UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
ESPECIALIZAÇÃO SEMI PRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA PROJETO DE REDE BASEADA EM *SOFTWARE* LIVRE

NILSON SÉRGIO DALLABONA

CURITIBA
2013

NILSON SÉRGIO DALLABONA

SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA PROJETO DE REDE BASEADA EM *SOFTWARE* LIVRE

Trabalho de Monografia apresentado ao Curso de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Gerenciamento de Servidores e Equipamentos de Rede".

Orientador: Prof. MSc. Fabiano Scriptore de Carvalho

CURITIBA

2013

AGRADECIMENTOS

À Deus, pela dádiva da vida.

À minha mãe Edília, pelo apoio e incentivo que me deu durante toda minha vida. Ela que é Mãe e Pai desde a minha adolescência.

À Minha esposa Maria Luiza, pelo amor, paciência, compreensão e incentivo durante todo o percurso de estudos.

Aos meus irmãos que sempre estiverem presentes durante toda esta etapa, incentivando e apoiando.

Ao meu orientador, Professor Fabiano, pela paciência, orientação, ajuda e colaboração.

RESUMO

Não há como voltar atrás. Qualquer organização, desde a pequena empresa com dois ou três PCs, até uma complexa organização com atuação em diversos países, sabe que em maior ou menor grau a tecnologia é essencial para seu negócio. E é justamente por ser vital, que esse bem não palpável traz consigo uma necessidade básica: segurança. Primeiro eleva-se a informação ao patamar mais crítico da empresa, tornando-a peça principal do jogo. Em seguida, vê-se que esse dado, pela forma e processo com que é disponibilizado, corre o risco de ser corrompido, alterado, roubado ou disponibilizado na própria Internet ou, em casos piores, usurpado por funcionários e passado para a concorrência ou ainda simplesmente causando danos financeiros à empresa. A segurança da informação não depende única e exclusivamente de equipamentos de segurança de rede de alto custo, mas também, de políticas de segurança, treinamento, educação profissional e conscientização em todos os níveis hierárquicos dentro da organização. Este trabalho não tem por objetivo apresentar uma solução única e definitiva para implantação de um nível de segurança alto dentro das organizações, pois chegou-se a conclusão que não existe uma receita infalível. Cada organização, dentro do seu ramo de atividade ou rede de computadores possui características únicas que devem ser analisadas individualmente antes da escolha da tecnologia eficaz na proteção de seus dados e informações. Sugere-se então, a utilização de ferramentas em *Software* Livre, que respeitadas às características de cada organização, podem trazer uma camada de segurança com um baixo custo para a entidade.

Palavras-chave: Informação. Segurança. Políticas de Segurança. Treinamento. *Software* Livre.

ABSTRACT

There´s no turning back, any organization, since a small company with two or three PCs to a complex organization with a acting in different countries, it know that in greater or lesser extend the technology is essential for your business. And it is justly because it is vital and it brings a basic need: security. First rises the information in the critical level in the company, making a main piece in the game. Then one sees that given in the form and process that is available, run the risk of being corrupted, altered, stolen or made available in the Internet or in worst cases, infringed by staff and passed to competition or simply causing financial damage to the company. The information security does not depend only and exclusively of security equipments of costly network but also security policies, training, professional education and awareness at all levels within the organization. This work does not have like purpose to present a single and definitive solution to implement a high level of security within organizations, as we arrived to the conclusion that there is not a foolproof recipe. Each organization, in its industry or computer network has unique characteristics that must be analyzed individually before choosing effective technology for protecting their data and information. It is then suggested the use of Free Software tools that met the requirements of each organization, can bring a security layer with a low cost to the entity.

Key words: Information, safety, security policies, training and free software.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E/OU SIGLAS

ACL	*Access Control Listsi.*
AD	*Active Directory*.
AIX	Sistema Operacional UNIX® baseado em padrões abertos para rodar aplicações nos servidores IBM Power Systems.
ABNT	Associação Brasileira de Normas Técnicas.
BSD	*Berkely Software Distribution*.
CARP	*Common Address Redundancy Protocol* ou Protocolo de Redundância de Endereço Comum.
CD-ROM	*Compact Disc-Read Only Memory* ou Disco Compacto com Memória somente para Leitura.
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.
CPU	Unidade Central de Processamento.
CSIRTs	Grupos de Segurança e Resposta a Incidentes de Rede.
DHCP	*Dynamic Host Configuration Protocol*.
DIO	Distribuidor Interno Óptico.
DMZ	***D**e**M**ilitarized **Z**one*.
DNS	Domain Name System.
DoS	*Denial of Service*.
FOSS	*Free Open Source Software*.
FreeBSD	Sistema Operacional *UN*X-like* para plataformas i386 e Alpha/AXP.
FSF	*Free Software Foundation*.
FTP	*File Transfer Protocol* – Protocolo de Transferência de Arquivo.
GB	*GigaBytes*.
GUI	Graphical User Interface – Interface Gráfica do Usuário.
GPL	*General Public Licence*.
HP-UX	Sistema Operacional da Hewlett-Packard (HP), sendo uma variação do sistema Unix.
HTTP	*HyperText Transfer Protocol*.
HTTPS	*HyperText Transfer Protocol Secure*.

ICMP	*Internet Control Message Protocol*.
ID	Identificação do usuário.
IEC	*International Engineering Consortium*.
IPsec	Internet Protocol Security ou Protocolo de Segurança IP.
IRIX	Sistema Operacional baseado no Unix com o BSD desenvolvido pela Silicon Graphics (SGI).
ISO	*International Standartization Organization*.
LAN	*Local Area Network*.
LDAP	Lightweight Directory Access Protocol ou Protocolo Leve de Acesso a Diretórios.
Log-on	Ganhar acesso a determinado sistema através de uma senha.
Log-off	Terminar o uso de um sistema computacional.
MAC	*Media Access Control*.
MacOS	Sistema Operacional utilizado nos computadores *Apple*, deriva de *Macintosh Operating System*.
MB	Megabytes.
Mbps	Mega *bits* por segundo – velocidade de tráfego de dados, equivalente a um milhão de bits por segundo.
MHZ	Mega *Hertz*. Um milhão de *hertz* (um ciclo) por segundo.
NBR	Norma Brasileira de Referência.
NetBSD	Sistema Operacional UNIX-like baseado no padrão BSD 4.4.
NFS	*Network File System* ou Sistema de Arquivos Distribuídos.
NIC.br	Núcleo de Informação e Coordenação do Ponto BR.
Ntop	*Network* Top: ferramenta automatizada para análise e gerenciamento de redes.
NTP	Protocolo para sincronização dos relógios dos computadores.
OSI	*Open System Interconection* ou Sistema de Interconexão aberto.
OSS	*Open Source Software*.
Pfsync	Interface de rede que expõe certas alterações feitas na Tabela de Estados.
PAM	*Pluggable Authentication Module*.
PC	*Personal Computer*.
PPTP	*Point to Point Tunneling Protocol*.
PSI	Plano de Segurança da Informação.

RAM	Random Acces Memory ou Memória de Acesso Randômico.
RJ45	*Registred Jack* 45. Conector padrão para cabeamento de rede.
SMB	*Server Message Block*.
TCP	*Transmission Control Protocol*.
TCP/IP	*Transmission Control Protocol / Internet Protocol*.
TI	Tecnologia da Informação.
UDP	*User Datagram Protocol*.
UTC	*Coordinated Universal Time*.
VLAN	*Virtual Local Area Network* ou *Virtual LAN*.
VOIP	Voz sobre Protocolo de Internet.
VPN	*Virtual Private Network*.
XML	*eXtensible Markup Language*.
XMPP	*eXtensible Messaging and Presence Protocol*.

GLOSSÁRIO

Backup	Cópia de segurança.
Blacklist	Lista de domínios ou endereços IP reconhecidos como fontes spam.
Boot	Processo de inicialização de um computador.
Bridge	Ponte. Dispositivo que conecta segmentos de redes permitindo a transmissão de dados entre elas.
Cache	Dispositivo de acesso rápido.
Container seguro	são volumes ou discos virtuais encriptados.
Copycenter	Centro de Cópias.
Copyleft	Direito de permissão de cópia de uma obra por outros usuários, dando a liberdade de copiar, modificar e redistribuir, exigindo que esse direito seja mantido em todas as versões.
Copyright	Direito autoral, a propriedade literária, que concede ao autor de trabalhos originais direitos exclusivos de exploração de uma obra artística, literária ou científica, proibindo a reprodução.
Desktop	Designação comum para computadores pessoais de mesa.
DNS Primary	Endereço IP principal na resolução de nomes.
DNS Secondary	Endereço IP secundário na resolução de nomes.
Domain	Domínio.
Download	Transferir **(**baixar**)** um ou mais arquivos de um servidor remoto para um computador local.
Ethernet	Arquitetura de interconexão de redes locais.
Failover	Processo no qual uma máquina assume os serviços de outra, quando esta última apresenta falha. Ou ainda, transferência automática por falha.
Firmware	Conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico.
Flag	Utilizado como interruptor (ligado/desligado ou ativo/inativo).
Gateway	Porta de ligação, equipamento intermediário geralmente destinado a interligar redes.

Gigabit	Unidade de medida de informação que equivale a um bilhão de *bits*.
Gopher	Protocolo de rede desenhado para distribuir, procurar e aceder a documentos na Internet.
Hardware	Parte física de um computador e de seus periféricos.
Host	(máquina) – um computador que faz parte da rede.
Hostname	Nome pelo qual um computador é conhecido em uma rede.
Ipchains	Componente do *Kernel* Linux responsável por habilitar o filtro de pacotes através de regras de *Firewall*.
Iptables	Componente do *Kernel* Linux responsável por habilitar o filtro de portas através de regras de firewall.
Linux	Sistema Operacional Multitarefa para computadores pessoais.
Live CD	CD que contém um sistema operacional que não precisa ser instalado no disco rígido do usuário, sendo executado diretamente a partir do CD e da memória RAM do computador.
OpenBSD	Sistema Operacional do tipo UNIX, livre, multiplataforma, baseado no 4.4BSD.
OpenVPN	*Software* livre desenvolvido por James Yonan e publicado pela GNU, destinado à administração da VPN.
Open Source	"Código aberto" - significa que o código fonte do *software* está disponível aos interessados.
Password	senha.
Patch Cord	Cabos de conexão.
Patches	Correção de segurança de um determinado *software* ou Sistema Operacional.
Pendrive	Dispositivo portátil de armazenamento com memória *flash*, acessível através da porta *USB*.
Pentium	5ª geração de microprocessadores com arquitetura x86 fabricados pela Intel.
pfSense	É um *open source* baseado em *FreeBSD* utilizado como *Firewall* e Roteador.
Proxy	Intermedeia o tráfego entre o servidor principal e o cliente controlando os acessos.
Restore	Processo no qual se restaura ou recupera um *backup*.

Scrubbing	É um processo de limpeza e reparo ou eliminação de partes de dados com mau funcionamento, incompletos ou duplicados.
Setup	É um programa de configuração que todo micro tem e que está gravado dentro da memória ROM do micro.
Serpro	Serviço Federal de Processamento de Dados.
Snort	Ferramenta *open source* que monitora o tráfego de pacotes em redes IP.
Software	Parte lógica de um computador (Sistema Operacional e Programas).
Stateful	Tipo de *Firewall* (com estado) no qual a decisão sobre a passagem ou não de um pacote leva em consideração outros pacotes que atravessaram anteriormente o *Firewall*.
Storage	Dispositivos projetados especificamente para armazenamento de dados.
Switch	Equipamento que possibilita a conexão de computadores em rede.
Timezone	Zonas horárias ou fusos horários.
Throughput	Capacidade total de um canal ou dispositivo em processar e transmitir dados durante um determinado período de tempo.
Truecrypt	Aplicativo de código aberto para Windows e Linux que cria volumes criptografados, os quais podem ser montados como unidades virtuais.
UPLoad	Envia arquivos de texto, vídeo ou imagens do seu computador para um servidor remoto.
Unionfs	*Stackable unification file system* – sistema de arquivos que permite que diretórios sejam sobrepostos de uma forma transparente criando, assim, um diretório virtual resultante destes.
Username	Nome de usuário.

SUMÁRIO

1 INTRODUÇÃO

O tema segurança em redes atualmente ocupa posição de destaque em grande parte dos ambientes corporativos, sejam eles de pequeno, médio ou grande porte. As empresas cada vez mais instigadas à competição, e com a concorrência alta no mercado, precisam estar em desenvolvimento tecnológico constante. Neste cenário, as ferramentas de segurança desempenham um papel importante para levar a organização ao topo dos negócios.

As decisões são tomadas com base nos dados e informações, os quais precisam ser confiáveis e para isso os métodos, regras e procedimentos se tornam indispensáveis. Os dados de uma entidade são de extremo valor para sua evolução e quando revelados a terceiros com intenções maliciosas, podem trazer tanto prejuízos financeiros, quanto à imagem da organização.

Ocorre que às vezes gerentes e profissionais da área de redes tratam a segurança visando coibir invasões externas às informações de suas empresas e acabam por esquecer de um fator não menos importante, as falhas de segurança interna, sejam elas relacionadas aos colaboradores da empresa, os quais mal intencionados ou mesmo sem a intenção de causar um mal maior acabam provocando danos; pela inexistência de uma política interna de segurança, a qual deve ser divulgada entre os usuários dos meios de tecnologia existentes na rede; ou físicas em relação a possíveis danos aos equipamentos da rede.

Ao fazer referência à Segurança da Informação, recordam-se as tecnologias diversas para se proteger sistemas, criar “muralhas” contra os inimigos capazes de invadir servidores dos mais variados portes, antivírus e *firewall* eficazes para detectar e barrar ameaças perigosas exige altos investimentos e pessoal treinado para implantar, gerenciar e manter funcionando toda essa estrutura.

A segurança da informação está relacionada com a proteção dos valiosos dados de um indivíduo ou de uma determinada empresa, defendendo a confidencialidade, integridade e disponibilidade da informação.

É possível ter segurança aplicando-se as ferramentas certas da maneira correta, aliadas a uma política de segurança bem elaborada e amplamente divulgada e praticada por cada um dos colaboradores que fazem parte da instituição para utilização consciente dos meios de tecnologia da informação.

O *software* livre atente com eficiência às necessidades de segurança utilizando-se de ferramentas que executam tarefas similares a de equipamentos, por vezes caros, aos quais muitas empresas e instituições não teriam condições financeiras de adquiri-los.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Implementar o projeto lógico da rede de dados de uma organização, apresentando uma proposta para uso de ferramentas em *software* livre nos serviços a serem disponibilizados aos usuários, estabelecendo regras visando a segurança da informação, sem a necessidade de adquirir equipamentos e *softwares* proprietários de alto custo.

1.1.2 Objetivos Específicos

- Levantar junto aos usuários da rede, a relação dos serviços, sites e outras informações necessárias sobre a rotina de trabalho, para definir o enlace de Internet e o planejamento das regras de acesso a Internet e servidores;
- Buscar junto às empresas fornecedoras de enlaces de acesso à Internet existente na cidade sede da Instituição/Organização em questão, a opção mais adequada às necessidades do grupo;
- Realizar reuniões com a gerência da organização para a definição das restrições de acesso às informações, as quais serão detalhadas em uma cartilha de segurança da informação a ser elaborada;
- Realizar testes com o *firewall* pfSense utilizando as regras de segurança e acesso propostas pela gerência da Instituição/Organização;
- Documentar o detalhamento do projeto lógico, os quais serão armazenados no departamento responsável pela segurança da Instituição/Organização.

1.2 JUSTIFICATIVA

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples, pois bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e com o uso de computadores, a necessidade de uma estrutura de segurança ficou mais evidente. Em função da chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, com ou sem fins lucrativos, já que sem computadores e redes de comunicação, as atividades podem se tornar inviáveis.

O local escolhido para o desenvolvimento deste projeto é uma Unidade do Governo Federal, com estrutura física dividida em 7(sete) prédios já ocupados e em funcionamento, contendo diversas seções que estão distribuídas dentro desse espaço.

A Organização, desde o ano de 2010, com a Elaboração do Plano de Padronização do Ambiente e Migração para *Software* Livre, vem trabalhando para se alinhar às determinações contidas no plano, tanto no que tange a ferramentas e aplicativos utilizados bem como a elaboração de políticas e regras de segurança, tomando-se como princípio básico a adoção de *software* livre em todo o parque de máquinas.

Este trabalho tem como base o projeto para implantação de uma rede de dados desde o seu início, ou seja, identificando a estrutura de rede adequada a ser adotada, até a implantação dos serviços que estarão disponíveis na rede, baseados em *software* livre, passando pela elaboração da política de segurança a ser adotada de acordo com as características da instituição, definição do *firewall* e suas regras de segurança.

No que diz respeito às formas de segurança, pode-se citar a segurança física: voltada à estrutura material da tecnologia, servidores e equipamentos necessários ao funcionamento da Instituição/Organização e o local onde ficam instalados os

mesmos. A segurança lógica: tratando de *softwares* (*firewall*, antivírus) e arranjos lógicos na organização das redes de computadores. E por último, mas não menos importante, apresenta-se a segurança operacional (humana), que visa estipular normas de utilização a serem seguidas pelas pessoas envolvidas em todo o processo tecnológico corporativo, sejam usuários leigos ou profissionais de TI.

Desta forma, têm-se uma estrutura de segurança em camadas (física, lógica e operacional), as quais serão regidas por normas como a ABNT NBR ISO[1]/IEC[2] 17799:2005, ABNT NBR ISO/IEC 27001:2013 e 27002:2013, para esclarecimento e elaboração dos principais pontos relacionados à gestão de segurança da informação em redes de computadores.

1 ISO (*International Standartization Organization).* Trata-se de uma organização internacional formada por um conselho e comitês com membros oriundos da maioria dos países. Seu objetivo é criar normas e padrões universalmente aceitos sobre como realizar as mais diversas atividades comerciais, industriais, científicas e tecnológicas.

2 IEC (*International Engineering Consortium*). É uma organização voltada para o aprimoramento da indústria da informação. Uma associação entre as duas instituições produz normas e padronizações internacionais.

2 NECESSIDADE DE UMA INFRAESTRUTURA SEGURA

Atualmente todos estão conectados via web a um “mundo virtual”, onde há uma infraestrutura que precisa ser segura.

A infraestrutura consiste nas instalações físicas, serviços e gestões, que dão suporte a todos os recursos de informática compartilhados na Instituição/ Organização.

2.1 CONSIDERAÇÕES INICIAIS

A seguir, serão descritos quais os fatores que levam à conscientização do quão importante e necessário é implementar uma infraestrutura de rede que garanta um bom nível de segurança das informações.

Neste capítulo, constarão as características que traduzem o significado da preocupação com a segurança dentro de um modelo de rede de computadores, tendo como foco principal sua aplicação em ambientes corporativos, pois é onde o fator segurança é mais preocupante devido ao grau de sensibilidade e importância das informações envolvidas.

2.2 DEFINIÇÃO DE INFORMAÇÃO

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. (ABNT NBR ISO/IEC 27002:2005).

A informação pode existir sob diversas formas, seja ela impressa, escrita em papel, armazenada eletronicamente, enviada pelo correio ou por meios eletrônicos, independente da forma como ela se apresenta, compartilhada ou armazenada é de vital importância não só para empresas e instituições como também para pessoas comuns.

Conhecimentos, conceitos, idéias e marcas são exemplos de formas intangíveis da informação. No mundo interconectado a informação e os processos a ela relacionados, sejam eles, sistemas, redes e pessoas envolvidas nas suas operações estão presentes no cotidiano de empresas e pessoas, com diferentes valores e importância.

2.3 DEFINIÇÃO DE SEGURANÇA

Nos dias de hoje, a questão da segurança[1] é algo tão imprescindível que não se pode sequer pensar em desconsiderá-la. As empresas fazem o possível para se adequarem à realidade existente no mundo da informática e procuram bons administradores para projetarem e administrarem suas redes de forma a não permitirem um acesso indevido, ou nocivo, às mesmas. Contudo, nada do que se relaciona à segurança pode ser definido como imutável, ou válido sobre quaisquer circunstâncias. Na verdade, o conceito "segurança" se traduz efetivamente em minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. "Vulnerabilidade é qualquer falha ou fraqueza que pode ser explorada para se ter acesso a um sistema ou os dados que ele contém", segundo definido por SOARES (1995).

Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

---

1 "*s.f.* (1391 cf. FichIVPM) **1** ação ou efeito de tornar seguro; **2** atitude de confiança nos próprios recursos; **3** estado em que a satisfação de necessidades e desejos se encontra garantida; **4** estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal; **5** situação em que não há nada a temer" (HOUAISS, 2001).

2.4 A SEGURANÇA DA INFORMAÇÃO

"Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 27002:2005).

O assunto *segurança da informação* está longe de ser consensual e compreendido em toda a sua abrangência e consequências, seja pela sociedade, seja por profissionais das mais diversas áreas de atuação.

Com o incremento da chamada *Internet comercial* em meados da década de 1990, a questão da manipulação de informações e da sua segurança ganha maior ênfase, pois a grande rede e seus protocolos, especialmente a família TCP/IP, foram construídos sem muita preocupação com a confidencialidade, a integridade, a disponibilidade e a autenticidade.

É imprescindível garantir que essa quantidade enorme de informações que trafegam e são armazenadas em volumes crescentes e imensuráveis esteja segura e disponível.

À semelhança do que ocorre em qualquer novo espaço aberto e pouco regulado no mundo físico, pessoas mal-intencionadas buscam obter vantagens ilícitas ou socialmente consideradas inaceitáveis explorando a falta de regras.

Assim ocorre na Internet, ou melhor, no chamado *espaço cibernético,* em que pessoas e grupos, acobertados pela distância e pelo anonimato, tentam burlar a segurança dos equipamentos e dos sistemas informatizados de qualquer empresa, instituição, governo ou indivíduo e extrair benefícios indevidos da exploração desse bem chamado informação.

A segurança da informação, definida como uma "área de conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2003), surge como nova especialidade, responsável por assegurar que as informações, sejam elas de caráter pessoal, institucional ou corporativo, estejam preservadas.

Como a informação é um bem incorpóreo, intangível e volátil, os ativos de informação tornam-se naturalmente os principais focos de atenção da segurança da informação. São exemplos de ativos de informação: os meios de armazenamento,

transmissão e processamento da informação; os equipamentos necessários a isso, como computadores, equipamentos de comunicações e de interconexão; os sistemas utilizados para tal; os locais onde se encontram esses meios; e também os recursos humanos.

2.5 OS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Para ser utilizada, a informação necessita de três características fundamentais: a integridade, a disponibilidade e a confidencialidade, características que devem ser preservadas, pois são tidas como princípios da segurança da informação. “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT NBR ISO/IEC 27002:2005).

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados. (ABNT NBR ISO/IEC 27001:2013).

A **integridade** é a garantia da exatidão e completeza da informação e dos métodos de processamento (ABNT NBR ISO/IEC 27002:2005).

Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente.

Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original. Contribuem para a perda da integridade: as inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

A **disponibilidade** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (ABNT NBR ISO/IEC 27002:2005).

Ocorre a quebra da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que fizer necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

A **confidencialidade** é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (ABNT NBR ISO/IEC 27002:2005).

Ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

2.6 PORQUE SE PREOCUPAR COM SEGURANÇA DA INFORMAÇÃO

A ABNT NBR ISO/IEC 27002 (2005, pag. x) traz que:

> As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, ***hackers*** e ataques de ***denial of service*** estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), entidade civil, sem fins lucrativos, que desde dezembro de 2005 implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

Estas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos Grupos de Segurança e Resposta a Incidentes de Rede (CSIRTs) no Brasil.

Esses grupos espalhados pelo Brasil, através dos profissionais que atuam nas áreas governamentais, provedores de acesso ou de informações, de representantes de usuários e da comunidade acadêmica, reportam ao CERT.br todos os incidentes de rede que ocorrem sob suas redes, alimentando assim as estatísticas que serão mostradas a seguir.

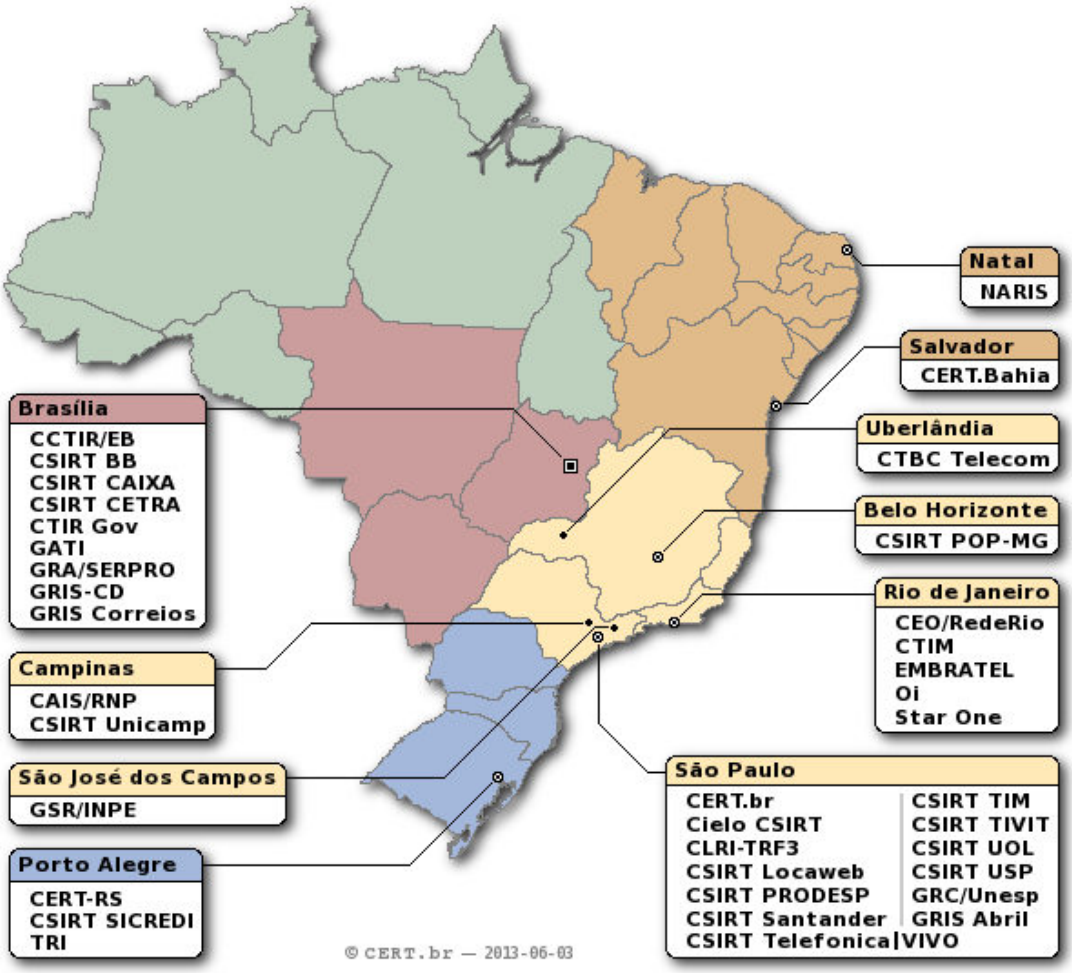


FIGURA 1 – LOCALIZAÇÃO DOS GRUPOS DE SEGURANÇA E RESPOSTA A INCIDENTES DE REDE (CSIRTS) NO BRASIL
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.

Antes de se tratar os pontos que devem ser defendidos em uma rede, regras e políticas de segurança a serem aplicadas, será analisado o que se passa na Internet segundo as estatísticas do CERT.br. Os dados a seguir referem-se até o dia 30 de junho de 2013.

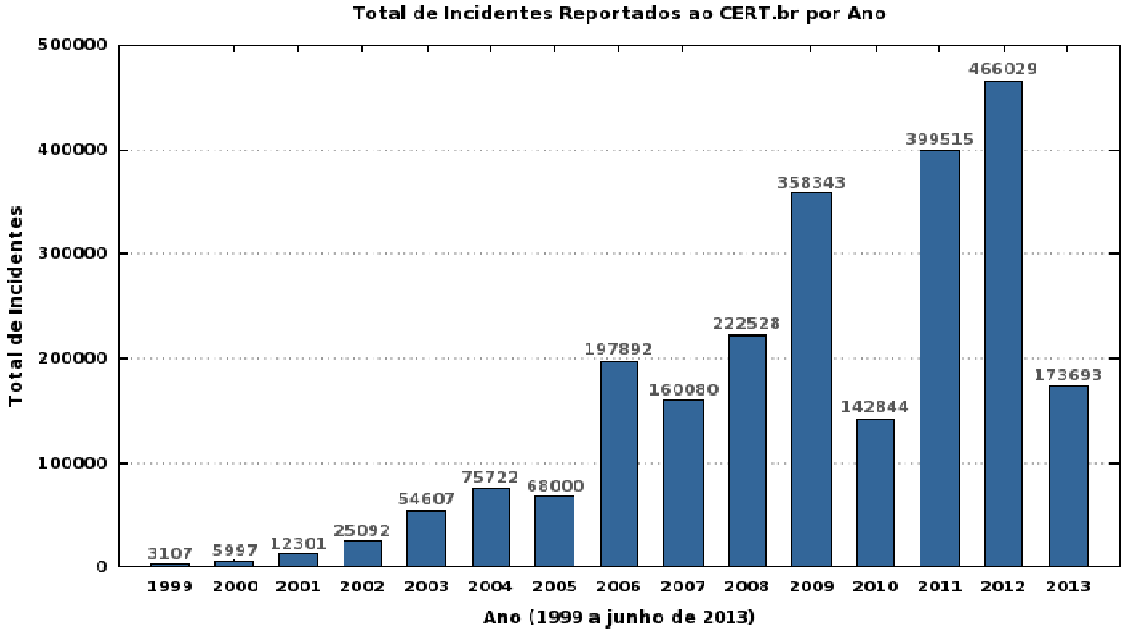
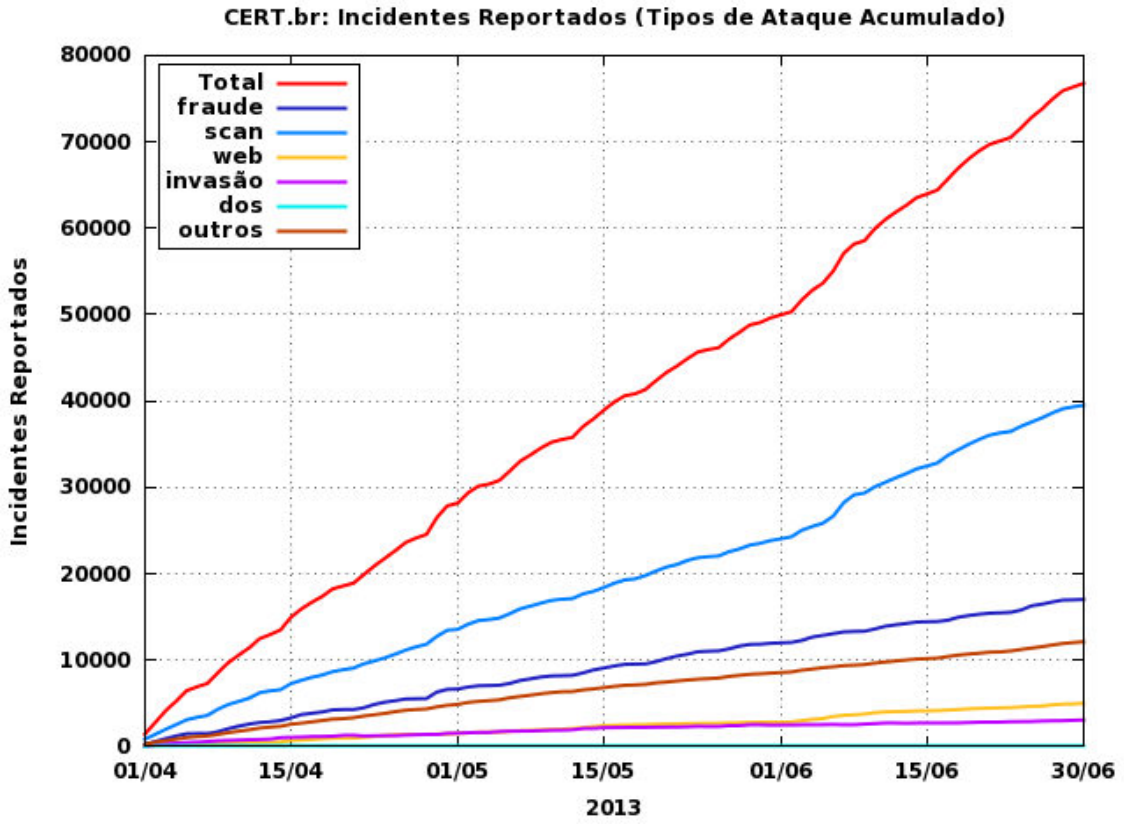


FIGURA 2 – TOTAL DE INCIDENTES REPORTADOS AO CERT.BR
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.



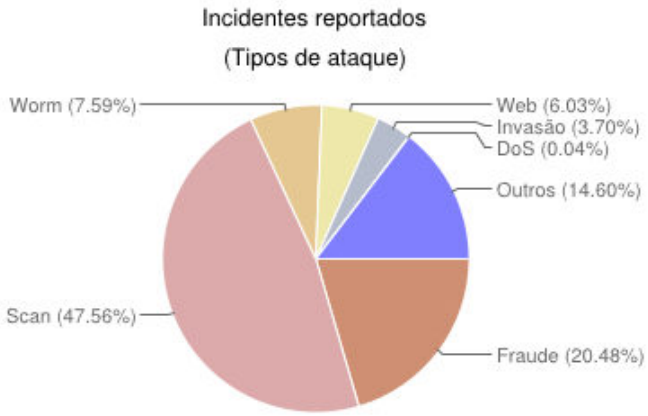


FIGURA 3 – INCIDENTES REPORTADOS AO CERT.BR POR TIPOS DE ATAQUE
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.

Legenda:

- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

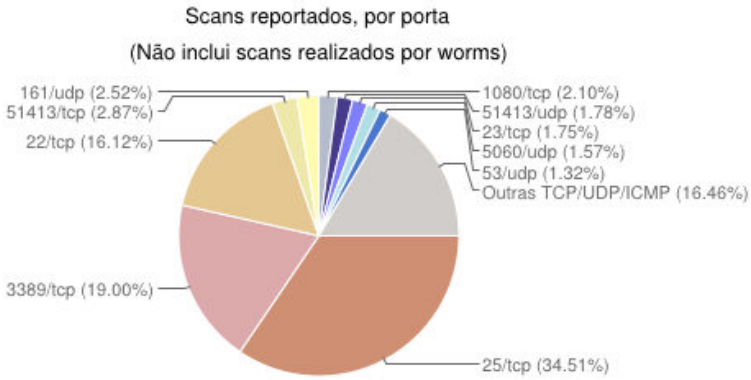


FIGURA 4 – *SCANS* REPORTADOS POR PORTA
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.

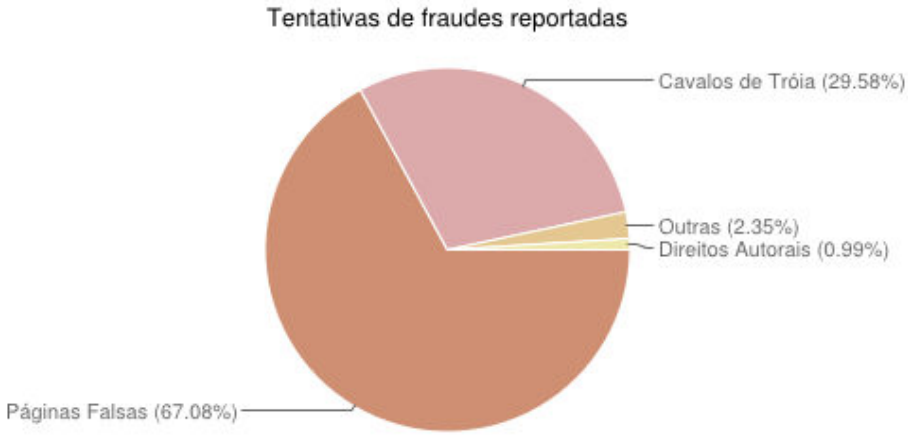


FIGURA 5 – TENTATIVAS DE FRAUDES REPORTADAS
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.

Legenda:

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
- **Outras**: Outras tentativas de fraude.

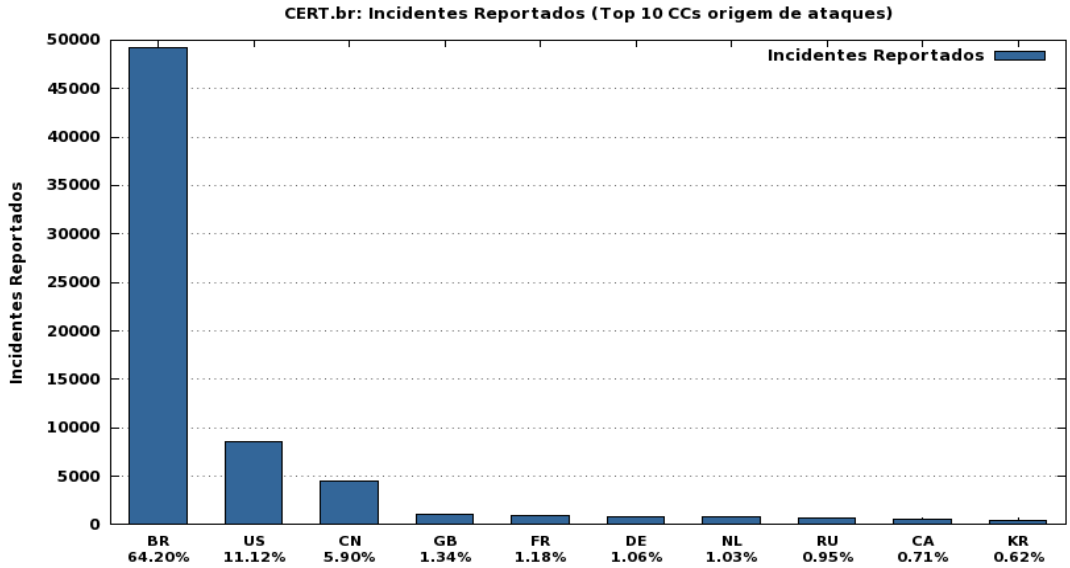


FIGURA 6 – ORIGEM DOS ATAQUES REPORTADOS (PAÍSES)
FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL.

Legenda:

BR: Brasil; **US**: Estados Unidos; **CN**: China; **GB**: Grâ-Bretanha; **FR**: França; **DE**: Alemanha; **NL**: Holanda; **RU**: Rússia; **CA**: Canadá; **KR**: Coréia do Sul

2.7 FATORES QUE COMPROMETEM A SEGURANÇA DE UMA REDE

A segurança absoluta ou perfeita é uma utopia. Convém, portanto, que se evidencie que as ameaças só se concretizam, ou seja, só produzem efeitos nocivos, quando exploram ou encontram condições favoráveis – vulnerabilidades[1]. “por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos” (Cartilha de Segurança para Internet, pág. 102). Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

1 vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

Quando se fala de fatores que possam comprometer a segurança de uma rede deve-se levar em consideração as particularidades de cada Instituição/Organização, ou seja, cada caso é um caso.

Alguns fatores gerais podem ser tratados igualmente em todos os casos, o que é chamado neste trabalho de segurança em camadas, sendo física, lógica e humana, independente da arquitetura organizacional da Instituição/Organização a qual pertence à estrutura de rede.

A ABNT NBR ISO/IEC 27002:2005 traz técnicas de segurança e práticas para a gestão de segurança da informação em vários níveis, desde a segurança física, lógica e de pessoal, para tanto, será utilizada esta NBR para elencar alguns fatores, que nem sempre são levados em consideração, aos quais os profissionais da área de redes devem estar atentos ao planejar a segurança dos dados de uma rede. Cabe salientar que este tópico não detalhará todos os pontos citados na referida Norma, haja vista que são muitos os itens de segurança tratados na documentação em questão, dessa forma, serão abordados os fatores principais para definições de pontos críticos para a estruturação de uma rede segura.

2.7.1 Segurança em camada física

As vulnerabilidades físicas dizem respeito aos ambientes em que estão sendo processadas ou gerenciadas as informações. Podem ser: instalações inadequadas, ausência de recursos para combate a incêndio, disposição desordenada dos cabos de energia e de rede, não identificação de pessoas e locais, portas e/ou janelas destrancadas, acesso desprotegido às salas de servidores, material inflamável utilizado na construção e no acabamento, paredes suscetíveis a roubo de equipamentos.

Quanto à vulnerabilidade de *hardware,* os possíveis defeitos de fabricação ou configuração dos equipamentos que podem permitir o ataque ou a alteração dos mesmos, a falta de configuração de suporte ou equipamentos de contingência, *patches* ausentes, *firmware* desatualizado, até sistemas mal configurados.

Os meios de armazenamento são todos os suportes físicos ou magnéticos utilizados para armazenar as informações, tais como: CD/DVD ROM, fita magnética,

discos rígidos dos servidores e dos bancos de dados, as suas vulnerabilidades advêm de prazo de validade e expiração, defeito de fabricação, utilização incorreta, local de armazenamento em áreas insalubres ou com alto nível de umidade, magnetismo ou estática, mofo, e até mesmo a falta de uma política de *backup*.

- Estrutura Física. Objetivo: Prevenir perda, dano ou comprometimento dos ativos, e a interrupção das atividades do negócio, onde equipamentos sejam fisicamente protegidos contra ameaças à sua segurança e perigos ambientais. A proteção é necessária para reduzir o risco de acessos não autorizados a dados e para proteção contra perda ou dano, que podem exigir controle especial para salvaguardar as instalações de suporte, como o fornecimento de energia elétrica e cabeamento.

- Localização. Objetivo: Prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização, aos recursos e instalações de processamento de informações críticas ou sensíveis do negócio, os quais devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso com o intuito de minimizar o risco de acesso não autorizado ou danos a papéis, mídias, recursos e instalações de processamento de informações.

- Energia Elétrica. Objetivo: Convém que os equipamentos sejam protegidos contra falhas de energia e outras anomalias na alimentação elétrica, através do fornecimento de energia apropriado em conformidade com as especificações do fabricante do equipamento. Algumas opções para alcançar a continuidade do fornecimento elétrico incluem a alimentação múltipla para evitar um único ponto de falha no fornecimento elétrico. Ainda, o uso de *no-break* (*Uninterruptable Power Supply – UPS*) em equipamentos que suportem atividades críticas para permitir o encerramento ordenado ou a continuidade do processamento. Convém que os planos de contingência contenham ações a serem tomadas em casos de falha no *no-break*.

- Cabeamento: Objetivo: Convém que o cabeamento elétrico e de telecomunicação que transmitem dados ou suporta os serviços de informação seja

protegido contra interceptação ou dano, de forma que as linhas elétricas e de telecomunicações das instalações de processamento da informação sejam subterrâneas, onde possível, ou sejam submetidas à proteção alternativa adequada. O cabeamento da rede seja protegido contra interceptações não autorizadas ou danos, por exemplo, pelo uso de conduítes ou evitando a sua instalação através de áreas públicas e que os cabos elétricos fiquem separados dos cabos de comunicação para prevenir interferências, através da sua instalação utilizando-se conduítes blindados e salas ou gabinetes trancados nos pontos de inspeção e terminais, além do uso de rotas e meios de transmissão alternativos. Em casos de ligação de instalações distantes é aconselhável a utilização de cabeamento de fibra óptica.

- Inventario de Ativos de *Hardware*. Objetivo: alcançar e manter a proteção adequada dos ativos da organização.

Manter os ativos (*hardware*) inventariados e que tenham um proprietário (usuário) responsável pela sua guarda e controle facilita o trabalho da equipe de TI, haja vista o fato de se saber quem é o responsável direto pela utilização de determinado equipamento e até mesmo, se necessário, atribuir responsabilidades sobre danos, alterações no hardware do terminal e tentativas de acesso indevidas partindo daquele equipamento.

Ainda neste quesito, temos o inventário de *software*, ou seja, sistema operacional, sistemas e ferramentas instaladas nos terminais de cada usuário, permitindo dessa forma uma varredura à procura de *softwares* não licenciados ou não autorizados no parque de máquinas da Organização/Instituição.

2.7.2 Segurança em camada lógica

Vulnerabilidades de *software* são constituídas por todos os aplicativos que possuem pontos fracos que permitem acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede, como os encontrados em configurações e instalações indevidas de programas, inclusive no uso de *e-mail,* que permitem a execução de códigos maliciosos.

- Firewall. Objetivo: Prevenir acessos não autorizados aos sistemas de informação, estabelecidos para controlar a concessão de direitos de acesso aos sistemas de informação e serviços, cobrindo todos os estágios do ciclo de vida de acesso de um usuário, do registro inicial de novos usuários até o registro final de exclusão dos usuários que não mais necessitam ter acesso aos sistemas de informação e serviços, com atenção especial, onde apropriado, à necessidade de controlar a concessão de direitos de acesso privilegiados, os quais permitem aos usuários sobrepor os controles do sistema.

Especificação de regras para controle de acesso, diferenciando as regras que sempre devem ser cumpridas das regras opcionais ou condicionais, estabelecendo regras baseadas na premissa “Tudo deve ser proibido a menos que expressamente permitido“, ao invés da regra “Tudo é permitido a menos que expressamente proibido” e a diferenciação entre regras que requerem aprovação do administrador ou outro funcionário antes da liberação e aquelas que não necessitam de tal aprovação.

- Segregação de Redes: grupos de serviços da informação, usuários e sistemas de informação segregados em redes. Método utilizado para controlar a segurança da informação, no caso de grandes redes, dividindo em diferentes domínios de redes lógicas, por exemplo, os domínios de redes internas de uma organização e domínios externos de uma rede, cada qual protegido por um perímetro de segurança definido, com um conjunto de controles aplicados a sistemas publicamente acessíveis, redes internas e ativos críticos, diferentes dentro de cada um dos domínios.

Tal perímetro de rede pode ser implementado instalando um *gateway* seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informações, configurado para filtrar tráfico e bloquear acesso não autorizado conforme a política de controle de acesso da Organização/Instituição. A esse exemplo de *gateway* é o que geralmente chamamos de *firewall*.

