CENTRO UNIVERSITÁRIO DO CERRADO PATROCÍNIO
UNICERP
Graduação em Sistemas de Informação

HIGOR VINICIUS DE OLIVEIRA FERREIRA

O USO DA FERRAMENTA MIKROTIK EM UMA REDE COMO FERRAMENTA DE GERÊNCIA E SEGURANÇA

PATROCÍNIO/MG
2019

HIGOR VINICIUS DE OLIVEIRA FERREIRA

O USO DA FERRAMENTA MIKROTIK EM UMA REDE COMO FERRAMENTA DE GERÊNCIA E SEGURANÇA

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do grau de bacharel em Sistemas de Informação, pelo Centro Universitário do Cerrado Patrocínio – UNICERP.

Orientador: Prof. Esp. José Côrtes de Castro Neto

Patrocínio/MG
2019

Centro Universitário do Cerrado Patrocínio
Curso de Graduação em Sistemas de Informação

Trabalho de Conclusão de curso intitulado **"O uso da ferramenta Mikrotik em uma rede como ferramenta de gerência e segurança"**, de autoria do graduando Higor Vinicius de Oliveira Ferreira, aprovado pela banca examinadora constituída pelos seguintes professores:

BANCA EXAMINADORA

Prof. Esp. José Côrtes de Castro Neto
Instituição: UNICERP

Célio Rafael Martins Júnior

Avaliador 1 – Esp. Célio Rafael Martins Júnior
Instituição: UNICERP

Sérgio Augusto Amaral Lopes

Avaliador 2 – Me. Sérgio Augusto Amaral Lopes
Instituição: UNICERP

Data de aprovação: 04/07/2019

Patrocínio, 04, julho de 2019.

AGRADECIMENTOS

A Deus pelo dom da vida e me acompanhar em todos os momentos;

Aos meus pais, que não mediram esforços para me ajudar em todas as etapas da minha vida;

Aos meus amigos e futuros companheiros de profissão que fiz ao longo do curso;

Ao meu orientador Professor José Côrtes de Castro Neto que com sua sabedoria não mediu esforços para me auxiliara concluir este trabalho;

A todos os professores que com sabedoria, paciência e dedicação transmitiram seu conhecimento e me ajudaram em minha formação profissional;

À instituição UNICERP;

A todos que contribuíram diretamente ou indiretamente para que esse trabalho pudesse ser concluído.

RESUMO

Introdução: A popularização da internet e as crescentes trocas de informações, compartilhamentos de recursos, houve a necessidade de dispositivos estabelecerem comunicação entre si para realizar tais informações com isso surgem às necessidades de proteção do sistema de redes. Os *firewalls* e hardwares como o Mikrotik vieram para auxiliar na proteção do sistema. **Objetivo:** Apresentar sobre a tecnologia Mikrotik, suas características, recursos, vantagens e desvantagens aplicadas ao desempenho de uma rede de computadores. **Material e métodos:** Foi realizada pesquisas bibliográficas em livros, artigos e sites, com vários autores distintos considerados confiáveis tecnicamente. **Resultados:** Se fez relevante o trabalho onde mostrou os resultados, através de estudos e artigos, da melhoria na segurança do sistema por meio da ferramenta da Mikrotik. **Conclusão:** Conclui se que com a avaliação do hardware Mikrotik RouterOS pode trazer benefícios como maior segurança, monitoramento e desempenho em redes de computadores quando comparada a uma rede convencional que não faz uso da mesma tecnologia.

Palavras-Chave: Automatização, Hardware, Monitoramento, Ataques.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

API - *Application Programming Interface*

BGP – *Border Gtway Protocol*

DoS - *Denial of Service*

IDS - *Intrusion Detection System*

IP – *Internet Protocol*

IPS - *Intrusion Prevention System*

NAT - *Network Translation Address*

NIC BR – Núcleo de Informação e Coordenação do Ponto BR

OSPF – *Open Shortest Path First*

PC – *Personal Computer*

PHP - *Hypertext Preprocessor*

SDN – *Softwares Defined Networking*

TCP/IP - *Transmission Control Protocol / Internet Protocol*

TIC – Tecnologia da Informação e Comunicação

VRRP – *Virtual Router Redundancy Protocol*

WAP – *Wireless Application Protocol*

WDS – *Wireless Distribution System*

WEP – *Wired Equivalent Privacy*

SUMÁRIO

1. INTRODUÇÃO

A popularização da internet e as crescentes trocas de informações, compartilhamentos de recursos, surgimento de novas tecnologias permitiu um grande avanço dos dispositivos que se comunicam entre si e realizam troca de informações por meio da rede (SOUZA; LUCA, 2014).

A utilização do acesso à internet da forma proposta tem sua usabilidade própria a qual sua finalidade foi projetada, alguns sistemas existentes e pessoas utilizam os recursos da rede de forma negativa. Em casos que sua utilização é feita de forma prejudicial ou ilegal, pode-se causar falhas ou danos em recursos por meio da internet, que em alguns casos são vazamento de informações (SURYANARAYANAN, 2014).

Os IDS (*Intrusion Detection System*, do português Sistema de Detecção de Intrusos) surgiram com a finalidade de monitoramento, identificação, registros e de informação aos administradores destes sistemas e/ou redes de computadores quando anormalidades por menor que sejam ocorram no sistema (NJOGU et al., 2013).

Comparando os dados coletados com as coleções de regras que consistem em identificar os ataques, estes IDS operam fazendo a leitura e diagnóstico das informações nos pacotes transmitidos pela rede e comparam com tais dados (HOQUE et al., 2014).

A responsabilidade de reparar os prejuízos e ou danos ocasionados por um ataque é do administrador da rede/sistema, fazendo a realização da leitura e identificação de prováveis e ou concretizados ataques em uma rede/sistema. Os sistemas de detecção podem auxiliar gestores de rede em sua tarefa diária, não impedindo ou bloqueando um ataque, mas apoiando por meio de relatórios no controle das falhas e problemas (NJOGU et al., 2013).

