INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES
CAMPUS MACAPÁ

HELDECIR LIMA NUNES
MARCIO ALBERTO MONTEIRO DE BRITO

GERENCIAMENTO DE REDE LOGICA COM ROTEADOR MIKROTIK NAS PEQUENAS E MEDIAS EMPRESAS

MACAPÁ – AP
2023

HELDECIR LIMA NUNES
MARCIO ALBERTO MONTEIRO DE BRITO

GERENCIAMENTO DE REDE LOGICA COM ROTEADOR MIKROTIK NAS PEQUENAS E MEDIAS EMPRESAS

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Me. Klenilmar Lopes Dias.

MACAPÁ - AP
2023

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

N972g Nunes, Heldecir Lima
Gerenciamento de rede lógica com roteadores Mikrotik nas pequenas e médias empresas / Heldecir Lima Nunes, Marcio Alberto Monteiro de Brito. - Macapá, 2023.
94 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2023.

Orientadora: Me. Klenilmar Lopes Dias.

1. Configurações de Mikrotik. 2. Segurança cibernética. 3. Redes lógicas. I. Brito, Marcio Alberto Monteiro de. I. Dias, Me. Klenilmar Lopes , orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP com os dados fornecidos pelo(a) autor(a).

HELDECIR LIMA NUNES

MARCIO ALBERTO MONTEIRO DE BRITO

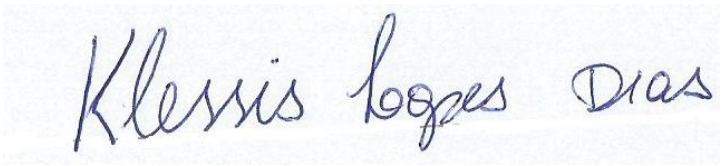
GERENCIAMENTO DE REDE LOGICA COM ROTEADOR MIKROTIK NAS PEQUENAS E MEDIAS EMPRESAS

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Me. Klenilmar Lopes Dias.

BANCA EXAMINADORA

Prof.° Me Klenilmar Lopes Dias - IFAP



Prof.° Me. Klessis Lopes Dias -IFAP

Prof.° Me Eonay Barbosa Gurjão - IFAP

Aprovados em: 16/11/2023

Nota:10

A minha amada esposa Stephanie Figueiredo Pimentel Nunes e seu apoio incondicional.

(NUNES, 2023)

A minha esposa Aline de Souza e as minhas duas filhas, Caliny Gabryelli Brito e Alicia Juliane Brito.

(BRITO, 2023)

AGRADECIMENTOS

A Deus, pelas nossas vidas, e por nos permitir ultrapassar todos os obstáculos encontrados ao longo da realização desta monografia.

Aos familiares por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho.

A todos aqueles que contribuíram de alguma forma para a realização deste trabalho.

A todos que participaram, direta ou indiretamente em seu desenvolvimento, enriquecendo o nosso processo de aprendizado na área tecnológica. Às pessoas com quem convivemos ao longo desses anos de curso, que nos incentivaram e que certamente tiveram impacto em nossa formação acadêmica.

“[...] O importante é que você tenha fé nas pessoas, que elas sejam boas e inteligentes, e se você lhes der ferramentas, elas farão coisas maravilhosas com elas”

(Steve Jobs)

RESUMO

A pesquisa realizada tem como objetivo analisar as funcionalidades dos roteadores MikroTik para o gerenciamento de redes lógicas em pequenas e médias empresas. A motivação para essa pesquisa surge dos avanços tecnológicos da MikroTik no campo de redes de computadores, com o desenvolvimento de equipamentos modernos e inteligentes que se adequam a diversos ambientes empresariais. A metodologia adotada é do tipo aplicada, com abordagem qualitativa e foco explicativo. Foram aplicadas oito configurações selecionadas da literatura em um ambiente de uma pequena empresa de saúde chamada Cooperativa Odontológica do Estado do Amapá, utilizando roteadores MikroTik modelo RB750GL. A fundamentação teórica inclui autores como Mosna e Moraes (2020), que abordam a configuração de VPNs site-to-site e client-to-site com OpenVPN e dispositivos MikroTik; Gazola (2013), que trata da configuração do failover de links de internet usando roteadores MikroTik; e Leão (2017), que explora a gestão de serviços de TI em um provedor de acesso à internet com enfoque na governança de TI. Verificou-se que o gerenciamento de redes lógicas com roteadores MikroTik nas pequenas e médias empresas trouxe resultados significativos, contribuindo para a resolução do problema proposto, destacando as funcionalidades relevantes desses roteadores e proporcionando uma formação acadêmica enriquecedora para os estudantes envolvidos. Os achados reforçaram a importância desses dispositivos como uma opção sólida para otimizar o desempenho e a segurança das redes empresariais em um ambiente cada vez mais digital e competitivo.

Palavras-chave: configurações de *Mikrotik*; segurança cibernética; gerenciamento de redes; redes lógicas.

ABSTRACT

The research conducted aims to analyze the functionalities of MikroTik routers for the management of logical networks in small and medium-sized companies. The motivation for this research arises from MikroTik's technological advances in the field of computer networks, with the development of modern and intelligent equipment that adapt to different business environments. The methodology adopted is of the applied type, with a qualitative approach and an explanatory focus. Eight configurations selected from the literature were applied in an environment of a small health company called Cooperativa Odontológica do Estado do Amapá, using MikroTik routers model RB750GL. The theoretical foundation includes authors such as Mosna and Moraes (2020), who address the configuration of site-to-site and client-to-site VPNs with OpenVPN and MikroTik devices; Gazola (2013), which deals with the configuration of internet link failover using MikroTik routers; and Leão (2017), which explores the management of IT services at an internet access provider with an approach to IT governance. It was verified that the management of logical networks with MikroTik routers in small and medium-sized companies brought satisfactory results, fortunately for the resolution of the proposed problem, highlighting the relevant functionalities of these routers and providing an enriching academic formation for the students involved. The findings strengthened the importance of these devices as a solid option to optimize the performance and security of corporate networks in an increasingly digital and competitive environment.

Keywords: Mikrotik settings; cybersecurity; network management; logical networks.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT NBR	Associação Brasileira de Normas Técnicas - Norma Brasileira
ACLs	Listas de Controle de Acesso
AP	Access Point
ARP	Address Resolution Protocol
CLI	Command Line Interface (Interface de Linha de Comando)
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface (Interface Gráfica do Usuário)
HTTP	Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto)
IP	Internet Protocol (Protocolo de Internet)
IPSec	Internet Protocol Security
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network (Rede de Área Local)
LEASE TIME	Tempo de validade da concessão de endereço IP pelo servidor DHCP
MAC	Media Access Control
Mbps	Megabits por segundo
MIKROTIK	Nome da plataforma de roteamento e gerenciamento de rede
MTBF	Mean Time Between Failures
NAT	Network Address Translation
OVPN	OpenVPN
P2P	Peer-to-Peer (Ponto a Ponto)
POOL DE IP	Conjunto de endereços IP disponíveis para atribuição pelo servidor DHCP
PPTP	Point-to-Point Tunneling Protocol

QoS	Quality of Service (Qualidade de Serviço)
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RouterOS	Sistema operacional usado nos roteadores MikroTik
SSH	Secure Shell
TCP	Transmission Control Protocol (Protocolo de Controle de Transmissão)
TI	Tecnologia da Informação
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuário)
VoIP	Voice over Internet Protocol (Voz sobre Protocolo de Internet)
VPN	Virtual Private Network
WAN	Wide Area Network (Rede de Área Ampla)
WEBFIG	Interface de gerenciamento gráfico do MikroTik via web
WINBOX	Interface de gerenciamento gráfico do MikroTik
WINS	indows Internet Name Service

LISTA DE SIMBOLOS

°C	Graus Celsius
Bps	Bits por segundo
C	Grau Celsius (temperatura)
G	Gramas
GHz	Gigahertz
MB	Megabytes
Mbps	Megabits por segundo
µs	Microssegundos

SUMÁRIO

1 INTRODUÇÃO

A MikroTik é uma empresa de tecnologia fundada na Letônia em 1996 por John Trully e Arnis Riekstins. Inicialmente, a empresa surgiu como um projeto para o desenvolvimento do sistema operacional de roteadores chamado RouterOS. Esse sistema operacional foi concebido para rodar em hardware de baixo custo, permitindo que a MikroTik oferecesse soluções acessíveis para redes de pequenas e médias empresas (MOZUCO, 2023). Ao longo do tempo, a MikroTik consolidou sua presença no setor de provedores e empresas, notadamente através de seus equipamentos modernos e inteligentes, os quais se adaptam a diversos ambientes, atendendo tanto empresas de pequeno porte quanto grandes corporações e provedores.

A motivação que nos levou a pesquisar sobre o gerenciamento de redes lógicas por meio de roteadores da MikroTik, com foco nas pequenas e médias empresas, está alinhada com os avanços tecnológicos notáveis no campo das redes de computadores. A MikroTik está constantemente evoluindo, apresentando novas tecnologias e funcionalidades de forma regular. Explorar as funcionalidades dos roteadores MikroTik nos permitiu adquirir uma experiência prática fundamental para os administradores de redes, possibilitando que acompanhem as últimas tendências e inovações no gerenciamento de redes lógicas em ambientes de pequenas e médias empresas.

O objetivo geral desta pesquisa é analisar as funcionalidades dos roteadores MikroTik no gerenciamento de redes lógicas em pequenas e médias empresas. Os objetivos específicos são os seguintes:

Identificar as funcionalidades dos roteadores MikroTik relevantes para o gerenciamento de redes lógicas nessas empresas de porte reduzido e médio.

Avaliar a eficiência e a capacidade de escalabilidade das funcionalidades dos roteadores MikroTik no contexto das redes lógicas em ambientes de pequenas e médias empresas.

Analisar o impacto das funcionalidades dos roteadores MikroTik no desempenho, segurança e disponibilidade das redes lógicas em pequenas e médias empresas.

Dessa maneira, obtivemos uma compreensão das funcionalidades dos roteadores MikroTik e como elas atendem às necessidades das pequenas e médias empresas. Isso nos permitiu avaliar o impacto dessas funcionalidades nas redes

lógicas em termos de eficiência, escalabilidade, desempenho, segurança e disponibilidade.

O problema de pesquisa em foco é: "Quais funcionalidades os roteadores MikroTik proporcionam para o gerenciamento de redes lógicas em pequenas e médias empresas?"

A justificativa desta pesquisa abrange um conjunto específico de fatores relacionados ao contexto das pequenas e médias empresas:

Eficiência e Otimização de Recursos:

No ambiente empresarial, a eficiência operacional é fundamental. A pesquisa sobre as funcionalidades dos roteadores MikroTik auxilia os administradores de redes na identificação de recursos e ferramentas que aprimoram a eficiência e otimizam a utilização dos recursos de rede. Isso resulta em um melhor desempenho, menor latência, maior disponibilidade e redução do custo operacional.

Necessidades Específicas das Pequenas e Médias Empresas:

Essas empresas possuem exigências singulares no que tange ao gerenciamento de redes, pois, comumente, têm recursos limitados e necessitam de soluções acessíveis e escaláveis. A pesquisa sobre as funcionalidades dos roteadores MikroTik oferece insights sobre como essas soluções atendem às necessidades específicas dessas empresas, permitindo que os administradores de redes tomem decisões embasadas ao projetar e implementar suas redes. Adicionalmente, a segurança da rede é um fator relevante, uma vez que representa uma preocupação crítica em qualquer ambiente de rede. Ao investigar as funcionalidades dos roteadores MikroTik para o gerenciamento de redes lógicas, os administradores de redes podem explorar recursos de segurança, como firewall, VPN, filtragem de conteúdo e controle de acesso, que são essenciais para proteger as redes contra ameaças e ataques cibernéticos.

Desenvolvimento Profissional:

O conhecimento aprofundado sobre as funcionalidades dos roteadores MikroTik para o gerenciamento de redes lógicas nas pequenas e médias empresas é relevante para o desenvolvimento profissional dos administradores de redes. Esse conhecimento pode abrir portas para oportunidades de emprego ou promoção, além de fortalecer a expertise técnica e a habilidade de solucionar problemas em ambientes de rede complexos.

Portanto, a pesquisa sobre as funcionalidades dos roteadores MikroTik para o gerenciamento de redes lógicas em pequenas e médias empresas apresenta uma motivação acadêmica ao explorar avanços tecnológicos, eficiência operacional, necessidades específicas das empresas, segurança da rede e desenvolvimento profissional dos administradores de redes de computadores.

A pesquisa em questão adota uma natureza eminentemente aplicada, centrada na geração de conhecimentos destinados à aplicação prática. Em relação à abordagem do problema, assume uma perspectiva qualitativa, dado que os conhecimentos teóricos selecionados serão empiricamente aplicados em um contexto específico, mais precisamente em uma pequena empresa situada no estado do Amapá. Nessa ótica, a revisão da literatura propicia a construção de um conhecimento qualitativo intrínseco ao ambiente investigado no âmbito tecnológico.

Em consonância com os objetivos delineados, a pesquisa adota uma abordagem explicativa. Seu propósito reside em identificar os fatores determinantes e contributivos para um gerenciamento eficaz de redes lógicas nas pequenas empresas.

A pesquisa aplicou oito configurações selecionadas da literatura, concebidas para serem implementadas na interface dos roteadores MikroTik. Tais configurações foram utilizadas para prototipar procedimentos práticos em um ambiente de Tecnologia da Informação (TI) de uma pequena empresa denominada "Cooperativa Odontológica do Estado do Amapá". Para contextualizar a pesquisa, é relevante mencionar que o CNPJ da empresa é 02.254.846/0001-83, com sede em Macapá, AP. A empresa possui 25 anos, 7 meses e 12 dias de existência, tendo sido fundada em 27/11/1997. Sua situação cadastral é ativa e sua principal atividade econômica é a prestação de serviços de planos de saúde.

As especificações técnicas do roteador utilizado são as seguintes: a) Código do produto: RB750GL; b) Arquitetura: MIPSBE; c) CPU: AR7242; d) Número de núcleos da CPU: 1; e) Frequência nominal da CPU: 400 MHz; f) Modelo do chip de comutação: AR8327-BL1A; g) Dimensões: 113x89x28mm; h) Peso sem embalagem e cabos: 129g; i) Licença do RouterOS: 4; j) Sistema Operacional: RouterOS; k) Tamanho da RAM: 64 MB; l) Tamanho do armazenamento: 64 MB; m) Tipo de armazenamento: NAND; n) MTBF: Aproximadamente 100.000 horas a 25°C; o) Temperatura ambiente testada: -30°C a +70°C.

No escopo teórico, destacam-se autores como Mosna e Moraes (2020), que oferecem um guia abrangente para a configuração de VPNs site-to-site e client-to-site

usando o OpenVPN e dispositivos MikroTik. Gazola (2013) proporciona um guia prático e abrangente para a configuração de failover de links de internet utilizando roteadores MikroTik. Leão (2017), por sua vez, explora a gestão de serviços de TI em um provedor de acesso à internet, com ênfase na aplicação da governança de TI.

Por fim, as considerações finais sintetizam os principais achados e descobertas que impactam na eficiência do gerenciamento de redes lógicas.

2 ROTEADORES MIKROTIK – POSSIBILIDADES E SEGURANÇA

O Mikrotik é uma plataforma de roteamento e gerenciamento de rede baseada em software que oferece uma ampla gama de recursos e funcionalidades. Ele é conhecido por sua confiabilidade, desempenho e flexibilidade. O Mikrotik é executado em hardware dedicado ou em computadores padrão, transformando-os em poderosos roteadores e firewalls[1] com recursos avançados. Ele possui um sistema operacional chamado RouterOS[2], que fornece uma interface intuitiva para configurar e controlar diversos aspectos da rede, (MIKROTIK, 2023).

Mosna e Moraes (2020), abordam o uso de tecnologias de VPN[3] (*Virtual Private Network*) para médias empresas utilizando o software OpenVPN[4] em conjunto com os roteadores Mikrotik[5], bem como, compreende que a VPN é uma ferramenta valiosa para empresas, permitindo a criação de uma rede privada virtual sobre a infraestrutura da Internet pública. Ela estabelece uma conexão segura entre diferentes locais ou dispositivos remotos, garantindo que os dados transmitidos sejam criptografados e protegidos contra acessos não autorizados.

Mosna e Moraes (2020), explicam sobre a *VPN site-to-site*[6], configurações nas quais são criadas conexões seguras entre duas ou mais redes geograficamente distintas da empresa. Isso permite que os escritórios da média empresa, localizados em diferentes lugares, se comuniquem de forma segura, como se estivessem conectados diretamente na mesma rede local. Isso proporciona maior eficiência, produtividade e compartilhamento de recursos entre os escritórios, sem comprometer a segurança dos dados.

Mosna e Moraes (2020), explanam também sobre a *VPN client-to-site*[7], nessa configuração, os funcionários ou dispositivos remotos podem se conectar à rede da

---

1 Firewall é um sistema de segurança de rede de computadores que limita o tráfego de entrada, saída ou trocas dentro de um rede privada. Acesse ‘Configurando MikroTik como Firewall’: https://dtnetwork.com.br/mikrotik-como-firewall/.
2 Acesse ‘RouterOS é o sistema operacional do RouterBOARD’: https://mikrotik.com/software.
3 É uma forma de conectar dois computadores através de uma rede pública, como a Internet. Acesse ‘O que é uma VPN?’: https://canaltech.com.br/internet/o-que-e-vpn-23748/.
4 Acesse ‘Acesso seguro e conectividade de rede reimaginados’: https://openvpn.net/.
5 Acesse ‘Como configurar o servidor OpenVPN no Mikrotik’: https://www.youtube.com/watch?v=pv10UCgG0yQ.
6 Acesse ‘Como funciona a VPN Site-to-Site’: https://4future.com.br/index.php/2021/04/09/como-funciona-a-vpn-site-to-site/.
7 Acesse ‘Client to Site’: https://learn.microsoft.com/pt-br/shows/technet-brasil-cursos-de-infraestrutura/client-to-site.

empresa de forma segura por meio de um cliente *OpenVPN* instalado em seus dispositivos. Isso é útil para colaboradores que trabalham de casa ou em locais externos, pois lhes permite acessar recursos internos da empresa de maneira segura e criptografada, como se estivessem fisicamente presentes na rede local da organização. A utilização desses tipos de configurações trazem benefícios para médias e pequenas empresas, enfatizados pelos autores como:

A utilização de VPNs garante que todas as comunicações e dados transmitidos entre os locais ou dispositivos remotos estejam criptografados, protegendo-os contra ataques cibernéticos e interceptações não autorizadas.

A configuração de *VPNs site-to-site* proporciona uma conexão eficiente entre os escritórios e filiais da média empresa, permitindo um compartilhamento rápido e seguro de informações e recursos. Com a VPN client-to-site, os funcionários podem acessar os recursos internos da empresa de forma segura, mesmo quando estão trabalhando remotamente, o que aumenta a flexibilidade e produtividade da equipe.

Ao criar uma rede privada virtual sobre a Internet pública, as médias empresas podem evitar o alto custo de investir em linhas de comunicação dedicadas entre escritórios e, ao mesmo tempo, garantir um alto nível de segurança. A configuração de VPNs com OpenVPN e Mikrotik, torna mais fácil para as médias empresas implementarem essas soluções em suas redes.

Leão (2017), aborda a importância da configuração e gerenciamento da rede usando roteadores Mikrotik em um provedor de acesso à Internet. O estudo está inserido no contexto da Governança de Tecnologia da Informação (TI) e foi realizado em 2017. O autor se concentra em um ambiente específico, um provedor de acesso à Internet. Essas empresas são responsáveis por fornecer conexão à Internet para clientes e, portanto, a qualidade, segurança e eficiência de seus serviços de rede são essenciais para garantir a satisfação dos clientes e a competitividade no mercado.

Leão (2017), aborda a Governança de TI, um conjunto de práticas e processos que garantem a gestão eficaz dos recursos de TI de uma organização. Ela visa alinhar as estratégias de TI aos objetivos do negócio, otimizar o uso dos recursos de tecnologia e assegurar a conformidade com normas e regulamentos.

Leão (2017), menciona os roteadores Mikrotik como uma das soluções tecnológicas utilizadas no provedor de acesso para configuração e gerenciamento da rede. Esses roteadores são amplamente reconhecidos no mercado devido à sua flexibilidade, recursos avançados e escalabilidade. A configuração correta dos

roteadores Mikrotik é essencial para garantir o funcionamento eficiente e seguro da rede. Uma configuração inadequada pode levar a problemas de desempenho, vulnerabilidades de segurança e, consequentemente, impactar negativamente a qualidade do serviço fornecido aos clientes.

A segurança é uma preocupação primordial em um provedor de acesso à Internet, pois a rede está constantemente exposta a ameaças externas. Os roteadores Mikrotik oferecem recursos de segurança avançados, como VPN, firewall, filtragem de pacotes, entre outros, que ajudam a proteger a rede e os dados dos clientes contra ataques maliciosos.

Portando, a configuração e o gerenciamento adequado da rede com roteadores Mikrotik são fundamentais para a eficiência operacional, a qualidade dos serviços prestados e a segurança da rede em um provedor de acesso à Internet o que pode ser estender ao contexto de segurança de redes de penas e médias empresas. Uma abordagem de Governança de TI bem estruturada em conjunto com tecnologias confiáveis como a Mikrotik pode levar a uma experiência positiva para os clientes e ao sucesso da empresa no mercado altamente competitivo.

Londoño Velásquez (2015), trata do projeto de uma rede para a empresa Surtitodo SA, usando roteadores Mikrotik como base. Verificando pontos positivos sobre o custo-benefício dos roteadores Mikrotik para pequenas e médias empresas, destacando os seguintes pontos:

Os roteadores Mikrotik são conhecidos por oferecer uma solução de rede de alta qualidade a um preço mais acessível em comparação com muitos outros roteadores disponíveis no mercado. Esse fator é particularmente atraente para pequenas e médias empresas, que geralmente possuem orçamentos mais limitados para investir em infraestrutura de rede. Mesmo sendo mais acessíveis em termos de custo, os roteadores Mikrotik são conhecidos por sua versatilidade e recursos avançados. Eles oferecem uma ampla gama de funcionalidades, incluindo roteamento dinâmico, VPN, firewall, balanceamento de carga, controle de banda e muito mais. Esses recursos permitem que as pequenas e médias empresas otimizem sua rede, garantindo desempenho e segurança adequados para atender às suas necessidades específicas.

Os roteadores Mikrotik são conhecidos por sua interface de gerenciamento intuitiva e amigável, o que torna mais fácil para pequenas e médias empresas configurarem, monitorarem e gerenciarem sua rede sem a necessidade de um

profundo conhecimento técnico em redes. Os roteadores MikroTik são escaláveis, o que significa que eles podem se adequar ao crescimento das pequenas e médias empresas. Conforme a empresa expande suas operações e requisitos de rede, os roteadores Mikrotik podem ser facilmente atualizados ou adicionados, sem a necessidade de substituir toda a infraestrutura.

A Mikrotik tem uma comunidade de usuários ativa e engajada, o que significa que as pequenas e médias empresas podem encontrar uma rica fonte de informações, tutoriais e suporte online para ajudá-las a resolver problemas ou otimizar sua rede. A segurança é uma preocupação crítica para qualquer empresa, independentemente do tamanho. Os roteadores Mikrotik oferecem recursos avançados de segurança, como firewall, filtragem de pacotes, criptografia e autenticação, protegendo a rede e os dados da empresa contra ameaças cibernéticas.

A plataforma BrasilPeeringForum (2019), disponibiliza algumas boas práticas de segurança para roteadores Mikrotik em pequenas e médias empresas:

Quadro 1 – Boas práticas de segurança para roteadores Mikrotik

ACLs (Listas de Controle de Acesso):
Restrinja o acesso aos serviços do Mikrotik, como Winbox[8], Telnet, SSH e web, apenas às redes confiáveis. Desabilite os serviços não utilizados para reduzir possíveis pontos de entrada para invasores.
Credenciais de Acesso:
Nunca mantenha o login e senha padrão. Altere-os imediatamente antes de conectar o equipamento à rede. Evite usar o login "admin" e use senhas seguras com pelo menos oito caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais. Utilize sistemas de autenticação seguros, como RADIUS[9], se possível.
Acesso via VPN:
Utilize VPNs (PPTP, L2TP, OVPN, IPSec) para acessar os equipamentos. Configure ACLs em /ip services para restringir o acesso à IPs de VPN e outras redes confiáveis.
Filtros anti spoofing:
Utilize o recurso "Reverse Path Filter (RPF)" para controlar o IP spoofing. Configure o RPF no modo "strict" para equipamentos com caminhos simétricos para redes externas. Teste e homologue o funcionamento antes de ativá-lo definitivamente na rede.
Firewall para clientes banda larga:

8 Acesse: ‘Software de configuração para utilização em RouterOS’: https://winbox.softonic.com.br/.
9 Acesse: ‘Integrar a autenticação RADIUS com o Servidor de Autenticação Multifator do Azure’: https://learn.microsoft.com/pt-br/azure/active-directory/authentication/howto-mfaserver-dir-radius.

Bloqueie portas não utilizadas pelos clientes, como 19 (Chargen), 25 (SMTP), 1900 (SSDP) e 11211 (Memcached), para evitar abusos e ataques.
Atualizações:
Mantenha o firmware do roteador MikroTik sempre atualizado para garantir que as correções de segurança mais recentes estejam em vigor e proteger contra vulnerabilidades conhecidas.

Fonte: BrasilPeeringForum (2019).

Essas boas práticas visam melhorar a segurança da rede, minimizando riscos de invasões e garantindo a integridade e confidencialidade dos dados para pequenas e médias empresas que utilizam roteadores Mikrotik. É importante entender e modificar as configurações de acordo com as necessidades específicas de cada ambiente antes de aplicá-las.

Ribeiro (2016), baseia-se em recomendações de segurança nas diretrizes estabelecidas na norma ABNT NBR ISO/IEC 27001. Essa norma estabelece processos e controles para gerenciar e proteger a segurança da informação em uma organização.

