

UNIVERSIDADE ESTADUAL DE GOIÁS
CÂMPUS ITABERAÍ
CURSO DE SISTEMAS DE INFORMAÇÃO

JOSÉ NUNES DIAS NETO

SEGURANÇA DA INFORMAÇÃO: Um Estudo de Caso Sobre Firewall
Aplicado na Prefeitura Municipal de Itaguaru

ITABERAÍ-Go
2018

JOSÉ NUNES DIAS NETO

SEGURANÇA DA INFORMAÇÃO: Um Estudo de Caso Sobre Firewall
Aplicado na Prefeitura Municipal de Itaguaru

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação da Universidade Estadual de Goiás – Campus de Itaberaí, sob orientação do prof^o. Jeferson Silva Araujo.

ITABERAÍ-Go

2018

JOSÉ NUNES DIAS NETO

SEGURANÇA DA INFORMAÇÃO: Um Estudo de Caso Sobre Firewall
Aplicado na Prefeitura Municipal de Itaguaru

Trabalho de Conclusão de Curso apresentado como requisito parcial à conclusão do Curso de Sistema de Informação da Universidade Estadual de Goiás, Câmpus Itaberaí. Este TC foi aprovado em 04/12/2018, pela banca examinadora constituída pelos professores:

Prof. Esp. Jeferson Silva Araujo
(Orientador – UEG – Câmpus Itaberaí)

Prof: Danilo Borges Caetano
(Convidado – UEG – Câmpus Itaberaí)

Prof (a): Lêda Carolina Zago Lima
(Indicado – UEG – Câmpus Itaberaí)

DEDICATÓRIA

Eu, José Nunes Dias Neto, dedico este trabalho aos meus pais Iracema Soares de Oliveira Nunes e Indalécio Nunes Dias, à minha irmã Layla Fernanda Soares Nunes Filardi e ao meu primo Saulo Nunes dos Santos que nunca mediram esforços para que eu conseguisse chegar até aqui, dedico também à todos os meus professores do curso de Sistemas de Informação, que sempre me auxiliaram e apoiaram nos momentos mais difíceis desse curso.

Não poderia deixar também de dedicar, aos meus amigos (as) que de alguma forma me ajudaram, que me apoiaram e que sempre estiveram ao meu lado, sempre me levantando nos momentos de fraquezas, angústias e nas crises de ansiedade.

A estes dedico este trabalho, sem a ajuda, confiança e compreensão de todos, este sonho não teria se realizado.

Meu muito obrigado. Vocês são tudo para mim!

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me concedido forças para que eu tenha chegado até aqui, também à nossa instituição que sempre me propiciou tudo quando precisei, ao meu orientador que foi grande difusor de conhecimento durante esse período de graduação, por último e não menos importante, todos os meus professores e mestres que nos guiaram durante essa jornada.

“É preciso sentir a necessidade da experiência, da observação, ou seja, a necessidade de sair de nós próprios para aceder à escola das coisas, se as queremos conhecer e compreender”.

(Émile Durkheim)

RESUMO

A presente monografia tem como eixo-norteador a pesquisa que aborda como temática central: **SEGURANÇA DA INFORMAÇÃO: Um Estudo de Caso Sobre Firewall Aplicado na Prefeitura Municipal de Itaguaru**, desenvolvida com um arcabouço teórico sustentado pela pesquisa bibliográfica e firmado pela pesquisa de campo realizada na prefeitura municipal de Itaguaru- Go. A estrutura deste trabalho contempla os requisitos necessários para atingir o objetivo geral deste trabalho, ou seja, demonstrar qual o firewall ideal para a segurança da informação em determinadas repartições, com recorte para o objeto de pesquisa aqui exposto, sendo dividido em três capítulos que contemplam a metodologia a fundamentação teórica e a exposição de resultados. Dentre outros, destacam-se como referência Sêmola (2007), Damásio (2007), Alves (2006), Moreira (2001), Simon (2003) e Hadnagy (2011). A relevância social da presente pesquisa está enraizada na contribuição para com futuras fontes de pesquisa acerca da mesma temática e ainda como uma diretriz norteadora para os usuários de serviços que demandam de segurança da informação. O trabalho aqui exposto, perpassa desde o contexto histórico, as transformações no tempo e no espaço, etapas de implantação, eficiência e eficácia até o resultado prático cotidiano. Ademais, vislumbra-se que a segurança da informação carece estar cercada de elementos indispensáveis a sua proteção, sejam eles: confidencialidade, disponibilidade e integridade.

Palavras-chave: Informação. Segurança. Firewall.

ABSTRACT

This monograph has as its guiding principle the research that addresses as the central theme: INFORMATION SECURITY: A Case Study on Firewall Applied to the Municipal Government of Itaguaru, developed with a theoretical framework supported by the bibliographic research and established by the field research carried out in the The structure of this work contemplates the necessary requirements to reach the general objective of this work, that is, to demonstrate the ideal firewall for the information security in certain departments, with a cut for the object of research presented here, being divided in three chapters that contemplate the methodology the theoretical foundation and the exposition of results. Among others, the following stand out as reference Seman (2007), Damásio (2007), Alves (2006), Moreira (2001), Simon (2003) and Hadnagy (2011). The social relevance of the present research is rooted in the contribution to future sources of research on the same subject and still as a guiding directive for the users of services that demand information security. The work presented here, runs from the historical context, the transformations in time and space, stages of implementation, efficiency and effectiveness to the daily practical result. In addition, it is envisaged that the security of information needs to be surrounded by elements indispensable to its protection, be they confidentiality, availability and integrity.

Keywords: Information. Safety. Firewall.

LISTA DE FIGURAS

- Figura 1 - Segurança da Informação: Tríade CIA
- Figura 2 - Representação básica de um firewall
- Figura 3 - Filtro de Pacotes
- Figura 4 - Firewall de Aplicação ou Proxy de serviços
- Figura 5 - Funcionamento de um WAF(Web Application Firewalls)
- Figura 6 - RouterBoard MikroTik
- Figura 7 - Servidor da Prefeitura
- Figura 8 - RB250GS e Equipamentos de Rede
- Figura 9 - Tela Inicial
- Figura 10 - Tela inicial e ferramentas extras do Sistema Operacional Mikrotik
- Figura 11 - Estrutura do Firewall-Regras
- Figura 12 - Regras Estabelecidas no Firewall da Prefeitura
- Figura 13 - Monitoramento de acesso
- Figura 14 - Estrutura NAT
- Figura 15 - Segmento de conexões

LISTA DE SIGLAS E ABREVIATURAS

CIA – *Confidentiality, Integrity and Availability*.

SO – Sistemas Operacionais.

TI – Tecnologia da Informação

TCP - Transmission Control Protocol (Protocolo de Controle de Transmissão)

IP - Internet Protocol (Protocolo de Internet)

VPN - Rede Virtual Privada

URL - Uniform Resource Locator (Localizador Padrão de Recursos)

QoS – Quality of Service (Qualidade de Serviço)

UTM - Unified Threat Management (Gerenciamento Unificado de Ameaças)

UDP - *User Datagram Protocol* (Protocolo de Datagrama do Usuário)

WAF - Web Application Firewalls (Firewalls de Aplicação Web)

RB – Router Board

SUMÁRIO

INTRODUÇÃO	12
1 SEGURANÇA DA INFORMAÇÃO	14
1.1 Evolução Tecnológica Global (o começo de tudo -----	14
1.1.1 Conceitos Tradicionais de Segurança da Informação-----	15
1.1.2Segurança da Informação -----	17
1.2 Princípios Básicos de Segurança da Informação	18
1.3 Ameças e Tipos de Invasores	19
1.4 Formas de Proteção de Ataques	20
1.5 Engenharia Social	21
2 FIREWALL	22
2.1 Firewall Contexto Histórico -----	24
2.1.1 Firewall Contexto Geral-----	25
2.2 Importância de um Firewall	26
2.3 Tipos de Firewall	28
2.3.1 Filtragem de Pacotes-----	28
2.3.2 Firewall de Aplicação ou Proxy de Serviços-----	30
2.3.3 Firewall de Inspeção de Estados-----	31
2.4 Histórico Firewall Web	32
2.4.1 Firewall Web-----	34
2.5 Mikrotik -----	35
2.5.1 Mikrotik RouterOS – Recursos-----	35
2.5.2 Mikrotik RouterOS – Firewall de Aplicação Web-----	36
3 ESTUDO DE CASO: Prefeitura Municipal de Itaguaru	38
3.1 Breve Histórico	38
3.2 Firewall Implantado na Prefeitura de Itaguaru: Entrevista com o Responsável pela TI -----	39
3.3 Equipamento e Sistemas de Gerenciamento do Firewall Web	41
3.3.1 Equipamentos	41
3.3.2 Sistemas de Gerenciamento do Firewall-----	43
3.3.3 Tela Inicial-----	43
3.3.4 Regras do Firewall-----	45
3.3.5 Estrutura NAT-----	47
3.3.6 Connection-----	48
3.3.7 ... Entrevista com Usuários da Rede-----	49
4 CONSIDERAÇÕES FINAIS	50
ANEXO 1: Regras do firewall implementadas na Prefeitura de Itaguaru -	54

INTRODUÇÃO

A segurança da informação é fundamental para garantir o bom funcionamento dos sistemas e evitar que invasores capturem informações essenciais para uma empresa, o que pode ocasionar impactos dos mais diferentes níveis.

Em função da necessidade de proteger os dados, os recursos e os próprios computadores, surgiram ferramentas de bloqueio de acessos indesejados, denominadas firewalls.

O software de firewall é um dispositivo que fica instalado em um host ou servidor que interconecta uma rede interna a uma rede externa. Seu objetivo principal é proteger a rede interna, filtrando e analisando os pacotes que transitam por meio dele. Baseado em algumas análises, o firewall pode avaliar se os pacotes podem transitar pela rede ou devem ser descartados.

Nesse contexto, o presente trabalho objetiva mostrar um estudo de caso na Prefeitura Municipal de Itaguaru, enfatizando-se os aspectos que a nortearam a implantação dessa ferramenta e, principalmente, como ela contribuiu para aumentar a segurança da informação nessa instituição.

No tocante à metodologia para o desenvolvimento do trabalho, foram utilizadas a pesquisa bibliográfica, constituída principalmente de livros e artigos científicos, o que permitirá uma visão ampla sobre o assunto. A pesquisa permite compreender o tema, elucidando as dúvidas e traz a referência necessária para o estudo de caso.

O estudo de caso foi realizado em uma instituição pública municipal com fins de analisar os aspectos relacionados à gestão e práticas de segurança da informação, verificando os controles e ações adotadas. Em relação ao estudo de caso, a coleta de dados foi através da seguinte fonte: entrevista realizada junto ao profissional de TI (Tecnologia da Informação) da Prefeitura Municipal de Itaguaru.

Com relação à organização do texto, o trabalho está organizado em três capítulos:

O Primeiro capítulo faz uma contextualização geral de Segurança da Informação, abrangendo as políticas de segurança, caracterizando as

vulnerabilidades e descrevendo os diversos tipos de ameaças e ferramentas de proteção.

Por se tratar do tema central do trabalho, o segundo capítulo aborda o tema firewall, apresentando: tipos de firewall, localização de um firewall, filtragem de pacotes e principais características do Iptables.

O terceiro capítulo traz um estudo de caso desenvolvido na Prefeitura Municipal de Itaguaru.

E por fim, as considerações finais, bem como as perspectivas futuras deste trabalho.

1 SEGURANÇA DA INFORMAÇÃO

1.1 Evolução tecnológica global (o começo de tudo)

Segundo Damásio (2007, p.45), “a tecnologia pode ser entendida como sendo a soma de um dispositivo, das suas aplicações, contextos sócios de uso e arranjos sociais e organizacionais que constituem em seu torno”.

A tecnologia teve seu surgimento em períodos muito distantes, pode se dizer que o homem pré-histórico foi o primeiro responsável por estas descobertas tecnológicas, devido a sua necessidade de aprimoramento na caça e pesca, e necessidades básicas do dia-a-dia. Entretanto, toda a evolução tecnológica tem o intuito de deixar a humanidade em constante evolução, um ponto positivo que visa aprimorar algo e tornar a vida em sociedade mais fácil. A tecnologia tem evoluído de modo tão rápido, que a geração atual tem que se adaptar para que não fique excluída na sociedade. Com o constante crescimento desta tecnologia tornou-se cada vez mais possível o contato maior e melhor com diversas partes do mundo, porém na maioria das vezes os países mais desenvolvidos têm acesso mais fácil e produz essa tecnologia de ponta, fazendo com que os demais países fiquem um pouco atrás com uma certa dificuldade de aprimorar tal ganho tecnológico. Com o crescimento tecnológico surgiu também a necessidade da segurança da informação, pois, toda entidade, empresa ou até mesmo toda pessoa tem informações importantes cujo as quais devem ser protegidas.

De acordo com pesquisas feitas o Brasil na década de 1930, importava quase toda sua tecnologia dos países mais desenvolvidos, e isso conseqüentemente fez com que ele fosse visto como um país atrasado em relação aos demais. Entretanto ao decorrer dos tempos foi se aprimorando, embora hoje ainda não seja uma das superpotências no setor tecnológico o país consegue acompanhar de forma mais lenta os demais que são destaque nesse setor. O uso da internet por exemplo, no Brasil na década de 80 e 90 somente a elite tinha acesso, hoje em dia qualquer pessoa que tenha porte de um computador ou algum dispositivo móvel pode utiliza-la. Mas, com todos esses avanços surgiu inúmeras dificuldades, pois o roubo de informações e ataques cibernéticos tem crescido gradativamente em nosso meio, e isso faz com que os

profissionais da área de TI especialmente os profissionais em segurança da informação se preocupem e busquem medidas para se prevenir a tais ataques.

