interlock*. Em 1 de Outubro de 1993, foi lançado o *TIS* (*Trusted Information Systems*) *FWTK* (*Firewall Tookit*) em código fonte para a comunidade da *internet*. Ele disponibilizava a base para o produto comercial *TIS firewall*. Um tempo depois ele foi chamado de *Gauntlet*. Esse produto foi usado por desenvolvedores, governos e indústria como base para sua segurança de acesso a *internet* (MADEIRA, 2006, p. 1).

Com um *modem* deve-se estabelecer uma nova conexão cada vez que quiser se conectar à *internet*. De um ponto de vista da segurança, no entanto, a característica de uma conexão *dial-up* é salutar para a gestão. Durante todas as outras vezes, ninguém na *internet* poderá contatar o computador e entrar via sua conexão (O'REILLY, 1999).

As ligações *RDIS*, linha *ISDN* (*Integrated Services Digital Network*) e conexão *dial-up* têm uma grande semelhança. São usados para as comunicações de voz e transmissão de dados. Uma diferença principal entre as tecnologias consiste em que usar uma linha *ISDN* permite uma chamada de voz e transferência de dados ao mesmo tempo (O'REILLY, 1999). A outra diferença principal é que um *ISDN* permite transferir dados a velocidades superiores que a conexões *dial-up* permite. Dependendo da implementação *ISDN* exata, são possíveis velocidades de até 128 *Kbps*. Instalar e configurar o *ISDN* requer mais habilidade e esforço do que ligar um *modem* a uma linha telefônica, mas muitas pessoas acham que vale a pena o esforço extra para conseguir uma conexão mais rápida (O'REILLY, 1999).

O mais novo tipo de conexão que as companhias telefônicas estão oferecendo é chamado de *Digital Subscriber Line* (*DSL*). *DSL* é um acessório interessante para o serviço de telefone que permite que dados de alta velocidade sobre as transmissões de

linhas telefônicas comuns, permitindo usar a linha telefônica para uma chamada de voz ao mesmo tempo.

Comunicação interna consiste nas interações, nos processos de trocas e nos relacionamentos dentro de uma empresa, sendo responsável pela circulação das informações e conhecimentos entre todos os níveis (Leite, 2006). A comunicação interna oferece agilidade e leveza nos processos organizacionais, criando o hábito nos colaboradores de busca e transmissão de comunicação constante. De acordo com Veríssimo (2003) uma equipe que não se comunica não tem comprometimento, perde tempo e não alcança os objetivos. Para Pessoa (2003), a comunicação interna forma multiplicadores dos valores, atividades e produtos da empresa. É importante que o público interno esteja sempre bem informado, sendo o primeiro, a saber, sobre as notícias da empresa, pois quanto mais o funcionário conhece a organização, mais se integra e se adapta ao estilo administrativo.

O processo de comunicação deve ser valorizado e disponibilizado de forma eficaz e atrativa, visando integrar os maiores propagandistas da organização, que são seus funcionários. Segundo Nassar (2006), ao promover a comunicação interna, deve-se levar em conta que comunicar é uma tarefa única, que deve atrair e envolver.

Os gestores devem compreender a importância da comunicação no ambiente dos negócios e no relacionamento com seus funcionários, prezando o espírito de trabalho em equipe, gerando confiança e lealdade entre os membros. Para Argenti (2006) os funcionários esperam que quando suas opiniões são solicitadas, a gerência os escute e atue para atendê-las. O papel dos gestores não se restringe apenas ao processo da comunicação, pois gerenciar bem os projetos é fator indispensável para a obtenção dos resultados de forma satisfatória. De acordo com Nassar (2006) no ambiente atual de constantes mudanças sociais, políticas e econômicas, é inquestionável o papel do gestor em manter atualizado seu público interno (funcionários, terceirizados e prestadores de serviço) sobre o papel que devem desempenhar.

2.1.2 Necessidade da segurança em redes

Computadores com conexões *online* permanentes são o alvo favorito dos *hackers*. Alguns computadores, especialmente computadores baseados no sistema operacional *windows* com recursos compartilhados, do tipo pastas compartilhadas ou impressoras, podem ter esses recursos compartilhados facilmente encontrados e conectados. Em uma rede doméstica que utiliza um *modem* por cabo, os computadores podem anunciar seus recursos compartilhados para todos no mesmo segmento de cabo. Apesar de uma conexão de *modem* por cabo não representar um perigo para um computador configurado com segurança, muitas pessoas não tomam as precauções de segurança adequadas e de repente descobrem que um desconhecido foi conectado ao seu computador ou que tenha sido enviada uma mensagem à impressora (O'REILLY, 1999).

É possível que persistam falhas de segurança na configuração de um *firewall* (KAMARA, 2003; NOURELDIEN, 2000; WOLL, 2004a), o que permite perceber a complexidade de projetar, implementar, gerenciar e testar uma ou mais bases de regras de *firewalls*, o que dependendo da dimensão da rede, quantidade e modelos de equipamentos existentes, o que pode tornar essa tarefa ainda mais complexa. Como

conseqüência dessas dificuldades, pode-se ter uma configuração inadequada do *firewall*, resultando em uma falsa sensação de segurança.

Dessa forma, existe a necessidade de conhecer efetivamente que tipo de pacotes o que o *firewall* permite, descarta ou restringe e mecanismos de proteções existentes, ou seja, necessita-se conhecer o comportamento do *firewall*. Essa necessidade pode surgir em diversas situações como, por exemplo, quando é efetuada uma análise pela equipe de segurança de redes, por uma equipe de auditoria para confirmação de que as normas definidas na política de segurança foram aplicadas conforme a especificação, ou até mesmo para se descobrirem falhas de segurança de rede (BARBOSA, 2006, p. 1).

A pilha de protocolos *TCP/IP* (POSTEL, 1981a; POSTEL, 1981b), cujo projeto original possui mais de 25 anos de existência, é largamente utilizada para interligação de redes atualmente. O propósito do projeto original não previa uma variedade de aplicações e um crescimento na escala como nos dias atuais. Desta forma, apresenta diversas vulnerabilidades de segurança inerentes aos protocolos originais e também aos que foram sendo implementados e incorporados desde então, para atender as novas tecnologias e necessidades dos usuários das redes de computadores (BARBOSA, 2006, p. 1).