De outra forma, os responsáveis no controle de garantia de acesso à rede ou dispositivo, prevenindo ou reduzindo o acesso de dispositivos, conforme protocolos de controle e políticas de segurança instituídas pelo administrador da rede/sistema são os sistemas de *firewall* (JUNQI; ZHENGBING, 2008).

A Mikrotik foi fundada em 1996 para desenvolvimento de roteadores e sistemas ISP sem fio, seu país de origem é a Letônia no continente Europeu. Mikrotik agora fornece *hardware* e *software* para conectividade com a Internet na maioria dos países ao redor do mundo. Sua experiência em usar *hardware* de PC padrão da indústria e sistemas de roteamento completos que permitiu, em 1997, criar o sistema de software RouterOS que fornece estabilidade extensiva, controles e flexibilidade para todos os tipos de interfaces de dados e roteamento (MIKROTIK, 2015).

2. OBJETIVOS

2.1. Geral:

Analisar e apresentar sob a perspectiva teórica recursos, técnicas e métricas da tecnologia Mikrotik para melhorar a gestão de segurança em redes de informação, este trabalho terá como base o estudo do hardware e do software da empresa.

2.2. Específicos:

- Apresentar uma revisão bibliográfica dos recursos de redes de computadores, internet e segurança da informação, além de conceitos gerais.
- Apresentar uma análise de recursos e características da tecnologia Mikrotik, hardware e software.
- Conceituar e verificar as vantagens e desvantagens do uso da tecnologia Mikrotik.

3. DESENVOLVIMENTO

O USO DA TECNOLOGIA MIKROTIK EM UMA REDE COMO FERRAMENTA DE GERÊNCIA E SEGURANÇA

HIGOR VINICIUS DE OLIVEIRA FERREIRA[1]
ESP. JOSÉ CÔRTES DE CASTRO NETO[2]

RESUMO

Introdução: A popularização da internet e as crescentes trocas de informações, compartilhamentos de recursos, houve a necessidade de dispositivos estabelecerem comunicação entre si para realizar tais informações com isso surgem às necessidades de proteção do sistema de redes. Os *firewalls* e hardwares como o Mikrotik vieram para auxiliar na proteção do sistema. **Objetivo:** Apresentar sobre a tecnologia Mikrotik, suas características, recursos, vantagens e desvantagens aplicadas ao desempenho de uma rede de computadores. **Material e métodos:** Foi realizada pesquisas bibliográficas em livros, artigos e sites, com vários autores distintos considerados confiáveis tecnicamente. **Resultados:** Se fez relevante o trabalho onde mostrou os resultados, através de estudos e artigos, da melhoria na segurança do sistema por meio da ferramenta da Mikrotik. **Conclusão:** Conclui se que com a avaliação do hardware Mikrotik RouterOS pode trazer benefícios como maior segurança, monitoramento e desempenho em redes de computadores quando comparada a uma rede convencional que não faz uso da mesma tecnologia.

Palavras-Chave: Automatização, Hardware, Monitoramento, Ataques.

ABSTRACT

Introduction: The popularization of the Internet and the increasing exchanges of information, sharing of resources, there was a need for devices to establish communication with each other to carry out such information with this arise to the protection needs of the network system. Firewalls and hardware like Mikrotik have come to help protect the system. **Objective:** To present Mikrotik technology, its characteristics, features, advantages and disadvantages applied to the performance of a computer network. **Material and methods**: Bibliographical research was carried out in books, articles and websites, with several different authors considered technically reliable. **Results:** It was relevant the work where he showed the results, through studies and articles, of the improvement in the security of the system through the Mikrotik tool. **Conclusion:** It is concluded that Mikrotik RouterOS hardware evaluation can bring benefits such as greater security, monitoring and performance in computer networks when compared to a conventional network that does not use the same technology.

[1] Autor, Graduando em Sistemas de Informação pelo UNICERP.
[2] Professor orientador. Especialista e docente do Curso de Sistemas de Informação e outros cursos UNICERP.

Keywords: Automation, Hardware, Monitoring, Attacks.

3.1 INTRODUÇÃO

A utilização da internet é um item que pode andar em companhia da segurança e proteção dos dados. Com um controle que pode ser realizado por meio de softwares e hardwares de redes de computadores a administração destes equipamentos na rede tradicional pode ser feita de maneira individual, onde dificulta-se o trabalho do administrador da rede. Este fato também pode complicar uma análise para a obtenção de resoluções dos problemas ou mesmo ajustes de melhorias na configuração de uma política de segurança (BITENCOURT, 2014).

A Mikrotik em seu dia a dia além de oferecer todo os equipamentos de segurança em rede trabalha com sessões de treinamentos fornecidas pelos Centros de Treinamento da Mikrotik em vários locais ao redor do mundo. Engenheiros de rede, integradores e gerentes são atendidos para melhor entendimento sobre roteamento e gerenciamento de redes com e sem fio usando o Mikrotik RouterOS (MIKROTIK, 2015).

Ainda segundo Mikrotik (2015) a empresa possui cursos de graduação onde os certificados são reconhecidos em todo o mundo e representam um bom conhecimento sobre administração de rede, usando RouterBOARD e RouterOS (MIKROTIK, 2015).

As redes SDN (*Softwares Defined Networking*) apresentam uma escolha para o gerenciamento logicamente centralizado permitindo um melhor uso dos administradores de rede por meio de maior flexibilidade. O conceito de redes SDN é ajustar um novo modelo para administração das redes de computadores, permitindo com isso o controle de toda a rede e uma administração centralizada em um único equipamento (KIM, 2013).