O estado de Goiás é bastante conhecido por sua agropecuária, pecuária e agricultura, a tecnologia chegou no estado e ajudou no desenvolvimento e execução das tarefas nestas áreas. Embora o estado seja conhecido por tais práticas, e a localização estratégica no centro dos mercados consumidores, favorecer o desenvolvimento da TI era dificultado pela mão-de-obra especializada. No entanto, com o investimento do estado e das faculdades em cursos desta área ajudou no crescimento do mercado de TI e incentivou as pessoas a estudarem e atuarem na área. Esse crescimento também pode ser observado pelo fato da existência de softwares e tecnologias de ponta, além de trazer mais agilidade aos processos empresariais promover a transparência e a segurança da informação.

Já no município de Itaguaru, a tecnologia tem chegado aos poucos, pois, por ser uma pequena cidade que está em crescimento os investimentos na área de TI é menor. Contudo a atual administração juntamente com profissionais da área, tem implementado soluções tecnológicas para facilitar o desenvolvimento, a praticidade e eficiência dos sistemas e tecnologias integradas a prefeitura e município. Uma dessas tecnologias utilizadas na prefeitura é a que será apresentada no decorrer deste trabalho. Tecnologia essa que visa a proteção de dados, o controle e mapeamento da rede, além de proporcionar eficácia e velocidade a mesma. Vale lembrar que, com o crescimento do município a tecnologia tenderá a acompanhar.

1.1.1 Conceitos Tradicionais de Segurança da Informação

A internet surgiu em meados de 1969 nos Estados Unidos, e no princípio de sua criação foi nomeada de Arpanet, tinha como função interligar laboratórios de pesquisas americanos. Logo após essa ferramenta foi utilizada pelo Departamento de Defesa norte-americano, e tinha como função garantir a comunicação entre os militares e cientistas mesmo em casos de bombardeios. Em 1982, o uso da Arpanet tornou-se maior no ambiente acadêmico, nesta época era de uso restrito aos EUA, porém logo depois se expandiu para outros países, como Holanda, Dinamarca e Suécia. Desde então, começou a ser

utilizado o nome internet. Somente em 1987 o uso da internet a fins comerciais foi liberado nos EUA, e com isso começou a surgir diversas empresas provedoras de acesso a internet.

Com o crescimento da internet de alguns milhares de usuários no início da década de 1980 para centenas de milhões de usuários ao redor do mundo nos dias atuais, os incidentes de segurança da informação vêm crescendo consideravelmente com diversos tipos de ataques. A internet colaborou com a democratização da informação e se tornou um canal on-line para fazer negócios, entretanto, com tais benefícios a atuação de ladrões do mundo digital e a propagação de códigos maliciosos aumentaram também, e isso colocou a segurança da informação em risco. Com tantas ameaças presentes, as fronteiras da segurança da informação se expandiram. Isso devido ao constante crescimento tecnológico até então imprevisível, com esses avanços os profissionais de segurança são colocados em posições desconfortáveis, tentando estabelecer controle e proteção a um recurso que se modifica e melhora constantemente.

A segurança da informação é muito mais do que um simples antivírus instalado ou utilizar qualquer ferramenta que impeça tipos de ataques. Segurança da informação está relacionada com a proteção de dados, a segurança física, a segurança ambiental, alinhando os objetivos de missão da empresa, com fins de dar continuidade às funções essenciais dos negócios. A informação é um bem de suma importância seja para uma empresa/instituição ou até mesmo qualquer indivíduo, pois é essencial para tomadas de decisões e execução de qualquer tarefa. Muitas das vezes qualquer conteúdo que é gerado por operações diárias destas empresas deve ser armazenado e protegido. E o objetivo dos profissionais da área é garantir por meio de uso de mecanismos de defesas que a rede não seja invadida por pessoas maliciosas que não tem autorização no acesso de tais dados.

1.1.2 Segurança da informação

Com o advento da informática, o mundo tornou-se cada vez mais interligado e as informações passaram a serem instantâneas. A globalização acarretou a necessidade do desenvolvimento de novas tecnologias, possibilitando realizar diversas funcionalidades para facilitar o trabalho desenvolvido nas organizações e o contato destas com o público externo.

Contudo, tais facilidades muitas vezes expõem os computadores a vulnerabilidades e ameaças. Para evitar essas exposições, surge a segurança da informação, diretamente ligada à proteção de um conjunto de informações e dados, com fins de preservar o valor, a integridade, e a importância que estes dados têm para uma pessoa ou para uma organização.

Segundo Alves (2006) a segurança da informação visa proteger a informação e garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e oportunidades.

Atualmente vivemos em um mundo onde a informação digital é um dos principais produtos e sua grande utilização faz com que a segurança de tais dados seja necessária. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. A segurança de determinadas informações pode ser afetada por vários fatores, sejam eles comportamentais e do usuário, pelo local ou ambiente em que ela se encontra e por pessoas de má índole que poderia roubar, modificar ou destruir essas informações.

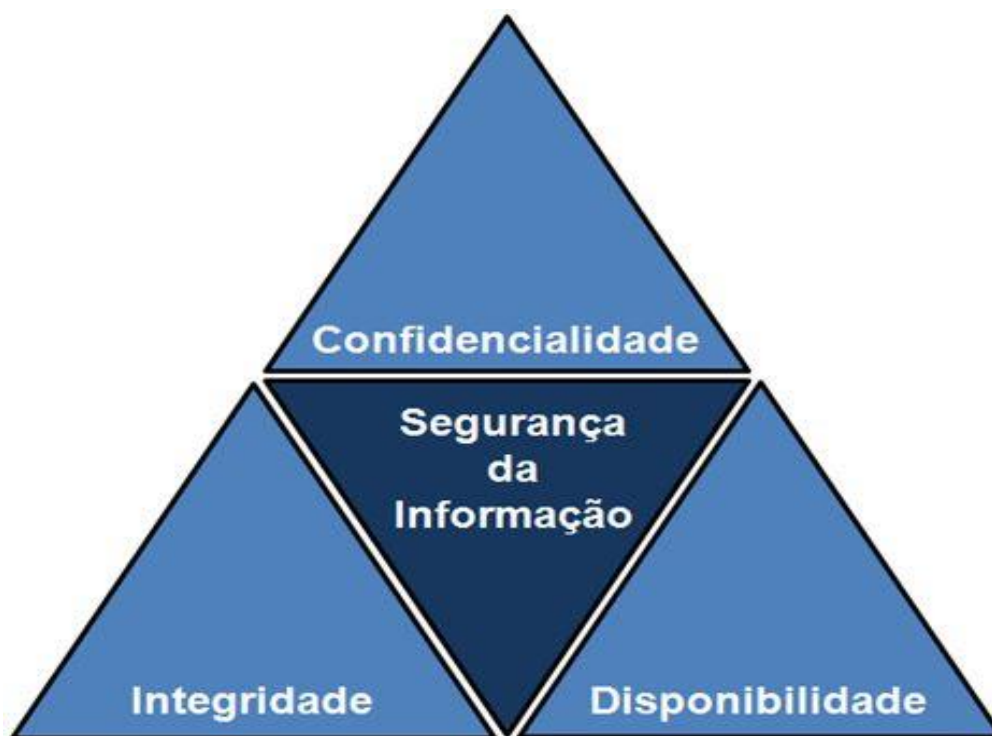
Existem níveis de segurança que podem ser estabelecidos, tais como identificados em políticas de segurança para garantir que o nível de segurança que se deseja estabelecer seja mantido. Para a construção de uma política de segurança existem alguns fatores que devem ser considerados, quais sejam: riscos, benefícios, custos e esforços de implementação dos mecanismos.

Dentro desse contexto, Stoneburner (2001), evidencia que a segurança é obtida somente através da relação e correta implementação dos princípios básicos, os quais será abordado no item a seguir.

1.2 Princípios Básicos de Segurança da Informação

Sêmola (2003), define que a segurança da informação tem como objetivo a preservação de três princípios básicos que são representadas pela tríade conhecida por CIA: Confidencialidade, Integridade e Disponibilidade (*Confidentiality, Integrity and Availability*), sendo eles demonstrados na figura abaixo:

Figura 1-Segurança da Informação: Tríde CIA



Fonte: Sêmola (2003)

Estes são os principais atributos do conceito de segurança da informação, orientando a análise, o planejamento e a implementação da segurança para um determinado conjunto de informações que se deseja proteger, e são definidos a seguir:

Confidencialidade: é garantir que a informação não será conhecida por pessoas que não estejam autorizadas para tal, limitando o acesso a informação tão somente às entidades legítimas, ou seja, as que são autorizadas pelo proprietário da informação. Dados confidenciais não são divulgados a pessoas que não necessitam ou que não deveriam ter acesso a eles. Garantir a

confidencialidade significa que a informação é organizada em termos de quem deveria ter acesso, bem como a sua sensibilidade.

Integridade: refere-se à certeza de que os dados não são adulterados, destruídos ou corrompidos. É a certeza de que os dados não serão modificados por pessoas não autorizadas. Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida: durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados.

Disponibilidade: para que um sistema demonstre disponibilidade, deve dispor um sistema computacional, de controles de segurança e canais de comunicação de bom funcionamento. A maioria dos sistemas disponíveis são acessíveis em todos os momentos e tem garantias contra falhas de energia, desastres naturais, falhas de hardware e atualizações de sistemas.

1.3 Ameaças e Tipos de Invasores

Cabe destacar que os princípios da segurança da informação podem ser comprometidos com possíveis ameaças, classificadas em físicas e lógicas.

Ameaça física: Incluem todo e qualquer processo de natureza física que possa comprometer os princípios da segurança da informação. Tem como objetivo proteger equipamentos e informações contra usuários não autorizados e prevenção de danos por causas naturais. Exemplos: alagamentos, tempestades, raios e etc.

Ameaça lógica: aplica-se em casos onde um usuário ou processo da rede tenta obter acesso a um objeto que pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc.), sendo assim, um conjunto de medida e procedimentos, adotados com objetivo de proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas. Exemplos: vírus, ataques de quebra de senhas e etc.

Moreira (2001) aponta a vulnerabilidade como sendo o ponto onde qualquer sistema é suscetível a um ataque, condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção.

São invasões de computadores, que costumam ser o tipo de ataque mais praticado/temido.

Scan: É um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como S.O, atividade e serviços) e identificar possíveis alvos para outros ataques.

Fraude: A fraude, abrange uma quantidade ampla de tipos de ataque. Um dos mais comuns deles é o *phishing*, que, para obter informações do usuário, usa de estratégias como a cópia da interface de sites famosos e envio de e-mails ou mensagens falsas com links suspeitos. O principal meio de evitar fraudes é a conscientização dos usuários por meio de treinamentos sobre cuidados na rede.

Worm: *Worms* são alguns dos malwares mais comuns e antigos. *Malware* são *softwares* com o intuito de prejudicar o computador “hospedeiro”. São considerados perigosos devido à sua capacidade de se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa ou entidade atingida.

1.4 Formas de Proteção de Ataques

São meios de segurança que visam controlar o acesso às informações de forma física e lógica.

Criptografia: é um meio de converter os dados em um formato do qual seja impossível decifrá-lo, ou seja, impedir completamente a interpretação das informações, e elas só voltam ao estado nítido quando uma senha é inserida.

Assinatura digital: Tem garantia de integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.

Certificação: uma certificação é como um atestado de autenticidade de um arquivo. Uma garantia de que o mesmo é válido.

Honeypot: É um *software* que age como um antivírus em tempo real, seu objetivo é proteger os dados de ameaças na *internet*. A diferença é que, em vez de mantê-lo em quarentena, por exemplo, o *honeypot* engana esse invasor, fazendo-o acreditar que está tendo acesso real às informações.

1.5 Engenharia Social

Atualmente o avanço da tecnologia está visível em nosso cotidiano, e é quase impossível conhecer alguém que não tenha algum aparelho tecnológico ou redes sociais.

Com isso cresce a vulnerabilidade das informações das pessoas, pois expõem muito suas intimidades na rede, tornando-se alvos fáceis de serem roubados. Esse tipo de técnica muito antiga é chamada de Engenharia Social.

A engenharia social é um termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, abusando da ingenuidade ou confiança do usuário. (HADNAGY, 2011)

A estratégia utilizada para esses roubos pode ser pensada como um meio de hackear os usuários, e não seus dispositivos, com o objetivo de convencê-los que estão disponibilizando suas informações a pessoas ou serviços confiáveis. Exemplos de táticas usadas incluem, mensagens de e-mails, páginas falsas ou truques psicológicos para distrair as vítimas.

Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro. (MITNIK; SIMON, 2003, p.3).

Diante dessa frase citada por Mitnik, entende-se que os ataques da engenharia social podem ter sucesso quando as pessoas são sem discernimento sobre as boas práticas da segurança.

Para evitar e minimizar estes ataques às entidades ou empresas podem implantar políticas de segurança, conscientizando e capacitando os usuários da rede da sua importância no ambiente de trabalho além de demonstrar a importância das informações que eles detêm.