2.1.3 Perímetros com o uso de *firewall*

O *software* inseguro, particularmente do tipo *shareware*, gratuitos ou pacotes de baixo custo, muitas vezes têm *bugs* ou falhas de projeto, geralmente resultantes de um projeto deficiente ou testes de *software* insuficientes. Entretanto, devido a sua pronta disponibilidade e baixo custo, muitas pessoas continuam a usar esses tipos de pacotes. Exemplos incluem: o programa *sendmail* do UNIX, o qual teve inúmeras vulnerabilidades relatadas, e um produto de FTP *freeware* que continha um *malware* do tipo *cavalo de tróia* que permitia privilégio de acesso ao servidor (O'REILLY, 1999).

Opções exclusivas para pacotes *TCP / UDP* (BARTH, 2007, P. 19):
- *Source Port*: Porta de origem do pacote;
- *Destination Port*: Porta de destino do pacote;

Opções exclusivas para pacotes *ICMP* (BARTH, 2007, P. 19);
- *ICMP Type*: Tipo de mensagem ICMP.

Opções explícitas (BARTH, 2007, P. 19):
- *State*: Estado da conexão utilizada pelo pacote.

Em 1994, o CERT relatou que milhares de sistemas na *internet* tinham sido comprometidos por *hackers* e programas *sniffer* instalado neles. Os programas *sniffer* de rede monitoram o tráfego de usuários e senhas, tornando essas informações disponíveis para o *hacker* posteriormente (O'REILLY, 1999).

Os programas do tipo *cracker*, amplamente disponíveis na *internet*, são executados em segundo plano em uma máquina, criptografando milhares de palavras diferentes e comparando com as senhas criptografadas armazenadas na máquina. Estes ataques chamados de dicionário (porque as palavras são realizadas em um dicionário)

muitas vezes são bem sucedidos, proporcionando ao *hacker* obter até um terço das senhas em uma máquina (O'REILLY, 1999).

Existe uma grande importância na realização de um esquema de testes para descoberta do comportamento de mecanismos de proteção ativos em *firewalls*. Por esta razão existem tantas ferramentas disponíveis visando efetuar testes de *firewalls* e tanto esforço por parte dos pesquisadores para aprimorar essas ferramentas.

Para assegurar um alto nível de segurança, um *firewall* deve ser capaz de acessar, analisar e utilizar (DAMASCENO, 2005):

- **Comunicação da Informação**: Informação das 07 camadas do pacote;
- **Estado derivado da comunicação**: O estado derivado de comunicações anteriores. Por exemplo, o comando de porta de saída de uma sessão FTP deve ser salvo assim que o canal de informação FTP for verificado, mantendo o estado da conexão;
- **Estado derivado da aplicação**: É a informação de estado derivado de outras aplicações. Por exemplo, uma autenticação feita anteriormente por um usuário deveria ser permitida através do firewall para somente os serviços autorizados;
- **Manipulação da informação**: A habilidade de executar funções lógicas ou aritméticas de informações em qualquer parte do pacote.

Conforme Damasceno (2005), a engrenagem de inspeção denominada *stateful inspection* supera todos os requisitos de segurança definidos por qualquer outra tecnologia de *firewall*, tal como filtros de pacotes e *gateways* de camada de aplicação (*proxys*). Com o *stateful inspection* os pacotes são interceptados na camada de rede, pois gera melhor performance para análise (como filtro de pacotes), então os dados derivados de todas as camadas de comunicação são acessados e analisados para prover o melhor estado de segurança (análise comparada aos *gateways* de aplicação, camadas de 4 a 7), isto introduz um alto nível de segurança por incorporar o estado derivado de comunicações e aplicações e o contexto de informações que são armazenadas e atualizadas dinamicamente. Esta tecnologia também pode rastrear protocolos sem conexão, como por exemplo, *RPC* e *UDP*, nenhuma outra tecnologia de *firewall* pode executar estas funções.

Existe uma lacuna deixada quando se trata de ferramentas de análise ativa, por injeção de pacotes e observação de resultados aplicadas a testes de *firewalls*, já que a maioria das ferramentas são desenvolvidas para descoberta de erros de sintaxe nas bases de regras, geração automática de regras, efetuando análise passiva e geralmente se aplicando a *firewalls* de fabricantes específicos.

Damasceno (2005) ainda cita que os *softwares* de *firewall* são muito utilizados. Os *firewalls* com tecnologia "*stateful inspection*" e os anteriores a esta 3ª geração, tiveram início somente como *softwares* funcionando em servidores não-dedicados a esta função, sem um *hardware* especificamente criado para a tecnologia. Denomina-se de *appliance* este tipo de *hardware* específico, criado unicamente para atender a aplicações específicas de *firewall*. Os *appliances* são procurados devido a sua fácil instalação e custo baixo, pois o *software* que roda em um *appliance* tem seu preço menor do que as aplicações similares para servidores de redes. Outra vantagem do *appliance* é que o *firewall* é desenvolvido voltado para o *hardware* do *appliance*, ou seja, ganha maior velocidade, pois não depende de paradigmas de compatibilidade de placas e sistemas que os servidores de redes tendem a enfrentar. Possui também algumas desvantagens, como por exemplo, o *appliance* pode cair no esquecimento e não sofrer atualizações,

afinal não tem o mesmo manuseio que um servidor de rede e quando tem interface gráfica (*web*), esta não é interativa como a GUI (*Graphic User Interface*) dos servidores. No caso da empresa já possuir em seu legado servidores com sistemas operacionais *Microsoft*, *Novell Netware*, *UNIX*, *AS400*, e *Linux*, torna-se lucrativo utilizar os *softwares* de *firewall* compatíveis com seus fabricantes, para não favorecer o desperdício de recursos com a aquisição de um *appliance*. Entretanto, em um projeto que se inicia, a melhor opção consiste na utilização de um *appliance*.