Ribeiro (2016), faz a aplicação das diretrizes da norma na configuração e gerenciamento do sistema de roteamento Mikrotik, visando aprimorar a segurança da rede de computadores. Isso incluiu a configuração adequada de ACLs, autenticação de usuários, controle de banda, VPNs, firewall, entre outros recursos de segurança disponíveis no Mikrotik.

Ribeiro (2016), aponta benefícios envolvem a proteção contra ameaças cibernéticas, o controle de acesso a recursos, a integridade e confidencialidade dos dados, o aumento da disponibilidade da rede e a conformidade com padrões de segurança reconhecidos. Assim, enfatiza a importância de adotar uma abordagem proativa para a gestão da segurança em redes de computadores. Isso envolve não apenas a implementação de tecnologias e práticas de segurança, mas também a conscientização e o treinamento dos usuários e a atualização contínua das medidas de segurança conforme as ameaças evoluem.

A partir das percepção e estudos do autores Mosna e Moraes (2020), Leão (2017), Londoño Velásquez (2015), Ribeiro (2016), ficou evidente que os roteadores MikroTik apresentam uma série de benefícios e vantagens para pequenas e médias empresas. Sua versatilidade, confiabilidade, recursos avançados, escalabilidade e interface de gerenciamento intuitiva tornam-nos uma solução ideal para melhorar a eficiência, a produtividade e a segurança das redes empresariais. A combinação com

tecnologias de VPN permite o estabelecimento de conexões seguras entre diferentes locais e dispositivos remotos, promovendo a colaboração e o compartilhamento de recursos. Além disso, seu custo-benefício atrativo e a adoção de boas práticas de segurança reforçam o valor dos roteadores Mikrotik como uma opção sólida para o crescimento e sucesso das empresas em um ambiente cada vez mais digital e competitivo.

2.1 Instalação e configuração do servidor DHCP de um MikroTik

A instalação e configuração do servidor DHCP (Dynamic Host Configuration Protocol) em um roteador MikroTik é uma etapa fundamental para a criação de uma rede funcional e eficiente. O DHCP é responsável por atribuir automaticamente endereços IP e outras informações de configuração a dispositivos na rede, tornando o processo de conexão e configuração mais simples e automatizado.

2.1.1 Dynamic Host Configuration Protocol (DHCP)

Rahman, Sumarna e Nurdin (2020), avaliam o desempenho do DHCP no RouterOS MikroTik em uma rede de internet. Os autores procuram entender como o protocolo é implementado e executado no ambiente do roteador MikroTik e como ele lida com a atribuição de endereços IP e outras configurações para dispositivos conectados. Eles configuraram um ambiente de teste com o RouterOS MikroTik como roteador principal e conectam vários dispositivos a essa rede. Em seguida, realizam testes e medições para coletar dados sobre o tempo de resposta, eficiência e escalabilidade do serviço DHCP nesse cenário.

Rahman, Sumarna e Nurdin (2020), após os testes, apresentam em forma de gráficos, estatísticas e análises detalhadas do desempenho do DHCP no MikroTik em diferentes condições de carga de rede e número de dispositivos conectados.

Eles destacam métricas como o tempo médio de concessão de endereços IP, a taxa de sucesso na atribuição de IPs e a capacidade do serviço DHCP em lidar com muitas solicitações simultâneas.

Os autores enfatizam a importância de configurar adequadamente o serviço DHCP para obter um desempenho otimizado e garantir uma experiência de conectividade mais eficiente para os usuários da rede.

Portando, Rahman, Sumarna e Nurdin (2020), contribuem para a compreensão da performance do DHCP no RouterOS MikroTik e fornece insights relevantes para profissionais de redes e administradores que utilizam roteadores MikroTik.

As informações obtidas podem ser usadas para otimizar o serviço DHCP e melhorar o desempenho geral da rede em ambientes que utilizam esse sistema operacional.

2.1.2 Servidor DHCP

O servidor DHCP é um componente que opera em uma rede e é responsável por gerenciar o pool de endereços IP disponíveis e atribuí-los aos dispositivos que solicitam conexão à rede.

Marcillo e Benites (2019), abordam a importância e a justificativa para a utilização de um servidor DHCP no MikroTik como uma medida de segurança fundamental para proteger a rede contra ataques internos. O trabalho destaca os desafios associados aos ataques de ARP Spoofing, MAC Flooding e DHCP Spoofing, e como a implementação adequada do DHCP pode ser uma estratégia eficaz para mitigar essas ameaças. Ataques internos, como ARP Spoofing, MAC Flooding e DHCP Spoofing, representam um risco significativo para a segurança das redes de computadores. Esses ataques exploram vulnerabilidades nas camadas de comunicação da rede e podem levar a interrupções de serviço, interceptação de dados confidenciais e violações de privacidade.

A necessidade de proteção surge da crescente complexidade das redes e a proliferação de dispositivos conectados aumentaram o potencial de ataques internos. Isso torna fundamental a adoção de medidas de segurança eficazes para proteger a integridade e a confidencialidade dos dados. O DHCP desempenha um papel crucial na configuração automática de endereços IP e outras configurações de rede para dispositivos conectados. Utilizar um servidor DHCP no MikroTik é relevante porque permite um controle centralizado da atribuição de endereços IP, evitando assim a utilização de IPs duplicados e identificando possíveis ataques de *spoofing*.

O ARP *Spoofing* é um ataque que visa manipular a tabela ARP de um dispositivo, redirecionando o tráfego para um atacante. Com a utilização de um servidor DHCP no MikroTik, é possível implementar técnicas como "DHCP *Snooping*", que monitora o tráfego DHCP e ARP para detectar possíveis tentativas de spoofing, (MARCILLO; BENITES, 2019).

O MAC *Flooding* é um ataque em que um atacante inunda a tabela de endereços MAC de um *switch*, resultando em perda de conectividade. Ao implementar um servidor DHCP no MikroTik, é possível configurar limites de endereços MAC por porta para prevenir esse tipo de ataque, (MARCILLO; BENITES, 2019).

O DHCP *Spoofing* envolve um atacante fornecendo informações de configuração de rede falsas, levando dispositivos a se conectarem a um servidor

malicioso. Com um servidor DHCP bem configurado no MikroTik, é possível implementar autenticação DHCP para garantir que apenas servidores DHCP autorizados possam fornecer configurações de rede aos dispositivos, (MARCILLO; BENITES, 2019).

Com os aspectos apresentados por Marcillo e Benites (2019) pode-se afirmar que a utilização de um servidor DHCP no MikroTik é essencial para garantir a segurança e a integridade da rede contra os ataques internos de ARP Spoofing, MAC Flooding e DHCP Spoofing. A implementação adequada do DHCP permite uma gestão centralizada dos endereços IP e configurações de rede, além de possibilitar a aplicação de medidas de prevenção e detecção contra esses tipos de ataques, fortalecendo a infraestrutura de rede e protegendo os dados dos usuários.

2.1.3 Cliente DHCP

Os dispositivos na rede que solicitam um endereço IP e outras configurações ao se conectar são chamados de clientes DHCP. Quando um dispositivo é ligado ou conectado à rede, ele envia uma solicitação DHCP para obter suas configurações de rede.

Kurina (2020), aborda a exploração de vulnerabilidades do Cliente DHCP em roteadores MikroTik, especificamente o ataque conhecido como "DHCP *Starvation Attack*". O estudo analisa os riscos associados a esse tipo de ataque e explora formas de segurança para mitigar os impactos dessas vulnerabilidades.

O Cliente DHCP é uma parte essencial do protocolo DHCP, que permite aos dispositivos obterem automaticamente configurações de rede, como endereço IP, *gateway* padrão e servidor DNS. No entanto, algumas implementações do Cliente DHCP em roteadores MikroTik podem apresentar vulnerabilidades, permitindo ataques maliciosos como o "DHCP Starvation Attack". O DHCP Starvation Attack é uma técnica na qual um atacante envia uma grande quantidade de solicitações DHCP falsas para o servidor DHCP do roteador MikroTik, esgotando o pool de endereços disponíveis para novos dispositivos legítimos. Como resultado, os dispositivos legítimos não conseguem obter endereços IP válidos, levando à interrupção do serviço e indisponibilidade da rede, (KURINA, 2020).

Kurina (2020), analisa a exploração do Cliente DHCP em roteadores MikroTik por meio do DHCP Starvation Attack. Apontando as condições em que esse tipo de

ataque pode ser bem-sucedido, incluindo o comportamento do servidor DHCP do MikroTik em relação ao número de solicitações recebidas e a capacidade de processamento. A autora propõe formas de segurança para mitigar o impacto do DHCP Starvation Attack e outras vulnerabilidades relacionadas ao Cliente DHCP em roteadores MikroTik.

Implementar limites de solicitações DHCP por endereço MAC ou por porta, a fim de impedir que um único dispositivo ou atacante sobrecarregue o servidor DHCP do roteador MikroTik com solicitações falsas. Monitorar e registrar as atividades do servidor DHCP para detectar padrões de comportamento suspeitos e identificar possíveis ataques em tempo real. Ajustar a configuração do pool DHCP para garantir que haja endereços suficientes disponíveis para atender à demanda da rede e evitar o esgotamento de endereços por meio de ataques, (KURINA, 2020).

A principal contribuição que Kurina (2020) traz é a necessidade de adotar medidas proativas para proteger a infraestrutura de rede contra ataques, como o DHCP Starvation Attack. A implementação de formas de segurança adequadas é fundamental para garantir o funcionamento confiável e seguro da rede e evitar interrupções ou danos causados por exploração de vulnerabilidades no protocolo DHCP.

2.1.4 Pool de endereços IP

É o conjunto de endereços IP disponíveis que o servidor DHCP pode atribuir aos clientes. O pool é definido pelo intervalo de endereços IP que serão utilizados para alocar aos dispositivos na rede.

Silva (2017), explica que o pool de endereços IP é uma parte essencial da gestão de uma rede, permitindo que os dispositivos conectados obtenham endereços IP de forma dinâmica. Através do roteador MikroTik, é possível configurar e administrar o pool de endereços IP para atender às necessidades da rede. A correta alocação de endereços IP é fundamental para evitar esgotamento do pool e garantir que todos os dispositivos possam ser conectados sem conflitos.

Silva (2017), explana sobre políticas de atribuição de endereços IP, como a duração do tempo de concessão do endereço (lease time) e a forma de atribuição de endereços (por exemplo, endereços estáticos para determinados dispositivos e

endereços dinâmicos para outros). Essas políticas podem ser configuradas no roteador MikroTik para otimizar o uso dos endereços IP disponíveis.

Silva (2017), oferece uma contribuição significativa para os administradores de redes em pequenas e médias empresas em relação à gestão do pool de endereços IP em roteadores MikroTik. Através de uma abordagem prática e bem documentada, o trabalho demonstra como configurar o pool de endereços IP no MikroTik para fornecer atribuição dinâmica e automática de endereços para dispositivos na rede.

Os administradores de redes em pequenas e médias empresas se beneficiam com a otimização dos recursos de rede por meio da correta gestão do pool de endereços IP. Ao configurar adequadamente o DHCP no roteador MikroTik, o trabalho permite uma utilização mais eficiente dos endereços disponíveis, evitando conflitos de IP e garantindo que todos os dispositivos conectados tenham acesso à rede.

A implementação eficiente do DHCP contribui para facilitar a administração e manutenção da rede. Ao utilizar o pool de endereços IP gerenciado pelo roteador MikroTik, os administradores de redes não precisam configurar manualmente os endereços IP para cada dispositivo, economizando tempo e esforço.

Silva (2017) com seu estudo abre margem para os administradores de redes em pequenas e médias empresas, oferecendo uma solução eficiente e escalável para a gestão do pool de endereços IP em roteadores MikroTik. Ao otimizar os recursos de rede, facilitar a administração e manutenção e fornecer maior segurança, a proposta do trabalho é valiosa para tornar a gestão de endereços IP mais eficiente e confiável em ambientes empresariais de menor porte.

2.1.5 Concessão DHCP

Ribeiro (2016), apresenta uma abordagem relevante sobre a concessão de endereços IP no roteador MikroTik como parte de um conjunto de medidas para fortalecer a segurança em redes de computadores, alinhado com as diretrizes da norma ABNT NBR ISO/IEC 27001. Quando um dispositivo cliente solicita um endereço IP, o servidor DHCP oferece uma "concessão", que é o endereço IP e outras configurações fornecidas temporariamente ao dispositivo. A concessão tem um tempo de validade (chamado de "lease time") que define por quanto tempo o dispositivo pode utilizar esse endereço IP antes de renovar a solicitação.

A segurança em redes de computadores é uma preocupação fundamental para empresas e organizações. A norma ABNT NBR ISO/IEC 27001 é um padrão internacional que estabelece diretrizes para a gestão de segurança da informação, abordando uma ampla gama de aspectos, incluindo a concessão de endereços IP em roteadores.

Ribeiro (2016), explora como o roteador MikroTik pode ser utilizado para implementar um sistema seguro de concessão de endereços IP. Ao configurar o DHCP no MikroTik, os administradores podem fornecer uma atribuição dinâmica e controlada de endereços IP para dispositivos na rede. A concessão de endereços IP no roteador MikroTik permite o monitoramento e registro das atividades do DHCP. Isso inclui a capacidade de identificar possíveis tentativas de ataques, como o DHCP Starvation Attack, e rastrear a utilização dos endereços IP atribuídos. Portanto, ao utilizar o DHCP de forma segura e controlada, os administradores podem fortalecer a proteção da rede e garantir uma gestão eficiente e confiável dos endereços IP atribuídos aos dispositivos conectados.

2.1.6 Configuração do servidor DHCP no MikroTik

Para configurar o servidor DHCP em um MikroTik, é necessário acessar a interface de gerenciamento do roteador (Winbox, Webfig ou CLI) e configurar o serviço DHCP. Isso inclui definir o pool de endereços IP disponíveis, as opções de rede, como gateway padrão e servidores DNS, e outros parâmetros relevantes para a rede.

Além do endereço IP, o servidor DHCP pode fornecer várias opções adicionais aos clientes, como máscara de sub-rede, gateway padrão, servidores DNS, servidor WINS, entre outras. Essas opções são configuradas no servidor DHCP para que os clientes as recebam automaticamente. Em redes com mais de um segmento, é necessário utilizar o recurso de DHCP Relay para permitir que os dispositivos em um segmento solicitem endereços IP a partir de um servidor DHCP localizado em outro segmento da rede. O DHCP Relay encaminha as solicitações dos clientes para o servidor DHCP e retransmite as respostas para os clientes.

A instalação e configuração adequadas do servidor DHCP em um MikroTik são essenciais para garantir que todos os dispositivos na rede obtenham endereços IP e configurações corretas, tornando o processo de conexão à rede mais eficiente e simplificado. Além disso, a configuração correta do pool de endereços IP e das opções

DHCP ajudam a otimizar o uso dos recursos de rede e a promover um ambiente de rede estável e funcional.

2.1.7 Prática para o MicroTik – Servidor DHCP

Para fins práticos, apresenta-se o processo de configuração do servidor DHCP no MikroTik em uma empresa pequena com 4 computadores:

Quadro 2 – Processo prático de configuração do servidor DHCP

Passo 1: Conectar o Roteador MikroTik à Rede
Certifique-se de que o roteador MikroTik esteja corretamente conectado à rede da empresa, seja através de uma porta Ethernet conectada a um switch ou diretamente aos computadores.
Passo 2: Acessar o Roteador MikroTik
Acesse o roteador MikroTik através de um navegador da web digitando o endereço IP padrão do MikroTik na barra de endereços. O endereço IP padrão costuma ser 192.168.88.1, mas pode variar dependendo da configuração inicial do dispositivo.
Passo 3: Login no Roteador
Faça login no roteador MikroTik usando as credenciais de acesso padrão (por exemplo, usuário "admin" e senha em branco). Caso as credenciais padrão tenham sido alteradas, utilize as credenciais atualizadas.
Passo 4: Acesso à Interface Winbox (opcional)
Você também pode usar a interface Winbox para configurar o roteador MikroTik, que é uma ferramenta de gerenciamento gráfico disponibilizada pela MikroTik. Baixe e instale o Winbox em seu computador, insira o endereço IP do roteador e faça login com as credenciais de acesso.
Passo 5: Acesso à Interface WebFig (opcional)
Outra opção para configuração é a interface WebFig, que também oferece uma interface gráfica para gerenciar o roteador MikroTik. Você pode acessar digitando o endereço IP do roteador no navegador seguido de ":8080" (por exemplo, http://192.168.88.1:8080).
Passo 6: Configuração do Servidor DHCP
Agora que você está conectado à interface do roteador, siga os passos para configurar o servidor DHCP: 1. Acesse a aba "IP" no menu lateral esquerdo e clique em "DHCP Server". 2. Na janela "DHCP Setup", selecione a interface onde o DHCP será executado (por exemplo, a interface Ethernet onde os computadores estão conectados). 3. Clique em "Next" e defina o "Pool Name" (por exemplo, "pool1"). 4. Na opção "Address Range", defina o intervalo de endereços IP que o DHCP irá atribuir aos dispositivos conectados. Por exemplo, você pode usar a faixa de 192.168.1.100 a 192.168.1.200.

5. Defina o "Gateway" como o endereço IP do próprio roteador MikroTik (por exemplo, 192.168.1.1).
6. Na opção "DNS Servers", insira os endereços IP dos servidores DNS que você deseja que os computadores utilizem (por exemplo, os servidores DNS do provedor de internet).
7. Clique em "Next" e configure o "Lease Time", que é o tempo que os dispositivos mantêm o endereço IP atribuído pelo DHCP (por exemplo, 1d para um dia).
8. Clique em "Next" e verifique as configurações na última janela.
9. Por fim, clique em "Finish" para aplicar as configurações do servidor DHCP.

Passo 7: Verificação da Configuração

Após a configuração, os quatro computadores conectados à rede devem receber automaticamente endereços IP dentro do intervalo configurado pelo servidor DHCP. Você pode verificar os endereços IP atribuídos aos computadores através do comando "ipconfig" no prompt de comando do Windows ou usando ferramentas de diagnóstico de rede em outros sistemas operacionais. Com a configuração do servidor DHCP no MikroTik, a empresa terá uma gestão mais eficiente de endereços IP, evitando conflitos e facilitando a adição de novos dispositivos à rede.

Fonte: Kurina (2020), Marcillo e Benites (2019), Rahman, Sumarna e Nurdin (2020), Ribeiro (2016), Silva (2017). (Adaptado).

O Quadro 1 apresenta uma síntese em forma de protótipo de aplicação para a interface do roteador Mikrotik.

Quadro 3 – Protótipo para aplicação no Mikrotik - Servidor DHCP

1. Acesse o MikroTik através do Winbox ou de um navegador web.
2. Vá para o menu "IP" e selecione "DHCP Server".
3. Clique em "+ Add" para adicionar um novo servidor DHCP.
4. Defina uma interface de rede na qual o servidor DHCP será executado.
5. Especifique o intervalo de endereços IP que será fornecido aos clientes.
6. Configure as opções adicionais, como gateway padrão, DNS e tempo de concessão.
7. Salve as configurações e inicie o servidor DHCP

Fonte: Kurina (2020), Marcillo e Benites (2019), Rahman, Sumarna e Nurdin (2020), Ribeiro (2016), Silva (2017). (Adaptado).

Assim, a configuração do servidor DHCP em um roteador MikroTik é uma etapa fundamental para criar uma rede funcional e eficiente. Através do DHCP, os dispositivos conectados à rede podem obter automaticamente endereços IP e outras configurações de rede, tornando o processo de conexão e configuração mais simples e automatizado.

A partir dos estudos abordados tornou-se evidente a importância do servidor DHCP no roteador MikroTik para o estabelecimento de redes funcionais e seguras. Rahman, Sumarna e Nurdin (2020),forneceram insights valiosos sobre o desempenho do DHCP no RouterOS MikroTik, permitindo a otimização do serviço para uma experiência de conectividade mais eficiente. Marcillo e Benites (2019) e Kurina (2020), destacaram a relevância do servidor DHCP como uma medida essencial para mitigar ameaças de ataques internos e exploração de vulnerabilidades do Cliente DHCP. Silva (2017) e Ribeiro (2016), Silva trouxeram abordagens práticas para a gestão do pool de endereços IP e concessão de IPs em redes MikroTik, facilitando a administração e garantindo a segurança da infraestrutura de rede. Em conjunto, esses estudos reforçam a importância do DHCP para uma gestão eficiente, segura e confiável das redes em empresas de pequeno e médio porte, possibilitando uma conectividade sólida e protegida para usuários e administradores.

2.2 Configuração de firewall básico, bloqueio de conteúdo, porta e liberação em um MikroTik

A configuração de firewall básico em um roteador MikroTik é uma parte essencial da administração de rede para garantir a segurança e o controle de tráfego na rede. Adiante é feito um detalhamento dos conceitos mais relevantes para essa pesquisa.

2.2.1 Firewall MikroTik

Levy (2020), conceitua o firewall como um componente crucial que controla o tráfego de rede entre diferentes interfaces e ajuda a proteger a rede contra ameaças externas, bem como a controlar o acesso a recursos internos. O Firewall MikroTik oferece diversas funcionalidades que contribuem para a segurança da rede nessas empresas. Ele permite a criação de regras de filtragem e inspeção de pacotes, controlando o tráfego entre diferentes interfaces. Isso ajuda a proteger a rede contra ameaças externas, como ataques DDoS e tentativas de invasão.

Levy (2020), explica que o firewall Mikrotik possibilita o controle de acesso granular, permitindo a definição de políticas de acesso personalizadas para diferentes grupos de usuários. Essa capacidade de controle contribui para restringir o acesso a recursos internos e proteger informações sensíveis da empresa. A integração do firewall MikroTik com a funcionalidade Hotspot do RouterOS é destacada pelo, permitindo que pequenas e médias empresas gerenciem redes públicas com autenticação e controle de banda para os usuários.

Levy (2020), entende que para atender às necessidades de controle e segurança, o firewall Mikrotik oferece diversas funcionalidades, como regras de filtragem e inspeção de pacotes. Isso ajuda a proteger a rede contra ameaças externas, como invasões e ataques DDoS.

Portando, verifica-se que o firewall MikroTik é uma solução importante para garantir a segurança e o controle de acesso em redes de pequenas e médias empresa. Através de suas configurações avançadas, o firewall MikroTik contribui para proteger a rede contra ameaças e permitir um gerenciamento eficiente da conectividade.

2.2.2 Chain, input, forward, output e packet filtering

No MikroTik, o firewall é configurado em diferentes "chains" (cadeias), que são sequências específicas pelas quais o tráfego passa. As principais cadeias de firewall são "input" (entrada), "forward" (encaminhamento) e "output" (saída).

Ari Muzakir (2022), aborda a importância dos sistemas de segurança em redes de computadores, especialmente no contexto da Internet, onde a abertura do acesso representa um desafio para garantir a segurança dos usuários conectados. Para tal, é necessária a implementação de um firewall que possa proteger a rede contra ameaças internas e externas.

Ari Muzakir (2022), compreende o firewall como um componente crucial para garantir a segurança de uma rede e é definido como um conceito dentro do sistema operacional. No caso do Mikrotik RouterOS, o firewall desempenha um papel essencial na proteção da rede, permitindo controlar o fluxo de pacotes de dados que entram e saem da rede.

Ari Muzakir (2022), enfatiza conceitos relacionados ao firewall Mikrotik:

Chain no Mikrotik RouterOS, o conceito de "Chain" é fundamental para especificar em qual etapa do processamento de pacotes o firewall deve atuar. Existem várias chains, como "Input", "Forward" e "Output", que correspondem às diferentes fases do processamento de pacotes na rede.

Input Chain no Mikrotik RouterOS, a chain "Input" é responsável por processar pacotes que têm como destino o próprio dispositivo, ou seja, pacotes que se destinam ao próprio Mikrotik RouterOS. O firewall atua nessa chain para aplicar regras de filtragem e controle de acesso para o tráfego que chega ao dispositivo.

Forward Chain no Mikrotik RouterOS, a chain "Forward" é responsável por processar pacotes que serão encaminhados entre interfaces da rede, ou seja, pacotes que não têm como destino o próprio dispositivo. O firewall atua nessa chain para controlar o encaminhamento dos pacotes entre diferentes partes da rede.

Output Chain no Mikrotik RouterOS, a chain "Output" é responsável por processar pacotes que serão enviados pelo próprio dispositivo, ou seja, pacotes gerados pelo próprio MikroTik RouterOS. O firewall pode ser configurado para aplicar regras de filtragem e controle de acesso nessa chain também.

Packet Filtering no Mikrotik RouterOS, é uma ação realizada por um dispositivo ou software que estritamente controla o encaminhamento de pacotes que contêm

informações obtidas de uma rede. Nesse contexto, o firewall do Mikrotik é responsável por realizar o packet filtering, o que permite controlar o tráfego de dados que entra e sai da rede.

Visando a fixação desses conceitos o Quadro contém um resumo com as principais características de cada conceito abordado por Ari Muzakir (2022).

Quadro 4 – Característica dos conceitos abordados por Ari Muzakir (2022)

1. Firewall MikroTik RouterOS
    - Input Chain
        - Processa pacotes destinados ao dispositivo
        - Filtragem e controle de acesso para tráfego que chega ao dispositivo
    - Forward Chain
        - Processa pacotes encaminhados entre interfaces da rede
        - Controle do encaminhamento dos pacotes.
    - Output Chain
        - Processa pacotes enviados pelo próprio dispositivo
        - Filtragem e controle de acesso no tráfego de saída
2. Packet Filtering
    - Controle estrito do encaminhamento de pacotes
    - Análise de conteúdo dos pacotes
    - Aplicação de regras de filtragem
    - Baseado em endereços IP, portas, protocolos, etc.
3. MikroTik RouterOS
    - Sistema operacional de roteador e firewall

Fonte: Ari Muzakir (2022). (Adaptado)

Portando, Ari Muzakir (2022), colabora no entendimento geral das principais características do firewall Mikrotik RouterOS, destacando sua importância como uma ferramenta de segurança essencial para redes de computadores e a aplicação do "Packet Filtering" para controlar o fluxo de pacotes de dados na rede. O conhecimento desses conceitos é fundamental para o gerenciamento adequado e seguro de uma rede utilizando o Mikrotik RouterOS.