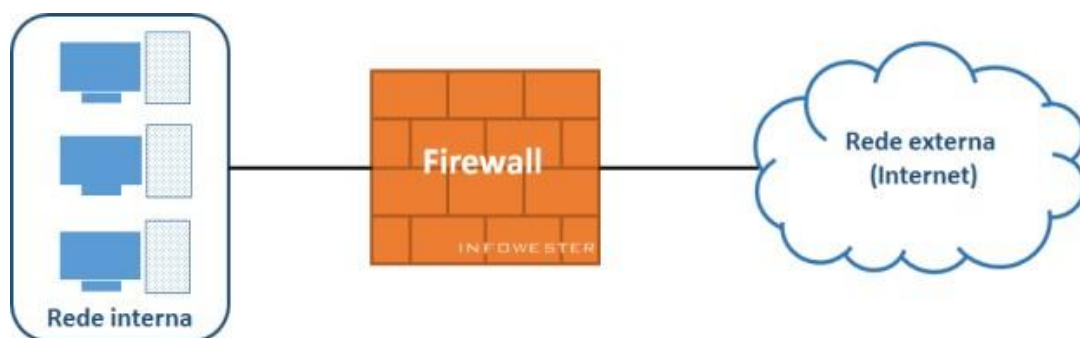
2 FIREWALL

Até mesmo as pessoas menos familiarizadas com a tecnologia e seus avanços significativos no mundo sabem que a internet não é um território livre de perigos e ameaças. É por esta razão que é importante conhecer e utilizar ferramentas de proteção para computadores e redes, a fim de proteger nossos dados e informações importantes. Uma das várias opções de segurança mais importantes dos ambientes computacionais é o firewall. Este, é um dispositivo de segurança que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança impostas pelo usuário. Este dispositivo tem sido a linha de frente da defesa na segurança de rede há mais de 25 anos, e tem como uma de suas funções colocam uma barreira entre redes internas protegidas e controladas, que podem acessar redes externas confiáveis ou não, como a Internet.

Segundo Ford L. (2002), “os firewalls é um dispositivo ou programa desenvolvido para detectar e proteger seu computador e rede contra ameaças internas e externas”.

A figura abaixo demonstra uma representação simples da função de um firewall:

Figura 2-Representação básica de um firewall



Fonte: Ford L. (2002)

De acordo com (CHESWICK, 2003), um *firewall* é um sistema que impõe uma política de controle de acesso entre duas redes, tendo as seguintes propriedades:

- * Todo tráfego de dentro para fora de uma rede, e vice-versa, deve passar pelo *firewall*.
- * Apenas tráfego autorizado, como definido pela política de segurança local, terá permissão de passar.
- * O próprio *firewall* deve ser imune à penetrações.

De acordo com a NBSO (2003), “um *firewall* é um instrumento importante para implantar a política de segurança da sua rede. Ele pode reduzir a informação disponível externamente sobre a sua rede, ou, em alguns casos, até mesmo barrar ataques a vulnerabilidades ainda não divulgadas publicamente e para as quais correções não estão disponíveis”.

Para uma melhor compreensão de um *firewall*, pode se imaginar que o mesmo é como se fosse uma portaria de um condomínio que para entrar, é necessário obedecer a determinadas condições do lugar, como se identificar, ser esperado por um morador e não portar qualquer objeto que possa trazer riscos à segurança, e para sair, não se pode levar nada que pertença aos moradores do lugar sem a devida autorização destes.

Um *firewall* pode impedir uma série de ações maliciosas como: um malware que utiliza determinada porta para se instalar em um computador sem o usuário saber, um programa que envia dados sigilosos para a internet, uma tentativa de acesso à rede a partir de computadores externos não autorizados, entre outros.

Com tantas portas abertas a rede, a utilização do *firewall* é essencial, para a proteção de nossos computadores e informações. Sabendo disto são vários os tipos de *firewall* que se pode ser utilizado.

2.1 Firewall Contexto Histórico

O termo firewall não é novo, ele se popularizou em especial com a disseminação da pilha de protocolos TCP/IP na década de 80. Pois, uma vez que o protocolo IP tem a capacidade de intercomunicação, deixar redes com propósitos ou domínios (empresas, universidades, organizações, etc.) diferentes sem qualquer controle ou proteção é um risco potencial para acessos não autorizados, e pode comprometer dados, entre outras possibilidades. Por conta disso, é necessário criar uma espécie de barreira que separa a parte pública de interconexão oferecida pela internet. A primeira proposta de firewall, surgiu em 1989 por Jeff Mogul, assim está proposta ficou conhecida como a primeira geração de firewall.

A segunda geração ficou marcada pela consolidação do conceito de Steve Bellovin e Bill Cheswick com a filtragem de pacotes stateful, ou firewall stateful. Essa filtragem nada mais é do que um mecanismo capaz de analisar os cabeçalhos em determinadas camadas da suíte TCP/IP, com base em um padrão de regras pré-estabelecido, que logo depois é encaminhado para o próximo passo ou é desconsiderado.

A terceira geração de firewall surgiu logo em seguida, onde a comercialização do DEC SEAL foi iniciada, esse firewall contava com recursos mais modernos de proxies de aplicação. Essa combinação de filtro de pacotes e proxy fez com que o nome firewall híbrido começasse a ser mais utilizado no mercado.

Com todo esse avanço e descobertas no final da década de 90, surgiram outras empresas, que agregaram recursos e soluções a segurança, a tornando cada vez mais confiável. Surgiram características como, filtros de URL, QoS, integração ou incorporação de soluções de antivírus, e o mais utilizado, o VPN (Rede Virtual Privada), uma rede privada, estruturada sobre uma infraestrutura de uma rede pública como a internet, essa prática é comum por empresas dos mais variados portes e segmentos com fins de utilizar esse recurso para permitir que escritórios e funcionários remotos se conectem com total segurança a sua rede privada. Isso tudo permitiu uma maior robustez na construção de ambientes seguros para as empresas.

Com a melhoria dos firewalls, e incorporações de soluções e medidas complementares de segurança, em 2004 surgiu pela primeira vez o termo UTM (Unified Threat Management) que veio com a necessidade e a evolução do próprio mercado de segurança, pois, na medida em que novos ataques ou vulnerabilidades eram descobertos, incrementava-se o firewall com novos recursos e funcionalidades. Em contextos gerais a UTM pode ser entendido como um ativo software combinado com um hardware, que centraliza em plataforma única as várias características de solução de firewall, filtragem stateful, proxy web, antivírus e IDS/IPS.

Embora a chegada da UTM trouxe vários benefícios com a união de diversas funcionalidades e recursos de segurança em uma única solução, o lado negativo surgiu, em relação a performance tendo em vista esse montante de recursos, e assim em 2008 o mercado é surpreendido com a aparição de firewalls de próxima geração (NGFW). Diferente da UTM, os firewalls de próximas gerações separam os recursos complementares de proxy web, proteção contra vírus, terceirizando esses recursos e assim fez com que sua garantia de altas taxas de escalabilidades para grandes ambientes fosse melhor. Sua grande vantagem era nos avanços tecnológicos de inspeção profunda de pacotes e na visibilidade de aplicações, independente de protocolos e portas.

Contudo o firewall tem passado por muitos upgrades desde sua criação, melhorando suas funcionalidades e características. Isso tudo devido a constante evolução das tecnologias e necessidades de proteção de informações para o mundo eletrônico, ressaltando também a importância da evolução da internet para que tais avanços sejam alcançados.

2.1.1 Firewall Contexto Geral

Com a disseminação e constante crescimento da tecnologia, a necessidade de criar restrições de acesso entre as redes existentes fez com que no final dos anos de 80 o então Firewall fosse criado, isso tudo devido a necessidade de proteger as redes de constantes ataques de hackers. Com isso pensadores e estudiosos da época pensaram em medidas para dificultar ou até mesmo permitir acessos de pessoas autorizadas. Pensando assim a utilização

do firewall era viável e confiável em meio a tantas tempestades que a área tecnológica enfrentava.

Firewall que em português tem o significado de “muro corta-fogo”, é uma ferramenta que tem a função de ajudar na política de segurança em um determinado ponto da rede. Uma de suas funcionalidades consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessórios nocivos ou não autorizados de uma rede para a outra. Essa ferramenta utiliza de equipamentos de filtro de pacotes e de proxy de aplicação, comumente associados a redes TCP/IP (Transmission Control Protocol ou Protocolo de Controle de Transmissão// Internet Protocol ou Protocolo de Internet). Os primeiros firewalls nasceram com a exclusividade de suportar a segurança no conjunto de protocolos TCP/IP. O termo “Firewall” faz uma comparação da função que o mesmo desempenha, pois evita o alastramento de acessos não permitidos em uma rede de computadores utilizando uma espécie de parede corta-fogo, ou seja, uma parede que impede a continuidade e alastramento de tais ataques. O Firewall existe na forma de software e hardware, ou até mesmo na combinação de ambos. Sua instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informação e qual o grau de segurança que você deseja.

Em termos um pouco mais técnicos, o firewall é responsável pelo controle dos dados que são transferidos de um computador para o outro utilizando como ferramenta de ligação a internet, também é uma maneira de prevenir que informações pessoais ou confidenciais sejam transmitidas através de ferramentas de softwares maliciosos. Dependendo do tipo de conexão usada pelo computador, é possível utilizar de dois tipos de firewalls, um por hardware e/ou software. As maneiras de operação do firewall tanto software quanto hardware são similares, conforme a configuração definida pelo usuário, o firewall compara os dados recebidos conforme o padrão descrito pelo usuário e logo após faz uso de uma espécie de liberação ou permissão dos pacotes.

2.2 Importância de um firewall

O termo “firewall”, em português, quer dizer, “parede/muro de fogo” e sua função é barrar os acessos indesejados. A partir de uma política de segurança

bem definida, estabelecemos as regras de acesso, definindo o que será acessado e por quem. Um firewall não deve ser encarado apenas como uma máquina que faz filtros, mas sim como um conjunto de ferramentas que ampliam a segurança de sua rede (segundo a política de segurança), e precisa ser constantemente “acompanhado”. (JUCÁ, 2005, p. 15).

Para GEUS e NAKAMURA (2003), o firewall é um ponto único entre duas ou mais redes, sendo um componente ou um conjunto de componentes, por onde ronda todo o tráfego, capaz de realizar o controle e a autenticação desse tráfego. Sua importante função é:

Esse ponto único constitui um mecanismo utilizado para proteger, geralmente, uma rede confiável de uma rede pública não confiável. O firewall pode ser utilizado também para separar diferentes sub-redes, grupos de trabalho ou LANs dentro de uma organização. (GEUS; NAKAMURA, 2003, p. 207).

Contudo, a importância dessa utilização de um firewall está diretamente ligada à sua definição. Se pararmos para imaginar uma empresa ou organização que presta serviços à população, como bancos, locadoras de automóveis, instituições públicas, etc. Sabe-se que esses tipos de empresas sempre têm salvo alguns dados do cliente como forma de garantir sucesso e segurança na realização de suas funções. Com a chegada da Internet, a maioria das empresas passaram a disponibilizar seus serviços em sites pessoais da mesma, como forma de simplificar e ajudar seus clientes, assim como atrair nova clientela no mercado. Entretanto, nem tudo é esse mar de rosas, a Internet assim como trouxe inúmeros benefícios, trouxe também, inúmeros riscos para os seus usuários.

Se eventualmente, alguma dessas empresas sofresse um ataque e conseqüentemente perdessem dados e informações importantes sobre seus clientes, certamente isso iria trazer prejuízos enormes para suas atividades, bem como uma mancha enorme para sua reputação no mercado.

Assim, surgiu uma necessidade de que as organizações separassem seus bancos de dados da internet. Para que isso fosse feito, as empresas dividiram sua rede em interna (banco de dados e informações) e externa (internet). No entanto, não bastava apenas dividir a rede, também era necessário que entre a rede interna e a rede externa houvesse alguma ferramenta de

segurança capaz de realizar a filtragem dos acessos permitidos e não permitidos. Para isso, criou-se o firewall, uma ferramenta que suprisse essas necessidades.

2.3 Tipos de firewall

As tecnologias de firewall evoluíram bastante, desde os primeiros anos de surgimento da internet. Atualmente, é possível comprar excelentes dispositivos e construí-los fazendo uso de software livre. Mesmo se houver a necessidade de pagar por um firewall, o usuário poderá contar com interfaces sofisticadas, assim como obter uma ferramenta com excelente capacidade de filtragem em nível de aplicação. Outra vantagem é a obtenção de suporte técnico, caso haja necessidade, item cujo qual não será disponível se a ferramenta tiver sido projetada por conta própria. (CHESWICK; BELLOVIN; RUBIN, 2003).

Dependendo de vários fatores como, por exemplo, critérios do desenvolvedor, estrutura de uma rede, necessidades específicas dos usuários ou características do sistema operacional que mantém o firewall, seu trabalho poderá ser realizado de diferentes formas. Sabendo disso, existem três tipos dessa solução de segurança que são bastante conhecidos.

2.3.1 Filtragem de Pacotes

As primeiras soluções de firewall surgiram na década de 1980 baseando-se em filtragem de pacotes de dados (*packet filtering*), um método mais simples e mais limitado, embora o mesmo oferece um nível de segurança significativo para o usuário e sistema.

