UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

LUIZ HENRIQUE ZIBETI

IMPLANTAÇÃO DE ROTEADOR DE BAIXO CUSTO EM MICROEMPRESA

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO
2015

LUIZ HENRIQUE ZIBETI

IMPLANTAÇÃO DE ROTEADOR DE BAIXO CUSTO EM MICROEMPRESA

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Fábio Favarim.

PATO BRANCO
2015

TERMO DE APROVAÇÃO

Implantação de Roteador de Baixo Custo em Microempresa

por

Luiz Henrique Zibeti

Esta monografia foi apresentada às 19h00min do dia 26 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora

Prof. Dr. Fábio Favarim
Orientador / UTFPR-PB

Prof. M.Sc. Adriano Serckumecka
UTFPR-PB

Prof. Esp. Anderson Kiyoshi Yoshitome

Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

AGRADECIMENTOS

Agradeço ao meu orientador professor Dr. Fábio Favarim que me deu luz nos momentos difíceis, aos meus pais e amigos pelo apoio e compreensão e a empresa Leosoft pela oportunidade de implementação do trabalho.

A vingança nunca é plena, mata a alma e a envenena.

Seu Madruga

RESUMO

ZIBETI, Luiz Henrique. Implantação de roteador de baixo custo em microempresa. 2015. 72 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

A utilização da Internet é cada vez mais vital para o funcionamento de uma empresa. A necessidade de ferramentas que auxiliem o analista de redes no trabalho de gerenciar e controlar o uso de Internet está presente na maioria das empresas. Empresas de pequeno porte tendem a não investir no controle de sua rede de computadores, uma vez que os equipamentos específicos têm um valor elevado no ponto de vista dessas empresas, deixando a cargo do modem/roteador todo o gerenciamento de sua rede. Este trabalho propõe a utilização de roteadores compactos e de baixo custo, mais especificamente a série Routerboard da empresa Mikrotik, para gerenciar e controlar a rede de uma microempresa, retirando este trabalho do modem e dando liberdade ao analista de redes para fazer adaptações as suas necessidades.

Palavras-chave: Mikrotik. Routerboard. RouterOS. Gerenciamento de rede. Firewall.

ABSTRACT

ZIBETI, Luiz Henrique. Low cost router deployment in microenterprise. 2015. 72 pages. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

Internet usage is increasingly vital to the functioning of a company. The need for tools which helps the networking analyst at work to manage and control Internet use is present in most companies. Small companies tend not to invest in control of their computer network, since specific equipment have a high value in view of these companies, leaving to the modem / router all management of their network. This work proposes the use of compact routers and low cost, specifically the series Routerboard from Mikrotik company, to manage and control the network of a microenterprise, removing that work from modem and giving freedom to the network analyst to make adjustments to their needs.

Palavras-chave: Mikrotik. Routerboard. RouterOS. Network Management. Firewall.

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ADSL	*Asymmetric Digital Subscriber Line*
AP	*Access Point*
ARK	*Acknowledgment*
CIDR	*Classless Inter-Domain Routing*
DMZ	*Demilitarized Zone*
DPI	*Deep Packet Inspection*
EAP	*Extensible Authentication Protocol*
FTP	*File Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IP	*Internet Procotol*
IPS	*Intrusion Prevention Systems*
IPv4	*Internet Protocol* versão 4
IPv6	*Internet Protocol* versão 6
ISP	*Internet Service Provider*
HTTP	*Hypertext Transfer Protocol*
LAN	*Local Area Network*
LEAP	*Lighweight Extensible Authentication Protocol*
Mb	*Megabit*
MAC	*Media Access Control*
NAT	*Network Address Translation*
OSPF	*Open Shortest Path First*
QoS	*Quality of Service*
RAM	*Random Access Memory*
RDP	*Remote Desktop Protocol*
RFC	*Request for Comments*
RPC	*Remote Procedure Call*
SSH	*Secure Shell*
SYN	*Synchronize Sequence Numbers*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
WDS	*Wireless Distribution System*
WLAN	*Wireless Local Area Network*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Neste capitulo são apresentadas as considerações iniciais a respeito das redes de computadores, os objetivos e motivos que justificam este trabalho.

1.1 CONSIDERAÇÕES INICIAIS

A utilização da Internet é cada vez mais vital para o funcionamento de uma empresa. A necessidade de ferramentas que auxiliem o analista de redes no trabalho de gerenciar e controlar o uso de Internet está presente na maioria das empresas.

Esse gerenciamento pode ser feito através do uso de roteadores, *switches* gerenciáveis e servidores que controlam o fluxo de dados da rede, priorizando serviços e acessos.

Empresas de pequeno porte tendem a não investir no controle de sua rede de computadores, uma vez que os equipamentos específicos têm um valor elevado no ponto de vista dessas empresas, deixando a cargo do modem/roteador todo o gerenciamento de sua rede.

Uma alternativa de baixo custo é a utilização de dispositivos conhecidos como Routerboards, da empresa Mikrotik. As Routeboards consistem de um roteador compacto que pode ser adquirido com suporte a redes sem fio e que dá ao analista de redes funções de gerenciamento e controle como QoS, firewall, controle de banda, proxy, entre outras, de maneira simplificada, graças ao sistema operacional RouterOS que vem instalado nele.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Implementar um roteador de baixo custo para gerenciamento, organização e análise da rede em uma empresa de pequeno porte.

1.2.2 Objetivos Específicos

- Permitir maior controle ao analista de redes no gerenciamento da rede;
- Auxiliar o administrador na detecção de problemas no desempenho da rede;

• Permitir a utilização de mais de um link de Internet, caso a empresa possua, concomitantemente, provendo balanceamento de carga e tolerância a falhas das conexões com a Internet;

• Priorizar o tráfego de aplicações insensíveis ao atraso, como vídeo conferencia, voz sobre IP no acesso à Internet;

• Redirecionar portas externas para computadores e servidores internos da empresa;

• Auxiliar o administrador de rede na tomada de decisões para melhorias da rede, a partir de dados de utilização da mesma.