2.2.3 Regras de firewall

As regras de firewall são configurações específicas aplicadas às cadeias de firewall. Cada regra contém critérios de correspondência (como endereços IP de origem ou destino, portas, protocolos, etc.) e ações a serem tomadas (aceitar, rejeitar, encaminhar, etc.) com base nos critérios.

A empresa Entelco Telecom (2018), apresenta informações sobre o firewall Mikrotik e destaca o processo de criação de regras para garantir a proteção e segurança da rede. Algumas das principais características do Firewall MikroTik são:

O Firewall MikroTik tem como objetivo aplicar uma política de segurança em uma rede TCP/IP. Ele regula o tráfego de dados entre redes distintas e impede a transmissão e/ou recepção de acessos nocivos ou não autorizados, (ENTELCO TELECOM (2018).

As regras de Firewall MikroTik são processadas por cadeia, listadas de cima para baixo. Se um pacote não atende todas as condições de uma regra, ele passa para a próxima regra, (ENTELCO TELECOM (2018).

Existem algumas exceções ao processamento sequencial das regras, como as ações de "passthrougth" (passar adiante), log e add to address list. Um pacote que não se enquadra em nenhuma regra da cadeia será, por padrão, aceito, (ENTELCO TELECOM (2018).

Entelco Telecom (2018), também apresenta exemplos de regras de Firewall MikroTik para diferentes cenários, como bloqueio de acesso FTP por força bruta, configuração de uma cadeia TCP e negação de algumas portas TCP.

Quadro 5 – Regra para bloquear tentativas de força bruta no serviço FTP

```
/Ip firewall filter
add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blocked-list action=drop comment=” Descarta força bruta FTP”
add chain=output action=accept protocol=tcp content=”530 Login incorreto” dst-limit=1/1m,9, dst-address 1m
add chain=output action=add-dst-to-address-list protocol=tcp content=”530 Login incorreto” address-list=ftp_blacklist address-list-timeout=3h
```

Fonte: Entelco Telecom (2018).

Nesse exemplo, a regra de firewall tem como objetivo bloquear tentativas de força bruta no serviço FTP. Quando um endereço IP faz 10 tentativas de login incorreto em um intervalo de 1 minuto, o firewall adiciona o endereço IP à lista de bloqueio ("ftp_blacklist") e bloqueia futuras tentativas de acesso ao serviço FTP por esse endereço IP por 3 horas.

Quadro 6 – Configurando uma cadeia TCP e Negação de algumas portas TCP

```
/Ip firewall filter
add chain=tcp protocol=tcp dst-port=69 action=drop comment=” Negar TFTP”
add chain=tcp protocol=tcp dst-port=111 action=drop comment=” Negar RPC portmapper”
add chain=tcp protocol=tcp dst-port=135 action=drop comment=” Negar RPC portmapper”
add chain=tcp protocol=tcp dst-port=137-139 action=drop comment=” Negar NBT”
add chain=tcp protocol=tcp dst-port=445 action=drop comment=” Negar cifs”
add chain=tcp protocol=tcp dst-port=2049 action=drop comment=” Negar NFS”
add chain=tcp protocol=tcp dst-port=12345-12346 action=drop comment=” Negar NetBus”
add chain=tcp protocol=tcp dst-port=20034 action=drop comment=” Negar NetBus”
add chain=tcp protocol=tcp dst-port=3133 action=drop comment=” Negar BackOriffice”
add chain=tcp protocol=tcp dst-port=67-68 action=drop comment=” Negar DHCP”
```

Fonte: Entelco Telecom (2018).

Nesse exemplo, uma cadeia de regras TCP é criada para negar o tráfego em determinadas portas TCP. Cada regra corresponde a uma porta específica e utiliza a ação "drop" para negar o tráfego que chega a essas portas. Por exemplo, as regras "Negar TFTP", "Negar RPC portmapper", "Negar NBT", entre outras, bloqueiam o tráfego nas portas associadas a esses serviços conhecidos por apresentarem vulnerabilidades ou riscos de segurança. Essas regras exemplificam como o Firewall MikroTik pode ser configurado para fornecer um controle mais preciso sobre o tráfego de rede e garantir a segurança da rede TCP/IP ao negar acessos indesejados ou perigosos.

O Quadro 7 apresenta uma breve orientação do processo de criação de regras de firewall no Mikrotik para assimilação.

Quadro 7 – Processo de criação de regras de firewall no Mikrotik

O processo de criação de regras de firewall no MikroTik RouterOS envolve alguns passos essenciais. Aqui está um guia básico para criar regras de firewall no MikroTik: **Acesse o MikroTik RouterOS:** Conecte-se ao roteador MikroTik usando o Winbox (aplicativo de gerenciamento gráfico) ou o acesso via terminal (SSH ou Telnet). **Acesse o menu "IP" e selecione "Firewall" no painel esquerdo:** No menu principal do MikroTik, vá para "IP" e, em seguida, clique em "Firewall". **Selecione a chain adequada:** O MikroTik possui várias chains de firewall, como "Input", "Forward" e "Output". Escolha a chain apropriada com base na direção do tráfego que você deseja controlar. Por exemplo, se você deseja controlar o tráfego que entra no roteador, selecione a chain "Input". **Crie uma regra de firewall:** Clique em "Add New" ou "Add" para criar uma regra de firewall na chain selecionada. **Configure os parâmetros da regra:** Na janela de configuração da regra de firewall, você definirá os parâmetros da regra, como "Src. Address" (endereço de origem), "Dst. Address" (endereço de destino), "Protocol" (protocolo), "Action" (ação) e outras opções relacionadas à filtragem de pacotes. **Defina a ação da regra:** Escolha a ação que deseja aplicar aos pacotes que correspondem à regra. As ações típicas são "Accept" (aceitar), "Drop" (descartar) ou "Reject" (rejeitar). "Accept" permite que os pacotes passem, "Drop" descarta os pacotes silenciosamente e "Reject" descarta os pacotes, mas envia uma mensagem ICMP ao remetente indicando o descarte. **Ajuste a ordem das regras (opcional):** Você pode definir a ordem das regras de firewall para garantir que as regras mais específicas sejam aplicadas antes das mais genéricas. Para ajustar a ordem, use os botões "Move Up" ou "Move Down". **Aplique a regra de firewall:** Clique em "OK" ou "Apply" para aplicar a regra de firewall ao MikroTik RouterOS.

Fonte: Entelco Telecom (2018).

Verifica-se que o firewall MikroTik é uma ferramenta eficiente para a aplicação de políticas de segurança em redes TCP/IP, oferecendo controle e proteção adequados para garantir a integridade e confiabilidade das comunicações em um ambiente conectado à Internet. Com o devido planejamento e configuração de regras, os administradores de rede podem garantir um alto nível de segurança em suas redes e proteger seus sistemas e dados contra potenciais riscos.

2.2.4 Bloqueio de conteúdo

Zibeti (2015), apresenta conceitos relacionados ao roteador Mikrotik e aborda o "Bloqueio de conteúdo" como uma prática para impedir que determinados tipos de tráfego ou conteúdo específico acessem a rede ou sejam transmitidos através dela, incluindo bloqueio de sites, protocolos ou certos tipos de arquivos. Dialoga-se sobre os conceitos apresentados e como eles se aplicam ao roteador Mikrotik, implicando em uma análise de cada parte para fornecer informações mais detalhadas.

2.2.5 Portas

Zibeti (2015), discorre que as portas são canais virtuais através dos quais os dados são enviados e recebidos em um dispositivo de rede. As portas são associadas a protocolos específicos e são identificadas por números. Por exemplo, a porta 80 é comumente usada para tráfego HTTP.

No contexto dos roteadores MikroTik, as portas desempenham um papel fundamental no encaminhamento eficiente de dados entre redes ou dispositivos conectados. As portas podem ser comparadas a canais virtuais por meio dos quais os dados entram e saem de um dispositivo de rede. Cada porta está associada a um protocolo específico e é identificada por um número único, permitindo que o roteador direcione o tráfego corretamente.

Em um roteador MikroTik, é possível configurar regras de redirecionamento de portas para permitir que determinados serviços sejam acessíveis a partir da Internet ou de outras redes. Por exemplo, se um servidor web estiver sendo executado em uma rede local protegida por um roteador MikroTik, é necessário redirecionar a porta 80 (tráfego HTTP) do roteador para o endereço IP local do servidor na rede interna. Isso permitirá que os usuários acessem o site hospedado no servidor através da interface WAN (Wide Area Network) do roteador MikroTik.

A configuração das portas no roteador MikroTik é realizada através do utilitário de firewall. Para ilustrar esse processo, vamos considerar o exemplo de como abrir a porta 22 para possibilitar o acesso SSH a um dispositivo de rede a partir da Internet.

O Quadro 8 explica os passos para realizar essa configuração:

Quadro 8 – Configurando a permissão para acesso SSH através da porta 22

O processo de criação de regras de firewall no MikroTik RouterOS envolve alguns passos essenciais. Aqui está um guia básico para criar regras de firewall no MikroTik:

Passo 1: Acesse o painel de controle do MikroTik através do navegador web.

Passo 2: Vá para o menu "IP" e selecione "Firewall" para acessar as opções de configuração do firewall.

Passo 3: Na guia "Portas", clique em "Adicionar nova regra" ("Add new rule") e preencha os campos necessários, como:

Chain: deve ser "input";

Protocolo: selecione "TCP";

DST Port: insira o número da porta que deseja abrir, por exemplo, 22 para SSH;

Ação (Action): defina como "aceitar" ("accept");

Informações adicionais: você pode adicionar uma descrição para a regra, como "Permitir acesso SSH".

Passo 4: Clique em "OK" para salvar a regra.

Agora o roteador MikroTik está configurado para permitir o acesso SSH através da porta 22. Esse processo pode ser adaptado para outras portas e serviços, conforme necessário.

Fonte: Zibeti (2015).

Portanto, o correto gerenciamento das portas é essencial para garantir a segurança da rede. Abrir indiscriminadamente portas sem a devida configuração de firewall pode expor serviços indesejados ou até mesmo permitir acesso não autorizado a dispositivos internos. É recomendável que apenas as portas necessárias para os serviços que se deseja disponibilizar sejam abertas, e todas as outras portas permaneçam fechadas para evitar potenciais riscos de segurança.

2.2.6 Bloqueio de porta

Zibeti (2015), enfatiza que o bloqueio de portas pode ser usado para impedir que determinados serviços ou protocolos específicos sejam acessados a partir de ou para a rede. Isso ajuda a proteger a rede contra tráfego indesejado ou potencialmente malicioso. Nem todos os serviços ou protocolos precisam estar acessíveis o tempo todo, e é aí que o bloqueio de portas desempenha um papel crucial. Ao bloquear portas específicas, evitar-se que determinados tipos de tráfego indesejado entrem ou saiam da sua rede, reduzindo assim possíveis vulnerabilidades e protegendo os dispositivos contra atividades maliciosas.

A configuração de bloqueio de portas geralmente é realizada através da criação de regras de firewall. O firewall atua como uma barreira de segurança entre a rede interna e externa, permitindo ou negando o tráfego com base em regras pré-definidas. O Quadro 9 apresenta um exemplo prático de como bloquear a porta 23, que é comumente utilizada pelo protocolo Telnet, um serviço desatualizado e inseguro, utilizando o firewall do MikroTik.

Quadro 9 – Bloqueio da porta 23

1. Primeiro, é necessário acessar a interface do MikroTik, geralmente através do navegador, inserindo o endereço IP do roteador na barra de endereços.

2. Em seguida, autentique-se com as credenciais de administrador para acessar o painel de controle.

3. No painel de controle, procure e clique na opção "Firewall" ou "IP Firewall".

4. Agora, clique na aba "Filter Rules" ou "Regras de Filtro" e selecione "Add New" ou "Adicionar Nova" para criar uma regra de firewall.

5. Na nova regra, defina as seguintes configurações:
   Chain: Escolha se a regra se aplicará ao tráfego de entrada (input), saída (output) ou encaminhamento (forward).
   Protocol: Selecione o protocolo que deseja bloquear (TCP, UDP, etc.).
   Port: Digite o número da porta que deseja bloquear (neste caso, 23 para Telnet).
   Action: Escolha a ação a ser tomada quando o tráfego corresponder a essa regra. Para bloquear, selecione "Drop" ou "Reject".

6. Após configurar as opções acima, clique em "OK" ou "Apply" para salvar a regra de bloqueio de porta.
   A partir deste momento, o MikroTik bloqueará qualquer tráfego que tente utilizar a porta 23, o que significa que tentativas de acesso via Telnet serão impedidas. Essa ação contribui significativamente para a segurança da rede, uma vez que Telnet é um protocolo desatualizado e inseguro, e bloqueá-lo reduzirá a superfície de ataque da rede contra potenciais invasores.

Fonte: Zibeti (2015).

Verifica-se que a configuração do firewall e o bloqueio de portas devem ser feitos com cuidado e planejamento, pois bloquear portas inadequadamente pode afetar o funcionamento legítimo de serviços e aplicativos na rede, ter backups de configuração é essencial.

2.2.7 Liberação de porta

A liberação de porta refere-se à abertura de portas específicas para permitir que determinados serviços ou protocolos sejam acessados a partir de ou para a rede. É necessário liberar portas para permitir o funcionamento adequado de aplicativos e serviços específicos.

A configuração da liberação de portas é realizada através da criação de regras de firewall que permitem explicitamente o tráfego através das portas específicas que precisam ser liberadas. Dessa forma, apenas as portas selecionadas ficam abertas para comunicação, enquanto as demais permanecem bloqueadas por padrão, aumentando a segurança da rede, pois reduz a exposição a possíveis ataques maliciosos.

A seguir, apresenta-se um exemplo prático de como liberar a porta 3389, que é comumente utilizada pelo protocolo RDP (Remote Desktop Protocol), permitindo que você acesse remotamente um computador da rede através da Área de Trabalho Remota. Para isso, configura-se uma regra de firewall no MikroTik para liberar a porta 3389:

Quadro 10 – Liberação da porta 3389

1. Acesse a interface do MikroTik por meio de um navegador da web, inserindo o endereço IP do roteador na barra de endereços e faça o login usando as credenciais de administrador.
2. No painel de controle, procure e clique na opção "Firewall" ou "IP Firewall".
3. Em seguida, clique na aba "Filter Rules" ou "Regras de Filtro" e selecione "Add New" ou "Adicionar Nova" para criar uma regra de firewall.
4. Agora, configure as seguintes opções na nova regra:
   Chain: Escolha a opção "input" se desejar permitir o tráfego de entrada na porta ou "forward" para permitir o tráfego de passagem pela porta.
   Protocol: Selecione o protocolo que deseja liberar (normalmente TCP ou UDP).
   Port: Digite o número da porta que deseja liberar (neste caso, 3389 para o RDP).
   Action: Escolha a ação "Accept" para permitir o tráfego que corresponda a essa regra.
5. Após configurar as opções acima, clique em "OK" ou "Apply" para salvar a regra de liberação da porta.

A partir de agora, a porta 3389 estará liberada no seu roteador MikroTik, permitindo que você acesse remotamente um computador na rede através do RDP.

Fonte: ZIbeti (2015).

Assim, realizar a liberação de portas com cautela e somente para serviços ou aplicativos realmente necessários. Deixar portas desnecessárias abertas pode aumentar o risco de ataques cibernéticos. Sempre mantenha a configuração de firewall atualizada e considere implementar outras medidas de segurança.

2.2.8 Network Address Translation (NAT)

Zibeti (2015), explica que o Network Address Translation (NAT) é uma técnica utilizada em roteadores MikroTik e em outros dispositivos de rede para permitir que vários dispositivos na rede local compartilhem um único endereço IP público para se comunicarem com a internet. Nesse contexto, o NAT age como um intermediário entre a rede local (LAN) e a rede externa (Internet), traduzindo os endereços IP internos em endereços IP públicos e vice-versa.

O funcionamento do NAT é simples. Quando um dispositivo da rede local solicita acesso à Internet, o roteador Mikrotik atribui um endereço IP público para esse dispositivo, permitindo a comunicação com a internet. Quando os dados de resposta da Internet retornam, o roteador utiliza a tabela de tradução NAT para identificar o dispositivo da rede local ao qual a resposta deve ser enviada. Dessa forma, vários dispositivos internos podem usar o mesmo endereço IP público para acessar a internet, economizando endereços IP públicos e facilitando a conexão de múltiplos dispositivos em uma única rede.

Suponha uma pequena empresa que possui uma rede local com vários dispositivos, como computadores, smartphones e impressoras, todos conectados a um roteador MikroTik. A empresa possui um único endereço IP público fornecido pelo provedor de Internet.

Sem o NAT, apenas um dos dispositivos da empresa poderia acessar a internet de cada vez, pois há apenas um endereço IP público disponível. No entanto, com o NAT habilitado no roteador Mikrotik, todos os dispositivos da rede local podem compartilhar esse mesmo endereço IP público para acessar a internet.

Por exemplo, quando um dos computadores da empresa deseja acessar um site na internet, o roteador Mikrotik atribui temporariamente o endereço IP público a esse computador e cria uma entrada na tabela de tradução NAT. Essa entrada permite que as respostas do site da internet retornem ao computador correto da rede local. Ao mesmo tempo, outros dispositivos da rede local podem acessar diferentes sites na

internet, e o roteador Mikrotik gerencia a tradução dos endereços IP de forma dinâmica para garantir que todos os dispositivos funcionem corretamente.

Portanto, o NAT em roteadores Mikrotik é uma solução eficiente para compartilhar um único endereço IP público entre vários dispositivos da rede local, permitindo que a empresa se conecte à internet de maneira eficaz e econômica. Além disso, essa técnica de tradução de endereços é amplamente utilizada em roteadores e firewalls para melhorar a segurança da rede interna, ocultando os endereços IP internos dos dispositivos da Internet.

2.2.9 Mangle

Oliveira Júnior (2022), explana que o mangle é uma funcionalidade essencial do firewall do Mikrotik que permite manipular os pacotes de dados em nível de roteamento. Essa funcionalidade é amplamente utilizada para diversas finalidades, como marcar pacotes, alterar a rota de pacotes específicos ou aplicar políticas específicas a pacotes de dados.

Quando os pacotes de dados chegam ao roteador Mikrotik, eles passam por uma série de regras de firewall, incluindo as regras de mangle, antes de serem encaminhados para o destino. As regras de mangle permitem que os administradores de rede tomem decisões específicas sobre como os pacotes devem ser tratados com base em critérios específicos.

Oliveira Júnior (2022), faz um apontamento das principais Aplicações do Mangle:

É possível marcar pacotes específicos com rótulos que serão usados posteriormente para aplicar políticas de QoS (Qualidade de Serviço), como priorização ou limitação de banda, (OLIVEIRA JÚNIOR, 2022).

As regras de mangle podem ser usadas para alterar a rota padrão de pacotes com base em critérios específicos, como endereço IP de origem ou destino, interface de entrada, etc., (OLIVEIRA JÚNIOR, 2022).

É possível utilizar o mangle para distribuir o tráfego de saída entre várias rotas, proporcionando balanceamento de carga e redundância, (OLIVEIRA JÚNIOR, 2022).

O mangle pode ser usado para limitar a banda de upload ou download de determinados clientes ou serviços, garantindo uma distribuição justa dos recursos de rede, (OLIVEIRA JÚNIOR, 2022).

O mangle permite definir prioridades para diferentes tipos de tráfego, garantindo que aplicações críticas tenham maior largura de banda disponível, (OLIVEIRA JÚNIOR, 2022).

Suponha que um administrador de uma rede precisa priorizar o tráfego VoIP para garantir uma comunicação de voz mais estável e livre de atrasos. Nesse cenário, pode ser feita a utilização do mangle para marcar pacotes VoIP específicos e, em seguida, aplicar políticas de QoS para garantir a priorização adequada. O processo de criação é expresso no Quadro 11.

Quadro 11 – Criando a Regra Mangle

1. **Criando a Regra de Mangle**
   Você criaria uma regra de mangle para marcar os pacotes VoIP com um rótulo especial. Isso pode ser feito com base na porta de origem ou destino, que é comumente usada para identificar o tráfego VoIP. Por exemplo:
   /Ip firewall mangle
   add action=mark-packet chain=prerouting port=5060,5061 new-packet-mark=voip
2. **Configurando Políticas de QoS**
   Em seguida, você configuraria políticas de QoS usando a marcação de pacotes "voip" para priorizar esse tráfego. Isso pode envolver a definição de limites de banda ou garantias de largura de banda específicas para o tráfego VoIP em relação a outros tipos de tráfego.
   /Queue tree
   add name=voip parent=global-out packet-mark=voip limit-at=1M max-limit=2M
   Neste exemplo, os pacotes VoIP seriam marcados com o rótulo "voip" e, em seguida, tratados pelas políticas de QoS definidas na árvore de filas.

Fonte: Oliveira Júnior (2022). Adaptado

Em suma, o mangle é uma poderosa ferramenta disponível no Mikrotik para manipular pacotes em nível de roteamento. Suas diversas aplicações permitem que administradores de rede otimizem e personalizem o tráfego de acordo com suas necessidades específicas, garantindo um melhor desempenho e controle da rede.

Ao configurar o firewall básico em um Mikrotik, é importante definir regras cuidadosamente para permitir apenas o tráfego necessário e bloquear ou restringir o acesso a conteúdo ou serviços não autorizados. Isso ajuda a proteger a rede contra ameaças externas, garantir o bom funcionamento dos serviços internos e manter um ambiente de rede seguro e confiável. O conhecimento dos conceitos acima é

fundamental para realizar uma configuração de firewall eficaz e personalizada de acordo com as necessidades específicas da rede e dos usuários. Além disso, é importante revisar regularmente as configurações de firewall para garantir que estejam atualizadas e em conformidade com as políticas de segurança da rede.

2.3 Configuração de QoS (Quality of Service) para limitar a banda por IP em um MikroTik

A configuração de QoS (Quality of Service) em um roteador MikroTik é uma técnica importante para gerenciar o uso da largura de banda e priorizar o tráfego na rede, garantindo uma melhor experiência para os usuários e aplicações críticas.

2.3.1 Quality of Service (QoS)

O QoS é uma técnica usada para priorizar e gerenciar o tráfego de rede com base em suas características e requisitos de desempenho. Ele é usado para garantir que aplicações e serviços importantes tenham prioridade sobre o tráfego menos crítico, melhorando a qualidade e a consistência da experiência do usuário.

Bolano e Lapez (2008), implementam cinco práticas de laboratório para configurar a qualidade de serviço (QoS) em uma rede específica, utilizando informações das camadas 3 e 4 (endereço IP, porta, protocolo, etc.) aplicadas aos links de menor velocidade e enlaces WAN, as práticas são (Configuração do MikroTik RouterOS; Controle de largura de banda por meio de marcação de pacotes por endereço IP; Controle de largura de banda por diferenciação de serviços; Divisão equitativa de largura de banda entre um número específico de usuários em uma rede IP; Balanceamento de carga por tipo de tráfego). As contribuições desses autores são importante para entendimentos de alguns conceitos específicos de QoS.

2.3.2 Banda

A largura de banda é a quantidade máxima de dados que podem ser transmitidos através de uma conexão de rede em um determinado período, geralmente medido em bits por segundo (bps) ou megabits por segundo (Mbps).

No contexto de "Configuração de QoS (Quality of Service) para Limitar a Banda por IP em um MikroTik", a banda refere-se à capacidade de transmissão de dados de uma rede. A implementação do Quality of Service (QoS) em uma rede é essencial para priorizar determinados tipos de tráfego, garantindo que os serviços em tempo real, como voz IP, videoconferência e streaming de vídeo, recebam uma largura de banda adequada para funcionar sem interrupções.

Bolano e Lapez (2008), abordam o controle de largura de banda através do marcado de pacotes por Endereço IP, são implementados scripts para marcar pacotes com base nos endereços IP dos dispositivos. Ainda, são criadas filas para controlar a largura de banda de cada grupo ou categoria, priorizando o tráfego de acordo com as necessidades.

Bolano e Lapez (2008), fazem o controle de banda por diferenciação de Serviços de forma prática, o controle de largura de banda é realizado com base na diferenciação de três tipos de serviços: HTTP, P2P e outros. Scripts são implementados para marcar os pacotes de acordo com o serviço e definir filas para limitar a largura de banda de upload e download para cada tipo de tráfego.

Bolano e Lapez (2008), efetuam a divisão equitativa de largura de banda entre usuários, o compartilhamento da largura de banda de forma equitativa entre um número específico de usuários na rede. O router é configurado para implementar esse controle, utilizando filas diferentes para upload e download e definindo velocidades limites para cada usuário.

Bolano e Lapez (2008), realizam o balanceamento de carga por tipo de Tráfego na prática, configura-se o router para realizar o balanceamento de carga entre dois canais de saída para a internet, com base no tipo de tráfego. Isso permite otimizar o fluxo de pacotes, utilizando vantagens específicas de cada canal.

Através das práticas de Bolano e Lapez (2008), foi possível verificar a eficiência das técnicas de QoS em redes IP, avaliando o consumo de largura de banda, a transmissão em tempo real e o envio/recebimento de pacotes. A implementação de QoS é essencial para garantir um acesso mais flexível e eficiente aos recursos e informações em tempo real, priorizando os serviços que requerem uma largura de banda adequada para funcionar corretamente. Verificou-se as vantagens de uma rede com QoS em comparação com uma rede sem gestão de qualidade de serviço. Embora a configuração de QoS possa envolver complexidade e requisitos adicionais de equipamentos, seus benefícios em relação ao controle do tráfego e à priorização de serviços em tempo real tornam-se fundamentais para redes que oferecem serviços sensíveis à largura de banda.

Adiante, para praticar apresenta-se alguns exemplos com adaptação dos conceitos trazidos por Bolano e Lapez (2008).

