UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTAÇÃO

UTFPR

FERNANDO DERENIEVICZ ZOTTO

SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA SEGURANÇA DE REDES EM PEQUENAS E MÉDIAS EMPRESAS.

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2012

FERNANDO DERENIEVICZ ZOTTO

SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA SEGURANÇA DE REDES EM PEQUENAS E MÉDIAS EMPRESAS.

Trabalho de Monografia apresentado ao curso de Especialização em Teleinformática e Redes de Computadores da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do titulo de “Especialista em Teleinformática e Redes de Computadores”.

Orientador: Prof. Dr. Kleber Nabas

Coordenador: Walter Godoy Junior

Curitiba, 28 de Fevereiro de 2012.

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

FERNANDO DERENIEVICZ ZOTTO

SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA SEGURANÇA DE REDES EM PEQUENAS E MÉDIAS EMPRESAS.

Monografia aprovada como requisito parcial para obtenção do título de Especialista em Teleinformática e Redes de Computadores, da Universidade Tecnológica Federal do Paraná, pela banca formada pelos seguintes professores:

NOTA: 9,0 (NOVE INTEIROS)

Orientador:
Prof. Dr. Kleber Nabas

Coordenador:
Prof. Dr. Walter Godoy Júnior

CURITIBA, 28 de FEVEREIRO de 2012

Agradecimentos

À minha mãe Iolanda, pelo apoio e incentivo que me deu durante toda minha vida. Seus princípios sempre nortearam minhas ações e me fizeram alcançar muitos objetivos.

À Minha esposa Milene, pelo amor, paciência e incentivo durante todo este árduo percurso de estudos.

Ao meu orientador Kleber pela orientação, ajuda e colaboração.

LISTA DE FIGURAS

LISTA DE SIGLAS

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BFW	Brazil Firewall and Router
BGP	Border Gateway Protocol
CIO	Chief Information Officer
DOS	Denial Of Service
ERP	Enterprise Resource Planning
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P2P	Peer To Peer
PPOE	Point-to-Point Protocol Over Ethernet
PPP	Point To Point Protocol
PWC	PriceWaterHouseCoopers
RIP	Routing Information Protocol
SCSI	Small Computer System Interface
SMTP	Simple Message Tranfer Protocol
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
WAN	Wide Area Network

RESUMO

A segurança da informação bem como a segurança das redes de computadores têm se tornado um tema bastante comum ao longo dos anos que decorreram após o surgimento da internet. Porém mesmo com a evolução da tecnologia e a disponibilidade de um acervo infinito de informações sobre o tema, empresas de pequeno e médio porte ainda têm grandes dificuldades na implantação de políticas e ferramentas eficazes na segurança da informação. Isto ocorre por que grande parte das ferramentas disponíveis no mercado exigem um nível de conhecimento técnico alto, ou uma grande disponibilidade para gerenciar tais tecnologias.

Ao decorrer deste trabalho serão apresentadas informações e conceitos sobre redes de computadores e segurança da informação, bem como uma pesquisa atualizada sobre o nível de preocupação das organizações com o tema segurança da informação.

Este trabalho não tem o objetivo de trazer uma solução definitiva para implantar um nível de segurança alto dentro das organizações, pois conclui-se que não exista uma receita infalível. Cada organização, ramo de atividade ou rede de computadores possui características únicas que devem ser analisadas com particularmente antes de prescrever uma tecnologia eficaz na proteção de seus dados e informações.

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais é difícil imaginar um computador “só”, ou seja, que esteja totalmente isolado de qualquer rede de computadores, nem mesmo os dispositivos móveis como celulares, ipads, tablets estão isolados de qualquer rede que seja. E neste âmbito, temos a maior parte destas redes e destes computadores interligados em uma grande rede, formando uma conectividade global através da Internet. Um mundo de computadores 100% interligados de alguma maneira, cada um com seu endereço físico, conectado em algum lugar do mundo.

A internet possibilitou a criação da rede mundial de computadores, e desde então cresce a cada ano a preocupação com a segurança da informação. Porém, mesmo diante de tantos riscos em que as empresas estão expostas, grande parte das empresas no Brasil e no mundo ainda não possui uma estratégia eficaz para assegurar seus dados e informações corporativas como veremos no decorrer deste.

Desta forma este trabalho abordará alguns tópicos relacionados à segurança da informação, mais especificamente segurança da informação dentro das redes corporativas de pequeno e médio porte. Também trará uma proposta de implantação de uma ferramenta de baixo custo e de fácil configuração e administração para prevenção de falhas de segurança na rede, e um maior controle das informações que trafegam na rede.

1.2 OBJETIVOS

Este trabalho tem como objetivo principal, explicar o processo de segurança da informação no ambiente de rede em uma organização, bem como apresentar uma proposta para uso de uma ferramenta de segurança de rede de baixo custo e de fácil implantação.

1.2.1 Objetivo Geral

Apresentar o conceito de segurança em redes, e auxiliar na implantação e gerenciamento de uma solução prática e confiável para segurança e roteamento da rede.

1.2.2 Objetivos Específicos

Apresentar o conceito de Rede, e o conceito de Segurança da Informação nas redes de computadores de pequeno e médio porte.

Apresentar os métodos mais comuns de roubo de informação e invasão das redes de computadores, e os principais pontos de vulnerabilidades na rede.

Auxiliar na implantação e configuração de uma ferramenta de auxilio para segurança de redes de computadores.

1.3 JUSTIFICATIVA

Atualmente o assunto da segurança em redes esta em pauta em grande parte dos ambientes corporativos, a cada ano o nível de preocupação cresce conforme pesquisas realizadas no setor. Porém por mais que existam inúmeras tecnologias e ferramentas disponíveis no mercado para a segurança em rede, pequenas e médias empresas ainda encontram dificuldades na implantação de uma política de segurança de rede eficaz e de fácil gerenciamento. Parte por falta de conhecimento dos profissionais de TI que atuam nestas empresas, parte por falta de planejamento da área de TI, e ainda uma parte pela falta de interesse em investimentos neste departamento.

Existem hoje no mercado todos os tipos de soluções em segurança de redes, robustas e muito complexas, enxutas mas pouco confiáveis, simples e seguras porém com custo muito elevado. Desta forma torna-se difícil decidir qual seria a solução ideal. E neste ponto muitas empresas nem ao menos começam com o básico, deixando a segurança de rede sempre em segundo plano.

2 SOBRE REDES DE COMPUTADORES

Uma rede de computadores é uma infraestrutura que permite interligar dois ou mais computadores (chamados hosts) para que possa haver troca de informações (mensagens) entre estes.

Isso é possível devido a um conjunto de regras pré-estabelecidas para a comunicação, chamadas de protocolos. Os protocolos devem obrigatoriamente ser respeitados e seguidos por todos os hosts da rede de forma uniforme.

A necessidade de um protocolo dá-se ao fato de que os hosts precisam comunicar-se de uma forma padrão ou, “falar a mesma língua”. Para isso necessitam-se não apenas de um protocolo, mas sim de uma pilha de protocolos separados em camadas, cada qual com suas características e funcionalidades, a seguir vamos abordar algumas características conceituais sobre as camadas de rede e suas funcionalidades.

Os tópicos que seguirão, servirão de apoio para o entendimento dos conceitos de rede, dos protocolos de rede, camadas, protocolos de roteamento, topologias de rede entre outros. Pois estas características estarão presentes na ferramenta proposta nesta monografia.

2.1 REDES LOCAIS (LANs)

Uma rede LAN (Local Area Network – Rede de Trabalho Local), é uma rede de computadores concentrada em uma área geográfica, como por exemplo um prédio, uma empresa, um escritório ou um campus universitário. Atualmente a grande maioria das redes empresariais e domésticas são qualificadas como LANs, o acesso a internet também é realizado através destas redes LANs. Por meio das redes LAN pode-se compartilhar o uso dos dispositivos da rede, ou ate mesmo o uso de dispositivos dos Hosts que compõe a rede, como unidades de CD/DVD, impressoras, discos rígidos entre outros.

2.2 REDES MANs E WANs

Além das redes LANs, existem outras formas de redes que pode-se citar, apenas para efeito de comparação, pois não falaremos de características mais profundas de redes que não as LANs.

Redes MANs: (*Metropolitan Area Networks*), são redes de médio porte, redes MANs interligam redes LANs, normalmente são redes de abrangência estadual.

Redes WANs: (*Wide Area Network*), sao redes utilizadas para interligar outras redes geograficamente distantes, as redes WAN utilizam a infraestrutura de transmissão de empresas de telecomunicações, como COPEL, EMBRATEL entre outras.

2.3 TOPOLOGIA BÁSICA DE REDE

É a forma como os pontos de rede se interligam, a infra-estrutura utilizada para a comunicação entre dois ou mais computadores da rede.

As topologias de redes rede em geral tem dos tipos de comunicação, que são redes do tipo Ponto A Ponto e redes do tipo Multiponto.

2.3.1 Ponto A Ponto

Uma forma de comunicação exclusiva entre dois pontos (*hosts*), ou seja, se um Host A deseja comunicar com um Host B, deve haver uma linha exclusiva entre um e outro, não possibilitando a comunicação com um terceiro Host através desta mesma comunicação. Em redes LAN`s atuais, utilizando-se de cabos de rede do tipo

Par Trançado, dá-se o nome ao cabo que interliga dois Hosts Ponto A Ponto de *Crossover*.

2.3.2 Multiponto

Em uma rede Multiponto, uma única linha de comunicação servirá na comunicação de vários Hosts ao mesmo tempo. Obviamente o controle para isto é mais complexo, mas um Host A poderá se comunicar com outros Hosts (B, C, D) sem que haja a necessidade de uma linha exclusiva entre cada um deles.

2.4 PROTOCOLO TCP/IP E PILHAS DE PROTOCOLOS

TCP/IP (*Transition Control Protocol / Internet Protocol*) é o conjunto de protocolos de comunicação ou pilha de protocolos. Desenvolvido essencialmente para resolver problemas de compatibilidade de diferentes tecnologias e plataformas no âmbito das redes intranets e também na internet.

Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa. Como exemplo, pode-se empregar estruturas de rede como Ethernet, Token-Ring, FDDI, PPP, ATM, X.25, Frame-Relay, barramentos SCSI, enlaces de satélite, ligações telefônicas discadas e várias outras como meio de comunicação do protocolo TCP/IP.

A arquitetura TCP/IP, assim como OSI realiza a divisão de funções do sistema de comunicação em estruturas de camadas. Em TCP/IP as camadas são:

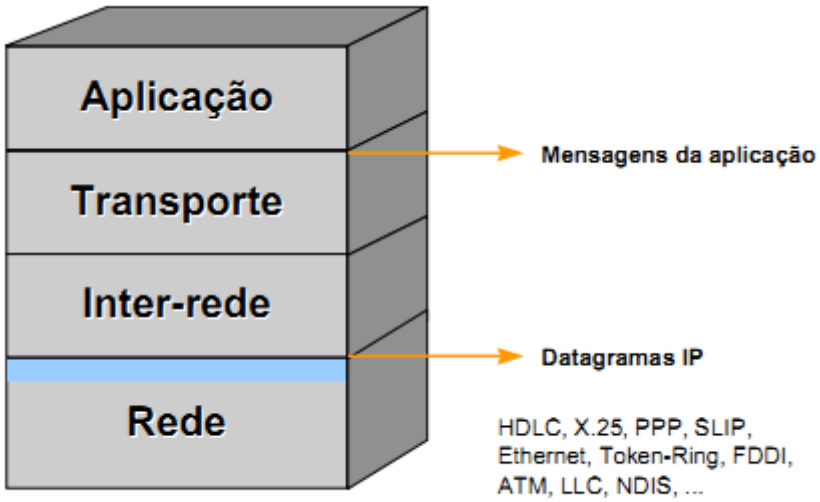


Figura 1 – Camada de redes do modelo TCP/IP.