Contudo, ao mesmo instante que a SDN apresenta-se promissora, esta nova tecnologia têm alguns desafios de segurança a serem vencidos. As vantagens da centralização do plano de controle, como lógica centralizada e visão global da rede é fato importante (NADEAU, 2013).

Para melhor auxiliar na segurança, são desenvolvidos alguns sistemas, o Snort é uma ferramenta IDS de código-fonte aberto, seu desenvolvedor foi Martin Roesch, seu diferencial é a flexibilidade nas configurações de regras e as constantes atualizações, que é fator importante em redes, frente às técnicas de invasão cada dia mais inovadoras (SNORT, 2016).

O presente trabalho tem como objetivo apresentar a tecnologia Mikrotik RouterOS como ferramenta de segurança e desempenho de uma rede de computadores. O trabalho

apresenta uma revisão bibliográfica da literatura, constituída de uma base teórica para aplicação da pesquisa, envolvendo assim conceitos de redes de computadores, segurança e também itens relacionado a tecnologia em questão.

3.2. MATERIAL E MÉTODOS

Este trabalho foi desenvolvido com base em pesquisas bibliográficas, artigos acadêmicos e no estudo da tecnologia Mikrotik. Em um primeiro momento, foram analisados os itens iniciar acerca da internet e a segurança da informação, também foi apresentado um estudo sobre sistemas de proteção como *firewall*. Na sequência, foram abordados os recursos, características, vantagens e desvantagens da tecnologia Mikrotik.

3.3. RESULTADOS E DISCUSSÃO

3.3.1. Conceituando o ambiente virtual

Sendo considerado um item de grande importância, a internet tem se destacado na vida pessoal, por meio da interação e comunicação nas redes sociais; fomentando novos negócios e empreendimentos, alterando até mesmo o modo de pensar e agir diante de diversas situações. Percebe-se que este fenômeno "vem alterando ou modificando a qualificação profissional, os relacionamentos, o meio acadêmico, o crescimento pessoal, enfim todas as relações humanas [...]" (CARVALHO & OLIVEIRA, 2017, p. 2).

Em uma sociedade da informação, a comunicação não é somente por meio das redes sociais, haja vista que as tecnologias e o sistema de informação conseguem chegar bem mais longe e um leque de possibilidades e oportunidades surgem, a exemplo das TIC's – Tecnologia da Informação e Comunicação, do processo eletrônico e das cidades envolvidas com a tecnologia, ferramentas estas que oportuniza a inclusão e com isso medidas de segurança são necessárias. A sociedade da informação, conforme a Almeida Filho (2015, p.50), rompe barreiras e "espaços geofísicos criados pela eletrônica" (ALMEIDA FILHO, 2015, p.50).

Em todo ambiente de rede a segurança da informação trata da proteção dos sistemas de informação e do acesso, fazendo com que tudo que é gerado na mesma seja preservado a confidencialidade, integridade / autenticidade e disponibilidade de informações geradas. O objetivo dos sistemas de hardwares de segurança é mitigar riscos e proteger a todas as informações das ameaças que têm impactos negativos e prejuízo no retorno sobre investimentos e oportunidades de negócios feitos nas redes (SOUZA et al, 2016, p. 241).

3.3.2. Segurança da informação e redes

Segundo Rios e Teixeira Filho (2018) apud Quintella e Branco (2013, p. 51), dizem a respeito da segurança da informação: “proteção da informação contra ameaças que possam valer-se das vulnerabilidades dos ativos, preservando suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade”. Sendo norteadores da segurança da informação, seus princípios básicos são de extrema relevância para “guerrear”, combater as ameaças às informações, que por meio das vulnerabilidades possam existir.

O CERT.BR é um grupo de resposta a incidentes de segurança para a internet brasileira, mantido pelo NIC.BR – Núcleo de Informação e Coordenação do Ponto BR, do Comitê Gestor da Internet no Brasil. Este grupo é o responsável por tratar os incidentes de segurança pertinentes em computadores que envolvam redes conectadas a internet brasileira (CERBT.BR, 2017).

Por meio de estatísticas dos incidentes ocorridos com segurança nas redes o CERT.BR divulga os resultados conforme **Figura 1**, onde a maior parte de incidentes apresentados na imagem é do tipo Scan, seguido de DoS (CERBT.BR, 2017).