Quadro 12 – Controle de largura de banda através do marcador de pacotes por endereço ip

Neste exemplo, vamos criar um controle de largura de banda para um grupo específico de dispositivos com base nos endereços IP.

1) **Acesse o MikroTik RouterOS através do WinBox ou outras formas de acesso.**
2) **Na aba "IP" do menu lateral, clique em "Firewall" e depois em "Mangle".**
3) **Clique em "Add New" para criar uma regra de mangle.**
4) **Defina a cadeia como "forward" (encaminhamento) e o protocolo como "tcp" ou "udp", dependendo do tipo de tráfego que deseja controlar.**
5) **Em "Action", escolha "Mark Packet" e, em "New Packet Mark", coloque um nome para identificar o tráfego que será controlado (por exemplo, "trf_grupo1").**
6) **Em "Src. Address", insira o endereço IP ou o intervalo de IPs do grupo específico de dispositivos que deseja controlar.**
7) **Clique em "OK" para aplicar a regra de mangle.**
8) **Na aba "Queue" do menu lateral, clique em "Simple Queue".**
9) **Clique em "Add New" para criar uma fila de controle de largura de banda.**
10) **Defina o nome da fila, por exemplo, "fila_grupo1".**
11) **Em "Target", selecione "Global" para controlar o tráfego de upload e download.**
12) **Em "Packet Mark", escolha o nome que você atribuiu à regra de mangle ("trf_grupo1").**
13) **Em "Max Limit", defina a largura de banda máxima que você deseja atribuir a esse grupo de dispositivos (por exemplo, 1M/1M para 1 Mbps de upload e download).**
14) **Clique em "OK" para aplicar a fila de controle de largura de banda.**

Agora, o tráfego proveniente do grupo de dispositivos com o endereço IP especificado será marcado e terá sua largura de banda controlada pela fila "fila_grupo1"..

Fonte: Bolano e Lapez (2008). Adaptado

Quadro 13 – Comtrole de Banda por Diferenciação de Serviços

Neste exemplo, vamos implementar um controle de largura de banda diferenciando três tipos de serviços: HTTP, P2P e outros.

1) **Acesse o MikroTik RouterOS através do WinBox ou outras formas de acesso.**
2) **Na aba "IP" do menu lateral, clique em "Firewall" e depois em "Layer7 Protocols".**
3) **Clique em "Add New" e crie padrões de protocolo Layer7 para identificar o tráfego HTTP e P2P. Por exemplo, use expressões**

regulares para identificar os padrões de tráfego associados a cada serviço.

4) **Na aba "IP" do menu lateral, clique em "Firewall" e depois em "Mangle".**
5) **Clique em "Add New" para criar uma regra de mangle.**
6) **Defina a cadeia como "forward" e o protocolo como "tcp".**
7) **Em "Action", escolha "Mark Packet" e, em "New Packet Mark", coloque um nome para identificar cada tipo de tráfego (por exemplo, "trf_http" para HTTP e "trf_p2p" para P2P).**
8) **Em "Layer7 Protocol", selecione o padrão de protocolo Layer7 correspondente ao tráfego (por exemplo, "HTTP" para tráfego HTTP).**
9) **Crie uma regra de mangle para identificar o tráfego P2P usando o padrão de protocolo Layer7 correspondente.**
10) **Repita os passos 5 a 9 para criar regras de mangle para os outros tipos de tráfego.**
11) **Na aba "Queue" do menu lateral, clique em "Simple Queue".**
12) **Clique em "Add New" para criar uma fila de controle de largura de banda.**
13) **Defina o nome da fila, por exemplo, "fila_http" para tráfego HTTP.**
14) **Em "Target", selecione "Global" para controlar o tráfego de upload e download.**
15) **Em "Packet Mark", escolha o nome que você atribuiu à regra de mangle correspondente a cada tipo de tráfego.**
16) **Em "Max Limit", defina a largura de banda máxima que você deseja atribuir a cada tipo de tráfego.**
17) **Clique em "OK" para aplicar a fila de controle de largura de banda.**

Agora, o tráfego HTTP, P2P e outros serão diferenciados e controlados em filas de largura de banda separadas.

Fonte: Bolano e Lapez (2008). Adaptado

Quadro 14 – Divisão Equitativa de Largura de Banda entre Usuários

Neste exemplo, vamos dividir equitativamente a largura de banda entre dois usuários na rede.

1) **Acesse o MikroTik RouterOS através do WinBox ou outras formas de acesso.**
2) **Na aba "Queue" do menu lateral, clique em "Simple Queue".**
3) **Clique em "Add New" para criar uma fila de controle de largura de banda.**
4) **Defina o nome da fila, por exemplo, "user1_queue" para o primeiro usuário.**
5) **Em "Target", selecione "Global" para controlar o tráfego de upload e download.**
6) **Em "Max Limit", defina a largura de banda máxima que você deseja atribuir a esse usuário (por exemplo, 2M/2M para 2 Mbps de upload e download).**

7) **Clique em "OK" para aplicar a fila de controle de largura de banda.**
8) **Crie uma fila de controle de largura de banda para o segundo usuário seguindo os mesmos passos.**

Agora, a largura de banda será compartilhada equitativamente entre os dois usuários através das filas "user1_queue" e "user2_queue".

Fonte: Bolano e Lapez (2008). Adaptado

Quadro 15 – Balanceamento de Carga por Tipo de Tráfego

Neste exemplo, vamos configurar o MikroTik RouterOS para realizar o balanceamento de carga entre dois canais de saída para a internet, com base no tipo de tráfego.

1) **Acesse o MikroTik RouterOS através do WinBox ou outras formas de acesso.**
2) **Na aba "IP" do menu lateral, clique em "Firewall" e depois em "Mangle".**
3) **Clique em "Add New" para criar uma regra de mangle.**
4) **Defina a cadeia como "prerouting" e o protocolo como "tcp".**
5) **Em "Action", escolha "Mark Routing" e, em "New Routing Mark", coloque um nome para identificar o tipo de tráfego (por exemplo, "trf_http" para HTTP e "trf_p2p" para P2P).**
6) **Em "Layer7 Protocol", selecione o padrão de protocolo Layer7 correspondente ao tráfego (por exemplo, "HTTP" para tráfego HTTP).**
7) **Crie uma regra de mangle para identificar o tráfego P2P usando o padrão de protocolo Layer7 correspondente.**
8) **Repita os passos 3 a 7 para criar regras de mangle para os outros tipos de tráfego.**
9) **Na aba "IP" do menu lateral, clique em "Routes".**
10) **Clique em "Add New" para criar uma nova rota de balanceamento de carga.**
11) **Em "Dst. Address", insira o endereço IP da saída para a internet que você deseja balancear.**
12) **Em "Gateway", selecione a interface de saída que você deseja usar para esse tipo de tráfego (por exemplo, "WAN1" ou "WAN2").**
13) **Em "Routing Mark", escolha o nome que você atribuiu à regra de mangle correspondente a cada tipo de tráfego.**
14) **Crie rotas para os outros tipos de tráfego, selecionando a interface de saída adequada para cada um.**

Com essas configurações, o MikroTik RouterOS realizará o balanceamento de carga entre os dois canais de saída para a internet, direcionando o tráfego com base no tipo de serviço identificado nas regras de mangle.

Observação: A implementação exata pode variar dependendo da versão do RouterOS e da topologia da rede.

Fonte: Bolano e Lapez (2008). Adaptado

Portanto, a configuração de QoS em um MikroTik é uma prática altamente benéfica para proporcionar uma experiência de rede mais eficiente, garantindo a qualidade dos serviços críticos e melhorando o desempenho geral da rede. Ao limitar a banda por IP e adotar diferenciação de serviços, os administradores podem garantir que os recursos de largura de banda sejam alocados de maneira justa e adequada, mantendo uma rede responsiva e confiável mesmo em situações de alto tráfego. Isso resulta em maior satisfação dos usuários, maior produtividade e melhor aproveitamento dos recursos de rede disponíveis. Portanto, investir na configuração de QoS em um MikroTik é uma estratégia inteligente para alcançar um ambiente de rede eficiente e com alta qualidade de serviço.

2.3.3 Limitação de Banda

A configuração de QoS (Quality of Service) no MikroTik é uma prática essencial para garantir um desempenho eficiente e justo da rede, especialmente em ambientes com múltiplos dispositivos e usuários compartilhando a mesma largura de banda. Dentre os diversos conceitos utilizados para implementar QoS no MikroTik, destacam-se a limitação de banda, filas de tráfego, marcadores de pacotes, hierarquia de filas, tree de filas, fila pai e fila filho.

A limitação de banda é uma prática que impõe um limite máximo na quantidade de largura de banda que um determinado dispositivo, IP ou grupo de IPs pode usar. Isso evita que determinados dispositivos ou usuários consumam toda a largura de banda disponível, garantindo uma distribuição equitativa da largura de banda entre os usuários, (BOLANO; LAPEZ, 2008).

A limitação de banda é uma estratégia valiosa para evitar que dispositivos ou usuários monopolizem toda a largura de banda disponível. Ao impor um limite máximo na quantidade de largura de banda que um determinado dispositivo ou grupo de IPs pode usar, a rede garante uma distribuição equitativa dos recursos, evitando gargalos e garantindo que todos os usuários tenham acesso razoável à largura de banda.

2.3.4 Filas de tráfego

No MikroTik, as filas de tráfego são usadas para controlar o fluxo de pacotes em diferentes interfaces de rede. É possível criar filas de saída para limitar a taxa de

transmissão de pacotes, aplicando regras de QoS específicas, (BOLANO; LAPEZ, 2008). Para controlar o fluxo de pacotes em diferentes interfaces de rede, o uso de filas de tráfego é imprescindível no MikroTik. Através das filas de saída, é possível limitar a taxa de transmissão de pacotes, aplicando regras específicas de QoS. Essas filas permitem priorizar o tráfego de acordo com as necessidades da rede, garantindo que aplicações críticas, como voz sobre IP, tenham prioridade em relação a atividades menos importantes, como downloads.

2.3.5 Marcadores de Pacotes

Os marcadores de pacotes são usados no MikroTik para identificar pacotes específicos com base em suas características, como endereço IP de origem ou destino, porta, tipo de serviço, etc. Eles são frequentemente usados para classificar o tráfego em categorias distintas para aplicar QoS, (BOLANO; LAPEZ, 2008). Os marcadores de pacotes são uma ferramenta poderosa no MikroTik, permitindo a identificação de pacotes com base em suas características, como endereço IP de origem ou destino, porta ou tipo de serviço. Essa classificação de tráfego em categorias distintas facilita a aplicação de regras de QoS específicas, tornando possível a priorização de certos tipos de tráfego.

2.3.6 Hierarquia de Filas

O MikroTik suporta a criação de hierarquias de filas, permitindo a configuração de prioridades de tráfego em diferentes níveis. Isso possibilita priorizar determinados tipos de tráfego, como VoIP ou videoconferência, em relação a outras atividades de menor prioridade, como navegação na web ou downloads, (BOLANO; LAPEZ, 2008). A hierarquia de filas é uma funcionalidade importante no MikroTik que permite configurar prioridades de tráfego em diferentes níveis. Com isso, é possível priorizar o tráfego crítico, garantindo a qualidade de serviços como videoconferência e telefonia IP, em relação a outras atividades menos sensíveis à latência.

2.3.7 Tree (árvore) de Filas

O conceito de árvore de filas é comumente usados no MikroTik para organizar as filas de tráfego em uma estrutura hierárquica. Isso permite o controle mais granular sobre a alocação de largura de banda para diferentes IPs ou grupos de IPs, (BOLANO; LAPEZ, 2008). A tree de filas é uma técnica comum para organizar as filas de tráfego em uma estrutura hierárquica. Isso oferece controle mais granular sobre a alocação de largura de banda para diferentes IPs ou grupos de IPs, permitindo que as configurações sejam aplicadas de maneira mais eficiente e organizada.

2.3.8 Parent Queue (Fila Pai)

Uma fila pai é o nível superior na hierarquia de filas e define as configurações gerais para limitar a largura de banda total disponível para um determinado grupo de IPs, (BOLANO; LAPEZ, 2008).

2.3.9 Child Queue (Fila Filho)

As filas filho estão abaixo das filas pai e podem herdar as configurações da fila pai ou ter configurações específicas adicionais para limitar a largura de banda de IPs individuais ou grupos de IPs, (BOLANO; LAPEZ, 2008). As filas pai e filho também desempenham papéis cruciais na hierarquia de filas. A fila pai define configurações gerais para limitar a largura de banda total disponível para um grupo de IPs específico, enquanto as filas filho herdam essas configurações ou podem ter configurações específicas adicionais para limitar a largura de banda de IPs individuais ou grupos de IPs. Isso permite uma personalização ainda maior do controle de largura de banda, adaptando-se às necessidades específicas da rede.

Em linha conclusivas, ao configurar o QoS para limitar a banda por IP em um MikroTik, é importante entender a estrutura de filas e como os pacotes são classificados e priorizados. A configuração adequada do QoS ajuda a garantir que serviços importantes, como VoIP ou videoconferência, tenham prioridade sobre outras atividades de menor prioridade, evitando congestionamentos na rede e garantindo uma experiência de usuário mais estável e eficiente. Além disso, a revisão e monitoramento regular das configurações de QoS são fundamentais para garantir que a largura de banda seja alocada de forma adequada e que o tráfego seja gerenciado de acordo com as necessidades e políticas da rede.

Esclareceu-se que a configuração de QoS no MikroTik é uma prática complexa e abrangente, mas com os conceitos apresentados, é possível criar uma rede mais eficiente, justa e confiável. Ao empregar a limitação de banda, filas de tráfego, marcadores de pacotes e a hierarquia de filas, os administradores podem otimizar o fluxo de dados, priorizando serviços críticos e garantindo uma experiência de rede mais fluida e satisfatória para todos os usuários. A utilização dessas ferramentas possibilita uma melhor alocação dos recursos disponíveis e um controle mais apurado do tráfego, resultando em maior produtividade, menor latência e maior satisfação geral dos usuários. Portanto, investir na configuração de QoS no MikroTik é uma estratégia fundamental para alcançar um ambiente de rede eficiente e com alta qualidade de serviço.

3 METODOLOGIA

3.1 Classificação da pesquisa

A natureza da pesquisa ela é do tipo aplicada. Os autores fornecem uma compreensão clara das características distintivas da pesquisa aplicada, enfatizando sua relevância na solução de problemas práticos em diversas áreas do conhecimento. Ainda, orientam para práticas e ferramentas metodológicas em que pesquisadores e profissionais possam conduzir investigações aplicadas de forma eficaz e eficiente. Fleury e Werlang (2016), fornecem uma definição clara e precisa do que é a pesquisa aplicada, enfatizando sua natureza orientada para a prática e sua relação com o contexto real de aplicação. São apresentadas diferentes abordagens utilizadas na pesquisa aplicada, permitindo aos leitores compreender as diversas formas como esse tipo de investigação.

Paranhos e Paranhos (2014), apresentam uma metodologia detalhada, focada na pesquisa aplicada à tecnologia, que abrange desde a formulação do problema de pesquisa até a análise e interpretação dos resultados. São fornecidas ferramentas e técnicas específicas para a coleta e análise de dados em pesquisas aplicadas no campo da tecnologia, permitindo aos pesquisadores uma abordagem prática e fundamentada. A metodologia proposta neste trabalho é direcionada para a aplicação prática, visando gerar resultados que possam ser implementados e utilizados no contexto tecnológico, contribuindo assim para a solução de problemas e o desenvolvimento de novas tecnologias.

O objetivo principal desta pesquisa é gerar conhecimentos para aplicação prática, buscando identificar os fatores que determinam e contribuem para um bom gerenciamento em redes lógicas em pequenas empresas. Consonante a abordagem do problema é do tipo qualitativa, uma vez que houve a interpretação dos resultados extraídos dos procedimentos técnicos em laboratório para atribuição de significados e valores para responder ao problema levantado, sendo um processo prático e dinâmico para adaptação de soluções nos ambientes de corporações, sendo esses ambientes diversos e complexos também. O enfoque dos objetivos da pesquisa tem caráter explicativo, pois visa identificar os fatores que devem ser adotados para a segurança a partir dos eventos de ocorrência de invasões e ataques externos a redes corporativas.

3.1.1 Procedimentos técnicos e local de aplicação das configurações

Os procedimentos técnicos consistem na aplicação de 8 configurações específicas direcionadas para a interface dos roteadores MikroTik. Em seguida, essas configurações foram aplicadas a partir de protótipos em um ambiente de TI da empresa "Cooperativa Odontológica do Estado do Amapá", que atua no segmento de Planos de Saúde e possui sede em Macapá, Amapá. A utilização desse ambiente de pesquisa específico proporcionou insights qualitativos intrínsecos ao campo tecnológico em questão. O equipamento utilizado para a realização dos testes foi o roteador MikroTik com as seguintes especificações técnicas:

Quadro 16 – Especificações técnicas do roteador RB750GL

a) Código do produto: RB750GL;b) Arquitetura: MIPSBE; **c) CPU: AR7242;** **d) Contagem de núcleos da CPU: 1;** **e) Frequência nominal da CPU: 400 MHz;** **f) Modelo de chip de comutação: AR8327-BL1A;** **g) Dimensões: 113x89x28mm; Peso sem embalagem e cabos: 129g**	**h) Licença do RouterOS: 4;** **i) Sistema Operacional: RouterOS;** **j) Tamanho da RAM: 64 MB;** **k) Tamanho do armazenamento: 64 MB;** **l) Tipo de armazenamento: NAND;** **m) MTBF: Aproximadamente 100.000 horas a 25°C;** **n) Temperatura ambiente testada: -30°C a +70°C.**

Fonte: Mikrotik (2013).

A fundamentação teórica da pesquisa abrange contribuições de diversos autores relevantes no campo da configuração e gerenciamento de redes usando roteadores MikroTik. Alguns dos autores citados são: Mosna e Moraes (2020), oferecem um guia abrangente para configurar VPNs site-to-site e client-to-site usando o OpenVPN e dispositivos MikroTik. Gazola (2013), fornece um guia prático e abrangente para configurar o failover de links de internet usando roteadores MikroTik. Leão (2017), explora a gestão de serviços de TI em um provedor de acesso à internet, com ênfase na aplicação da governança de TI.

A pesquisa culminou em considerações e principais achados, que visam impactar positivamente a eficiência do gerenciamento de redes lógicas, fornecendo

informações relevantes e aplicáveis para pequenas empresas que utilizam roteadores MikroTik em seus ambientes de TI. A abordagem qualitativa permitiu uma análise mais profunda e contextualizada dos resultados obtidos, garantindo que os conhecimentos gerados sejam diretamente aplicáveis e adaptáveis às necessidades específicas da Cooperativa Odontológica do Estado do Amapá.

3.1.2 Protótipos de aplicação prática

Quadro 17 – O configurações para aplicação no router MikroTik

(1) Protótipo de aplicação no Mikrotik - Servidor DHCP	**(2) Protótipo para aplicação no Mikrotik – Firewall básico**
1. Acesse o MikroTik através do Winbox ou de um navegador web. **2. Vá para o menu "IP" e selecione "DHCP Server".** **3. Clique em "+ Add" para adicionar um novo servidor DHCP.** **4. Defina uma interface de rede na qual o servidor DHCP será executado.** **5. Especifique o intervalo de endereços IP que será fornecido aos clientes.** **6. Configure as opções adicionais, como gateway padrão, DNS e tempo de concessão.** **7. Salve as configurações e inicie o servidor DHCP**	**1. Acesse o Winbox e conecte-se ao roteador.** **2. No menu "IP", vá para "Firewall" e na guia "Filter Rules", crie regras de firewall.** **3. Crie regras para bloquear todo o tráfego de entrada, permitir tráfego de loopback, permitir conexões estabelecidas e relacionadas e permitir tráfego ICMP (ping).** **4. Configure outras regras conforme necessário, como permissões de portas específicas ou bloqueio de IPs.** **5. Defina a ordem das regras de acordo com a prioridade desejada.** **6. Clique em "OK" para salvar as configurações.** **7. Clique em "Apply" para aplicar as configurações.**
(3) Protótipo para aplicação no Mikrotik – QoS para limitar a banda por IP	**(4) Protótipo para aplicação no Mikrotik – Configuração de uma Rota Dinâmica**
1. Crie uma regra de marcação no "Firewall" (Mangle) para identificar o tráfego por IP. **2. Crie uma regra de fila (Queue) para definir a largura de banda máxima para o IP identificado na etapa 1.**	**1. Acesse o Winbox e conecte-se ao roteador.** **2. Vá para "IP" -> "Routes".** **3. Clique em "Add New" para criar uma nova rota.** **4. Configure o "Destino" (endereço IP ou prefixo de rede), "Gateway" (próximo salto) e**

3. Aplique a regra de marcação antes da regra de fila. 4. Clique em "Apply" para aplicar as configurações de QoS.	"Pref. Source" (interface de saída). 5. Marque as opções "Gateway" e "Dynamic" para indicar que é uma rota dinâmica. 6. Clique em "OK" para salvar. 7. Clique em "Apply" para aplicar as configurações..
(5) Protótipo para aplicação no Mikrotik – Configuração de uma Rota Estática 1. Acesse o Winbox e conecte-se ao roteador. 2 . Vá para "IP" -> "Routes". 3. Clique em "Add New" para criar uma nova rota estática. 4. Configure o "Destino" (endereço IP ou prefixo de rede) e o "Gateway" (próximo salto). 5. Clique em "OK" para salvar. 6. Clique em "Apply" para aplicar as configurações..	**(6) Protótipo para aplicação no Mikrotik – Configuração de Load Balancing** 1. Marque pacotes de saída com regras de marcação em "IP" -> "Firewall" -> "Mangle". 2. Crie rotas para suas conexões de Internet em "IP" -> "Routes". 3. Adicione uma rota padrão com a primeira conexão de Internet como gateway. 4. Configure regras NAT para balanceamento de carga em "IP" -> "Firewall" -> "NAT". 5. Crie regras de filtro conforme necessário em "IP" -> "Firewall" -> "Filter Rules". 6. Clique em "OK" e depois em "Apply" para salvar e aplicar as configurações..
(7) Protótipo para aplicação no Mikrotik – Configuração de Fail Over 1. Marque pacotes de saída com regras de marcação em "IP" -> "Firewall" -> "Mangle". 2. Crie rotas para suas conexões de Internet em "IP" -> "Routes". 3. Adicione uma rota padrão com a primeira conexão de Internet como gateway. 4. Configure regras NAT em "IP" -> "Firewall" -> "NAT" para cada conexão. 5. Crie regras de filtro em "IP" -> "Firewall" -> "Filter Rules" para direcionar o tráfego para cada conexão.	**(8) Protótipo para aplicação no Mikrotik – Configuração de um Servidor VPN** 1. Acesse o Winbox e conecte-se ao roteador. 2. Vá para "PPP" -> "PPTP Server" e habilite o servidor. 3. Defina um perfil de autenticação em "Profile" e associe-o ao servidor PPTP. 4. Configure as credenciais dos usuários em "Secrets". 5. Personalize as configurações avançadas, como faixa de IPs e DNS. 6. Clique em "OK" e depois em "Apply" para salvar e aplicar as configurações.

6. Clique em "OK" e depois em "Apply" para salvar e aplicar as configurações.	

Fonte: Elaborado pelos acadêmicos (2023).

4 DISCUSSÃO E RESULTADOS

4.1 Os roteadores Mikrotik para pequenas e médias empresas

A discussão científica revela que os roteadores MikroTik oferecem uma série de benefícios para pequenas e médias empresas que buscam aprimorar o gerenciamento de suas redes lógicas. Com base nos estudos e percepções dos autores Mosna e Moraes (2020), Leão (2017), Londoño Velásquez (2015) e Ribeiro (2016), pode-se destacar alguns pontos relevantes:

Os roteadores MikroTik são reconhecidos por oferecer uma ampla gama de funcionalidades que vão além do roteamento tradicional. Eles fornecem recursos avançados como VPN, firewall, controle de banda, balanceamento de carga e muito mais. Essa versatilidade permite que as pequenas e médias empresas otimizem suas redes de acordo com suas necessidades específicas.

O preço acessível dos roteadores MikroTik em comparação com outras soluções disponíveis no mercado é uma vantagem significativa para as pequenas e médias empresas com orçamentos limitados. Mesmo sendo mais acessíveis em termos de custo, eles não comprometem a qualidade, confiabilidade e recursos oferecidos. A interface de gerenciamento dos roteadores MikroTik é elogiada por ser intuitiva e amigável. Isso torna mais fácil para as empresas configurarem, monitorarem e gerenciarem suas redes, mesmo sem um profundo conhecimento técnico em redes.

Os roteadores MikroTik são escaláveis, o que significa que podem crescer de acordo com as necessidades das empresas. À medida que a empresa expande suas operações, os roteadores MikroTik podem ser facilmente atualizados ou adicionados sem a necessidade de substituir toda a infraestrutura.

A possibilidade de implementar VPNs com os roteadores MikroTik é uma vantagem importante para médias empresas. As VPNs proporcionam conexões seguras entre diferentes locais ou dispositivos remotos, garantindo a criptografia dos dados transmitidos e protegendo-os contra acessos não autorizados.

Os recursos avançados de segurança dos roteadores MikroTik, como firewall, filtragem de pacotes e autenticação, ajudam a proteger a rede contra ameaças cibernéticas e ataques maliciosos. Isso é particularmente relevante para provedores de acesso à Internet e empresas que precisam garantir a segurança de suas operações e dos dados de seus clientes. A aplicação de boas práticas de segurança, como a configuração adequada de ACLs, autenticação de usuários e controle de acesso, reforça a proteção contra invasões e garante a integridade e confidencialidade dos dados nas redes.

A abordagem da Governança de TI, conforme mencionada por Leão (2017), desempenha um papel crucial no uso eficiente e seguro dos roteadores MikroTik em um provedor de acesso à Internet. Isso envolve alinhar as estratégias de TI com os objetivos de negócio, otimizar o uso dos recursos de tecnologia e assegurar a conformidade com normas e regulamentos.