Independente da escolha entre *appliance* ou *softwares*, Damasceno (2005) recomendou que uma boa escolha consiste em produtos de empresas consolidadas no mercado, como por exemplo:

- Firewall appliances

- *CiscoPIX;*
- *Nokia Checkpoint Firewall;*
- *Watchguard Firebox;*

- ***Firewall softwares***

- *Check Point NGAI - Next Generation Application Intelligence;*
- *Microsoft ISA Server;*
- *IPTables Project.*

A escassez, bem como as limitações apresentadas pelas ferramentas de testes existentes, quando se deseja verificar a aderência das regras implementadas à política de restrição de acesso a rede da empresa, impedem uma estimativa mais precisa sobre o comportamento dos *firewalls* (BARBOSA, 2006, p. 1).

Esses programas, disponíveis livremente na *internet*, enviam mensagens para todas as portas *TCP* e *UDP* de um computador remoto, visando verificar se alguma delas estão abertas e à espera para receber uma chamada. Uma vez que uma porta aberta foi localizada, o *hacker* tenta chegar ao computador através da mesma (O'REILLY, 1999).

O *Masquerade* (*Spoofing*) faz com que seja relativamente fácil para os *hackers* explorarem a confiança inerente à *internet*, ou capturar senhas e reproduzi-las. Falhas de segurança incluem: o protocolo *SMTP* que usa mensagens *ASCII* para transferir mensagens, possibilitando a um *hacker* acessar via *Telnet* uma porta *SMTP* e simplesmente digitar uma mensagem de *e-mail* falsa; um recurso chamado *roteamento IP fonte* permite que um chamador falsifique seu endereço IP, e forneça ao destinatário com um caminho de retorno diretamente de volta a si mesmo. (O'REILLY, 1999).

A função *Masquerade* é muito parecida com a do *Snat*, porém um pacote que é tratado por essa tabela demora um pouco mais para ser processado, pois, ao invés de trocar o IP de origem para um IP determinado, o *Masquerade* procura qual o IP válido, e somente então faz a troca do IP de origem. Essa técnica é muito usada quando o acesso à *internet* que o *firewall* controla possui IP dinâmico (BARTH, 2007, P. 22).

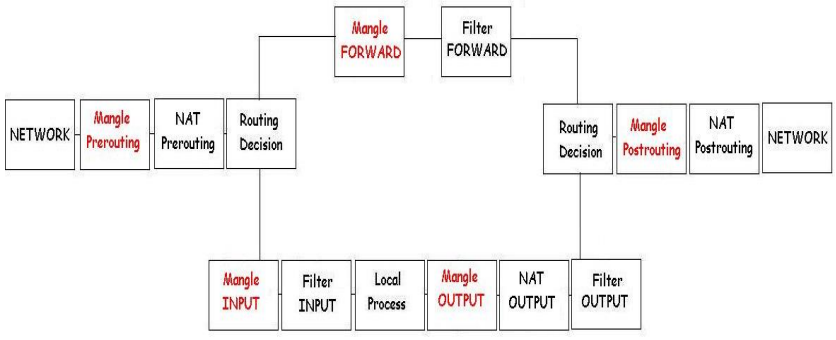

Figura 4 - Diagrama de fluxo de pacotes IPTables, considerando todas as tabelas. Fonte: Barth, 2007, p.22.

Downtime: falhas na rede acontecem, e muitas vezes a melhor coisa que os empregados podem fazer é cruzar os braços e dizer ao cliente para ligar novamente mais tarde. Prevenção de intrusões da *internet* podem custar um pouco de dinheiro, mas a quantidade de dinheiro perdido devido a interrupções causadas por uma tal intrusão pode custar muito mais (O'REILLY, 1999).

Cada vez que um ataque a uma rede for bem sucedido, deve levar tempo para consertar o problema e para reparar qualquer dano. Por exemplo, se um vírus infecta os computadores da empresa, o mesmo deve ser removido de cada computador e reparados os danos. Outra consideração importante de segurança, que se aplica a cada tipo de conexão, consiste no tipo de endereço de rede que está atribuído ao computador. Alguns tipos de conexões, como conexões *dial-up* via modem, dão ao computador uma nova rede de endereços cada vez que o mesmo se conecta, o que é referido como um endereço dinâmico. Endereços dinâmicos tornam difícil para um *hacker* iniciar qualquer esforço prolongado para invadir um computador. Algumas ligações à *internet* utilizam endereços estáticos. Usar um endereço estático significa que o computador recebe o mesmo endereço toda vez que se conecta à *internet* (O'REILLY, 1999).

As conexões *T1* e *T3* quase sempre usam endereços estáticos, algumas conexões *DSL* e ainda *cable modem*. Mesmo com endereços que mudam as conexões, essas mudanças não podem ocorrer freqüentemente. Quando um *hacker* sabe que ele ou ela pode se conectar a um endereço único e conectar ao computador, o *hacker* é capaz de lançar ataques. Apesar de endereços estáticos representarem um risco, eles fornecem um método previsível para se acessar o computador via *internet*, incluindo as conexões que são legítimas. Por exemplo, ao executar um servidor *web*, as pessoas precisam ser capazes de encontrar o seu computador. Ao mesmo tempo, os endereços estáticos facilitam a vida dos *hackers* (O'REILLY, 1999).

Uma das principais deficiências no aspecto de segurança do protocolo IP é sua fraqueza em identificar e autenticar um computador na rede (Bellovin, 1989), ou seja, com base no endereço IP de origem de um *datagrama IP* recebido, nem sempre é possível determinar com certeza a identidade do computador que o tenha originado. Além disso, também há poucas garantias de que o conteúdo de um *datagrama IP* recebido não tenha sido modificado ou observado quando em tráfego pela rede, ou seja, que a integridade dos dados contidos no pacote tenha sido preservada. Os ataques que exploram tal falha têm como tática mais comum a personificação de um computador na rede. A finalidade consiste desde obter informações sigilosas como senhas, abuso da confiança que as máquinas mantêm entre si, até alterações do conteúdo dos dados que estejam de passagem para outros computadores de destino (BARBOSA, 2006, p. 1).