O *gateway* de segurança pode ser usado ainda para validar endereços de origem e destino nos pontos de controle de rede interna ou externa se um *proxy* for empregado.

Redes podem ser segregadas usando também a funcionalidade de dispositivo de rede, por exemplo, IP *switching*, onde domínios separados podem ser

implementados controlando os fluxos de dados de rede, do mesmo modo que listas de controle de acesso.

- Registro do Usuário: A existência de um procedimento formal de registro e cancelamento de usuário para obtenção de acesso a todos os sistemas de informação e serviços multiusuários, com acesso controlado através da utilização de identificador de usuário (ID) único, de forma que cada usuário possa ser identificado e responsabilizado por suas ações. Aprovação do direito de acesso pelo gestor pode também ser necessária, assim como a verificação de que o nível de acesso concedido está adequado aos propósitos do negócio e está consistente com a política de segurança da organização, por exemplo, por meio da entrega de um documento escrito aos usuários sobre seus direitos de acesso e até mesmo a inclusão de cláusulas especificando as sanções em caso de tentativa de acesso não autorizado, no qual o usuário assina, indicando que está ciente das condições de seus direitos de acesso. Há a necessidade de manutenção de um registro formal de todas as pessoas cadastradas para usar os serviços, bem como, a remoção imediata dos direitos de acesso dos usuários que tenham mudado de função ou deixado a Organização/Instituição.

O uso inadequado de privilégios em sistemas é freqüentemente apontado como o maior fator de vulnerabilidade de sistemas.

- Identificação e autenticação do usuário. Objetivo: prevenir acesso não autorizado aos sistemas operacionais.

Todos os usuários do sistema devem possuir um identificador único (ID de usuário) para uso pessoal e exclusivo, estendido inclusive para o pessoal de suporte técnico e administradores da rede, o qual será utilizado para rastrear as atividades do indivíduo na rede.

A utilização de senha é uma maneira muito comum de se prover identificação e autenticação, para isso, a escolha da senha deve ser primordial, ou seja, utilizar-se de letras, números e caracteres, tornando-a a mais segura e forte possível.

Os recursos de segurança da informação devem ser usados para restringir o acesso aos sistemas operacionais para usuários autorizados, conforme a política de controle de acesso definida, através do registro das tentativas de autenticação no

sistema com sucesso ou falha. A restrição do tempo de conexão dos usuários, quando ociosos.

A inserção de limite para o número de tentativas de entradas no sistema (*log-on*) sem sucesso é de grande utilidade no monitoramento de tentativas de acesso indevido e até mesmos para se averiguar um possível usuário, não autorizado, utilizando a senha de outra pessoa.

A obrigatoriedade na troca de senhas, a cada espaço de tempo estipulado pelo Plano de Segurança da Informação (PSI), bem como a não reutilização de senhas, através de um registro de senhas anteriormente utilizadas pelos usuários.

- Antivírus. Objetivo: Proteger a integridade do *software* e da informação.

É necessário que se adotem precauções para prevenir e detectar a introdução de *software* malicioso. Os ambientes de processamento da informação são vulneráveis à introdução de *software* malicioso, tais como vírus de computador, cavalos de Tróia e outros. A indispensável conscientização dos usuários sobre os perigos do uso de *software* sem licença ou malicioso, onde os gestores devem implantar controles especiais para detecção e prevenção de vírus nos computadores. Há ainda, a necessidade de uma política formal exigindo conformidade com as licenças de uso do *software* e proibindo o uso de *software* não autorizado, contra os riscos associados à importação de arquivos e *software*, seja de redes externas ou por qualquer outro meio, indicando quais as medidas preventivas que devem ser adotadas, bem como, a investigação formal quando da presença de qualquer arquivo ou atualização não autorizada. A adoção da prática de verificação, antes do uso, da existência de vírus em qualquer arquivo em meio magnético de origem desconhecida ou não autorizada, e em qualquer arquivo recebido a partir de redes não confiáveis, e em qualquer arquivo recebido através de correio eletrônico ou importado (*download*). Planos de contingência adequados para a recuperação em caso de ataques por vírus, incluindo os procedimentos necessários para salva e recuperação dos dados e *software*. Esses controles são especialmente importantes para servidores de arquivo de rede que suportem um grande número de estações de trabalho.

- Backup. Convém que os equipamentos de contingência e meios magnéticos de reserva (*Backup*), sejam realizados regularmente e guardados a uma

distância segura da instalação principal, para evitar que desastres neste local os afetem. A adoção de recursos e instalações alternativos sejam disponibilizados de forma a garantir que todos os dados e sistemas aplicativos essenciais ao negócio possam ser recuperados após um desastre ou problemas em mídias. Testes regulares dos *backups* de sistemas individuais devem ser feitos, visando garantir que satisfaçam os requisitos dos planos de continuidade de negócios, como também, a adoção de um nível mínimo de cópias de segurança, juntamente com o controle consistente e atualizado dessas cópias e com a documentação dos procedimentos de recuperação, os quais devem ser mantidos em local remoto, com adequação física e ambiental compatível com os padrões utilizados no ambiente principal. Especificação do período de retenção para informações essenciais ao negócio e também qualquer requerimento para o arquivamento de cópias de segurança com retenção permanente.

- Serviços de Rede. Os serviços de rede incluem o fornecimento de conexões, serviços de rede privados, soluções de segurança de rede gerenciadas por *firewalls* e sistemas de detecção de intrusos. As definições de segurança para serviços específicos, como características de segurança, níveis de serviço e requisitos de gerenciamento devem ser identificados e incluídos no Plano de Segurança da Informação (PSI).

Dentre as funcionalidades de segurança de serviços de rede estão às tecnologias aplicadas para segurança de serviços de redes como autenticação, encriptação e controles de conexões de rede, a adoção de parâmetros técnicos para uma conexão segura com os serviços de rede e procedimentos visando restringir o acesso aos serviços de rede ou aplicações onde for necessário.

- Monitoramento. Objetivo: detectar atividades não autorizadas de processamento de informação.

Os serviços de rede devem ser monitorados e eventos de segurança registrados (*log*). Os registros (*log)* de operador e de falhas devem ser utilizados para assegurar que os problemas de sistemas de informação sejam identificados, logicamente que a Organização/Instituição deve atentar para que seus procedimentos estejam de acordo com os requisitos legais relevantes aplicáveis as suas atividades de registro e monitoramento. O monitoramento do sistema deve ser

utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

Os registros (*log*) de auditoria produzidos devem ser mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso. Para uma eficiente auditoria, os registros (*log*) devem manter alguns itens, tais como: identificação dos usuários, datas, horários de entrada (*log-on*) e saída (*log-off*) do sistema, identificação do terminal, registro das tentativas de acesso ao sistemas aceitas e rejeitadas, possíveis alterações no sistema, uso de privilégios, aplicações e utilitários do sistema utilizados, arquivos acessados e tipo de acesso, endereços.

Os registros (log) gerados pelas ações dos administradores do sistema não devem ser excluídos, bem como, os referidos administradores não devem ter permissão para exclusão ou desativação desses registros.

Um fator de extrema importância no trabalho de monitoramento é que todos os relógios dos sistemas de processamento de informações sejam sincronizados com uma fonte de tempo precisa, visando assegurar a exatidão dos registros (*log*) de auditoria, que podem ser requeridos para investigações ou como evidência em casos legais ou disciplinares, evitando assim causar danos à credibilidade das evidências. Pode ser utilizados, por exemplo, o tempo coordenado universal (*Coordinated Universal Time – UTC*), ou um padrão de tempo local.

Logs são essenciais para notificação de incidentes, pois permitem que diversas informações importantes sejam detectadas, como por exemplo: a data e o horário em que uma determinada atividade ocorreu, o fuso horário do *log*, o endereço IP de origem da atividade, as portas envolvidas e o protocolo utilizado no ataque (TCP, UDP, ICMP, etc.), os dados completos que foram enviados para o computador ou rede e o resultado da atividade (se ela ocorreu com sucesso ou não).

2.7.3 Segurança em camada humana

As vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior fragilidade.

Sua origem pode ser: falta de capacitação específica para a execução das atividades inerentes às funções de cada um, falta de consciência de segurança diante das atividades de rotina, erros, omissões, descontentamento, desleixo na elaboração e segredo de senhas no ambiente de trabalho, não utilização de criptografia na comunicação de informações de elevada importância, quando possuídas na empresa.

As vulnerabilidades de origem organizacional dizem respeito a políticas, planos e procedimentos, e a tudo mais que possa constituir a infraestrutura de controle da organização e que não seja enquadrado em outras classificações. Podem ser: ausência de políticas de segurança e treinamento; falhas ou ausência de processos, procedimentos e rotinas; falta de planos de contingência, recuperação de desastres e de continuidade.

- Segurança dos Recursos Humanos. Não pode ser esquecido que, assim como as informações é um grande patrimônio para a Organização/Instituição, o fator recursos humanos tem vital importância e peso também. Manter os recursos humanos conscientes das ameaças que os mesmos podem vir a sofrer por elementos adversos ao seu meio de trabalho, na busca por informações que possam permitir acesso a dados vitais da Organização/Instituição é de vital importância, dar-lhes conhecimento das técnicas mais utilizadas, como por exemplo, a engenharia social, por pessoas mal intencionadas além de garantir uma maior segurança para a empresa, também é extremamente útil para a vida virtual particular do colaborador.

Em todo o caso, é preciso estar consciente de que o Engenheiro Social atua baseado em três aspectos, a saber: motivação pessoal (desafio, ganância ou sentimento de aventura), falta de controle da organização (vulnerabilidades) e oportunidade (exploração das vulnerabilidades existentes). Dos três aspectos, o único que não podemos controlar é o primeiro deles, a motivação, por ser estritamente pessoal. Nos demais, temos obrigação de atuar, dificultando ao máximo a ação dos invasores.

- Documentação de Procedimentos. Manter registro das atividades do pessoal de operação, no qual constem horário de início e fim dos processamentos, erros e ações corretivas adotadas nos processamentos, confirmação do correto tratamento dos arquivos de dados e dos resultados gerados nos processamentos e

a identificação de quem está efetuando a operação colabora para análise e melhoria nos processos durante a tomada de decisões quanto à correção de problemas e falhas nos sistemas.

Os registros de atividades dos operadores devem ser submetidos a uma auditoria regular e independente, em conformidade com os procedimentos operacionais.

- **Conscientização, educação e treinamento**. Todos os funcionários/colaboradores da Organização/Instituição devem ser conscientizados, receber treinamentos apropriados, bem como atualização regulares das políticas e procedimentos organizacionais no que diz respeito ao uso dos recursos tecnológicos utilizados por cada um destes, as consequências de suas ações e o que pode vir a ocorrer em caso de falhas causadas por uma possível atitude indevida.

2.8 SERVIÇOS DE REDE EM *SOFTWARE* LIVRE

Uma rede local baseada em *software* livre é um conjunto formado por sistema operacional mais programas que fornecem diversas funcionalidades para essa rede.

Aliar sistema operacional, aplicações e ferramentas para gerenciamento de redes a um baixo custo pode ser o sonho de qualquer administrador de rede e gerentes de Organizações/Instituições sejam elas públicas ou privadas.

Neste tópico, serão abordados apenas alguns serviços, em *software* livre, que podem rodar em uma rede e atender as principais necessidades de seus usuários. Deixando claro que não há somente estas ferramentas disponíveis, cabe aos gerentes e equipe de TI buscarem, dentro do mundo do *software* livre, aplicações que atendam às suas necessidades específicas.

2.8.1 *Software* livre

Quando se fala em *software* livre, está se falando de uma categoria específica de programas ou sistemas de computador. Categoria esta também conhecida pela sigla FOSS (*Free Open Source Software*), ou OSS (*Open Source Software*). Embora já bastante utilizado, ainda se observa, tanto por parte de pessoas, como por parte de empresas ou instituições dúvidas e/ou questionamentos em relação ao *software* livre.

Por "*software* livre" entende-se aquele *software* que respeita a liberdade e senso de comunidade dos usuários. **Os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o *software***. Com essas liberdades, os usuários (tanto individualmente quanto coletivamente) controlam o programa e o que ele faz por eles. (*Software* Livre – Projeto GNU, 2013).

Quando os usuários não controlam o programa, o programa controla os usuários. O desenvolvedor controla o programa e, por meio dele, controla os usuários.

Richard Stallman, fundador da "*Free Software Foundation (FSF)*", é citado por Mendonça (2009, p. 20), "que *software* livre deve respeitar quatro liberdades básicas, que são: usar, estudar, redistribuir e modificar", ou seja:

- Liberdade de execução para qualquer fim e por qualquer pessoa física ou jurídica (usar);

- Liberdade para que o código seja analisado e adaptado às necessidades locais (estudar);

- Liberdade para repassar cópias para outros, ajudando assim outras pessoas/instituições (redistribuir); e

- Liberdade para que seja aperfeiçoado e as modificações disponibilizadas, para que toda a comunidade seja beneficiada (modificar).

A principal diferença entre *software* livre e *software* gratuito, portanto, consiste no fato de que este último não pode ser estudado e nem modificado, pois o código fonte fica em poder do autor ou da instituição que o desenvolveu.

2.8.1.1 Licenças GPL e BSD

GNU - *General Public License* (Licença Pública Geral), **GNU GPL** ou simplesmente **GPL**, é a designação da licença para *software* livre idealizada por Richard Stallman no final da década de 1980, no âmbito do projeto GNU da *Free Software Foundation* (FSF). A GPL é a licença com maior utilização por parte de projetos de *software* livre, em grande parte devido à sua adoção para o Linux.

A GPL permite que os programas sejam distribuídos e reaproveitados, mantendo, porém, os direitos do autor por forma a não permitir que essa informação seja usada de uma maneira que limite as liberdades originais. A licença não permite, por exemplo, que o código seja apoderado por outra pessoa, ou que sejam impostos sobre ele restrições que impeçam que seja distribuído da mesma maneira que foi adquirido. Assim como em outras licenças livres, na GPL não é necessário o acordo do usuário com a licença, ou seja, o usuário não precisa concordar com a GPL para utilizar um programa GPL, ao contrário dos programas proprietários, como o Windows. Por esse motivo, em um programa livre não faz sentido haver um botão de "*I agree*". Quem precisa seguir a licença, é quem vai desenvolver, distribuir, vender ou alterar.

A licença **BSD** - ***Berkely Software Distribution*** (Distribuição de *Software* de Berkeley) impõe poucas restrições quando comparada aquelas impostas por outras licenças, como a GNU *General Public License* ou mesmo as restrições padrão determinadas pelo *copyright*, colocando-a relativamente próxima do domínio público. De fato, a licença BSD tem sido chamada de *copycenter*, ou "centro de cópias", em comparação com o *copyright* padrão e o *copyleft* da licença GPL: "Leve até o *copycenter* e faça quantas cópias quiser".

A licença BSD permite que o *software* distribuído sob a licença, seja incorporado a produtos proprietários. Trabalhos baseados no material podem até ser liberados com licença proprietária. Alguns exemplos notáveis são: o uso de código do BSD (funções de rede de computadores) em produtos da Microsoft, e o uso de muitos componentes do FreeBSD no sistema Mac OS X da Apple Computer.

Também é possível que *softwares* sejam distribuídos pela licença BSD junto de outra licença, isto ocorreu em versões antigas do BSD Unix, que incluíam material proprietário da AT&T.

Na sua versão original, a licença BSD contém termos que a tornam incompatível com a licença GPL. Como elas estão entre as licenças mais utilizadas no mundo do *software* livre, a impossibilidade em combinar os seus componentes

tornou-se um grande problema para os autores destes *softwares*. Na revisão sofrida em 1999 a cláusula controversa foi retirada. Desde esta data, os autores estão livres para incorporar *softwares* BSD naqueles licenciados pela GPL.

2.8.2 Os serviços de rede

Serviços de rede é o que está disponível para ser acessado pelo usuário. No TCP/IP, cada serviço é associado a um número chamado porta que é onde o servidor espera pelas conexões dos computadores clientes. Uma porta de rede pode ser referenciada tanto pelo número como pelo nome do serviço.

A definição dos serviços que irão rodar na rede é um ponto a ser decidido em conjunto com colaboradores e gerentes, a fim de proporcional subsídios a equipe de TI quanto a melhor escolha das ferramentas que atenderão às necessidades da Instituição/Organização.

2.8.2.1 *Firewall*

Seguindo sua tradução literal, *Firewall* significa “parede corta fogo”. Essa analogia se explica por ele atuar literalmente como uma barreira contra incêndio e sua função na rede é a de controlar acessos tanto internos quanto externos. Segundo definido por Kurose (2010, p. 535):

> *Firewall* é uma combinação de *hardware* e *software* que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros. Um firewall permite que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra gerenciando o fluxo de tráfego de e para esses recursos. (KUROSE, 2010, p. 535)

Todo o tráfego de fora para dentro, e vice-versa, passa por um *firewall* o que é situado diretamente no limite entre a rede administrada e o resto da Internet. Alocar um *firewall* num único ponto de acesso à rede facilita o gerenciamento e a execução de uma política de acesso seguro.

Somente o tráfego autorizado, como definido pela política de segurança local poderá passar, dessa forma, todo o tráfego que entra e sai da rede institucional passa pelo *Firewall*.

O *Firewall* é um mecanismo conectado à rede, se não for projetado ou instalado adequadamente, pode ser comprometedor, oferecendo apenas uma falsa sensação de segurança.

Podemos classificar um *Firewall* em três categorias: filtros de pacote, filtros de estado e *gateways* de aplicação:

- Filtro de Pacotes - Primeira Geração: o modelo trata da avaliação de pacotes do conjunto de protocolos TCP/IP. Todo o tráfego que sai ou que entra na rede interna é analisado e ocorre a filtragem de pacotes, ou seja, é examinado cada datagrama e determinado se deve passar ou bloquear, baseado nas regras especificadas pelo administrador com base na política da Instituição/Organização. As filtragens são normalmente baseadas em endereço IP de origem e destino e no tráfego através da porta TCP ou UDP do serviço.

Ainda hoje, este tipo de tecnologia é adotada em equipamentos de rede para permitir configurações de acesso simples, as chamadas “listas de acesso”. O *ipchains* é um exemplo recente de *Firewall* que utiliza a tecnologia dessa geração. Hoje o *ipchains* foi substituído pelo *iptables* que é nativo do Linux e com maiores recursos.

Esta talvez seja a categoria mais utilizada de *Firewall*, não aplicar seus conceitos é deixar as portas abertas e permitir a livre circulação de pacotes não confiáveis por sua rede.

- Filtro de Estado – Segunda Geração: os filtros de estado rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem.

Pelo fato de o principal protocolo de transporte TCP orientar-se por uma tabela de estado nas conexões, os filtros de pacotes não eram suficientemente efetivos se não observassem estas características.

Neste tipo são aceitas todas as regras da primeira geração além das suas específicas:

- Restringir o tráfego para início de conexões (*NEW*);

- Restringir o tráfego de pacotes que não tenham sido iniciados a partir da rede protegida (*ESTABLISHED*);

- Restringir o tráfego de pacotes que não tenham número de sequência corretos (*RELATED*).

Também chamado *Firewall Statefull* armazena o estado das conexões e filtra com base nesse estado. Existem três estados para uma conexão: - *NEW*: novas conexões; - *ESTABLISHED*: conexões já estabelecidas, e – *RELATED*: conexões relacionadas a outras existentes.

- *Gateway* de Aplicação – Terceira Geração: também conhecidos como *Firewall* de Aplicação ou *Firewall Proxy*. O *Firewall* de *Proxy* trabalha recebendo o fluxo de conexão, tratando as requisições como se fosse uma aplicação e originando um novo pedido sob a responsabilidade do mesmo *Firewall* para o servidor de destino. A resposta para o pedido é recebida pelo *Firewall* e analisada antes de ser entregue para o solicitante original.

Os *gateways* de aplicação conectam as redes corporativas à Internet através de estações seguras rodando aplicativos especializados para tratar e filtrar os dados. Esses *gateways* ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber estes dados, acabam por esconder a identidade os usuários nestas requisições externas, oferecendo uma proteção adicional contra a ação de elementos mal intencionados.

A tecnologia atual permite que o custo de implementação seja bastante reduzido ao utilizar *CPUs* de alto desempenho e baixo custo, bem como sistemas operacionais abertos (Linux), porém, exige-se manutenção específica para assegurar que seja mantido um nível de segurança adequado, através da aplicação de correções e configuração adequada dos servidores.

2.8.2.2 Servidor de arquivos

Para este serviço vamos tratar em específico do Samba, que é um *software* servidor capaz de integrar máquinas Windows e Linux na rede.

O Samba é um "*software* servidor" para Linux que permite o gerenciamento e compartilhamento de recursos em redes formadas por computadores com o Windows. Assim, é possível usar o Linux como servidor de arquivos, servidor de

impressão, entre outros, como se a rede utilizasse servidores Windows. Isso é possível através do protocolo *Server Message Block* (SMB).

Com o servidor Samba, é possível compartilhar arquivos, compartilhar impressoras e controlar o acesso a determinados recursos de rede exatamente como em redes Microsoft. Mas neste caso, o sistema operacional utilizado é o Linux. O Samba é compatível com praticamente qualquer versão do Windows. Todo trabalho feito pelo Samba é provido de grande parcela de segurança, uma vez que há grande rigor nos controles dos recursos oferecidos. Nele ficam cadastrados todos os usuários da rede e cada usuário terá acesso ou não às pastas do servidor de acordo com a necessidade.

O Samba também possui uma lixeira onde todos os arquivos excluídos do servidor ficam armazenados, é gerado um registro por usuário de tudo o que este excluiu do servidor. O servidor Samba é gratuito, totalmente configurável, trazendo uma grande economia a curto e longo prazo em investimentos de TI.

Abaixo algumas funcionalidades importantes de aplicações do samba e seu conjunto de ferramentas:

- Controle de acesso aos recursos compartilhados no servidor através de diversos métodos (compartilhamento, usuário, domínio, servidor);
- Controle de acesso leitura/gravação por compartilhamento;
- Controle de acesso de leitura/gravação por usuário autenticado;
- Possibilidade de definir contas de "Convidados", que podem se conectar sem fornecer senha;
- Possibilidade de uso do banco de dados de senha do sistema *(/etc/passwd*), autenticação usando o arquivo de dados criptografados do samba, LDAP, PAM, etc;
- Permite ocultar o conteúdo de determinados diretórios que não quer que sejam exibidos ao usuário de forma fácil;
- O samba possibilita ajuste fino nas configurações de transmissão e recepção dos pacotes TCP/IP, como forma de garantir a melhor performance possível de acordo com suas instalações;
- Faz auditoria tanto dos acessos à pesquisa de nomes na rede como acesso a compartilhamentos. Entre os detalhes salvos estão a data de acesso, IP de origem, etc;

- Permite montar unidades mapeadas de sistemas Windows ou outros servidores Linux como um diretório no Linux;
- Permite a configuração de recursos simples através de programas de configuração gráficos, tanto via sistema, como via web;
- Com um pouco de conhecimento e habilidade de administração de sistemas Linux, é possível criar ambientes de auditoria e monitoração até monitoramento de acesso a compartilhamento em tempo real.