Uma arquitetura de camadas foi desenvolvida para que as funções fossem divididas dentro de uma estrutura de comunicação em rede. Segundo (KUROSE, 2006), “O sistema de camadas de protocolos tem vantagens conceituais e estruturais.”, segundo ele “...a divisão em camadas proporciona um modo estruturado de discutir componentes de sistema.”.

Camada de Rede – A camada de rede fica responsável pelo envio de datagramas construídos na camada de Inter-redes, esta camada possui um mapeamento de endereço de identificação no nível físico das rede, no caso de redes Ethernet cada estação possui um endereço único chamado de endereço MAC (Media Access Control). Pode-se citar que na camada de redes e na camada de inter-redes do modelo TCP/IP, um protocolo muito comum utilizado é o protocolo ARP (Address Resolution Protocol), que é um protocolo de mapeamento de endereços tanto físicos quanto lógicos.

Camada Inter-Rede – Esta camada é responsável pela comunicação entre maquinas vizinhas através do protocolo IP. O protocolo IP realiza a função de roteamento que consiste no transporte da mensagem entre redes e nas decisões de qual rota cada mensagem devera seguir até seu destino.

Camada de Transporte – A camada de Transporte possui os protocolos UDP (User Datagram Protocol) e TCP (Transmission Control Protocol). Esta camada reúne os protocolos que realizam as funções de transporte de dados fim-a-fim,

considerando apenas a origem e destino da comunicação, sem se preocupar com os elementos intermediários.

Camada de Aplicação – A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário. Esta camada possui a comunicação direta entre a aplicação propriamente dita, como exemplo o sistema operacional, e as camadas mais baixas.

2.5 MODELO OSI

A arquitetura TCP/IP difere e muito do modelo OSI, devido fato de que a arquitetura TCP/IP agrupa como subcamadas, as camadas utilizadas no modelo OSI.

As principais diferenças são:

- Modelo OSI trata todas as camadas, enquanto TCP/IP apenas a partir do nível de Rede do modelo OSI;
- TCP/IP é largamente compatível com diversos modelos de arquiteturas, enquanto OSI não;
- OSI oferece serviços de orientados a conexão no nível de rede, o que demanda um trabalho e uma inteligência muito maior, já o TCP/IP tem uma função muito simples de roteamento.
- TCP/IP trata os níveis superiores de forma monolítica, desta forma OSI é mais eficiente pois oferece reaproveitamento de funções comuns a diversos tipos de aplicação, o TCP/IP necessita montar uma estrutura completa para cada tipo de aplicação.

A Figura 2 mostra um comparativo entre as arquiteturas OSI e TCP/IP, note que muitas camadas do modelo OSI são tratadas de forma única no modelo TCP/IP, existe um agrupamento das camadas.

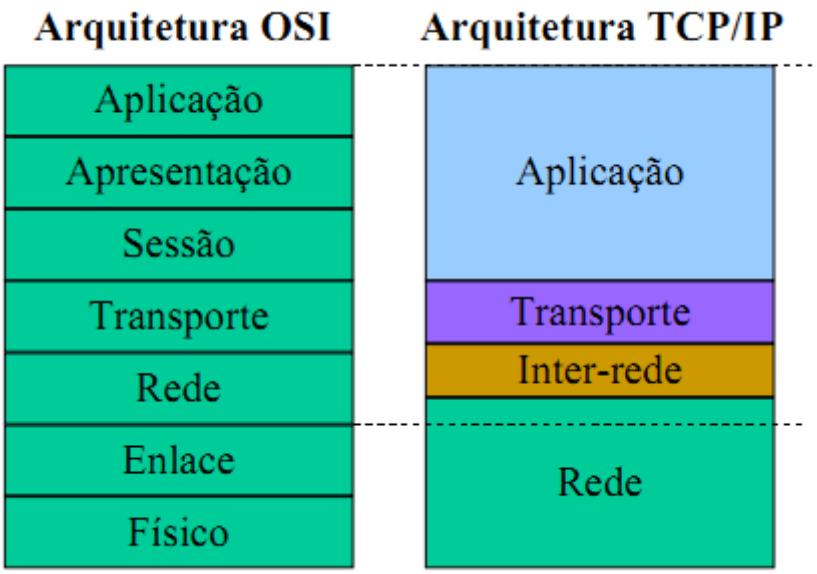


Figura 2 – Comparativo das camadas de rede dos modelos OSI e TCP/IP.

2.6 ROTEAMENTO DE REDE E PROTOCOLOS DE ROTEAMENTO

Uma das funções principais da camada de rede é prover o roteamento dos pacotes que transitam em rede. Segundo KUROSE (2006), “A camada de rede deve determinar a rota ou o caminho tomado pelos pacotes ao fluírem de um remetente a um destinatário.”.

O papel de um roteador é definir qual será a rota que aquele pacote deverá seguir, utilizando o conceito de *repasse*, ou seja, o pacote de dados chegará através de uma das portas do roteador, e o mesmo se encarregará em repassar este pacote para outra porta, usando uma tabela de rotas que pode ser estática (definida manualmente), ou dinâmica (utilizando um protocolo que crie esta tabela dinamicamente).

Para que o rota seja definida, os roteadores realizam os cálculos das métricas através de um algoritmo de roteamento, que irá definir o melhor caminho para enviar aquele pacote. A Métrica é o padrão de medida que é usado pelo algoritmo de roteamento, que utilizara um ou vários parâmetros para definir a rota, entre os parâmetros mais comuns encontran-se:

- Tamanho do caminho;
- Confiabilidade;
- Atraso;

- Largura de Banda;
- Carga;
- Custo da comunicação.

Roteamento Estático: No roteamento estático as tabelas de rotas são construídas manualmente, atribuído a redes pequenas com um numero limitado de roteadores. As rotas podem ou não serem divulgadas para outros dispositivos, sendo que a não divulgação é uma das características positivas deste tipo de roteamento devido ao aumento da segurança. Outro ponto positivo é que as tabelas estáticas diminuem o overhead introduzido pela troca de mensagens de roteamento na rede.

Roteamento Dinâmico: O roteamento dinâmico ocorre quando há mais de uma rota possível para o mesmo ponto, desta forma uma tabela de rotas é construída automaticamente a partir da troca de informações dos protocolos de roteamento. Os protocolos de roteamento mais comuns são RIP e seu sucessor OSPF, o IGRP, BGP entre outros.

3 SEGURANÇA DA INFORMAÇÃO

O conceito geral sobre segurança da informação, esta diretamente relacionado à segurança de um conjunto de dados, a fim de preservar seu valor de informação.

> O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos.
> Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém.
> A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança. (SOARES; LEMOS e COLCHER,1995, p.448):

A segurança em rede de computadores foi se tornando uma preocupação gradativa, à medida que as organizações necessitavam “esconder” seus dados importantes, medidas de segurança começaram a ser pensadas para a proteção destes dados. Nesta esfera pode-se entender que a partir do momento que se necessita proteger algo, tem-se este algo como um objeto ou informação de valor, e aí crescem cada vez mais as motivações para roubar estes dados das empresas.

Com a criação da Internet, e seu crescente uso, inimagináveis formas de roubar dados foram sendo utilizadas por “piratas da internet” ou atualmente conhecidos como hackers, crackers entre outros. Estes são “bandidos” virtuais, que se utilizam de recursos computacionais para infringir a segurança das redes. Diante disto empresas começam a investir cada vez mais em segurança da informação a fim de manter seus dados protegidos, bem como manter sua rede em perfeito funcionamento, visto que hoje a grande maioria das empresas dependem das redes de computadores para sua sobrevivência, enviar emails, acessar sites, pesquisar, trocar informações, acessar o sistema ERP, concretizar negócios e até vender seus produtos on-line, tudo isto não seria possível sem o uso das redes de computadores, então julga-se extremamente necessário sua segurança.

3.1 POLITICA DE SEGURANÇA

A política de segurança refere-se a um conjunto de regras, normas e diretrizes que estabelecem padrões desejáveis e aceitáveis de uso dos sistemas, bem como define as limitações aferidas aos usuários da rede.

Com o crescente uso da internet, das operações realizadas através dela e dos riscos que ela oferece, deve-se pensar em Política de Segurança, não apenas das redes de computadores, mas sim de todo um conjunto de diretrizes que administrem os pontos cruciais para a segurança, desde os direitos e deveres do uso de computadores pelos colaboradores, até uma política de acesso restrito á área de servidores e políticas funcionais para o conjunto de dados que necessitam ser gravados em Backups. Tudo deve ser pensado para a proteção de qualquer dado ou bem, seja intelectual ou físico.

3.2 SEGURANÇA DE REDE

Partindo de um princípio lógico sobre segurança em rede de computadores, pode-se afirmar que a segurança esta na preservação dos dados mantidos nos elementos que integram esta rede, como por exemplo um banco de dados do sistema que a empresa possui, ou a troca de informações de entrada e saída da rede corporativa de forma segura e confidencial.

Segundo KUROSE (2006), para que possamos estabelecer uma conexão de forma segura, é desejável que sejam atendidos as seguintes propriedades:

“Confidencialidade: Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida.” Sendo para isto necessário o uso de alguma forma de criptografia de dados, fazendo com que a mensagem não possa ser decifrada por algum intruso.

“Autenticação: O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é

que alega ser.” Um dos pontos mais difíceis de tratar quando o assunto é comunicação segura, hoje em dia existem inúmeras formas de se passar por outra pessoa na internet, como por exemplo, a camuflagem de IP, que com um programa é possível disfarçar um endereço de IP por outro.

“Integridade e não-repudiação de mensagem: Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.” Ou seja, a mensagem tem que chegar ao destinatário exatamente como saiu do remetente, utilizando técnicas de criptografia e comparação de dados.

Disponibilidade e controle de acesso: Um dos maiores fatores que levaram ao uso de políticas de segurança de rede, que surgiu principalmente após o advindo da internet, foi devido aos ataques *DoS (denial of service)*. Que indisponibilizam os serviços da rede para os usuários legítimos, de forma que nenhum usuário consegue acessar um Server ou um Host da rede.

Confidencialidade, autenticação, integridade e não-repudiação de mensagem vêm sendo considerados componentes fundamentais da comunicação segura há bastante tempo (McCumber, 1991). Disponibilidade e controle de acesso são extensões mais recentes da noção de comunicações seguras (Bishop, 2003).

3.3 FALHAS QUE COMPROMETEM A SEGURANÇA DE REDE

Diante de todo o exposto sobre as características das redes de computação, dos conceitos e políticas da segurança em redes de computadores e das motivações para ataques a redes corporativas por crakers e outros piratas da internet, vamos entender quais são as principais formas de ataques, e discutir as principais vulnerabilidades das redes corporativas, vamos utilizar sempre um case de redes de pequenas e medias empresas, visto que esse tipo de rede é o objeto de estudo desta monografia.

3.3.1 Falta de Políticas de Segurança da Informação

Esta é sem dúvidas uma das principais falhas na segurança da rede em uma organização. Como em qualquer sociedade que não possuem Diretrizes e Leis que orientem como deve ser o comportamento dos cidadãos, esta sociedade não terá limites e estará completamente vulnerável a qualquer situação de risco, assim também é dentro de uma rede que não possui suas diretrizes e normas de uso, sem estas é impossível controlar o que esta sendo feito dentro da rede, assim como também não será possível tomar medidas de notificação aos usuários, uma vez que estas não foram definidas em uma política de uso da rede.

Infelizmente uma das principais causas de invasões, e problemas de proliferação de vírus e key-logers em redes de computadores corporativas é o mau uso da internet, email e mensageiros eletrônicos por parte dos usuários desta rede. Atualmente existem milhares de correspondências e links falsos que disseminam programas maliciosos, principalmente sendo espalhadas nos últimos anos através das redes sociais.