1.3 JUSTIFICATIVA

A necessidade de um maior controle na utilização da Internet e da rede na empresa exige a instalação equipamentos que permitam a implementação dessas necessidades.

O custo de equipamentos dedicados que permite se ter um melhor gerenciamento da utilização normalmente é elevado, sendo viável somente para empresas com maior porte. No entanto, existem equipamentos de baixo custo, com recursos mais limitados, mas que atendem as necessidades empresas de pequeno porte, auxiliando assim o analista de redes nas tomadas de decisões, gerando economia e evitando desperdício de recursos.

Neste sentido, este trabalho visa utilizar um desses equipamentos existentes e mostrar como este pode ser utilizado por pequenas empresas.

1.4 ESTRUTURA DO TRABALHO

Este texto está organizado em capítulos, dos quais este é o primeiro e apresentou a ideia do trabalho a ser desenvolvido, incluindo os objetivos e a justificativa.

O Capitulo 2, contém o embasamento teórico sobre roteadores, abordando o histórico e tipos de roteadores.

No Capítulo 3 estão os materiais e o método empregados no desenvolvimento deste trabalho.

No Capítulo 4, são demonstrados os resultados dos métodos utilizados no desenvolvimento deste trabalho, aonde as atividades realizadas são descritas e detalhadas de maneira a contextualizar o uso da tecnologia de informação na sequencial para reproduções futuras.

No Capítulo 5 está a conclusão com as considerações finais.

2 REFERENCIAL TEÓRICO

Nesse capítulo são apresentados alguns conceitos básicos relacionados a redes de computadores que são essenciais para o melhor entendimento deste trabalho. Em cada assunto é discorrido sobre alguns conceitos para fundamentar o uso de roteador em uma rede.

2.1 ENDEREÇAMENTO IP

O Protocolo da Internet, abreviado e tratado simplesmente como IP (*Internet Protocol)*, é um protocolo da camada de rede projetado para interligação de redes. Tanembaum (2003, p. 334) define a tarefa do IP como "fornecer a melhor forma possível (ou seja, sem garantias) de transportar datagramas[1] da origem para o destino, independente dessas máquinas estarem na mesma rede ou de haver outras redes entre elas".

Dentre os componentes que formam o protocolo IP, existem um em especial chamado endereçamento IP. O endereço IP é o número que identifica exclusivamente a interface de um dispositivo conectado à uma rede TCP/IP. É através deste número que é possível saber a origem e o destino de um pacote que trafega na rede.

O protocolo IP ainda utilizado hoje é a versão 4, também conhecida como IPv4, que consiste em endereços de 32bits, totalizando 4.294.967.296 endereços disponíveis. O endereço é escrito em forma decimal, sendo separado por ponto a cada 8 bits. Por exemplo, o endereço IPv4 192.168.1.5, o número 192 consiste nos 8 primeiros bits do endereço IP na forma decimal.

Os endereços IP podem ser divididos em endereços públicos e privados, sendo os endereços IP privados visíveis somente na rede interna e os endereços IP públicos visíveis por todas a Internet.

Como exemplo, na Figura 1 é possível observar que os equipamentos ligados ao modem com o endereço IP 192.168.1.X estão utilizando endereço IP privado, não ficando visíveis a rede externa.

O modem, por sua vez, possuí o endereço IP privado 192.168.1.1 (que faz a ligação com a rede interna) e o endereço IP externo 189.17.156.49 que é informado por toda a Internet.

[1] Denominação dada a um pacote de camada de rede.