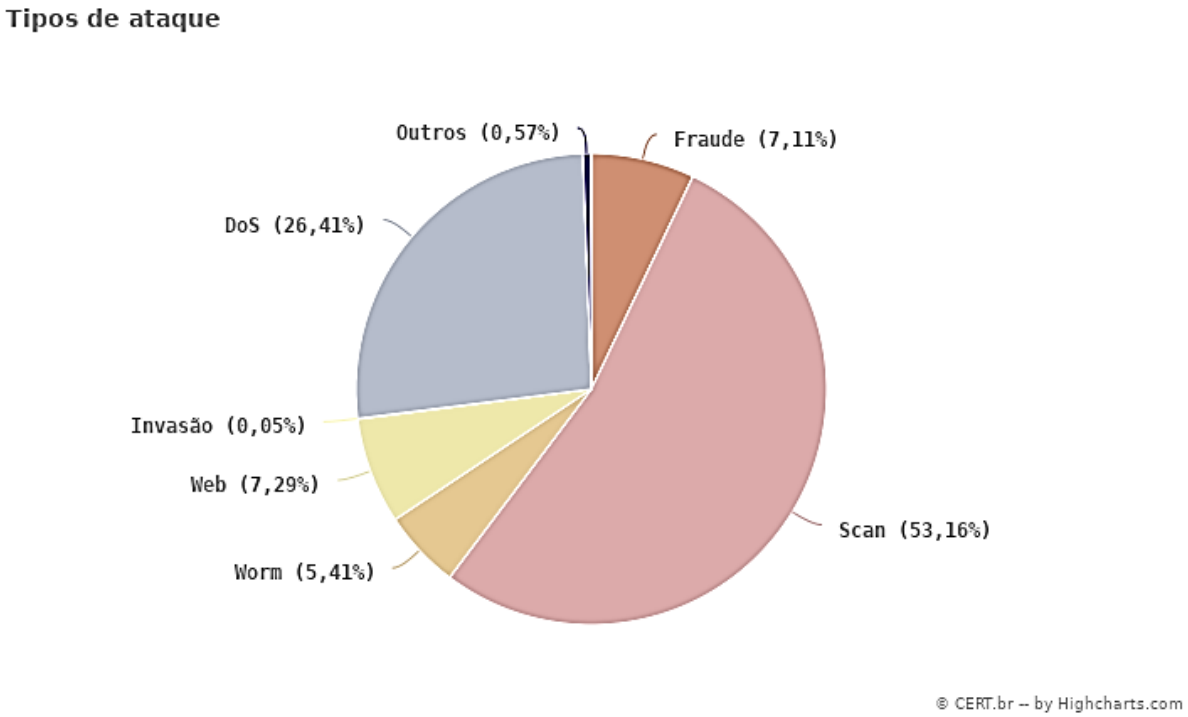

Figura 1: Incidentes segundo CERT.br - 2017
Fonte: CERT (2017).

Como apresentado na **Figura 1**, segundo o CERT.BR (2017) incidentes do tipo Scan caracterizam-se por notificações de varreduras com o objetivo de identificar quais aparelhos de computador estão ativos e quais serviços estão sendo disponibilizados por eles nesta rede. Utilizado por pessoas que ataca a rede, este sistema é feito para verificar possíveis alvos, onde permite a associação de vulnerabilidades dos serviços habilitados no computador.

A **Figura 1**, também apresenta índice de invasão de 0,05% que configura os atos ardilosos e de má-fé, com a finalidade de lesar ou enganar. Essa categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem, sendo as fraldes de 7,11% que é um ataque bem-sucedido onde resulta no acesso não autorizado a um computador ou rede.

3.3.3. Detecção e proteção de dados

As definições e objetivos conforme a concepção de Kurose e Ross (2013) de um *firewall*, em três conceitos, sendo o primeiro passando pelo mesmo é o tráfego que vem de fora da rede e, o tráfego que sai de dentro da rede; o segundo somente o conteúdo que foi antecipadamente definido pela política de segurança da organização poderá passar pelo

firewall; e o terceiro e último, por ser uma ferramenta conectada à rede, sua instalação dever ser de maneira correta, a fim de ser imune às invasões.

O IDS (*Intrusion Detection System*) é um sistema de proteção com finalidade de identificação, baseadas em assinaturas de tráfego ou detecção de anomalias. Em rede ele detecta, examina e confere todo o tráfego buscando os pacotes com assinaturas conhecidas, em host ele se baseia em dados presentes no cabeçalho dos pacotes de dados históricos e consequente detecta alguma anormalidade (FERREIRA e CARLOS W, 2015).

O IPS (*Intrusion Prevention System*) é considerado e visto como um complemento do IDS (Intrusion Detection System) pode ser *Host-Based* e ou *InLine*, ele tem e possui a capacidade de rastrear e bloquear intrusos nas redes. A partir da detecção, um IPS executará ações para interromper o ataque e evitar ataques futuros. As ações desse software podem ser desde a invalidação de uma conexão até uma reconfiguração do *firewall* para interromper o ataque em utilização (FERREIRA e CARLOS W, 2015).

O autor Carvalho et al (2018) apresenta que os protocolos e algoritmos de criptografia (registros embaralhados por meio de uma tecnologia) são a encriptação simétrica que é conhecida como criptografia de Chave Secreta, é utilizada pela sua rapidez, a encriptação assimétrica que é conhecida como criptografia de chave pública. Pode ser mais lenta e necessita de uma maior capacidade computacional por parte das máquinas, mais é o melhor método para garantir segurança num canal público, a de algoritmo de decriptação que é fundamentalmente o processo de mudança de texto para cifra, dificultando sua leitura a quem não tem acesso, exceto aqueles que possuem a chave.

3.3.4. Entendendo e conhecendo o hardware do Mikrotik

O hardware do Mikrotik RouterOS possui variados filtros de conteúdo fundamentado em listas de IP, podendo ser estático ou dinâmico. Pode-se ainda aplicar filtros em portas nos escopos de portas e ou específicos. Utilizado estes recursos com grande granularidade de proteção a rede controlando assim o acesso por meio do emprego de diversos parâmetros (MIKROTIK, 2015).

Comparado às outras soluções de *firewall*, como por exemplo, o sistema IPTABLES e IPFW, o sistema Mikrotik se mostra como uma solução eficaz por se tratar de uma proposta de hardware e software desenvolvidos buscando aproveitar ao máximo o potencial um do outro. No caso da solução da Mikrotik, tanto o software quanto o hardware são

especificamente desenvolvidos para um propósito específico e suas disposições são direcionadas para tais tarefas (MIKROTIK, 2015).

3.3.5. Configuração e aplicabilidade

O sistema Mikrotik dispõe de diversos recursos, como roteamento de redes de computadores, controle e filtro de tráfego e conteúdo e sistema de proteção para estas redes. Além de recursos para controle e gestão de redes, o sistema operacional embarcado no hardware desenvolvido pela Mikrotik é denominado *RouterBOARD* (MIKROTIK, 2015).