Portanto, os roteadores MikroTik oferecem uma solução confiável e acessível para pequenas e médias empresas que buscam melhorar o gerenciamento de suas redes lógicas. Sua versatilidade, recursos avançados, interface intuitiva e foco na segurança os tornam uma escolha atraente para empresas que desejam aprimorar a eficiência operacional, compartilhar recursos entre locais remotos e proteger suas redes contra ameaças cibernéticas. A adoção de boas práticas de segurança e uma abordagem de Governança de TI adequada complementam os benefícios dos roteadores MikroTik, contribuindo para o sucesso e competitividade das empresas em um cenário de negócios cada vez mais digital e desafiador.

4.2 Relevância das configurações e seu uso adequado

Os principais resultados do capítulo sobre "Instalação e configuração do servidor DHCP de um MikroTik" são:

Rahman, Sumarna e Nurdin (2020) conduziram testes e medições para avaliar o desempenho do DHCP no ambiente do roteador MikroTik. Eles destacaram métricas como o tempo médio de concessão de endereços IP, a taxa de sucesso na atribuição de IPs e a capacidade do serviço DHCP em lidar com muitas solicitações simultâneas. Isso fornece insights valiosos para otimizar o serviço DHCP e melhorar o desempenho geral da rede em ambientes que utilizam o sistema operacional MikroTik.

Marcillo e Benites (2019) destacam a importância do servidor DHCP como uma medida fundamental para proteger a rede contra ataques internos, como ARP Spoofing, MAC Flooding e DHCP Spoofing. Eles discutem como a implementação adequada do DHCP pode ser uma estratégia eficaz para mitigar essas ameaças e fortalecer a segurança da infraestrutura de rede.

Kurina (2020) aborda as vulnerabilidades do Cliente DHCP em roteadores MikroTik, especificamente o ataque conhecido como "DHCP Starvation Attack". Ela explora formas de segurança para mitigar essas vulnerabilidades e destaca a necessidade de medidas proativas para proteger a infraestrutura de rede contra ataques desse tipo.

Silva (2017) apresenta uma abordagem prática sobre a gestão do pool de endereços IP em roteadores MikroTik. Ela destaca a importância da correta alocação de endereços IP para evitar esgotamento do pool e garantir que todos os dispositivos possam ser conectados sem conflitos.

Ribeiro (2016) apresenta uma abordagem relevante sobre a concessão de endereços IP no roteador MikroTik como parte de um conjunto de medidas para fortalecer a segurança em redes de computadores. Ele destaca a importância de configurar o DHCP de forma segura e controlada para fortalecer a proteção da rede e garantir uma gestão eficiente dos endereços IP atribuídos.

A relevância dessa configuração no contexto de pequenas e médias empresas é significativa. Pequenas e médias empresas geralmente possuem recursos limitados e uma infraestrutura de rede mais simples em comparação com grandes empresas. Nesse contexto, a configuração do servidor DHCP em um roteador MikroTik é crucial para criar uma rede funcional e eficiente. Ao automatizar a atribuição de endereços IP e outras configurações de rede, o servidor DHCP facilita a conexão de dispositivos à rede, tornando o processo mais simples e reduzindo a carga de trabalho dos administradores de rede. Além disso, a configuração adequada do pool de endereços IP e das opções DHCP ajuda a otimizar o uso dos recursos de rede e a evitar conflitos de IP, o que é especialmente relevante em ambientes com vários dispositivos conectados. A segurança é outra consideração crucial para as pequenas e médias empresas. O servidor DHCP pode ser configurado para mitigar ameaças internas, como ARP Spoofing, MAC Flooding e DHCP Spoofing, fornecendo uma camada adicional de proteção à infraestrutura de rede. Além disso, a concessão de endereços

IP de forma controlada e segura contribui para a proteção da rede contra ataques e exploração de vulnerabilidades. Portanto, a configuração adequada do servidor DHCP em um roteador MikroTik é essencial para uma rede funcional, eficiente e segura para pequenas e médias empresas. Isso proporciona uma experiência de conectividade sólida para os usuários e permite que os administradores de rede gerenciem de forma eficiente os recursos de IP e a segurança da infraestrutura de rede.

4.3 Funcionamento do firewall e relevância para segurança cibernética

Ao configurar o firewall básico em um Mikrotik, é importante definir regras cuidadosamente para permitir apenas o tráfego necessário e bloquear ou restringir o acesso a conteúdo ou serviços não autorizados. Isso ajuda a proteger a rede contra ameaças externas, garantir o bom funcionamento dos serviços internos e manter um ambiente de rede seguro e confiável. Os conceitos explanados pelos autores Levy (2020), Ari Muzakir (2022), Entelco Telecom (2018) e Zibeti (2015) são fundamentais para realizar uma configuração de firewall eficaz e personalizada de acordo com as necessidades específicas da rede e dos usuários. Além disso, é importante revisar regularmente as configurações de firewall para garantir que estejam atualizadas e em conformidade com as políticas de segurança da rede.

Levy (2020), destacou a importância do firewall MikroTik para garantir a segurança da rede, proteger contra ameaças externas e controlar o acesso a recursos internos e redes públicas. O firewall oferece funcionalidades como filtragem e inspeção de pacotes, controle de acesso granular e integração com o Hotspot do RouterOS.

Ari Muzakir (2022), explica as diferentes cadeias (chains) do firewall MikroTik, como "input," "forward," e "output," que correspondem a diferentes fases do processamento de pacotes na rede. Além disso, destaca o conceito de "packet filtering," que controla o tráfego de dados com base em regras de filtragem, como endereços IP, portas e protocolos.

Entelco Telecom (2018), ressalta a importância das regras de firewall, que são configurações aplicadas às cadeias de firewall e contêm critérios de correspondência e ações específicas. Exemplos de regras incluem bloqueio de tentativas de força bruta no serviço FTP e negação de acesso a determinadas portas TCP.

Zibeti (2015), enfatiza a relevância do bloqueio de portas para impedir o acesso a serviços ou protocolos indesejados, contribuindo para a segurança da rede. Por

outro lado, a liberação de portas é necessária para permitir que serviços ou protocolos específicos sejam acessados na rede.

Portanto, ao implementar as lições aprendidas com os conceitos apresentados pelos autores, os administradores de rede podem criar uma configuração de firewall sólida, que permita apenas o tráfego necessário e bloqueie ou restrinja o acesso a conteúdo não autorizado.

4.4 QoS para o gerenciamento de tráfego nos roteadores MikroTik

A contribuição do QoS (Quality of Service) para o gerenciamento de tráfego nos roteadores MikroTik é inegável e extremamente relevante. A implementação adequada do QoS em um roteador MikroTik permite priorizar e gerenciar o tráfego de rede com base em suas características e requisitos de desempenho, resultando em uma melhor experiência para os usuários e aplicações críticas.

O QoS é uma técnica essencial para garantir que aplicações e serviços importantes tenham prioridade sobre o tráfego menos crítico, melhorando a qualidade e a consistência da experiência do usuário. Ao limitar a banda por IP e adotar diferenciação de serviços, os administradores podem garantir que os recursos de largura de banda sejam alocados de maneira justa e adequada, mantendo uma rede responsiva e confiável mesmo em situações de alto tráfego.

Uma das principais vantagens da configuração de QoS no MikroTik é a possibilidade de evitar que dispositivos ou usuários monopolizem toda a largura de banda disponível. Com a limitação de banda, é possível impor um limite máximo na quantidade de largura de banda que um determinado dispositivo ou grupo de IPs pode usar, garantindo uma distribuição equitativa dos recursos e evitando gargalos conforme demonstrado por Bolano e Lapez (2008).

Além disso, as filas de tráfego e os marcadores de pacotes são ferramentas poderosas que permitem classificar o tráfego em categorias distintas, facilitando a aplicação de regras específicas de QoS. A hierarquia de filas e a tree de filas permitem organizar as filas de tráfego em uma estrutura hierárquica, o que oferece controle mais granular sobre a alocação de largura de banda para diferentes IPs ou grupos de IPs, priorizando o tráfego crítico em relação a atividades menos importantes. O uso adequado do QoS também possibilita o balanceamento de carga entre diferentes canais de saída para a internet, direcionando o tráfego com base no tipo de serviço

identificado nas regras de mangle. Isso otimiza o fluxo de pacotes, aproveitando as vantagens específicas de cada canal.

Portanto, investir na configuração de QoS em um MikroTik é uma estratégia inteligente para alcançar um ambiente de rede eficiente e com alta qualidade de serviço. Com as práticas apresentadas por Bolano e Lapez (2008), é possível criar uma rede mais eficiente, justa e confiável, garantindo uma experiência de usuário mais estável e eficiente para todos os usuários.

4.5 Resultados das aplicação prática das configurações selecionadas

Após estudar e planejar a implementação de um servidor DHCP em nosso roteador MikroTik RB750GL, o Quadro 18 destaca as configurações realizadas:

Quadro 18 – Síntese do processo realizado no roteador para configurar o DHCP

1 para adicionar um servidor DHCP é preciso adicionar 1 IP fixo na porta de onde vai ser jogado o DHCP
caminho: IP/Addresse, clica no sinal de +
adiciona a faixa de IP desejada para a rede no Address e escolha a interface para a distribuição
2° Após adicionado o IP na porta, vamos criar o servidor DHCP.
caminho: IP/DHCP Server e clique em DHCP Setup
Exemplo de criação de DHCP porta 8 do mikrotik rb4011
Adiciona-se um IP local na porta 8 /24
Clica-se no servidor dhcp ip/dhcp server/ dhcp setup porta 8
Faixa do IP do dhcp /24
ip que vai ser o Gateway
a faixa que vai ser distribuida quantidade de IP podendo ser alterado conforme o tecnico quiser.
o dns que vai ser no dhcp
o tempo de vida do IP
após isso criado o dhcp, se eu plugar um notebook na porta 8 vai pegar a faixa 10/24
indo na aba Networks aparece o outro dhcp ativo com seu dns e gateway

Fonte: Elaborado pelos acadêmicos (2023).

Após a conclusão da configuração do servidor DHCP, pudemos observar os seguintes resultados:

a) Atribuição Automática de Endereços IP: Os dispositivos clientes conectados à interface "ether2" começaram a receber automaticamente endereços IP

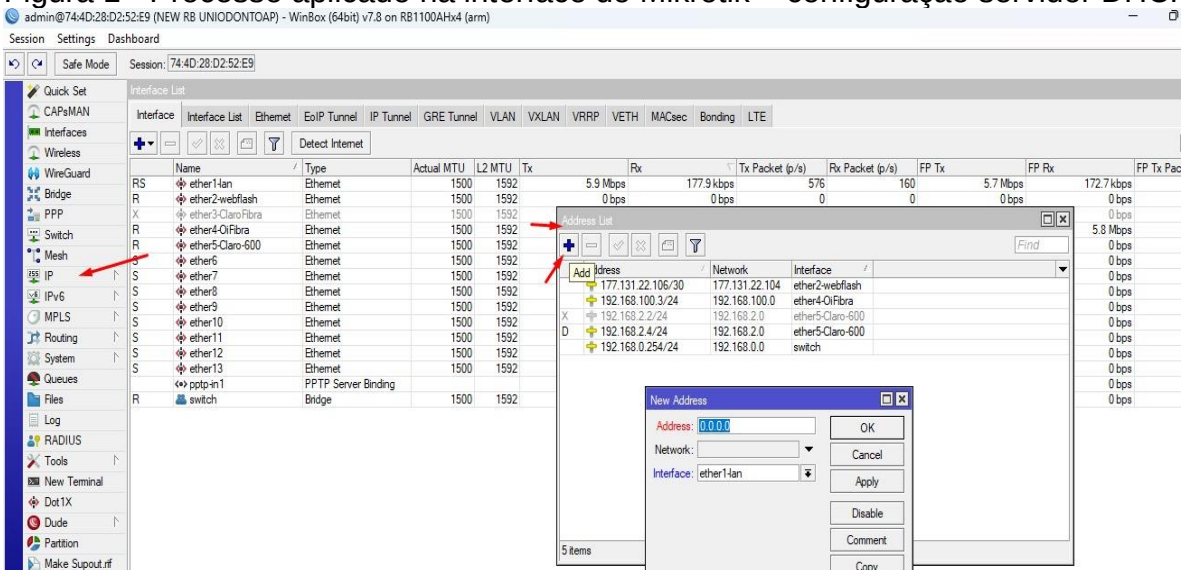
dentro do intervalo especificado (192.168.1.100 a 192.168.1.200). Isso facilitou o gerenciamento de dispositivos na rede, pois não precisávamos configurar manualmente cada um deles.

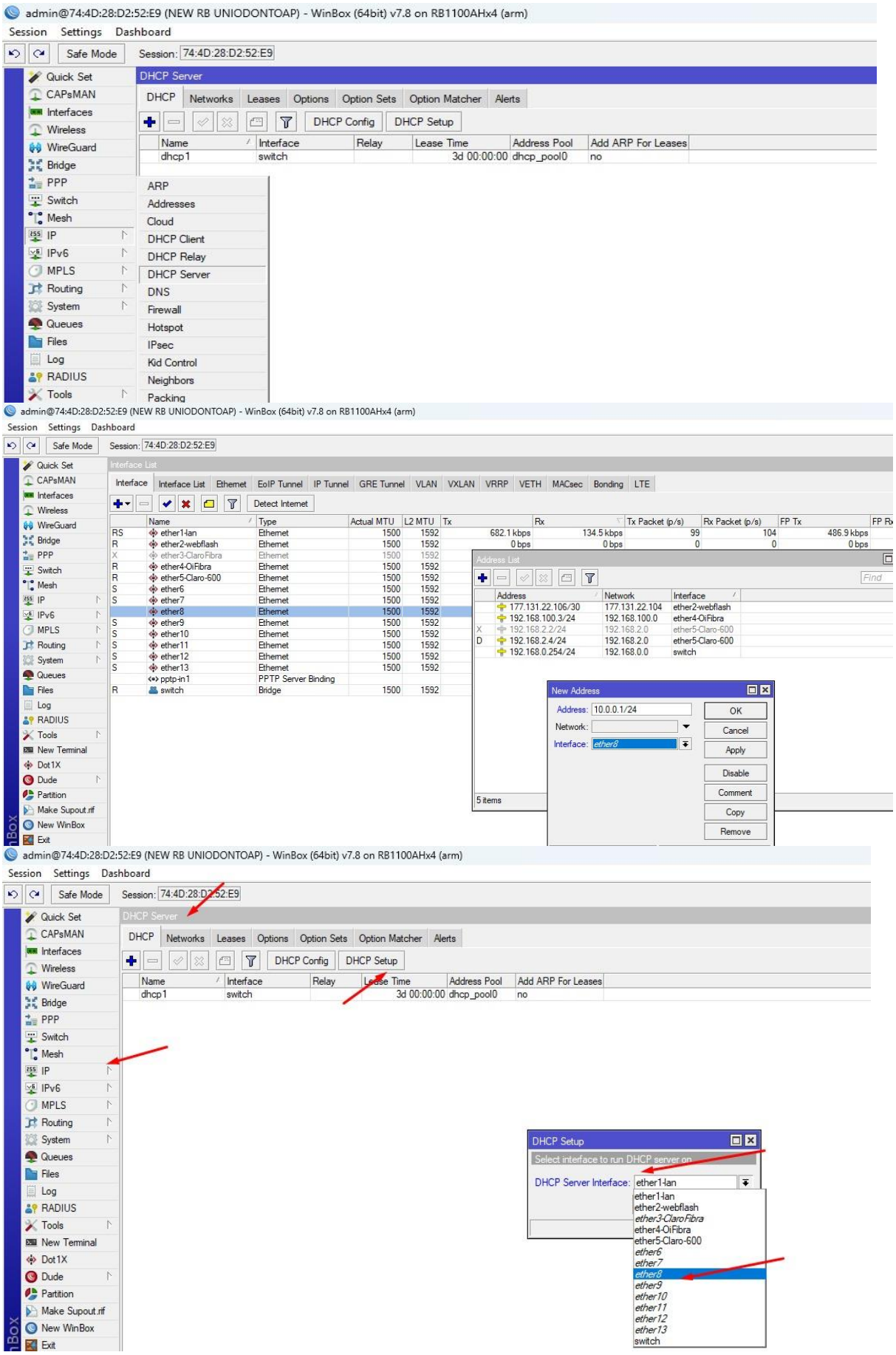
b) Gateway Padrão Configurado: O servidor DHCP também atribuiu o endereço IP da interface "ether2" do roteador MikroTik como o gateway padrão para os dispositivos clientes. Isso permitiu que eles acessassem a Internet e outros dispositivos na rede local sem problemas.

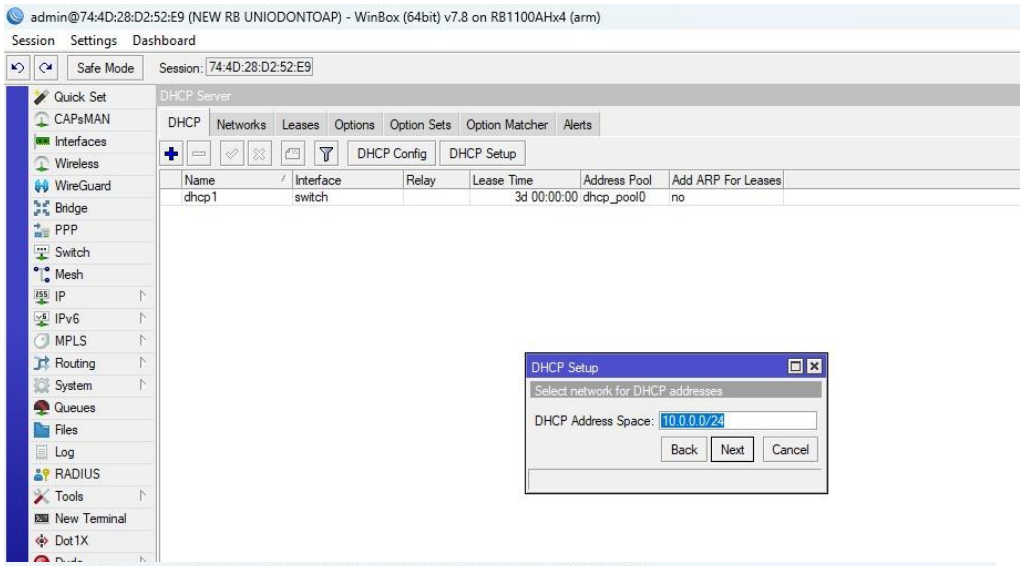
c) Servidores DNS Configurados: Os servidores DNS foram configurados corretamente para os dispositivos clientes como 8.8.8.8 e 8.8.4.4 (Google Public DNS). Isso garantiu que os dispositivos pudessem resolver nomes de domínio corretamente e acessar sites na Internet sem dificuldades.

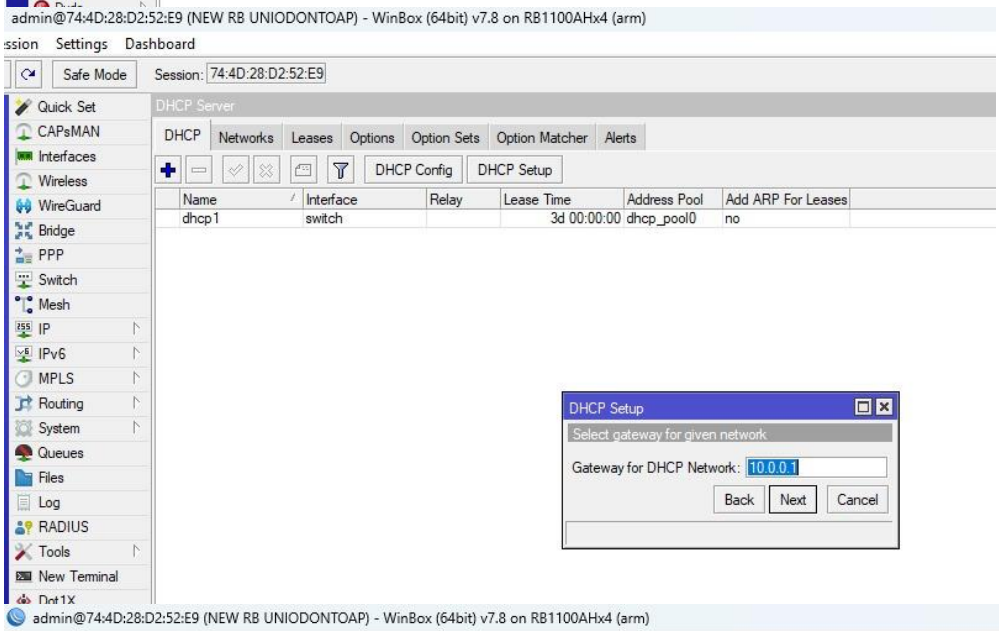
d) Facilidade de Adição de Novos Dispositivos: A aplicação do servidor DHCP facilitou a conexão de novos dispositivos à rede, pois eles obtiveram automaticamente os endereços IP necessários para se comunicarem na rede local e na Internet.

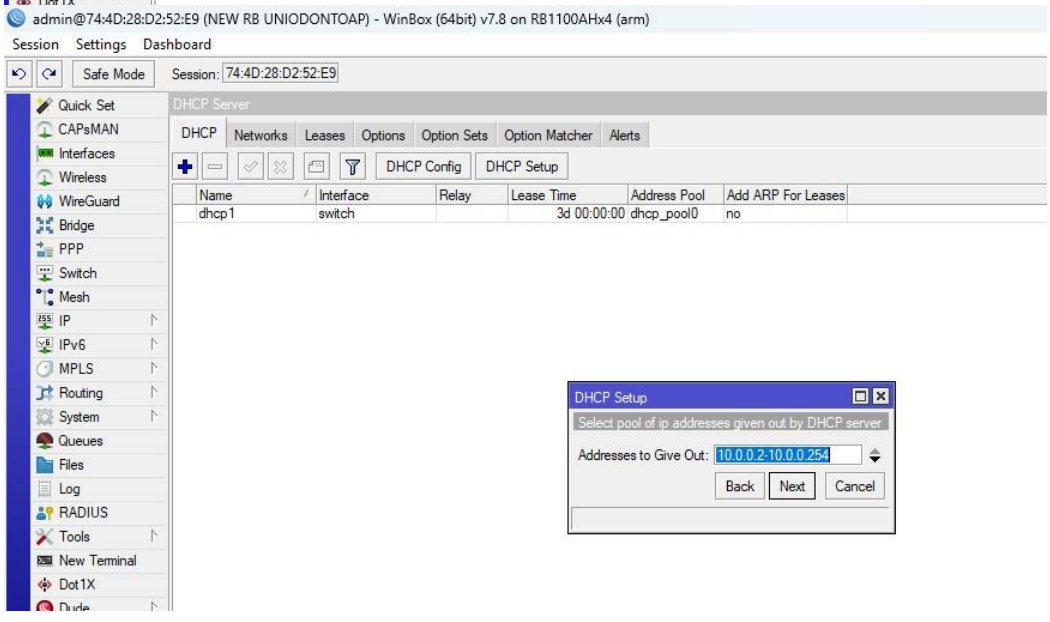
Figura 1 - Processo aplicado na interface do Mikrotik – configuração servidor DHCP

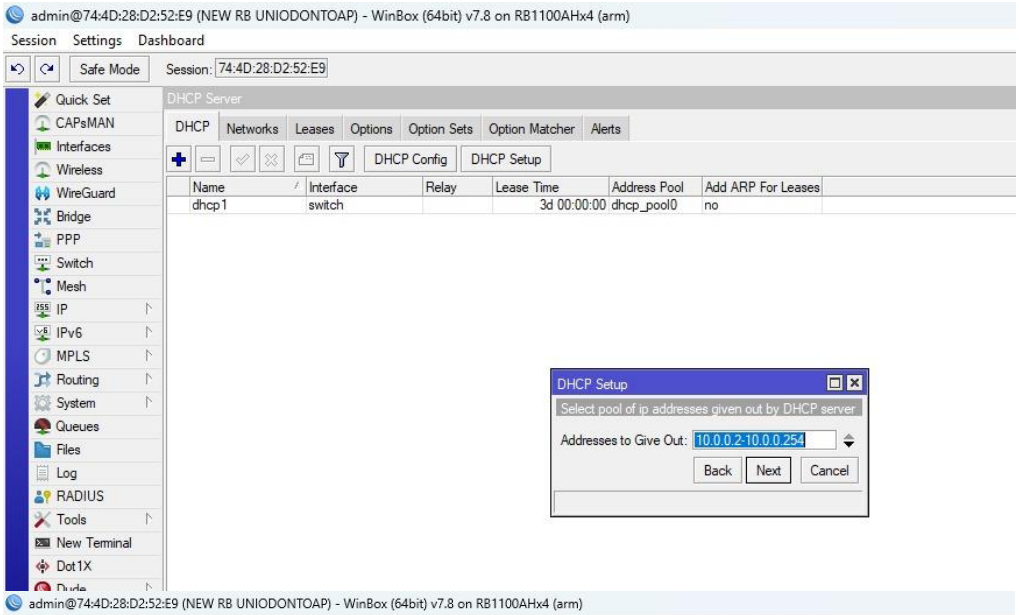


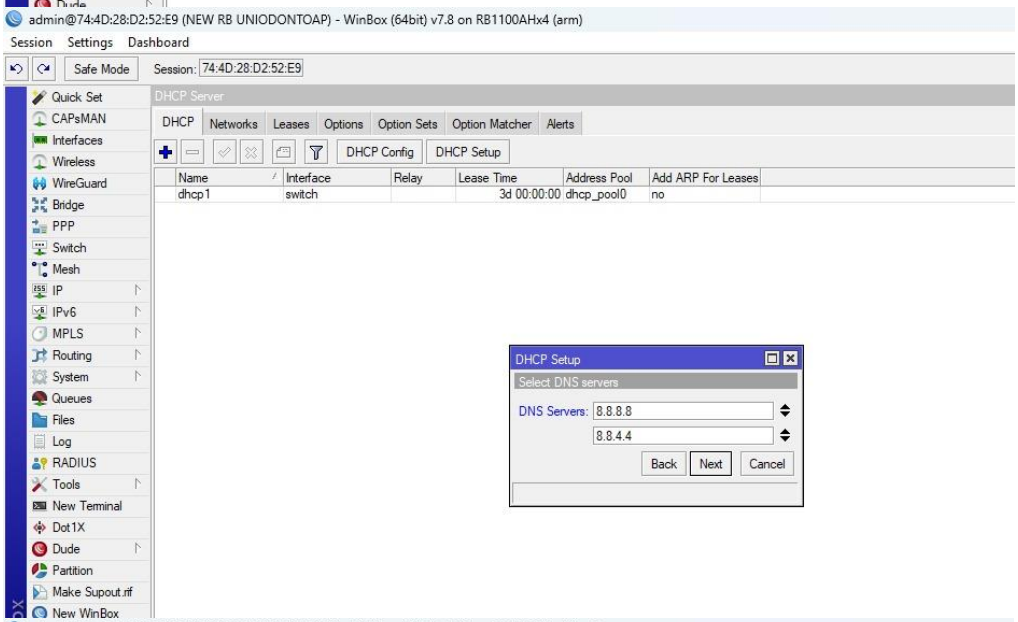

admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
ARP
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Neighbors
Packing
Interface List
Interface
Interface List
Ethernet
EoIP Tunnel
IP Tunnel
GRE Tunnel
VLAN
VXLAN
VRRP
VETH
MACsec
Bonding
LTE
Detect Internet
Type
Actual MTU
L2 MTU
Tx
Rx
Tx Packet (p/s)
Rx Packet (p/s)
FP Tx
ether1-lan
ether2-webflash
ether3-ClaroFibra
ether4-OiFibra
ether5-Claro-600
ether6
ether7
ether8
ether9
ether10
ether11
ether12
ether13
pptp-in1
PPTP Server Binding
Address List
Address
Network
177.131.22.106/30
192.168.100.3/24
192.168.2.2/24
192.168.2.4/24
192.168.0.254/24
5 items
New Address
Address: 10.0.0.1/24
Network:
Interface: ether8
OK
Cancel
Apply
Disable
Comment
Copy
Remove
New Terminal
Dot1X
Dude
Partition
Make Supout.rif
New WinBox
Exit
DHCP Setup
Select interface to run DHCP server on
DHCP Server Interface: ether1-lan