3.3.2 Falta de Controle de Acesso á Rede

Poucas são as organizações de pequeno e médio porte que possuem um controle adequado de acesso á rede por meio de autenticação de segurança, bem como dificilmente possuem uma gerencia destes acessos, ou seja, não se sabe ao certo quem esta usando a rede, se este usuário é um colaborador ou um intruso, se algum usuário esta realizando acessos a locais indevidos, o que o usuário esta acessando na internet.

3.3.3 Uso de Senhas e configurações Universais nos equipamentos

Certa vez fui realizar um atendimento a uma empresa que estava sendo invadida através da rede Wireless que possuíam, pois diariamente alguém alterava a senha de acesso à rede sem fio. Nesta ocasião fizemos alguns testes e constatamos que dificilmente seria alguém de fora da rede, que provavelmente seria alguém de dentro da própria empresa, foi alterada a senha de acesso à administração do Access Point que estava como padrão “ADMIN”, e o problema foi resolvido. É extremamente comum encontrar empresas que compram equipamentos como Modems, Access Point, Roteadores entre outros, e não alteram suas senhas padrões, ou seja, quando o intruso conseguir “enxergar” a rede, seja ela sem fio ou cabeada, os equipamentos estarão ao seu deleite, pois todos estão com suas configurações de fabrica.

3.3.4 Emails e Links Falsos

Esta é uma das formas muito comuns de invasão a redes corporativas, estes links e emails falsos encaminham os usuários a paginas que possuem o intuito de instalar programas maliciosos na rede, como keylogers, sniffers entre outros. Estes programas por sua vez tem o intuito ou de roubar dados, ou de danificar os arquivos dos PC`s ou Servidores.

3.3.5 Falta de Firewalls e Proxies

Sem o controle do que entra e sai da rede, e sem o controle do que pode ser acessado pelos usuários, fica ainda mais fácil invadir uma rede, com técnicas de varredura de portas, Vírus, IP Spoofing, Roteamento dirigido, Trojan Horse entre outros, falaremos sobre tais técnicas no item x.x.x.

3.3.6 Falta de Gerenciamento da Rede

Por fim apontamos um dos motivos que levam empresas a sofrerem ataques de todos os tipos é o não gerenciamento de uma Rede de computadores, bem como o não gerenciamento da segurança da informação como um todo. Definitivamente uma rede sem gerenciamento esta muito mais suscetível á falhas de segurança. Vêm crescendo o nível de preocupação das empresas com a Gerência da Segurança da Informação, mas ainda assim o numero de empresas de pequeno e médio porte que crescem sem nenhum profissional gerenciando a segurança da informação ainda é preocupante. Esta é uma área da tecnologia que já é indispensável, porém quando trata-se de investir em tecnologias e em profissionais para gerenciá-las, o pensamento em pelo menos um terço das empresas é de que não há ainda necessidade de tais investimentos, porém uma concepção que deve ser levada em conta é a de que quanto antes forem os investimentos em segurança da informação, menor será os gastos para reparar os estragos que um invasor pode fazer no futuro.

3.4 COMO EVITAR FALHAS NA SEGURANÇA DE REDE

Assim como falamos dos meios de invasão utilizados por piratas da internet, abordaremos neste tópico os meios de proteção para evitar desastres por roubo ou estragos causados por vírus e pragas em rede.

3.4.1 Políticas de Segurança

Já falamos muito sobre políticas de segurança e voltamos no mesmo tópico para frisar sua importância. A necessidade de uma política bem escrita e usual é definitiva quando o assunto é segurança, cada empresa possui características e necessidades distintas, desta forma cada política deve conter diretrizes conforme as

necessidades da empresa. Segundo alguns autores, mesmo com as diferentes necessidades das organizações, existem algumas premissas que devem ser levadas em conta na elaboração de uma política de segurança, mais precisamente três principais pontos devem ser levados em consideração.

Segundo Melo (2003), as políticas de segurança de sistemas se diferem em três ramos principais: segurança física, segurança gerencial e segurança lógica.

- **Segurança física** – trata-se da segurança física do sistema, o meio físico em que o sistema se sustenta. Que define as medidas de segurança contra desastres como: alagamentos, terremotos, incêndios, ou qualquer evento natural que venha prejudicar ou interromper o funcionamento dos sistemas. Bem como as restrições e delimitações de acesso aos equipamentos e etc.

- **Segurança gerencial** – trata-se do ponto de vista estratégico organizacional, definindo os processos, normatizando e gerenciando as tomadas de decisão.

- **Segurança lógica** – trata-se das definições de segurança no nível da aplicação, como permissões de usuários, direitos e monitoramentos das atividades.

3.4.2 Uso de Firewall e Proxy de Rede

O Firewall é uma ferramenta extremamente importante na proteção das redes corporativas, visto que ele é o responsável por filtrar os pacotes que entram e saem da rede, bem como ajuda no bloqueio das portas de uso comum nos ataques de intrusos.

Os proxies também são ferramentas de grande ajuda na proteção da rede, seu intuito é limitar o acesso dos usuários da rede para o mundo externo, ou seja, proxies bloqueiam o acesso dos usuários da rede interna para a internet, sites

impróprios, downloads, execução de complementos, programas de downloads como: P2P, torrents entre outros. O uso de Proxies é muito recomendado visto que grande parte das vulnerabilidades da rede ocorre devido ao mau uso da internet por parte dos usuários.

3.4.3 Alterar senhas e configurações dos equipamentos regularmente

Esta também é uma característica imprescindível quando se trata de segurança em rede, todos os equipamentos utilizados como: MODEMS, ROTEADORES, SWITCHS, FIREWALLS, PROXIES, SERVIDORES, ACCESS POINTS, entre outros, devem ter suas senhas atualizadas periodicamente, seguindo um padrão aceitável dê segurança, com uma quantidade mínima de caracteres aceitável. Por exemplo, a senha de um MODEM, normalmente pelo padrão vem configurado com Usuário: Admin e a sua Senha: Admin, o correto é que se possível altere-se os dois campos, tanto usuário quando senha, se não for possível alterar o usuário, cria-se um novo usuário máster e inativa-se o usuário Admin. A senha deve ter um mínimo de 8 caracteres em qualquer situação, e sempre utilizar senhas Alfanuméricas com caracteres especiais, intercalando letras MINUSCULAS e MAIUSCULAS.

3.4.4 Utilizar equipamentos de proteção à rede física

Uma rede se sustenta através do meio físico e todos os componentes que o compõe, Servidores, Computadores, Switchs, Roteadores entre outros. A proteção física destes equipamentos previne desastres e perca de dados e informações. Ou seja, uma rede não sofre apenas problemas de ataques de intrusos, a segurança da rede envolve a perca, roubo ou destruição de dados e informações importantes, e neste contexto a falha de proteção com os equipamentos físicos da rede pode trazer prejuízos aos dados da empresa. Pode-se exemplificar tal situação com a hipótese de um raio queimar os servidores da empresa por falta de protetores Anti-Surto, ou

até mesmo uma queda de luz danificar o software ERP por falta de NO-BREAKS. Todo e qualquer problema que atrapalhe ou impeça o perfeito funcionamento da rede é considerada como falha de segurança da informação, mais precisamente no contexto de segurança de redes de computação. Desta forma o uso de NO-BREAKS, Anti-Surtos Elétricos, Estabilizadores, e outras formas de proteção são imprescindíveis para a segurança da rede.

3.4.5 Alocar os equipamentos físicos em local adequado

Por varias vezes me deparei com empresas que alocam os equipamentos que compõe a rede, em locais inadequados, sem ventilação, sujos, muitos vezes locais onde qualquer colaborador tem acesso, totalmente vulneráveis e sem nenhuma condição adequada. É muito importante a conscientização de que os equipamentos da rede precisam estar em um local adequado, arejado, alocados em um Rack, de preferência em local onde se possa controlar a temperatura com o uso de Ar-Condicionado. Dentre todas estas características, que pelo menos algumas delas possam ser seguidas, muitas vezes a empresa não possui um espaço adequado, como uma sala só para os equipamentos, mas nestes casos que haja ao menos uma estrutura de divisórias impedindo o acesso livre aos equipamentos.

3.4.6 Uso de Redundâncias

O uso de redundâncias também é uma prevenção à indisponibilidade de sistemas, sejam eles compostos por softwares como hardwares. A rede sempre deve ter uma segunda ou terceira alternativa, assim como um roteador precisa de rotas alternativas, uma rede precisa opções para um funcionamento alternativo. Todo o trafego de uma rede pode parar simplesmente porque um roteador parou de funcionar, deve haver um equipamento pré configurado sobressalente, ou uma rota alternativa para não comprometer o funcionamento da rede. Assim também como links de redundância de internet, uma rede que necessita do uso da internet para o

funcionamento de suas aplicações não pode depender de um único link de internet, ou de uma única operadora. Deve haver sempre ao menos dois links distintos de operadoras distintas, e ainda se possível que haja balanceamento de carga destes links, ou seja, se um link cair por algum motivo, outro link é acionado automaticamente sem que haja queda da internet, o balanceamento de carga também é útil na divisão do fluxo da rede em links diferentes, não permitindo que ocorra excesso de carga em um único link, ou uma única rota na rede.

3.4.7 Monitoramento, Controle e Gerencia de rede

Existem ferramentas no mercado que possibilitam o monitoramento e controle da rede através de protocolos específicos para estas finalidades, como por exemplo, o protocolo SNMP (Simple Network Management Protocol). O SNMP tem por objetivo principal coletar informações da rede e fornecê-las para possibilitar seu gerenciamento, controle, resolver eventuais problemas e fornecer informações para planejar expansões.

Uma rede de computadores precisa ser monitorada, controlada e gerenciada por alguém, o uso de equipamentos e ferramentas de rede não tem valor algum se estes não forem gerenciados por um departamento ou um profissional da empresa. O próprio protocolo SNMP que possui uma utilidade enorme torna-se obsoleto se não for gerenciado por alguém, pois nenhuma aplicação, software ou hardware poderá tomar decisões gerenciais pela empresa, estas podem apenas fornecer as informações necessárias para as tomadas de decisão.

4 PESQUISA GLOBAL DE SEGURANÇA DA INFORMAÇÃO

Antes de partir para o âmbito de uma proposta de implantação de uma ferramenta de Segurança e Controle de Rede, objeto principal desta monografia, vamos entender o cenário atual do conceito de Segurança da Informação como objeto de preocupação das organizações pelo mundo. Como as empresas estão programando seus investimentos em tecnologias seguras, ferramentas de segurança, desenvolvimento de competências, desenvolvimento de departamentos de Tecnologia e Segurança da Informação. Estas e outras indagações são de interesse da Pesquisa Global de Segurança da Informação.

Foram retirados dados atualizados da Pesquisa Global de Segurança da Informação 2012 (Global State of Information Security Survey), que é uma iniciativa da PwC, da CIO Magazine e da CSO Magazine. A pesquisa foi conduzida on-line entre 10 de fevereiro e 18 de abril de 2011. Foram convidados leitores das revistas CIO Magazine e CSO Magazine, bem como clientes da PwC ao redor do mundo à responder a pesquisa. Dentre os convidados 9.600 CEOs, CFOs, CISOs, CIOs, CSOs, vice-presidentes e diretores de TI e de segurança da informação. O Brasil teve uma participação relativa de 10% na pesquisa, totalizando 961 executivos de empresas do Brasil.

A pesquisa possui um total de 25 questões fundamentais no que se refere á Segurança da Informação, porém foram selecionadas apenas aquelas que julgadas de grande relevância no contexto deste trabalho. A pesquisa completa pode ser encontrada no site da PwC através do endereço: http://www.pwc.com.br/pt/estudos-pesquisas/giss-2012.jhtml.

4.1 IDENTIFICANDO OS PERFIS

Primeiramente para que o cerne da questão seja entendido, necessitamos primeiro entender e definir os perfil existentes no que se refere a estratégias e

gerencia da Segurança da Informação, a pesquisa caracterizou cada perfil como mostra a Figura 3.