A tecnologia de filtragem de pacotes atua tanto na camada de rede quanto na camada de transporte do modelo TCP/IP, de forma que toma parte de todas as decisões de filtragem com base nas informações do cabeçalho dos pacotes. Estas informações incluem endereço de origem, endereço de destino, porta de origem, porta de destino e a direção do fluxo de conexões. (GEUS; NAKAMURA, 2003)

Para melhor entendimento, é importante saber que cada pacote possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, e etc. Assim, o Firewall

então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote de dados sejam eles para sair ou para entrar na máquina/rede, podendo também executar alguma tarefa relacionada, como registrar o acesso ou tentativa de acesso em um arquivo de log.



Na filtragem de pacotes a transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas. Normalmente a filtragem se limita às camadas de rede e de transporte. As camadas de rede são onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo. As camadas de transporte são onde estão os protocolos que permitem o tráfego de dados, como o TCP e o UDP (*User Datagram Protocol*).

É possível encontrar dois tipos de firewall de filtragem de pacotes, a filtragem estática e a dinâmica.

Na filtragem estática, todos os dados são liberados ou bloqueados com base nas regras pré-definidas, não importando a ligação que cada pacote tem entre si. A princípio, esta abordagem não é um problema, mas alguns serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão e execução de suas tarefas. É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem as respostas necessárias, impedindo a execução da tarefa desejada. Esta situação pode ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar,

aumentando os riscos de o firewall não filtrar pacotes que deveriam ser bloqueados.

A filtragem dinâmica, surgiu com fins de superar as limitações dos filtros estáticos. Nesse tipo de filtragem, os filtros consideram o contexto em que os pacotes estão inseridos para criar regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente. Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

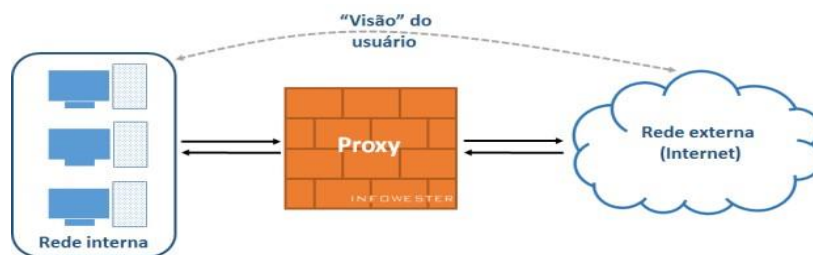
2.3.2 Firewall de Aplicação ou Proxy de Serviços

O firewall de aplicação, também conhecido como proxy de serviços, é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede externa, (normalmente a internet).

Os *proxies* são sistemas que atuam como um gateway entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições, de acordo com a política de segurança definida. Eles podem atuar simplesmente como um *relay*, podendo também realizar uma filtragem mais apurada dos pacotes, por atuar na camada de aplicação do modelo *International Organization for Standardization/Open Systems Interconnection* (ISO/OSI). (GEUS; NAKAMURA, 2003, p. 209).

Geralmente são instalados em servidores potentes por precisarem lidar com um grande número de solicitações de serviços. Este tipo de firewalls são opções interessantes e bastante utilizadas na segurança da informação, porque não permitem a comunicação direta entre origem e destino, assim fazendo com que todo o fluxo de dados passe por ele, e tornando possível o estabelecimento de regras que impedem o acesso de determinados endereços externos. Em vez de a rede interna se comunicar diretamente com a internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o proxy; e entre o proxy e a internet. A imagem a seguir faz uma ilustração desse contexto:

Figura 4-Firewall de Aplicação ou Proxy de serviços



Fonte: Geus; Nakamura (2003)

Todo o fluxo de dados precisa passar pelo proxy, assim é possível, estabelecer regras que impeçam o acesso de determinados endereços externos, como que proíbam a comunicação entre computadores internos e determinados serviços remotos. Este tipo de controle amplo, também possibilita o uso do proxy para tarefas complementares como: o equipamento pode registrar o tráfego de dados em um arquivo de log, conteúdos muito utilizados podem ser guardado em uma espécie de cache (uma página Web muito acessada fica guardada temporariamente no proxy, fazendo com que não seja necessário requisitá-la no endereço original a todo instante.), determinados recursos podem ser liberados apenas mediante autenticação do usuário, entre outros.

A implementação de um proxy não é uma tarefa fácil, tendo em vista a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de firewall não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos. Entretanto é uma ferramenta de considerável nível de segurança para sua rede, seja ela interna ou externa.

2.3.3 Firewall de Inspeção de Estados

Considerado como uma evolução dos filtros dinâmicos, os firewalls de inspeção de estado fazem uma comparação entre o que está acontecendo e o que é esperado para acontecer.

Os filtros de pacotes dinâmicos, também conhecidos como filtros de pacotes baseados em inspeção de estados, tomam as decisões de filtragem tendo como referência dois elementos:

- As informações dos cabeçalhos dos pacotes de dados, como no filtro de pacotes.
- Uma tabela de estados, que guarda os estados de todas as conexões. (GEUS;NAKAMURA, 2003, p. 217).

Para isso os firewalls de inspeção analisam todo o tráfego de dados em busca de padrões aceitáveis por suas regras, as quais, inicialmente, serão utilizados para manter a comunicação ou o cancelamento de tal comunicação. Estas informações são então mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente. Ou seja, se a transação de dados ocorrer por uma porta não mencionada, o firewall possivelmente detectará isso como uma anormalidade e efetuará o bloqueio do processo.

Para melhor entender, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão usadas para estas tarefas. Se de repente o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

Além destes tipos de firewall mais conhecidos podemos também citar sobre os WAF (Web Application Firewall).

2.4 Histórico Firewall Web

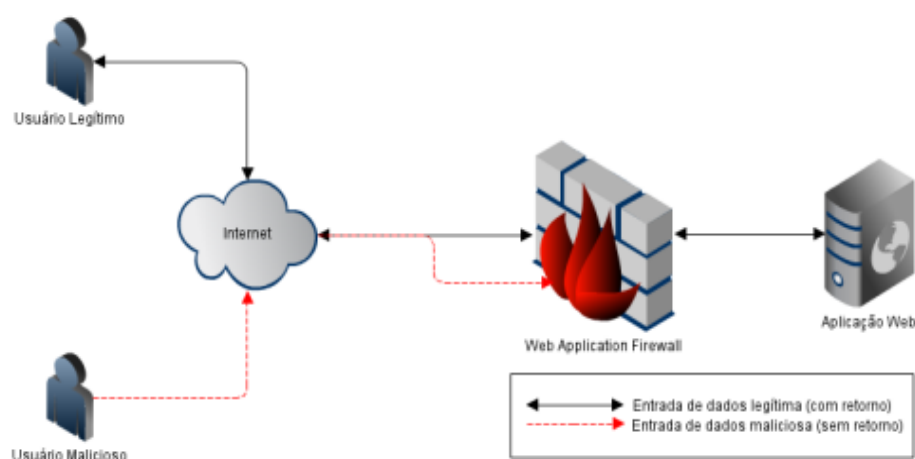
Segundo IPA (2011, p. 9), “o WAF é um hardware ou software que protege aplicações Web de ataques que exploram as vulnerabilidades nas aplicações Web”.

Os firewalls de aplicações web (WAF), são responsáveis por controlar a entrada, saída e acesso de aplicativos ou serviços WEB, estes foram desenvolvidos pela primeira vez no início dos anos 90 por Gene Spafford, Bill Cheswick e Marcus Ranum. A finalidade deste produto era baseado em um firewall baseado em rede que visava a proteção quando se navega pela internet, mas de princípio poderia lidar com poucas aplicações, logo após sua criação foi lançado ao mercado, para ajudar na solução dos problemas de ataques cibernéticos, porém com o passar dos anos essa aplicação acompanhou a constante evolução tecnológica.

Com a popularização da internet muitos serviços e aplicações passaram a centralizar suas operações na web, com isso aumentou consideravelmente a necessidade de proteger sistemas específicos baseado no protocolo HTTP (é sigla de HyperText Transfer Protocol que em português significa "Protocolo de Transferência de Hipertexto"). Em 2006 apareceram de forma mais concreta com fins de saciar essas necessidades os Web Application Firewalls (WAF)/Firewalls de Aplicação Web, como soluções independentes, mas também incorporadas como recurso para UTM (UTM é abreviatura em inglês para Unified Threat Management, que em uma tradução literal para o português seria algo como: *Gerenciamento Unificado de Ameaças*).

A função do WAF é inspecionar as transações entre os usuários e a aplicação Web, baseando-se em regras criadas pelo responsável que controla a aplicação. Vale lembrar que, o WAF é uma ferramenta que ajuda a minimizar o impacto dos ataques, e não uma solução definitiva que elimina as vulnerabilidades em uma aplicação Web. Alguns dos benefícios esperados por este método são: proteger aplicações Web de ataques que tentam explorar vulnerabilidades, detectar ataques que tentam explorar vulnerabilidades e proteger múltiplas aplicações Web de ataques. A figura a seguir demonstra como funciona um WAF.

Figura 5-Funcionamento de um WAF(Web Application Firewalls)



Fonte: Eveo (2016)

Pode ser visto na figura 5 dois tipos de usuário, o usuário legítimo e o usuário malicioso. A seta de cor preta, indica o fluxo de dados executados com liberação das regras do firewall. Nela se pode perceber que a solicitação enviada pelo usuário chega até a aplicação Web, que retorna o que o usuário solicitou. Já no fluxo indicado pela linha tracejada, pode ser observado que o usuário malicioso tenta invadir através de alguma vulnerabilidade, porém o WAF nega este acesso, sem dar qualquer retorno ao usuário.

2.4.1 Firewall Web

Com o surgimento dos firewalls para redes e computadores, notou-se um aumento significativo para a segurança de dados de indivíduos e organizações.

O desenvolvimento de aplicações Web distingue-se do desenvolvimento de aplicações tradicionais por dois motivos. O primeiro é pelo rápido crescimento dos requisitos das aplicações Web. O segundo é pela rápida mudança de conteúdo, ou seja, as aplicações Web evoluem e sofrem constantes mudanças. (PRASAD E RAMAKRISHNA, 2011, p. XX)

Porém, com práticas cada vez mais eficientes de ciber-ataques, algumas dessas ferramentas de segurança (firewall) ficaram, no entanto, ultrapassadas, necessitando assim de uma constante evolução para suprir a necessidade de proteção de dados. Essa urgência com fins de proteger os dados fez surgir novas soluções de segurança, como o Web Application Firewall. O WAF trabalha para impedir a exposição de dados não autorizada em um site ou aplicativo baseado na web ele visa monitorar, filtrar e bloquear automaticamente o tráfego de dados potencialmente maliciosos, fazendo com que assim a TI da empresa tenha uma rede mais segura. Várias são as empresas que trabalham oferecendo os sistemas de WAF, porém a mais conhecida em nosso meio é a MikroTik.

2.5 Mikrotik

A Mikrotik fundada em 1995, tem sua sede situada em Riga cidade de grande importância na Letônia. Ela ficou conhecida no cenário mundial com a prática de desenvolvimento e venda de sistemas WISP (*Wireless Internet Service Providers*/Prestador de serviços de Internet sem fio). A Mikrotik provê estes sistemas WISP em vários outros países como: Iraque, Brasil, Gana, Kosovo entre outros. Seu sistema operacional próprio de suas ferramentas foi desenvolvido para manipular servidores e roteadores “routerboard”, e com este sistema sua fama se propagou mundialmente pois, seus equipamentos já são oferecidos com o próprio sistemas operacionais instalado, facilitando assim a manipulação e desenvolvimento de tarefas de acordo com a necessidade do usuário. Vale lembrar que seu sistema operacional pode ser também instalado em um Desktop comum, e atualmente esse sistema operacional é considerado um dos melhores e mais completos para servidores e roteadores do mercado, sendo referência nacional e internacional. Vários são os equipamentos que empresa Mikrotik fabrica, porém o mais conhecido é o Mikrotik RouterOS.

2.5.1 Mikrotik RouterOS - Recursos

O Mikrotik RouterOS é um equipamento operacional que tem marcado o mercado de TI expressivamente devido às suas inúmeras funcionalidades, robustez, estabilidade e principalmente pela facilidade de uso.

O Mikrotik routerOS, assim como muitos roteadores profissionais, pode ser utilizado de várias maneiras. No entanto, uma rede depende de um planejamento adequado para sua aplicação. Podemos citar vários itens que fazem parte de um planejamento apropriado, mas é o conhecimento somado ao bom senso que deverão fazer parte desta estrutura. (BARION, 2011, p. 30).

É baseado em Linux, e o seu sistema pode ser instalado em um PC comum ou embarcado em placas compactas, as Routerboards fabricadas pelos próprios desenvolvedores do Mikrotik RouterOS. Uma das características que distinguem este equipamento de outros sistemas concorrentes é a facilidade e praticidade que a interface de configuração proporciona ao

usuário/administrador de rede. Fazendo com que, um simples click's de mouse possa implementadas complexas regras de Firewall, QoS, protocolos de roteamento dinâmico e etc.