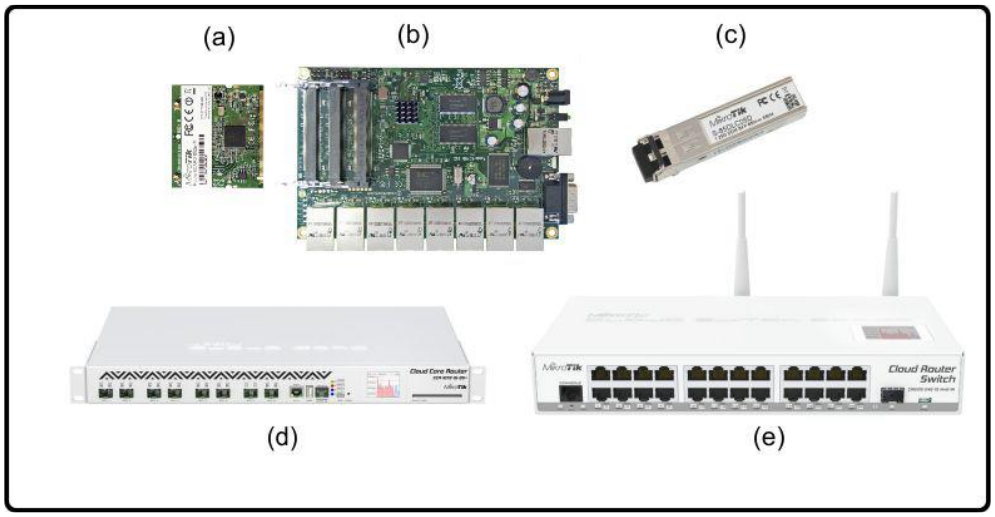

Figura 2: Dispositivos desenvolvidos pela Mikrotik
Fonte: Mikrotik, 2015.

Na **Figura 2** observa-se (a) um cartão de expansão de conexão sem fio de tecnologia 802.11 a/n ou 802.11 b/g/n conjuntamente utilizado com a (b) Routerboard RB 493, composta por *slots* de expansão para cartões sem fio e também, *8 interfaces ethernet Gigabit* e outras (MIKROTIK, 2015).

Ainda na **Figura 2** (c) exibe um adaptador para conexões ópticas, podendo ser empregada nos dispositivos (d) e (e). Já a imagem (d) apresenta uma RouterBOARD de alta performance suportando 72 unidades de processamento e 8 portas ópticas de 10 Gigabits. Por fim, na imagem (e) é notório o exemplo composto por conexões de rede se fio, redes *ethernet Gigabit* e conexões de fibra óptica num mesmo dispositivo, todos estes gerenciados pelo

mesmo sistema RouterOS, confirmando a flexibilidade e fortaleza deste sistema (MIKROTIK, 2015).

O Mikrotik RouterOS é um sistema operacional "*carrier class*" que vem ocupando seu espaço de uma forma expressiva no mercado de Tecnologia da Informação por suas inúmeras funcionalidades, força, estabilidade e principalmente por possuir um sistema simplificado. Fundamentado em Linux, o sistema pode ser instalado em um computador convencional ou embarcado em placas compactas SBC (Single Board Computer), como por exemplo, as RouterBoards fabricadas pelos próprios desenvolvedores do Mikrotik RouterOS (MD BRASIL, 2019).

A grande característica que diferencia o Mikrotik de outros sistemas concorrentes é a absoluta facilidade que a interface de configuração proporciona ao usuário/administrador de rede. Tais recursos são úteis tanto para profissionais que já possuem sólidos conceitos de redes de computadores como para iniciantes. Os primeiros encontram no Mikrotik recursos para aumentar significativamente sua produtividade e conseguem com esforços reduzidos utilizar o máximo que o sistema oferece (MD BRASIL, 2019).

Ainda segundo MD Brasil (2019), profissionais iniciantes encontram no Mikrotik a ferramenta ideal para seu crescimento, pois a simplicidade da manipulação das configurações permite uma maior concentração nos conceitos envolvidos sem as preocupações com detalhes de implementação como sintaxe de regras, por exemplo, proporcionando assim uma curva de aprendizado bastante acentuada (MD BRASIL, 2019).

Para melhor administração do sistema e sua configuração, o Mikrotik RouterOS possui uma ferramenta desenvolvida por ela na realização da configuração do sistema, conhecido como Winbox. Por meio do acesso via Winbox, o sistema permite o acesso via *Telnet* e *Secure Shell* – SSH, onde disponibiliza um console para efetivação dos comandos em modo linha. A **Figura 3** apresenta a tela de configuração do sistema utilizando a ferramenta Winbox (MIKROTIK, 2015).

Devido ao conhecimento deste autor o mesmo define a ferramenta Mikrotik como algo de grande usabilidade e que tem grande potencial presente ao mercado da atualidade. Relacionado a segurança o item estudado apresenta uma forte capacidade de atender as demandas dos usuários.

