**FACULDADE DE TECNOLOGIA DE AMERICANA**

**Curso Superior de Tecnologia em Segurança da Informação**

Robson José Carvalho

# SEGURANÇA DA INFORMAÇÃO DE PEQUENAS E MÉDIAS EMPRESAS:

## Proposta de implantação de firewall

**Americana, SP**

**2015**

**FACULDADE DE TECNOLOGIA DE AMERICANA**

**Curso Superior de Tecnologia em Segurança da Informação**

Robson José Carvalho

# SEGURANÇA DA INFORMAÇÃO DE PEQUENAS E MÉDIAS EMPRESAS:

## Proposta de implantação de firewall

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação da Prof.(a) Me. Maria Elizete Luz Saes.

Área de concentração: Firewall

**Americana, SP**

**2015**

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS**
**Dados Internacionais de Catalogação-na-fonte**

Carvalho, Robson José
C327s Segurança da Informação de pequenas e médias empresas: proposta de implantação de firewall. / Robson José Carvalho. – Americana: 2015.
36f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Maria Elizete Luz Saés

1. Segurança em sistemas de informação I. Saés, Maria Elizete Luz II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Robson José Carvalho

# SEGURANÇA DA INFORMAÇÃO DE PEQUENAS E MÉDIAS EMPRESAS:

## Proposta de implantação de firewall

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação da Prof.(a) Me. Maria Elizete Luz Saes.
Área de concentração: Firewall

Americana, 09 de dezembro de 2015

**Banca Examinadora:**

Maria Elizete Luz Saes
Mestre
FATEC Americana

Silvia Aparecida José e Silva
Mestre
FATEC Americana

Juliane Borsato Beckedorff Pinto
Graduada
FATEC Americana

# AGRADECIMENTOS

A professora Maria Elizete Luz Saes, pela orientação, apoio e confiança.

Agradeço a todos os professores por me proporcionaram o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender. A palavra mestre, nunca fará justiça aos professores dedicados aos quais sem nominar terão os meus eternos agradecimentos.

# DEDICATÓRIA

Aos meus pais, irmãos, minha esposa Greice, meu filho e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

# RESUMO

Este trabalho traz de maneira funcional e prática aspectos da segurança da informação, aprofundando-se em firewalls, tipos, características, funcionalidades, recursos e diferenças, utilizando-se da ferramenta de código aberto Endian Firewall Community (EFW) em um estudo de caso realizado com o auxílio da ferramenta de virtualização VirtualBox da Oracle, com recursos de DHCP (Dynamic Host Configuration Protocol), VPN (Virtual Private Network), Proxy e outros.

**Palavras-chave:** Endian. Firewall. Segurança da Informação

# ABSTRACT

This paper presents a functional way and practice aspects of information security, deepening in firewalls, types, features, functionality, features and differences, using the open source tool Endian Firewall Community (EFW) in a conducted case study with the help of Oracle VirtualBox virtualization tool, with features DHCP (Dynamic Host Configuration Protocol), VPN (Virtual Private Network), Proxy and others.


***Keywords:*** Endian. Firewall. Information Security.

# LISTA DE ILUSTRAÇÕES

Figura 1 - Ataques anuais acumulados .....13
Figura 2 - Posicionamento estratégico do firewall para controle de tráfego da rede .16
Figura 3 - Comparação entre os modelos de camadas OSI e TCP/IP .....20
Figura 4 - Posicionamento das chains no processo .....21
Figura 5 - O vermelho indica o tunelamento e o verde o tráfego encriptado em uma rede VPN.....25
Figura 6 - Principais funcionalidades do EFW.....28
Figura 7 - Topologia de rede adotada pelo Endian Firewall .....30
Figura 8- Atual estrutura da rede Alimentos Personalizados SA. .....32

# SUMÁRIO

INTRODUÇÃO ..... 10
1 SEGURANÇA DA INFORMAÇÃO ..... 12
2 FIREWALL ..... 15
2.1 Características do Firewall ..... 16
2.2 Tipos de *Firewall* ..... 17
2.3 RECURSOS DE UM *FIREWALL* ..... 18
*2.4 IPTABLES* ..... 20
2.5 DHCP ..... 23
*2.6 Failover* ..... 23
2.7 IDS ..... 23
2.8 VPN ..... 24
3 ESTUDO DE CASO: Endian Firewall Community ..... 27
3.1 Funcionalidades do EFW ..... 27
3.2 A aplicação do EFW ..... 30
4 CONSIDERAÇÕES FINAIS ..... 33
REFERÊNCIAS ..... 34

# INTRODUÇÃO

Tomada de decisões, controle de processos e outros termos associados à tecnologia da informação já não fazem parte apenas de grandes ambientes corporativos, eles estão cada vez mais presentes no cotidiano das pequenas e médias empresas. A competitividade e a necessidade de se manter no mercado as fazem enfrentar novos paradigmas como, por exemplo, gerar e manter informações de suas atividades internas e externas. Essas informações devidamente colhidas, armazenadas e disponibilizadas, tornam-se uma base segura para obtenção de conhecimentos estratégicos e de sobrevivência tanto no mercado atual quanto no futuro.

Neste contexto de competitividade, sobrevivência e geração de conhecimento de mercado, a informação se torna uma aliada fundamental. No mercado de hoje as pequenas e médias empresas veem a necessidade de investir em sistemas computacionais que possuem capacidade de manipular grandes quantidades de dados simultaneamente, além de precisão e velocidade, assim proporcionando importantes vantagens no mercado.

Com a busca cada vez maior por tecnologia, há no mercado uma disseminação muito grande de sistemas informatizados. Uma empresa pode começar controlando apenas suas vendas e estoque, e depois pode evoluir, ao agregar novos módulos, como controle de produção, controle financeiro, auditoria, entre outros.

Uma ferramenta que precisa estar na alça de mira das empresas é a Internet, que proporciona agilidade no atendimento e contato com clientes e fornecedores, além de outros benefícios como pesquisas de mercado, integração dos funcionários com a empresa e escritórios remotos, tornando-se, assim, uma ferramenta cada vez mais essencial para a sobrevivência do negócio.

Fica evidente a importância desses sistemas para as empresas, mas temos que assegurar o bom funcionamento dos mesmos. As informações devido a sua importância precisam estar seguras e disponíveis apenas para as pessoas certas, já a Internet deve ser usada de maneira cautelosa, pois é uma porta para a entrada de programas maliciosos e roubo de dados.

Para garantir o compartilhamento seguro, a integridade dos dados, a integração das empresas com suas unidades via trabalho remoto, devem ser feitos por instrumentos tecnológicos específicos para tais funções. Para atender essa

necessidade existem ferramentas proprietárias e gratuitas, um bom exemplo de solução que deve estar presente em todas as redes bem planejadas é o *firewall.*

O firewall é uma solução de segurança, que pode ser baseada em hardware ou software, a partir de um conjunto de regras, analisa o tráfego que passa por ele determinando quais operações de transmissão ou recepção podem ou não ser executadas. O *firewall* poderia ser interpretado como uma barreira de defesa cuja missão é barrar o tráfego indesejado e liberar o bem-vindo.