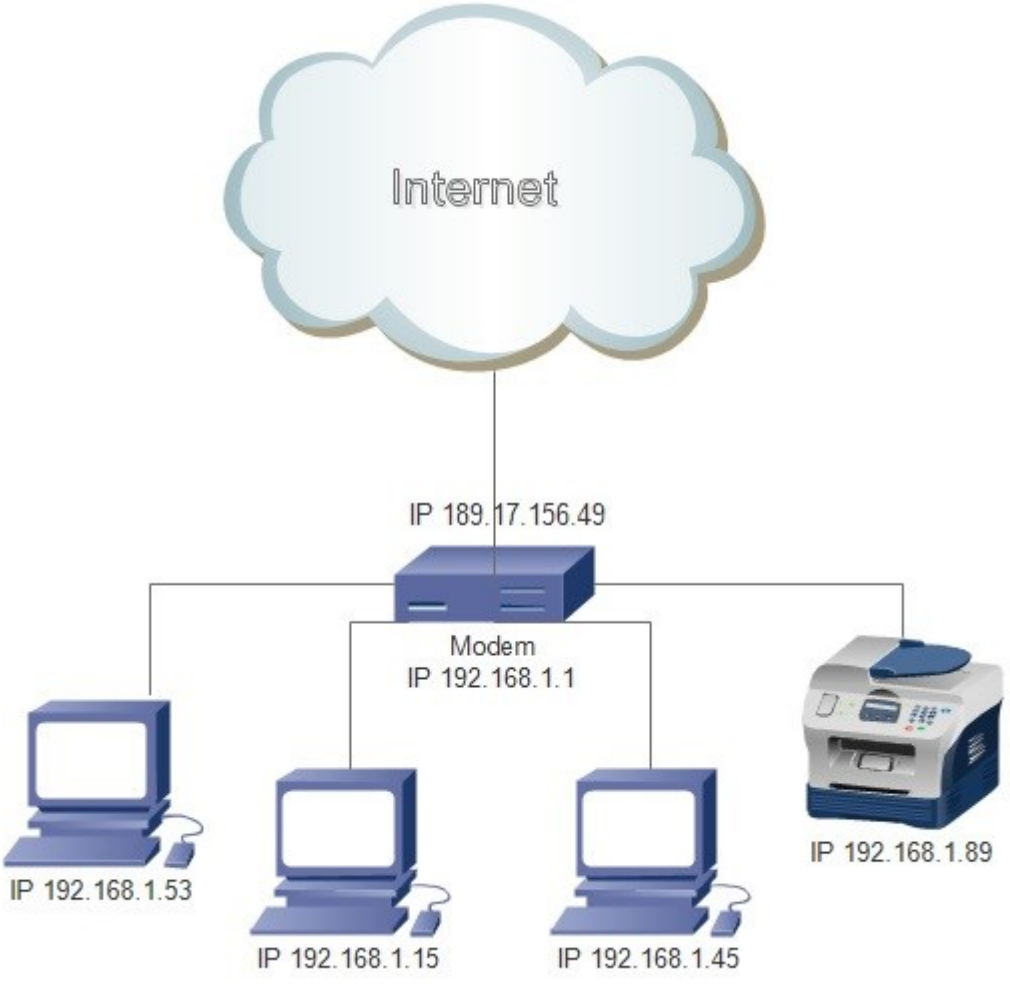

Figura 1 – Exemplo de endereçamento IP
Fonte: Autoria própria

É o enderenço IP externo que é informado aos servidores quando feito um acesso à Internet e é através dele que o os servidores externos conseguem enviar seus pacotes para os computadores presentes na rede interna.

Com o passar dos anos, a Internet se popularizou estando presente na maioria dos ambientes, corporativo e residencial, gerando assim um novo problema: a redução dos endereços IP públicos disponíveis.

Sendo o endereço IP público cada vez mais escasso, foi apresentado como solução a longo prazo, a versão 6 do protocolo IP, conhecida também como IPv6. O IPv6 tem endereços de 128 bits, enderençando até 340.282.366.920.938.463.463.374.607.431.768.211.456 dispositivos, o que é equivalente a 79 octilhões de vezes a quantidade de endereços IPv4.

2.2 ROTEAMENTO

O roteador é um dispositivo que conecta duas ou mais redes de computadores, encaminhando os pacotes de dados entre as redes. Kurose e Ross (2010, p.228) dizem que "roteamento envolve todos os roteadores de uma rede, cujas interações coletivas por meio do protocolo de roteamento determinam os caminhos que os pacotes percorrem em suas viagens do nó de origem ao nó de destino".

Quando um pacote de dados chega ao roteador, ele lê a informação de endereço de destino contida no pacote para determinar o seu destino final. O roteador verifica em sua tabela de roteamento a rede de destino do pacote, e direciona o pacote para o enlace que dá acesso à rede de destino, conforme visto na Figura 2.

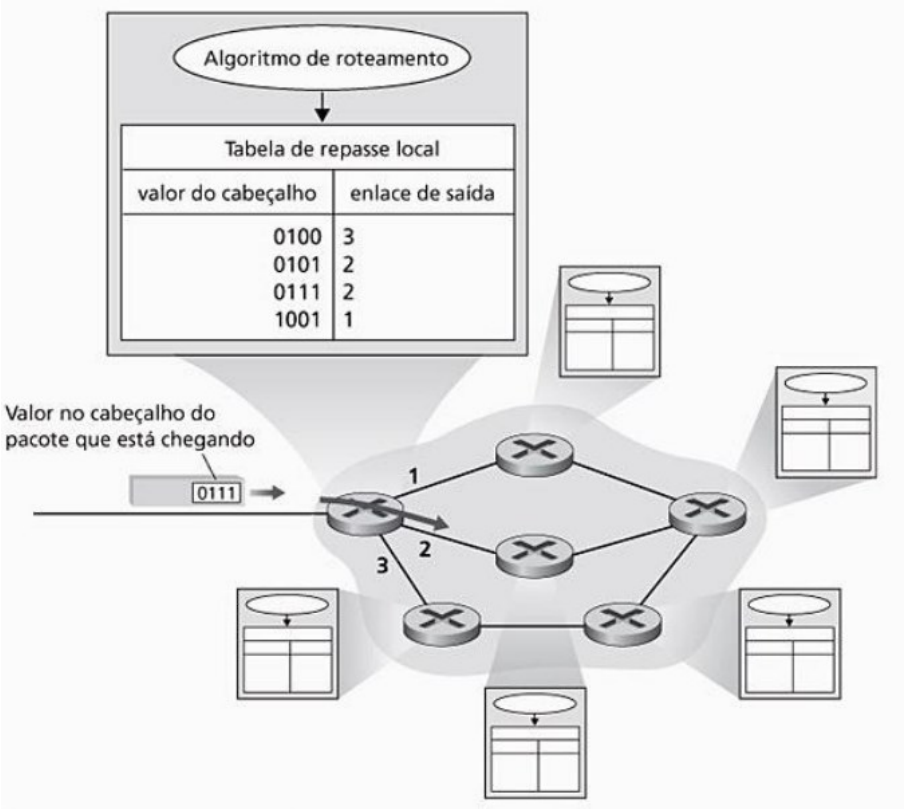

Figura 2 – Tabela de roteamento
Fonte: KUROSE; ROSS (2010, p. 231)

A tabela de roteamento consiste de uma tabela que contem basicamente a rede de destino e a informação do enlace que permite chegar até esse destino. O preenchimento dessa tabela pode ser realizado de forma estática ou dinâmica, sendo a forma estática preenchida manualmente pelo administrador e a dinâmica preenchida a partir de informações trocadas através dos protocolos de roteamento entre os roteadores.

2.2 NAT (NETWORK ADDRESS TRANSLATION)

A transição entre o protocolo IPv4 para o IPv6 tem se mostrado demorada e, como solução temporária, foi desenvolvido o NAT (*Network Address Translation*), descrita na RFC 3022.

Segundo Tanembaum (2003, p. 343), a ideia básica por trás do NAT é "atribuir a cada empresa um único endereço IP para tráfego da Internet. Dentro da empresa, todo computador obtém um endereço IP exclusivo, usado para roteamento de tráfego interno e quando um pacote sai da empresa e vai para o ISP, ocorre uma conversão de endereço".