Figura 3 – Perfil dos Profissionais e departamentos de TI nas empresas participantes.
Fonte: 2012 Global State of Information Security Survey.

4.2 INFORMAÇÕES VALIOSAS

Como se trata de uma pesquisa global, onde a maior parte das empresas respondentes está situada na America do Norte (29%) e Europa (26%), pode-se deduzir que os números para o Brasil provavelmente distinguem destes apresentados, visto que o Brasil tem um percentual menor em investimentos em segurança da informação do que países da Europa e America do Norte.

Muitos anos após a Globalização, o que os Líderes consideram no mundo atual, uma informação valiosa para as empresas.

Figura 3: Percentual dos respondentes que consideram extremamente importantes os tipos de informação a seguir

	Líderes	Estrategistas	Táticos	Bombeiros
Informações de clientes	73%	57%	63%	45%
Dados financeiros	65%	43%	48%	40%
Segredos de propriedade intelectual e comerciais	63%	42%	42%	34%
Informações corporativas	60%	41%	42%	31%
Informações de funcionários	51%	37%	40%	28%

Fonte: 2012 Global State of Information Security Survey®
Os valores totais não somam 100%. Os respondentes puderam indicar diversos fatores.

Figura 4 – Informações consideradas valiosas pelas empresas participantes da pesquisa.
Fonte: 2012 Global State of Information Security Survey.

4.3 PREOCUPAÇÕES COM A WEB

Conforme a Figura 4 pode-se perceber um aumento significativo e gradual na preocupação e investimentos das empresas no que se refere à segurança na Web, e também em ferramentas que previnam invasores em nível de rede.

Figura 7: Percentual dos respondentes que relataram salvaguardas de segurança da informação relacionadas às seguintes áreas de detecção, prevenção e à web

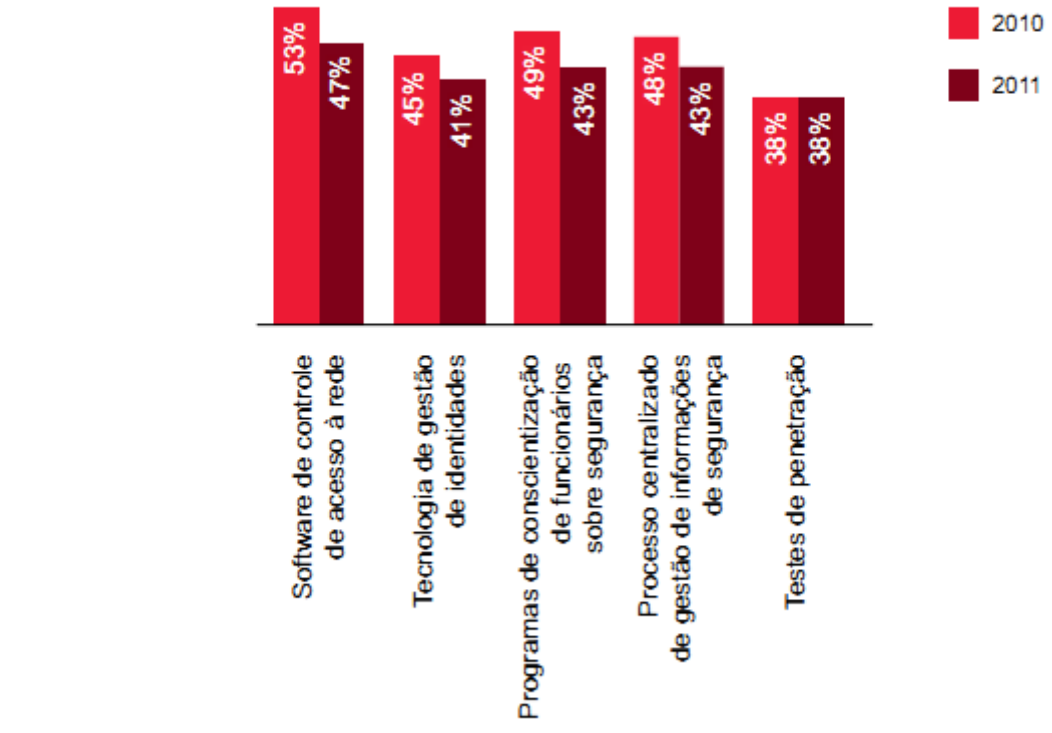
Fonte: 2012 Global State of Information Security Survey®
Nem todos os fatores são ilustrados. Os valores totais não somam 100%.

Figura 5 – Salvaguardas de segurança relacionados à Web.
Fonte: 2012 Global State of Information Security Survey.

4.4 AMEAÇA PERSISTENTE AVANÇADA

Atualmente uma ameaça que vem assolando grandes corporações é conhecida como Ameaça Persistente Avançada (APT – Advanced Persistent Thread). São ataques massivos de grupos de interesse ou países a fim de espionar ou sabotar informações relevantes. Por mais que estes ataques tem 85% de sua atenção a grandes corporações, pequenas e médias empresas de alguns setores particulares despertam a atenção para seus dados sigilosos, e podem ser alvos de ataques como este, mas será que as empresas estão preparadas para isto? Segundo a pesquisa da PwC as empresas tem adotado algumas medidas de segurança como veremos a seguir:

Figura 9: Percentual dos respondentes segundo os quais suas empresas possuem internamente as competências relacionadas à prevenção, à detecção e ao combate ao APT



Fonte: 2012 Global State of Information Security Survey®
Nem todos os fatores são ilustrados. Os valores totais não somam 100%.

Figura 6 – Tecnologias utilizadas contra a APT.
Fonte: 2012 Global State of Information Security Survey.

4.5 PREOCUPAÇÃO E MONITORAMENTO DOS USUÁRIOS

Assim como algumas novas praticas e tecnologias surgem e são adotadas pelas organizações, outras porém sofrem degradação com o passar dos anos, talvez a preocupação com a violação dos dados por colaboradores da própria empresa esta diminuindo, talvez as empresas estejam confiando mais em sua equipe, enfim, a preocupação e o monitoramento das atividades do funcionários esta ficando em segundo plano como mostra a figura que segue:

Figura 10: Percentual dos respondentes que relataram dispor das seguintes competências de segurança e privacidade em suas organizações

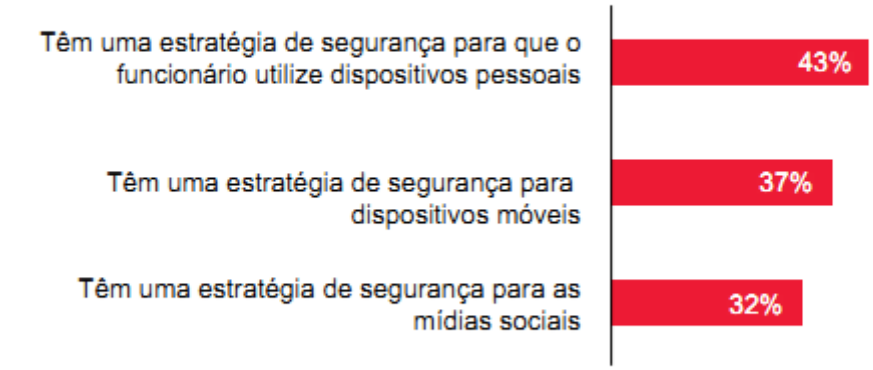
Fonte: 2012 Global State of Information Security Survey®

Figura 7 – Preocupações com Privacidade de usuários e principais competências. Fonte: 2012 Global State of Information Security Survey.

4.6 DISPOSITIVOS MÓVEIS E MÍDIAS SOCIAIS

Com a crescente inovação de tecnologia pessoal, assim como o BUM das mídias sociais no mundo, é cada vez mais comum, ou melhor, é cada vez mais incomum indivíduos que não possuem ao menos um dispositivo móvel, como Pen Drives ou celulares com cartões de memória, e não participam ativamente de pelo menos uma mídia social, como Facebook, Orkut entre outros. Sendo assim as empresas devem estar preparadas para encarar mais essa barreira, como lidar com esta nova era digital:

Figura 15: Percentual dos respondentes segundo os quais suas empresas apresentam os seguintes recursos em vigor para abordar os riscos relacionados aos dispositivos móveis e às mídias sociais



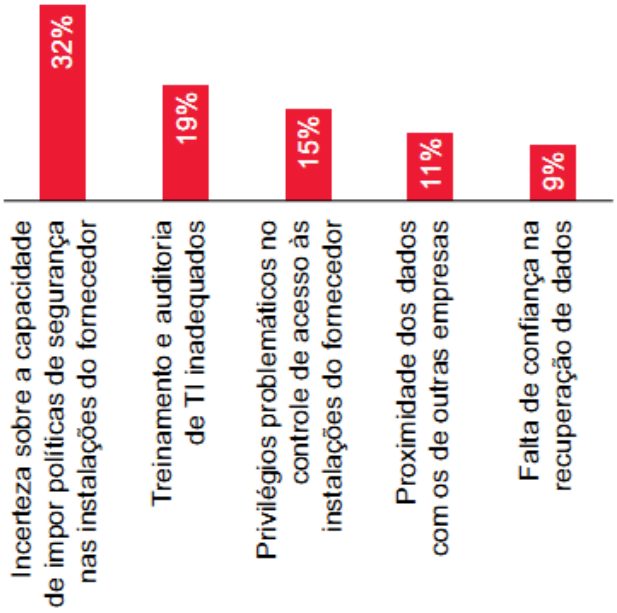
Fonte: 2012 Global State of Information Security Survey®
Nem todos os fatores são ilustrados. Os valores totais não somam 100%.

Figura 8 – Dispositivos pessoais e mídias sociais.
Fonte: 2012 Global State of Information Security Survey.

4.7 COMPUTAÇÃO EM NUVEM

E quanto à computação em nuvem, quais são os apontamentos das empresas como principais dificuldades enfrentadas quando o assunto é o risco de segurança de computação em nuvem:

Figura 17: Percentual de respondentes que identificaram os itens abaixo como principal risco de segurança à estratégia de computação em nuvem nas suas organizações



Fonte: 2012 Global State of Information Security Survey®
Nem todos os fatores são ilustrados. Os valores totais não somam 100%.

Figura 9 – Principais preocupações quanto á computação em nuvem.
Fonte: 2012 Global State of Information Security Survey.

4.8 FONTES DOS INCIDENTES DE SEGURANÇA

Vindo de encontro com o que foi relacionado como risco de segurança à rede no item 3.3.2 (Falta de controle de acesso à rede), e também como ultimo dado selecionado da Pesquisa Global de Segurança da Informação, veremos quais são as principais fontes dos incidentes de segurança apontados pelas empresas:

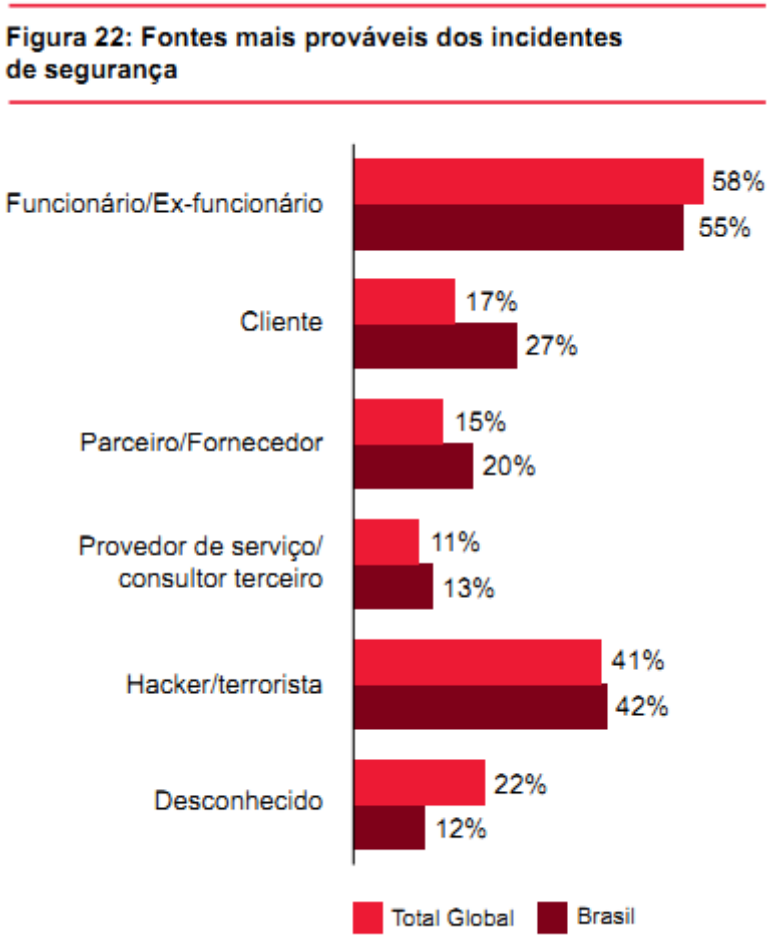


Figura 10 – Principais fontes dos incidentes de segurança.
Fonte: 2012 Global State of Information Security Survey.