No se refere à *internet* e *firewalls* a forma de comunicação mais importante, consiste no *TCP/IP* (*Transmission Control Protocol / Internet Protocol*). Um nível de consideração importante para o protocolo *IP* do ponto de vista para a filtragem de pacotes é a fragmentação e remontagem de *datagramas*, se necessário, para transmissão por uma rede de computadores. Ou seja, o protocolo *IP* tem capacidade de dividir um grande *datagrama* que, caso contrário, não conseguiria atravessar algum enlace de rede (devido a limitações de *MTU* do enlace), em *datagramas* menores, denominados fragmentos, e remontá-los posteriormente. A *RFC 791* (Postel, 1981b) descreve um algoritmo de remontagem de fragmentos que assume a sobreposição de fragmentos, caso o valor do campo *FO* (*Fragment Offset*) seja inferior ao tamanho do fragmento anterior. (BARBOSA, 2006, p. 1).

A maioria dos *firewalls* examina o cabeçalho do pacote para determinar se o pacote deve ser permitido entrar ou sair de uma rede atrás de um *firewall*. O cabeçalho

contém informações importantes sobre um pacote, tais como o origem, o destinatário e, mesmo se o programa no computador de destino deve processar as informações contidas no pacote. Este programa poderia ser um servidor *web* ou um aplicativo de servidor de *email*. Alguns *firewalls* também podem examinar o interior de um pacote ou o interior de vários pacotes, como todos os pacotes que compõem uma mensagem de correio eletrônico ou uma página da *web* e, em seguida, decidir como lidar com esse tráfego (O'REILLY, 1999).

Os principais campos existentes nos cabeçalhos dos pacotes que podem ser comparados são (BARTH, 2007, P. 19):

- Protocolo: Protocolo do pacote (TCP/UDP/ICMP);
- *Source*: IP de origem do pacote;
- *Destination*: IP para qual se destina o pacote;
- *In Interface*: Interface de entrada utilizada pelo pacote;
- *Out Interface*: Interface de saída utilizada pelo pacote.

Como o tráfego de rede passa pelo *firewall*, o mesmo decide se o tráfego vai para a frente, com base em regras definidas anteriormente. Todo o tráfego de *firewall* vem em rede, mas um bom *firewall* também deve ter tela de tráfego de saída. Normalmente, um *firewall* é instalado na rede interna quando conecta-se à *internet* (O'REILLY, 1999).

Normalmente, qualquer roteador pode fragmentar um *datagrama*, a não ser que um sinalizador no cabeçalho IP esteja negando esta permissão. Porém, se um roteador precisar fragmentar um *datagrama* e encontrar esta permissão negada, descartará o pacote, possivelmente causando uma falha na comunicação. Geralmente este fato é menos desejável do que ter o pacote fragmentado (ZIEMBA, 1995).

O problema com a fragmentação consiste em que apenas o primeiro fragmento de cada pacote contém as informações de cabeçalho de protocolos de nível mais alto (como o TCP) de que o sistema de filtragem de pacotes necessita para decidir se deve ou não deixar passar o pacote completo (BARBOSA, 2006, p. 1).

Embora as organizações maiores possam colocar *firewalls* entre as diferentes partes de sua rede própria, que exijam diferentes níveis de segurança, o tráfego maior do conjunto de *firewalls* passa entre uma rede interna e a *internet*. Essa rede interna pode ser um único computador ou pode conter milhares de computadores (O'REILLY, 1999).

As características mais comuns de *firewalls* são:

✓ **Bloquear o tráfego de rede com base na origem ou destino** é a característica mais comum de um *firewall*.

✓ **Bloquear o tráfego de saída da rede com base na origem ou destino**: Muitos *firewalls* podem bloquear pelo tráfego de rede de sua rede interna à Internet.

✓ **Bloquear o tráfego de rede com base no conteúdo**: *Firewalls* mais avançados podem monitorar o tráfego de rede para o conteúdo inaceitável. Por exemplo, um *firewall* que é integrado com um scanner de vírus pode impedir que os arquivos que contêm vírus entrem na rede.

✓ **Tornar os recursos internos disponíveis**: Embora o objetivo principal de um *firewall* seja impedir o tráfego de rede indesejado através dele, pode-se configurar muitos *firewalls* para se permitir o acesso seletivo aos recursos internos, tais como um servidor *web* público, mas ainda impedindo o acesso de outros da *internet* para a rede interna.

✓ **Permitir conexões de rede interna**: Um método comum para os empregados se conectarem a uma rede usando redes privadas virtuais (VPNs). A VPN permite conexões seguras a partir da *internet* para uma rede corporativa.

✓ **Relatório sobre tráfego de rede e atividades do *firewall***: Quando o tráfego de rede para a *internet* é guardado em *logs*, é importante se saber o que o *firewall* está fazendo, durante as tentativas de invasão à rede, e ainda quem tentou acessar material impróprio na *internet*. A maioria dos *firewalls* incluem um mecanismo para gerar *logs* de informação de algum tipo ou de outro.

No caso de um único computador (PC), ou talvez dois ou três computadores em um único *site*, ligado à *internet*, existem duas opções lógicas: executar o programa de *firewall* no PC ou no *Internat Service Provider* (ISP). Executando o programa no PC o controle é maior, mas também aumenta a responsabilidade pela gestão do *firewall* (O'REILLY, 1999).

Executar o *firewall* no ISP tem o encargo de gestão, mas normalmente reduz a liberdade em termos de escolha e customização de *software.* No caso de vários PCs no mesmo local compartilhando uma rede local (LAN) e/ou DSL, via cabo ou outra conexão de *internet* de alta velocidade, o *software* de *firewall* deve ser executado em um computador especialmente projetado, também chamado de *firewall*. Esse fato permite que múltiplos computadores compartilhem o *firewall* e diminui os custos administrativos. Sistemas de *hardware* de *firewall* permitem um "faça você mesmo" e o projeto pode ser gerido e controlado por um terceiro (O'REILLY, 1999).

Conforme Liu (2012), uma grande causa para os erros de política que existem nos *firewalls* são as mudanças na política. As políticas do *firewall* devem ser mudadas à medida que a rede evolui e surgem novas alternativas. Os usuários por trás do *firewall* frequentemente solicitam ao administrador do *firewall* a modificação das regras, de forma a proteger a operação de alguns serviços. O autor apresentou um *framework* para a execução da análise de impacto para mudanças de políticas de *firewall*.