Inicialmente será apresentado informações sobre a Segurança da Informação, apresentado conceitos sobre o que é um *firewall*, os tipos existentes e suas características. Também será apresentado alguns recursos que podem ser utilizados junto com firewalls, como DHCP, *WEB Proxy*, IDS, *Failover*, VNP e outros. Posteriormente um estudo de caso utilizando a ferramenta Endian Firewall Community com os recursos apresentado em um ambiente de uma empresa de médio porte na busca de satisfazer necessidades que surgem com o crescimento e informatização da empresa.

# 1 SEGURANÇA DA INFORMAÇÃO

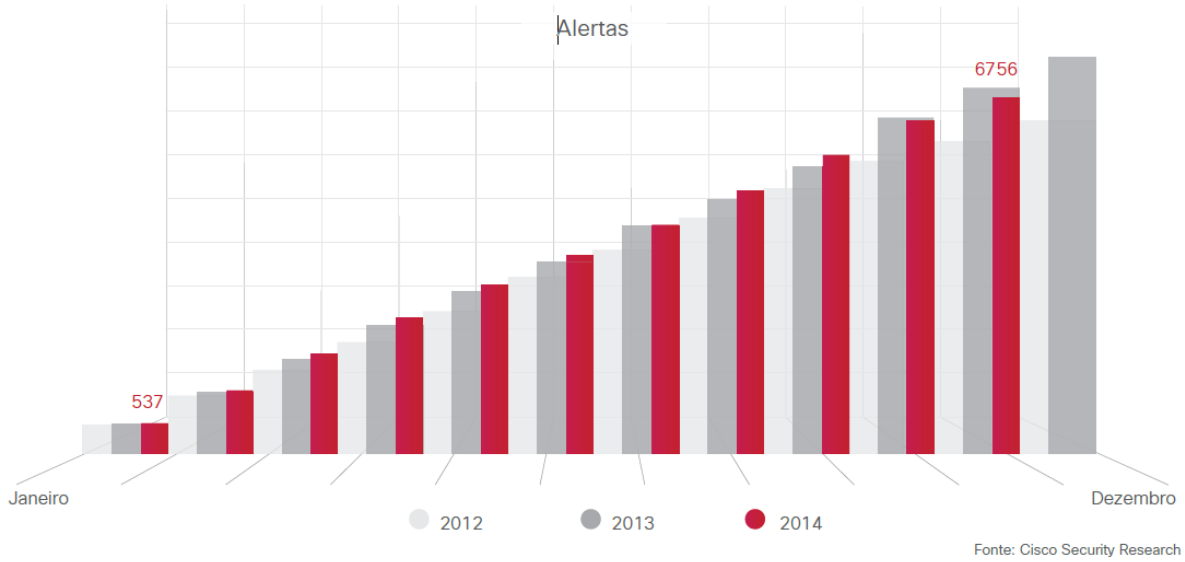
Há tempos quando as informações eram armazenadas em papel, realizar a segurança das mesmas era relativamente fácil, bastava trancar os documentos em algum lugar e restringir o acesso físico a ele. Com o passar do tempo, essas informações passaram a ser informatizadas e com isso também surgiu a necessidade de que elas estivessem disponíveis, íntegras e com acesso somente a pessoas devidamente autorizadas. Dessa forma, torna-se necessário realizar a segurança dessas informações, que cada dia ganha mais valor e importância, ainda mais no ambiente corporativo.

Ferreira afirma que a segurança da informação é formada por três pilares. A confidencialidade é o pilar que limita o acesso a informação às entidades e pessoas autorizadas pelo proprietário da informação. A integridade é o pilar que garante que a informação manipulada mantenha todas as características originais, controlando as mudanças e garantindo o ciclo de vida da informação, desde seu nascimento, passando por sua manutenção até sua destruição. O último pilar, a disponibilidade, garante que a informação esteja sempre disponível para uso das entidades, pessoas autorizadas pelo proprietário da informação.

Para se ter uma segurança da informação eficaz e eficiente é preciso mais do que apenas um bom antivírus, um firewall *e patches* de segurança aplicados. O profissional que trabalha com segurança da informação deve estar atento a outros itens como determinação de políticas, normas, procedimentos, controles de acesso (físico e lógico), auditoria, criptografia, gerenciamento de incidentes, continuidade de negócios, entre tantos outros aspectos (MAIA, 2013).

Quando se fala em ameaças à informação, para muitos o que vem à mente são acontecimentos como o de Edward Snowden (G1 2013), que trouxe a público vários detalhes sobre sistemas de vigilância global. O Relatório Anual de Segurança da Cisco (2015), revela que as ameaças voltadas para obter proveito da confiança do usuário nos sistemas, aplicações e redes pessoais atingiram níveis alarmantes, porém inferiores ao ano de 2013, sendo 2014 a primeira vez que esse número diminui, conforme gráfico apresentado na figura 1.

**Figura 1 - Ataques anuais acumulados**




Fonte: Cisco Security Research

O mesmo relatório ainda traz alguns pontos muito importantes em relação a ameaças à informação, como, por exemplo, o aumento das vulnerabilidades do cliente no Adobe Flash Player e no Microsoft IE (Internet Explorer), tirando a liderança do Java.

Em se tratando de ameaças à rede interna é possível citar alguns casos de ameaças/vulnerabilidades, conforme aponta Watchguard (2009):

(i) Ataques Internos

A Verizon's Intrusion Response Team investigou 500 casos de intrusões em quatro anos e pode atribuir 18% das brechas e violações a funcionários, sendo a metade deles surgidas na própria equipe de TI.

(ii) Uso indevido da Internet pelos funcionários

Muitos funcionários usam a Internet para acessar *blogs*, sites de jogos online, redes sociais e até mesmo sites pornográficos, que podem ser um abrigo muito grande para pragas virtuais – *trojans, spyware, malware, keyloggers* e outros - o usuário estaria convidando essas pragas para a rede da empresa.

(iii) E-mail maliciosos

Talvez seja essa a forma mais comum de *phishing*, na qual o usuário recebe um e-mail, normalmente com alguma promoção ou comunicado, as vezes basta um clique para desencadear um *download* de programas maliciosos.