5 UMA PROPOSTA PARA MELHORIA DA SEGURANÇA DE REDES

Depois de todos os pontos apresentados neste trabalho, surge uma inquietação eminente: Por onde devo começar? Qual é o primeiro passo?

A primeira coisa para ter em mente é o conceito de que qualquer investimento em segurança é melhor do que nenhum investimento. Porém de nada adianta investir em ferramentas, por mais simples e de baixo custo que sejam, se as mesmas não forem eficazes, e acima de tudo se não forem gerenciadas, ou seja, se não houver um acompanhamento das informações, um monitoramento e uma análise para levantar as reais necessidades da rede para que seja feito uma configuração correta da ferramenta, ela não trará a proteção ideal para a rede. Muitas vezes empresas investem muito em ferramentas de alto nível de segurança, ferramentas de custo elevado que são colocadas na rede e abandonadas, como se elas por si só entendessem as necessidades da empresa e da rede, tomando decisões de gerenciamento automaticamente. O que na verdade não ocorre, estas ferramentas sem um correto gerenciamento tornam-se obsoletas, e é justamente neste contexto que julgo correto que empresas que não possuem nenhuma política ou ferramenta de segurança, comecem por ferramentas de baixo custo e de fácil gerenciamento, para que não se tornem apenas um computador a mais na rede.

5.1 POLÍTICAS DE SEGURANÇA E DIRETRIZES DE USO DA REDE

O primeiro passo para empresas que não possuem quase ou nenhuma política de segurança ou regras de acesso e uso da rede, bem como nenhum departamento específico para monitorar ou gerenciar esta política, é criar uma política de segurança com normas simples que contemplem as necessidades primordiais da empresa. Porém devera seguir algumas características básicas, que são elas:

- Deve ser implementável, de fácil administração, devem ser publicadas as diretrizes de uso aceitável, devem ser de ciência de todos.

- Deve ser reforçada com o uso de ferramentas de segurança apropriadas, configuradas e orientadas pelas necessidades apontadas pela analise empresarial.
- Deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerência.

Os componentes básicos de uma boa política de segurança incluem:

- Uma política de acesso que defini direitos de acesso e privilégios necessários para proteger os recursos da rede, bem como o acesso a dispositivos da rede, dispositivos móveis pessoais, mídias em ROM, horários de uso dos equipamentos, instalação de aplicativos, adição de atualizações ou aplicativos de uso pessoal, busca de diretórios compartilhados não pertinentes ao uso especificamente profissional.
- Uma política que defina as responsabilidades dos usuários, bem como a capacidade de auditoria caso seja constatada uma falha na segurança.
- Uma política de autenticação de usuários, bem como as diretrizes sobre o uso individual das senhas utilizadas na rede ou aplicações que a empresa possua. Também a especificação das características mínimas exigidas para a criação de senhas e o tempo de expiração das mesmas.
- Uma política de definição de disponibilidade da rede, bem como suas redundâncias e as capacidades de backup que a rede possui.
- Uma declaração de horários de manutenção, previsões para solução de problemas pertinentes a rede ou aos usuários especificamente. Muito importante é a informação das manutenções realizadas de forma remota, onde o administrador ou técnico terá acesso e controle total ao equipamento.
- Informações claras e objetivas do que esta sendo monitorado na rede, uma política de controle e monitoramento de informações que trafegam pela rede através de email, mensageiros instantâneos, acessos a sites, downloads realizados, tempo de acesso e permanência em sites.
- E obviamente uma política descrevendo os direitos e atitudes da empresa caso sejam encontradas violações das normas pelos usuários da

rede, bem como a eleição de um fórum trabalhista/criminalista caso seja constatado crime cibernético ou ciberespionagem por parte de colaboradores da empresa.

5.2 BRAZIL FIREWALL E ROUTER

O Brazil Firewall e Router é uma mini distribuição Linux, composta pelas funções de Roteador e FireWall, bem como em sua última versão também a função de Proxy integrado.

O BrazilFW, ou apenas BFW como será tratado aqui, é baseado no Coyote Linux, que foi idealizado por Joshua Jackson em 1998, o qual descontinuou o projeto na versão 2.24 em agosto de 2005. Neste mesmo mês os brasileiros “Claudio” e ”Marcelo – Brazil”, deram continuidade no projeto mudando seu nome para o atual BrazilFW.

No início o do projeto BFW, ainda na versão 2.24 usando a Base do Coyote, a distribuição rodava apenas por disquete. Posteriormente o BFW passou a ser Instalando em mídias de grande capacidade, como os discos rígidos.

Atualmente o BFW esta na versão 3.x, que foi inteiramente codificada e recomeçada do zero por Washington Rodrigues - (Woshman).

5.3 ANALISE SWOT DO BFW

Apresentarei neste tópico uma análise Swot dos pontos fortes e fracos do BrazilFW para entendermos a escolha desta ferramenta como servidor Firewall / Proxy e Roteador de rede.

PONTOS FORTES	PONTOS FRACOS
• Fácil Instalação e Configuração básica;	• Alguns Updates podem matar alguns addons;

• Contempla as funções de Firewall, Proxy e Roteador na mesma ferramenta; • Baixo custo de Hardware; • Software Livre (Open source); • Software Estável; • Atualizações constantes e comunidade participativa; • Fácil gerenciamento; • Muitos Addons que permitem embutir diversas funcionalidades; • Possui um limite imenso de usuários;	• Para uma maior eficácia e personalização requer um pouco de conhecimento em Linux; • Não possui Suporte, visto que se trata de um projeto livre; • Não trabalha com integração em Cluster; • À medida que novas funcionalidades são acrescentadas, exige maior capacidade de Hardware; • Regras mais complexas exigem um conhecimento mais profundo;

5.4 PRINCIPAIS FUNÇÕES DO BFW NA VERSÃO 3.x OU SUPERIOR

- Modos de Conexão
  - STATIC (IP fixo)
  - DHCP
  - Dinamico (PPPoE)
- Acesso seguro ao WebAdmin pelo protocolo SSL
- Servidor Bind (DNS Server)
- Squid-3.0.STABLE19 - 3.0.205
- QOS
- Sub-Redes
- Load Balance (balanceamento de carga) integrado.
  - Com qualquer tipo de Conexão (STATIC, PPPOE, DHCP e edge)
- DHCP Server para rede e Sub-Redes
- GSM

- Novo Cálculo do conntrack automático:
  - Com o novo cálculo, agora são possíveis 1.652 conexões aproximadamente por MB de memória RAM instalada.
- IPupdate 2.0 por link independente.
- Suporte a wireless em modo cliente
- Email com suporte a SSL (gmail)
- Port Forwarding - (Redirecionamento de Portas)
- Smart Route
- Amarração IP X MAC
- DansGuardian - Ideal para uso em Rede Empresariais
- Sarg para uso em Redes Empresariais
- WebAlizer para uso em Provedores
- Modo Bridge - 3.0.206
- Memtest Versão 3.5 - 3.0.206
- Functions.php (Desenvolvido pelo cmartin) - 3.0.206

- Novo "framework" para WebAdmin
- Suporte nativo à SSL
- Ilimitadas Interfaces de Conexão
- Ilimitadas conexões PPOE
- Ilimitados clientes DHCP
- Detecção automática de Hardware

5.5 CONFIGURAÇÕES MÍNIMAS DE HARDWARE

Uma das principais vantagens do BFW é que a exigência de Hardware é mínima, fazendo com que computadores com configurações mínimas possam se tornar Servidores robustos de rede.

- Requerimentos mínimos: Processador 233MMX / 200 MB de memória RAM / 680 MB de HD.

- Requerimentos recomendados: Processador 1 GHZ / 1 GB de memória RAM / 10 GB de HD.

5.6 INSTALANDO O BRAZILFW DO ZERO

O primeiro passo para a instalação do BFW é o Download e a gravação de uma mídia “CD” através de uma imagem ISO. Caso você não conheça o processo de gravação de uma ISO, o Anexo 4 possui um tutorial para Download e gravação da ISO do BFW.

Configurando o Boot: Configure na BIOS do computador que será o servidor para que o boot seja iniciado pelo Drive de CD.

Dependendo da ISO escolhida para instalação aparecerão as telas abaixo:

- As opções para teste de memória (sem e com suporte a multiprocessador respectivamente) é comum às todas as .ISO do BFW 3.x.
- Utilize as setas para cima e para baixo, para selecionar a opção desejada seguida da tecla <enter>.

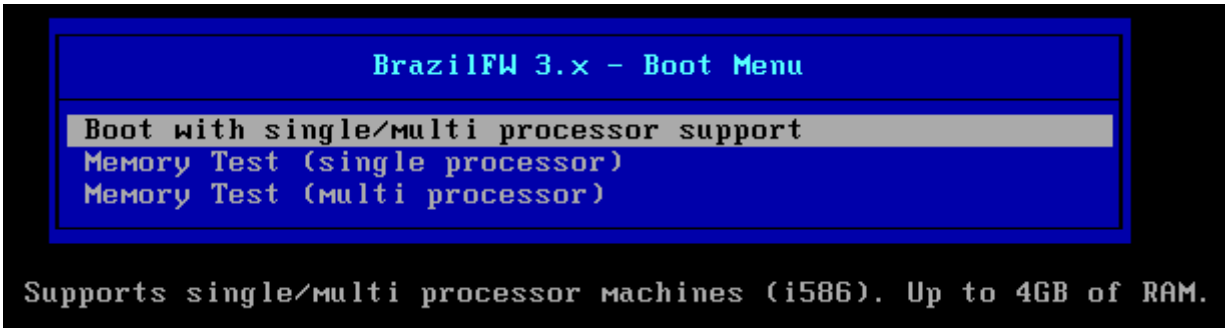


Figura 11 – Tela de Boot para processadores 32bits com até 3GB de memória RAM.
Fonte: BrazilFW Firewall e Router.