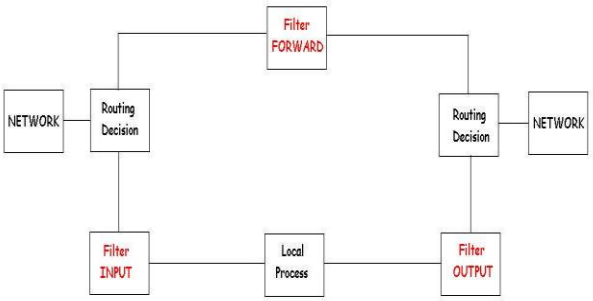

Figura 5 - Diagrama de fluxo de pacotes IPTables, levando em conta a tabela filter. Fonte: Barth, 2007, p.20.

2.1.4 Tendências do mercado com o uso do Gerenciamento Unificado de Ameaças

A necessidade de proteção das aplicações é uma verdade fundamental para as organizações, um desafio interminável. Uma ampla gama de tendências em curso garante muita atividade para a segurança pessoal. Uma mudança na motivação dos *hackers* levou ao desenvolvimento de ameaças cada vez mais fugazes que estão

surgindo e se espalhando em uma taxa alarmante. Outros fatores incluem um fluxo constante de novas vulnerabilidades que precisam ser abordadas, o crescente nível de mobilidade dos usuários, a inter-conectividade entre as organizações - tendências de introduzir mais "pontos de entrada" e enfatizar a necessidade de implantar medidas defensivas não apenas nos limites de *internet* óbvios, mas em todo o ambiente computacional interno e nos terminais individuais (BOUCHARD, 2006).

As organizações necessitam de uma melhor maneira de aumentar sua visibilidade, definir e aplicar políticas de segurança, bem como identificar e prevenir ameaças. Nesse sentido, o gerenciamento unificado de ameaças (UTM) é uma medida poderosa e adequada na direção certa. As reduções de custo e complexidade e melhorias na eficácia que podem ser alcançadas tem uma ampla gama de recursos de segurança disponíveis em um único dispositivo são claramente vantajosas. No entanto, é extremamente importante o reconhecimento de que nem todos os produtos de UTM são criados da mesma forma. Realizar plenamente os benefícios associados dependerá em última análise na medida em que um determinado produto tem as características de uma melhor solução na sua classe, como a qualidade e abrangência da segurança individual e componentes de rede (BOUCHARD, 2006).

Para a maioria das organizações, dedicada (ou seja, um único propósito) a ameaça de gestão produtos também precisa ser implementada para explicar uma grande variedade de locais físicos e outras situações onde os dispositivos UTMs não são adequadas (por exemplo, centros com alto volume de dados). Diante desse fato, é evidente que um outro ingrediente chave para o sucesso da administração seja unificado, um recurso que possa ser capaz de gerenciar facilmente o UTM e dispositivos de gestão dedicados à gerenciar a ameaça a esse sistema. "*Universal Threat Management*" é o termo que está sendo introduzido para representar o triunvirato resultante de UTM, gerenciamento de ameaças específicas, e administração unificada (BOUCHARD, 2006).

A intenção é transmitir a necessidade de uma solução baseada em rede, para as ameaças de gestão, que seja aplicável e unificado não apenas a um subconjunto de locais físicos, mas sim através de todo o ambiente de computação da organização (BOUCHARD, 2006).

Vários fatores impactam atualmente nas organizações e nos seus ambientes de computação, adicionado o desafio de proteger os sistemas associados, aplicativos e dados. O principal deles foi uma mudança no objetivo principal dos *hackers* de ganhar notoriedade e construir sua reputação, para o objetivo de realmente ganhar dinheiro. O resultado dessa mudança foi um aumento substancial na atividade de *hackers* e maior foco em fugir comumente da implantação de contramedidas de sucesso, para o objetivo de se "obter" informações valiosas. Um resultado significativo da mudança na motivação *hacker* é que as ameaças estão sendo geradas mais rapidamente do que nunca. O período médio de tempo entre o anúncio de uma nova vulnerabilidade e o lançamento de uma ameaça correspondente leva poucos dias, horas, ou - no caso de ataques de dia zero - ainda menos. Isso é devido em grande parte, à grande disponibilidade de estruturas de desenvolvimento de *malware* que facilitam tanto a geração de novas ameaças, bem como a modificação rápida das ameaças já existentes em novas variantes (por exemplo, ajustes e recompilação do código fonte) (BOUCHARD, 2006).

Independentemente da causa, ao se ter menos tempo para responder aos ataques significa que a reativação de *patches* e outras contramedidas estão se tornando menos efetivas, em especial durante as fases iniciais de novos ataques. Dessa forma, as organizações devem buscar a complementação de suas ferramentas de defesa (BOUCHARD, 2006). A preocupação predominante do passado (por exemplo, os vírus de

nível de arquivo, *worms* e de negação de serviço ataques) são significativas, mas existe um conjunto de competidores mais novos, tais como *phishing*, *spyware*, *keylogging,* trojans e *rootkits* (BOUCHARD, 2006).

Os alvos dos ataques são ainda mais preocupantes, pois *hackers* constroem e exploram ataques de maneira personalizada, visando tirar proveito das características e deficiências únicas do ambiente computacional de uma organização específica. Existe ainda a questão de ameaças a migração. A implicação desse subconjunto específico de desafios requer uma solução de gerenciamento de ameaças que incorpore uma ampla gama de mecanismos de proteção, incluindo aqueles com maior visibilidade e controle na camada de aplicação (O'REILLY, 1999).

Alguns fatores adicionais que também estão contribuindo para os requisitos que definem uma solução de gestão ideal das ameaças incluem:

✓ O número de vulnerabilidades que devem ser abordadas está aumentando, e já há mais de 5000 casos documentados em 2006. Para se manterem competitivas, as organizações devem adotar constantemente tecnologias emergentes (por exemplo, *VoIP*, serviços *web* e virtualização), comprar ou construir novos aplicativos, e aplicar as novas versões dos produtos que já possuem. Não somente deve-se agregar mais infraestrutura, mas aplicativos e informações devem ser gerenciados e protegidos. O resultado é uma população crescente de vulnerabilidades, tanto em termos de *software* baseado em falhas como em erros de configuração.