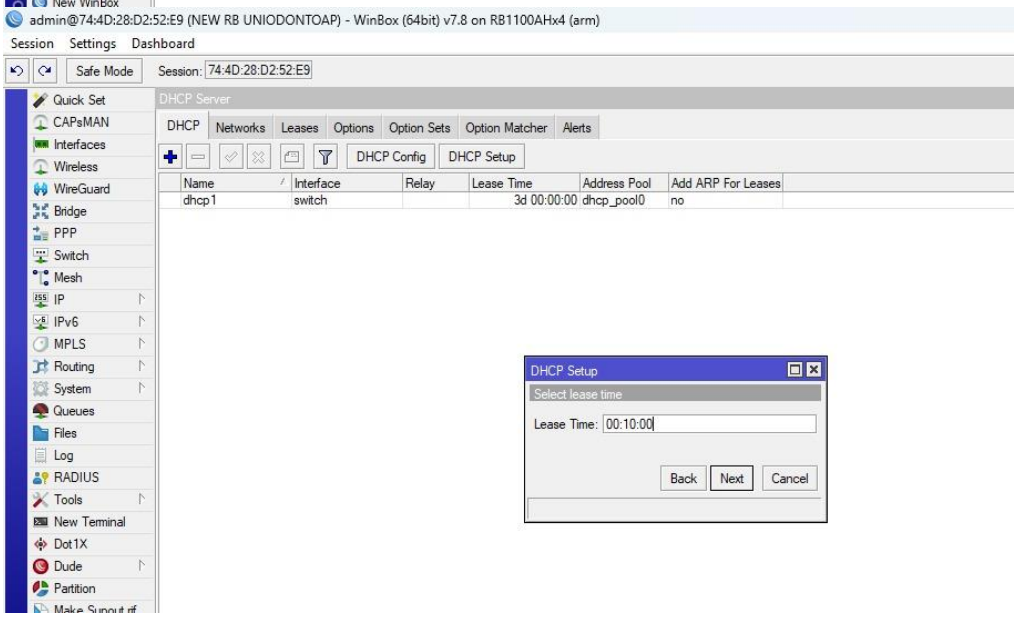

admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select network for DHCP addresses
DHCP Address Space: 10.0.0.0/24
Back
Next
Cancel

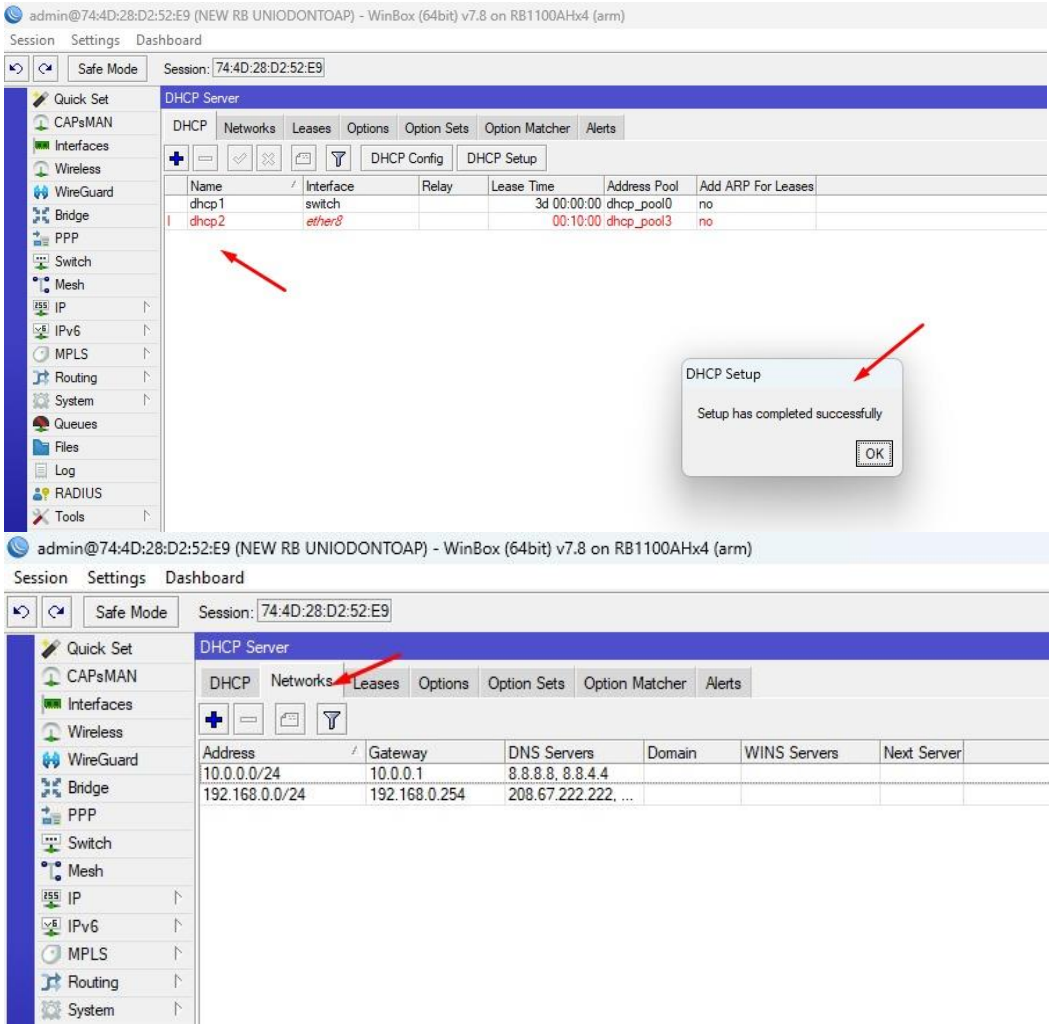

admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
ssion Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select gateway for given network
Gateway for DHCP Network: 10.0.0.1
Back
Next
Cancel


admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select pool of ip addresses given out by DHCP server
Addresses to Give Out: 10.0.0.2-10.0.0.254
Back
Next
Cancel


admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select pool of ip addresses given out by DHCP server
Addresses to Give Out: 10.0.0.2-10.0.0.254
Back
Next
Cancel


admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
Partition
Make Supout.rif
New WinBox
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select DNS servers
DNS Servers: 8.8.8.8
8.8.4.4
Back
Next
Cancel


admin@74:4D:28:D2:52:E9 (NEW RB UNIODONTOAP) - WinBox (64bit) v7.8 on RB1100AHx4 (arm)
Session Settings Dashboard
Safe Mode
Session: 74:4D:28:D2:52:E9
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
Partition
DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
Add ARP For Leases
dhcp1
switch
3d 00:00:00
dhcp_pool0
no
DHCP Setup
Select lease time
Lease Time: 00:10:00
Back
Next
Cancel



Fonte: Elaborado pelos acadêmicos (2023).

Após estudarmos as necessidades de segurança da nossa rede, decidimos aplicar um conjunto de regras de firewall básico no nosso roteador MikroTik RB750GL.

Aplicamos o grupo de regras firewall do Anexo A. Esse conjunto de regras de firewall básico consiste em: (1) Drop de conexões inválidas, essa regra bloqueia qualquer conexão que não seja válida, evitando conexões potencialmente maliciosas ou corrompidas. (2) Permitir conexões estabelecidas, essa regra permite o tráfego para conexões que já foram estabelecidas anteriormente. Isso é essencial para permitir respostas a solicitações iniciadas pela rede interna. (3) Permitir conexões relacionadas, essa regra permite o tráfego para conexões que estão relacionadas às conexões estabelecidas. Isso é útil para permitir o tráfego associado a conexões estabelecidas, como transferências de dados em uma conexão estabelecida. (4) Permitir SSH, HTTP, HTTPS, DNS UDP e DNS TCP, essas regras permitem o tráfego para os serviços essenciais do servidor, como acesso SSH (para gerenciamento remoto), acesso HTTP e HTTPS (para navegação na web segura) e resolução de DNS

(para tradução de nomes de domínio em endereços IP). (5) Bloquear todo o tráfego não especificado, essa regra bloqueia qualquer tráfego que não corresponda às regras anteriores, garantindo que somente o tráfego permitido seja aceito.

O Quadro 19, contém o processo realizado para configurar o firewall:

Quadro 19 – Síntese do processo realizado no roteador para configurar o firewall

Passo 1: Acesso ao Roteador > Abrimos o Winbox e inserimos o endereço IP do roteador MikroTik. Informamos as credenciais de administrador para acessar a interface do roteador. **Passo 2:** Configuração das Regras de Firewall > No menu lateral, clicamos em "IP" e, em seguida, selecionamos "Firewall". Criamos cada uma das regras mencionadas anteriormente, preenchendo os campos apropriados para cada uma delas. **Passo 3:** Verificação e Aplicação > Antes de aplicar as configurações, revisamos cuidadosamente todas as regras para garantir que elas estavam corretas e atendiam aos requisitos de segurança da nossa rede. Confirmamos que as regras estavam na ordem adequada, pois a ordem das regras no firewall é importante, uma vez que as regras são aplicadas em sequência, da primeira à última. Com tudo verificado, clicamos no botão "Apply" para aplicar as configurações de firewall no roteador MikroTik.

Fonte: Elaborado pelos acadêmicos (2023).

Após a aplicação das configurações do firewall básico, observamos os seguintes resultados na proteção da rede:

a) **Bloqueio de Conexões Inválidas:** O roteador começou a filtrar e bloquear conexões que não eram consideradas válidas, o que ajudou a prevenir potenciais ataques e tráfego malicioso.
b) **Tráfego Essencial Permitido:** As regras de firewall permitiram o tráfego essencial para os serviços necessários, como acesso SSH, navegação na web e resolução de DNS, garantindo a continuidade das operações normais da rede.
c) **Tráfego Não Especificado Bloqueado:** Qualquer tráfego não correspondente às regras permitidas foi bloqueado, ajudando a evitar tráfego indesejado ou mal-intencionado.
d) **Proteção Básica Implementada:** Embora as configurações de firewall básico não ofereçam uma proteção completa contra todas as ameaças, elas forneceram uma camada inicial de segurança para a nossa rede.

Concluímos que a aplicação das configurações de firewall básico no roteador MikroTik RB750GL melhorou significativamente a segurança da nossa rede, fornecendo um controle mais refinado sobre o tráfego que entra e sai do roteador. No entanto, lembramos que a segurança da rede é uma jornada contínua e que medidas adicionais podem ser necessárias para enfrentar ameaças mais avançadas.

Após perceber que a rede da Cooperativa Odontológica do Estado do Amapá estava enfrentando problemas com a largura de banda e o controle do tráfego, tomamos a iniciativa de aplicar configurações QoS no roteador MikroTik RB750GL para melhorar a experiência dos usuários e otimizar o uso da internet.

Primeiramente, acessamos o MikroTik RouterOS através do WinBox e seguimos os passos do Quadro 12 do referencial teórico, para configurar o controle de largura de banda por endereço IP. Identificamos um grupo específico de dispositivos, como computadores dos funcionários administrativos, que necessitava de um controle mais rígido para evitar sobrecarga da rede. Utilizando a função "Mark Packet", criamos uma regra de mangle nomeada como "trf_administrativo" para marcar o tráfego proveniente desses dispositivos. Em seguida, criamos uma fila chamada "fila_administrativo" para esse grupo. Definimos a largura de banda máxima para 2 Mbps de upload e download, garantindo que o tráfego do setor administrativo não afetasse negativamente outros setores da cooperativa.

Além disso, observamos que havia um grande volume de tráfego HTTP e P2P na rede, impactando negativamente o desempenho geral. Utilizando a funcionalidade "Layer7 Protocols" e "Mark Packet", criamos regras de mangle específicas para identificar o tráfego de cada tipo. Em seguida, criamos filas de controle de largura de banda separadas para HTTP e P2P, limitando-as a 5 Mbps cada.

Quadro 20 – Síntese do processo realizado no roteador para configurar o controle de banda por IP

1. Acesso ao MikroTik RouterOS: Acessamos o MikroTik RouterOS através do WinBox com as credenciais de login corretas para acessar o roteador.
2. Controle de Largura de Banda por Endereço IP: Identificamos um grupo específico de dispositivos, que neste caso são os computadores dos funcionários administrativos, que necessitava de um controle mais rígido para evitar sobrecarga na rede. Para isso, aplicamos a seguinte configuração:
3. Criamos uma regra de mangle denominada "trf_administrativo" na aba "IP" > "Firewall" > "Mangle". Definimos a cadeia como "forward" e o protocolo como "tcp" para aplicar o controle no tráfego encaminhado. Em "Action", escolhemos "Mark Packet" e criamos um nome para identificar o tráfego, que é o "trf_administrativo".

Na opção "Src. Address", inserimos o intervalo de endereços IP dos computadores administrativos. **4.** Em seguida, criamos uma fila chamada "fila_administrativo" na aba "Queue" > "Simple Queue". Definimos a largura de banda máxima para 2 Mbps de upload e download, selecionamos "Global" como alvo e associamos a regra de mangle "trf_administrativo" à fila. Isso garantiu que o tráfego dos computadores administrativos fosse controlado, evitando impactos negativos em outros setores da cooperativa.

Fonte: Elaborado pelos acadêmicos (2023).

Quadro 21 – Processo realizado para configurar o controle de banda diferenciando serviços

1. Controle de Largura de Banda Diferenciando Serviços: Observamos que o tráfego HTTP e P2P estava afetando negativamente o desempenho geral da rede. Para lidar com isso, aplicamos a seguinte configuração: **2.** Criamos padrões de protocolo Layer7 para identificar os tráfegos HTTP e P2P na aba "IP" > "Firewall" > "Layer7 Protocols". Utilizamos expressões regulares para identificar os padrões de tráfego associados a cada serviço. **3.** Em seguida, criamos regras de mangle específicas na aba "IP" > "Firewall" > "Mangle" para identificar o tráfego de cada tipo. Usamos "Mark Packet" e criamos os nomes "trf_http" para HTTP e "trf_p2p" para P2P, associando os respectivos padrões de protocolo Layer7. **4.** Para controlar a largura de banda desses tipos de tráfego, criamos filas de controle de largura de banda separadas na aba "Queue" > "Simple Queue". Para o tráfego HTTP, denominamos a fila como "fila_http" e definimos a largura de banda máxima para 5 Mbps de upload e download, associando a regra de mangle "trf_http". Da mesma forma, criamos a fila "fila_p2p" para P2P, com largura de banda máxima também de 5 Mbps, associando a regra de mangle "trf_p2p".

Fonte: Elaborado pelos acadêmicos (2023).

Os resultados após a aplicação das configurações foram notáveis. Os funcionários administrativos perceberam uma melhoria significativa na velocidade de navegação e no desempenho das aplicações internas. A rede não estava mais sendo sobrecarregada pelos dispositivos do setor, o que resultou em uma experiência de uso mais estável para todos os usuários. Além disso, com a diferenciação do tráfego entre HTTP e P2P, o consumo excessivo de largura de banda causado por downloads e uploads de arquivos grandes foi controlado. Os serviços essenciais, como sistemas de gestão e atendimento ao cliente, puderam operar com mais fluidez, já que tinham uma parcela de largura de banda garantida. Outro benefício foi o balanceamento de carga entre os canais de saída para a internet, que evitou congestionamentos e garantiu uma distribuição equitativa do tráfego. Isso resultou em um aproveitamento

mais eficiente dos links de internet disponíveis, reduzindo o risco de quedas de conexão e melhorando a resiliência da rede.

Assim, a aplicação das configurações QoS no roteador MikroTik RB750GL na Cooperativa Odontológica do Estado do Amapá trouxe resultados altamente positivos. A rede se tornou mais estável, a largura de banda foi utilizada de forma mais eficiente e os principais serviços da cooperativa puderam ser acessados com maior rapidez e confiabilidade. O ambiente de TI da empresa experimentou um aumento significativo na satisfação dos usuários e na produtividade geral dos funcionários, tornando-se mais adequado para atender às necessidades em constante evolução da cooperativa.

Com o objetivo de melhorar a eficiência da comunicação entre os diferentes setores da Cooperativa Odontológica do Estado do Amapá e garantir uma conexão estável com a internet, decidimos aplicar uma configuração de rota dinâmica no roteador MikroTik RB750GL. O Quadro 22 sintetiza o processo realizado:

Quadro 22 – Processo realizado para configurar a rota dinâmica

1. Acesso ao MikroTik RouterOS: Inicialmente, acessamos o MikroTik RouterOS através do WinBox utilizando as credenciais de administração.
2. Configuração de Interface de Rede: Na aba "Interfaces", verificamos quais interfaces estavam conectadas aos diferentes links de internet disponíveis na cooperativa. No nosso caso, identificamos duas interfaces: "WAN1" e "WAN2", que correspondiam a duas conexões de internet distintas fornecidas por provedores diferentes.
3. Configuração de Rotas: Na aba "IP", acessamos "Routes" e criamos uma nova rota de balanceamento de carga e redundância para as interfaces de internet disponíveis.
4. Criação da Rota Dinâmica: Para configurar uma rota dinâmica, atribuímos o valor "0.0.0.0/0" no campo "Dst. Address", indicando que essa rota abrange todos os destinos de IP. Em seguida, selecionamos as interfaces "WAN1" e "WAN2" no campo "Gateway", pois desejamos que o roteador balanceie o tráfego entre as duas conexões.
5. Configuração de Métricas: Definimos a métrica para cada rota para que o roteador saiba como distribuir o tráfego adequadamente. Atribuímos uma métrica menor à rota conectada ao link de internet de melhor desempenho e uma métrica maior à rota conectada ao link secundário. Dessa forma, o roteador encaminhará a maioria do tráfego para a interface com a métrica menor e, em caso de falha, redirecionará o tráfego para a outra interface.
6. Teste e Monitoramento: Após aplicar a configuração, realizamos testes para garantir que o balanceamento de carga e a redundância estavam funcionando conforme o esperado. Monitoramos a utilização de banda em cada interface e verificamos a troca automática entre as rotas em caso de falha em uma das conexões.

Fonte: Elaborado pelos acadêmicos (2023).

A rota dinâmica é um conceito utilizado em roteadores para permitir que as tabelas de roteamento sejam atualizadas automaticamente, sem a necessidade de intervenção manual por parte do administrador da rede. Em outras palavras, uma rota dinâmica é uma rota que é aprendida e atualizada automaticamente com base em informações trocadas entre roteadores vizinhos ou protocolos de roteamento.

A principal função da rota dinâmica é facilitar o encaminhamento de pacotes de dados entre redes diferentes. Quando um pacote chega a um roteador, ele precisa ser encaminhado para o destino correto. O roteador consulta sua tabela de roteamento para determinar qual é o próximo salto (próximo roteador) a ser usado para levar o pacote ao seu destino. Nesse processo, a rota dinâmica se torna relevante.

A rota dinâmica é utilizada em cenários onde a topologia da rede pode mudar com frequência, seja por adição ou remoção de roteadores, enlaces de rede ou falhas de conexão. Ao invés de ter que atualizar manualmente as tabelas de roteamento em cada roteador toda vez que houver uma mudança na rede, os roteadores que utilizam roteamento dinâmico trocam informações entre si para que todos tenham uma visão atualizada da topologia da rede.

Os protocolos de roteamento dinâmico, como o OSPF (Open Shortest Path First), RIP (Routing Information Protocol) e BGP (Border Gateway Protocol), são responsáveis por atualizar e propagar informações de roteamento através da rede, permitindo que os roteadores se adaptem às mudanças e encontrem os caminhos mais eficientes para o encaminhamento de pacotes.

A rota dinâmica é mais adequada em redes que possuem uma topologia complexa, com múltiplos roteadores interconectados, ou em ambientes onde a rede pode sofrer mudanças frequentes. Além disso, é uma opção recomendada quando a rede precisa de redundância e alta disponibilidade.

Com a implementação da rota dinâmica, a Cooperativa Odontológica do Estado do Amapá obteve diversos benefícios significativos:

a) **Balanceamento de Carga:** A distribuição do tráfego entre os dois links de internet resultou em um aproveitamento mais eficiente dos recursos disponíveis. Isso permitiu que a cooperativa utilizasse a largura de banda de forma equilibrada, evitando sobrecargas e melhorando a velocidade geral da conexão.

b) **Redundância:** Em caso de falha em um dos links de internet, o roteador automaticamente redirecionou o tráfego para a outra interface funcional. Essa redundância garantiu que a cooperativa continuasse com acesso à internet e aos serviços online mesmo diante de possíveis problemas em um dos provedores.

c) **Maior Confiabilidade:** A rota dinâmica proporcionou uma maior confiabilidade na conectividade, minimizando o tempo de inatividade e interrupções nos serviços. Isso foi especialmente importante para os setores que dependiam de acesso constante à internet e a sistemas online.

d) **Melhoria na Produtividade:** Com uma conexão mais estável e com balanceamento de carga eficiente, os colaboradores da cooperativa puderam realizar suas atividades com maior agilidade e produtividade, uma vez que não enfrentavam interrupções frequentes e lentidão na conexão.

Portanto, a configuração de rota dinâmica no roteador MikroTik RB750GL da Cooperativa Odontológica do Estado do Amapá resultou em uma rede mais resiliente, confiável e com melhor desempenho. Essa solução permitiu o aproveitamento máximo dos recursos de internet disponíveis, garantindo uma experiência de uso mais satisfatória para todos os usuários e contribuindo para o bom funcionamento dos serviços oferecidos pela cooperativa. A rota dinâmica é uma estratégia poderosa para otimizar o encaminhamento de pacotes em redes complexas e dinâmicas, proporcionando eficiência, flexibilidade e alta disponibilidade ao ambiente de rede.

Com o objetivo de melhorar a conectividade entre a rede interna da Cooperativa Odontológica do Estado do Amapá e um servidor específico localizado em uma rede externa, decidimos aplicar uma configuração de rota estática no roteador MikroTik RB750GL. O Quadro 23 mostra o processo realizado.

Quadro 23 – Processo realizado para configurar a rota estática

1. Acesso ao MikroTik RouterOS: Iniciamos acessando o MikroTik RouterOS através do WinBox com as credenciais de administração necessárias.
2. Identificação do Destino da Rota Estática: Identificamos o endereço IP do servidor externo que desejamos acessar a partir da rede interna da cooperativa.
3. Configuração da Rota Estática: Na aba "IP", acessamos "Routes" e criamos uma rota estática para o servidor externo.
4. Definição dos Parâmetros da Rota Estática: Para criar a rota estática, definimos o endereço IP do servidor externo no campo "Dst. Address" e, em "Gateway", inserimos o endereço IP do próximo salto para alcançar o servidor

externo. O próximo salto, nesse caso, é o endereço IP do roteador que faz a interconexão entre a rede interna da cooperativa e a rede externa.

5. Monitoramento e Verificação: Após aplicar a configuração, monitoramos a conectividade com o servidor externo para garantir que a rota estática estava funcionando corretamente. Realizamos testes de ping e acesso a serviços específicos hospedados no servidor externo para confirmar o sucesso da configuração.

Fonte: Elaborado pelos acadêmicos (2023).

A rota estática é um tipo de rota configurada manualmente pelo administrador da rede em um roteador, sem o uso de protocolos de roteamento dinâmico. Em outras palavras, é uma rota fixa que é inserida na tabela de roteamento do roteador de forma estática e não é atualizada automaticamente com base em informações de outros roteadores.

A função principal da rota estática é permitir que o administrador da rede tenha controle total sobre o encaminhamento de pacotes de dados em sua rede. Ao configurar rotas estáticas, o administrador determina explicitamente o caminho que o tráfego de dados seguirá para alcançar destinos específicos. Isso pode ser feito para diferentes finalidades, tais como:

A rota estática pode ser utilizada para criar conexões diretas entre redes ou dispositivos específicos, sem a necessidade de depender de rotas aprendidas dinamicamente. Em alguns casos, redes isoladas podem ser conectadas de forma controlada por rotas estáticas, permitindo comunicação entre elas sem expor toda a rede a roteamentos complexos ou potenciais ameaças.