# 2 FIREWALL

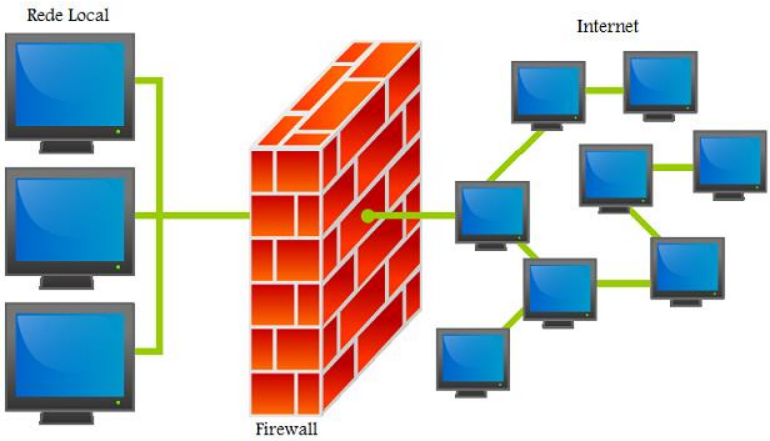
A argumentação mais comum para a utilização de um *firewall* é a proteção da rede interna de uma empresa contra acessos não autorizados, oriundos de uma rede externa, normalmente a Internet. Contudo, um *firewall* pode ir além dessa tarefa. Em muitos casos, o *firewall* desempenha funções mais sofisticadas. Além de impedir esses acessos provenientes de ambientes externos, é utilizado para impedir que máquinas internas acessem computadores e/ou serviços externos duvidosos ou proibidos, podendo impedir também que usuários enviem, para além dos limites da empresa, informações inerentes às atividades produtivas, financeiras ou estratégicas da empresa.

Um aspecto muito importante de um *firewall* é permitir que o administrador da rede possa implementar uma política de controle de acessos. Atuando como um filtro de pacotes e serviços baseado em regras definidas pelo administrador, o *firewall* age como controlador de rede e tem poder de definir quais acessos, sejam eles internos ou externos, podem ser ou não aceitos.

Um *firewall*, com características voltadas para redes empresarias, normalmente é uma máquina exclusivamente designada para este fim. No momento da implantação, a empresa pode optar por dois tipos de *firewall*: o disponibilizado apenas em software, através de programas comerciais ou de código livre ou ainda os nomeados de *appliance*, constituídos de hardware e software devidamente desenvolvidos para tal função.

Posicionado em um ponto estratégico da rede e devidamente configurado, o *firewall* torna-se uma importante ferramenta de segurança, controle, monitoramento, auditoria e integração entre redes de computadores (MACEDO, 2012), conforme apresentado na figura 2.

**Figura 2 - Posicionamento estratégico do firewall para controle de tráfego da rede**




Fonte: Disponível em http://www.diegomacedo.com.br/como-funciona-um-firewall/

## 2.1 Características do Firewall

A grande maioria dos *firewalls* é alicerçada em cinco características:

(i) Roteamento e Filtragem de Pacotes que, baseado em regras definidas, atua de maneira seletiva na liberação ou negação da passagem de pacotes de dados;

(ii) NAT (*Network Address Translation*) que realiza o mascaramento dos endereços IP e permite o compartilhamento da Internet para a rede interna;

(iii) Servidores *Proxy* que policiam a camada de aplicação da rede intermediando as relações entre os pontos internos e externos;

(iv) Autenticação segura e criptografada de usuários que acessam a rede localmente e remotamente;

(v) VPN (*Virtual Private Network*) que é uma rede virtual segura que utiliza uma terceira rede pública, normalmente a Internet, para interligar duas ou mais redes privadas.

Macedo (2012) classifica os *firewalls* em três tipos: filtro de pacotes, filtro de pacotes com controle de estados e proxy de aplicação:

(i) Filtro de Pacotes: Neste tipo de *firewall* os controles de permissão e negação de tráfego são baseados nas portas de comunicação e nos endereços de origem e destino. Por padrão, todo o tráfego é inicialmente bloqueado e o administrador da rede permite a passagem de pacotes de acordo com as reais necessidades da rede local.

(ii) Filtros de pacotes com Controle de Estados: É uma evolução do filtro de pacotes tradicional. Com um controle de estados das conexões, este tipo de *firewall* consegue saber qual o estado atual de determinada conexão e se um pacote é recebido fora do contexto atual ele é rejeitado.

(iii) *Proxy* de Aplicações: Atuando na camada de aplicação do modelo OSI, o *Proxy* de aplicação é um intermediário entra a máquina solicitante e o servidor. Ele recebe todas as requisições do cliente e examina o pacote baseado em seu conteúdo. Caso o conteúdo não esteja previsto nas permissões definidas o pacote é rejeitado.

## 2.2 Tipos de *Firewall*

É possível citar alguns tipos de *firewall*, como as opções pagas ou proprietárias quanto as opções de software livre, Microsoft ISA Server, IPCop Firewall, Endian Community Firewall entre outros.

O Microsoft ISA Server é um *firewall* de múltiplas camadas, inclui também os serviços de *Web Proxy* e VNP, proporcionando assim uma proteção contra ameaças vindas da internet. Proporciona também a facilidade de gerenciamento através de integração com o Windows Server. Trata-se de um software proprietário, ou seja, é preciso um investimento para poder utilizá-lo.

O IPCop Firewall é uma solução de *firewall*, que oferece serviços como DNS dinâmico e estático, DHCP, VPN, sistema de prevenção de intrusão (IDS) e

administração via web. Trata-se de um software livre, ou seja, não é preciso um investimento para poder utilizá-lo.

Dentre os softwares livres destaca-se o Endian Firewall Community, desenvolvido pela empresa italiana Endian, usando como base o IPCop Firewall, que oferece todos os recursos que o IPCop e mais alguns como e-mail antivírus e *anti-spam*, ponto de acesso sem fio, suporte a VoIP, servidor NTP e outros.

## 2.3 RECURSOS DE UM *FIREWALL*

Para que a comunicação entre duas ou mais pessoas ocorra é imprescindível estabelecer uma linguagem comum. Não existe a comunicação sem que códigos ou linguagens sejam previamente estabelecidas e adotadas. Em uma rede de computadores isto não é diferente e estes códigos de comunicação são chamados de protocolos. É através dos protocolos de comunicação que os dados são transmitidos, recebidos e entendidos pelos computadores pertencentes a uma rede.

Os protocolos de rede são constituídos por uma sequência hierárquica de camadas ou níveis sobrepostos, semelhante a uma pilha, cuja camada, por meio de uma interface, oferece informações e serviços para a camada imediatamente superior ou inferior. Os serviços que estão dispostos na mesma camada em máquinas diferentes são chamados de pares e são estes pares que, utilizando o protocolo, realizam a comunicação. Os pares não se comunicam diretamente. Os dados as informações de controle são transferidos para a camada imediatamente inferior até chegar ao meio físico.

O modelo de protocolo em camadas é normalmente explicado utilizando-se o modelo OSI (*Open System Interconnection*). Uma introdução a esta modelagem é útil para os profissionais que trabalham em rede, em particular para os que administram firewalls.

O modelo OSI (*Open System Interconnection*) é conhecido como modelo de padronização de tecnologias de redes de computadores e serviu de base para a indústria do segmento. Desenvolvido pela ISO (*International Standards Organization*) ele possui sete camadas hierárquicas.

A camada física é o meio físico de comunicação em que a rede está inserida. É nesta camada que estão definidas especificações como voltagens, sequência de pinos, conversão elétrica e conversão ótica.