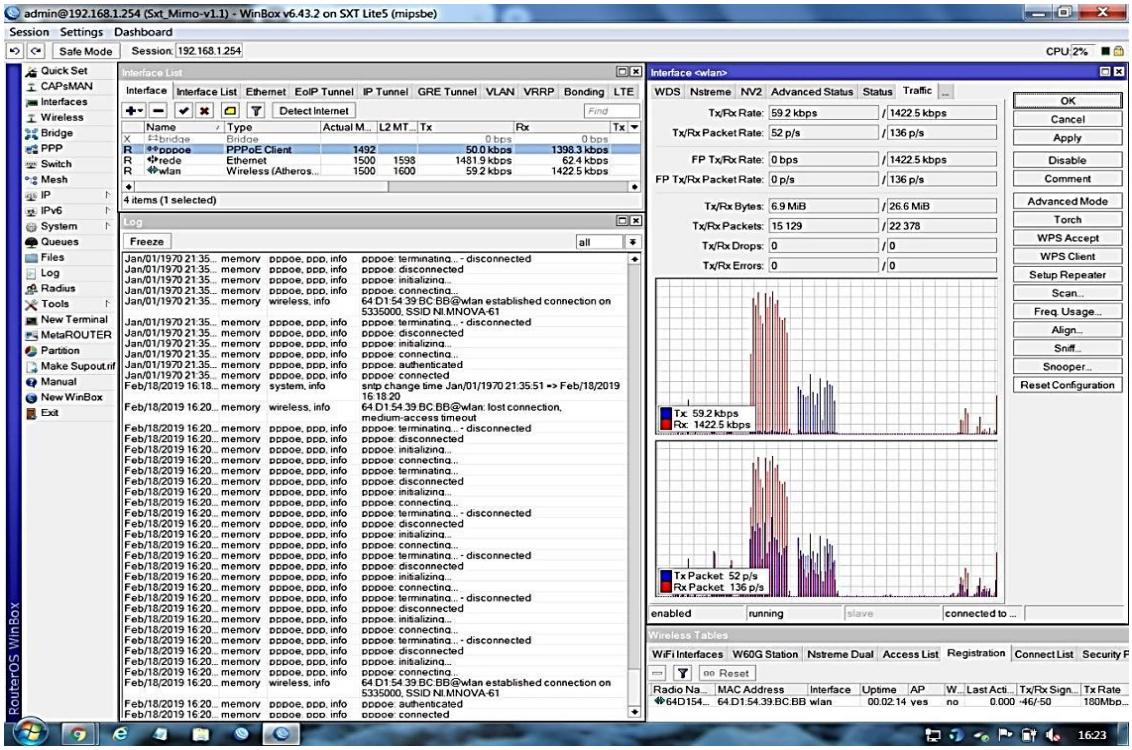

Figura 3: Ferramenta de configuração Winbox da Mikrotik.
Fonte: Do autor.

Na **Figura 3** pode-se observar um gráfico (a direita) de acompanhamento da interface (selecionável), bem como uma apresentação de todas as interfaces do tipo internet existentes para uso no hardware no caso uma RouterBoard 1100 AHX2). O Winbox permite ver em tempo real informações sobre utilização do processador, memória de acesso randômico disponível, tempo que o equipamento está ligado e data/hora do sistema. À esquerda é apresentado o menu com as opções de configuração e funcionalidades do sistema.

Recursos feitos pela Mikrotik podem ser aplicados em diversos cenários. Pode-se tanto utilizar soluções Mikrotik para redes domésticas quanto, por exemplo, para soluções para monitoramento e controle de provedores de acesso à internet. Além disso, estas soluções podem desempenhar a grande maioria das funcionalidades de soluções que apresentam um custo mais elevado, como por exemplo, soluções da líder de mercado Cisco e seu maior concorrente, a Juniper (MIKROTIK, 2015).

Segundo informações do site Mikrotik (2015) é importante destacar que sistemas como o IPTABLES – que é um conjunto de ferramentas e medidas que permite o controle e a definição dos protocolos de *firewalls* e NATs, admitindo que o servidor tenha maior e melhor filtragem de pacotes, tolerando passar apenas os seguros. Além disso, sua instalação é realizada, por padrão, sobre um hardware também de propósito geral, diferentemente da solução da Mikrotik.

Traçando um comparativo entre a solução Mikrotik e outras soluções de proteção e controle, é de relevância lembrar que este sistema, distinto das demais aplicações apresentadas que abordam apenas o desempenho do sistema *firewall*, é uma solução especialista, completa e aplicada as mais diversas finalidades de gestão de redes. (MIKROTIK, 2015).

3.3.6. Resultados e análise do Mikrotik

Os benefícios e vantagens em ter o Mikrotik é a infraestrutura de tecnologia, sendo que em priori seus protocolos condiciona o melhoramento e aprimoramento dos sinais transmitidos, permite melhorar e aprimorar os sinais transmitidos, pois se fala aqui de otimização da segurança na rede com seu *firewall* (SILVA, 2019).

Segundo a MD Brasil (2019) algumas funcionalidades e aspectos vantajosos do Mikrotik Router-OS:

- Desempenho otimizado com o protocolo;
- Alta disponibilidade com o protocolo VRRP;
- Possibilidade de agregar interfaces (*bonding*);
- Poucas exigências de recursos de *hardware*;
- Qualidade de serviço avançado;
- *Firewall* "*stateful*";
- 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 e console;
- Configuração e monitoramento em tempo real.

Segundo Silva (2019) a desvantagem é que possui e exige certa complexidade na hora da implantação deste produto, pois depende muito do profissional estar ou não habituado e qualificado para a instalação do mesmo. Para não ter nenhuma contra tempo e poder desfrutar

de toda sua excelência e segurança, é preciso elaborar, planejar e montar uma rede Mikrotik de maneira correta, somando assim o máximo da solução juntamente com o fim de problemas de instabilidade no sistema.

Compreendendo e estudando melhor o tema de segurança em rede, pode-se observar que o espaço entre as ferramentas de segurança é possível converter as detecções realizadas pelo IDS SNORT em princípios de proteção e segurança junto ao sistema de *firewall* do Mikrotik RouterOS, expandindo sua competência de execução em relação aos ataques em uma rede de dispositivos por meio de das duas ferramentas e de forma automatizada (SILVA, 2019).

Com base nas informações apresentadas foi possível abordar de forma teórica e parcialmente técnica quanto ao tema Mikrotik. Dentre os diversos itens abordados o estudo abordou sobre hardware, software e conceitos correlacionados

3.4. CONSIDERAÇÕES FINAIS

O trabalho realizado permitiu contextuar formas de segurança contra ataques indesejados nas redes. Conclui-se que o objetivo do trabalho foi alcançado, onde a avaliação do hardware Mikrotik RouterOS pode trazer benefícios como maior segurança e desempenho em redes de computadores quando comparada a uma rede comum que não faz uso da mesma.