Uma rota estática padrão (gateway padrão) é frequentemente utilizada para encaminhar todo o tráfego de uma rede local para a internet através de um roteador específico. Em cenários de balanceamento de carga, rotas estáticas podem ser configuradas para distribuir o tráfego entre múltiplos links de internet, sem a necessidade de usar protocolos de roteamento dinâmico.

A rota estática é indicada em alguns cenários específicos, tais como:

Em redes pequenas com poucos roteadores e topologia estável, rotas estáticas podem ser simples e eficientes para definir as conexões entre os dispositivos. Quando é necessário garantir que o tráfego siga um caminho específico para um destino determinado, as rotas estáticas permitem essa configuração exata.

Em ambientes onde a segurança é uma preocupação, a utilização de rotas estáticas pode ajudar a controlar o tráfego e evitar possíveis pontos de acesso não

autorizados. Em situações em que o roteamento dinâmico não é viável ou necessário, como redes com poucos dispositivos ou redes isoladas, as rotas estáticas podem ser uma escolha apropriada.

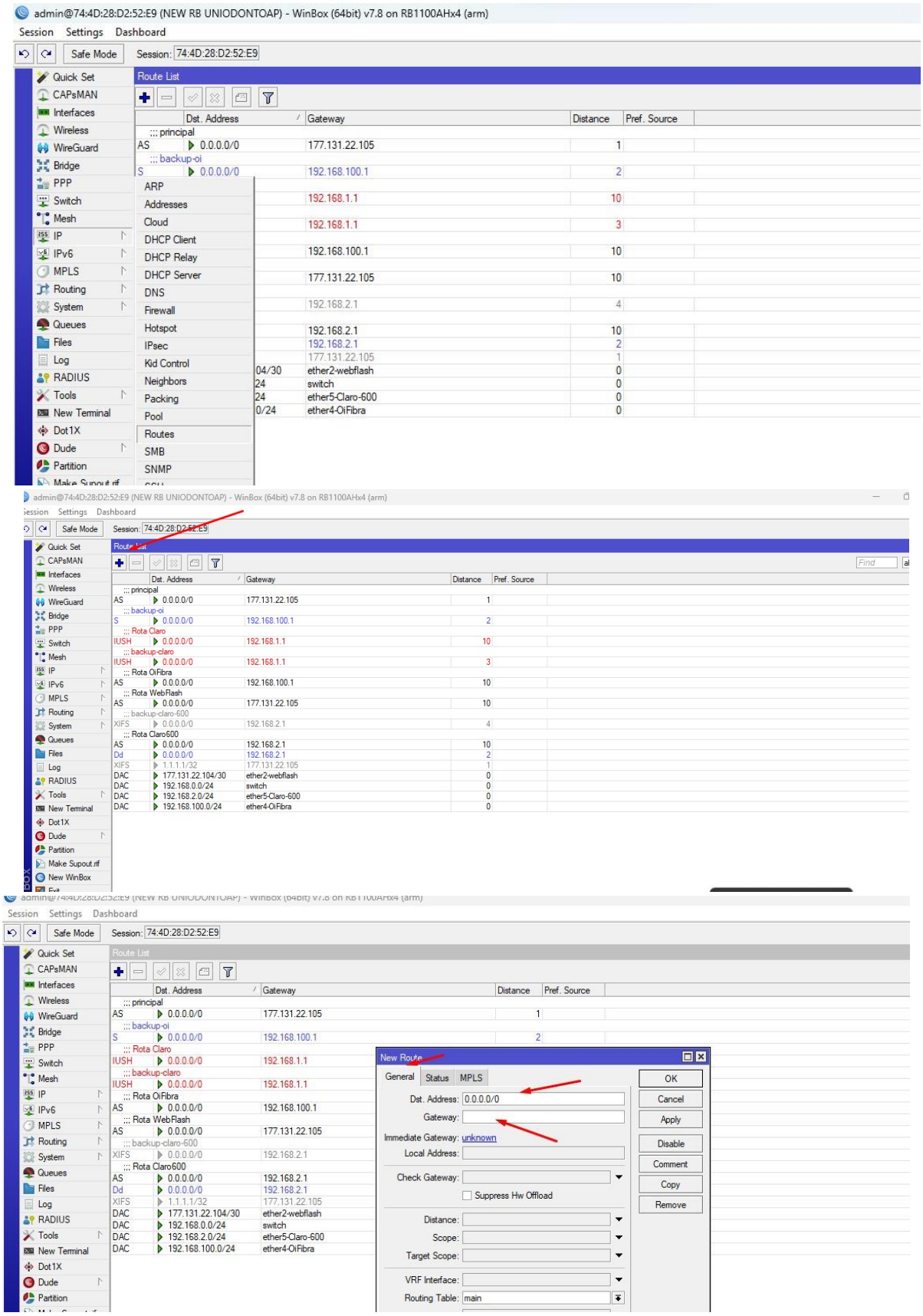
Por outro lado, a rota estática não é recomendada em redes complexas e dinâmicas, onde há muitos roteadores, links de internet ou onde a topologia pode mudar frequentemente. Nestes cenários, o uso de protocolos de roteamento dinâmico é mais indicado, pois eles permitem uma atualização automática e eficiente da tabela de roteamento conforme a rede evolui.

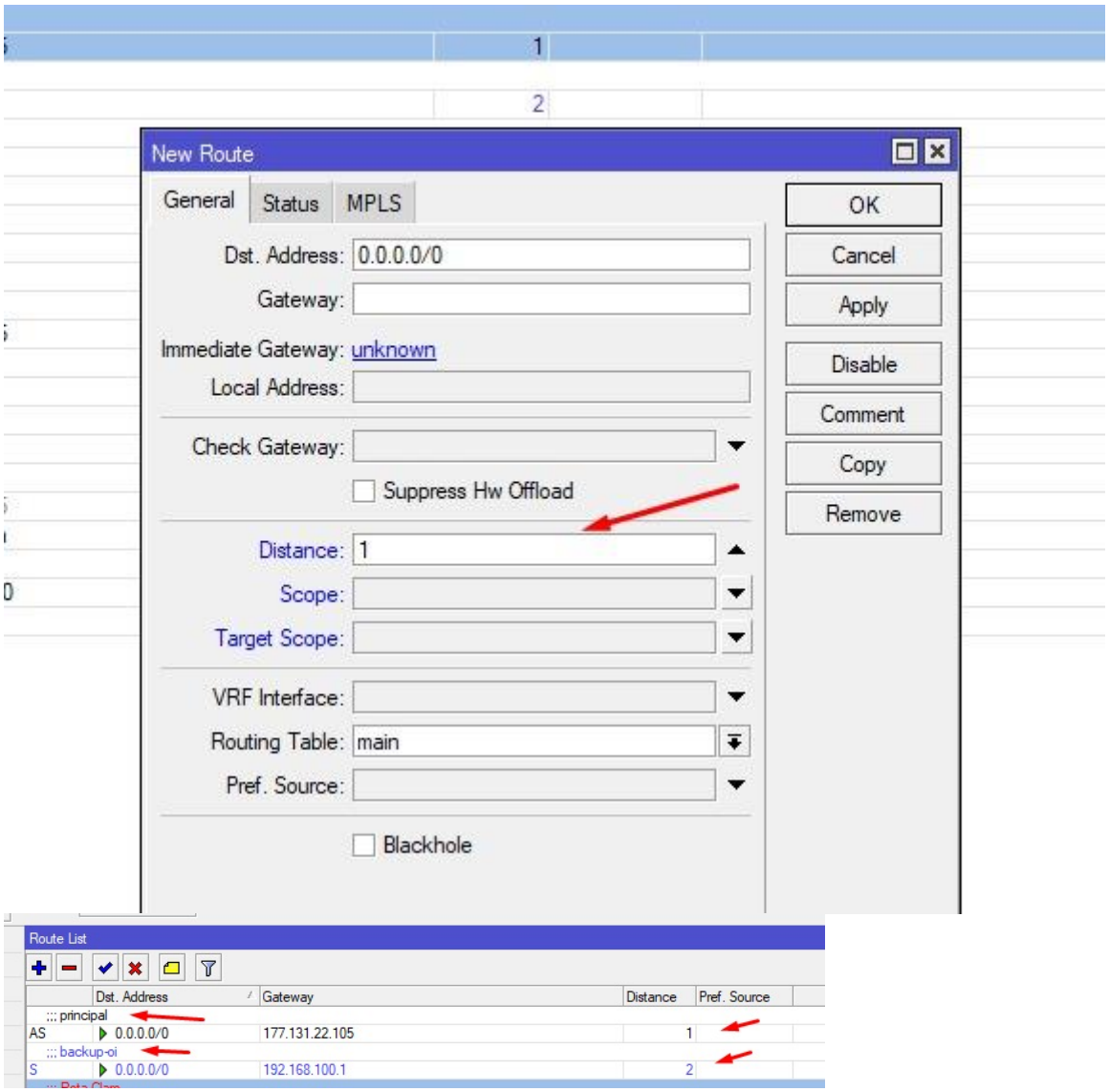
Com a implementação da rota estática, a Cooperativa Odontológica do Estado do Amapá alcançou diversos benefícios importantes:

a) **Conectividade Direta com o Servidor Externo:** A configuração de rota estática permitiu que os dispositivos da rede interna da cooperativa se comunicassem diretamente com o servidor externo, sem depender de roteamentos complexos ou da necessidade de consultas a outros roteadores intermediários.
b) **Acesso Rápido e Confiável ao Servidor:** Com a rota estática configurada, o acesso ao servidor externo tornou-se mais rápido e confiável, uma vez que o roteador agora possui um caminho definido e direto para o servidor, sem atrasos causados por cálculos de roteamento dinâmico.
c) **Melhoria no Desempenho e Latência:** Ao evitar roteamentos complexos e usar um caminho direto, a latência e o tempo de resposta para acessar serviços hospedados no servidor externo foram reduzidos, proporcionando uma melhor experiência de uso para os colaboradores da cooperativa.
d) **Maior Segurança e Controle:** A rota estática ofereceu maior controle sobre o tráfego entre a rede interna da cooperativa e o servidor externo. Essa configuração específica direcionou o tráfego apenas para o destino pretendido, reduzindo a exposição da rede a possíveis ameaças externas.

Verificamos que a configuração de rota estática no roteador MikroTik RB750GL proporcionou uma conexão mais direta, rápida e segura entre a rede interna da Cooperativa Odontológica do Estado do Amapá e um servidor externo específico. Isso resultou em melhorias significativas no desempenho, latência e experiência geral de uso, beneficiando diretamente os colaboradores da cooperativa em suas atividades diárias e garantindo maior controle sobre o tráfego de rede.

Figura 2 - Processo aplicado na interface do Mikrotik – configuração de uma Rota Estática





Fonte: Elaborado pelos acadêmicos (2023).

Após notarmos que a rede da Cooperativa Odontológica do Estado do Amapá estava enfrentando problemas de congestionamento e lentidão devido ao alto tráfego de dados, decidimos aplicar uma configuração de Load Balancing no roteador MikroTik RB750GL para otimizar o uso de múltiplas conexões de internet disponíveis, sendo mais uma camada de segurança para a rede. O Quadro 24 mostra o processo realizado:

Quadro 24 – Processo realizado para configurar o load balancing

1. Verificação das Interfaces de Rede: Iniciamos acessando o MikroTik RouterOS através do WinBox e verificamos quais interfaces de rede estavam conectadas aos diferentes links de internet disponíveis. Identificamos duas

interfaces: "WAN1" e "WAN2", que correspondiam a duas conexões de internet fornecidas por provedores distintos.

2. Configuração do Load Balancing: Acessamos a aba "IP" do menu lateral e clicamos em "Routes". Criamos duas rotas de Load Balancing, uma para cada interface de internet ("WAN1" e "WAN2").

3. Definição das Métricas: Para que o Load Balancing funcione adequadamente, atribuímos métricas iguais para ambas as rotas criadas. Isso garante que o tráfego seja distribuído de forma equilibrada entre as duas conexões de internet.

4. Seleção dos Gateways: No campo "Gateway", selecionamos as interfaces "WAN1" e "WAN2" para as rotas de Load Balancing. Dessa forma, o roteador saberá que deve distribuir o tráfego entre essas duas interfaces.

5. Monitoramento e Testes: Após a configuração, monitoramos o tráfego em cada interface e realizamos testes para garantir que o Load Balancing estava funcionando conforme o esperado. Verificamos a distribuição equitativa de carga entre as conexões de internet e testamos a tolerância a falhas, desconectando uma das interfaces para confirmar se o tráfego foi redirecionado adequadamente para a outra interface.

Fonte: Elaborado pelos acadêmicos (2023).

A função do Load Balancing, ou balanceamento de carga, é distribuir o tráfego de rede de forma equilibrada entre várias interfaces ou caminhos de rede. Essa técnica é aplicada para otimizar a utilização dos recursos disponíveis, aumentar a capacidade de tráfego e garantir maior disponibilidade e redundância na rede. O Load Balancing é utilizado em diversos cenários, especialmente quando existem múltiplas conexões de internet ou caminhos de rede disponíveis.

O Load Balancing é uma estratégia eficaz para otimizar o uso de recursos de rede, aumentar a capacidade, fornecer redundância e garantir uma distribuição equilibrada do tráfego. Ele é especialmente útil em cenários com várias conexões de internet, múltiplos servidores ou links WAN, onde o objetivo é melhorar o desempenho, a disponibilidade e a experiência do usuário.

Com a implementação do Load Balancing, a Cooperativa Odontológica do Estado do Amapá obteve resultados significativos:

a) **Otimização do Uso de Recursos:** O Load Balancing permitiu que a cooperativa utilizasse de forma mais eficiente as duas conexões de internet disponíveis. O tráfego de dados foi distribuído equitativamente entre as interfaces, evitando sobrecargas e gargalos em uma única conexão.

b) **Aumento da Capacidade de Banda:** Com a distribuição do tráfego entre duas conexões, a capacidade de banda total da rede foi aumentada, resultando em uma maior largura de banda disponível para os usuários.

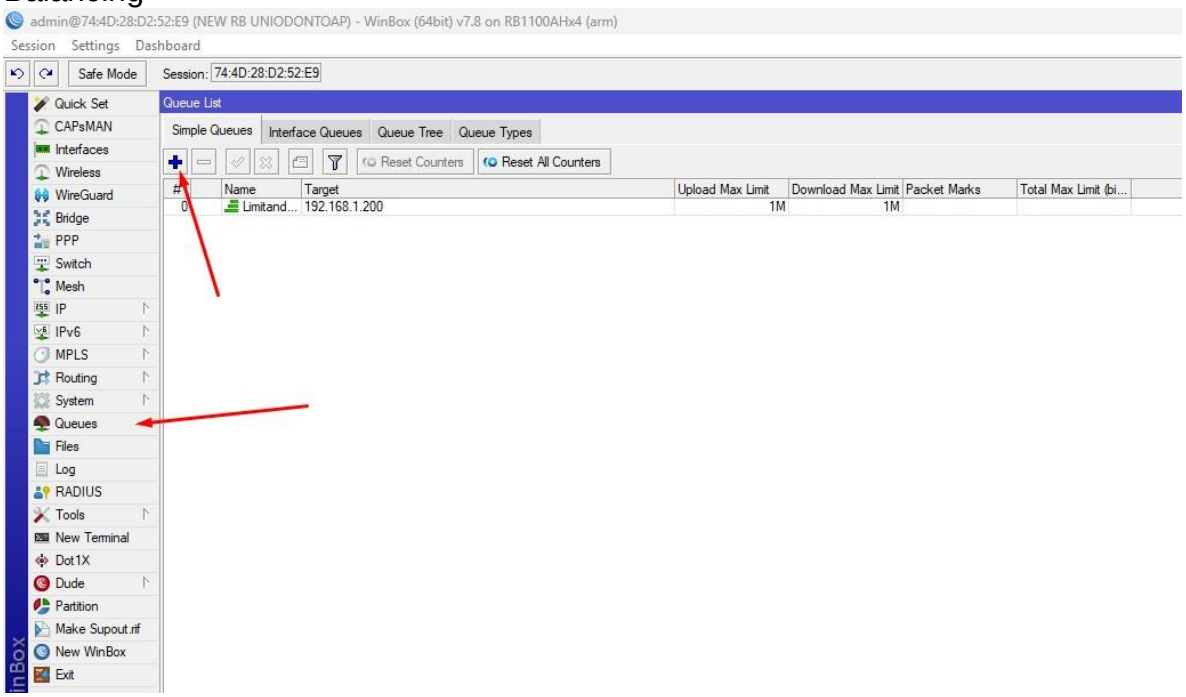
c) **Tolerância a Falhas:** O Load Balancing proporcionou redundância e tolerância a falhas. Em caso de falha em uma das conexões de internet, o tráfego foi redirecionado automaticamente para a outra interface funcional, garantindo a continuidade dos serviços e minimizando o tempo de inatividade.

d) **Melhoria na Experiência do Usuário:** Com uma maior capacidade de banda e distribuição equilibrada do tráfego, a experiência dos usuários melhorou significativamente. A navegação na internet, o acesso a sistemas online e o uso de aplicativos foram realizados com maior velocidade e menor latência.

e) **Redução de Custos:** Ao aproveitar ao máximo as conexões de internet existentes, a configuração de Load Balancing ajudou a cooperativa a otimizar seus recursos e evitar gastos desnecessários com a contratação de mais largura de banda.

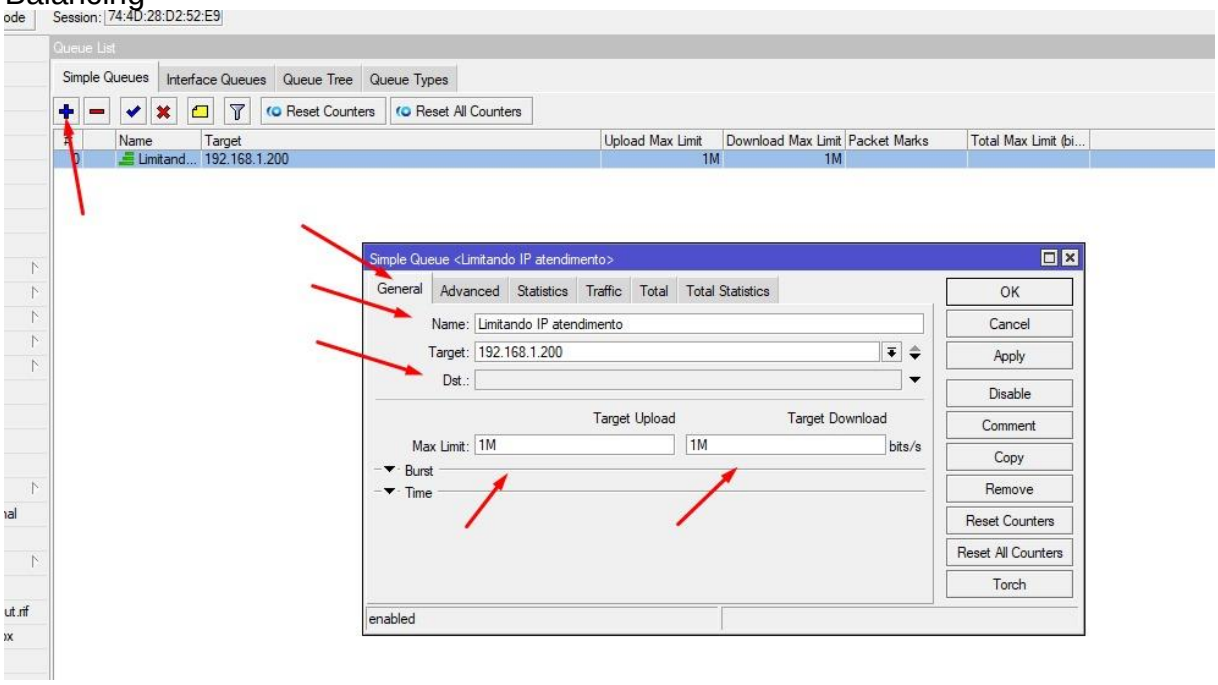
Verificamos que a configuração de Load Balancing no roteador MikroTik RB750GL da Cooperativa Odontológica do Estado do Amapá proporcionou uma melhor utilização dos recursos de internet disponíveis, aumentou a capacidade de banda, ofereceu maior redundância e melhorou a experiência geral dos usuários. Essa abordagem resultou em uma rede mais estável, eficiente e resiliente, permitindo que a cooperativa atendesse às demandas crescentes de conectividade de forma mais eficaz.

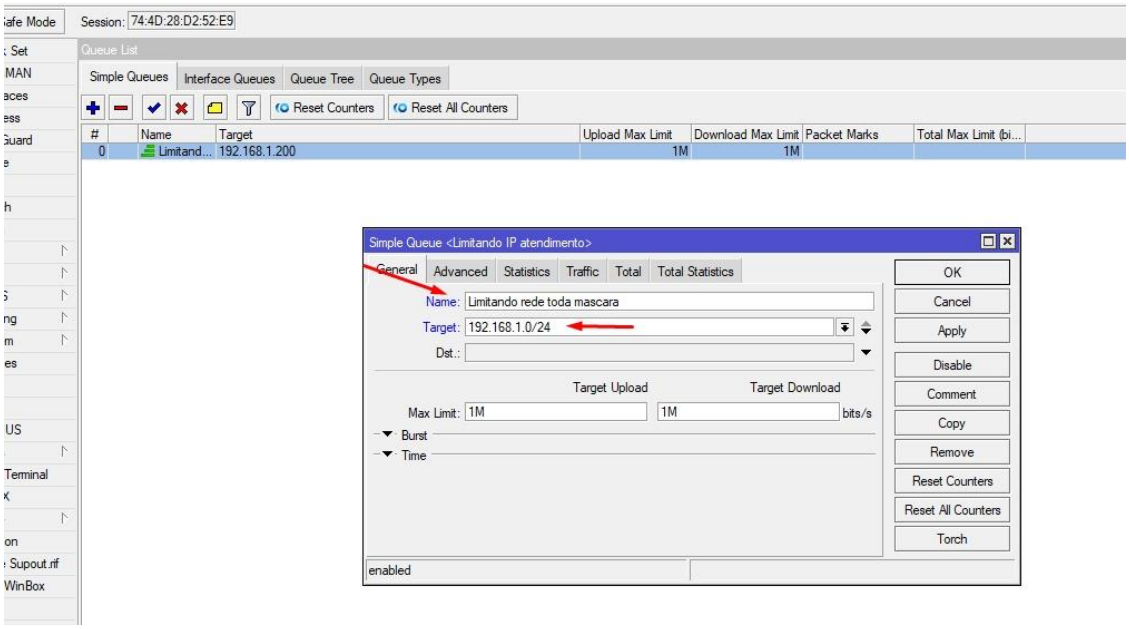
Figura 3 - Processo aplicado na interface do Mikrotik – configuração de Load Balancing



Fonte: Elaborado pelos acadêmicos (2023).

Figura 4 - Processo aplicado na interface do Mikrotik – configuração de Load Balancing





Fonte: Elaborado pelos acadêmicos (2023).

Diante da necessidade de garantir maior disponibilidade da conexão de internet na Cooperativa Odontológica do Estado do Amapá, decidimos aplicar uma configuração de Failover no roteador MikroTik RB750GL. O objetivo era garantir a continuidade dos serviços em caso de falha de uma das conexões de internet. O Quadro 25 demonstra o processo realizado:

Quadro 25 – Processo realizado para configurar o Fail Over

1. Verificação das Interfaces de Rede: Iniciamos acessando o MikroTik RouterOS através do WinBox e identificamos as duas interfaces de internet disponíveis: "WAN1" e "WAN2", fornecidas por provedores diferentes.
2. Configuração do Failover: Acessamos a aba "IP" do menu lateral e clicamos em "Routes". Criamos duas rotas de Failover, uma para cada interface de internet ("WAN1" e "WAN2").
3. Prioridade das Rotas: Atribuímos uma prioridade maior (menor valor de distância administrativa) para a rota da interface "WAN1", pois essa seria a conexão principal e preferencial. A rota da interface "WAN2" recebeu uma prioridade menor, tornando-a uma rota secundária.
4. Monitoramento das Conexões: Utilizamos a funcionalidade de monitoramento do MikroTik para verificar a disponibilidade das conexões de internet. Configuramos a ferramenta de ping para verificar periodicamente a conectividade com endereços externos, como servidores DNS ou outras referências confiáveis na internet.
5. Redirecionamento do Tráfego: Criamos uma regra de marcação de pacotes para identificar o tráfego proveniente da interface "WAN1" e atribuímos um valor específico a essa marcação. Em seguida, configuramos uma tabela de roteamento, especificando que o tráfego marcado com a interface "WAN1" deveria

seguir a rota principal. Para a interface "WAN2", não foi necessária nenhuma marcação, pois ela já estava configurada como rota secundária.

6. Falha na Conexão Primária: Para testar o Failover, desconectamos fisicamente a conexão da interface "WAN1". O roteador, ao detectar a falha através do monitoramento, automaticamente redirecionou o tráfego para a interface "WAN2".

Fonte: Elaborado pelos acadêmicos (2023).

A função do Fail Over é garantir a alta disponibilidade de conexões de rede ou serviços, de forma que, em caso de falha de um componente ou link principal, um backup seja ativado automaticamente para manter a continuidade das operações. O Fail Over é uma estratégia de contingência que busca minimizar o tempo de inatividade e as interrupções no acesso a serviços essenciais, assegurando que os sistemas permaneçam operacionais mesmo diante de eventos inesperados. O Fail Over é utilizado em várias situações em que a alta disponibilidade é essencial.