Essa ideia é exemplificada na Figura 3, em que o endereço IP interno, também chamado de privado, 10.0.0.1, é convertido para o endereço IP externo, também conhecido como IP válido ou público, 198.60.42.12, através do NAT.

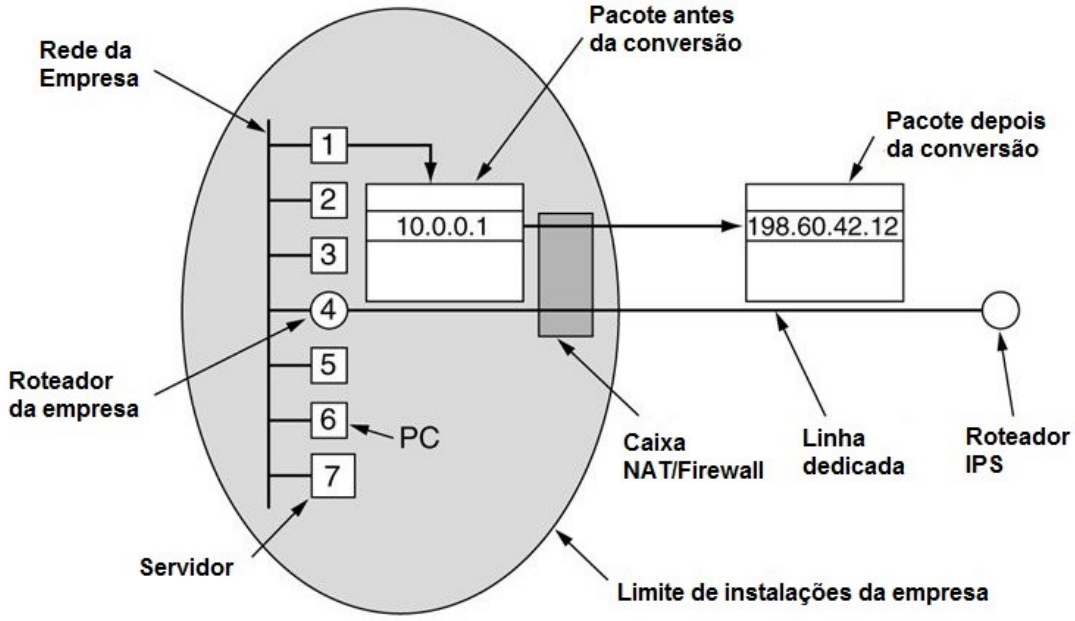

Figura 3 – Posicionamento e operação do NAT
Fonte: TANEMBAUM (2003, p.344)

Antes de converter o endereço IP privado em público, o NAT armazena a porta de origem e endereço IP original do pacote em uma tabela de conversão. Após, o NAT converte o endereço IP privado em público e substituí a porta de origem por um índice da tabela de conversão, recalculando o cabeçalho IP e o cabeçalho TCP e inserindo esses novos cabeçalhos no pacote.

Quando o NAT recebe do ISP um pacote, o campo de porta de origem do cabeçalho TCP é extraído e usado como índice na tabela de conversão. A partir da entrada localizada na tabela de conversão, o endereço IP interno e a porta de origem original são extraídos e inseridos no pacote. Os totais de verificação de IP e do TCP são recalculados, inseridos no pacote, e por fim, repassado ao roteador interno que entrega normalmente o pacote para o endereço IP interno.

2.3 FIREWALL

A conectividade que a Internet oferece abre brechas para ataques de pessoas mal-intencionadas, seja através de vírus ou força bruta, nos equipamentos ligados à rede de empresas e residências.

Uma maneira de contornar esse problema é através da implantação de firewall que é definido por Kurose e Ross (2010, p.535) como "uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros". A Figura 4 exemplifica esta definição, mostrando o firewall como uma parede que protege a rede interna da rede externa.

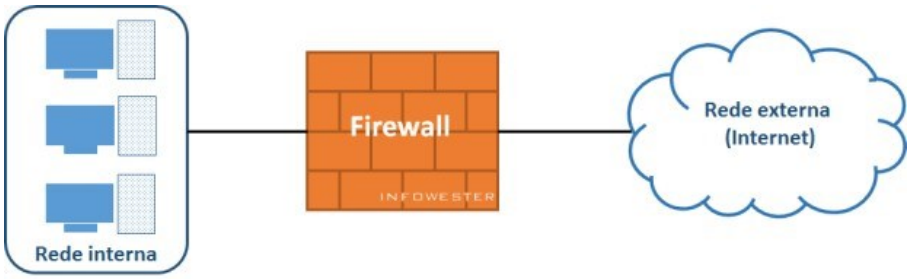

Figura 4 – Exemplo de firewall
Fonte: ALECRIM (2013)

O firewall pode ser implantado em software, rodando em um servidor, ou em hardware dedicado apenas para rodar o software do firewall.

Os firewalls de modo geral trabalham analisando os cabeçalhos do pacote e tomando decisões de acordo com as regras estabelecidas para liberar ou não o pacote, conforme pode ser visto na Figura 5.

Figura 5 – Exemplo de filtragem de pacotes
Fonte: ALECRIM (2013)

Kurose e Ross (2010, p. 536 e 357) dizem que as decisões de filtragem são normalmente baseadas em:

- Endereços IP de origem e destino;
- Tipo de protocolo no campo do datagrama IP: TCP, UDP, ICMP, OSPF, etc.;
- Portas TCP ou UDP de origem e de destino;
- *Flag* bits do TCP: SYN, ACK, etc;
- Tipo de mensagem ICMP;
- Conteúdo da mensagem enviada pelo usuário.

As decisões adotadas são aplicadas independentes do meio que o firewall é implantado, ele pode ser desenvolvido com metodologias diferentes baseados em diversos fatores como critérios do desenvolvedor, necessidades específicas de proteção, características do sistema operacional, estrutura de rede.