Dotada de mecanismos de detecção e correção de erros, a camada de enlace tem como objetivo transformar a informação em quadros a serem transmitidos de maneira confiável pela camada física. Os endereços de MAC (*Media Access Control*) são utilizados nesta camada para distinguir e permitir a comunicação entre os diferentes adaptadores de rede.

A camada de rede fornece a conectividade entre os pontos de redes diferentes. É nessa camada que ocorrem o roteamento e endereçamento de pacotes. Os protocolos IP (*Internet Protocol*) e ARP (*Address Resolution Protocol*) estão presentes nesta camada.

É na camada de transporte que atuam os protocolos TCP e UDP. Esta camada é normalmente responsável pela integridade dos dados. Ela divide os dados recebidos da camada acima e gera os pacotes a serem transmitidos para o destino. A mesma camada no receptor é a responsável pela junção e remontagem correta dos pacotes recebidos.

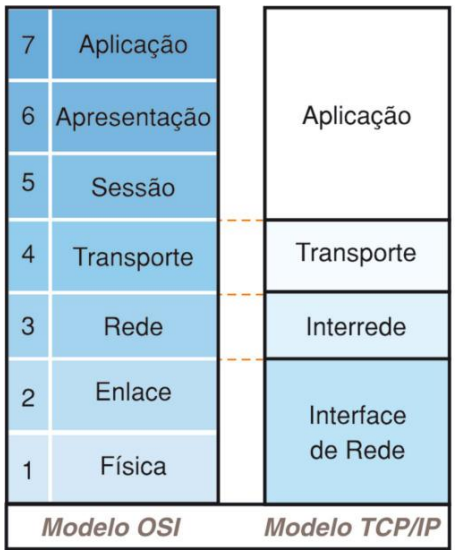
Esta é a camada responsável por iniciar, gerenciar, sincronizar e terminar a comunicação.

A camada de apresentação é responsável por manter um formato universal que possa ser entendido por cada aplicativo da rede e pelos computadores. É nesta camada que são realizadas a criptografia ou a decodificação de dados.

Esta é a camada que realiza a interface entre a os processos de comunicação de rede e as aplicações utilizadas pelo usuário. É nesta camada que atuam os protocolos HTTP, SMTP e FTP.

O protocolo TCP/IP, desenvolvido como uma solução para a interconexão de várias redes diferentes, tornou-se o padrão mais utilizado na Internet e nas redes internas. Baseado no modelo OSI, o TCP/IP, acrônimo que faz referência aos seus dois principais protocolos de origem, não tem as sete camadas definidas pelo modelo OSI. Ele possui apenas quatro camadas.

**Figura 3 - Comparação entre os modelos de camadas OSI e TCP/IP**




Fonte: Disponível em http://www.mecatronicaatual.com.br/educacao/1442-ethernet-industrial-parte-4-protocolos-industriais

Os *firewalls* podem oferecer diversos recursos que podem ser utilizados para o melhoramento contínuo da segurança da informação de empresas, dentre todos esses recursos estão *Web Proxy*, normalmente fazendo o uso do Squid, acesso SSH, serviço de DHCP, redirecionamento de portas, IDS e VPN.

## *2.4 IPTABLES*

O Iptables muitas vezes é confundido com um *firewall*, mas na verdade é uma ferramenta de *Front-End* que permite manipular as tabelas do Netfilter. Como principais características, o Iptables nos dá um amplo leque de possibilidades tais como a implementação desde filtro de pacotes utilizando as tabelas e mais controles avançados como o redirecionamento de endereçamento e portas, mascaramento de conexões, detecção de fragmentos, monitoramento de tráfego, bloqueio de ataques *Spoofing, DOS*, scanners ocultos, pings da morte entre outros. Essa ferramenta também traz a opção de utilizar módulos externos na composição de regras, o que amplia ainda mais as suas funcionalidades.

O Iptables possui cinco tabelas, que são áreas nas quais uma cadeia de regras pode ser aplicada, ARCHLINUX:

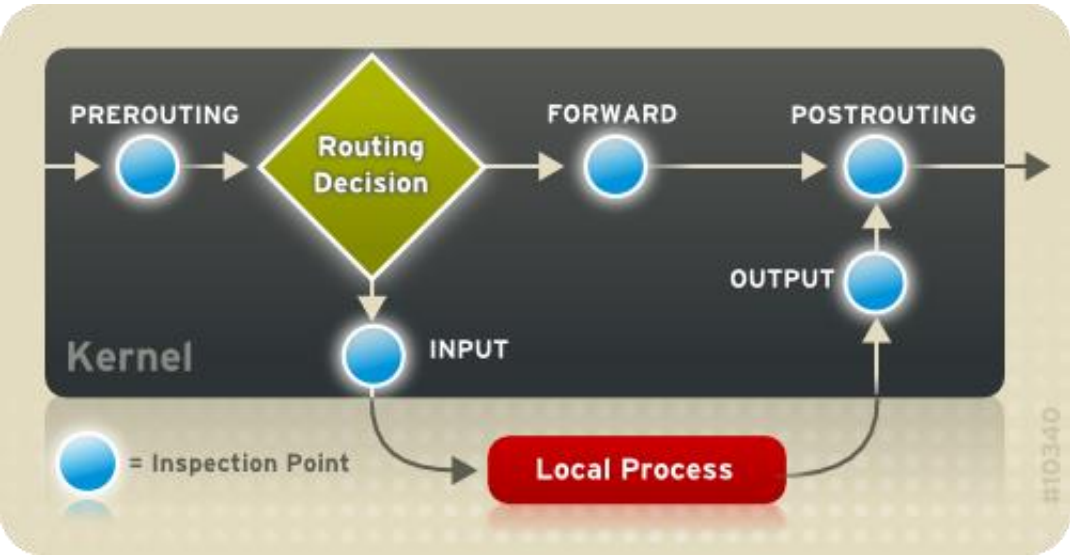
- Raw, filtra os pacotes antes de qualquer outra tabela. É usada principalmente para configuração de isenções de rastreamento de conexões;
- Filter, é a tabela padrão (se a opção –t não for passada);

- Nat, é usada para a tradução de endereços de rede (o redirecionamento de porta, por exemplo);
- Mangle, é usada para alteração de pacotes especializados;
- Security, é utilizada para as regras obrigatórias de controle de acesso a rede.

As tabelas mais utilizadas são a filter, nat e mangle.

As *chains* são locais onde ficam armazenadas as regras definidas pelo administrador. A tabela filter por padrão possui três chains, a *INPUT* (tráfego de entrada para a própria máquina), a *OUTPUT* (o tráfego gerado localmente para fora da máquina) e a *FORWARD* (faz o roteamento do tráfego para outra interface de rede ou outra máquina). A tabela nat possui outra três chains a *PREROUTING* (utilizada quando os pacotes precisam ser alterados logo que chegam), a *OUTPUT* (utilizada quando os pacotes precisam ser alterados antes de serem roteados) e a *POSTROUTING* (utilizada quando os pacotes precisam ser alterados após a tratativa de roteamento).