✓ *Backhauling* se refere à prática de transportar tráfego da *internet* através das ligações *WAN* entre filiais e escritórios remotos. Em outras palavras, o acesso à *internet* não é direto para escritórios remotos, mas sim através de uma localidade central. Historicamente, esta tem sido a abordagem preferida porque elimina a necessidade de duplicar infraestrutura de segurança complicada e onerosa em cada local.

3 ESTUDO REALIZADO

3.1 NATUREZA DA PESQUISA

O presente estudo é de natureza aplicada, tendo-se em vista que possui uma finalidade imediata e prática para a busca da solução do foco da pesquisa (GIL, 1991), que gere conhecimentos úteis para a solução de problemas (BOAVENTURA, 2004).

A forma de abordagem do problema representa a perspectiva qualitativa. De acordo com Roesch (1999), o enfoque qualitativo é o mais indicado para a avaliação de programas ou planos, ou também para a proposta de programas ou planos. Bogdhan (1999) reforça ainda o uso da abordagem qualitativa, onde os dados coletados são detalhados e complexos, e as questões são formuladas com o objetivo de investigar os fenômenos em toda a sua complexidade.

3.2 POPULAÇÃO E AMOSTRAS

A amostra desta pesquisa foi composta por três empresas do setor têxtil. A escolha das três empresas pesquisadas teve motivação por se pretender realizar um comparativo entre as empresas de um mesmo segmento de negócio, no caso o setor têxtil. Por

questões de confidencialidade do negócio, os nomes das empresas pesquisadas não serão citados, afirmando-se apenas que se tratam de empresas posicionadas entre as maiores do setor têxtil no estado do Ceará.

3.3 INSTRUMENTOS PARA COLETA DOS DADOS

Foram planejados e desenvolvidos questionários para a pesquisa, os quais foram respondidos pelas empresas participantes. A amostra analisada representa três empresas do segmento têxtil. Conforme explicitado anteriormente o estudo consiste em uma pesquisa de ordem qualitativa, que busca evidenciar os aspectos concernentes ao tema analisado nessa amostra. As empresas acessaram o *survey* enviado por *email* pelos pesquisadores. Buscou-se observar as recomendações de Runerson & Host (2009) e de Wohlin & Runerson (2000) durante a fase de planejamento da pesquisa e projeto do questionário utilizado.

As variáveis trabalhadas nesta pesquisa envolveram os temas abaixo relacionados, os quais foram objetos da pesquisa feita por meio de questionário (*survey*):

1. Estimativa de recursos financeiros para segurança da informação;
2. Existência de *firewalls*;
3. Existência de políticas de segurança da informação aprovadas;
4. Existência de programas de conscientização sobre segurança;
5. Implantação de *software* ou *hardware* que possibilitem a detecção de violações da política de segurança, gravando informações para a auditoria;
6. Existência de *software* ou *hardware* para filtragem de SPAM;
7. Existência de filtro de URL na rede da empresa;
8. Existência de sistema de detecção de intrusão (IDS) na rede da empresa; e
9. Distribuição de *patches* de segurança automáticos, que englobam servidores *desktops* e *notebook* na rede da empresa.

Com o uso dessas variáveis foi possível a obtenção dos dados de investimento na área de TI por parte das empresas. Além disso, questionou-se sobre a existência de *firewall*, se existia política de segurança na empresa, programa de conscientização acerca da segurança, além de perguntas sobre existência de *softwares* e *anti spammers*, filtro URL e IDS/IPS e sobre a existência de *patches* de segurança rodando de maneira automática. A partir dessas questões, buscou-se evidenciar a importância da atenção a esses detalhes na política de segurança das empresas.

4 ANÁLISE DOS RESULTADOS

As duas primeiras perguntas do questionário de onze questões aplicado neste estudo se referiam ao levantamento de dados cadastrais e informações sobre os avaliadores, onde foi verificado em mais de 90% dos entrevistados a existência de um bom perfil técnico e gerencial, com conhecimento sobre gerenciamento de serviços de TI, segurança da informação e de segurança em redes de computadores.

Ao se analisar os resultados obtidos para a questão 03 (Gráfico 3), cujo teor se referia a estimativa de recursos financeiros destinados para a área de segurança da

informação na empresa, a maioria das empresas indicou não ter definido os investimentos na área, enquanto que 33% informou gastar mais do que 500 mil reais.

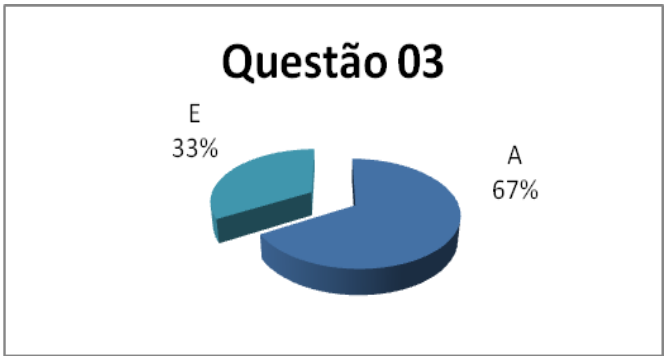

Gráfico 1 - Investimento em segurança da informação

Os resultados indicam que ainda não existe uma preocupação formal na maioria das empresas pesquisadas com o investimento em segurança da informação.

A *questão 04* da pesquisa indagava se a empresas teriam algum *firewall* instalado e qual seria a solução adotada. Nessa pergunta, todas as empresas avaliadas (100%) informaram que possuem um *firewall*, sendo citados como a solução adotada por elas o *Fortigate*, e *Iptables*. Os resultados indicaram que todas as empresas pesquisadas tem conhecimento sobre a necessidade de terem *firewalls* configurados em suas redes.

Já a *questão 05* perguntava se existia algum tipo de política de segurança da informação aprovada na empresa avaliada. Nesse quesito, foi verificado na pesquisa que a totalidade de empresas possuem política de segurança da informação aprovada.