Mesmo sendo gratuito, existem milhares de programadores no mundo todo ajudando no desenvolvimento do Samba, isso permite que exista uma grande estrutura de suporte para todos os tipos de problemas que venham a ocorrer.

2.8.2.3 Atribuição de endereçamento IP

Uma das tarefas mais árduas no gerenciamento de uma rede é a atribuição e manutenção do endereçamento dos *hosts*. Em redes de pequeno porte configurar os equipamentos com IP fixo é comum e de certa maneira fácil, porém pode causar pequenos contratempos quando se fizer necessário a troca de *gateway* ou DNS. Para automatizar esta tarefa foi criado o protocolo DHCP que além de atribuir um endereço IP a um cliente solicitante, envia-lhe outros parâmetros como máscara de rede, endereços de roteadores, de servidores DNS entre outros dados ao equipamento cliente, a partir de uma solicitação deste, podendo inclusive ser controlado a faixa de endereços IP que serão distribuídos aos clientes.

DHCP significa Protocolo de Configuração Dinâmica de Máquinas. É usado para controlar parâmetros de rede vitais para as máquinas, com a ajuda de um servidor.

A configuração do DHCP *Server* envolve definições básicas válidas para o servidor e informações sobre a concessão de endereços IP para a rede local.

Uma forma de se melhorar a segurança é definindo que o servidor irá conceder sempre o mesmo IP para um determinado equipamento, baseado em seu endereço físico (MAC *Address*), ou seja, o endereço IP será atribuído ao *host* após a confirmação do MAC *Address*.

MAC ou *Media Access Control* é o endereço físico de uma interface de rede. É um endereço de 48 *bits*, representado em hexadecimal. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet. Este endereço é o utilizado na camada 2 do Modelo OSI.

2.8.2.4 Servidor de backup

Bacula é um *software* de *backup* de código aberto. Com ele é possível fazer *backups* remotamente de sistemas como Linux, FreeBSD, MacOS, NetBSD, Windows OpenBSD, HP-UX, Tru64, AIX e IRIX.

No Brasil, o Bacula tem despertado o interesse de diversas e grandes empresas, como por exemplo, o Serpro que já utiliza a ferramenta de acordo com o alinhamento estratégico de utilização de *Software* Livre.

Algumas das características do Bacula:

- Estrutura cliente/servidor (permitindo *backup* centralizado em uma máquina);
- Estrutura modular independente (diretor, cliente, *database*, administrador do console);
- GPL - economia de custos com licenças, conhecimento e possibilidade de customização da ferramenta;
- Portabilidade (módulos para diferentes sistemas operacionais);
- Infinidade de recursos para a customização de *backups*;
- Funcionalidade que permite a execução de *scripts* (ou executáveis) antes/depois do início dos trabalhos de *backup*/*restore*, tanto no cliente quanto no servidor Bacula;
- Existência de ferramenta de operação via linha de comando ou GUI (inclusive, com diferentes interfaces web desenvolvidas pelas comunidades. Destaque: bacula-web – ferramenta de visibilidade gerencial, com gráficos, etc);
- Suporte a maioria dos dispositivos de *storage* do mercado (inclusive mídias ópticas);

- Funcionalidade customizável para o envio de mensagens de *log* dos trabalhos de *backup*/*restore* ou ainda instruções para o operador de *backup* (diferentes perfis).

2.8.2.5 Solução de Mensagem Instantânea Corporativa

Uma das opções, em *software* livre, é o servidor **Openfire** é um poderoso servidor de mensagem instantânea que utiliza o protocolo *Extensible Messaging and Presence Protocol* (XMPP), ou Protocolo Extensível de Mensagens e Presença que pode ser utilizado em sua rede local, com possibilidade de troca de arquivos entre os usuários.

O Openfire possui interface gráfica e pode ser instalado, por exemplo, em uma versão Linux Ubuntu. No lado do cliente é instalada outra ferramenta, o **Spark**, também em *software* livre.

O Openfire tem uma gama imensa de recursos, um dos mais interessantes é o uso de *plugins*, que permitem estender as funcionalidades do servidor. Existe quase uma dezena de *plugins* disponíveis (e outros que já estão em desenvolvimento), como por exemplo, o SIP Phone Plugin, que provê a comunicação dos usuários com contas VOIP.

Algumas características do servidor Openfire com cliente de mensagens Spark:

- Ferramenta de mensagem instantânea corporativa interna;
- Todas as conversas são gravadas e pode ser pesquisado por usuário ou palavra chave;
- Mostra o tempo de duração de cada conversa;
- Pode ser acessado via web nas máquinas que não tem o Spark Instalado;
- Existe a opção de enviar mensagens em massa para comunicados;
- Quem utiliza Spark somente poderá se comunicar com contatos internos, não consegue adicionar contatos externos (melhora a produtividade);
- Área administrativa via web em português e intuitiva onde podem ser gerenciados os grupos e usuários.

2.8.2.6 Repositório local de atualizações

Em uma rede quando existe um parque de máquinas que utiliza o mesmo Sistema Operacional (SO), é comum em determinado momento que este SO necessite de atualizações, havendo a necessidade de buscar na Internet essas atualizações. A questão é o quanto esse acesso a Internet vai comprometer o desempenho da rede quando várias máquinas clientes fazem requisições para buscar informações que são comuns para todas elas.

Esse problema pode ser corrigido através de um repositório local para aliviar nossa banda de Internet. Podemos utilizar um repositório local da mesma forma que os repositórios localizados em ftps e *mirrors* das diversas versões de Linux existentes, e ao invés dos computadores da rede ir buscar pacotes na Internet buscará na rede local.

O **apt-cacher** é um programa para criar repositórios locais de atualizações sob demanda. Ou seja, configura-se o servidor e coloca os clientes de uma rede local apontando para os canais de *software* (repositórios) desse servidor. Assim, quando uma máquina cliente solicita um pacote, o apt-cacher verifica se ele já existe no servidor, caso exista ele baixa do repositório para a máquina cliente solicitante, caso não existe, ele baixa o pacote primeiro para o servidor (repositório) e depois copia para a máquina cliente. Isso evita que diversas máquinas em uma rede baixem os mesmos pacotes, economizando assim tempo e banda de conexão.

Um ponto interessante do apt-cacher é que não há necessidade de se instalar qualquer pacote ou aplicativo no lado do cliente, apenas apontar para o endereço do servidor apt-cacher.

2.8.2.7 Antivirus para Linux

Na maior parte, o Linux é idealizado de uma maneira que dificulta os vírus de rodarem. E também, por existirem mais PC's com Windows, é mais vantajoso escrever vírus para a plataforma Windows. No entanto, existem muitas razões para se querer ter um localizador de vírus instalado no seu PC com Linux:

- Para localizá-los na partição/drive onde está instalado o Windows;
- Para localizá-los em máquinas com Windows em uma rede;
- Para localizá-los em arquivos que pretende mandar para outras pessoas;
- Para localizá-los em e-mails que você vai mandar para outras pessoas.

Segurança é hoje uma questão bastante debatida no mundo, principalmente com relação ao ponto comum: manter todas as informações seguras é primordial.

Mas do que adianta ter senhas fortes, sistemas de segurança complexos se o próprio sistema operacional está comprometido?

Muitos usuários acham que por usarem Linux não tem que se preocupar com isso. Linux também pega vírus.

Existe uma lenda no mundo livre há muito tempo que diz que vírus, no Linux, é conto de fadas. Essa lenda é isso, só uma lenda. Existem sim vírus para sistemas operacionais baseados no *Kernel* Linux. Se não existissem vírus para Linux, não haveria tanta preocupação com servidores, afinal de contas, eles estariam sempre seguros.

O *Android*, sistema operacional móvel da Google, é hoje um dos sistemas operacionais móveis mais afetados por *malwares* do mundo! E ele é Linux.

Já quando se olha para *desktops* Linux, realmente, há mais segurança. Mas isso não quer dizer que se pode dormir tranquilo. O Linux é mais seguro, pois é *opensource*. *Hackers* ajudam a descobrir e concertar vulnerabilidades, mas só porque se tem uma quantidade de vírus menor do que o Windows, por exemplo, não quer dizer que é possível relaxar na segurança.

Um bom antivírus é fundamental em qualquer sistema operacional, e o Linux oferece algumas possibilidades interessantes, como o ClamAV no Ubuntu, um dos antivírus mais conhecidos para Linux, tanto para *desktops* quanto para servidores.

3 PROPOSTA DE UMA REDE BASEADA EM *SOFTWARE* LIVRE

Nenhum modelo de segurança pode resolver todos os problemas. Para burlar um *host* seguro ou um bom modelo de segurança de rede, um indivíduo pode simplesmente usar métodos físicos. Estes podem ser até derramar refrigerante em seus teclados, com o intuito de impossibilitar a continuidade de seus afazeres no local de trabalho e poder levar documentos de alta confidencialidade para casa.

Nenhum modelo de segurança pode cuidar dos problemas de gerenciamento. A segurança dos computadores não impedirá as pessoas de desperdiçarem tempo ou chatearem uns aos outros.

Nenhum modelo de segurança prevê proteção perfeita. Pode-se fazer com que as invasões sejam raras, breves, e com baixo ônus, mas não se pode esperar evitá-las completamente. Até mesmo os locais mais seguros e dedicados esperam ter um incidente de segurança em determinado momento.

A segurança pode não prevenir todos os incidentes, mas pode impedir que um incidente danifique seriamente, deixe fora de operação determinado sistema ou mesmo cause qualquer tipo de dano à imagem da Instituição/Organização. Às ameaças advém tanto de pessoas de fora da Instituição/Organização, quanto do seu público interno.

A proposta que será apresentada visa atender às necessidades de segurança, utilizando-se ferramentas em *software* livre que atendam aos requisitos da Instituição/Organização, sem a necessidade de grandes investimentos financeiros em equipamentos de alto valor, devido às dificuldades de investimento nessa área, o que muitas vezes faz parte da realidade de empresas/instituições.

3.1 CONSIDERAÇÕES INICIAIS

Um *Firewall* deve impossibilitar um usuário de sistema de enviar informações restritas de uma organização pela conexão de rede, o que é feito pelas regras de restrição de tráfego. Mas aquele mesmo usuário poderia copiar os dados em um HD externo, em uma *pendrive*, num CD/DVD, ou mesmo retirar um documento

fisicamente. Ameaças internas requerem segurança interna de rede, como segurança de *host* e educação de usuário.

A seguir, serão descritos algumas questões do Plano de Segurança da Informação, as quais não irão abrangir todos os pontos, pois deve-se ter em mente que cada Instituição/Organização tem suas peculiaridades e regras a serem definidas.

Apresentar e configurar algumas sugestões de ferramentas em *software* livre que podem ser utilizadas na implementação de uma rede.

3.2 A ESTRUTURAÇÃO DA REDE

A estrutura existente na qual foi desenvolvida esta proposta é composta por seis prédios de dois andares cada, com distâncias entre eles variando de 150 a 400 metros.

Para a interligação dos mesmos, foi utilizada fibra óptica monomodo, seguindo o padrão utilizado pela empresa prestadora do serviço acesso à Internet, lançada nos postes da rede elétrica existentes à retaguarda de cada uma das instalações.

A fibra óptica com o serviço de Internet está ancorada no prédio da administração onde foi instalado um equipamento próprio da empresa e deste é distribuído para um *Switch Gigabit Ethernet* 24 portas 10/100/1000 Mbps, não gerenciável, através de conversores de mídia 10/100/1000, porta RJ-45.

Nos demais prédios a fibra óptica chega até um Distribuidor Interno Óptico (DIO) de parede, também segue o padrão utilizado pela empresa prestadora do serviço de acesso à Internet, deste é distribuído para um *Switch Gigabit Ethernet* 24 portas 10/100/1000 Mbps, não gerenciável, através de conversores de mídia 10/100/1000, porta RJ-45.

Para a ligação *Switch* até os terminais dos usuários foi utilizado o cabeamento par trançado categoria 6 conectado à caixa externa com tomada para rede RJ45 fêmea na parede próxima ao terminal, concluindo com a conexão ao terminal através de um *Patch Cord* categoria 6 de 2,5 metros.

3.2.1 Dos servidores

Quando se fala em servidor, imagina-se uma máquina com alta capacidade de processamento, discos rígidos de grande capacidade e velocidade e uma grande quantidade de memória.

Existem vários tipos de servidores, como servidores web, de arquivos, de impressão, etc..., sendo que uma única máquina pode rodar simultaneamente vários serviços, dependendo apenas dos recursos de hardware e da carga de trabalho.

Uma das vantagens do uso do *software* livre (Linux) como sistema operacional para servidores é a sua baixa exigência em termos de configuração de hardware em relação a outros sistemas proprietários, o que favorece e muito quando se tem alguns PC's que não estão mais sendo utilizados.

3.2.2 Definição do serviço de acesso à Internet

Após realizadas as reuniões para levantamento dos acessos que as diversas Seções/Setores da Instituição/Organização necessitam, há a necessidade da escolha do serviço de acesso à Internet que melhor atenda ao grupo como um todo.

Uma das opções oferecidas foi a utilização de um serviço de Internet por meio de acesso em fibra óptica com garantia de banda, *upload* e *download* simétricos e endereçamento IP fixo que oferece alta disponibilidade e continuidade, livre de interferência, com cabeamento interligando os prédios 100% em fibra óptica e monitoramento 24 horas do serviço disponibilizado, podendo assim atender perfeitamente às necessidades da Instituição/Organização.

3.3 POLÍTICA DE SEGURANÇA

A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

É considerada como um importante mecanismo de segurança, tanto para as instituições como para os usuários, pois com ela é possível deixar claro o comportamento esperado de cada um. Desta forma, casos de mau comportamento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas e principalmente dar conhecimento aos usuários do que é permitido, evitando que um usuário venha a apresentar um mau comportamento e alegue desconhecer que sua atitude não é permitida dentro da Instituição/Organização.

3.3.1 Reuniões para planejamento da Política de Segurança da Informação

A política de segurança deve ser tratada em conformidade com políticas, regras, regulamentos e leis existentes, às quais a empresa já está sujeita.

A criação da política deve ser um esforço associado do pessoal técnico (TI e segurança), administrativo (gerência) e dos usuários, ou seja, todos os envolvidos pela política de segurança.

Assim, a Instituição/Organização pode promover uma reunião onde participam todos os envolvidos no processo para expor como seria criado o PSI da Instituição/Organização em questão.

Após a reunião, todas as Seções/Setores, através dos usuários e seus chefes diretos elaboraram um documento detalhado e encaminham a gerência, no qual constam as necessidades de ferramentas e de quais sites essas equipes precisam ter acesso para atender as necessidades de trabalho diário.

As solicitações dos diversos setores da Instituição/Organização devem ser analisadas, entre os grupos envolvidos, e após o aval da gerência, repassadas para a equipe de TI para que a mesma tome os procedimentos necessários para atender as solicitações e mantenha em arquivo todos os documentos encaminhados pelas Seções/Setores para acompanhamento.

3.3.2 Plano de Segurança da Informação (PSI)

Como já foi dito anteriormente, serão propostos no PSI ou Cartilha de Segurança como é mais conhecida, alguns pontos comuns nas redes de qualquer Instituição/Organização. As peculiaridades de cada uma devem ser tratadas caso a caso. Quanto ao uso dos recursos de tecnologia disponibilizados aos usuários, pode-se enfatizar alguns pontos, os quais podem fazer parte também do Termo de Compromisso de Segurança da Informação, documento no qual constarão as regras que vão nortear os procedimentos aos quais os usuários estarão sujeitos e que deve ser entregue ao usuário assim que o mesmo for contratado, lido pelo mesmo e assinado manualmente:

- Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na Instituição/Organização ou para outras situações formalmente permitidas;

- Quando o usuário se comunicar através de recursos de tecnologia da Instituição/Organização, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da mesma;

- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da Instituição/Organização devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário;

- O uso dos recursos de tecnologia da Instituição/Organização pode ser examinado, auditado ou verificado pela equipe de TI, ou por uma equipe designada pelo Gerencia, sempre respeitando a legislação vigente;

- Cada usuário deve ser responsável pelo uso dos recursos que lhe foram fisicamente entregues e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (*softwares*) instalados;

- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deverá comunicar imediatamente à equipe de TI;

- A obrigatoriedade que o equipamento a ser utilizado pelos usuários pertença ao patrimônio da Instituição/Organização, ou seja, proibir a utilização de computadores pessoais (*notebook*, PC, etc.) em suas dependências. Dessa forma, todos os equipamentos (computadores, *notebooks* e impressoras de rede) devem

estar registrados no servidor, utilizando-se para isso da atribuição de endereço IP atrelado ao endereço MAC do equipamento;

- A obrigatoriedade de que os programas aplicativos, programas produto e sistema operacional e os componentes físicos a serem utilizados no equipamento sejam os autorizados pela equipe de TI, bem como, a sua instalação e configuração mediante solicitação por meio de ordem de serviço;

- Cada computador deve ter o seu detentor, que é o responsável direto por esse equipamento. O controle da distribuição dos equipamentos deve constar nos controles da equipe de TI, juntamente com o inventário de todo o parque de máquinas da Instituição/Organização;

- O acesso à Internet somente acontecerá após o usuário se identificar no ambiente de tecnologia da Instituição/Organização, ou seja, através do usuário e senha entregues a ele quando da assinatura do Termo de Compromisso, o qual rege a conduta dos usuários que se utilizam dos recursos tecnológicos da Instituição/Organização;

- O usuário deverá ter o acesso a sites permitidos de acordo com o nível de utilização e das tarefas que o mesmo irá realizar. Caso o usuário necessite realizar acesso a qualquer outro site que não está autorizado para ele, o mesmo deverá efetuar uma solicitação (ordem de serviço) a equipe de TI, através de seu Chefe de Seção ou Departamento, contendo a justificativa para o acesso. O pedido será analisado e se julgado pertinente terá o acesso liberado;

- Será responsabilizado por todo acesso realizado com a sua identificação/autenticação. Caso o usuário de uma determinada máquina se afaste da mesma e qualquer outra pessoa realize um acesso indevido, através daquele equipamento, a responsabilidade será imputada ao usuário que estiver registrado no "*log* de acesso" registrado no servidor;

- A proibição de acessos locais virtuais (sites) que possam violar direitos de autor, marcas, licenças de programas (*software*s) ou patentes existentes. Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia. Contenham informações que não façam parte dos assuntos da Instituição/Organização. Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física. Que não tenham relação direta com a atividade profissional desempenhada pelo usuário;

- A Instituição/Organização disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (Ex.:nome_usuario@nomedaempresa.com.br), bem como o nome de usuário que antecede o símbolo @ e a senha do mesmo, servirão como chave de acesso a todos os outros serviços disponibilizados na rede, evitando dessa forma que um mesmo usuário possua um *login* e senha para cada serviço existente na rede;

- O endereço eletrônico disponibilizado para o usuário deverá ser individual e intransferível;

- O endereço eletrônico cedido para o usuário deverá ser o mesmo durante todo o seu período de vínculo com a Instituição/Organização. Se houver necessidade de troca de endereço, a alteração deverá ser realizada pela equipe de TI e registrada para possibilitar uma posterior verificação de autoria;

- Quando ocorrer desligamento da Instituição/Organização ou transferência de setor do usuário, o setor de Recursos Humanos deverá comunicar formalmente a equipe de TI para que a mesma exclua o usuário dos cadastros do qual faz parte, em caso de desligamento, ou providencie a alteração de setor para aquele usuário;

- A equipe de TI deverá providenciar o registro de todas as mudanças ocorridas nas configurações dos diversos serviços disponibilizados na rede. Nesse registro deverão constar dados como: data/hora do procedimento, nome do responsável pela mudança, motivo, à pedido de quem e uma descrição do procedimento executado;

- As senhas do pessoal da equipe de TI, dos usuários da rede, dos servidores deverão ser criadas pela equipe de TI da Instituição/Organização e armazenados em arquivos digitais criptografados, como também em papel e guardados no cofre do departamento de controle de documentação de acesso restrito;

- A equipe de TI deverá registrar detalhadamente todos os passos efetuados durante a instalação de todos os serviços disponibilizados na rede da Instituição/Organização, bem como as senhas dos sistemas em arquivos digitais criptografados, como também em papel e guardados no cofre do departamento de controle de documentação de acesso restrito;

Mesmo que a Instituição/Organização providencie o Plano de Segurança da Informação ou Cartilha de Segurança, que o usuário receba o Termo de Compromisso, tome ciência e assine, é de suma importância que sejam realizados treinamentos e palestras sobre os assuntos abordados no PSI ou Cartilha, com o

intuito de manter os usuários sempre atentos a qualquer tipo de situação anormal ou atentatória a segurança da Instituição/Organização. Essas orientações além de serem úteis para a segurança da Instituição/Organização, também servem de aprendizado para aos usuários quando os mesmos estiverem em ambientes virtuais em suas residências, pois o mesmo levará os hábitos adquiridos no ambiente de trabalho para o seu ambiente pessoal.

3.4 AS CARACTERÍSTICAS DO *FIREWALL* PFSENSE

3.4.1 *Firewall* pfSense

O uso de um *Firewall* está relacionado ao tamanho da rede, o grau de complexidade das regras que restringem o fluxo de entrada e saída de dados e o nível de segurança desejado. Além da aplicação na forma de *software*, um *Firewall* apresenta-se também na forma de *hardware*. Contudo, o foco desta proposta está baseado na utilização de um *Firewall* aplicado na forma de *software*, mais precisamente em *software* livre.

Como proposta de *Firewall* a ser utilizado na rede, apresentamos o *pfSense* na versão 2.1, uma distribuição livre, *open source* e personalizada do *FreeBSD,* adaptada para ser usada como *Firewall* e roteador. Além de ser uma flexível plataforma de *Firewall* e roteamento, inclui uma longa lista de recursos relacionados e um sistema de pacotes permitindo futuras expansões, sem acrescentar falhas e vulnerabilidades de segurança em potencial na base da distribuição. As instalações vão desde pequenas redes domésticas, protegendo desde um PC ou um *Xbox*, até grandes corporações, universidades e outras organizações protegendo milhares de dispositivos de rede.

A implementação mais comum do *pfSense* é como um *Firewall* de perímetro, com suporte a várias ligações à Internet, bem como várias interfaces internas, podendo ser utilizado em configurações mais complexas, como múltiplas redes LAN e múltiplas redes DMZ.