**Figura 4 - Posicionamento das chains no processo**




Fonte: Disponível em https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html

A filtragem de pacotes é feita com base em regras, que são comandos passados o Iptables para que realize uma determinada ação, as regras são armazenadas nas *chains*. Uma regra é composta por qual tabela ela pertence, qual

*chain* ela vai ficar armazenada e a ação a ser tomada quando um pacote estiver de acordo com essa regra.

# iptables -t TABLE -A CHAIN DADOS -j AÇÃO

As regras podem operar em determinado protocolo (-p), endereço de origem (-s), endereço de destino (-d), interface de chegada (-i) e interface de saída (-o). É possível realizar as seguintes ações: aceitar o pacote (*ACCEPT*); ignorar completamente o pacote (*DROP*); indicar que o pacote deve ser passado ao userspace; retornar ao chain anterior sem completar o processamento no chain atual (*RETURN*); registrar o pacote no sistema de log (*LOG*); e rejeitar o pacote (*REJECT*).

Exemplo de comando para ignorar completamente pacotes com destino a máquina de IP 10.1.1.11:

# iptables –t filter -A OUTPUT -d 10.1.1.11 -j DROP

Localizado entre o solicitante e o servidor, o *Proxy* é uma ferramenta intermediadora das solicitações e das respostas entre ambos. Atuando na camada de aplicação do modelo OSI, o servidor *Proxy* tem a habilidade de alterar, de maneira transparente, as solicitações provenientes do cliente e as respostas vindas do servidor.

Duas características do *Proxy* são muito úteis em redes locais, a capacidade de armazenar localmente os conteúdos mais solicitados pela rede interna, diminuindo assim o tempo de resposta e o tráfego para a rede externa e a possibilidade de filtrar o conteúdo das informações que trafegam pela rede, retendo os acessos a conteúdos não permitidos pelo administrador. Estas duas características são chamadas de cachê web e filtro de conteúdo respectivamente.

Por ser um *Proxy WEB* extremamente popular e funcional, o pacote *open source* Squid é adotado por alguns *Firewalls* para os gerenciamentos do Proxy web e do cachê de Internet.

O Squid oferece suporte a conexões HTTP, HTTPS, FTP e outros. Ele também reduz o uso da largura de banda e tempo de resposta realizando cache das requisições usadas frequentemente. Permite também diversos modos de autenticação de usuário, o que também inclui a possibilidade de criação de listas de sites e/ou palavras proibidas para acesso. Pode esperar de um proxy-cache alguns

benefícios como velocidade de acesso, disponibilidade, capacidade de trabalhar com redes heterogêneas e simplicidade PEARSON, 2012.

## 2.5 DHCP

Serviço de DHCP (*Dynamic Host Configuration Protocol*), em uma abordagem simplificada, é o serviço responsável por atribuir automaticamente endereços de IP, pré-definidos dentro de um intervalo de endereços IP, aos computadores da rede interna. Ao ativar este serviço, o administrador permite que o servidor atribua um endereço IP para cada máquina da rede que esteja configurada para esta solicitação, o uso deste serviço não proíbe que o administrador atribuía IPs fixos às máquinas da rede.

Dessa forma, o administrator pode determinar um divisão de endereços, por exemplo do endereço 192.168.1.100 até o endereço 192.168.1.240 para as estações de trabalho da empresa, também permite colocar o endereços fora dessa faixa para seus servidores, realizando essa configuração nos servidores de forma manual (BATTISTI, 2013).

## *2.6 Failover*

*Failover* é a capacidade que o sistema tem de alterar o acesso a um determinado serviço, considerado principal, para sua respectiva alternativa de *backup*. Esta alteração é automática e transparente e pode ser realizada em serviços como acessos a banco de dados ou redes. Alguns *firewalls* permitem a utilização de *failover* para as conexões de rede. Um exemplo comum é a utilização de dois acessos para a Internet onde um deles será classificado e utilizado como principal e caso este acesso passe por problemas, automaticamente o fluxo de dados será direcionado para o segundo acesso.

## 2.7 IDS

O IDS (*Intrusion Detection System*) é uma ferramenta que atua como um analisador, em tempo real, de eventos da rede buscando informações sobre possíveis ataques. Baseado em regras pré-definidas, o IDS analisa os pacotes enviados às interfaces de rede e gera alarmes quando algum pacote suspeito é encontrado.

Um exemplo de ferramenta IDS é o *open source* SNORT. Atuando como um analisador eficiente e confiável dos pacotes que trafegam pelas interfaces de rede, o SNORT exige poucos recursos do sistema. Suas análises são baseadas em algumas

estratégias, entre elas a verificação das assinaturas dos pacotes, os protocolos de rede ativos e a busca por atividades anômalas. A empresa *SourceFire*, mantenedora do SNORT oferece atualizações periódicas das regras para *download* (ROESH, 2015).

Prover este acesso por meio de protocolos tradicionais como HTTP ou NFS permite que pessoas com acesso à estrutura da rede, localizadas entre a origem e o destino, possam interceptar, ler, copiar ou alterar as informações em trânsito.

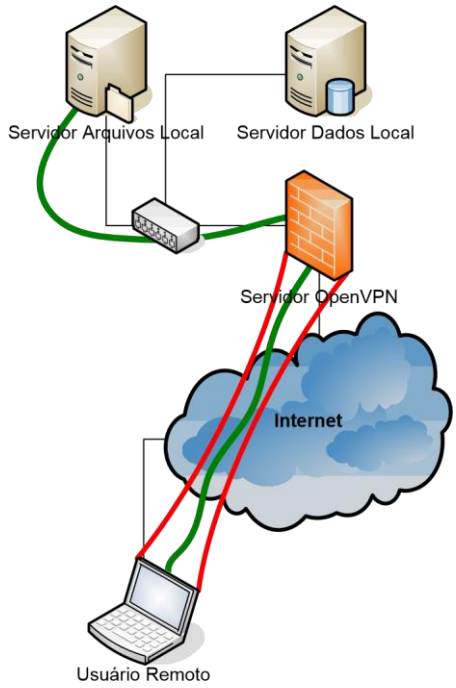
## 2.8 VPN

Simplesmente disponibilizar o acesso às informações e serviços por meio de protocolos tradicionais não é uma medida segura. Para manter o gerenciamento, controle e segurança destas conexões provenientes do ambiente externo uma boa alternativa é oferecê-las amparadas por uma rede virtual privada ou VPN (*Virtual Private Network*).

Diferente das redes locais, baseadas em metros e metros de cabos, roteadores e outros *hardwares* de rede, a rede virtual privada (*Virtual Private Network*), como o próprio nome indica, é uma rede virtual constituída entre dois ou mais pontos remotos interligados por uma terceira rede pública, que na grande maioria dos casos é a Internet. O nome também indica que é uma rede privada envolvendo assim conceitos de segurança como criptografia dos dados e autenticação de usuários (OPENVPN, 2015).