De acordo com a BARION (2011) as vantagens oferecidas pelo sistema Operacional routerOS são:

- Performance otimizada com o protocolo proprietário
- Alta disponibilidade com o protocolo VRRP
- Possibilidade de agregar interfaces
- Poucas exigências de recursos de hardware
- Qualidade de serviço avançado
- Firewall
- Protocolo Spanning Tree em bridge com filtros.
- Alta velocidade com 802.11a/b/g com criptografia WEP/WPA
- WDS e AP's Virtuais
- Portal Captativo (Hotspot) com acesso Plug & Play
- Roteamento com os protocolos RIP, OSPF e BGP
- Acesso remoto com amigável aplicativo Windows – Winbox e também administração WEB
- Administração por telnet, mac-telnet, ssh e console
- Configuração e monitoramento em tempo real

Nota-se a enorme quantidade de aplicações desse dispositivo, porém o que será abordado neste trabalho é a sua funcionalidade para o desenvolvimento e controle de um Firewall de aplicação web.

2.5.2 Mikrotik RouterOS – Firewall de aplicação web

O firewall implementa a filtragem de pacotes e, permite o fornecimento de funções de segurança que são usadas para gerenciar o fluxo de dados do roteador e para o mesmo. Junto com a Network Address Translation, serve como uma ferramenta que impedir o acesso não autorizado a redes conectadas diretamente e ao próprio roteador, igual a um filtro de dados para o tráfego de entrada e saída.

Os firewalls de rede mantêm as ameaças externas longe dos dados confidenciais disponíveis na rede. Sempre que as redes diferentes são unidas,

há sempre uma ameaça que alguém de fora da sua rede invadirá sua LAN. Tais arrombamentos podem resultar em dados privados sendo roubados e distribuídos, dados esses que são valiosos e não podem ser alterados ou destruídos, ou discos rígidos inteiros sendo apagados. Os firewalls são usados como um meio de prevenir ou minimizar os riscos de segurança inerentes à conexão com outras redes. O firewall configurado corretamente desempenha um papel importante na implantação de infra-estrutura de rede eficiente e segura.

De acordo com a empresa MikroTik, o Sistema Operacional RouterOS possui uma implementação de firewall muito poderosa com recursos, incluindo:

- inspeção de pacotes com estado
- Detecção de protocolo de camada 7
- filtragem de protocolos peer-to-peer
- classificação de tráfego por:
 - endereço MAC de origem
 - Endereços IP (rede ou lista) e tipos de endereço (broadcast, local, multicast, unicast)
 - porta ou faixa de portas
 - Protocolos IP
 - Opções de protocolo (tipo ICMP e campos de código, sinalizadores TCP, opções de IP e MSS)
 - interface do pacote chegou ou saiu através
 - fluxo interno e marcas de conexão
 - Byte DSCP
 - conteúdo de pacotes
 - taxa na qual os pacotes chegam e números sequenciais
 - tamanho do pacote
 - horário de chegada do pacote

No estudo de caso será mostrado algumas dessas funcionalidades do Firewall do Mikrotik routerOS.

3 ESTUDO DE CASO: Prefeitura Municipal de Itaguaru

Neste capítulo será apresentado um estudo de caso desenvolvido na Prefeitura Municipal de Itaguaru. O conteúdo desse estudo inicia-se com o capítulo um com a apresentação da prefeitura, contendo história da mesma, juntamente com a história do município, sendo este bem sucinto e de fácil entendimento.

Em seguida será apresentado o sistema de firewall responsável pela segurança da informação e controle da rede da instituição abordada. Software esse que abrange os recursos computacionais utilizados, com a implementação do firewall via web fornecido pela Mikrotik.

3.1 Breve Histórico

A Prefeitura Município de Itaguaru foi criada pela lei nº 2.101, de 14/11/1958 e instalado em 01/01/1959. Sua história começa por dois fazendeiros, Napoleão Pires de Barros e Urgélio Teixeira que queriam a criação desse município visando facilitar o intercâmbio com as cidades vizinhas e possivelmente uma maior valorização das terras que eram de excelente qualidade. Mas a lei de criação ocorreu, no mandato do primeiro prefeito de Itaguaru, Morbeck José de Andrade, que na época foi nomeado pelo governador do estado. O primeiro prefeito municipal constitucional foi o Sr. Napoleão Pires de Barros, e como vice-prefeito o Sr. Oscar de Oliveira Barbosa. O município de Itaguaru está localizado na zona fisiográfica de Mato Grosso de Goiás, e limita-se com os municípios de Heitorai, Itaberaí, Jaraguá, Uruana, Itaguari e Taquaral de Goiás.

Atualmente a Prefeitura Municipal de Itaguaru tem como prefeito o Sr. Euripedes Potenciano da Silva e como vice o Sr. Oscar Martins. A prefeitura é subdividida em sete secretarias com vários departamentos espalhados pelo prédio da mesma e suas unidades localizadas em várias regiões da cidade. Um dos objetivos da administração pública municipal é, proporcionar e assegurar a satisfação das necessidades coletivas variadas, tais como a segurança, a educação, a cultura, a saúde e o bem-estar da população em geral. A Prefeitura conta com vários aparatos tecnológicos, espalhados por todas as suas secretarias e respectivos departamentos, lida também com informações de

grande risco e que devem ser tratadas com sigilo e proteção total, para isso a mesma conta com a área da TI que ajuda na segurança e garante a integridade de informações e dados da instituição.

3.2 Firewall Implantado na Prefeitura de Itaguaru: Entrevista com o responsável pela TI.

A seguir, entrevista feita com o Sr Klayton Pimenta responsável pela TI da Prefeitura Municipal de Itaguaru.

Surgimento da Ideia de Implantação do Firewall na Prefeitura:

A princípio a prefeitura não tinha nenhum mecanismo de segurança para auxiliar na proteção de dados, só tinha um roteador cuja função era gerenciar a rede disponibilizando acesso a todos. O mesmo não oferecia segurança as informações, fazendo com que todo elas fossem totalmente abertas, qualquer um podia chegar conectar-se e acessar os arquivos da rede ou o próprio sistema. Essa foi a principal fragilidade encontrada, assim juntamente com o prefeito foi sugerido a implantação do firewall para poder ter um controle de acesso além de filtrar quais informações poderiam ser acessadas em determinados departamentos e computadores. Fazendo com que as informações pudessem ser trabalhadas com sigilo e ficassem seguranças, com um risco menor de perda de informações. O firewall está em funcionamento na prefeitura desde março de 2012.

Etapas de Implantação:

O primeiro passo foi entrar em contato com o prefeito mostrando para o mesmo que a rede poderia ser facilmente invadida e que os dados e informações corriam risco. A solução foi apresentada com a utilização do WAF, após a aprovação o segundo passo foi a compra do equipamento (um routerboard fornecido pela mikrotik cuja versão é RB 250GS, e seu custo foi de

aproximadamente R\$:70,00) para a construção desse mecanismo. Logo em seguida foi feita toda a instalação do equipamento e configuração do mesmo, estipulando as regras de acesso e filtragem de dados.

Dificuldades Encontradas na Implementação:

Até então as dificuldades foram poucas, pois o equipamento é facilmente encontrado para compra, a rede se adapta rapidamente, a instalação é rápida, porém o profissional deve ser capacitado para a configuração do equipamento. A única dificuldade encontrada foi com o usuário, pois com o acesso livre eles podiam fazer qualquer coisa, como assistir vídeos do youtube baixar arquivos e etc. Depois do firewall já instalado esse acesso aberto do usuário ficou totalmente controlado.

Comportamento do Usuário Antes e Depois da Implementação:

Como dito anteriormente o acesso era totalmente livre o usuário poderia acessar qualquer página sem qualquer restrição podiam conectar outros aparelhos a rede e fazer o que bem entender, depois do firewall pronto essa realidade mudou, pois as regras de acesso foram estabelecidas o compartilhamento de dados dentro da rede foi filtrado fazendo com que somente os autorizados pudessem compartilhar das informações, além de que somente os computadores autorizados pudessem acessar a rede. E a navegação na internet foi restringida em algumas páginas, além de toda rede ser monitorada pela TI.

O Ganho Que a Prefeitura Obteve com o WAF:

Foram vários os ganhos que se obteve, a começar pela proteção dos dados e a filtragem de pacotes recebidos e enviados externamente e internamente, pode se observar a redução de vírus nos computadores pois, com a navegação sem preocupação do usuário e a quantidade de arquivos baixados os computadores muita das vezes tinham que ser formatados, além do risco que eles corriam em ser atacados por qualquer tipo de prática de hackers. A banda

de consumo de internet ficou menor, então, com essa diminuição foi possível fazer com que as operações nos sistemas utilizados pela prefeitura fossem mais rápidos. A integridade e a autenticidade das informações detidas pela entidade ficaram seguras, entre outros benefícios.

As vantagens de utilizar esse WAF:

A mais importante vantagem é a segurança, com essa ferramenta você vai ter uma rede segura, podendo aplicar suas próprias políticas e regras, tendo um mapeamento total da rede, podendo também definir quais máquinas podem acessar essa rede. É um dos métodos mais eficazes e utilizados no mundo todo. Além de poder utilizar essa ferramenta em uma rede doméstica, dentro da sua própria casa, para bloquear os acessos dos seus filhos ou de qualquer outra pessoa, é uma ferramenta muito eficiente. É barato também, então é acessível para todos.

3.3 Equipamentos e Sistemas de Gerenciamento do Firewall Web

3.3.1 Equipamentos

Neste tópico serão mostrados os equipamentos utilizados para a construção do firewall as telas de controle do mesmo, e as regras de segurança da prefeitura municipal de Itaguaru. A Figura 6 mostra algumas das RBs Mikrotik que podem ser utilizadas para a criação do Firewall Web. Temos o exemplo na figura 6 da RB250GS e RB1100AH.

Figura 6-RouterBoard MikroTik



Fonte: Arquivo do Autor

Lembrando que as RBs (Routerboard MikroTik), são especificadas em 3 tipos: pequeno, médio e grande porte. A utilização de cada uma depende da necessidade e tamanho da empresa ou instituição. Nessa figura temos o exemplo de uma RB de pequeno porte e outra de grande porte, ambas podem ser utilizadas em uma empresa, instituição ou até mesmo em uma rede doméstica.

A seguir, temos a imagem do servidor da prefeitura e o RB250GS instalado no mesmo.

Figura 7-Servidor da Prefeitura



Fonte: Arquivo do Autor

O servidor da prefeitura contém todos os dados e informações importantes da mesma, então a necessidade de proteger essas informações é grande, com isso a implementação do firewall foi eficaz para que a segurança da informação seja garantida.

Figura 8-RB250GS e Equipamentos de rede



Fonte: Arquivo do Autor

O sistema operacional routerOS Mikrotik permite a instalação em padrões de servidores, seja Standard, PC Profissional ou Desktop convencional. Esse equipamento auxilia no controle da rede e do firewall permitindo a configuração e implementação de regras de segurança.

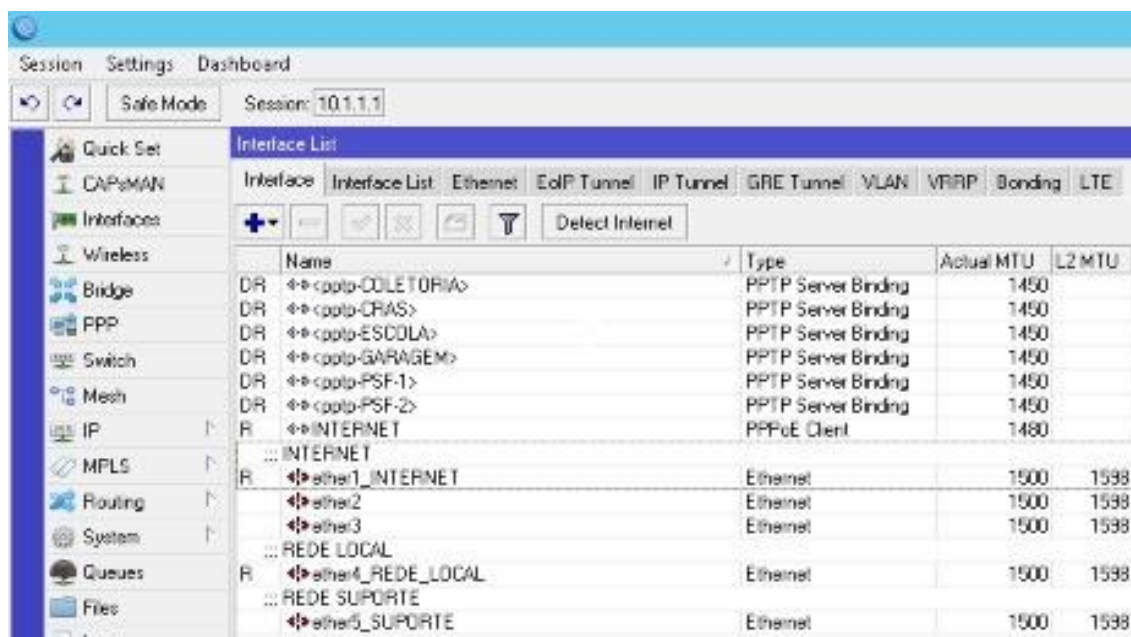
3.3.2 Sistemas de Gerenciamento do Firewall

As figuras a seguir são prints de tela do sistema operacional routerOS da Mikrotik, em operação na prefeitura de Itaguaru.