3.4.1.1 Recursos disponíveis no pfSense

PfSense inclui a maior parte das características disponíveis em *Firewalls* comerciais de alto custo. A lista de recursos disponíveis a partir da versão 1.2 do pfSense, estão disponíveis via interface web:

- Firewall

- Filtragem por endereço IP de origem e destino, protocolo IP, porta de origem e destino para tráfego TCP e UDP;
- Capaz de limitar as conexões simultâneas para cada regra;
- *pfSense* utiliza p0f, um avançado utilitário de detecção de Sistemas Operacionais e Redes que lhe permite filtrar conexões baseado no Sistema Operacional que a iniciou. Deseja permitir acesso de máquinas Linux e *FreeBSD* à Internet, mas bloquear máquinas Windows, o pfSense pode passivamente detectar o sistema operacional em uso;
- Opção para registrar (*log*) ou não registrar o tráfego correspondente a cada regra;
- Política de roteamento altamente flexível, sendo possível selecionar o *gateway* associado com a regra (para balanceamento de carga, *failover*, múltiplas WAN);
- Permite criação de grupos de IPs, redes e portas e usá-los na criação de regras. Isso ajuda a manter limpas suas regras de *Firewall* e de fácil compreensão, especialmente em ambientes com múltiplos IPs públicos e diversos servidores;
- Capacidade para operar em modo transparente na camada 2 – pode-se ligar interfaces em modo *bridge* e filtrar o tráfego entre elas, podendo configurar um *Firewall* sem endereço IP;
- Normalização de pacotes - Descrição da documentação do PF scrub - "*scrubbing*" é a normalização de pacotes para que não haja ambiguidades na interpretação pelo destino final do pacote. A diretiva *scrub* também remonta pacotes fragmentados, protegendo alguns sistemas operacionais de algumas formas de ataque, e descarta pacotes TCP que têm combinações de *flag* inválidas. Ativado por padrão no *pfSense*. Pode ser desabilitado, se necessário. Esta opção pode causar problemas para

algumas implementações de NFS, mas é seguro e deve ser deixado habilitado na maioria das instalações;

- Desativar filtro – pode-se desligar o filtro de *Firewall* completo se o Administrador deseja transformar *pfSense* em um roteador puro.

- Tabela de Estados

A tabela de estados do firewall mantém informações sobre as conexões de rede abertas. O *pfSense*, por padrão, possui todas as regras *stateful*.

- Tamanho da tabela de estados ajustável - existem várias instalações de produção *pfSense* usando centenas de milhares de membros. O tamanho padrão da tabela de estados é de 10.000, mas pode ser aumentada em tempo real para o tamanho desejado. Cada estado tem cerca de 1KB de memória RAM, você deve ter em mente o uso de memória na hora de dimensionar a sua tabela de estados e não definí-la arbitrariamente alta.
- Baseado por regra:
  - Limite de conexões simultâneas de clientes;
  - Limite de estados por host;
  - Limite de novas conexões por segundo;
  - Definir timeout de estado;
  - Definir tipo de estado.
- Tipos de estados - O *pfSense* oferece múltiplas opções para manipulação dos estados.
  - *keep state* - Funciona com todos os protocolos. Padrão para todas as regras;
  - *Modulate state* - Funciona apenas com TCP. O *pfSense* irá gerar uma Seqüência Inicial Numérica (ISNs) para o *host;*
  - *Synproxy state* - Faz um *proxy* das conexões TCP de entrada, serve para proteger os servidores de ataques de TCP SYN falsos. Esta opção inclui a funcionalidade de *keep state* e *modulate state* combinadas;
  - Nenhum - Não mantém nenhuma entrada na Tabela de Estados para este tráfego. Isso é muito pouco desejável, mas está disponível porque pode ser útil em algumas circunstâncias limitadas.

- Opções de otimização da Tabela de Estados - O pfSense oferece quatro opções para a otimização da tabela de estados.
  - Normal - O algoritmo padrão;
  - Alta latência - Útil para links de alta latência, como conexões via satélite. Expira conexões inativas mais tarde que o normal;
  - Agressivo - Expira conexões ociosas mais rapidamente. Uma utilização mais eficiente dos recursos de hardware, mas pode derrubar conexões legítimas;
  - Conservador - Tenta evitar quedas de conexões legítimas, em detrimento do uso de memória e maior utilização da CPU.

- Network Address Translation (NAT)

- Redirecionamento de Portas, incluindo faixas e a utilização de múltiplos IPs públicos;
- Redirecionamento 1:1 para o IP ou sub-redes inteiras;
- NAT de saída
  - A configuração padrão mascara todo o tráfego de saída usando o endereço IP da interface WAN. Em cenários com múltiplas WANs, as configurações padrão fazem NAT do tráfego de saída para IP utilizado na interface WAN;
  - As configurações avançadas de NAT de saída permitem que esse comportamento padrão seja desativado, e permite a criação de regras de NAT (ou nonat) muito flexíveis.
- Reflexão NAT - Em algumas configurações, a reflexão NAT é possível para que os serviços possam ser acessados pelo IP público à partir de redes internas.

- Redundância

CARP do *OpenBSD* permite falha do hardware. Dois ou mais *Firewalls* podem ser configurados como um grupo *failover* (redundância de *Firewall*). Se uma interface, principal ou primária, fica *offline* completamente, a interface secundária é ativada, o *pfSense* também inclui capacidades de sincronização de configuração,

para que quando forem realizadas alterações de configuração no primário elas sejam sincronizadas automaticamente no *Firewall* secundário.

pfsync garante que a tabela de estados do firewall seja replicada para todos os *Firewalls* configurados no *failover*. Isto significa que as conexões existentes serão mantidas em caso de falha, que é importante para evitar quedas nas conexões ativas.

- Balanceamento de carga

Balanceamento de carga de saída: é utilizado com várias conexões WAN para fornecer balanceamento na carga e *failover*. O tráfego é direcionado para o *gateway* desejado ou um *pool* de balanceamento de carga, configuração feita para cada regra de *Firewall*.

Balanceamento de carga de entrada: é usado para distribuir a carga entre vários servidores, isto é comumente usado em servidores web, servidores de email e outros. Os servidores que não respondem às solicitações *ping* ou conexões da porta TCP são removidos do pool.

- VPN

O pfSense oferece três tipos de conexões para VPN, IPsec, OpenVPN, e PPTP.

IPsec permite conexão com qualquer outro dispositivo que suporte o seu protocolo. É normalmente usado para conexões lan-to-lan com outras instalações de pfSense, outro *Firewalls* de código aberto e a maioria das soluções comerciais de *Firewall* (Cisco, Juniper, etc.). Ele também pode ser usado para conexões com equipamentos móveis.

OpenVPN é uma solução de VPN flexível, com bom suporte à SSL que é suportado por uma vasta lista de Sistemas Operacionais.

Servidor PPTP é uma opção popular de VPN, pois muitos Sistemas Operacionais possuem em sua instalação um cliente PPTP, incluindo todas as versões de Windows desde o 96 OSR2. O servidor PPTP do pfSense pode usar uma base local de usuários ou um servidor RADIUS para autenticação. RADIUS *accounting* é também suportado. As regras de Firewall da interface PPTP controlam o tráfego iniciado pelos clientes PPTP.

3.4.1.2 Requisitos de hardware para instalação do *pfSense*

A configuração mínima de *hardware* necessária ao *pfSense* para instalação em plataformas individuais é um CPU – Pentium 100 MHz, com 128 MB de memória RAM, drive CD-ROM e 1 GB de espaço em disco rígido.

Os requisitos mínimos não são adequados para todos os ambientes. Ao dimensionar o *hardware* para uso do *pfSense*, dois fatores devem ser considerados: ***Throughput* necessário** e **recursos que serão utilizados**.

Se você precisa de menos de 10Mbps de *throughput*, você pode utilizar os requisitos mínimos. Para maiores requisitos de *throughput* é recomendado seguir algumas orientações visando não utilizar o seu *hardware* na sua capacidade total:

- 10-20 Mbps – CPU de 266 MHz.
- 21-50 Mbps – CPU de 500 MHz.
- 51-200 Mbps – CPU de 1.0 GHz.
- 201-500 Mbps - *hardware* de servidor com adaptadores de rede PCI-X ou PCI-e, ou *hardware* de *desktop* mais moderno com adaptadores de rede PCI-e, e uma CPU de 2.0 GHz.
- 501 ou + Mbps - *hardware* de servidor com adaptadores de rede PCI-X ou PCI-e, e uma CPU de 3.0 GHz.

Em relação aos recursos que serão utilizados a maioria não interfere no dimensionamento, porém alguns têm impacto significativo na utilização do *hardware*:

VPN - O uso pesado de qualquer um dos serviços de VPN incluídos no *pfSense* irá aumentar os requisitos da CPU. Criptografar e descriptografar o tráfego gera um uso intenso do processador. O número de conexões é muito menos preocupante do que o *throughput* necessário. Um processador de 266 MHz irá fornecer um *throughput* de *IPSec* em torno de 4 Mbps, um processador de 500 MHz pode obter em torno de 10-15 Mbps de *IPsec*, em um hardware relativamente novo de servidor (Xeon 800 FSB e mais recentes) implantações estão obtendo mais de 100 Mbps, com capacidade de sobra, cartões de criptografia são suportados e são capazes de reduzir significativamente os requisitos de CPU.

Portal de Captação - Embora a principal preocupação seja tipicamente *throughput*, ambientes com centenas de usuários simultâneos em portal de captação vai exigir um pouco mais poder de CPU do que o recomendado acima.

Grandes Tabelas de Estado - As entradas de tabelas de Estado necessitam de cerca de 1KB de RAM cada. Na Tabela de Estado padrão, quando o total de 10.000 entradas é preenchido, utiliza pouco menos de 10 MB de memória. Para ambientes que exigem grandes Tabelas de Estado com centenas de milhares de conexões, há a necessidade de certificar-se de ter memória suficiente disponível.

Pacotes - Alguns dos pacotes aumentam os requisitos de memória significativamente. *Snort* e *Ntop* são dois que não devem ser instalados em um sistema com menos de 512 MB RAM.

3.5 CONFIGURANDO OS SERVIÇOS DA REDE

3.5.1 Instalação do *Firewall* pfSense

A imagem pode ser obtida no site http://www.pfsense.org.br/, na seção de downloads e depois em *mirror*, sendo possível escolher versões para uma nova instalação, com suporte a i386 ou amd64, possui suporte para instalação em *pendrive* e também uma versão *live* cd. Caso sejam utilizados servidores com máquinas virtuais também há uma versão pronta para rodar neste tipo de sistema.

Depois de gravada a imagem, o CD funciona com um “live cd”, ou seja, todo o sistema pfSense já está previamente carregado e pronto para uso ao se iniciar o servidor a partir do CD ROM.

Para esta instalação será utilizado um PC com processador Intel Core 2 2.80Ghz, com HD de 80 Gb, 1 Gb de memória e 2 placas de rede PCI 10/100/1000.

De posse da mídia gravada e configurado o *setup* da máquina para *boot* via drive de CD, pode-se iniciar a instalação do pfsense:

Após o boot pelo CD, o pfSense faz uma leitura para detectar o *hardware* existente. A primeira tela de exibição inicial de instalação do pfSense, onde há a necessidade de se pressionar a tecla “i” para iniciar as configurações para instalação no HD. (Figura 7).

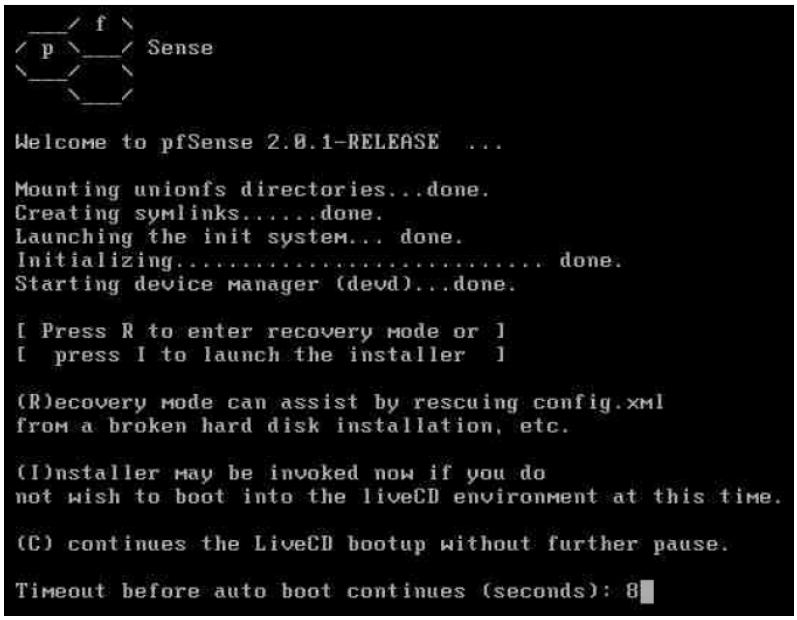


FIGURA 7 – TELA INICIAL PARA INSTALAÇÃO DO PFSENSE
FONTE: PFSENSE FIREWALL

Após isso, será apresentada a tela de configuração de vídeo e teclado, onde será selecionada a opção "*Accept these Settings*", pois serão utilizada as configurações padrão. A navegação é feita através das setas do teclado. (Figura 8).

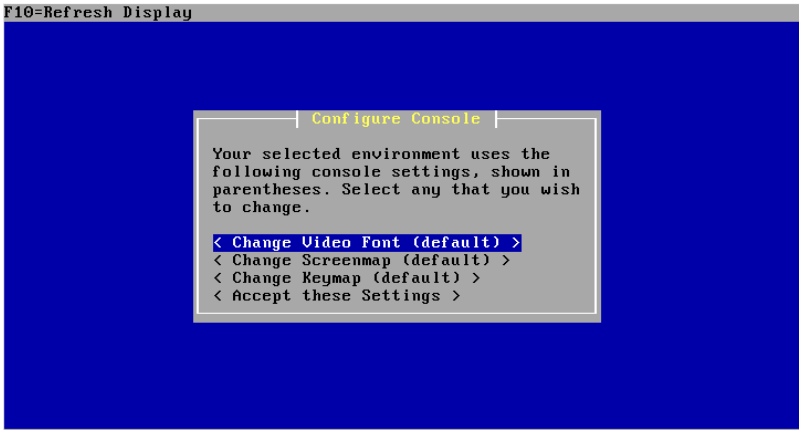


FIGURA 8 – TELA DE CONFIGURAÇÃO DE VÍDEO E TECLADO
FONTE: PFSENSE FIREWALL

Na próxima tela apresentada seleciona-se a opção “**Quick/Easy Install**” para instalação rápida e fácil do pfSense. (Figura 9).

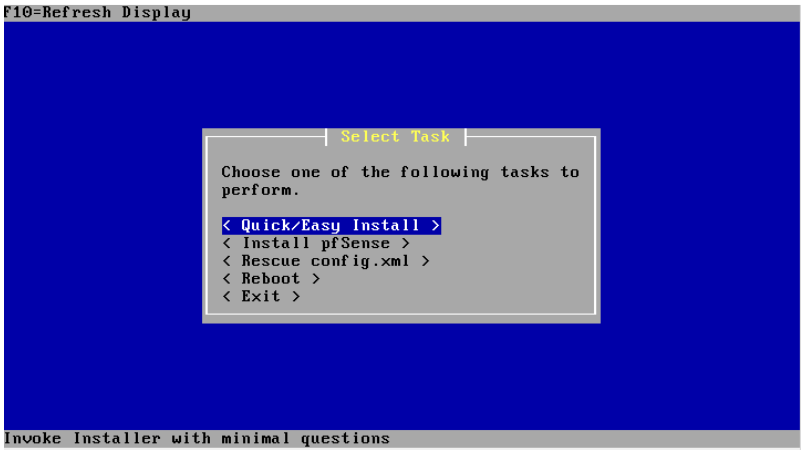


FIGURA 9 – SELEÇÃO DO TIPO DE INSTALAÇÃO
FONTE: PFSENSE FIREWALL

Nesta tela será emitido o aviso de que a instalação rápida não fará nenhuma pergunta a respeito de opções de instalação. Pressiona-se <enter> na opção “OK”. (Figura 10).

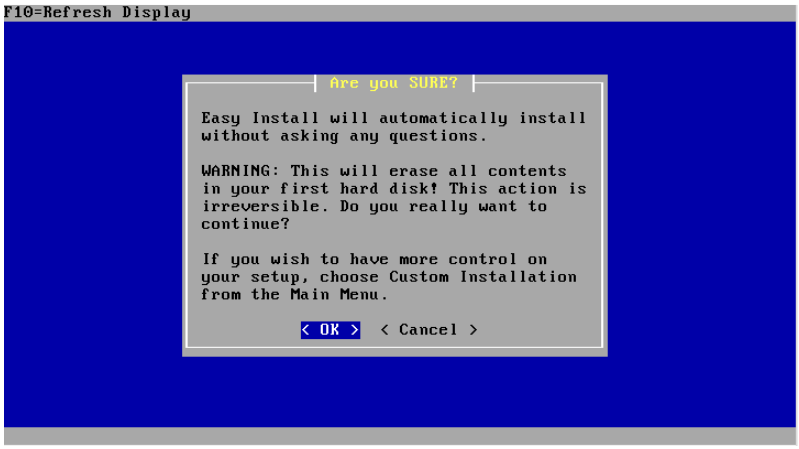


FIGURA 10 – CONCORDA COM O TIPO DE INSTALAÇÃO
FONTE: PFSENSE FIREWALL

A execução da formatação e a criação das pastas. (Figura 11).

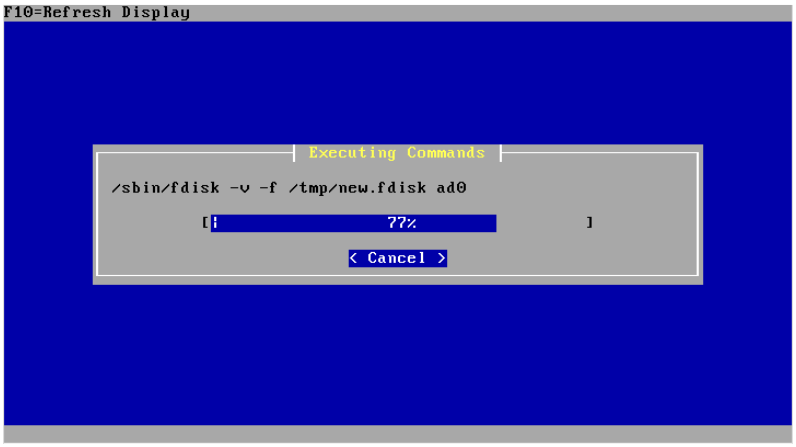


FIGURA 11 – FORMATAÇÃO E CRIAÇÃO DAS PASTAS DO SISTEMA
FONTE: PFSENSE FIREWALL

Nesta tela são apresentadas 2 opções:

Standard Kernel: esta opção indica que haverá monitor ligado ao *Firewall*.

Embedded Kernel (no VGA console, keyboard): com esta opção, estará selecionando que não terá monitor e nem teclado ligado no *Firewall*. (Figura 12).

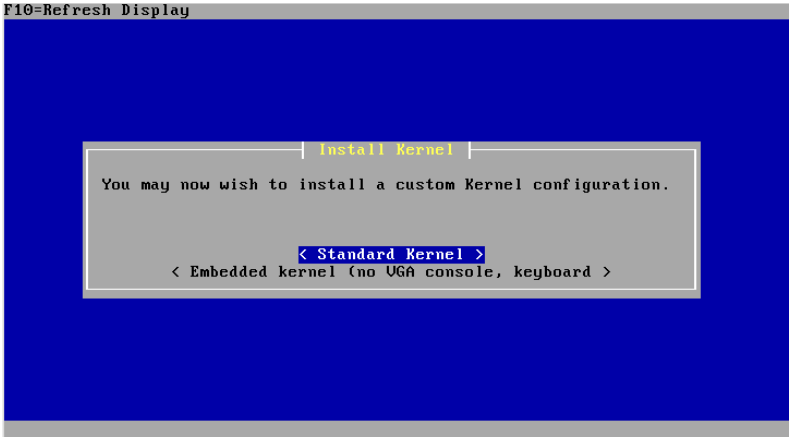


FIGURA 12 – SELECIONA SE HAVERÁ MONITOR CONECTADO AO FIREWALL
FONTE: PFSENSE FIREWALL

A tela final de instalação do pfSense. Pressiona-se <enter> na opção "***Reboot***" e retira-se o CD para reiniciar o sistema pelo HD. (Figura 13).

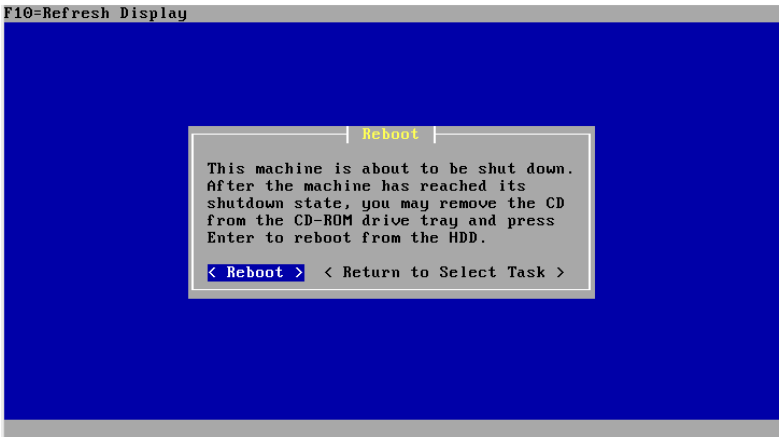


FIGURA 13 – REBOOT E REINICIALIZA O SISTEMA PELO HD
FONTE: PFSENSE FIREWALL

Após reinicializar o sistema pelo HD, a tela exibida mostra as 2(duas) placas de rede reconhecidas pelo sistema e seus respectivos endereços MAC, uma característica do pfSense é que ele as identifica como “em0”, “em1” ou “re0”, “re1” ou ainda “vr0”, “vr1”, dependendo da versão utilizada e do número de placas de rede conectadas.

A primeira pergunta que o sistema faz é se deseja utilizar VLAN (y/n), neste caso, optou-se dizer que não. (Figura 14).

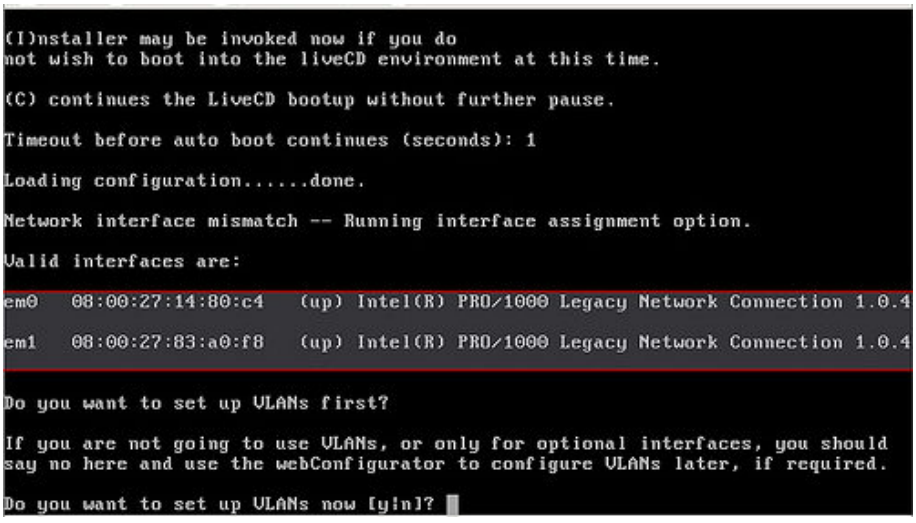


FIGURA 14 – IDENTIFICAÇÃO DAS PLACAS DE REDE CONECTADAS
FONTE: PFSENSE FIREWALL

Neste ponto é solicitado o nome da interface de rede (em0 ou em1) que será configurada a WAN ou então, digitar a opção “a” para auto-identificar em qual das interfaces a WAN será configurada por DHCP, caso esta opção esteja disponível. (Figura 15).