Um exemplo típico de utilização de VPN é o acesso de funcionários, vendedores externos por exemplo, às informações e serviços existentes na rede local da empresa. Um funcionário em trânsito utiliza um cliente de VPN que estabelece uma conexão remota segura com o servidor da empresa. O tráfego entre origem e destino é encapsulado e criptografado permitindo assim segurança das informações trocadas. Oferecendo acesso a serviços como clientes de e-mail, FTP e compartilhamento de arquivos, a VPN vem cada vez mais sendo utilizada pelas empresas.

**Figura 5 - O vermelho indica o tunelamento e o verde o tráfego encriptado em uma rede VPN**




Fonte: Próprio Autor

Entre várias topologias de VPN há duas que normalmente são utilizadas pelas empresas:

- ***Net-to-Net*:** quando duas ou mais redes privadas são interligadas por meio da Internet. Esta conexão e realizada utilizando-se roteadores VPN nas duas pontas da rede virtual;

- ***Host-to-Net*:** quando um usuário, normalmente utilizando-se de um computador móvel com acesso à Internet, realiza a conexão ao servidor por meio de um cliente VPN.

Muitos protocolos proprietários fazem parte do serviço de VPN. Além dos protocolos muitas outras tecnologias como *IP Security (IPSec), Layer Two Tunneling Protocol (L2TP), Point to Point Tunneling Protocol (PPTP)*, SSH e SSL estão envolvidos na criação de uma rede virtual privada.

Dentre os diversos protocolos de VPN, o IPSec é o mais independente, padronizado e é incorporado na maioria das soluções existentes no mercado. O IPsec foi desenvolvido baseado em duas características:

- **Modo Túnel:** o tráfego entre os pontos da rede virtual é realizado por meio de um túnel, no qual todo o pacote é criptografado e encapsulado na origem e decodificado no destino.

- **Modo Transporte:** neste modo, apenas o conteúdo do pacote passa pelos processos de criptografia e decodificação entre a origem e o destino.

Segundo Battisti (2013) o IPSec pode ser implantado de duas maneiras: por meio de uma chave compartilhada (*Pre-Shared Key*), atuando como uma senha entre os dois pontos da conexão ou por meio de certificados emitidos por Autoridades Certificadoras (CA) como Verisign, Thawte ou CAcert.org.

# 3 ESTUDO DE CASO: ENDIAN FIREWALL COMMUNITY

Com base nos itens apresentados anteriormente o estudo de caso foi realizado utilizando-se da distribuição *Linux Endian Firewall Community*, sendo simulado o ambiente da empresa Alimentos Personalizados SA.

Baseado no sistema operacional Linux, mais precisamente na distribuição IPCop, o EFW (*Endian Firewall Community* ) é uma ferramenta que contempla várias funcionalidades de segurança e integração de redes, concentrando em uma única distribuição várias soluções como roteador, firewall, proxy web, proxy de e-mails, antivírus, IDS (*Intrusion Detection System*) e servidor VPN, ENDIAN S.rl, 2015.

O EFW *Community* é desenvolvido e mantido pela empresa italiana Endian e pode ser obtido através do site oficial da empresa. Atualmente é oferecido na versão 3.0 e é consideravelmente pequeno com aproximadamente 215MB, comparado a outras distribuições completas do Linux.

Por ser uma ferramenta especializada, o EFW exige uma máquina exclusivamente dedicada para suas funções. Depois de instalado no computador, este será utilizado exclusivamente para as funcionalidades do EFW.

## 3.1 Funcionalidades do EFW

Além da interface web, que proporciona um ambiente de configuração e manutenção extremamente amigável, o EFW possui várias funcionalidades. A figura 6 a seguir, apresenta um quadro com as principais funcionalidades:

**Figura 6 - Principais funcionalidades do EFW**

| Funcionalidade | Características |
|---|---|
| Gerenciamento | • Interface Web SSL;<br>• SSH. |
| Firewall | • Possibilita o gerenciamento de até quatro redes diferentes separadas pelo sistema de cores Green (LAN), Red (WAN), Orange (DMZ), Blue (Wireless);<br>• Firewall baseado em iptables. |
| Segurança Web | • Proxy transparente para HTTP e FTP;<br>• Antivírus;<br>• Filtragem e bloqueio de arquivos;<br>• Listas de acesso proibido prontas (Blacklists);<br>• Dansguardian: ferramenta de controle de conteúdo;<br>• Proxy autenticado baseado em Squid (Local, LDAP, Radius e Active Directory);<br>• Controle de acesso à Internet por horário;<br>• Controle de acesso por grupos de usuários. |
| Segurança E-mail | • Anti-Spam;<br>• Proxy transparente para POP3, IMAP e SMTP;<br>• Lista de endereços de e-mail permitidos e proibidos;<br>• Redirecionamento transparente de cópias e-mails. |
| VPN | • OpenVPN e IPSec;<br>• Autenticação por usuário ou por chaves criptografadas. |
| Failover | • Suporte a duas ou mais conexões de Internet. |
| Logs, Estatísticas e Relatórios | • IDS (Intrusion Detection System);<br>• Estatísticas detalhadas de tráfego das redes;<br>• Estatísticas dos recursos de hardware do sistema (CPU, memórias, etc.);<br>• Envio de e-mails com informações do sistema para o administrador;<br>• Logs do Squid, Dansguardian, firewall e Antivírus ClamAV;<br>• Syslog local e remoto. |
| Backup | • Backup e restauração via web. |

Fonte: ENDIAN S.rl

A empresa Endian possui vários modelos comerciais de firewalls, além da distribuição *Open Source* do EFW. Estes modelos, baseados no mesmo *software* da versão *Community*, são comercializados na versão *appliance*, ou seja, em um de conjunto com um *hardware* e *software* especializados. Essas versões comerciais possuem mais funcionalidades quando comparadas à versão gratuita.

Quando confrontadas, as versões *Community* e *Appliance*, a segunda oferece algumas funcionalidades, como: suporte técnico; opção pela utilização de antivírus de versões comerciais; clientes VPN nativos para Microsoft Windows, MacOS e Linux; e *HotSpot*, que é disponibilidade de controle específico de pontos de acesso às redes sem fio.

*Firewalls*, como no caso do EFW, que também atuam como *proxies* necessitam de um computador com boa capacidade de processamento e memória. Quando se adiciona funcionalidades de VPN, antivírus e *AntiSpam*, esta demanda por processamento e memória fica ainda maior.

Na proposta aqui apresentada, considerando-se os usuários locais e remotos, espera-se a constituição de uma rede com aproximadamente cinquenta pontos de acesso.

Considerando-se a versão EFW 3.0, para atender uma rede deste porte, recomenda-se a seguinte configuração de hardware: processador Intel Core 2 Quad ou equivalente; 4 Gb Memória RAM; disco rígido de 250 Gb; no mínimo duas Interfaces de rede.