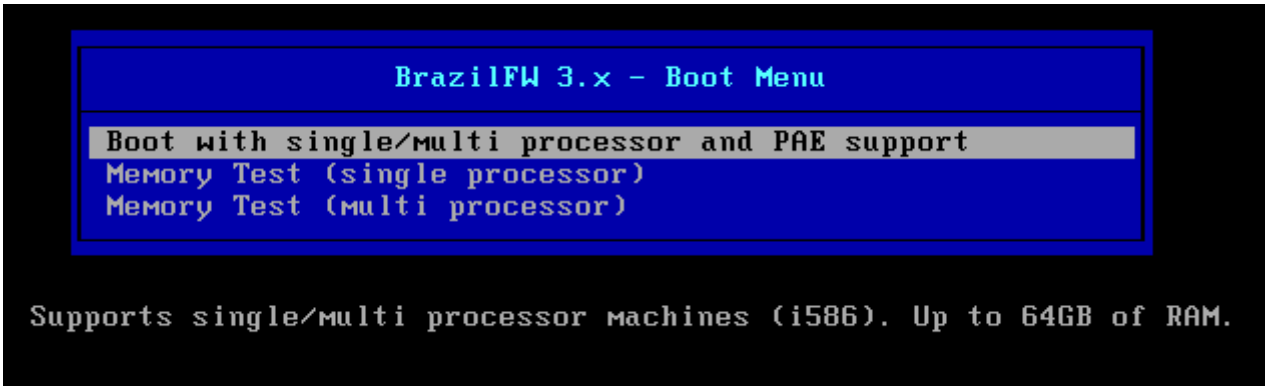


Figura 12 – Tela de Boot para processadores 32bits com mais de 3GB de memória RAM.
Fonte: BrazilFW Firewall e Router.

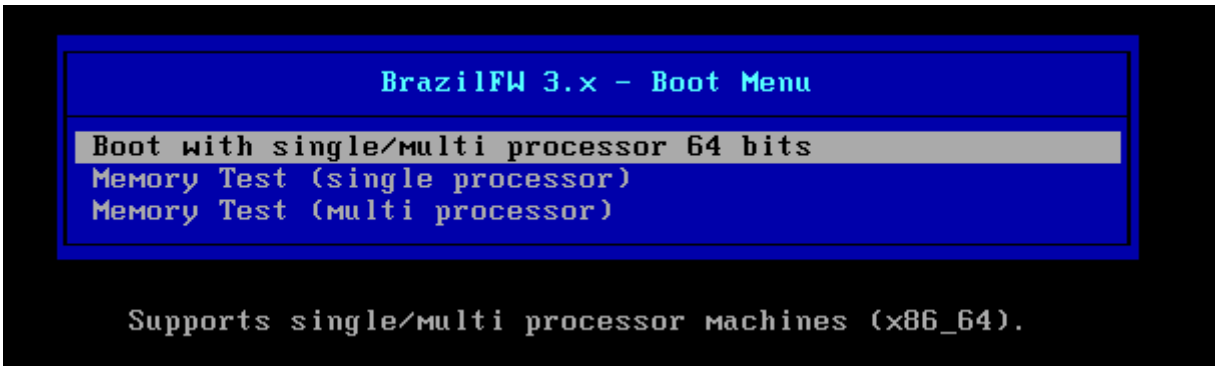


Figura 13 – Tela de Boot para processadores com suporte a 64bits.
Fonte: BrazilFW Firewall e Router.

- Depois do Sistema Operacional carregado estaremos aptos a realizar o processo de instalação no sistema.
- Será necessário inicialmente realizar o Login inicial no BFW conforme os dados abaixo:

Dados do Login inicial:

O Login Padrão do BrazilFW 3.x é:

Usuário: *root*
Senha: *root*

Instalação:

1. Devidamente Logado, você estará no console do BrazilFW 3.x.
2. Digite o comando <install> e tecle <enter>:

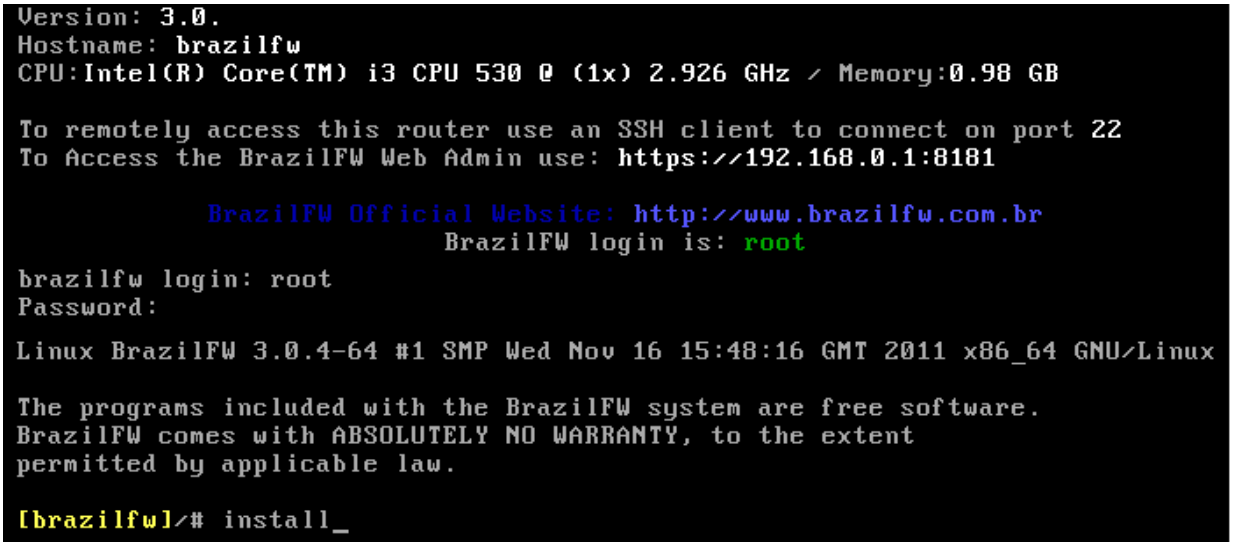


Figura 14 – Iniciar o instalador do sistema.
Fonte: BrazilFW Firewall e Router.

3. *Importante: O instalador criará a primeira partição com 300 MB e aloca o restante do espaço do Disco Rígido na segunda Partição.*

4. Nesta tela será exibido as configurações do disco onde será realizada a instalação, neste caso a instalação sendo feita em um disco virtual com VMware:

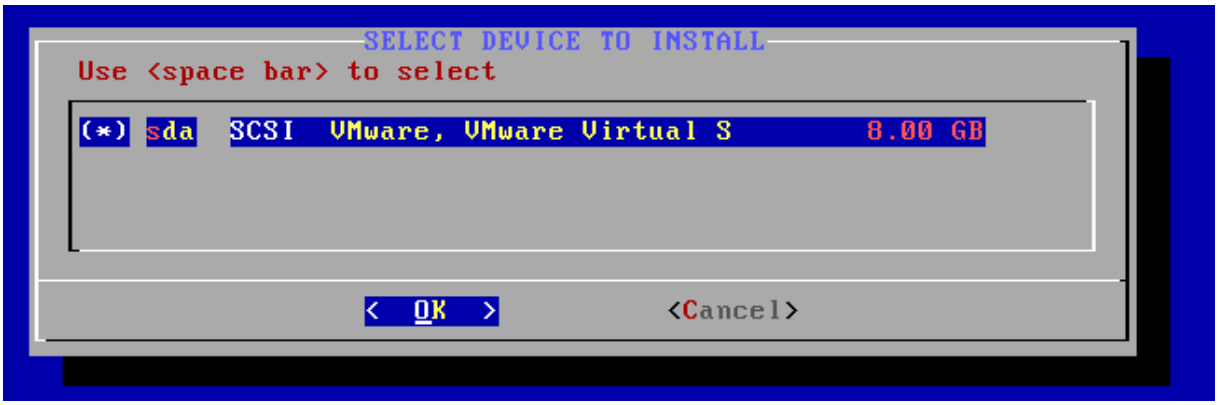


Figura 15 – Configurações da Partição.
Fonte: BrazilFW Firewall e Router.

5. Caso apareça mais de um disco utilize, as <setas direcionais> para navegar e a <barra de espaço> para selecionar, em seguida tecle <enter>.

a. Surgirá a seguinte tela, informando sobre sua escolha, tecle <enter> para continuar.

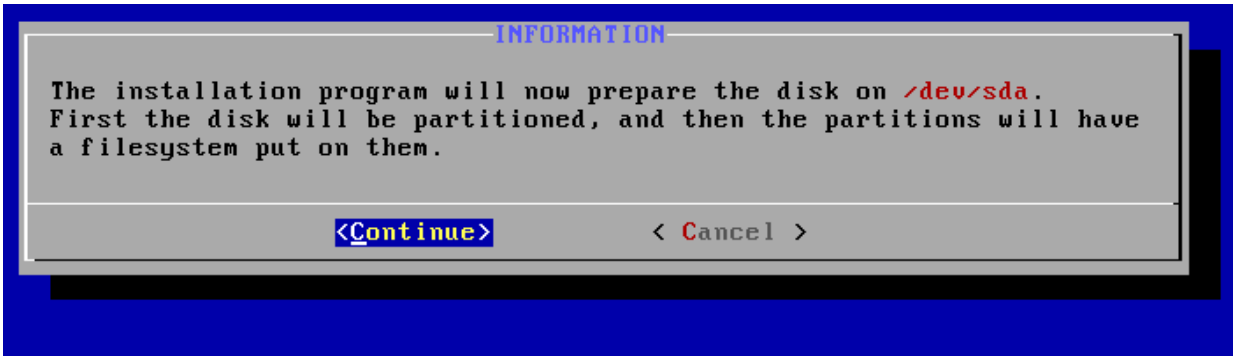


Figura 16 – Informações sobre a partição escolhida.
Fonte: BrazilFW Firewall e Router.

6. Na tela a seguir, o sistema alerta que o disco será formatado e todo o conteúdo anterior será apagado. Será solicitado mais uma confirmação, após isso não terá como voltar atrás.

   a. Tecle <enter> mais uma vez para continuar.

Figura 17 – Informação sobre a formatação do disco e perca dos dados.
Fonte: BrazilFW Firewall e Router.

7. Aguarde alguns minutos enquanto o sistema é instalado:

Figura 18 – Informação sobre a conclusão da instalação e solicita remover CD/DVD.
Fonte: BrazilFW Firewall e Router.

8. Retire o CD da unidade e tecle <enter> para reiniciar o computador.

Configuração Default:

O BrazilFW 3.x vem configurado como default o seguinte IP: 192.168.0.1 com máscara de sub-rede 255.255.255.0 (/24).

Por padrão, o serviço DHCP do BFW 3.x vem habilitado, desta forma configure os Hosts clientes para receberem o endereço de IP automaticamente. Caso o Host não consiga receber o endereçamento IP automaticamente, configure-o manualmente para que seja possível realizar o acesso ao BFW.

- Sugestão para configuração manual do endereço IP.

IP: 192.168.0.2
Máscara: 255.255.255.0 /24
Gateway: 192.168.0.1
DNS: 192.168.0.1

Para confirmar que o servidor esta acessível, digite através do Prompt de comando, tanto para estações Windows como para Linux, o seguinte comando:

- Ping 192.168.0.1 e tecle <enter>.

O resultado deverá ser semelhante a este:

Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64

Web Admin:

Como citado no ITEM “X.X”, uma das maiores vantagens da utilização do BrazilFW, é a sua simplicidade e facilidade para implantação em rede. E a principal característica que comprova esta afirmação, é o painel WebAdmin, desenvolvido com interface gráfica, que pode ser acessado de qualquer Host da rede, e que possui grande parte das funcionalidades do BFW facilmente configuráveis em um ambiente gráfico amigável.

Para acessar o Painel WebAdmin de um Host na rede, digite na barra de endereços de qualquer Browser a seguinte URL:

- https://192.168.0.1:8181

Como trata-se de um acesso seguro através de uma chamada SSL, o browser irá perguntar se você confirma o acesso a este endereço, responda que sim, e torne o endereço confiável para poder continuar o acesso.