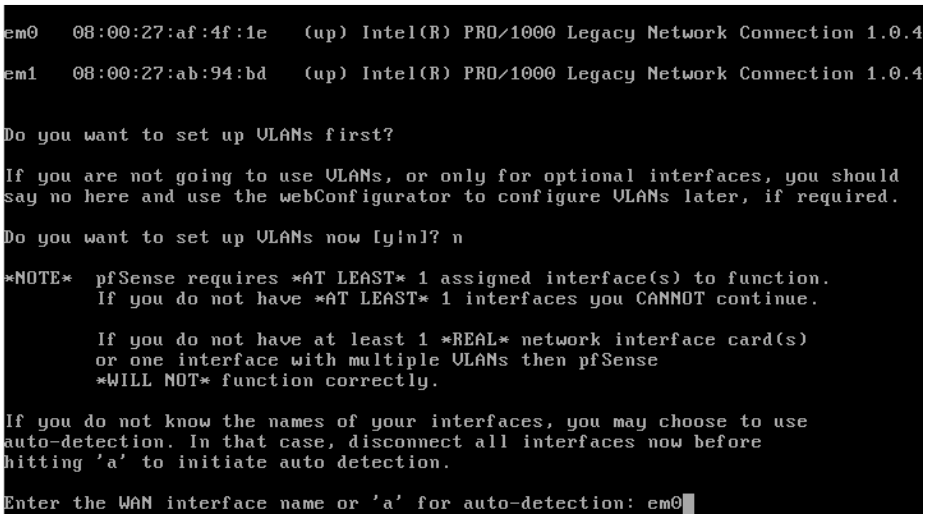


FIGURA 15 – ESCOLHA DA INTERFACE DE REDE PARA WAN
FONTE: PFSENSE FIREWALL

Na sequência, será apresentado o menu principal do pfSense, com todas as funções que poderão ser utilizadas. Caso seja necessário alterar as configurações das placas de rede da WAN ou LAN, isto pode ser feito através da opção 2) do menu. O pfSense adota por padrão o endereço 192.168.1.1 para acesso e configurações via navegador. Cabe ressaltar que ainda se está atuando na máquina escolhida para *Firewall*. (Figura 16).

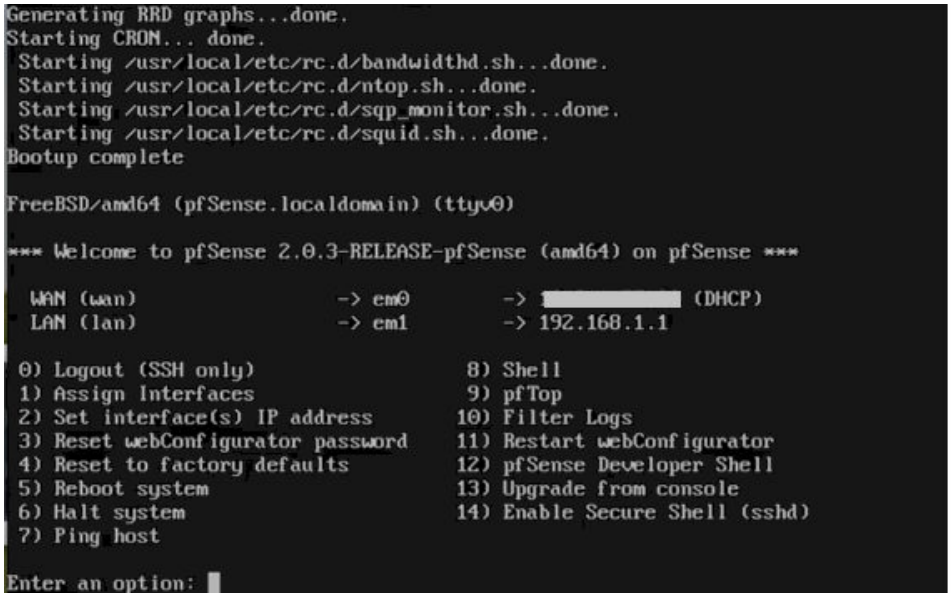


FIGURA 16 – MENU PRINCIPAL DO PFSENSE
FONTE: PFSENSE FIREWALL

A partir deste ponto pode-se começar a configurar o *Firewall* através de um navegador, a critério do administrador, digitando na barra de endereço o IP padrão do pfSense http://192.168.1.1. Em seguida, se tudo estiver configurado corretamente, irá mostrar a tela solicitando *Username* e *Password*, que por padrão é **admin** e **pfsense** (minúsculo). (Figura 17).

FIGURA 17 – TELA DE LOGIN DO FIREWALL PFSENSE
FONTE: PFSENSE FIREWALL

Após a confirmação do *login* pode-se iniciar as configurações do pfSense. Inicialmente é solicitado o *Hostname*, *Domain*, *Primary* e *Secondary* DNS *Server*, é possível configurar até 4(quatro) endereços de DNS. (Figura 18).

FIGURA 18 – TELA COM AS CONFIGURAÇÃO INICIAIS DO FIREWALL
FONTE: PFSENSE FIREWALL

A próxima configuração diz respeito ao NTP e *TimeZone*, importante para o servidor manter atualizado o horário no momento de armazenamento de *logs*. (Figura 19).

FIGURA 19 – CONFIGURAÇÃO NTP E TIMEZONE
FONTE: PFSENSE FIREWALL

A próxima tela é de extrema importância. Por uma questão óbvia de segurança deve-se alterar o Password de acesso às configurações do *Firewall* pfSense, seria uma falha de segurança deixar as configurações padrão. (Figura 20).

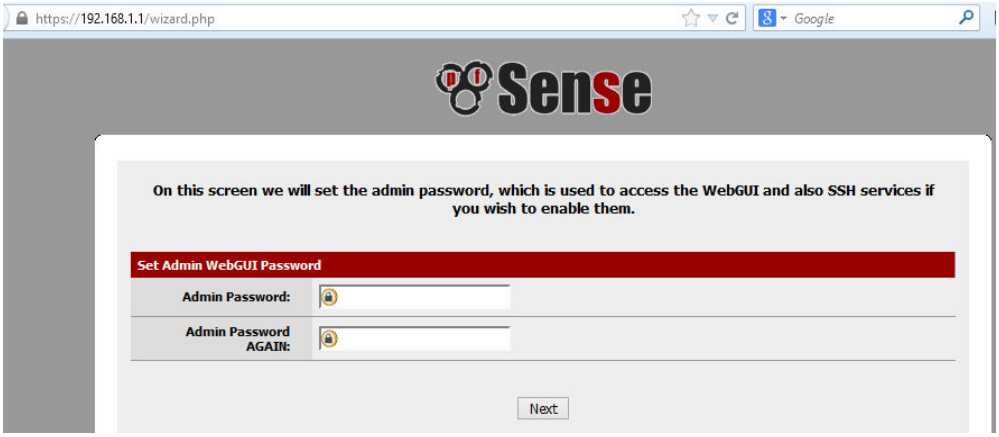


FIGURA 20 – TELA PARA ALTERAÇÃO DO *PASSWORD* DE ACESSO ÀS CONFIGURAÇÕES DO PFSENSE
FONTE: PFSENSE FIREWALL

Após configurar qualquer serviço ou realizar uma alteração, obrigatoriamente deve-se clicar no botão "*Reload*" para que as mudanças sejam efetivamente gravadas nas configurações do *Firewall* e tenham efeito sobre o mesmo. (Figura 21).

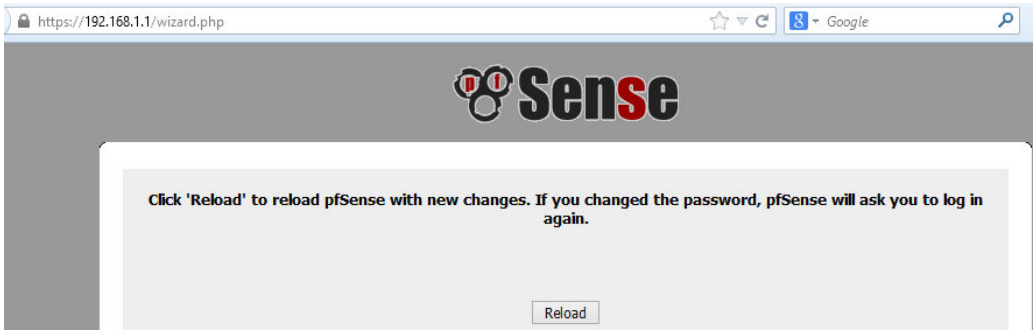


FIGURA 21 – BOTÃO RELOAD – GRAVA AS CONFIGURAÇÕES NO *FIREWALL*
FONTE: PFSENSE FIREWALL

Visando aumentar a segurança no acesso ao console de configuração do pfSense, há uma opção para permitir o acesso somente autorizado com senha. Navega-se em **Sistema - Avançado e Acesso de Administrador**. Ainda nesta tela, pode-se definir o número de acessos simultâneos ao console de configuração. (Figura 22).

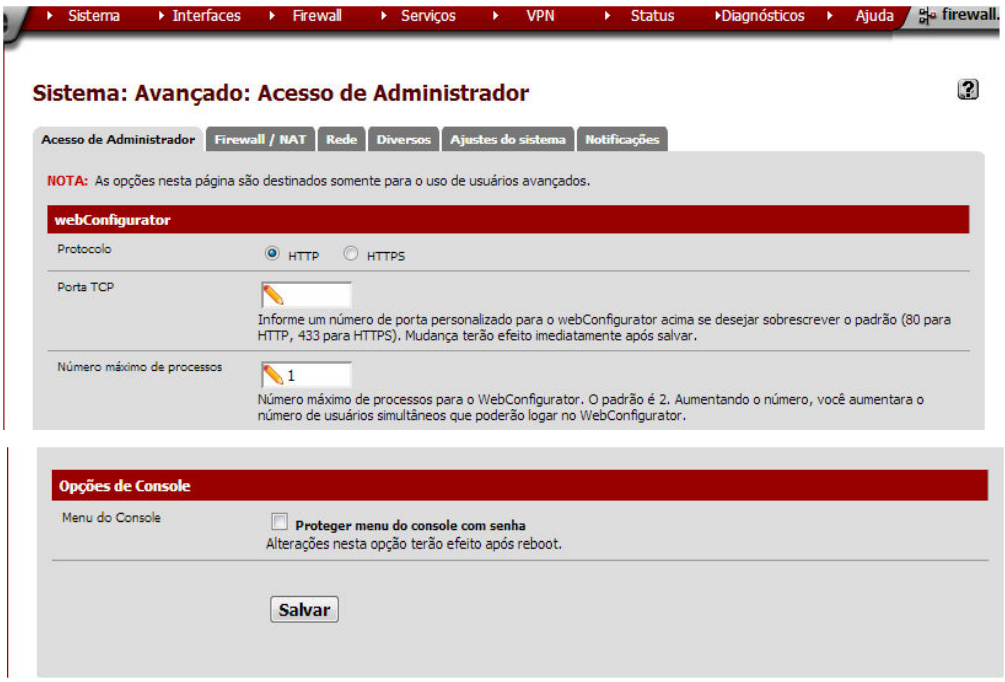


FIGURA 22 – AUMENTANDO A SEGURANÇA DE ACESSO AO CONSOLE DO PFSENSE
FONTE: PFSENSE FIREWALL

3.5.2 DHCP no pfSense

O pfSense só pode ser configurado como um servidor de DHCP se a interface estiver com endereço IP estático. Para configuração navega-se em **Serviços - Servidor DHCP**. A primeira configuração a se fazer é Habilitar servidor DHCP na interface LAN. O "**gateway**" das maquinas clientes por padrão será o IP da interface local usada como servidor de DHCP, mas isso pode ser mudado se necessário. Habilitar "**Negar clientes desconhecidos**" faz com que apenas os clientes com IP estático configurado junto com o MAC que constarem da relação, terão acesso ao *Firewall*. (Figura 23).

FIGURA 23 – INTERVALO DE IP FORNECIDOS PELO SERVIDOR DHCP
FONTE: PFSENSE FIREWALL

A opção "***Default Lease Time***" é um valor que pode ser usado para especificar um tempo mínimo que expire o acesso por DHCP. O tempo padrão é 7200 segundos. "***Maximum Lease Time***" é um valor que pode ser usado para especificar um tempo máximo para que expire o acesso por DHCP. O tempo padrão é 86400 segundos. "***Failover Peer* IP**" é um sistema que pode configurar um endereço de IP que sirva como *FailOver* de balanceamento de carga. Habilitar

“entradas ARP estáticas” faz com que somente máquinas que constarem na lista de endereços MAC podem se comunicar com o *Firewall*. (Figura 24).

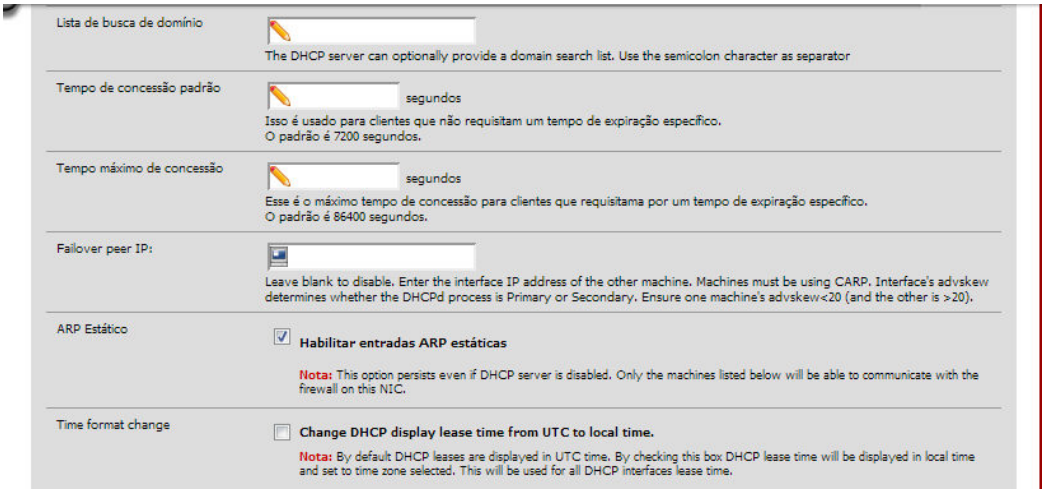


FIGURA 24 – CONFIGURAÇÕES DE TEMPO DE CONCESSÃO DE IP
FONTE: PFSENSE FIREWALL

Para acrescentar uma máquina e relacionar o endereço MAC a um IP estático, basta clicar no botão com o sinal de “**+**” e preencher com o MAC e o IP que se deseja atribuir ao cliente. Lembrando-se que a atribuição de endereço IP estático a um determinado MAC só pode ser feito com IP que estiverem fora do intervalo de IP fornecidos por DHCP. (Figura 25).

FIGURA 25 – LISTA DE CLIENTES COM ENDEREÇO IP RELACIONADO AO ENDEREÇO MAC
FONTE: PFSENSE FIREWALL

3.5.3 Instalação de pacotes de serviços no pfSense

A partir do seu lançamento já pode ser aplicada sobre o pfSense 2.1, a possibilidade de obter os pacotes separados por categorias no menu **Sistema - Pacotes**. Isso deixa o trabalho do *Administrador* mais fácil e organizado. Para aplicar o *patch*, deve-se executar alguns passos:

- Instale o *system patcher* (menu **Sistema – Pacotes**);
- Acesse seu menu e clique em "+" para adicionar um novo *patch*;
- Na descrição você pode colocar "Pacotes por Categoria", por exemplo;
- No campo *url/ID*, coloque o id **3740c81012**;
- Salve a configuração;
- No menu **Sistema – Patch**, é possível ver a descrição e a url do *patch*;
- Na sequência em *fetch*, *test* e *apply*.

Assim, o pfSense 2.1 terá a lista de pacotes (aproximadamente 100) devidamente separada por categorias. (Figura 26).

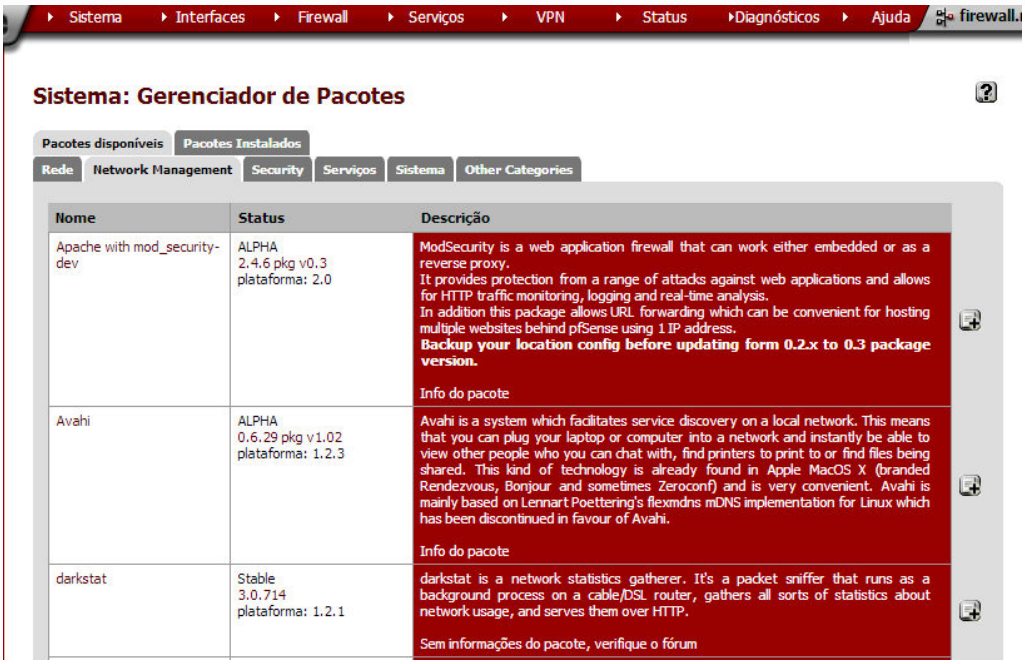


FIGURA 26 – GERENCIADOR DE PACOTES PARA INSTALAÇÃO NO PFSENSE
FONTE: PFSENSE FIREWALL

Alguns pacotes são importantes para a estrutura inicial de construção de um *Firewall*. Ainda no menu **Sistema – Pacotes**, seleciona-se três pacotes essenciais para a configuração das regras de segurança do Firewall, nesta ordem:

- *Squid*: Servidor *Proxy*. Reduz a utilização da conexão e melhora o tempo de resposta às solicitações fazendo *cache* de suas requisições, além de prover um nível básico de controle e segurança no acesso à URL's potencialmente perigosas.

- *SquidGuard*: ferramenta de acesso que integrada ao *Squid* permite controlar a navegação baseado no endereço de origem, destino, URL, por horário ou mesmo a combinação desses itens. Conta ainda com uma opção de uma *blacklist,* agrupados em categorias de sites com um tempo de resposta muito baixo.

- *LightSquid*: ferramenta responsável pela geração dos relatórios de acesso.

Para a instalação dos três pacotes, seguindo a ordem mencionada, basta clicar no botão com o sinal de "**+**" ao lado da descrição do pacote e aguardar a conclusão do *download* e instalação dos mesmos. (Figura 27).

FIGURA 27 – INSTALAÇÃO DOS PACOTES PARA CONFIGURAÇÃO DAS REGRAS DE SEGURANÇA
FONTE: PFSENSE FIREWALL

Para fazer a verificação dos pacotes instalados no sistema, pode-se consultar na aba "**Pacotes Instalados**", ao lado da aba com a lista de "**pacotes disponíveis**" para a instalação. (Figura 28).

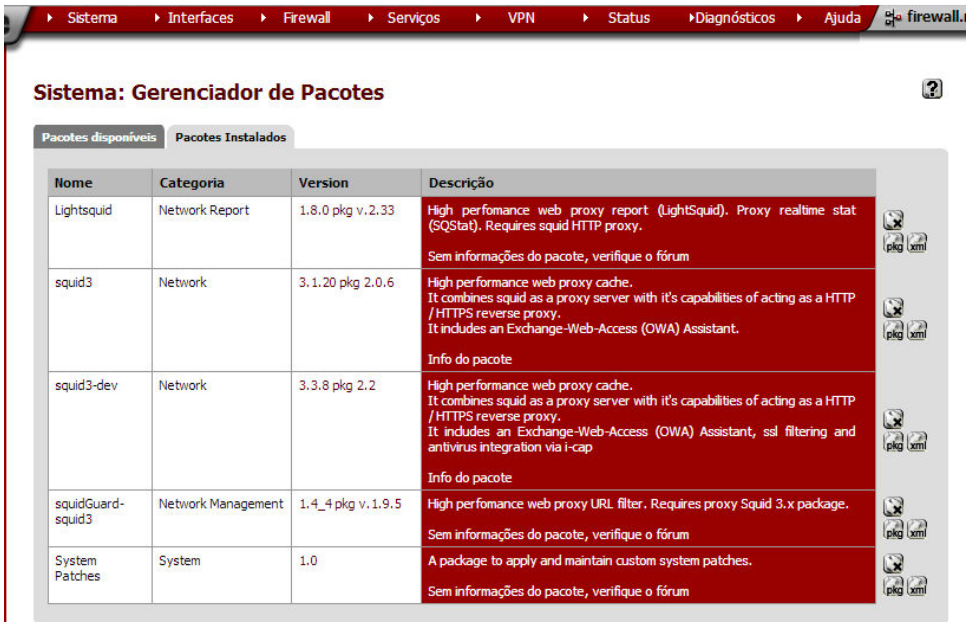


FIGURA 28 – LISTA DOS PACOTES INSTALADOS NO PFSENSE
FONTE: PFSENSE FIREWALL

3.5.4 Configuração de regras de acesso no pfSense

Após instalados os pacotes para configuração das regras de segurança do Firewall, o próximo passo é a definição das regras de acesso. No menu ***Firewall*** – **Regras**, pode-se editar as regras permitindo ou negando o acesso à protocolos e portas de qualquer origem para qualquer destino, definindo conforme a política de segurança estipulada pela Instituição/Organização.

Caso não exista nenhuma regra de liberação criada, o padrão do pfSense é bloquear todo tráfego de entrada e saída. Nesta área de configuração, tanto para WAN quanto para LAN, é possível editar a regra no botão "**e**", excluir a regra "**x**", acrescentar uma regra (**+**) e alterar a ordem de posicionamento da regra "◀". (Figura 29).