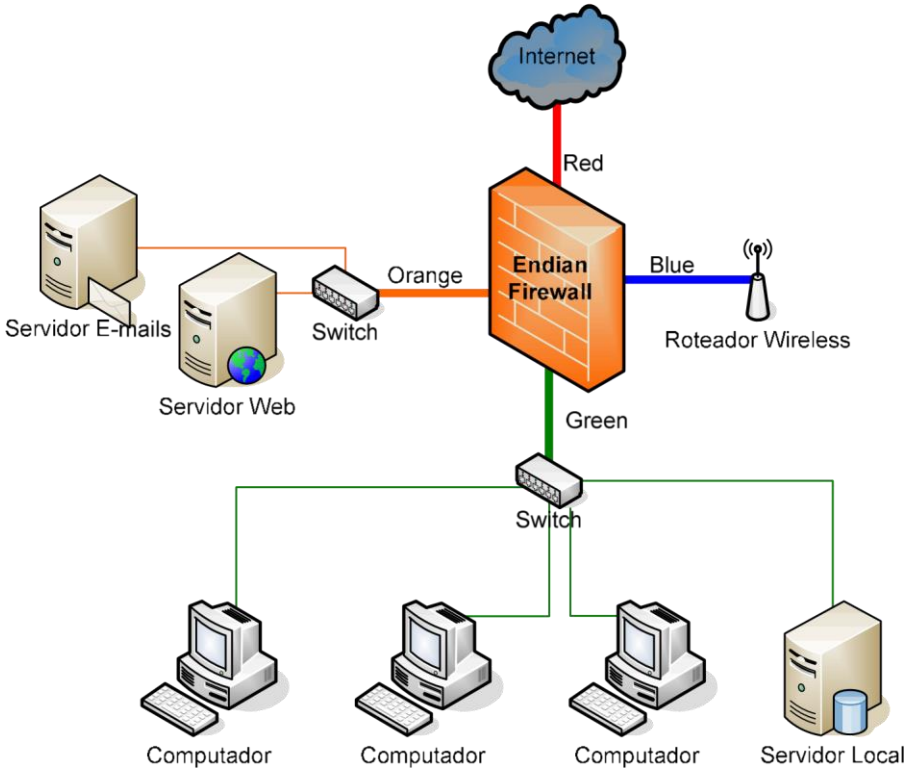
É importante salientar que antes de iniciar os trabalhos de instalação e configuração, algumas verificações de hardware devem ser realizadas pelo profissional. Respeitar as instruções de montagem e ventilação dos fabricantes é primordial, pois o computador destinado a esta função deve estar o tempo todo disponível para a rede. Com a popularização cada vez maior da tecnologia dos discos rígidos sólidos (SSD), estes tornam-se uma ótima alternativa para prevenção de falhas mecânicas, comum em discos rígidos tradicionais (HDD).

Baseado na distribuição IPCop, o EFW adotou a mesma classificação de redes. As redes são separadas em quatro segmentos nomeados por cores:

- ***Green* (verde):** associado à rede local (LAN), este é o segmento de rede confiável;
- ***Red* (vermelha):** conectado à Internet ou a uma rede externa (WAN), este é o segmento duvidoso e potencialmente inseguro;

- ***Orange* (laranja):** é neste segmento que devem estar os serviços de acesso público. Servidores Web e de e-mail devem estar associados a esta conexão, pois se um invasor burlar as proteções destes serviços, ele ficará restrito à essa região da rede, sem acesso direto à LAN. Este segmento de rede é conhecido como DMZ (*Demilitarized Zone*);
- ***Blue* (azul):** é uma conexão dedicada aos acessos wireless. As redes wireless de acesso público são potencialmente inseguras, sendo assim é uma importante questão de segurança mantê-las separadas da rede local.

**Figura 7 - Topologia de rede adotada pelo Endian Firewall**




Fonte: Próprio Autor

## 3.2 A aplicação do EFW

O estudo apresentando abaixo foi todo simulado utilizando-se de máquinas virtuais (VMs), com o auxílio da ferramenta *VirtualBox*.

Em 2010, vislumbrando o crescimento das atividades e das regiões de atuação da empresa Alimentos Personalizados SA, empresa que oferece o serviço de personalização de embalagens de alimentos, os gestores da mesma optaram por iniciar um plano mais ousado de informatização. Até então, a informática na empresa se resumia a dois terminais interligados por meio de um hub a um serviço de Internet wireless local. Não havia a preocupação com dispositivos que permitissem a segurança local e a interligação com os vendedores externos.

A busca começou por uma solução adequada de *software* que pudesse dar suporte às atividades de venda e produção da empresa. Além disso, era necessário manter e disponibilizar milhares de referências visuais (imagens) das produções realizadas. As versões das imagens deveriam estar disponíveis a alguns departamentos estratégicos da empresa e também aos vendedores em trânsito.

Paralelo ao início das atividades de informação, a empresa também começou a abrir e estruturar escritórios remotos em cidades consideradas estratégicas do território nacional. Era então necessária a interligação destes pontos remotos à estrutura interna em desenvolvimento.

Definida a questão da rede interna e do software de apoio às atividades comerciais, iniciou-se o processo de estruturação da segurança e da interligação entre os escritórios e funcionários remotos. A busca inicialmente foi por soluções proprietárias, mas o investimento era considerado relativamente alto quando somado ao que já havia sido gasto. A busca então virou-se para o software livre. Comparando várias versões *open source* com versões comerciais chegou-se à conclusão de que a primeira opção atenderia com extremo sucesso às necessidades de segurança e interconexão das redes.

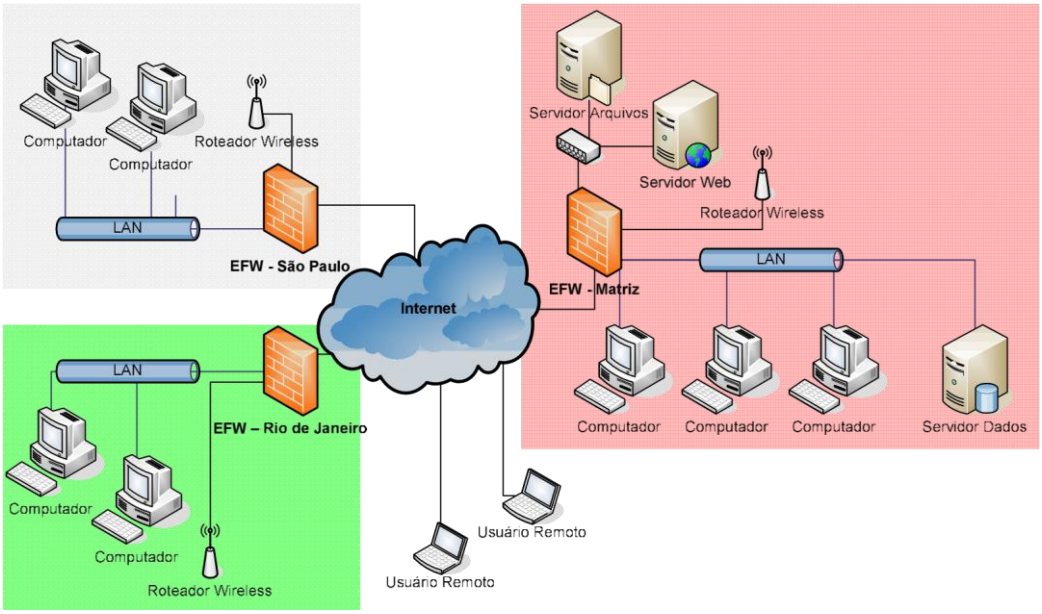
Dentre as várias soluções *open source* pesquisadas uma delas se destacava por oferecer várias funcionalidades e uma ferramenta prática de configuração, gerenciamento e monitoramento. Esta solução era o *Endian Firewall Community*.