É preciso colocar e instalar *softwares* e *hardwares* de segurança nas redes, mas também investir na contratação de bons profissionais da segurança de informação que compreendam e conheçam a melhor forma de usar essa ferramenta para que possa bloquear e dificultar as investidas dos atacantes mantendo assim as informações das empresas em constante proteção e segurança.

A Mikrotik combina o RouterOS com uma linha de hardware próprio. Suas principais características é que foi projetado para provedores de pequeno e médio porte, oferecendo acesso banda largos via rede sem fios. Conta ainda com equipamentos de rádio ou roteadores compactos, que tem a capacidade de montar links wireless com alta capacidade de tráfego, inclusive utilizando duas antenas e uma configuração especial. Além disso, conta com inúmeras ferramentas de análise e monitoramento, inclusive a execução de scripts.

Assim, pode-se concluir ainda que uma boa política de segurança em redes deve ser item obrigatório e frequente para garantir uma proteção aceitável e correta, pois os danos e prejuízos causados por falta de monitoramento e ou um monitoramento lento podem resultar

em falhas e comprometer todo um sistema, papel que a ferramenta Mikrotik possui para tal trabalho.

3.5. REFERÊNCIAS

ALMEIDA FILHO, José Carlos de. **Processo eletrônico e teoria geral do processo eletrônico. A informatização judicial no Brasil**. 5. ed. revista e atualizada. Rio de Janeiro: Forense, 2015.

BITENCOURT, William Lopes**. Implementação de politicas globais em redes SDN utilizando marcação de pacotes.** Unisinos, São Leopoldo, 2014.

BHUYAN, M.; BHATTACHARYYA, D.; KALITA, J. **Network Anomaly Detection: methods, systems and tools.** Communications Surveys Tutorials, IEEE, v.16, n.1, 2014. p.303–336.

CARVALHO, Rubens dos Santos et al. **Usando criptografia em digitalização em redes**. 1. ed. Belém/PA: Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, 2018. cap. 1, p. 31-32. v. 1.

CARVALHO, P. B. S.; OLIVEIRA, J. P. Q. (2017). **E-commerce: perfil de estudantes universitários como consumidores virtuais**. Ano XIII, n. 02. Fevereiro/2017. Temática. - http://www.periodicos.ufpb.br/ojs2/index.php/tematica/article/view/33010/17145.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Org.). **Estatísticas dos Incidentes Reportados ao CERT.BR**. São Paulo: Comitê Gestor da Internet no Brasil, 2017. Disponível em: < https://www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html >. Acesso em 19 fev. 2019.

COMER, Douglas. **Internetworking with TCP/IP: principles, protocols, and architecture.** Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1988.

JUNQI, W.; ZHENGBING, H. **study of intrusion detection systems (idss) in network security. in: wireless communications, networking and mobile computing**, 2008. WICOM ’08. 4TH INTERNATIONAL CONFERENCE ON, 2008. p.1–4.

FERREIRA, CARLOS W. 2015, **Segurança de redes com IPS, sua relação com IDS e sua Importância no trabalho conjunto com o Firewall**. Disponível em: < https://goo.gl/GTi9CX>. Acesso em 20 Fev. 2019.

KIM, H; FEAMSTER, N**. Improving Network Management with Software Defined Networking.** Communications Magazine, IEEE, 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down.** Tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MD Brasil: Mikrotik RouterOS. **Mikrotik RouterOS**. 2019. Disponível em: <http://mdbrasil.com.br/solucoesemhardware/mikrotik-routeros/>. Acesso em: 02 maio 2019.

MIKROTIK. Mikrotik 2015. Disponível em: <http://www.mikrotik.com/>. Acesso em: 11 fev. 2019.

NADEAU, T. D; GRAY, K. SDN: Software **Defined Networks. ”O‟Reilly Media, Inc.”,** 2013.

NJOGU, H. W.; JIAWEI, L.; KIERE, J. N.; HANYURWIMFURA, D. A **Comprehensive Vulnerability Based Alert Management Approach for Large Networks.** Future Gener. Comput. Syst., Amsterdam, The Netherlands, The Netherlands, Janeiro de 2013. v.29, n.1, p.27–45.

RIOS, Orlivaldo Kleber Lima; RIOS, Vânia Patrícia da Silva; TEIXEIRA, FILHO, José Gilson de Almeida . **Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação.** Revista de Gestão e Tecnologia. Pernambuco, v. 7, n.2, p. 49-65, 14 nov. 2018. Disponível em: http://navus.sc.senac.br/index.php/navus/article/view/482/pdf Acesso em 19 fev. 2019.

SILVA, L. **O que é Mikrotik?**. [*S. l.*], 15 mar. 2019. Disponível em: https://www.4infra.com.br/o-que-e-mikrotik/. Acesso em: 15 mar. 2019.

SNORT, 2016. **The Snort Project. Disponível em**: <http://www.snort.org/>. Acesso em: 19 fev. 2019.

SOUZA, L. D. F.; LUCA, G. G. de. **Lei 12.965 de 2014: democratização da internet e efeitos do marco civil na sociedade da informação**. In: REVISTA PARADIGMA, 2014. p.76–96.

SOUZA, Jackson Gomes Soares et al. **Gestão de riscos da segurança da informação em uma instituição pública federal: um estudo de caso**. ENIAC Projetos, Guarulhos (SP),V.5, n.2, jun.- dez. 2016. Disponível em: < https://www.governodigital.gov.brplone/eixos-de-atuacao/governo/sistema-deadministracao-dos-recursos-de-tecnologia-da-informacao-sisp/seguranca-dainformacao> Acesso em: 19 fev. 2019.

SURYANARAYANAN, V. Revisão: técnicas de minimização de falsos alarmes em sistemas de detecção de intrusão baseados em assinatura: uma pesquisa. Comput. Commun., Amsterdam, The Netherlands, The Netherlands, Agosto de 2014. v.49, p.1–17.