Os firewalls são classificados em diferentes tipos de acordo com as decisões de filtragem que são realizadas. A seguir são apresentados alguns tipos de firewall normalmente utilizados.

2.3.1 Filtragem de Pacotes

Os firewalls baseados em filtragem de pacotes, trabalham com uma metodologia mais simples e limitada, normalmente se limitando a analisar os endereços IP de origem e de destino, as portas de origem e de destino e os protocolos da camada de transporte.

Conexões baseadas no protocolo TCP/IP podem ser filtradas baseadas nas informações encontradas no cabeçalho do pacote como *flags,* protocolo, endereço de origem e destino e porta de origem e destino.

Conexões baseadas no protocolo UDP e ICMP trabalham de maneira diferente, sendo o filtro realizado no cabeçalho do protocolo UDP baseado na porta de origem e destino (uma vez que a conexão não é orientada) e no protocolo ICMP realizado com base nos tipos e códigos das mensagens.

Nakamura e Geus (2007, p. 215) dizem que "as regras dos filtros de pacotes são definidas de acordo com endereços IP ou com os serviços (portas TCP/UDP relacionadas) permitidos ou proibidos, e são estáticas, de modo que esse tipo de firewall é também conhecido como *static packet filtering*[2]".

Entre as vantagens de utilizar o firewall de filtragem de pacotes, Nakamura e Geus (2007, p. 216) citam:

- baixo *overhead*/alto desempenho da rede;
- barato, simples e flexível;
- bom para o gerenciamento de tráfego;
- transparente para o usuário.

Entre as desvantagens de utilizar o firewall de filtragem de pacotes, Nakamura e Geus (2007, p. 216) comentam:

- permite a conexão direta para *hosts* internos de clientes externos;
- difícil de gerenciar em ambientes complexos;
- vulnerável a ataques como IP *spoofing*[3];
- não oferece autenticação de usuário.

2.3.2 Filtragem de Pacotes com Estado

As filtragens do firewall podem ser divididas em estática e dinâmica, sendo as estáticas bloqueiam ou liberam os dados baseados nas regras, não importando a ligação entre os pacotes, e as dinâmicas consideram o contexto em que os pacotes estão inseridos para criar regras que se adaptam ao cenário.

Segundo Kurose e Ross (2010, p. 538) "em um filtro de pacote tradicional, as decisões de filtragem são feitas em cada pacote isolado. Os filtros de estado rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem".

---

[2] Filtragem de pacotes estáticos.
[3] Técnica que consiste em substituir o endereço IP do remetente de um pacote IP pelo endereço IP de uma outra máquina.

O firewall analisa os cabeçalhos dos pacotes, assim como na filtragem de pacote estático, e guarda os estados de cada conexão em uma tabela de estados, de maneira que seja possível identificar e prever as respostas legítimas, inibindo assim o trafego de pacotes ilegítimos.

> O firewall trabalha verificando somente o primeiro pacote de cada conexão, de acordo com as regras de filtragem. A tabela de conexões que contém informações sobre os estados das mesmas ganha uma entrada quando o pacote inicial é aceito, e os demais pacotes são filtrados utilizando-se as informações da tabela de estado. (NAKAMURA; GEUS, 2007, p. 217)

Ao iniciar uma conexão TCP usando um pacote SYN[4], ele é comparado com as regras presentes na tabela de regras do firewall e, se aceito, sua sessão será inserida na tabela de estados do firewall, conforme demonstrado na Figura 6.

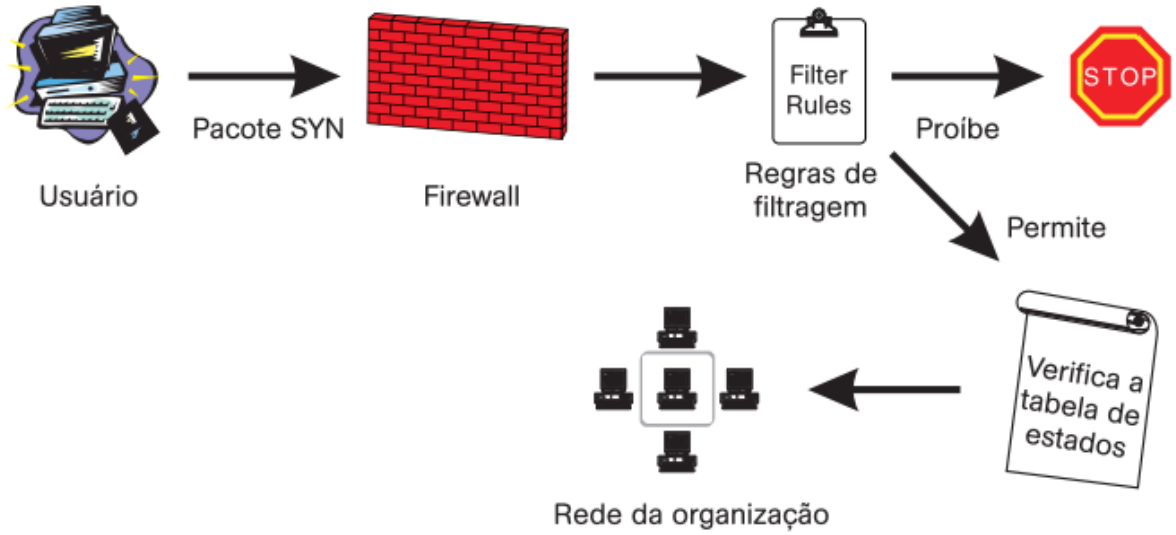

Figura 6 – Filtro de pacotes baseado em estados trabalhando na chegada de pacotes SYN
Fonte: NAKAMURA; GEUS (2007, p. 218)

Os demais pacotes da conexão, se a sessão estiver na tabela de estados e o pacote fizer parte dessa sessão, serão aceitos, não tendo necessidade de passar pela tabela de regras de filtragem.