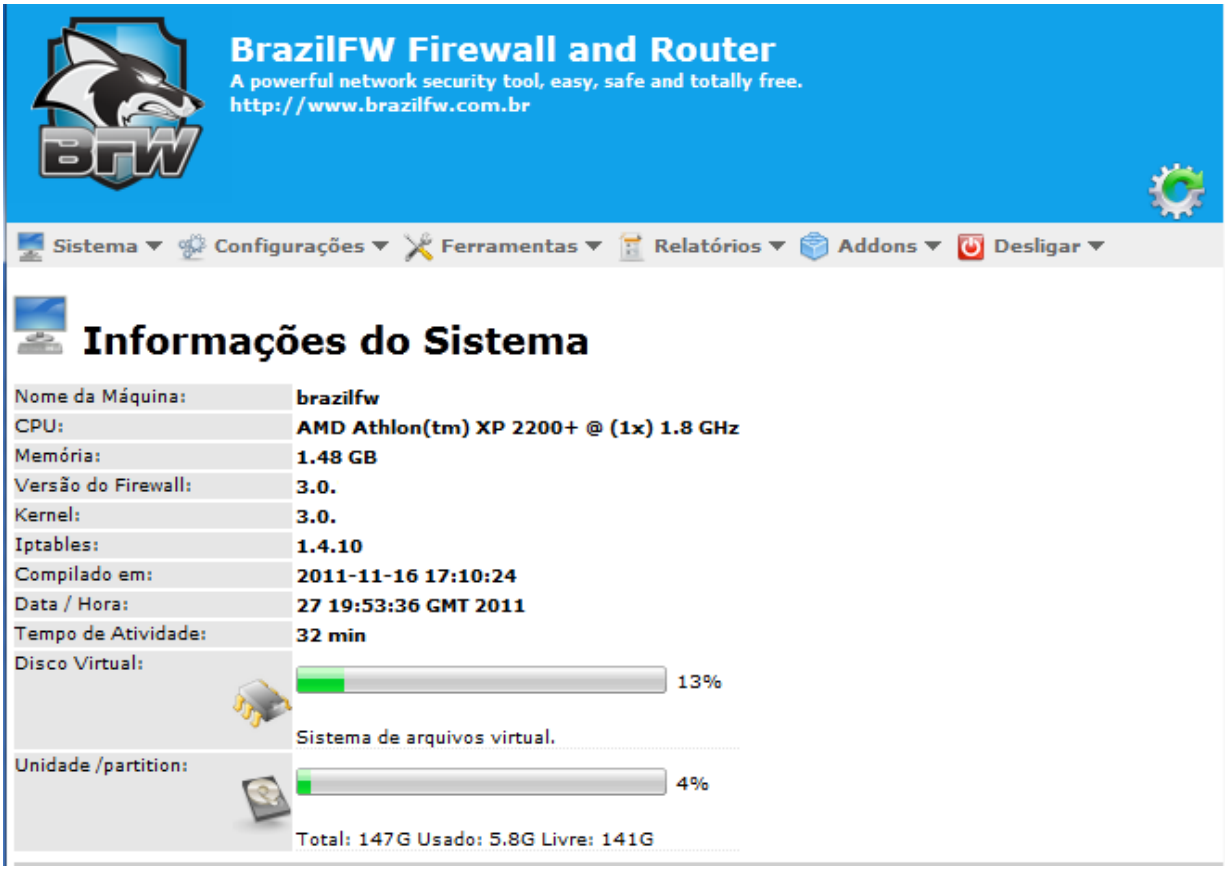


Figura 19 – Informações do Sistema exibido pelo WebAdmin.
Fonte: BrazilFW Firewall e Router.

Alterando a Senha padrão:

Como dito anteriormente a senha padrão do BFW 3.x é “root”, é de extrema importância que você realize a alteração desta senha:

Para alterá-la, siga os passos abaixo:

- *Webadmin => Configurações => Sistema => Senha do Sistema.*

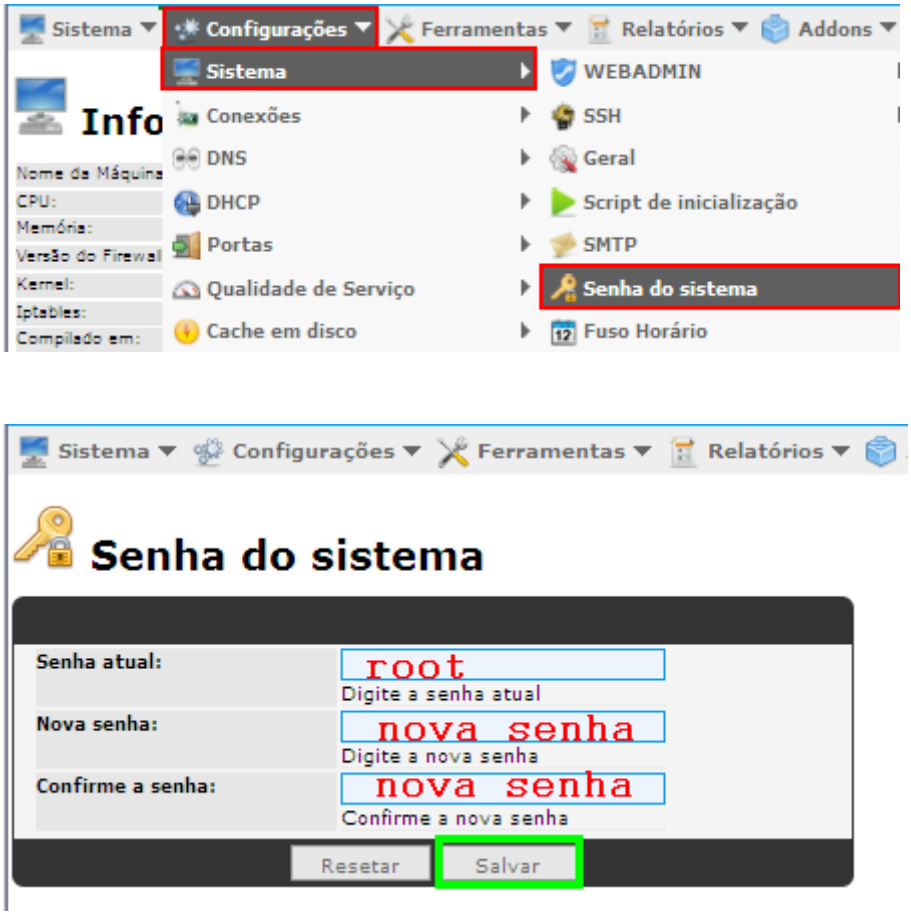


Figura 20 – Tela Mudança de senha pelo WebAdmin.
Fonte: BrazilFW Firewall e Router.

Ou via console do BFW 3.x, diretamente no servidor digite o comando <passwd> e tecle <enter>:

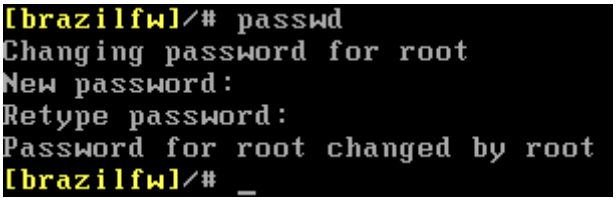


Figura 21 – Tela Mudança de senha pelo Console de comandos.
Fonte: BrazilFW Firewall e Router.

- Digite a nova senha e tecle <enter>
- Digite novamente a nova senha e tecle <enter>

Pronto, sua nova senha já está ativa, agora salve as alterações, para isso, faça:

- *Webadmin => Configurações => Salvar Configurações.*

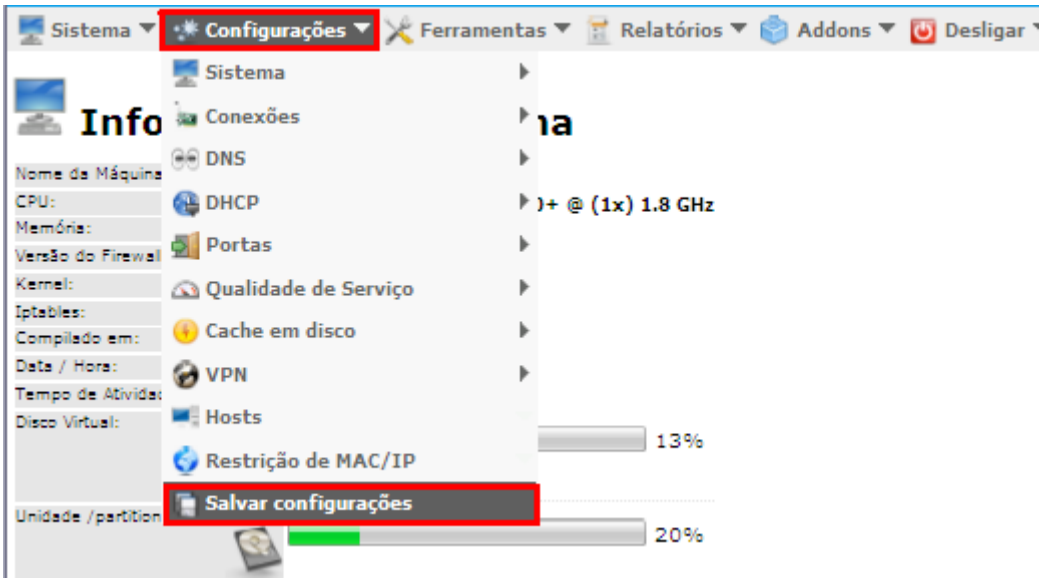


Figura 22 – Salvando configurações do Sistema.
Fonte: BrazilFW Firewall e Router.

5.7 REDUNDÂNCIAS E BALANCEAMENTO DE CARGA (LOAD BALANCE)

Vimos que redundâncias são de extrema importância quando o assunto é alta disponibilidade, no BFW pode-se trabalhar com redundâncias de Links de Internet (conexões ADSL) a fim de garantir alta disponibilidade de conexão com a internet, da mesma forma que pode-se utilizar redundâncias com o BFW, pode-se também configurar um sistema conhecido como balanceamento de carga, que nada mais é do que a divisão da carga de transmissão de internet por dois ou mais Links existentes simultaneamente, ou seja, falando em nível de roteamento, o servidor BFW fará um calculo do percentual que cada link estará utilizando, e enviará o pacote pelo Link com menor percentual de carga.

Outra grande vantagem do balanceamento de carga do BFW, é a alta disponibilidade conseguida através do reajuste de rota, caso algum dos links de conexão caia. O BFW fará automaticamente o redirecionamento de todo o trafego da rede pelo link que estiver com status UP, e desconsiderará temporariamente o Link que estiver com status Down.

Abaixo temos um diagrama que mostra como os Links são divididos e configurados no BFW, com uma única placa de rede. Uma observação importante é a de que a imagem mostra os modems configurados em modo Bridge, porém pode-se perfeitamente configurá-los em modo PPOE.