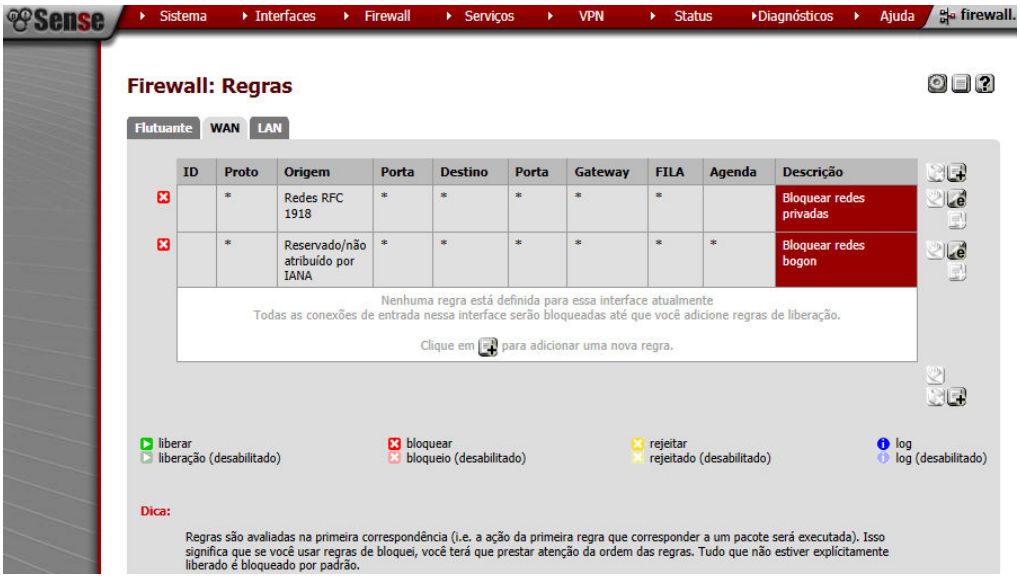


FIGURA 29 – CONFIGURAÇÃO DE REGRAS PARA WAN E LAN
FONTE: PFSENSE FIREWALL

3.5.5 Configuração do *Squid* no pfSense

O Squid é um dos servidores *Proxy* mais utilizados no mundo, devido algumas características como robustez, segurança e recursos que oferece. Trabalha com os protocolos HTTP, HTTPS, FTP e *gopher*, que são os principais protocolos da Internet. Funciona ouvindo requisições numa determinada porta padrão (3128), ou numa outra porta que pode ser configurada pelo Administrador.

Para as configurações iniciais do serviço de *Proxy*, através do menu **Serviços – *Proxy Server* – aba *General Settings***, estão localizadas as configurações básicas do servidor *Proxy*. Geralmente não é preciso alterar nada para que o Proxy funcione. Então pode-se deixar os valores como padrão para a maioria dos campos, alterando somente os campos "***Log store directory***" que é a indicação do local (diretório) para armazenamento de *log*, o campo "***Proxy port***" que é a porta do Proxy. O *Squid* utiliza por padrão a porta 3128, o campo **"*Language*"** para **"Portuguese"** (isso fará com que o *Squid* exiba as páginas de erro em Português) e a opção **"*Supress Squid Version*"** (para que o *Squid* não mostre a sua versão na página de erros). Clica-se em **"*Save*"** para guardar as configurações. (Figura 30).

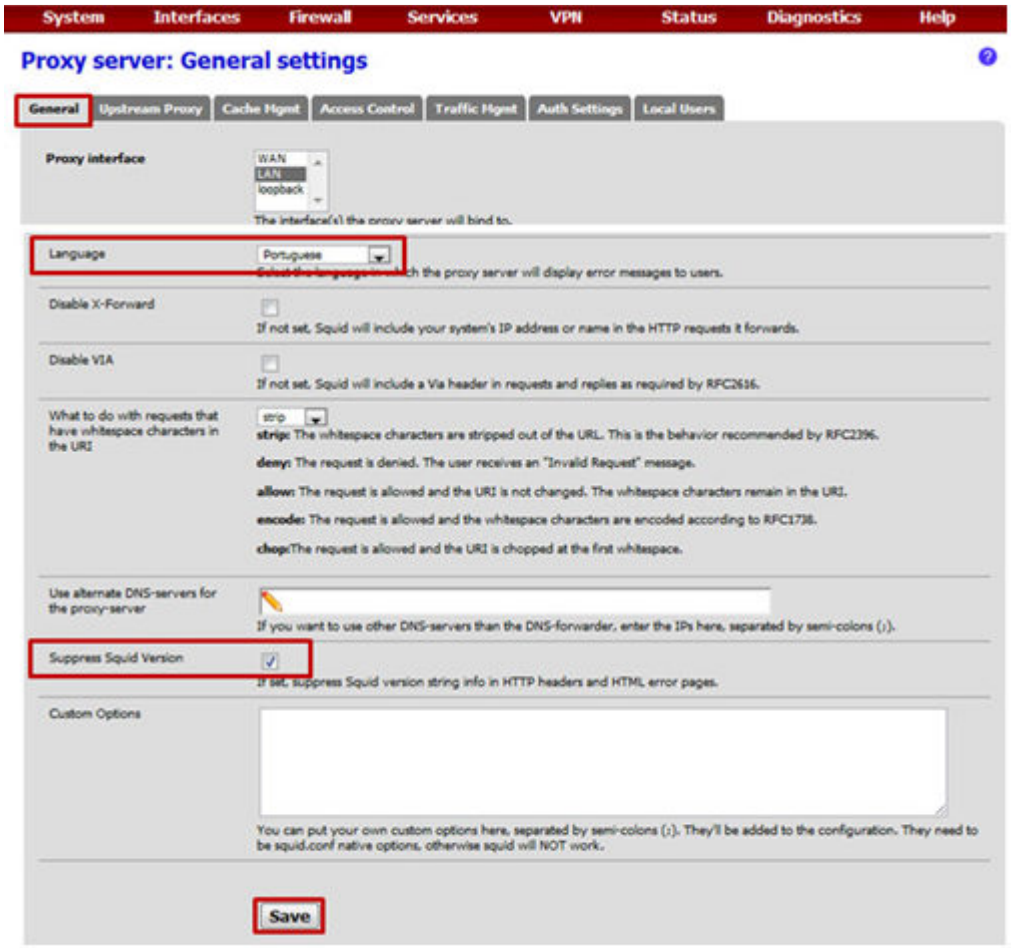


FIGURA 30 – CONFIGURAÇÕES INICIAIS DO SERVIÇO DE PROXY
FONTE: PFSENSE FIREWALL

3.5.5.1 Configurações de autenticação no Squid

Com relação a configuração do método de autenticação, o pfSense disponibiliza para utilização, três métodos:

- *Proxy* Transparente: a estação de trabalho se conecta ao pfSense como *Gateway* que se apropria da requisição para sair para Internet como *Proxy*. Para habilitar basta marcar a *check box* correspondente na aba geral do *Proxy Server*.

- Autenticação com usuário local: para este método de autenticação deve-se criar um ou mais usuários na aba "*Local Users*" e em seguida em "*Auth Settings*" definir o método de autenticação como Local.

- **Autenticação integrada com recursos externos (LDAP – *Windows Active Directory*)**: para que os usuários de um domínio Windows 2003, por

exemplo, possam autenticar com seus usuários do AD no pfSense, deve-se definir em "***Auth Setting***" o método de autenticação LDAP.

Ainda nas configurações do *Squid*, na aba **"*Auth Settings*"**, é possível configurar o *Squid* para que ele utilize a base de dados Local, sem a necessidade de se utilizar algum tipo de integração como o AD ou LDAP. Para isso, no campo **"*Authentication Method*"** seleciona-se a opção **"Local"**. Em **"*Authentication prompt*",** preenche com o texto que vai ser exibido na janela que pede o usuário e a senha. Em **"*Authentication processes*",** o número de autenticações simultâneas, ajustadas conforme a necessidade. E em **"*Authentication TTL*",** é o campo que define o tempo de vida da sessão de um usuário autenticado. (Figura 31).

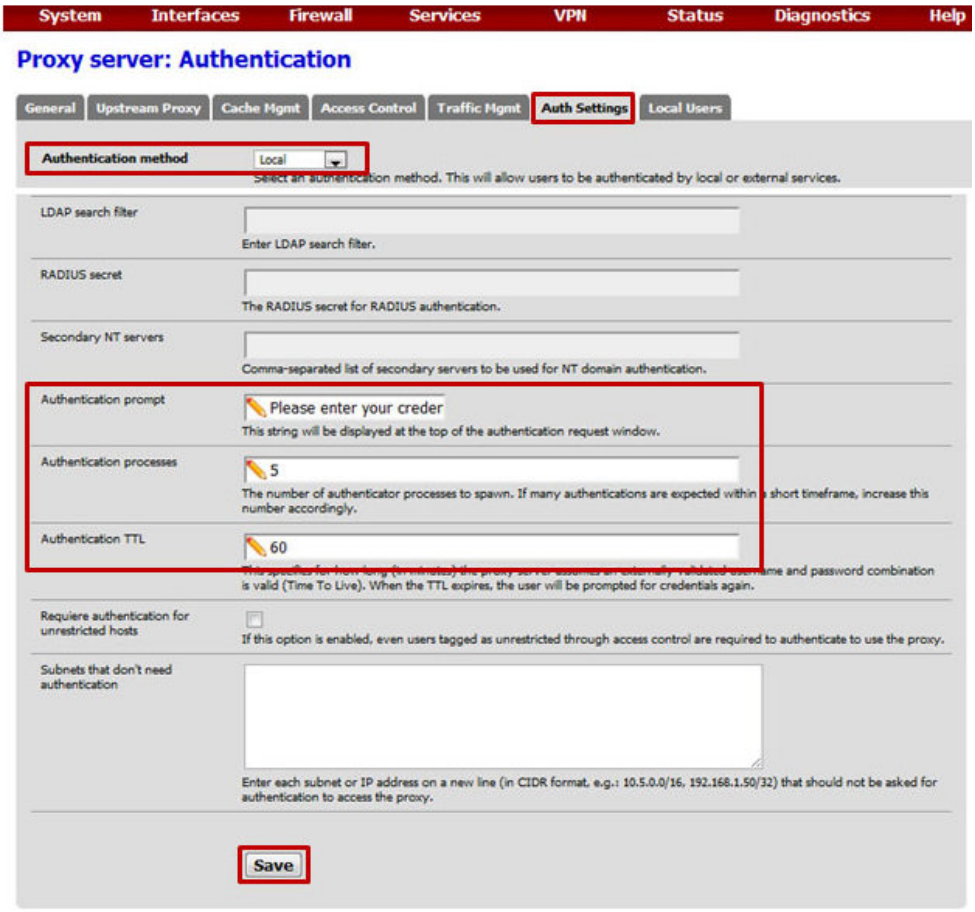


FIGURA 31 – CONFIGURAÇÕES DE AUTENTICAÇÃO NO SQUID
FONTE: PFSENSE FIREWALL

3.5.5.2 Cadastro e manutenção de usuários

Nas configurações do *Proxy* na aba **"*Local Users*"**, pode-se cadastrar os usuários que farão parte do sistema. Para cadastrar um usuário clica-se no ícone "**+**".

Na tela que se abre, há dois campos obrigatórios: **"*Username*"** e **"*Password*"**. Já o campo **"*Description*"** é opcional, porém é muito útil para caráter administrativo, por exemplo, esse campo pode definir a qual departamento o usuário pertence. Clica-se em **"*Save*"** para finalizar essa etapa de cadastro. (Figura 32).

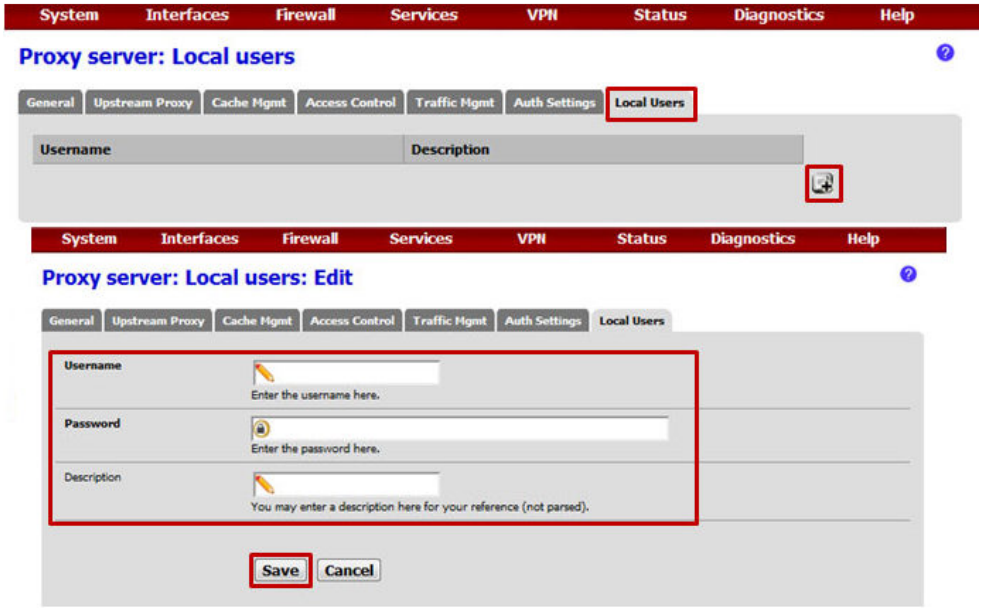


FIGURA 32 – CADASTRO DE USUÁRIO DO SISTEMA
FONTE: PFSENSE FIREWALL

Para realizar a manutenção dos usuários, em **"*Local Users*"**, pode-se perceber que na listagem dos usuários cadastrados no sistema, ao lado aparece dois pequenos ícones, eles têm a função editar "**e**" e deletar "**x**". Lembrando-se sempre da importância do controle de usuários que se afastam da Instituição/Organização e a sua exclusão do sistema a que pertenciam.

No botão editar pode-se alterar o nome de usuário e a senha. E no de remover, excluir o usuário do sistema.

No caso de alterar o dados do usuário, o pfSense traz o mesmo formulário só que preenchido com os dados originais bastando alterar aonde necessário. (Figura 33).

FIGURA 33 – ALTERAÇÃO E/OU EXCLUÃO DE USUÁRIO DO SISTEMA
FONTE: PFSENSE FIREWALL

3.5.5.3 Definindo os Grupos e os *sites* liberados

Para realizar a autenticação por grupos no pfSense, navega-se em menu ***Diagnostics - Edit File***. No campo que aparece digita-se: **"/usr/local/pkg/squid.inc"** e clica-se no botão **"*Load*"**. Uma vez o conteúdo do arquivo carregado, procura-se (Control + F) pelo seguinte conteúdo: **"*acl password proxy_auth REQUIRED*"** (sem as aspas). (Figura 34).

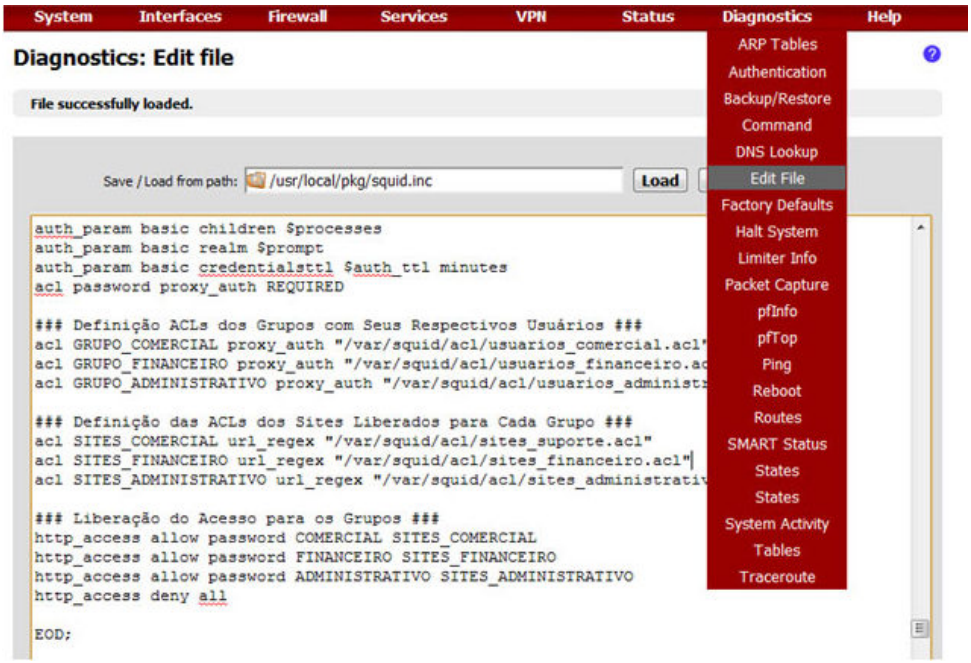


FIGURA 34 – ALTERANDO O ARQUIVO SQUID.INC
FONTE: PFSENSE FIREWALL

Entre a linha **"*acl password proxy_auth REQUIRED*"** e a **"EOD;"** inserir o código abaixo:

Definição ACLs dos Grupos com Seus Respectivos Usuários

acl COMERCIAL proxy_auth "/var/squid/acl/usuarios_comercial.acl"

acl FINANCEIRO proxy_auth "/var/squid/acl/usuarios_financeiro.acl"

acl ADMINISTRATIVO proxy_auth "/var/squid/acl/usuarios_administrativo.acl"

Definição das ACLs dos Sites Liberados para Cada Grupo

acl SITES_COMERCIAL url_regex "/var/squid/acl/sites_comercial.acl"

acl SITES_FINANCEIRO url_regex "/var/squid/acl/sites_financeiro.acl"

acl SITES_ADMINISTRATIVO url_regex "/var/squid/acl/sites_administrativo.acl"

Liberação do Acesso para os Grupos

http_access allow password COMERCIAL SITES_COMERCIAL

http_access allow password FINANCEIRO SITES_FINANCEIRO

http_access allow password ADMINISTRATIVO SITES_ADMINISTRATIVO

http_access deny all

Ao final das inclusões, salvar o arquivo **"squid.inc"** alterado.

Algumas observações. Nesta proposta utilizamos a autenticação por grupos, ou seja, cada grupo tem a sua própria lista de sites permitidos, conforme definido em reunião com os grupos componentes da Instituição/Organização, dessa forma, há um detalhe importante a se destacar, na interface de configuração do *Squid*, no menu ***Services – Proxy Server***, na aba "***Access Control***" há dois campos "***Whitelist***" e "***Blacklist***", estas duas opções de listas tem precedência sobre as demais liberações ou bloqueios que foram usadas no "**squid.inc**". Sendo assim, pode-se cadastrar os *sites* que serão liberados para os todos os grupos na ***Whitelist***, ou seja, os *sites* em comum a todos, restando a lista personalizada com os *sites* que são acessados por um grupo em específico.

3.5.5.4 Criação dos arquivos que definem os grupos e os sites para acesso

O próximo passo é criar e popular os arquivos referenciados nas ACL's de grupos e de *sites*. Como exemplo, a criação de ambos arquivos para o Grupo Comercial:

Navega-se no menu ***Diagnostics - Edit File***. No campo que aparece digita-se: **"/var/squid/acl/usuarios_comercial.acl"** e clica-se no botão **"*Load*"**. O pfSense vai exibir uma mensagem avisando que o arquivo não existe: **"*File does not exist or is not a regular file.*"**. Ignorando essa mensagem e deve-se povoar o arquivo com o nome do usuário do departamento Comercial, no caso **"joao"**. Se houver mais de um usuário por Seção/Setor, mantêm-se sempre o padrão de um usuário por linha. Ao término do processo clica-se em **"*Save*"**. A mensagem de arquivo inexistente irá ser alterada para **"*File Save Sucessfully*"**, informando que o arquivo agora existe e que foi criado com sucesso. (Figura 35).

FIGURA 35 – CRIAÇÃO DO ARQUIVO DO GRUPO ASSOCIANDO AO USUÁRIO
FONTE: PFSENSE FIREWALL

O processo acima é executado da mesma forma para criar o arquivo que irá conter a lista dos sites liberados para o grupo. Digita-se: **"/var/squid/acl/sites_comercial.acl"**. Nesse arquivo mantêm-se o padrão de um *site* cadastrado por linha. (Figura 36).

FIGURA 36 – CRIAÇÃO DO ARQUIVO CADASTRO DE SITES POR GRUPO
FONTE: PFSENSE FIREWALL

Os dois processos acima devem ser repetidos para todos os grupos da Instituição/Organização existentes e cadastrados.

3.5.5.5 Configuração do *cache* do *Squid* no pfSense

Uma importante configuração são as opções de *cache* do pfSense, pois é através desse recurso que o *Squid* armazena em *cache* o conteúdo acessado, de forma que se algum *host* fizer novamente uma requisição ao mesmo conteúdo, que já se encontra armazenado, ele recebe diretamente do *cache*, sem a necessidade de efetuar uma nova busca de dados na Internet. O uso desse recurso pode trazer uma rapidez maior ao acesso à Internet, pois provavelmente o *link* do *host* com o *Proxy* é bem mais rápido do que deste com a Internet. Para esta configuração navega-se em **Serviços - *Proxy Server* – aba *Cache Mgmt***, onde encontram-se as principais opções para configuração do *cache* do Proxy, segundo especificações do pfSense:

Hard disc cache size: 3000 (3GB). Tamanho total do *cache* que será armazenado no disco rígido;

Hard disk cache system: ufs (padrão). Sistema de arquivos que será usado pelo disco para armazenar os dados de *cache*;

***Hard disk cache location*:** "/var/squid/cache" (padrão). Local de armazenamento do *cachê*;

***Memory cache size*:** Tamanho reservado pelo sistema para alocar na memória os arquivos cacheados. No máximo 50% da capacidade de memória do servidor;

***Minimum object size*:** 0 (padrão);

***Maximum object size*:** opcional. Define o tamanho máximo de objetos em RAM para *cache*. Ex.: ao preencher o campo com 40000 (40MB) todos os arquivos e *downloads* com tamanho menor que 40MB será armazenado na memória até que a mesma fique cheia. Caso o arquivo tenha o valor maior que 40MB o mesmo será descartado pelo *Squid*;

***Maximum object size in RAM*:** quantidade de memória de objetos armazenados dentro da memória RAM do servidor. 32 objetos (padrão);

Low-water-mark in %: 90;

High-water-mark in %: 95;

Low e *High-water-mark* indicam a partir de qual porcentagem do tamanho total do *cache* o *Squid* começa a apagar os arquivos;

Memory Replacent Policy: a política de substituição de memória determina quais objetos são removidos da memória quando o espaço é necessário. A política padrão para troca de memória é GDSF;

***Do Not Cache*:** preencher com quais domínios ou IP's não serão cacheado pelo servidor.

3.5.6 Backup / Restauração das configurações do pfSense

Após todos os serviços instalados e configurados no *Firewall* faz-se necessário um *backup* de todas as configurações que estão ativas e em funcionamento na rede.

Para realizar o *backup* das configurações do pfSense, Navegua-se por **Diagnósticos, *Backup*/Restauração** e faz-se o *download* das configurações em XML que contém as configurações desejadas. É possível editar o arquivo XML com um bloco de notas a fim de realizar os ajustes necessários antes de realizar a restauração. Na caixa "Área de *backup*" pode-se selecionar uma configuração em específico ou todas as configurações do pfSense. (Figura 37).