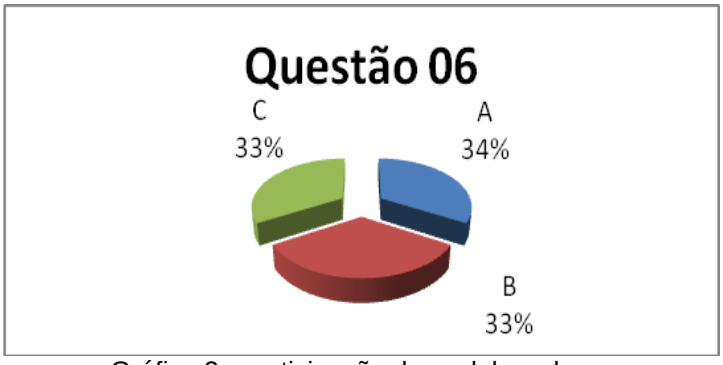

Gráfico 2 - participação dos colaboradores

Em relação a existência de programas de conscientização sobre a necessidade de segurança nas empresas, assunto abordado pela *questão 06* da pesquisa, verificou-se conforme mostrado no Gráfico 2, uma discrepância entre as ações das empresas, tendo em vista que uma das empresas possui programa de conscientização, outra está pensando em implantar e para uma das empresas essa é uma atividade ainda sem previsão. Esses resultados podem ser um indicativo de que mesmo com a adoção de políticas de segurança por todas as empresas, ainda não existe um consenso entre os gestores sobre a necessidade de se conscientizar todo o corpo de funcionários e colaboradores sobre a necessidade da segurança da informação.

A *questão 07* da pesquisa tinha como objetivo identificar se existia alguma implantação de *software* de segurança ou *hardware* que facilitasse a detecção de alguma

violação a política de segurança da informação e que gravasse os registros dos eventos para uma auditoria. Os resultados indicaram que 67% das empresas possuem alguma forma de detecção de violação da política de segurança, e apenas 33% não pensam em criar formas de detecção de violações em breve (vide Gráfico 3). Foi levantado ainda na pesquisa que as empresas que possuem utilizam as soluções *FortiAnalyzer* e *Symantec Endpoint*.

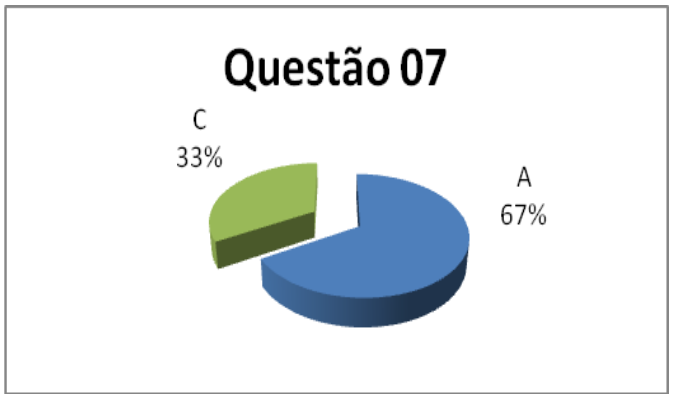

Gráfico 3 - Existência de Firewall

Já a *questão 08* da pesquisa visava identificar a existência de *software* ou *hardware* de filtragem de SPAM. Os resultados indicaram que 100% da amostra possuem esse tipo de solução. Ainda foi levantado na pesquisa que eram utilizadas as soluções *Ironport*, *Fortigate* e *SpamAssassine*.

Em relação à existência de filtros de URL na rede das empresas, assunto abordado pela *questão 09* da pesquisa, os resultados indicaram que 100% das empresas possuem esse filtro, tendo sido informadas pelas empresas como soluções utilizadas: *Webfilter, Fortigate* e *Squid*.

A *questão 10* da pesquisa visava descobrir a existência de sistemas de detecção de intrusão (IDS/IPS) na rede das empresas. Os resultados indicaram que todas as empresas (100%) possuem esse tipo de solução, tendo sido adotados: *Fortigate*, *Symantec Endpoint* e *SNORT*.

Em relação à questão 11 da pesquisa, que buscava avaliar se existia a distribuição de *patches* de segurança automáticos, englobando servidores, *desktops* e *notebooks* na rede da empresa, foi verificado que todas as empresas possuem e usam *Wsus*.

Ao se realizar uma análise comparativa dos resultados, percebe-se uma preocupação real das empresas em relação a segurança, apesar de parte dessas empresas não terem definido exatamente qual o quantitativo que deve ser investido na área de segurança.

Foi percebido ainda que existe uma carência de cuidados por parte das empresas no que tange ao planejamento para a conscientização dos colaboradores, no sentido de que estes, sensibilizados, façam parte do processo de segurança.

Verificou-se ainda que a importância da segurança da informação é conhecida, e que paulatinamente as empresas estão buscando soluções para prevenir a perda de dados, e garantir a continuidade dos negócios.

5 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este artigo apresentou uma revisão de literatura envolvendo segurança da informação e a evolução dos *firewalls* desde o seu surgimento até os dias atuais, procurando averiguar aspectos históricos e de relevância em termos de manutenção dos serviços de TI nas empresas. Visando a verificação de como as empresas do setor têxtil utilizavam os *firewalls* em suas políticas de segurança da informação, foi realizado um *survey* com três empresas do setor têxtil, confrontando-se os resultados com os dados coletados através da revisão de literatura. Através da análise das respostas de um questionário aplicado a essas empresas, foi possível verificar a existência de *firewalls* em todas elas, bem como entender aspectos relacionados às políticas de gestão.

Quais as principais conclusões ? Os resultados iniciais apresentados neste estudo contribuíram para reforçar os conceitos identificados na revisão de literatura, bem como para subsidiar os gestores de redes em relação a adoção de políticas de *firewall* e segurança nas empresas.

A partir das informações levantadas, pode-se concluir que as tecnologias de segurança protegem dados, conferem sigilo e são importantes para manter a reputação das empresas.

Ao se avaliar a segurança das redes e os perímetros de uso do *firewall*, ficou demonstrado que existem inúmeras soluções adaptáveis às necessidades e investimentos das empresas.

Identificou-se a partir dos dados e observações coletados, a existência de um senso de responsabilidade e preocupação com a política de segurança, apesar da maioria ainda estarem deficitárias em termos do programa de conscientização acerca da política de segurança com seus funcionários.