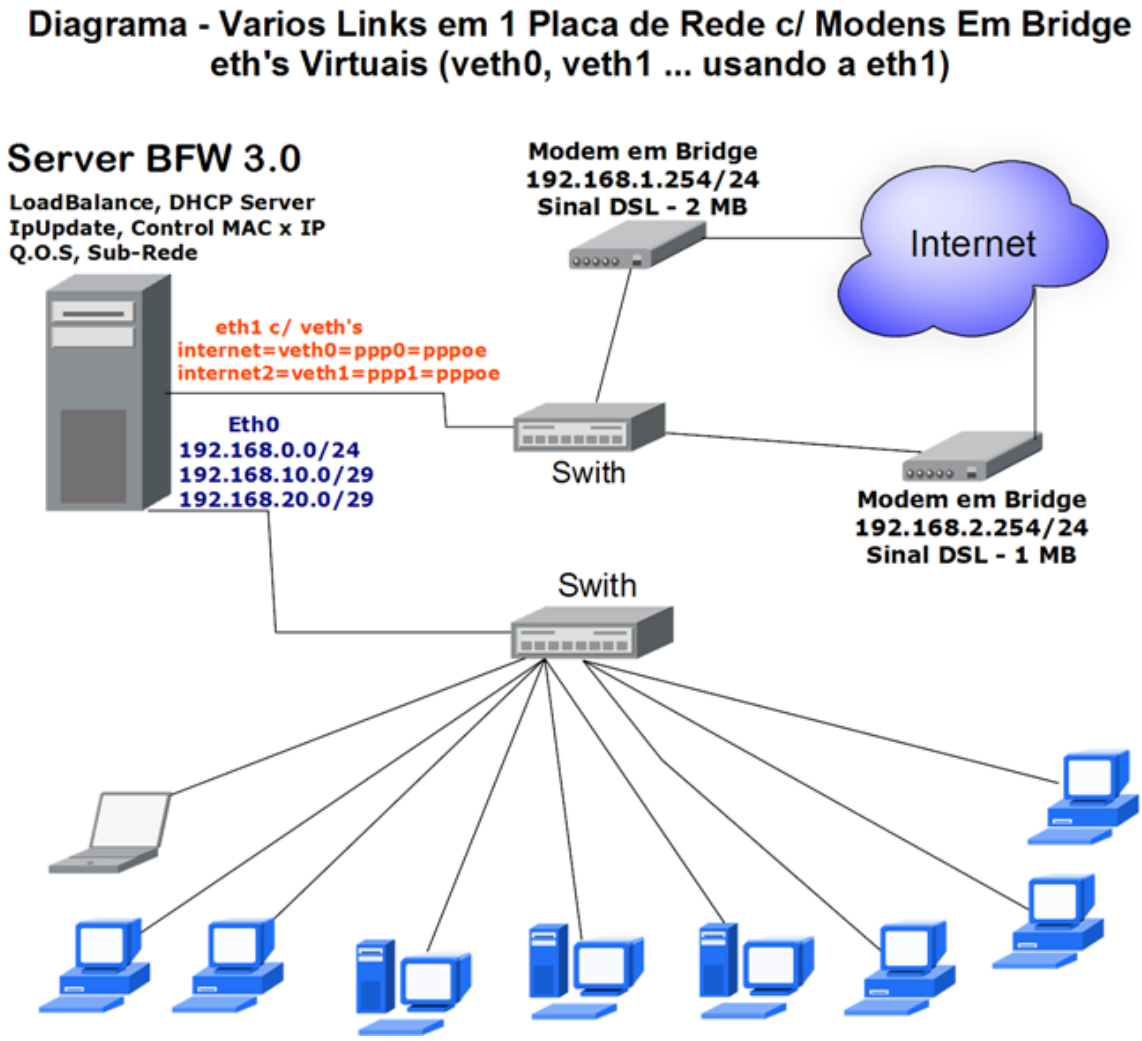


Figura 23 – Diagrama de redundâncias e balanceamento de carga.
Fonte: BrazilFW Firewall e Router.

5.8 SERVIDOR PROXY COM SQUID

Squid é um proxy-cache de alta performance para clientes web, suportando protocolos FTP, gopher e HTTP. O Squid mantém meta dados e especialmente objetos armazenados na RAM, cacheia buscas de DNS e implementa cache negativo de requests falhos.

Ele suporta SSL, listas de acesso complexas e logging completo. Por utilizar o Internet Cache Protocol, o Squid pode ser configurado para trabalhar de forma hierárquica ou mista para melhor aproveitamento da banda. Pode-se dizer que o Squid consiste em um programa principal - squid -, um sistema de busca e resolução de nomes - dnsserver - e alguns programas adicionais para reescrever requests, fazer autenticação e gerenciar ferramentas de clientes.
O Squid pode ser executado nas principais plataformas do mercado, como Linux, Unixes e Windows. O Squid está continuamente melhorando sua performance, além de adicionar novas features e ter uma excelente estabilidade em condições extremas. Sua compatibilidade com várias plataformas e a imensa gama de software para analisar logs, gerar relatórios, melhorar o desempenho e adicionar segurança, providos pela comunidade open source, combinados com ferramentas de administração simplificada e baseadas em web agregam grande valor ao produto. Pode-se ainda citar a capacidade de clustering, transparent proxy, cache de FTP e, é claro, seu baixo custo.

5.8.1 Habilitar e configurar o Squid

Para habilitar e configurar o Squid no *BFW 3.x* vá em *webadmin => Configurações => Cache em Disco.*

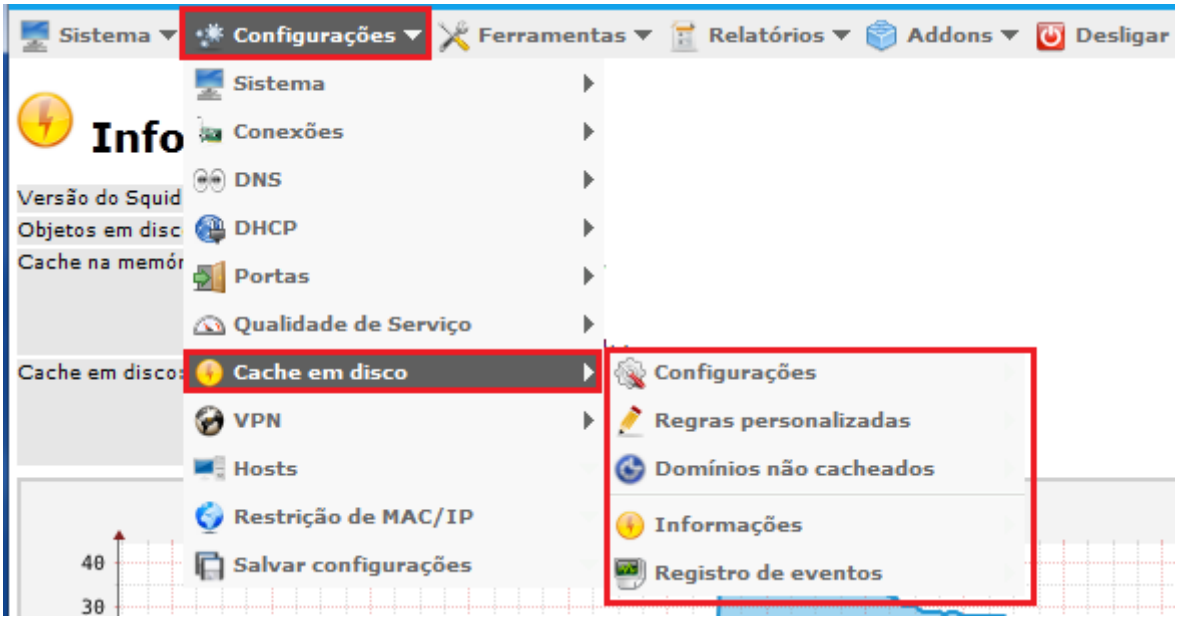


Figura 24 – Habilitar e configurar o Squid.
Fonte: BrazilFW Firewall e Router.

Abaixo teremos mais detalhes de cada campo da tela *webadmin => Configurações => Cache em Disco => Configurações*.

Figura 25 – Configurações do Cache.
Fonte: BrazilFW Firewall e Router.

CONCLUSÕES

O mercado de tecnologias de segurança em redes de computação esta em constante crescimento, já existe milhares de ferramentas que podem ser utilizadas para combater problemas de segurança, sejam estes de qualquer espécie. Porém muitas empresas de pequeno e médio porte possuem pouca ou nenhuma tecnologia de proteção à rede. E muitas vezes a falta de um Gerenciamento destas tecnologias, mesmo que existam, as tornam obsoletas ou ultrapassadas. Um segundo fator que prejudica as pequenas e medias empresas no quesito segurança da informação, é a falta de políticas de segurança da informação eficazes e tangíveis, ou a falta de quem elabore e gerencie estas políticas de segurança.

Este trabalho apresentou algumas características primordiais para elaboração de uma coerente política de segurança da informação, apontando as principais características que devem ser pensadas quando se trata de segurança da informação. Pois as políticas de segurança não devem ser tomadas como diretrizes que serão usadas no futuro quando a empresa atingir um nível desejado, elas devem ser elaboradas de forma que contemplem as necessidades atuais da empresa, auxiliando no cenário que a empresa se encontra no momento. Obviamente que se pode planejar e escrever regras que serão usadas no futuro, ou simplesmente ir moldando a política conforme o crescimento da empresa, e conforme novas necessidades surgirem.

Foi proposta também a implantação do Brazil Firewall e Router, uma ferramenta que contempla paralelamente um servidor Firewall, um Proxy e um roteador de fácil instalação, configuração e de fácil gerenciamento. Esta ferramenta foi selecionada dentre outras opções no mercado, pelo bom nível de proteção que oferece, pela baixa complexidade de gerenciamento e pelo baixo custo de implantação. Foram apresentadas suas principais características, uma manual de instalação e configuração, bem como um manual de configuração de suas principais funcionalidades.

Como conclusão de todas as pesquisas e leituras realizadas durante a elaboração deste trabalho, acredito que não seja possível ficar absolutamente protegido contra qualquer ameaça à segurança da informação. Visto que até mesmo sistemas como o da NASA, CIA e FBI já sofreram invasões de hackers. Quando o assunto tratar de segurança da informação, os criminosos virtuais sempre terão

vantagens em relação aos sistemas impostos pelas organizações, devido às três premissas básicas necessárias para criar qualquer sistema de segurança que seja: Necessidade, Conhecimento e Tempo. Quem cria sistemas de segurança da informação, os profissionais que pensam e elaboram as políticas de segurança, aqueles que implantam ferramentas de segurança de rede nas empresas, todos possuem a necessidade, pois estão sendo pagos para isto. Todos possuem conhecimento, em níveis diferentes, alguns com mais conhecimento outros com menos, mas todos com um nível intermediário e avançado de conhecimento no assunto. Porém, em quase 100% dos casos de profissionais, empresas ou equipes que elaboram sistemas de segurança da informação, a premissa que falha é o Tempo, pois ao mesmo tempo em que trabalham em um projeto, estão atuando em mais dois ou três projetos simultaneamente. Inúmeras demandas, muita cobrança e o curto espaço de tempo para conclusão dos projetos, é o que coloca os criminosos da internet sempre um passo a frente, pois em contrapartida o que não lhes falta é o tempo, mesmo que não tenham um conhecimento tão aprofundado, mas possuem tempo para pesquisar, estudar e aprender novas técnicas, e obviamente podem tentar burlar o sistema quantas vezes forem precisas.

E é isto que se caracteriza como segurança da informação, um sistema complexo, mas com bases simples, que esta em constante aprimoramento, que se desenvolve diariamente erguendo novas barreiras e preenchendo as brechas que surgem.

REFERÊNCIAS

BERNSTEIN, Terry; BHIMANI, Anish B.; SCHULTZ, Eugene; SIEGEL, Carol A. **Segurança na Internet.** Rio de Janeiro: Campus, 1997.

BISHOP, Matt. **Computer Security:** Art and Science. Boston: Pearson Education, 2003.

Brazil Firewall e Router. **BrazilFW 3.x.** Disponível na Internet: http://pt-br.wiki.brazilfw.com.br/Main_Page/pt-br. Acesso em Novembro - 2011.

KUROSE, James; ROSS, Keith. **Rede de computadores e a internet:** Uma abordagem top-down. 3.ed. São Paulo: Pearson Addison Wesley, 2006.

McCumber, John. **Assessing and Managing Security Risk in IT Systems:** A Structured Methodology. 1.ed. Auerbach, 2005.

MELLO, Emerson Ribeiro. **Redes de Confiança em Sistemas de Objetos CORBA**. Disponível na Internet: http://gcseg.das.ufsc.br/cadconf/artigos/mellossi2003.pdf. Acesso em Janeiro-2012.

PwC Brasil. **Pesquisa Global de Segurança da Informação 2012**. Disponível na Internet: http://www.pwc.com.br/pt/estudos-pesquisas/index.jhtml. Acesso em Dezembro-2011.

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