O Endian Firewall Community permitiu à empresa Alimentos Personalizados SA implementar uma rede para atender as necessidades de segurança local e remota. A mesma ferramenta foi utilizada para construir as redes VPN que interligam os escritórios e os usuários remotos ao servidor de dados local.

Com um tráfego diário de centenas operações de consulta, cadastro, e-mails e obtenção de imagens, hoje a rede é composta por três escritórios remotos e

aproximadamente cinquenta usuários em trânsito. Três *appliances* rodando EFW são responsáveis por manter a segurança e a interligação das redes e dos usuários.

**Figura 8- Atual estrutura da rede Alimentos Personalizados SA.**




Fonte: Próprio Autor

Em cada unidade foi utilizado um EFW, utilizando os recursos de DCHP, para realizar a distribuição de IP para as máquinas dos usuários, o serviço de *WEB Proxy* para maior controle e segurança das informações que são acessadas, o *failover* da comunicação com a Internet, garantindo maior disponibilidade, IDS para proteção contra intrusos na rede e serviço de VPN, *Host-to-Net* e modo túnel, para interligação das unidades e usuários transitantes.

O EFW se apresenta sempre estável e disponível para a rede. Por quatro anos não foram registradas ações bem sucedidas de invasão. O monitoramento indica tentativas, mas todas foram barradas. Nestes quatro anos, todo o tráfego da rede foi monitorado e gerenciado impedindo que as redes internas da empresa e dos escritórios acessassem conteúdos proibidos ou perigosos. Associada a uma política de educação digital e às ferramentas do EFW, não foram registradas ocorrências de vírus nas redes nos últimos 2 anos.

Hoje fica evidente ao administrador e aos gestores que o *Endian Firewall Comunnity* é uma solução econômica e confiável para o gerenciamento das atividades das redes locais.

# 4 CONSIDERAÇÕES FINAIS

Diante de competitivo cenário do mercado atual, fica evidente a importância das informações, da informatização e da Internet para as empresas. Diante dos custos, nem todas as empresas podem criar estruturas que dão suporte à informatização e consequente segurança de seu patrimônio digital.

Neste trabalho, mostrou-se uma alternativa de baixo custo para implementar dois dos pilares da estrutura de informatização: a segurança e a interconexão de redes de computadores.

A intenção não foi defender uma ferramenta específica ou pregar a utilização do software *open source*, mas sim propiciar a descrição prática de uma solução gratuita e de código aberto que atende todas as necessidades inerentes ao desafio proposto, criando-se assim uma base de conhecimento para que pequenas e médias empresas possam proteger e prover acesso seguro e controlado às suas informações.

## REFERÊNCIAS

ARCHLINUX. iptables. Disponível em: < https://wiki.archlinux.org/index.php/iptables >. Acesso em: 25 abr. 2015.

BATTISTI, Julio. Tutorial de TCP/IP - Júlio Battisti - Parte 09 Introdução ao DHCP, 2013. Disponível em: < http://juliobattisti.com.br/artigos/windows/tcpip_p9.asp >. Acesso em: 21 ago. 2015.

BATTISTI, Julio. Tutorial de TCP/IP - Júlio Battisti - Parte 18 Introdução ao IPSec, 2013. Disponível em: <http://juliobattisti.com.br/artigos/windows/tcpip_p18.asp >. Acesso em: 21 ago. 2015.

CISCO, Systems. Cisco 2015 Annual Security Report, 2015. Disponível em: < http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf >. Acesso em: 12 mar. 2015.

ENDIAN S.rl. Endian UTM Appliance Reference Manual 3.0. 2015. Disponível em: <http://docs.endian.com/>. Acesso em: 26 mar. 2015.

FERREIRA. Milton. O que vem ser Segurança da Informação? Disponível em: < http://www.apinfo.com/artigo81.htm>. Acesso em: 12 nov. 2015.

G1. Entenda o caso de Edward Snowden, 2013. Disponível em: < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 13 jun. 2015.

GALIARDO, L. S. V. W. G. Administrative Guide. 2006. Disponível em: <http://www.endian.com/fileadmin/documentation/efw-admin-guide/en/efw-admin-guide.html >. Acesso em: 26 mar. 2015.

IPCOP. IpCop Documentation. Disponível em: < http://www.ipcop.org/docs.php >. Acesso em: 13 jun. 2015.

JUNIOR, Alceu. Squidnomicon. 2013. São Paulo.

MACEDO. Diego. Como funciona um Firewall, 2012. Disponível em: < http://www.diegomacedo.com.br/como-funciona-um-firewall>. Acesso em: 12 mar. 2015.

MACEDO. Diego. Conceito de Filtragem de Pacotes e Firewall, 2012. Disponível em: < http://www.diegomacedo.com.br/conceito-de-filtragem-de-pacotes-e-firewall>. Acesso em: 12 mar. 2015.

MACEDO. Diego. Tipos de Firewall, 2012. Disponível em: < http://www.diegomacedo.com.br/tipos-de-firewall>. Acesso em: 12 mar. 2015.

MAIA. Marco. O que é Segurança da informação, 2013. Disponível em: < http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>. Acesso em: 12 nov. 2015.

OPENVPN, Technologies. Documentation. 2015. Disponível em: <http://openvpn.net/index.php/open-source/documentation.html>. Acesso em: 02 ago. 2015.

PEARSON, Oskar. The Squid Guide. 2012. Disponível em: <http://www.deckle.co.za/squid-users-guide/>. Acesso em: 13 jun. 2015.

REDHAT. Inc. Security Guide, 2014. Disponível em: < https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html>. Acesso em: 25 abr. 2015.

ROESH, Martin; GREEN, Chris SNORT Users Manual. Sourcefire, 2015. Disponível em: < http://manual.snort.org/ >. Acesso em: 08 ago. 2015.

SHARCNET. SSH, 2015. Disponível em: < https://www.sharcnet.ca/help/index.php/SSH >. Acesso em: 12 mar. 2015.

WATCHGUARD, Technologies. As Dez Maiores Ameaças de Segurança nas Empresas de Pequeno e Médio Porte, 2009. Disponível em: <http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_pt.pdf >. Acesso em: 02 maio. 2015.