As perguntas sobre existência de *softwares* e *anti spammers*, filtros URL e IDS/IPS, bem como sobre os *patches* de segurança rodando de maneira automática criaram um panorama, trazendo esse panorama para análise, contribuindo assim para que outras pesquisas mais específicas possam ser realizadas.

A partir do levantamento de todas estas questões foi evidenciada a importância real e a atenção que se deve dar a estes pontos na política de segurança das empresas.

Em relação à análise sobre a segurança aplicada percebeu-se que ainda há necessidade de planejamento em relação ao aspecto de conscientização dos colaboradores, para que os mesmos façam parte do processo de segurança.

Quais as limitações do trabalho ? Os resultados do estudo de caso realizado não são facilmente generalizáveis. Pode-se afirmar com segurança que os resultados desta pesquisa são válidos para a orientação de empresas do ramo da indústria têxtil, o que não impede sua validade para outros ramos de negócio. Entretanto, por conta das limitações de prazo, tempo e escopo do trabalho, não foi possível a repetição de casos no trabalho. Mesmo assim, ressalta-se que os resultados contemplam o estudo de três empresas do setor têxtil, com áreas de TI atuantes, grande infraestrutura e quantidade de funcionários, tendo assim contribuído para o avanço da pesquisa.

Quais as possibilidades de trabalhos futuros ? Pretende-se como trabalhos futuros proceder a avaliação de um outro ramo de negócio, além de buscar novas

repetições para o estudo, talvez até nas mesmas empresas, para se ter um *feedback* histórico e comparativos que possam dar maior confiabilidade aos resultados.

REFERÊNCIAS

AL-SHAER E., HAMED H. H. H. Firewall Policy Advisor for Anomaly Discovery and Rule Editing, **Proceedings of IFIP/IEEE Eighth Integrated Network Management**, 2003a.

AL-SHAER E., HAMED H. H. H. Management and Translation of Filtering Security Policies, *Proceedings of ICC '03.* **IEEE International Conference on Communications**, 2003b.

AL-SHAER E., HAMED H. H. H. Modeling and Management of Firewall Policies, **IEEE Transactions on Network and Service Management**, vol. 1, issue 1, pp. 2 - 10, 2004.

AL-HAJ S., AL-SHAER E., Measuring Firewall Security, **Proceedings of 4th Symposium on Configuration Analytics and Automation (SAFECONFIG)**, 2011.

BARTH, M. **Detecção de Incoerências em Regras de Firewall**, Santa Cruz do Sul, julho de 2007.

BARBOSA, Ákio Nogueira. **Um sistema para análise ativa de comportamento de firewall**. São Paulo 2006.

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

BOUCHARD, Mark. **Founder Missing Link Security Services**, LLC. 2006 http://www.juniper.net/solutions/literature/white_papers/universal_threat_management.pdf acesso em out/2009.

CLINCH J., ITIL v3 and Information Security, **Clinch Consulting***, White Paper*, 2009.

DAMASCENO, R. C., **Abordagem sobre Tecnologias para Segurança de Perímetro - Firewall, VPN IPSEC, NAT / PAT, IDS**, *monografia de especialização*, UNICAMP, 2005.

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

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

ISO/IEC 27004, first edition, **Information technology-Security techniques - Information security management-Measurement**, 2009.

LETTER TO EDITOR, Formal security policy implementations in network firewalls, **Computers & Security**, p. 253-270, 2012.

LIU Alex X., GOUDA Mohamed G. Firewall Policy Queries. **IEEE Transactions On Parallel and Distributed Systems**, v. 20, n. 6, 2009.

LIU Alex X. Firewall Policy Change-Impact Analysis. **ACM Transactions on Internet Technology**, v. 11, n. 4, Article 15, 2012.

MADEIRA, F. **História do Firewall**. www.madeira.eng.br, http://imasters.uol.com.br/artigo/4583/seguranca/a_historia_do_firewall, UFPE, 2006.

NBR ISO/IEC 17799 – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. *Associação Brasileira de Normas Técnicas*. Rio de Janeiro, 2003.

NETTO A. S., SILVEIRA M. A. P., Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas, **Revista de Gestão da Tecnologia e Sistemas de Informação**, v. 4, n. 3, p. 375-397, 2007.

OGC (Office of Government Commerce), ITIL V3 PUBLICATIONS, “Service Strategy”, “Continual Service Improvement”, “Service Design” “Service Operation”, “Service Transition”, 2007.

O’REILLY. Practical Unix & Internet Security. **Unix and Cisco forum. 1999. White paper**. O'Reilly & Associates, Inc. http: //docstore.mik.ua/orelly/ networking/ puis/index/ idx_0.htm, acesso em out/2009.

RANGEL, Ricardo. A História da Internet. **Revista Internet World 2009**, http://www.solunet.com.br/z83.htm acesso out/2009.

ROQUE, A. S., NUNES, R. C., DA SILVA, A. D. Proposição de um modelo dinâmico de gestão de segurança da informação para ambientes industriais, **Revista Eletrônica de Sistemas de Informação**, ISSN:1677-3071, vol. 9, n. 2, 2010.

RUNERSON, P., HOST, M., Guidelines for conducting and reporting case study research in software engineering, **Springer: Empiric Software Eng.** ,v. 14 pp. 31-164, 2009.

VILLAS, Marcos; FONSECA, Marcus; MACEDO-SOARES, T. Diana L. v. A. de. Ensuring the strategic fit of information and communication technology: the case of Petrobras' oil refinery units. **Rev. Adm. Pública**, Rio de Janeiro, v. 40, n. 1, Feb. 2006 . Available from. http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122006000100007&lng=en&nrm=iso>. access on 07 June 2010. doi: 10.1590/S0034-76122006000100007.

WOHLIN C., RUNERSON P., HOST, M., OHLSSON, B. R., WESSLÉN, A., **Experimentation in Software Engineering - An introduction**, Kluwer Academic Publishers, 2000.

RADACK, S., Security Metrics: Measurements to support the continued development of Information Security Technology, Computer Security Division, **Information Technology Laboratory, National Institute of Standards and Technology, white paper**, 2010.