3.3.3 Tela inicial

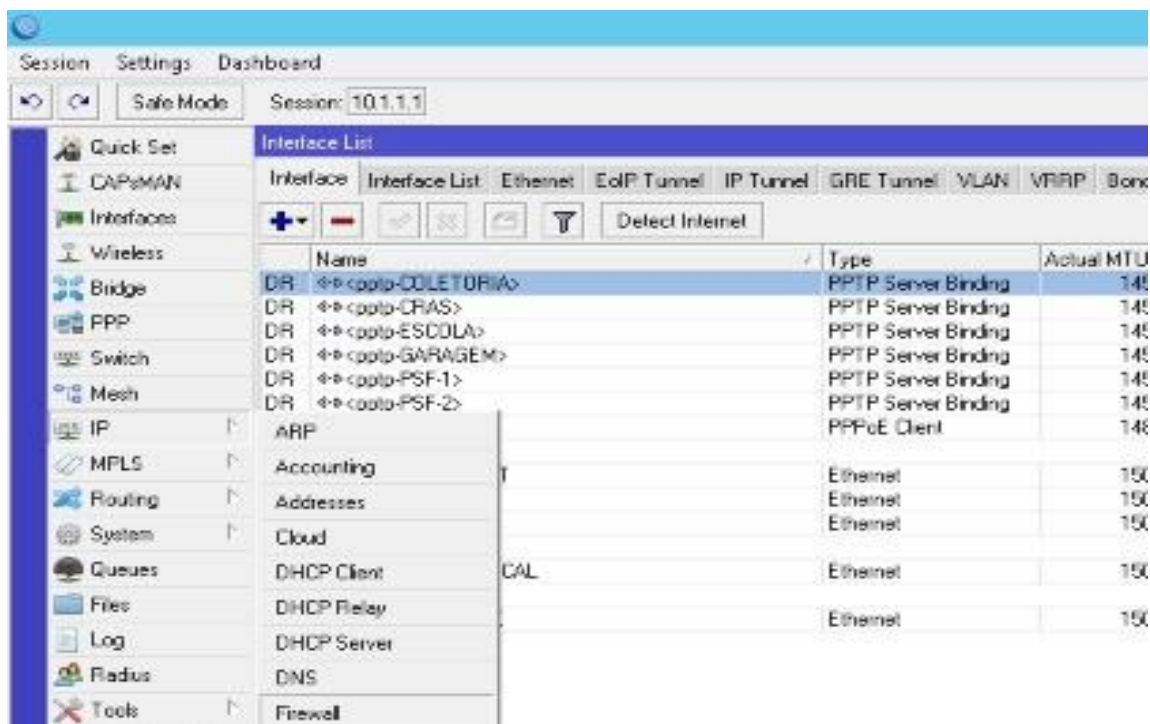
Nas imagens a seguir podemos observar as telas principais do sistema operacional da Mikrotik.

Figura 9-Tela Inicial



Fonte: Arquivo do Autor

Figura 10-Tela inicial e ferramentas extras do Sistema Operacional Mikrotik



Fonte: Arquivo do Autor

Estas, são as telas responsáveis pela configuração do firewall e de suas demais ferramentas que são integradas a esse SO. Pode se observar também o monitoramento do firewall sobre alguns departamentos que compõem a prefeitura, como por exemplo: Coletoria, Cras, Escola e etc.

3.3.4 Regras do Firewall

As figuras a seguir demonstra as estruturas do S.O. do firewall mikrotik, as regras estabelecidas e o monitoramento de acessos.

Figura 11-Estrutura do Firewall-Regras

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter.	Out. In...	Bytes	Packets
0	drop	forward								0B	0
1	drop	forward								120KB	206
2	drop	forward			6 (tcp)		443			0B	0
3	drop	forward			6 (tcp)		443			0B	0
4	drop	input								11,8KB	21
5	acc...	input								5,9MB	84.973
6	acc...	input			1 (ic...					22,3KB	363
7	drop	input								15,8MB	341.009
8	drop	forward			6 (tcp)					249,1KB	6.001

Fonte: Arquivo do Autor

Figura 12-Regras Estabelecidas no Firewall da Prefeitura

#	Action	Chain	Src. Address	Dst. Address
0	drop	forward		
1	drop	forward		
2	drop	forward		
3	drop	forward		
4	drop	input		
5	acc...	input		
6	acc...	input		
7	drop	input		
8	drop	forward		
9	acc...	forward		
10	acc...	forward		

Fonte: Arquivo do Autor

Figura 13- Monitoramento de acesso

Name	Address	Timeout	Creation Time
Facebook	31.13.24.0/21		Jul/30/2018 19:5...
Facebook	31.13.64.0/19		Jul/30/2018 19:5...
Facebook	31.13.64.0/24		Jul/30/2018 19:5...
Facebook	31.13.69.0/24		Jul/30/2018 19:5...
Facebook	31.13.70.0/24		Jul/30/2018 19:5...
Facebook	31.13.71.0/24		Jul/30/2018 19:5...
Facebook	31.13.72.0/24		Jul/30/2018 19:5...
Facebook	31.13.73.0/24		Jul/30/2018 19:5...
Facebook	31.13.76.0/24		Jul/30/2018 19:5...
Facebook	31.13.77.0/24		Jul/30/2018 19:5...
Facebook	31.13.79.0/24		Jul/30/2018 19:5...
Facebook	31.13.78.0/24		Jul/30/2018 19:5...
Facebook	31.13.79.0/24		Jul/30/2018 19:5...
Facebook	31.13.80.0/24		Jul/30/2018 19:5...
Facebook	66.220.144.0/20		Jul/30/2018 19:5...
Facebook	66.220.144.0/21		Jul/30/2018 19:5...
Facebook	66.220.0.0/16		Jul/30/2018 19:5...
Facebook	66.220.152.0/21		Jul/30/2018 19:5...
Facebook	66.220.159.0/24		Jul/30/2018 19:5...
Facebook	69.63.176.0/21		Jul/30/2018 19:5...
Facebook	69.63.176.0/24		Jul/30/2018 19:5...
Facebook	69.63.184.0/21		Jul/30/2018 19:5...
Facebook	69.171.224.0/19		Jul/30/2018 19:5...
Facebook	69.171.224.0/20		Jul/30/2018 19:5...
Facebook	69.171.0.0/16		Jul/30/2018 19:5...
Facebook	69.171.239.0/24		Jul/30/2018 19:5...
Facebook	69.171.240.0/20		Jul/30/2018 19:5...
Facebook	173.252.64.0/18		Jul/30/2018 19:5...
Facebook	173.252.70.0/24		Jul/30/2018 19:5...
Facebook	173.252.96.0/19		Jul/30/2018 19:5...
Facebook	204.15.20.0/22		Jul/30/2018 19:5...
Spotify	194.132.168.0/21		Aug/01/2018 11:...
Spotify	193.235.232.0/22		Aug/01/2018 11:...
Spotify	104.154.127.0/24		Aug/01/2018 11:...

Fonte: Arquivo do Autor

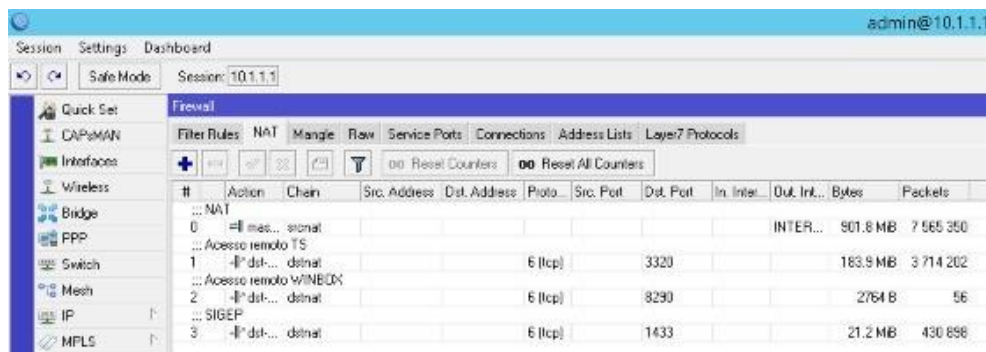
O Firewall mikrotik possui recursos que permitem integrar regras e exceções para cada computador da rede, um exemplo, um computador da rede pode acessar livremente a internet enquanto os demais não. Isso varia da política de segurança da instituição, empresa e etc. Nessas imagens pode ser visto algumas regras implantadas na prefeitura, regras essas que são para os computadores da rede, e que em alguns casos há exceções. Essas regras podem ser incluídas, alteradas ou apagadas pelo usuário do SO Mikrotik. Podemos observar o monitoramento de cada regra, se o usuário tenta acessar uma regra bloqueada o mesmo fica gravado mostrando o IP do computador e a data de acesso, e isso funciona para regras de acessos permitidos.

Todas as regras implementadas na Prefeitura Municipal de Itaguaru, estão em anexo 1.

3.3.5 Estrutura NAT

Aqui é onde é feita a tradução de endereços por exemplo: mascaramento do IP. Observe a figura 14.

Figura 14-Estrutura NAT



The screenshot shows the Mikrotik WinBox interface for Firewall NAT configuration. The 'Filter Rules' tab is active, and the 'NAT' sub-tab is selected. A table lists four NAT rules with their respective actions, chains, and traffic statistics.

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	Bytes	Packets
0	... NAT	...							INTER...	901.8 MB	7 565 350
1	... Acesso remoto TS	...			6 (tcp)		3320			183.9 MB	3 714 202
2	... Acesso remoto WINEDK	...			6 (tcp)		8290			2764 B	56
3	... SIGEP	...			6 (tcp)		1433			21.2 MB	430 898

Fonte: Arquivo do Autor

Esse tipo de técnica permite que um computador em uma rede possa utilizar endereços de IP diferentes para a comunicação interna e externa. Ou seja, um pacote de dados a ser enviado ou recebido de sua estação de trabalho em sua rede local, vai até o servidor onde seu IP é trocado pelo IP do servidor a substituição do IP da rede local valida o envio do pacote na internet, no retorno do pacote acontece a mesma coisa porém ao contrário o que garante que o pacote chegue ao seu destino. Essa opção ajuda para que os IPs pessoais não sejam expostos a internet.

3.3.6 Connection

É a habilidade do roteador em manter o estado da informação relativa às conexões, como endereços IP de origem e destino, estados da conexão, tipos de protocolos e etc. Na figura 15 pode ser observado todo o tráfego dos computadores da rede, tempos de acesso, os IPs acessados o fluxo de dados e etc.