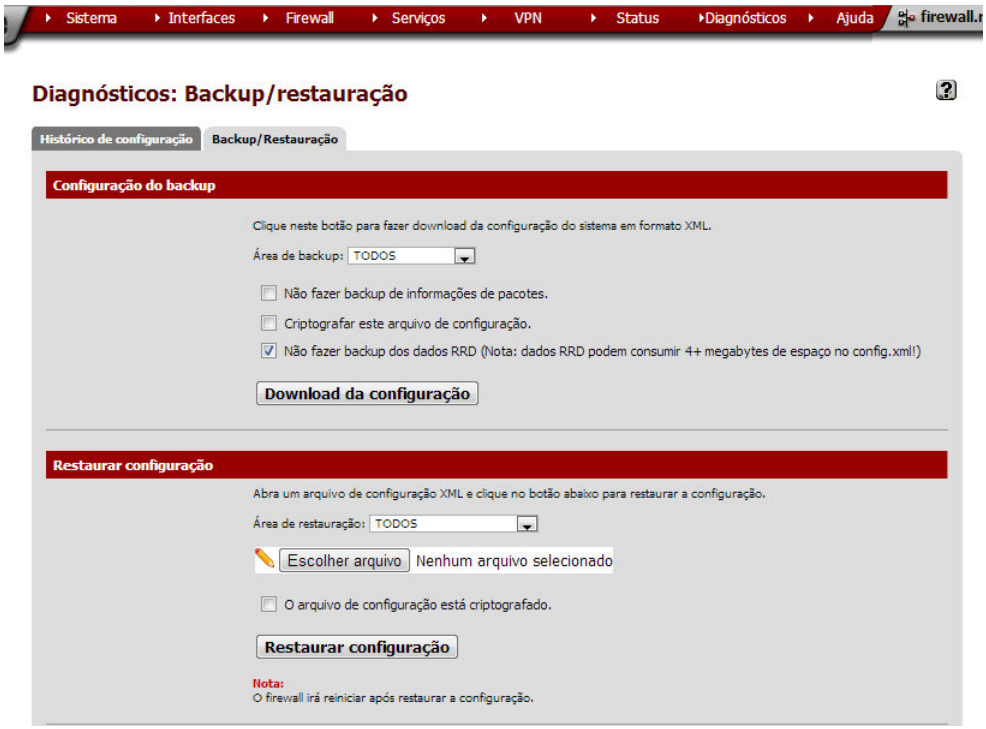


FIGURA 37 – CONFIGURAÇÃO BACKUP / RESTAURAÇÃO DAS CONFIGURAÇÕES DO PFSENSE
FONTE: PFSENSE FIREWALL

Na caixa “Área de restauração” pode-se restaurar exatamente a configuração especifica que deseja ou Todos. Caso seja feito alguma restauração em área incorreta, isto pode fazer com que o pfSense pare de funcionar visto que serão feitas alterações em locais incorretos.

3.5.7 Servidor de arquivos Samba

Esta é apenas uma opção do Administrador, realizar a instalação e configuração de um Servidor de Arquivos em uma máquina separadamente do *Firewall*, por uma questão de segurança, evitando o acesso de usuários ao *Firewall* da rede.

Para a instalação do Samba, como Servidor de Arquivos, pode ser feita em uma versão do *Ubuntu* modo gráfico ou em uma versão do *Debian* em modo texto puro. A escolha fica a critério do Administrador. Se a opção for pelo modo gráfico

pode-se utilizar o *Swat* (aplicativo de configuração em modo gráfico), caso seja em modo texto, o trabalho será feito através de comandos no terminal.

Nesta proposta, será utilizada uma versão do *Debian* em modo texto, uma instalação básica, sem recursos instalados, apenas o Samba.

Na configuração do Servidor de Arquivos será utilizado um PC com um processador Intel Core 2 2.80Ghz, com HD de 1 Tera, 1 Gb de memória e 1 placa de rede PCI 10/100/1000.

O Samba é composto por 3 Sessões:

[global] – contém as opções gerais do servidor.

[*share*] – indica o nome do compartilhamento – quantos desejar.

[*printers*] – compartilhamento de impressoras.

Para a instalação e configuração, segue-se os seguintes passos:

- Estando no modo gráfico, abre-se um terminal através das teclas Ctrl+Alt+t ou no menu **Aplicativos - Acessórios – Terminal**.

- Instalando o Samba:

Para realizar a instalação logue-se como *root*:

 # sudo su – (digita-se a senha de *root* quando solicitado)

 # apt-get install samba

- Editando o arquivo principal de configuração do Samba em /etc/samba/smb.conf

- inicialmente deve-se fazer uma cópia do arquivo smb.conf para preservar o original:

 # cp /etc/samba/smb.conf /etc/samba/smb.conf.bkp

- em seguida edita-se o arquivo smb.conf

 # vi /etc/samba/smb.conf

Uma observação, não se deve digitar os comentários ao final das linhas de configuração, pois se isso ocorrer o Samba passa a ignorar toda a linha. Os comentários devem ser colocados após o símbolo “#” e em uma linha acima do comando de configuração.

[global]

nome do grupo de trabalho

workgroup = grupo

```
  # nome dado ao servidor de arquivos
netbios name = arquivos
  # descrição do servidor
server string = servidor de arquivos samba

  [financeiro]
  # localização da pasta compartilhada
path = /home/arquivos/financeiro
# comentário descritivo do compartilhamento
comment = arquivos setor financeiro
# dá permissão de leitura e escrita no compartilhamento
writable = yes
# torna o compartilhamento visível (yes) ou oculto na rede (no)
browseable = yes
# somente o grupo financeiro e seus usuários tem acesso
valid users = +financeiro
# negando o acesso ao compartilhamento para um determinado usuário
invalid users = joao
```

Após alterar manualmente o arquivo "**smb.conf**" ou pelo *Swat* (aplicativo de configuração em modo gráfico) e desejar verificar se as configurações estão corretas, pode-se rodar o comando **testparm**. Ele funciona como uma espécie de debug, indicando erros grosseiros no arquivo e informando o papel do servidor na rede.

Depois de sair e salvar as alterações feitas no arquivo smb.conf, reinicia-se o serviço do Samba:

```
# /etc/init.d/smbd restart
```

Cadastrando os Usuários no Sistema e no Samba

Ao cadastrar usuários, deve-se fazê-lo tanto no Sistema, como no Samba. Pode-se criá-los com poderes "limitados" (não poderão acessar o servidor via SSH ou *Telnet*, evitando brechas na segurança) e ainda não criar no diretório home um diretório com o nome de cada usuário, como é o padrão do Samba:

 # adduser –disabled-login –no-create-home antonio

Caso o Administrador não deseje criar os usuários sem o home, pode-se criá-los da maneira padrão do Samba.

criar o usuário no sistema

 # adduser antonio

Após criar o usuário no sistema, deve-se cadastrá-lo no Samba:

 # smbpasswd –a antonio

Para realizar a manutenção das contas de usuário, estão disponíveis alguns comandos:

para desativar temporariamente a conta de um usuário

 # smbpasswd –d antonio

para reativar a conta de um usuário

 # smbpasswd –e antonio

para remover o usuário definitivamente

 # smbpasswd –x antonio

E em seguida, remove-se o usuário do sistema

 # deluser antonio

Criando Diretórios Compartilhados

Na sequência, deve-se criar os diretórios referentes aos compartilhamentos, normalmente é o mesmo nome da pasta compartilhada no arquivo smb.conf

 # mkdir /home/arquivos

 # mkdir /home/arquivos/financeiro

Criando Grupos

Para a criação de grupos (setores), é possível adicionar os funcionários (usuários) que pertencem aquele setor, melhorando assim a segurança dos dados compartilhados. É interessante que se crie grupos com o mesmo nome do compartilhamento.

 # groupadd financeiro

Adicionando Usuários aos Grupos

 # adduser antonio financeiro

É possível adicionar um mesmo usuário a mais de um grupo, se houver a necessidade, por exemplo, no caso do pessoal de TI.

Caso um determinado usuário (funcionário) deixou a Instituição/Organização, para eliminá-lo do grupo ao qual pertencia, basta executar o comando:

 # deluser antonio financeiro

Alterando Permissões de Acesso dos Usuários às Pastas

Após criar os grupos e adicionar os usuários a eles, deve-se ajustar as permissões de acesso da pasta, de forma que o grupo tenha acesso completo:

 # chgrp –R financeiro /home/arquivos/financeiro

 # chmod –R 775 /home/arquivos/financeiro

O "–R" atua de forma recursiva, ou seja, altera a permissão de todas às subpastas e arquivos.

Deve-se observar durante a atribuição das permissões dos usuários, o que se deseja que cada grupo possa realizar de tarefas em cada diretório:

0	-	nada	775	
1	-	execução	7 = 1+2+4	(root)
2	-	escrita	7 = 1+2+4	(grupo)
4	-	leitura	5 = 1+4	(outros)

Cabe algumas observações quanto as possíveis configurações a serem utilizadas no Servidor de Arquivos Samba:

- Não foi utilizada na configuração [global] a opção **security = user** pois o Samba já o assume por padrão a partir da versão 3.

- A questão dos nomes dos arquivos. No Windows, os nomes de arquivos são salvos da forma como foram digitados pelo usuário, preservando os caracteres maiúsculos e minúsculos. Entretanto, o sistema é case insensitive, de forma que não diferencia um arquivo chamado "Trabalho.txt" de outro chamado "trabalho.txt".

A solução para isso é orientar o Samba a salvar todos os arquivos em caracteres minúsculos, adicionando-se a seguinte linha na configuração [global]:

 # preserve case = no

 # default case = lower

- Outra questão é quando o usuário ao digitar o login o faz com um dos caracteres em maiúsculo e o resto em minúsculo ou todo ele em maiúsculo, fazendo com que o Linux recuse o login. Uma forma de evitar isso no Samba é usar a opção:

 # username level = 2

Esta opção faz com que o Samba verifique várias combinações de maiúsculas e minúsculas, caso o *login* seja recusado pelo sistema.

- Em caso de conflito direto entre uma regra definida na seção [global] e outra definida num dos compartilhamentos, a regra definida na seção [global] tem precedência.

3.6 OUTRAS OPÇÕES DE SEGURANÇA DO PFSENSE

Além de alguns serviços mostrados anteriormente, o pfSense disponibiliza ainda duas outras opções de configuração a serem acrescentadas, caso julgadas necessárias, que tornarão uma rede mais segura e eficiente.

Nesta proposta não será detalhado sobre os dois próximos assuntos, mas nem por isso deixam a desejar em sua utilização. Há possibilidade de configuração dentro do pfSense de camadas de segurança extras, como DMZ e VLAN.

3.6.1 DMZ

Muitas vezes a empresa possui um servidor de *Web*, um Servidor de *email*, ou qualquer tipo de servidor que será disponibilizado para acesso via Internet por clientes, funcionários ou até mesmo usuários anônimos. Nestes casos, a preocupação com o acesso externo aumenta bastante, por não saber quem são e quais serão as intenções das pessoas que farão esse acesso.

Nos casos de serviços disponibilizados ao público via Internet, deixar esses servidores dentro da rede privativa não é uma boa escolha, pois ao acessar tal recurso, os usuários, muitas vezes anônimos, estarão também navegando dentro da rede. Uma opção neste caso é colocar o servidor fora da rede privativa, evitando assim esses acessos indesejados que colocariam a rede interna (LAN) em risco. Colocar os servidores de Web fora da rede privativa e ainda assim controlar o acesso aos seus recursos, de forma que eles fiquem protegidos de eventuais ataques é possível.

Através da DMZ (Rede Desmilitarizada), uma segunda rede criada no *Firewall* para hospedar apenas os serviços que serão acessíveis pela Internet, evitando assim que, para acessar esses serviços, usuários anônimos entrem na rede privativa (LAN) e coloque em risco seus dados particulares. Normalmente para se criar uma DMZ é preciso pelo menos uma placa de rede extra no *Firewall*, uma para a WAN, outra para LAN e uma para a Rede de Perímetro (DMZ). (Figura 38).

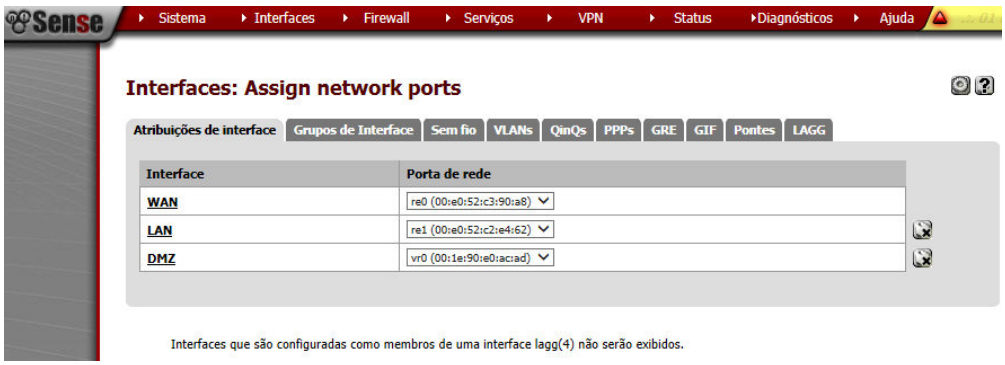


FIGURA 38 – CONFIGURAÇÃO DE DMZ NO PFSENSE
FONTE: PFSENSE FIREWALL

3.6.2 VLAN

A VLAN permite que um único interruptor físico possa hospedar varias camadas de rede, separando as portas com *tags* VLAN. A *tag* de VLAN define uma rede virtual separada. O pfSense pode anexar em cada VLAN, definindo *tags* nas interfaces do *Firewall*.

Todos os pacotes destinados ou originados de VLAN serão marcados com a *tag* VLAN. É assim que o pfSense os diferencia dos outros tráfegos, garantindo que esse tráfego vá para o lugar certo. (Figura 39).

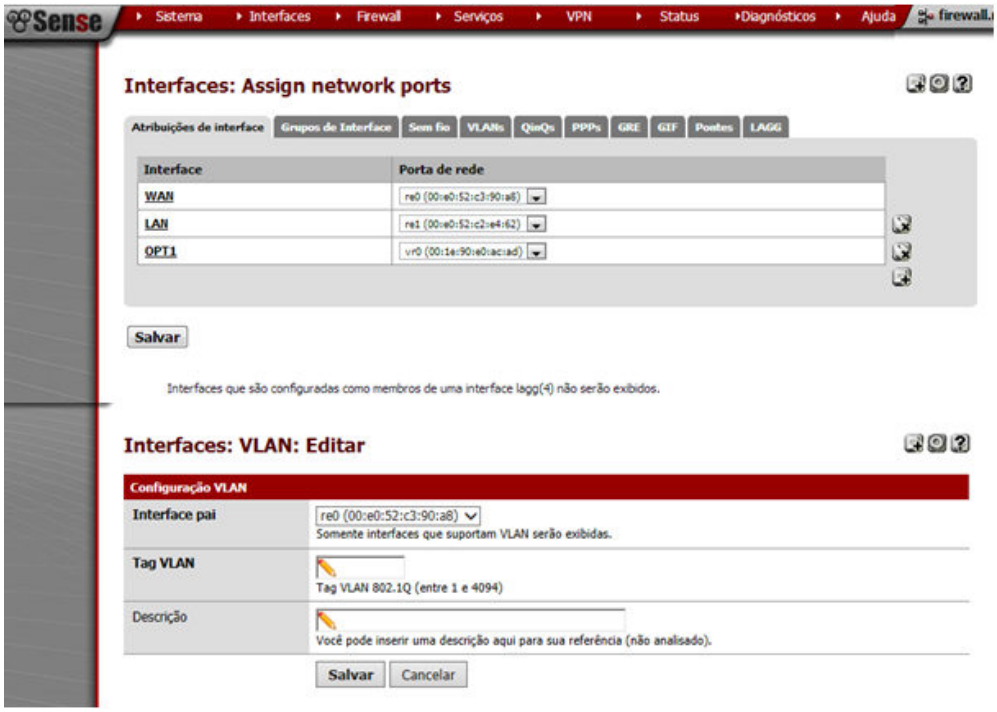


FIGURA 39 – CONFIGURAÇÃO DE VLAN NO PFSENSE
FONTE: PFSENSE FIREWALL

3.7 A SEGURANÇA DO TERMINAL DO USUÁRIO

Visando garantir a segurança da rede, do trabalho realizado pelos usuários e o plano de migração para *software* livre, sugere-se que os terminais utilizados dentro da rede tenham instalado a versão Linux *Ubuntu* 10.04 básica, ou seja, somente com as ferramentas que o usuário necessita para realizar seu trabalho dentro da Instituição/Organização.

Também, a colocação de senha no *setup* de todos os terminais, evitando assim que o usuário habilite a utilização do drive de DVD que deve estar desabilitado.

A instalação de lacres em todos os gabinetes do parque de máquinas da Instituição/Organização, evitando assim, casos de substituição de peças sem o

conhecimento da equipe de TI ou mesmo dano a algum dos componentes do equipamento.

Um dos pontos que exige cuidado dentro da rede é a possibilidade de um usuário mal intencionado retirar documentos digitais, por meio de *pendrive*, HD externo ou mesmo celular, que não devem ser de conhecimento de outras pessoas, algumas vezes sem ter a intenção de prejudicar a Instituição/Organização, apenas copiando para uma *pendrive* esses arquivos. Mas, e se o usuário perder essa *pendrive* e alguém de fora da Instituição/Organização encontrar? Dessa forma, uma alternativa segura é desabilitar as conexões USB dos terminais, sem comprometer o uso de teclado e mouse USB.

Para a execução dessa tarefa, deve-se editar o arquivo **blacklist.conf** (em qualquer versão *Ubuntu*) no caminho "**/etc/modprobe.d**" e ao final do arquivo digitar a seguinte linha: "***blacklist usb_storage***" (sem aspas). É interessante que se acrescente um comentário para identificar o que essa linha de comando vai executar. Dessa maneira, qualquer dispositivo de armazenamento que for conectado ao terminal, via conexão USB, não será reconhecido pelo sistema.

3.8 A SEGURANÇA DOS DISPOSITIVOS MÓVEIS

Às vezes, uma boa política de segurança móvel inclui dizer não a certas situações.

Como parte da política de segurança pode-se proibir o uso de *notebooks* e *pendrives* pessoais. Se a Instituição/Organização possuir algum desses dispositivos móveis, por questões de segurança, a equipe de TI deve ter um maior controle sobre os mesmos e quem os utiliza.

Uma boa prática a ser adotada é a criação de *containers* de segurança através do ***Truecrypt***, um *software* gratuito e de código aberto para esconder seus arquivos confidenciais, com foco na privacidade e segurança. Com ele é possível criar um drive virtual criptografado para proteger os seus arquivos de qualquer pessoa que queira acessá-los sem a sua permissão.

Assim, utilizando-se dessa ferramenta é possível criar um container seguro tanto no HD do *notebook*, quanto na *pendrive* e dentro destes armazenar todas as

informações da Instituição/Organização em segurança, principalmente se os usuários utilizarem esses dispositivos móveis em viagens à negócio, onde o risco de roubo ou perda é grande.

Alguém pode dizer, mas o equipamento pode ser roubado. Sim, pode, mas mesmo que seja roubado, a possibilidade de se quebrar essa criptografia é mínima, o que ainda garantiria a segurança das informações que foram roubadas.

4 CONSIDERAÇÕES FINAIS

Pode-se dizer que não existe segurança absoluta, tornam-se necessárias ações no sentido de descobrir quais são os pontos vulneráveis e a partir daí avaliar os riscos e impactos, e rapidamente providenciar para que a segurança da informação seja eficaz.

Infelizmente o que se vê na prática é que muitas empresas não dão o devido valor a esta questão e por muitas vezes o preço é muito alto, portanto, o melhor caminho é reduzir ao máximo quaisquer riscos às informações, seguindo um trajeto no sentido único de manter a integridade e a disponibilidade dos sistemas de informação. Para implantar uma eficaz segurança da informação dentro de uma Instituição/Organização deve-se ficar atento para algumas questões como uma boa análise de riscos, a definição da Política de Segurança e por fim um plano de contingência.

A análise de riscos basicamente visa à identificação dos pontos de riscos a que a informação está exposta, identificando desta maneira quais os pontos que necessitam de maior empenho em proteção. A política de segurança da informação é a formalização explícita de quais ações serão realizadas em um sentido único de garantir a segurança e disponibilidade dos mesmos, esta política é de extrema importância uma vez que descreve as regras necessárias para o uso seguro dos sistemas de informação. Os planos de contingência também possuem papel fundamental, pois descrevem o que deve ser feito em caso de problemas com as informações.

Nota-se que normalmente as pessoas são o elo mais frágil quando o assunto é segurança da informação, as soluções técnicas não contemplam totalmente sua segurança, desta forma torna-se necessário que os conceitos pertinentes a segurança sejam compreendidos e seguidos por todos dentro da organização, sem distinção de níveis hierárquicos.

Uma vez identificados quais os riscos que as informações estão expostas deve-se imediatamente iniciar um processo de segurança física e lógica, com o intuito de alcançar um nível aceitável de segurança. Quando se fala em nível aceitável de segurança, refere-se ao ponto em que todas as informações devam

estar guardadas de forma segura. Não se pode deixar de lembrar casos em que senhas e outros dados pessoais de usuários de algum sistema acabam sendo expostos na web. Quem é o culpado de tudo isso? A resposta é simples: a empresa a qual os usuários depositavam a sua confiança.

Corporativamente, muito é gasto em *hardware*, *software*s, firewalls, encriptação, dispositivos de acesso seguro, etc., mas, é muito importante notar que uma vez que os usuários desses sistemas são humanos, com todas as suas limitações humanas, este ainda é o elo mais fraco na segurança da informação. Logo, não é demais repetir: atente para seu comportamento seguro no uso das redes de computadores, pois o "fator humano" é, de fato, um importante componente da segurança.

REFERÊNCIAS

ABNT NBR ISSO/IEC 27001. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação - Requisitos**. Disponível na Internet: http://www.abntonline.com.br/consultanacional/projetodet.aspx?ProjetoID=13438&FileID=13798. Acesso em Outubro de 2013.

ABNT NBR ISSO/IEC 27002. **Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação.** Disponível na Internet: http://www.abntonline.com.br/consultanacional/projetodet.aspx?ProjetoID=13439. Acesso em Outubro de 2013.

ABNT NBR ISO/IEC 17799:2005 – **Tecnologia da informação – Técnicas de Segurança – Código de Prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005, 120pp.

ABNT NBR ISO/IEC 27001:2006 – **Tecnologia da informação – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2006, 34pp.

Cartilha de Segurança para Internet. Disponível na internet: http://cartilha.cert.br. Acesso em Outubro de 2013.

Dicionário de Informática Online – **Glossário e Termos de Informática**. Disponível na Internet: http://www.dicweb.com. Acesso em Outubro de 2013.

Firewall pfSense. **pfSense 2.1.** Disponível na Internet: http://www.pfsense.org.br. Acesso em Outubro de 2013.

HOUAISS, 2001 – **Dicionário Eletrônico Houaiss da Língua Portuguesa.** (CD-ROM). Objetiva, 2001.

Incidentes de Rede. Disponível na Internet: http://www.cert.br/stats/incidentes. Acesso em Outubro de 2013.

ISO/IEC 17799, renumerada em julho de 2007 para ISO/IEC 27002, é uma norma de Segurança da Informação – revisada em 2005 pelas referidas organizações ISO e IEC – composta por um conjunto de recomendações para práticas na gestão de Segurança da Informação, ideal para aqueles que querem criar, implementar e manter um sistema de segurança.

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

MENDONÇA, Tales Araújo. **GNU/Linux: aprenda a operar o sistema na prática.** São Paulo: Editora Viena, 2009.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva.** Rio de Janeiro: Editora Campus, 2003.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores das LANs, MANs e WANs às Redes ATM** (2ª Edição – 12ª tiragem). Rio de Janeiro: Editora Campus, 1995.

Software Livre. Projeto GNU. Disponível na Internet: http://www.gnu.org/philosophy/free-sw.pt-br.html. Acesso em Outubro de 2013.