O Fail Over é uma estratégia importante para garantir a continuidade dos serviços e operações, minimizando o impacto de falhas e mantendo a disponibilidade dos recursos críticos. Ele é especialmente útil em ambientes onde a interrupção de serviços pode causar perdas financeiras, afetar a produtividade ou prejudicar a experiência do usuário. Ao utilizar o Failover, as organizações podem assegurar que seus sistemas estejam preparados para enfrentar falhas e problemas imprevistos, mantendo a confiança dos clientes e usuários.

A configuração de Fail Over trouxe resultados significativos para a Cooperativa Odontológica do Estado do Amapá:

a) **Maior Disponibilidade:** Com a configuração de Failover, a cooperativa garantiu maior disponibilidade da conexão de internet. Em caso de falha da conexão principal (interface "WAN1"), o tráfego foi redirecionado automaticamente para a conexão secundária (interface "WAN2"), garantindo a continuidade dos serviços e minimizando o tempo de inatividade.

b) **Redundância e Tolerância a Falhas:** A configuração de Failover proporcionou redundância à rede da cooperativa. A existência de uma conexão de backup (interface "WAN2") permitiu que a rede continuasse operacional mesmo em caso de falha da conexão principal.

c) **Melhoria na Experiência do Usuário:** Com a disponibilidade contínua da conexão de internet, os usuários da cooperativa experimentaram uma maior

estabilidade nas comunicações, acesso a sistemas online e serviços hospedados na internet.

d) **Segurança e Controle:** A configuração de Failover também proporcionou maior segurança e controle sobre o tráfego de internet. A rota principal (interface "WAN1") foi utilizada para o tráfego normal, enquanto a conexão secundária (interface "WAN2") ficou disponível somente quando necessário, garantindo o melhor uso dos recursos disponíveis.

e) **Redução de Impactos Financeiros:** Ao evitar períodos prolongados de inatividade, a configuração de Failover ajudou a cooperativa a evitar perdas financeiras associadas a serviços interrompidos e falta de conectividade.

Verificamos que a configuração de Fail Over no roteador MikroTik RB750GL da Cooperativa Odontológica do Estado do Amapá proporcionou maior disponibilidade da conexão de internet, redundância, estabilidade e segurança para a rede. Essa abordagem resultou em uma operação mais resiliente, garantindo que a cooperativa pudesse continuar atendendo seus pacientes e funcionando normalmente, mesmo em situações de falha da conexão principal.

Devido à necessidade de conectar de forma segura e eficiente filiais e colaboradores remotos à rede da Cooperativa Odontológica do Estado do Amapá, optamos por configurar um servidor VPN OpenVPN no roteador MikroTik RB750GL. O objetivo era permitir duas conexões distintas: uma conexão site-to-site para interligar as filiais e uma conexão client-to-site para que colaboradores pudessem acessar a rede interna remotamente. O Quadro 26 sintetiza o processo realizado:

Quadro 26 – Processo realizado para configuração VPN e conexões

1. Configuração do Servidor OpenVPN: Acessamos o MikroTik RouterOS através do WinBox e, na aba "PPP", selecionamos "Interface". Em seguida, configuramos o servidor OpenVPN, criando uma interface "OVPN-Server".
2. Geração das Chaves e Certificados: Para garantir a segurança da conexão VPN, geramos as chaves e certificados necessários para o servidor OpenVPN. Utilizamos a ferramenta de geração de chaves do MikroTik para criar o conjunto de chaves público e privado.
3. Configuração dos Parâmetros do Servidor: Definimos as configurações do servidor OpenVPN, incluindo o tipo de criptografia, o endereço IP local e a porta de escuta para conexões.
4. Configuração do Pool de IPs: Criamos um pool de IPs para atribuir aos clientes VPN. Definimos uma faixa de endereços IP que seria utilizada para alocar IPs aos dispositivos e colaboradores que se conectassem ao servidor VPN.

5. Criação de Perfis de Autenticação: Configuramos os perfis de autenticação para definir as políticas de segurança, como o tipo de autenticação (usuário/senha ou certificado) e as permissões de acesso.

6. Configuração da Conexão Site-to-Site: Para a conexão site-to-site, criamos uma interface "OVPN-Site" e configuramos os parâmetros de conexão, como o endereço IP e a porta do roteador remoto.

7. Configuração da Conexão Client-to-Site: Para a conexão client-to-site, orientamos os colaboradores remotos a baixarem o cliente OpenVPN em seus dispositivos. Fornecemos os certificados e as configurações necessárias para estabelecer a conexão com o servidor VPN.

8. Teste e Monitoramento: Após a configuração, realizamos testes para garantir que ambas as conexões (site-to-site e client-to-site) estivessem funcionando corretamente. Monitoramos a estabilidade das conexões e verificamos o tráfego através das interfaces VPN.

Fonte: Elaborado pelos acadêmicos (2023).

A função do Servidor VPN (Virtual Private Network) é criar uma conexão segura e criptografada entre dispositivos ou redes remotas, permitindo que usuários e filiais acessem recursos internos de uma rede privada como se estivessem fisicamente conectados a ela. A VPN estabelece um "túnel" seguro através de uma rede pública (como a internet) para proteger os dados transmitidos e garantir a privacidade e integridade das informações.

A conexão Site-to-Site é uma configuração de VPN em que duas ou mais redes locais (filiais ou escritórios) são interligadas através de uma rede pública (como a internet). Nesse cenário, os roteadores ou firewalls de cada filial atuam como gateways de VPN e estabelecem um túnel seguro entre si. Isso permite que os dispositivos de uma filial acessem os recursos de rede da outra filial, como servidores, impressoras e sistemas internos, como se estivessem na mesma rede local. Essa configuração é amplamente utilizada em empresas com várias filiais, facilitando o compartilhamento de recursos e informações de forma segura e eficiente.

A conexão Client-to-Site é uma configuração de VPN em que dispositivos individuais ou usuários remotos se conectam a uma rede privada de forma segura através de uma rede pública (como a internet). Nesse caso, o servidor VPN (que pode ser um roteador ou um servidor dedicado) atua como o ponto central da VPN, enquanto os dispositivos dos usuários (clientes) precisam de um software cliente VPN para se conectar à rede privada. Essa configuração permite que colaboradores remotos acessem recursos internos da empresa, como arquivos, aplicativos e

sistemas internos, de maneira segura e protegida, independentemente de sua localização física.

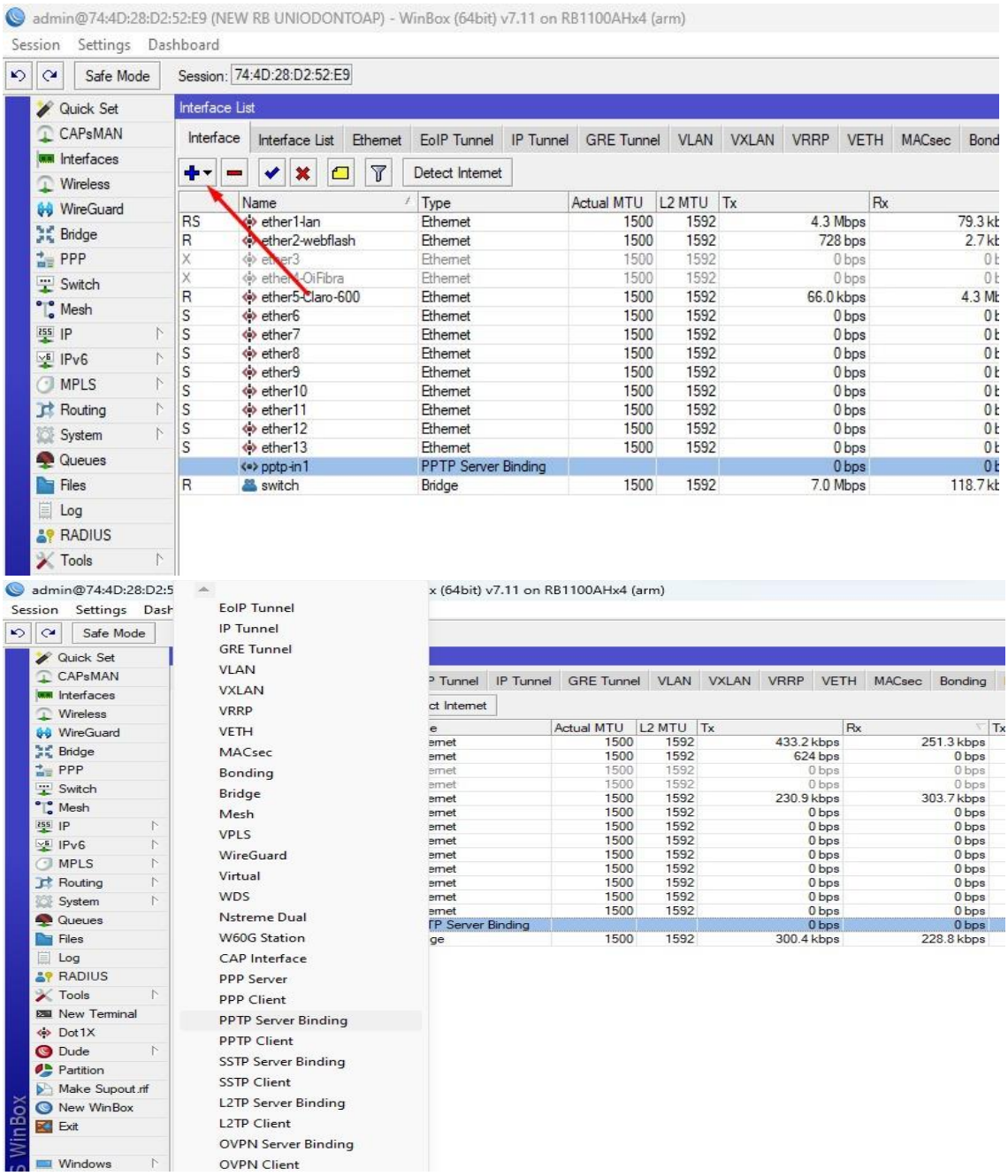
A VPN é utilizada em diversas situações em que a segurança e a privacidade das comunicações são fundamentais, ou quando é necessário estabelecer conexões entre redes ou dispositivos remotos de forma confiável. A VPN é uma solução versátil e segura que proporciona a interconexão de redes e dispositivos remotos de forma confiável e criptografada. Sua utilização é fundamental em ambientes corporativos para garantir a privacidade dos dados e permitir a conectividade segura de colaboradores e filiais, independentemente de sua localização física.

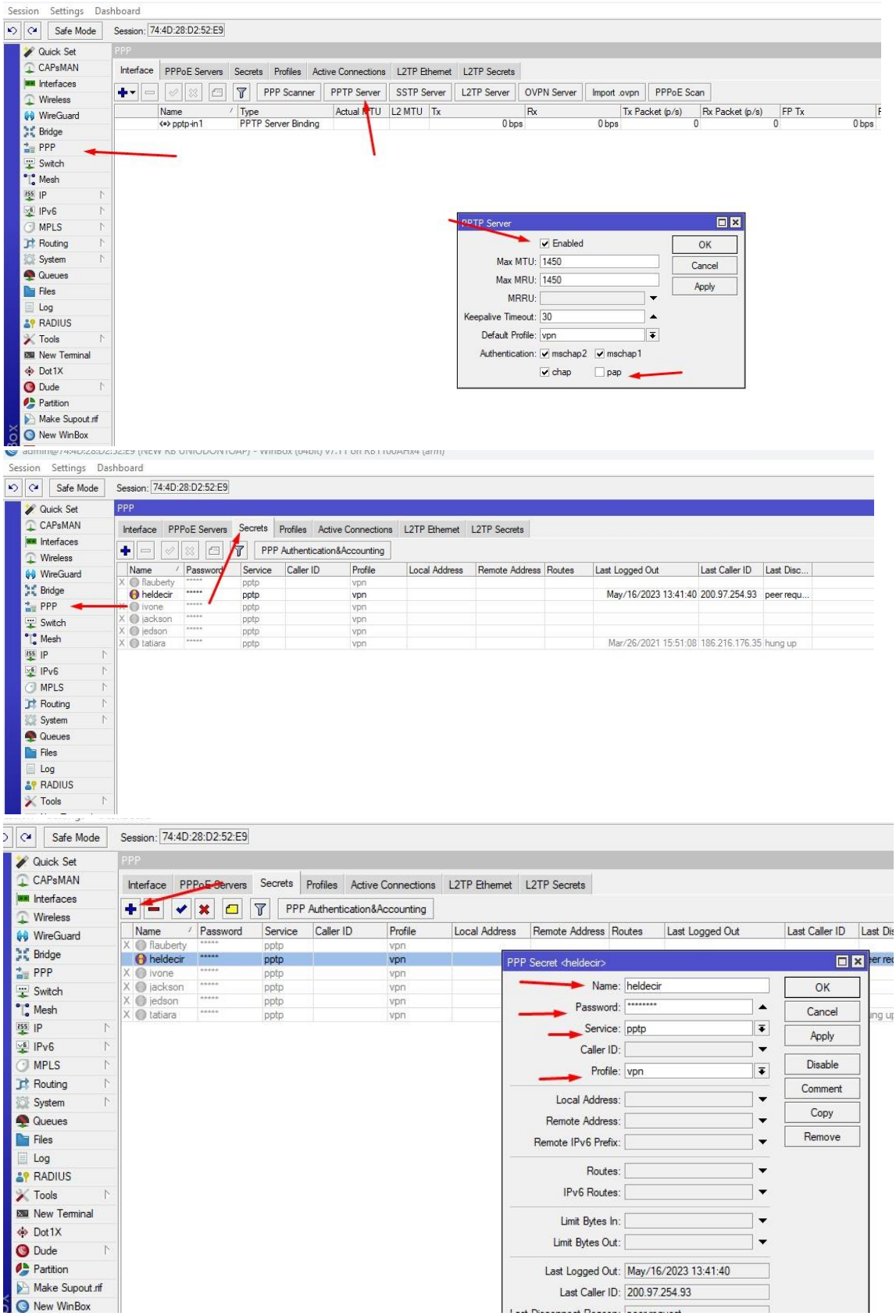
A configuração do servidor VPN OpenVPN trouxe resultados positivos para a Cooperativa Odontológica do Estado do Amapá:

a) **Conexão Segura e Criptografada:** Através da conexão VPN, as comunicações entre as filiais e colaboradores remotos e a rede da cooperativa foram protegidas por criptografia, garantindo a confidencialidade e integridade dos dados transmitidos.
b) **Acesso Remoto Simplificado:** Com a conexão client-to-site, os colaboradores remotos puderam acessar a rede interna da cooperativa de forma segura, como se estivessem fisicamente conectados à rede local, mesmo estando em locais remotos.
c) **Interligação de Filiais:** A conexão site-to-site possibilitou a interligação das filiais da cooperativa, permitindo o compartilhamento de recursos e informações entre elas de forma segura e eficiente.
d) **Aumento da Produtividade:** Com o acesso remoto simplificado, os colaboradores remotos tiveram maior flexibilidade e mobilidade, podendo acessar sistemas e dados da cooperativa a qualquer momento e de qualquer lugar, o que resultou em um aumento na produtividade.
e) **Economia de Custos:** A utilização da VPN OpenVPN proporcionou uma solução econômica em comparação com alternativas de conexão privada, pois não foi necessário investir em links de rede dedicados ou soluções proprietárias.
f) **Melhoria na Segurança:** A configuração do servidor VPN OpenVPN contribuiu para aumentar a segurança geral da rede da cooperativa, garantindo que o tráfego de dados entre filiais e colaboradores remotos estivesse protegido contra ameaças externas.

Verificamos que a configuração do servidor VPN OpenVPN no roteador MikroTik RB750GL proporcionou à Cooperativa Odontológica do Estado do Amapá uma solução segura, confiável e eficiente para conectar filiais e colaboradores remotos à rede interna. Com a implementação bem-sucedida do servidor VPN, a cooperativa conseguiu melhorar a comunicação e o acesso aos recursos da rede, resultando em maior produtividade, mobilidade e segurança para a organização.

Figura 5 - Processo aplicado na interface do Mikrotik – configuração de um Servidor VPN





Fonte: Elaborado pelos acadêmicos (2023).

5 CONSIDERAÇÕES FINAIS

A pesquisa sobre o gerenciamento de redes lógicas com roteadores MikroTik nas pequenas e médias empresas foi de extrema relevância para a resolução do problema levantado. Os objetivos geral e específicos estabelecidos foram cumpridos de forma eficiente, permitindo uma análise completa das funcionalidades desses roteadores e seu impacto nas redes da empresa pesquisada.

Os estudos realizados por Mosna e Moraes (2020), Leão (2017), Londoño Velásquez (2015) e Ribeiro (2016) ofereceram uma visão abrangente sobre o assunto, destacando pontos relevantes que podem ajudar as empresas a tomar decisões informadas sobre o uso desses roteadores em suas redes.

Identificou-se que os roteadores Mikrotik oferecem diversas funcionalidades avançadas que vão além do roteamento tradicional, como VPN, firewall, controle de banda e balanceamento de carga. Essa versatilidade permite que as empresas personalizem suas redes de acordo com suas necessidades específicas, otimizando o desempenho e a eficiência operacional.

Demostrou-se que a configuração adequada do QoS ajuda a evitar congestionamentos na rede, melhorar a produtividade, reduzir a latência e aumentar a satisfação geral dos usuários. A utilização dessas ferramentas permite uma melhor alocação dos recursos disponíveis e um controle mais apurado do tráfego, tornando-se fundamental para redes que oferecem serviços sensíveis à largura de banda.

Com relação à contribuição para a resolução do problema, a pesquisa identificou e detalhou as funcionalidades relevantes dos roteadores MikroTik para o gerenciamento de redes lógicas em pequenas e médias empresas. Os achados mais relevantes demonstraram que esses roteadores oferecem diversas vantagens para otimizar a eficiência operacional, melhorar a produtividade e aumentar a segurança das redes empresariais. Além disso, as funcionalidades de VPN, firewall, controle de banda e balanceamento de carga foram destacadas como ferramentas cruciais para alcançar um desempenho ideal.

Outro achado relevante foi a eficiência e escalabilidade das funcionalidades dos roteadores MikroTik, o que os torna uma solução sólida para atender às demandas crescentes de uma rede em constante crescimento. A capacidade de estabelecer conexões seguras entre diferentes locais e dispositivos remotos através

de VPN também foi destacada como uma forma de promover a colaboração e o compartilhamento de recursos.

Evidenciou-se que os roteadores MikroTik apresentam uma série de benefícios e vantagens para pequenas e médias empresas. Sua versatilidade, confiabilidade, recursos avançados, escalabilidade e interface de gerenciamento intuitiva tornam-nos uma solução ideal para melhorar a eficiência, a produtividade e a segurança das redes empresariais. A combinação com tecnologias de VPN permite o estabelecimento de conexões seguras entre diferentes locais e dispositivos remotos, promovendo a colaboração e o compartilhamento de recursos. Além disso, seu custo-benefício atrativo e a adoção de boas práticas de segurança reforçam o valor dos roteadores MikroTik como uma opção sólida para o crescimento e sucesso das empresas em um ambiente cada vez mais digital e competitivo.

Quanto ao impacto no processo de formação acadêmica, a pesquisa proporcionou uma oportunidade valiosa de aprofundar nossos conhecimentos em gerenciamento de redes e tecnologias avançadas de roteadores, como os da MikroTik. A análise e aplicação prática das funcionalidades desses dispositivos contribuíram para o desenvolvimento de habilidades de pesquisa, análise crítica e resolução de problemas complexos. Nos permitiu adquirir conhecimentos relevantes para o mercado de trabalho, já que as pequenas e médias empresas são um setor fundamental da economia e demandam profissionais capacitados para lidar com suas necessidades de gerenciamento de redes e infraestrutura de TI.

Finalmente, o gerenciamento de redes lógicas com roteadores MikroTik nas pequenas e médias empresas trouxe resultados significativos, contribuindo para a resolução do problema proposto, destacando as funcionalidades relevantes desses roteadores e proporcionando uma formação acadêmica enriquecedora para os estudantes envolvidos. Os achados reforçaram a importância desses dispositivos como uma opção sólida para otimizar o desempenho e a segurança das redes empresariais em um ambiente cada vez mais digital e competitivo.

REFERÊNCIAS

ABNT (Associação Brasileira de Normas Técnicas). **NBR ISO/IEC 27001:** Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

ARI MUZAKIR, A. **Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan,** 2022.

BOLANO, D. J. L.; LAPEZ, R. J. D. **Prácticas de calidad de servicio "QoS" en redes ip.** 2008.'

BRASILPEERINGFORUM. **Boas práticas de segurança para roteadores Mikrotik.** Disponível em: https://wiki.brasilpeeringforum.org/w/Boas_pr%C3%A1ticas_de_seguran%C3%A7a_para_roteadores_Mikrotik. Acesso em: 19 jul. 2023.

ENTELCO TELECOM. **Firewall MikroTik – Regras e Configurações. 2018.** Disponível em: https://www.entelco.com.br/blog/firewall-mikrotik-regras-e-configuracoes/. Acesso em: 25 jul. 2023.

FLEURY, M. T. L.; WERLANG, S. R.. **Pesquisa aplicada:** conceitos e abordagens. Anuário de Pesquisa GVPesquisa, 2016.

GAZOLA, R. **Failover de Links com roteador Mikrotik.** 2013.

KURNIA, D. Analisis Serangan DHCP Starvation Attack Pada Router OS Mikrotik. **Jurnal Ilmiah Core IT:** Community Research Information Technology, v. 8, n. 5, 2020.

LEÃO, J. A. Gestão de serviços de TI num provedor de acesso**. Governança de Tecnologia da Informação-Unisul Virtual,** 2017.

LEVY, G. Gerenciamento de uma rede pública utilizando a ferramenta Hotspot do Sistema Operacional RouterOS. **Voos Revista Polidisciplinar,** v. 7, n. 2, p. 133-152, 2020.

LONDOÑO VELÁSQUEZ, J. H. **Diseño de una red para la empresa compañía comercial universal Surtitodo sa basada en Mikrotik.** 2015.

MARCILLO, P. A.; BENITES, A. C. **Caso de estudio:** protegiendo la red con mikrotik de los ataques internos arp spoofing, mac flooding y dhcp spoofing, 2019.

MIKROTIK. **About us.** 2023. Disponível em: https://mikrotik.com/aboutus. Acesso em: 20 jul. 2023.

MOSNA, E.; MORAES, M. P. **Configuração de VPN site-to-site e client-to-site com OpenVPN e routerboard MikroTik.** 2020.

MOZUCO. V. **Curso completo de Mikrotik do básico ao avançado,** 2023. Disponível em: https://www.udemy.com/course/curso-completo-de-mikrotik-do-basico-ao-profissional/. Acesso em: 18 jul. 2023.

OLIVEIRA JUNIOR, C. E. P. et al. **Engenharia de tráfego aplicado à simulação de uma rede backbone de um provedor de internet regional utilizando o protocolo MPLS TE.** 2022.

PARANHOS, L. R. L; PARANHOS, P. J. R. **Metodologia da pesquisa aplicada à tecnologia.** São Paulo: SENAI-SP Editora, 2014.

RAHMAN, T.; SUMARNA, S.; NURDIN, H**.** Analisis performa routerOS mikrotik pada jaringan internet. **INOVTEK Polbeng-Seri Informatika,** v. 5, n. 1, p. 178-192, 2020.

RIBEIRO, R. M. O. **Utilização do sistema de roteamento Mikrotik para promover a segurança em rede de computadores com base nas diretrizes da ABNT NBR ISO/IEC 27001.** 2016.

SILVA, D. F. M. **Proposta para implantação de um modelo de autenticação de usuários em uma rede institucional.** 2017.

ZIBETI, L. H. **Implantação de roteador de baixo custo em microempresa.** 2015.

ANEXO A – GRUPO DE REGRAS FIREWALL

Criar as regras do firewall clique no botão "+" na janela "IP Firewall Rules" e insir os detalhes das regras uma por uma.

1. Regra para drop de conexões inválidas:
Chain: input
Action: drop
Comment: Drop All Invalid Connections
Connection State: invalid

2. Regra para permitir conexões estabelecidas:
Chain: input
Action: accept
Comment: Accept Established Connections
Connection State: established.

3. Regra para permitir conexões relacionadas:
Chain: input
Action: accept
Comment: Accept Related Connections
Connection State: related

4. Regra para permitir SSH:
Chain: input
Action: accept
Comment: Allow SSH
Protocol: tcp
Dst. Port: 22
In. Interface: ether1

5. Regra para permitir HTTP:
Chain: input
Action: accept
Comment: Allow HTTP
Protocol: tcp
Dst. Port: 80
In. Interface: ether1

6. Regra para permitir HTTPS:
Chain: input
Action: accept
Comment: Allow HTTPS
Protocol: tcp

Dst. Port: 443
In. Interface: ether1

7. Regra para permitir DNS UDP:

Chain: input
Action: accept
Comment: Allow DNS
Protocol: udp
Dst. Port: 53
In. Interface: ether1

8. Regra para permitir DNS TCP:
Chain: input
Action: accept
Comment: Allow DNS TCP
Protocol: tcp
Dst. Port: 53
In. Interface: ether1

9. Regra para bloquear todo o tráfego não especificado:
Chain: input
Action: drop
Comment: Drop All Other Traffic
In. Interface: ether1

Defina uma política padrão para encaminhamento do tráfego de saída

Clique na guia "Output" dentro da janela "IP Firewall Rules".
Clique no botão "+" e insira os seguintes detalhes:
Chain: output
Action: accept
Comment: Allow All Outbound Traffic
Out. Interface: ether1

Defina uma política padrão para o tráfego de encaminhamento entre interfaces locais

Clique na guia "Forward" dentro da janela "IP Firewall Rules".
Clique no botão "+" e insira os seguintes detalhes (se houver interfaces locais):
Chain: forward
Action: accept

Comment: Allow Local Traffic
Src. Interface: ether1
Dst. Interface: ether2 (substitua "ether2" pelo nome da interface local apropriada)

Verifique e aplique as alterações
Verifique todas as regras criadas para garantir que foram inseridas corretamente.
Clique no botão "Apply" para aplicar as configurações do firewall no roteador MikroTik.