Figura 15-Segmento de conexões

Filter	Src. Address	Out. Address	Proto.	Connect...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	0.0.0.0	224.0.0.1	2 (ig		00:09:56			543.6 K/B/0 B
C	0.0.0.0	255.255.255.255	139		00:09:57			1618.6 K/B/0 B
C	10.0.0.3:62469	17.249.53.32:5223	S (rspl		21:56:34	established	0 bps/0 bps	117 B/0 B
SAICs	10.0.0.3:62469	47.244.52.243:9091	S (rspl		22:13:05	established	0 bps/0 bps	116 B/40 B
SAICs	10.0.0.3:63171	157.240.12.54:5222	S (rspl		23:59:59	established	320 bps/415 bps	2672 B/2303 B
SAICs	10.0.0.3:63172	17.249.53.32:5223	S (rspl		23:59:40	established	0 bps/0 bps	6.0 K/B/5.5 K/B
SAICs	10.0.0.4:38400	84.233.190.198:5228	S (rspl		21:12:25	established	0 bps/0 bps	1351 B/640 B
SAICs	10.0.0.4:38704	84.233.190.198:5228	S (rspl		18:42:59	established	0 bps/0 bps	2218 B/770 K/B
SAICs	10.0.0.4:39170	84.233.190.198:5228	S (rspl		20:04:14	established	0 bps/0 bps	1289 B/640 B
SAICs	10.0.0.4:39167	84.233.190.198:5228	S (rspl		22:15:25	established	0 bps/0 bps	1742 B/620 B
SAICs	10.0.0.6:48170	77.234.42.39:89	S (rspl		23:59:59	established	2.7 Kbps/2.0 kbps	34.0 K/B/547.5 K/B
SAICs	10.0.0.6:48862	92.73.237.45:443	S (rspl		23:59:47	established	0 bps/0 bps	126.1 K/B/81.3 K/B
SAICs	10.0.0.6:48863	198.227.75.250:443	S (rspl		23:59:57	established	0 bps/0 bps	565.9 K/B/46.2 M/B
SAICs	10.0.0.6:48864	198.227.75.250:443	S (rspl		23:59:59	established	135.3 Kbps/0 bps	666.3 K/B/46.2 M/B
SAICs	10.0.0.6:48867	92.73.237.45:443	S (rspl		23:59:50	established	0 bps/0 bps	3116 B/2016 B
SAICs	10.0.0.6:48628	215.98.202.170:443	17 (M...		00:02:37		0 bps/0 bps	2419 B/2249 B
SAICs	10.0.0.6:48938	104.154.125.236:4070	S (rspl		00:04:59	established	0 bps/7320 bps	151.6 K/B/115.7...
SAICs	10.0.0.6:48899	208.45.117.181:443	S (rspl		23:58:13	established	0 bps/0 bps	27.3 K/B/23.4 K/B
SAICs	10.0.0.6:48812	84.233.190.198:5228	S (rspl		23:59:34	established	0 bps/0 bps	10.4 K/B/16.5 K/B
SAICs	10.0.0.6:50436	25.196.224.3:443	S (rspl		23:59:08	established	0 bps/0 bps	4636 B/21.7 K/B
SAICs	10.0.0.6:50442	151.149.231.100:80	S (rspl		23:57:57	established	0 bps/0 bps	434 B/1217 B
SAICs	10.0.0.6:50444	172.217.29.14:80	S (rspl		23:59:02	established	0 bps/0 bps	425 B/408 B
SAICs	10.0.0.10:33327	215.98.202.170:443	S (rspl		23:58:39	established	0 bps/0 bps	3968 B/6.5 K/B
SAICs	10.0.0.10:33328	215.98.202.170:443	S (rspl		23:59:37	established	0 bps/0 bps	12.4 K/B/483.7 K/B
SAICs	10.0.0.10:33330	215.98.202.170:443	S (rspl		23:58:39	established	0 bps/0 bps	1744 B/2244 B
SAICs	10.0.0.10:35120	191.7.29.220:443	17 (M...		00:00:53		0 bps/0 bps	3079 B/461.1 K/B
SAICs	10.0.0.10:35276	84.233.190.198:5228	S (rspl		23:57:53	established	0 bps/0 bps	4547 B/57.7 K/B
SAICs	10.0.0.10:36990	172.217.30.85:443	17 (M...		00:01:09		0 bps/0 bps	5.2 K/B/18.1 K/B
SAICs	10.0.0.10:36922	215.98.202.170:443	17 (M...		00:01:59		0 bps/0 bps	3774 B/2891 B
SAICs	10.0.0.10:41268	215.98.202.170:443	17 (M...		00:00:54		0 bps/0 bps	3538 B/3673 B
SAICs	10.0.0.10:42461	84.233.190.198:5228	S (rspl		00:09:57	established	0 bps/0 bps	2417 B/6395 B
SAICs	10.0.0.10:42462	84.233.190.198:5228	S (rspl		00:06:24	established	0 bps/0 bps	1549 B/640 B
SAICs	10.0.0.10:44076	13.107.3.128:443	S (rspl		23:59:43	established	0 bps/0 bps	1652 B/5.4 K/B
SAICs	10.0.0.10:44368	198.227.75.250:443	S (rspl		23:57:37	established	0 bps/0 bps	25.5 K/B/8.7 K/B
SAICs	10.0.0.10:44369	215.98.202.170:443	S (rspl		23:57:39	established	0 bps/0 bps	2308 B/1177 B
SAICs	10.0.0.10:46362	172.217.30.85:443	S (rspl		23:57:53	established	0 bps/0 bps	787 B/4755 B
SAICs	10.0.0.10:47076	84.233.190.198:5228	S (rspl		23:44:15	established	0 bps/0 bps	3604 B/6.3 K/B
SAICs	10.0.0.10:46746	172.217.152.110:443	S (rspl		23:59:36	established	0 bps/0 bps	1362 B/4649 B
SAICs	10.0.0.10:46748	172.217.152.110:443	S (rspl		23:59:41	established	0 bps/0 bps	1460 B/4700 B
SAICs	10.0.0.10:49775	215.98.202.132:443	17 (M...		00:02:36		0 bps/0 bps	6.1 K/B/2696 B
SAICs	10.0.0.10:51574	203.119.201.254:80	S (rspl		23:56:49	established	0 bps/0 bps	2298 B/2286 B
SAICs	10.0.0.10:54694	92.17.124.79:5223	S (rspl		23:56:50	established	0 bps/0 bps	2617 B/2980 B
SAICs	10.0.0.10:56019	157.240.12.54:443	S (rspl		23:46:30	established	0 bps/0 bps	2673 B/5.9 K/B
SAICs	10.0.0.10:58346	157.240.12.54:5222	S (rspl		23:57:39	established	0 bps/0 bps	21.3 K/B/25.7 K/B
SAICs	10.0.0.10:65624	157.240.12.54:5222	S (rspl		23:59:15	established	0 bps/0 bps	2640 B/6.9 K/B
SAICs	10.0.0.10:65624	84.233.190.198:5228	S (rspl		15:55:15	established	0 bps/0 bps	7.9 K/B/27.2 K/B
SAICs	10.0.0.11:56395	17.249.53.32:5223	S (rspl		23:59:57	established	0 bps/0 bps	6.9 K/B/5.6 K/B
SAICs	10.0.0.11:50465	157.240.12.54:5222	S (rspl		00:00:05	last ask	0 bps/0 bps	18.0 K/B/25.0 K/B
SAICs	10.0.0.11:60929	157.240.12.54:443	S (rspl		23:59:22	established	0 bps/0 bps	2440 B/6.1 K/B
SAICs	10.0.0.13:37764	108.177.127.189:443	S (rspl		21:59:04	established	0 bps/0 bps	2370 B/10.1 K/B
C	10.0.0.13:42470	84.233.190.198:5228	S (rspl		18:23:14	established	0 bps/0 bps	1380 B/4909 B
SAICs	10.0.0.13:42470	84.233.190.198:5228	S (rspl		18:15:09	established	0 bps/0 bps	1480 B/0 B
SAICs	10.0.0.13:42470	84.233.190.198:5228	S (rspl		17:53:59	established	0 bps/0 bps	1688 B/1565 B
SAICs	10.0.0.13:45418	84.233.190.198:5228	S (rspl		18:59:27	established	0 bps/0 bps	856 B/263 B
SAICs	10.0.0.13:47434	191.232.99.228:443	S (rspl		21:26:45	established	0 bps/0 bps	1338 B/640 B
SAICs								2569 B/5.6 K/B

Fonte: Arquivo do Autor

Vale lembrar que, todos os computadores da rede devem ser cadastrados no sistema operacional do firewall, caso o contrário o mesmo não terá acesso a rede nem ao servidor. Os prints de tela realizados foram das principais telas do SO RouterOs, e não foi aprofundado como cada regra é criada ou como o sistema é manipulado pois, esses quesitos devem ser feitos por um profissional capacitado.

3.3.7 Entrevista com usuários da rede

Foi feita uma entrevista estruturada com 20 usuários da rede de diferentes departamentos, sobre o antes e depois do Firewall aplicado. Nessa entrevista foi feita 4 perguntas com respostas de sim ou não:

***Houve melhora na segurança da rede?**

18 Responderam Sim 2 Responderam Não

***A comunicação da rede ficou mais rápida?**

13 Responderam Sim 7 Responderam Não

***O acesso à internet ficou mais rápido?**

16 Responderam Sim 4 Respondeu Não

***A formatação dos computadores continua frequentes?**

17 Responderam Sim 3 Responderam Não

4 CONSIDERAÇÕES FINAIS

Poucas são as pesquisas que perpassam a teoria, a metodologia e apresentam os resultados práticos, assim, em linhas findas, obsta ressaltar que a presente monografia se preocupou com essa totalidade, não só com o objetivo de encerrar o curso, mas, com o compromisso social de servir de fonte de pesquisa e instrução para futuros leitores.

Como exposto ao delongar da explanação deste, ficou constatado que até mesmo os analfabetos digitais são capazes de compreender, ainda que não apresentem exatidão, os perigos que a internet pode oferecer. Assim, também restou provado que com as transformações e a abrangência da tecnologia enquanto ferramenta social, fez com que todas as classes tivessem acesso a TI.

Com a popularização do conhecimento, manuseio e uso prático das tecnologias, foi necessário que os profissionais do meio se desdobrassem no campo da elaboração e criação de programas que pudessem se encarregar de garantir a segurança da informação para empresas e demais segmentos que assim desejar ou necessitar.

Uma vez compreendida a demanda de segurança da informação, faz-se necessária a busca pelo modelo mais confiável e mais adequado, não só para armazenar de forma segura os dados, mas para praticizar o trabalho de todos os setores envolvidos, dando celeridade e segurança adequada.

No presente trabalho ficou visível a segurança que um WAF oferece, a importância de se utilizá-lo e seu baixo custo. Lembrando também de suas outras vantagens para a empresa, entidade ou até mesmo em uma rede doméstica onde essa ferramenta é implementada.

Contudo, esse trabalho vai permitir a disseminação de conhecimento ampliando o assunto tratado, com uma grande expectativa que todos que tenham acesso a este, também consigam ter um conhecimento maior do assunto tratado.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTO ALVES, Gustavo. **Segurança da informação: Uma visão inovadora da gestão**. 1. Ed. Rio de Janeiro: Ciência Moderna Ltda, 2006 1 p.

Alerta Security. **Segurança da informação: entenda as principais ameaças**. Disponível em: <<https://www.alertasecurity.com.br/blog/188-seguranca-da-informacao-entenda-as-principais-ameacas>>. Acesso em: 19 de Março de 2018.

Alerta Security. **Tipos de Firewall e suas Especificações**. Disponível em: <<https://alertasecurity.com.br/downloads/ebook/TIPOS-DE-FIREWALL-E-SUAS-ESPECIFICA%C3%87%C3%95ES.pdf>>. Acesso em: 06 de Setembro de 2018.

ARAUJO, Nonata S. **Segurança da Informação (TI). Administradores**. Disponível em: <<http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933>>. Acesso em: 19 de março de 2018.

BARBOSA, Maxuel. **Firewall Via Web**. Rio de Janeiro: Editora Ciência Moderna., 2012. 139p.

BARION, Rogério. **Mikrotik RouterOS: guia prático**. Vol 1. Porto Alegre: Sulina, 2011. 247p.

BARION, Rogério. **Mikrotik: routerOS network associate : guia prático**. Vila Velha: Above publicações, 2012. 262p.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. **Firewall e Segurança na Internet**. 2ª ed. Tradução: Edson Frumankiewicz. São Paulo: Bookman, 2003. 400 p.

DAMÁSIO, M. J. **Tecnologia e educação: as tecnologias da informação e da comunicação e o processo educativo**. Lisboa: Vega, 2007. 45p.

Empreender em Goiás. **Mercado de TI ferve em Goiás**. Disponível em: <<https://www.empreenderemgoias.com.br/2017/05/28/mercado-de-ti-ferve-em-goias/>>. Acesso em: 18 de julho de 2018.

Eveo. **WAF- Web Application Firewall**. Disponível em: <<https://www.eveo.com.br/blog/waf-web-application-firewall/>>. Acesso 02 de Outubro de 2018.

Folha de São Paulo. **Internet foi criada em 1969 com o nome de Arpanet nos EUA**. Disponível em: <<https://www1.folha.uol.com.br/fofolha/cotidiano/ult95u34809.shtml>>. Acesso em: 18 de julho de 2018.

FORD L, **Manual Completo de Firewall Pessoal**. 1ª ed. São Paulo: Personal Education do Brasil, 2002. 244p.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. **Segurança de Redes em ambientes cooperativos**. 2.ed. São Paulo: Futura, 2003.

GUIMARÃES, Matuzalém. **Segurança da Informação na Internet. Viva o Linux**, Brasil, mai. 2008. Disponível em: <<http://www.vivaolinux.com.br/artigo/Seguranca-da-Informacao-na-Internet?pagina=1>>. Acesso em: 19 de março de 2018.

HADNAGY, Christopher, **Social Engineering The Art Of Human Hacking**. Disponível em: <<https://www.pdf-archive.com/2014/06/02/social-engineering-the-art-of-human-hacking/>>. Acesso em: 17 de julho de 2018.

IPA (INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN). **Web Application Firewall (WAF): A Handbook to Understand Web Application Firewall**. Japão, 2011.

JUCÁ, Humberto. **Técnicas avançadas de conectividade e Firewall em GNU/Linux**. Rio de Janeiro: Brasport, 2005.

MB Brasil. **Soluções em hardware Mikrotik RouterOS**. Disponível em: <http://mdbrasil.com.br/solucoesemhardware/mikrotik-routeros/>>. Acesso em: 04 de Outubro de 2018.

Mikrotik. **Manual de Firewall**. Disponível em: <<https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter>>. Acesso em 04 de Outubro de 2018.

MITNICK, Kevin D.; SIMON, William L. **MITNICK - A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: José Martins Braga, 2003. 286 p.

MOREIRA, Nilton Stringanci. **Segurança mínima: uma visão corporativa da segurança de informação**. Rio de Janeiro: Axcel Books, 2001.

NBSO. **Práticas de Segurança para Administradores de Redes Internet**. São Paulo, 2003. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html>. Acesso em: 21 Agosto de 2018.

Ostec. **Segurança Perimetro/Firewall**. Disponível em: <<https://ostec.blog/seguranca-perimetro/firewall>>. Acesso em 19 de julho de 2018.

Ostec. **Segurança Perimetro/Firewall UTM NGWF Diferença**. Disponível em: <<https://ostec.blog/seguranca-perimetro/firewall-utm-ngwf-diferenca>>. Acesso em 19 de julho de 2018.

Planalto. **Lei I11788** Disponível em:
<http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/I11788.htm>
Acesso em: 16 de Outubro de 2018.

PRASAD, A. V. K. and RAMAKRISHNA, S. **Mining for Web Engineering**. International Journal of Computer Trends and Technology (IJCTT), p. 151–156, 2011.

Prefeitura Municipal de Itaguara. **Sobre o Município/Nossa História**. Disponível em: <<https://itaguara.go.gov.br/sobre-o-municipio/nossa-historia/>>. Acesso em 16 de Outubro de 2018.

Profissionais TI. **Política de Segurança da Informação: conceitos característicos e benefícios**. Disponível em:
<<https://www.profissionaisiti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/>>. Acesso em 19 de março de 2018.

SÊMOLA, Marcos. **Gestão da Segurança Informação Uma visão executiva**. 2ª ed. Rio de Janeiro, RJ: Campus, 2003.

STONEBURNER, Gary. **Underlying Technical Models for Information Technology Security**. NIST Special Publication 800-33, 2001 22p.