Para os pacotes ACK[5], o firewall primeiramente verifica na tabela de estados a existência de uma sessão para esse pacote que, se for confirmada, será encaminhada diretamente para seu destino. Caso não existe sessão aberta, o pacote passa a ser analisado de acordo com a tabela de regras do firewall, demonstrado pela Figura 7.

---

[4] Pacote utilizado pelo protocolo TCP para iniciar uma conexão de um cliente a um servidor, solicitando a conexão.
[5] Pacote utilizado pelo protocolo TCP e enviado pelo cliente para confirmar ao servidor que a conexão foi aceita.

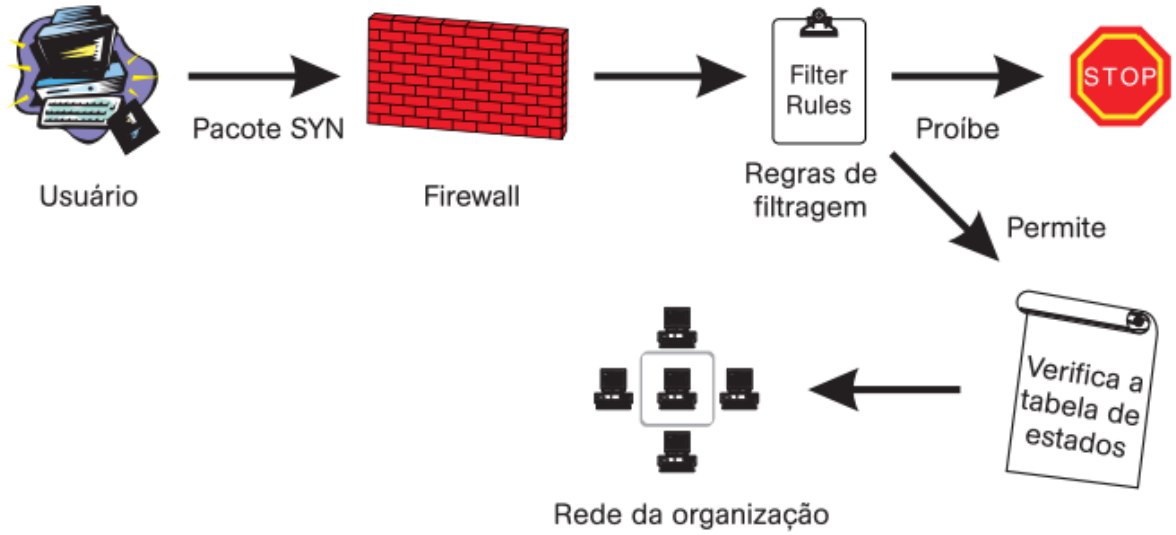

Figura 7 – Filtro de pacotes baseado em estados trabalhando na chegada de pacotes ACK
Fonte: NAKAMURA; GEUS (2007, p. 220)

É possível efetuar uma outra abordagem para os pacotes ACK, onde apenas os pacotes SYN podem iniciar uma conexão, tendo sua sessão inserida na tabela de estados, ficando os pacotes ACK filtrados apenas na tabela de estado (NAKAMURA; GEUS, 2007, p. 221).

As filtragens dos pacotes UDP e dos pacotes RPC (que utilizam alocação dinâmicas de portas) são feitas com o armazenamento dos dados de contexto por parte do firewall. Nakamura e Geus (2007, p. 221) explicam que com esse armazenamento de contexto, o firewall "pode manter uma conexão virtual das comunicações UDP ou RPC e, quando um pacote tenta entrar na rede, ele é verificado de acordo com a tabela de estados. Caso haja uma entrada na tabela dizendo que a sessão está pendente, o pacote é autorizado".

Como vantagem de utilizar o firewall de filtragem de pacotes com estado, Nakamura e Geus (2007, p. 222) citam:

- aberturas apenas temporárias no perímetro da rede;
- baixo *overhead*/alto desempenho da rede;
- aceita quase todos os tipos de serviço.

Entre as desvantagens, Nakamura e Geus (2007, p. 222) comentam:

- permite a conexão direta para *hosts* internos de clientes externos;
- não oferece autenticação de usuário.

2.3.3 Firewall de Aplicação

Também conhecido como gateway de aplicação, Kurose e Ross (2010, p. 539) definem como "um servidor específico de aplicação através do qual todos os dados da aplicação (que entram e que saem) devem passar. Vários gateways de aplicação podem executar no mesmo hospedeiro, mas cada gateway é um servidor separado, com seus próprios processos".

O firewall de aplicação recebe o fluxo de conexão, tratando as requisições como se fossem uma aplicação, originando um novo pedido sob sua responsabilidade para o servidor de destino. A resposta é recebida pelo gateway e analisada antes de ser entregue para o solicitante original.

Trabalhando em conjunto com o firewall de aplicação, existem os filtros de pacotes que podem fazer análises mais profundas ou superficiais nos pacotes, dependendo da tecnologia optada. Entre as tecnologias, a que mais se destaca é a *Deep Packet Inspection* (inspeção profunda de pacotes), abreviada por DPI.

A DPI além de analisar os campos feitos pelo firewall do tipo filtro de pacotes, também faz análise do conteúdo do pacote, isto é, dos dados do usuário. Esse tipo de firewall permite, por exemplo, bloquear o acesso a páginas que tenham determinadas palavras em seu conteúdo.

2.3.3.1 Proxy

Trabalhando em conjunto com o firewall, o proxy controla o acesso externo atuando como um intermediário entre o cliente, presente na rede interna, e o destino, presente na rede externa, que desejam se comunicar entre si, nunca permitindo uma conexão direta entre eles. Cada conexão entre os cliente-destino resulta em uma conexão entre o cliente e o servidor proxy e outra entre o servidor proxy e o destino.