4. CONSIDERAÇÕES FINAIS / CONCLUSÃO

O trabalho realizado permitiu contextuar formas de segurança contra ataques indesejados nas redes. Conclui-se que o objetivo do trabalho foi alcançado, onde a avaliação do hardware Mikrotik RouterOS pode trazer benefícios como maior segurança e desempenho em redes de computadores quando comparada a uma rede comum que não faz uso da mesma.

É preciso colocar e instalar *softwares* e *hardwares* de segurança nas redes, mas também investir na contratação de bons profissionais da segurança de informação que compreendam e conheçam a melhor forma de usar essa ferramenta para que possa bloquear e dificultar as investidas dos atacantes mantendo assim as informações das empresas em constante proteção e segurança.

Assim, pode-se concluir ainda que uma boa política de segurança em redes deve ser item obrigatório e frequente para garantir uma proteção aceitável e correta, pois os danos e prejuízos causados por falta de monitoramento e ou um monitoramento lento podem resultar em falhas e comprometer todo um sistema.

5. REFERÊNCIAS

ALMEIDA FILHO, José Carlos de. **Processo eletrônico e teoria geral do processo eletrônico. A informatização judicial no Brasil**. 5. ed. revista e atualizada. Rio de Janeiro: Forense, 2015.

BITENCOURT, William Lopes. Implementação de politicas globais em redes SDN utilizando marcação de pacotes. Unisinos, São Leopoldo, 2014.

BHUYAN, M.; BHATTACHARYYA, D.; KALITA, J. **Network Anomaly Detection: methods, systems and tools. Communications Surveys Tutorials**, IEEE, v.16, n.1, 2014. p.303–336.

CARVALHO, Rubens dos Santos et al. **Usando criptografia em digitalização em redes**. 1. ed. Belém/PA: Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, 2018. cap. 1, p. 31-32. v. 1.

CARVALHO, P. B. S.; OLIVEIRA, J. P. Q. (2017). **E-commerce: perfil de estudantes universitários como consumidores virtuais**. Ano XIII, n. 02. Fevereiro/2017. Temática. - http://www.periodicos.ufpb.br/ojs2/index.php/tematica/article/view/33010/17145.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Org.). **Estatísticas dos Incidentes Reportados ao CERT.BR**. São Paulo: Comitê Gestor da Internet no Brasil, 2017. Disponível em: < https://www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html >. Acesso em 19 fev. 2019.

JUNQI, W.; ZHENGBING, H. **study of intrusion detection systems (idss) in network security. in: wireless communications, networking and mobile computing**, 2008. WICOM ’08. 4TH INTERNATIONAL CONFERENCE ON, 2008. p.1–4.

FERREIRA, CARLOS W. 2015, **Segurança de redes com IPS, sua relação com IDS e sua Importância no trabalho conjunto com o Firewall**. Disponível em: < https://goo.gl/GTi9CX>. Acesso em 20 Fev. 2019.

KIM, H; FEAMSTER, N**. Improving Network Management with Software Defined Networking.** Communications Magazine, IEEE, 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down.** Tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MD Brasil: Mikrotik RouterOS. **Mikrotik RouterOS**. 2019. Disponível em: <http://mdbrasil.com.br/solucoesemhardware/mikrotik-routeros/>. Acesso em: 02 maio 2019.

MIKROTIK. Mikrotik 2015. Disponível em: <http://www.mikrotik.com/>. Acesso em: 11 fev. 2019.

NADEAU, T. D; GRAY, K. SDN: Software **Defined Networks. ”O‟Reilly Media, Inc.”,** 2013.

NJOGU, H. W.; JIAWEI, L.; KIERE, J. N.; HANYURWIMFURA, D. A **Comprehensive Vulnerability Based Alert Management Approach for Large Networks.** Future Gener. Comput. Syst., Amsterdam, The Netherlands, The Netherlands, Janeiro de 2013. v.29, n.1, p.27–45.

RIOS, Orlivaldo Kleber Lima; RIOS, Vânia Patrícia da Silva; TEIXEIRA, FILHO, José Gilson de Almeida . **Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação.** Revista de Gestão e Tecnologia. Pernambuco, v. 7, n.2, p. 49-65, 14 nov. 2018. Disponível em: http://navus.sc.senac.br/index.php/navus/article/view/482/pdf Acesso em 19 fev. 2019.

SILVA, L. **O que é Mikrotik?**. [*S. l.*], 15 mar. 2019. Disponível em: https://www.4infra.com.br/o-que-e-mikrotik/. Acesso em: 15 mar. 2019.

SNORT, 2016. **The Snort Project. Disponível em**: <http://www.snort.org/>. Acesso em: 19 fev. 2019.

SOUZA, L. D. F.; LUCA, G. G. de. **Lei 12.965 de 2014: democratização da internet e efeitos do marco civil na sociedade da informação**. In: REVISTA PARADIGMA, 2014. p.76–96.

SOUZA, Jackson Gomes Soares et al. **Gestão de riscos da segurança da informação em uma instituição pública federal: um estudo de caso**. ENIAC Projetos, Guarulhos (SP),V.5, n.2, jun.- dez. 2016. Disponível em: < https://www.governodigital.gov.brplone/eixos-de-atuacao/governo/sistema-deadministracao-dos-recursos-de-tecnologia-da-informacao-sisp/seguranca-dainformacao> Acesso em: 19 fev. 2019.

SURYANARAYANAN, V. Revisão: técnicas de minimização de falsos alarmes em sistemas de detecção de intrusão baseados em assinatura: uma pesquisa. Comput. Commun., Amsterdam, The Netherlands, The Netherlands, Agosto de 2014. v.49, p.1–17.