Tec Mundo. **Quem é Kevin Mitnick?**. Disponível em:
<<https://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm>>. Acesso em: 14 de março de 2018.

Tech Tudo. **O que é Engenharia Social**. Disponível em:
<<http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/11/o-que-e-engenharia-social.html>>. Acesso em 17 de julho de 2018.

Anexo 1

Todas as regras do firewall implementadas na Prefeitura Municipal de Itaguaru:

```
# oct/26/2018 17:08:22 by RouterOS 6.43rc45
# software id = 8XUA-NXAZ
#
# model = 750GL
# serial number = 467B02D94E6E
/interface ethernet
set [ find default-name=ether1 ] comment=INTERNET
name=ether1_INTERNET speed=\
    100Mbps
set [ find default-name=ether2 ] speed=100Mbps
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] comment="REDE LOCAL"
name=ether4_REDE_LOCAL \
    speed=100Mbps
set [ find default-name=ether5 ] comment="REDE SUPORTE"
name=ether5_SUPORTE \
    speed=100Mbps
/interface pppoe-client
add add-default-route=yes disabled=no interface=ether1_INTERNET \
    keepalive-timeout=60 name=INTERNET password=212112 use-peer-
dns=yes user=\
    pref.itaguaru
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool1 ranges=192.168.50.2-192.168.50.245
add name=dhcp_pool2 ranges=10.0.0.1-10.1.1.0,10.1.1.2-10.255.255.254
add name=dhcp_pool3 ranges=10.0.0.1-10.1.1.0,10.1.1.2-10.1.1.253
/ip dhcp-server
add address-pool=dhcp_pool3 authoritative=after-2sec-delay disabled=no \
```

```
interface=ether4_REDE_LOCAL name=dhcp1
/interface pptp-server server
set enabled=yes
/ip address
add address=172.168.100.10/28 disabled=yes interface=ether1_INTERNET
network=\172.168.100.0
add address=192.168.50.1/24 disabled=yes interface=ether5_SUPORTE
network=\192.168.50.0
add address=10.1.1.1/8 interface=ether4_REDE_LOCAL network=10.0.0.0
/ip cloud
set ddns-enabled=yes
/ip dhcp-server network
add address=10.0.0.0/8 gateway=10.1.1.1
/ip dns
set servers=8.8.8.8,8.8.4.4
/ip firewall address-list
add address=31.13.24.0/21 list=Facebook
add address=31.13.64.0/19 list=Facebook
add address=31.13.64.0/24 list=Facebook
add address=31.13.69.0/24 list=Facebook
add address=31.13.70.0/24 list=Facebook
add address=31.13.71.0/24 list=Facebook
add address=31.13.72.0/24 list=Facebook
add address=31.13.73.0/24 list=Facebook
add address=31.13.76.0/24 list=Facebook
add address=31.13.77.0/24 list=Facebook
add address=31.13.75.0/24 list=Facebook
add address=31.13.78.0/24 list=Facebook
add address=31.13.79.0/24 list=Facebook
add address=31.13.80.0/24 list=Facebook
add address=66.220.144.0/20 list=Facebook
add address=66.220.144.0/21 list=Facebook
add address=66.220.0.0/16 list=Facebook
add address=66.220.152.0/21 list=Facebook
```

```
add address=66.220.159.0/24 list=Facebook
add address=69.63.176.0/21 list=Facebook
add address=69.63.176.0/24 list=Facebook
add address=69.63.184.0/21 list=Facebook
add address=69.171.224.0/19 list=Facebook
add address=69.171.224.0/20 list=Facebook
add address=69.171.0.0/16 list=Facebook
add address=69.171.239.0/24 list=Facebook
add address=69.171.240.0/20 list=Facebook
add address=173.252.64.0/18 list=Facebook
add address=173.252.70.0/24 list=Facebook
add address=173.252.96.0/19 list=Facebook
add address=204.15.20.0/22 list=Facebook
add address=194.132.168.0/21 list=Spotify
add address=193.235.232.0/22 list=Spotify
add address=104.154.127.0/24 list=Spotify
/ip firewall filter
add action=drop chain=forward comment="Bloqueio Facebook" dst-address-
list=
    Facebook log=yes log-prefix="Block Face"
add action=drop chain=forward comment="Bloqueio Spotify" dst-address-list=
    Spotify log=yes log-prefix="Block Spotify"
add action=drop chain=forward comment="BLOQUEIO YOUTUBE" dst-
port=443 \
    protocol=tcp tls-host=*.youtube.com
add action=drop chain=forward comment="BLOQUEIO YOUTUBE" dst-
port=443 \
    protocol=tcp tls-host=*.youtube.com.br
add action=drop chain=input comment="Drop Invalid connections" \
    connection-state=invalid
add action=accept chain=input comment="Allow Established connections" \
    connection-state=established
add action=accept chain=input comment="Allow ICMP" protocol=icmp
add action=drop chain=input comment="Drop everything else"
```



```
add action=drop chain=forward comment="drop invalid connections" \  
    connection-state=invalid protocol=tcp  
add action=accept chain=forward comment=\  
    "allow already established connections" connection-state=established  
add action=accept chain=forward comment="allow related connections" \  
    connection-state=related  
add action=drop chain=forward src-address=0.0.0.0/8  
add action=drop chain=forward dst-address=0.0.0.0/8  
add action=drop chain=forward src-address=127.0.0.0/8  
add action=drop chain=forward dst-address=127.0.0.0/8  
add action=drop chain=forward src-address=224.0.0.0/3  
add action=drop chain=forward dst-address=224.0.0.0/3  
add action=jump chain=forward jump-target=tcp protocol=tcp  
add action=jump chain=forward jump-target=udp protocol=udp  
add action=jump chain=forward jump-target=icmp protocol=icmp  
add action=drop chain=tcp comment="deny TFTP" dst-port=69 protocol=tcp  
add action=drop chain=tcp comment="deny RPC portmapper" dst-port=111 \  
    protocol=tcp  
add action=drop chain=tcp comment="deny RPC portmapper" dst-port=135 \  
    protocol=tcp  
add action=drop chain=tcp comment="deny NBT" dst-port=137-139  
protocol=tcp  
add action=drop chain=tcp comment="deny cifs" dst-port=445 protocol=tcp  
add action=drop chain=tcp comment="deny NFS" dst-port=2049 protocol=tcp  
add action=drop chain=tcp comment="deny NetBus" dst-port=12345-12346 \  
    protocol=tcp  
add action=drop chain=tcp comment="deny NetBus" dst-port=20034  
protocol=tcp  
add action=drop chain=tcp comment="deny BackOrifice" dst-port=3133  
protocol=\  
    tcp  
add action=drop chain=tcp comment="deny DHCP" dst-port=67-68 protocol=tcp  
add action=drop chain=udp comment="deny TFTP" dst-port=69 protocol=udp  
add action=drop chain=udp comment="deny PRC portmapper" dst-port=111 \  
    protocol=udp
```

```
protocol=udp
add action=drop chain=udp comment="deny PRC portmapper" dst-port=135 \
    protocol=udp
add action=drop chain=udp comment="deny NBT" dst-port=137-139
protocol=udp
add action=drop chain=udp comment="deny NFS" dst-port=2049 protocol=udp
add action=drop chain=udp comment="deny BackOriffice" dst-port=3133
protocol=\
    udp
add action=accept chain=icmp comment="echo reply" icmp-options=0:0
protocol=\
    icmp
add action=accept chain=icmp comment="net unreachable" icmp-options=3:0 \
    protocol=icmp
add action=accept chain=icmp comment="host unreachable" icmp-options=3:1 \
    protocol=icmp
add action=accept chain=icmp comment=\
    "host unreachable fragmentation required" icmp-options=3:4 protocol=icmp
add action=accept chain=icmp comment="allow source quench" icmp-
options=4:0 \
    protocol=icmp
add action=accept chain=icmp comment="allow echo request" icmp-
options=8:0 \
    protocol=icmp
add action=accept chain=icmp comment="allow time exceed" icmp-
options=11:0 \
    protocol=icmp
add action=accept chain=icmp comment="allow parameter bad" icmp-
options=12:0 \
    protocol=icmp
add action=drop chain=icmp comment="deny all other types"
add action=drop chain=input comment="drop ftp brute forcers" dst-port=21 \
    protocol=tcp src-address-list=ftp_blacklist
add action=accept chain=output content="530 Login incorrect" dst-limit=\
```

```

1/1m,9,dst-address/1m protocol=tcp
add action=add-dst-to-address-list address-list=ftp_blacklist \
  address-list-timeout=3h chain=output content="530 Login incorrect" \
  protocol=tcp
add action=drop chain=input comment="drop ssh brute forcers" dst-port=22 \
  protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist \
  address-list-timeout=1w3d chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp
add action=drop chain=forward comment="drop ssh brute downstream" dst-
port=22 \
  protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list="port scanners" \
  address-list-timeout=2w chain=input comment="Port scanners to list " \
  protocol=tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="port scanners" \
  address-list-timeout=2w chain=input comment="NMAP FIN Stealth scan" \
  protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" \
  address-list-timeout=2w chain=input comment="SYN/FIN scan" protocol=tcp
\
  tcp-flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" \
  address-list-timeout=2w chain=input comment="SYN/RST scan" protocol=tcp
\

```

```

tcp-flags=syn,rst
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input comment="FIN/PSH/URG scan"
protocol=\
    tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input comment="ALL/ALL scan" protocol=tcp \
    tcp-flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input comment="NMAP NULL scan"
protocol=tcp \
    tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
add action=drop chain=input comment="dropping port scanners" \
    src-address-list="port scanners"
add action=tarptit chain=input connection-limit=3,32 protocol=tcp \
    src-address-list=blocked-addr
add action=jump chain=forward comment="SYN Flood protect" connection-
state=\
    new jump-target=SYN-Protect protocol=tcp tcp-flags=syn
add action=accept chain=SYN-Protect connection-state=new limit=400,5:packet
\
    protocol=tcp tcp-flags=syn
add action=drop chain=SYN-Protect connection-state=new protocol=tcp \
    tcp-flags=syn
add action=accept chain=SYN-Protect connection-state=new limit=400,5:packet
\
    protocol=tcp tcp-flags=syn
/ip firewall nat
add action=masquerade chain=srcnat comment="NAT " out-
interface=INTERNET
add action=dst-nat chain=dstnat comment="Acesso remoto TS" dst-port=3320 \
    protocol=tcp to-addresses=10.1.1.11 to-ports=3389
add action=dst-nat chain=dstnat comment="Acesso remoto WINBOX" dst-
port=8290 \

```

```
protocol=tcp to-addresses=10.1.1.1 to-ports=8290
add action=dst-nat chain=dstnat comment=SIGEP dst-port=1433 protocol=tcp \
to-addresses=10.1.1.11 to-ports=1433
/ip route
add comment="===== ROTA PSF-1 =====" distance=1 dst-address=\
192.168.200.10/32 gateway=192.168.10.2
add comment="===== ROTA PSF-2 =====" distance=1 dst-address=\
192.168.201.10/32 gateway=192.168.11.2
add comment="===== ROTA ESCOLA =====" distance=1 dst-
address=\
192.168.202.10/32 gateway=192.168.12.2
add comment="===== ROTA GARAGEM =====" distance=1 dst-
address=\
192.168.203.10/32 gateway=192.168.13.2
add comment="===== ROTA FUNASA =====" distance=1 dst-
address=\
192.168.204.10/32 gateway=192.168.14.2
add comment="===== ROTA CRAS =====" distance=1 dst-address=\
192.168.205.10/32 gateway=192.168.15.2
add comment="===== ROTA COLETORIA =====" distance=1 dst-
address=\
192.168.206.10/32 gateway=192.168.16.2
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www port=9090
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/ppp secret
add comment="RB PSF-1" local-address=192.168.10.1 name=PSF-1
password=PSF-1 \
profile=default-encryption remote-address=192.168.10.2 service=pptp
```

```
add comment="RB PSF-2" local-address=192.168.11.1 name=PSF-2
password=PSF-2 \
    profile=default-encryption remote-address=192.168.11.2 service=pptp
add comment="RB ESCOLA" local-address=192.168.12.1 name=ESCOLA
password=\
    ESCOLA profile=default-encryption remote-address=192.168.12.2 service=\
    pptp
add comment="RB GARAGEM" local-address=192.168.13.1 name=GARAGEM
password=\
    GARAGEM profile=default-encryption remote-address=192.168.13.2
service=\
    pptp
add comment="RB COLETERIA" local-address=192.168.16.1
name=COLETORIA \
    password=COLETORIA profile=default-encryption remote-
address=192.168.16.2 \
    service=pptp
add comment="RB CRAS" local-address=192.168.15.1 name=CRAS
password=CRAS \
    profile=default-encryption remote-address=192.168.15.2 service=pptp
add comment="RB FUNASA" local-address=192.168.14.1 name=FUNASA
password=\
    FUNASA profile=default-encryption remote-address=192.168.14.2 service=\
    pptp
add comment="RB PSF-1" local-address=192.168.100.1 name=123
password=123 \
    profile=default-encryption remote-address=192.168.100.2 service=pptp
/system clock
set time-zone-name=America/Sao_Paulo
/system package update
set channel=release-candidate
/system routerboard settings
set silent-boot=no
/tool graphing interface
```

```
add interface=ether1_INTERNET
```

```
/tool romon
```

```
set enabled=yes
```