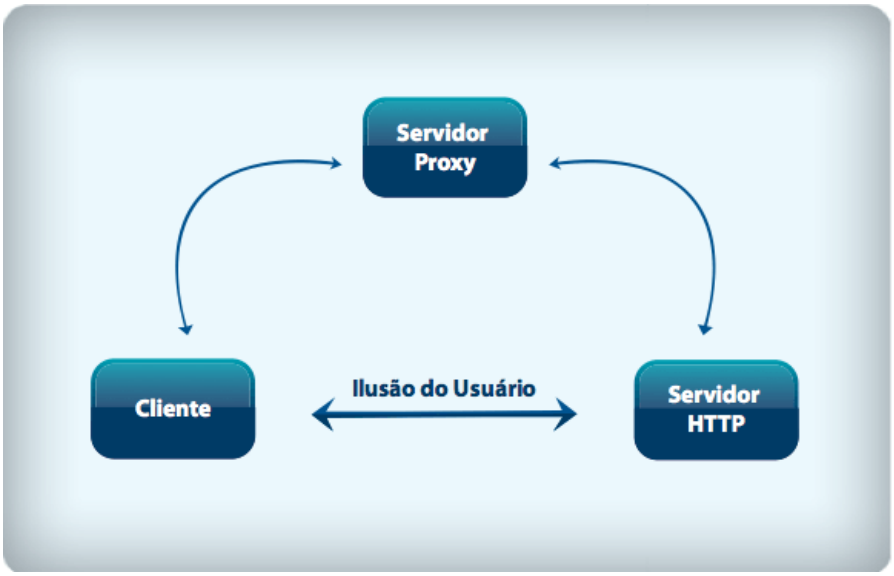

Figura 8 – Exemplificação de proxy
Fonte: MACÊDO (2012)

Como pode ser visto na Figura 8, o cliente tenta acessar o servidor HTTP sendo o seu pedido encaminhado primeiramente ao firewall. O servidor proxy verifica o pedido, inspeciona o pacote inteiro baseado nas regras configuradas pelo administrador, gera novamente o pedido e envia para o servidor HTTP. A resposta do servidor HTTP é recebida pelo servidor proxy que será analisada pelo firewall e, caso passe pelos filtros, ele constrói um pacote resposta, enviando para o cliente.

Além disso, o proxy pode melhorar o desempenho da rede através de cache de informações solicitadas, uma vez que, caso várias máquinas solicitem o mesmo dado, este já estará disponível no proxy.

Desta forma, Morimoto (2010) resume as vantagens de se usar um proxy nos seguintes itens:

- impõe restrições com base em horários, *login*, endereço IP e outras informações, além de bloquear páginas com conteúdo indesejados;
- funciona como um cache de páginas e arquivos, armazenando informações já acessadas. Ao acessar uma página que já foi apresentada, o proxy envia os dados que armazenou no cache;
- possibilita registrar todos os acessos (log) realizados através dele.

A utilização do proxy pode ser dividida em três métodos:

- Método da Conexão Direta. As informações como endereço e porta do servidor de proxy são configuradas diretamente no navegador do cliente.

- Método de proxy de Autenticação. Ao acessar algum serviço monitorado pelo proxy, o cliente é forçado a se identificar, autenticando seu acesso, ficando o acesso registrado e relacionado ao usuário;
- Método do Proxy Transparente. Todo o tráfego do cliente é analisado sem que o cliente tenha conhecimento da existência do servidor de proxy.

2.3.4 Firewall de Circuito

Segundo Stallings e Brown (2014, p. 273), o firewall de circuito "não permite conexão TCP fim a fim; em vez disso, o gateway estabelece duas conexões TCP, uma entre ele mesmo e um usuário TCP em uma estação interna e uma entre ele mesmo e um usuário TCP em uma estação externa", sendo que a estação externa enxerga apenas o firewall de circuito.

Ao solicitar a conexão, a estação interna conecta-se a uma porta TCP no firewall de circuito que, caso as regras de filtragem do firewall sejam atendidas, conecta-se com o destino que a estação interna deseja acessar através de uma outra conexão TCP. Após, o firewall de circuito repassa os dados de uma conexão para a outra, não verificando o seu conteúdo.

2.3.5 Arquiteturas de Firewall

O firewall pode ser aplicado de forma diferente em uma rede, atendendo as necessidades de um usuário ou empresa. A seguir, são apresentados alguns tipos de arquiteturas de firewall normalmente utilizados.

2.3.5.1 Dual-homed host

Formado por um equipamento que tem duas interfaces de rede, funciona como separador entre a rede interna e externa, torando-se um único ponto de falha uma vez que só este equipamento faz o papel de firewall na rede, conforme pode ser visto na Figura 9.

> Assim, as comunicações são realizadas por meio de proxies ou conexões em duas etapas, nas quais o usuário se conecta primeiramente ao *host dual-homed*, para depois se conectar ao servidor externo. Essa última abordagem causa problemas, principalmente para o usuário, pois o processo de acesso externo não é transparente, o que acaba influindo na produtividade dos usuários. (NAKAMURA; GEUS, 2007, p. 231)

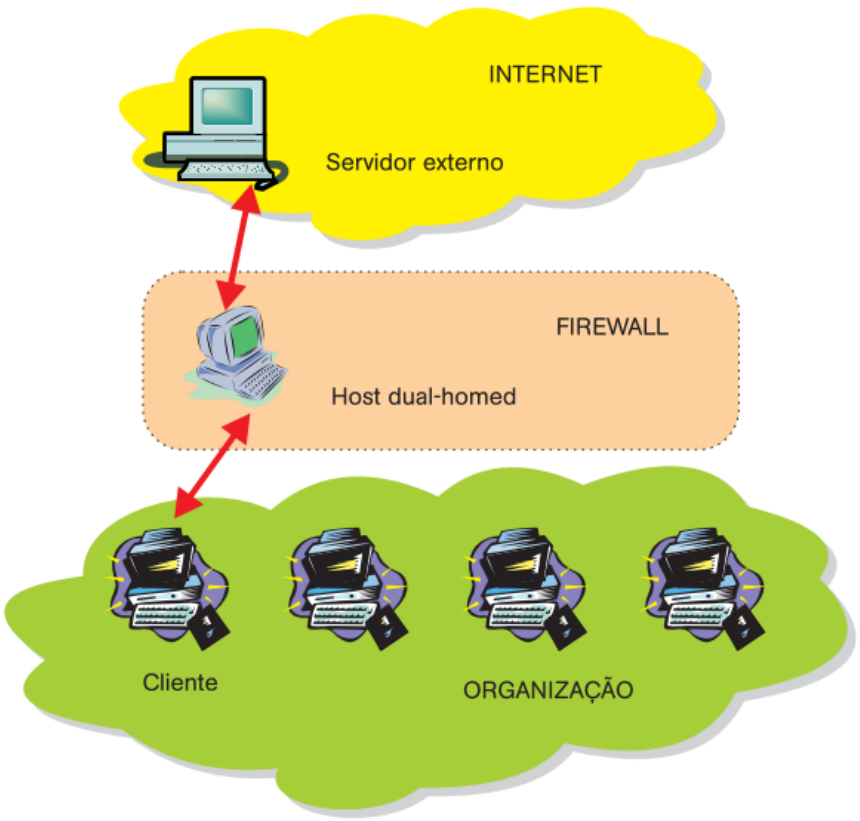

Figura 9 – Arquitetura *dual-homed host*
Fonte: NAKAMURA; GEUS (2007, p. 232)

Para Zwicky, Cooper e Chapman (2000, p. 83), esta arquitetura é indicada quando tráfico para a Internet é pequeno ou não é crítico para os negócios, nenhum serviço está sendo oferecido a usuários baseados na Internet ou a rede que está sendo protegida não contém dados extremamente valiosos.

2.3.5.2 Screened host

Não possuindo sub-rede de proteção, a arquitetura *screened host* trabalha com um filtro de pacotes e um *bastion host*. A rede protegida não possui acesso direto à rede externa e todo fluxo da rede passa pelo *bastion host* para depois seguir para o filtro de pacotes e, pôr fim, a rede externa. Por este motivo, o filtro de pacotes deve ter regras que permitam o trafego para a rede interna somente por meio do *bastion host*, demonstrado pela Figura 10.

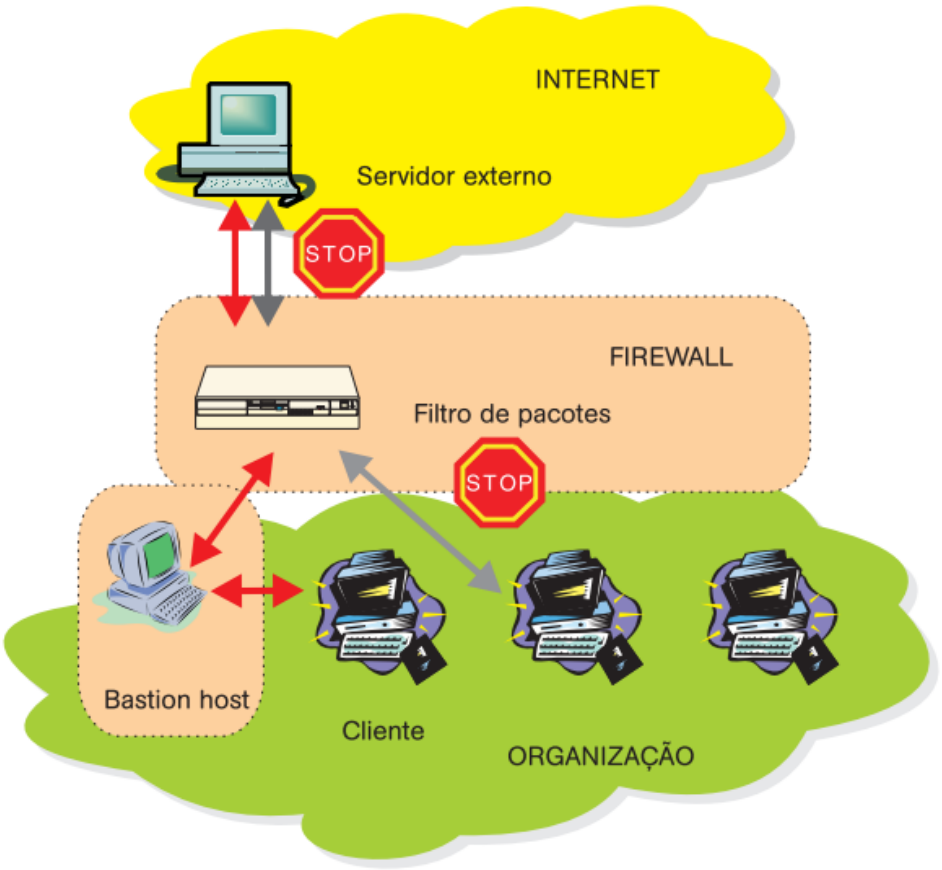

Figura 10 – Arquitetura *screened host*
Fonte: NAKAMURA; GEUS (2007, p. 233)

Pelo fato do *bastion host* residir na rede interna, se ele for comprometido o atacante terá acesso à rede interna além do fato que, caso o *bastion host* caia, várias funcionalidades da rede se perdem.

Zwicky, Cooper e Chapman (2000, p. 84) recomendam a utilização desta arquitetura quando há poucas conexões provenientes da Internet (não sendo adequada para casos onde a rede interna hospeda um servidor de *web* público) e quando a rede interna tem um nível relativamente elevado de segurança de *host.*

2.3.5.3 Screened Subnet

Apresentando múltiplos níveis de redundância, a arquitetura *screened subnet* é composta por filtros externos, *bastion hosts*, filtros internos, além de uma sub-rede intermediária chamada DMZ (*Demilitarized Zone*), como visto na Figura 11.

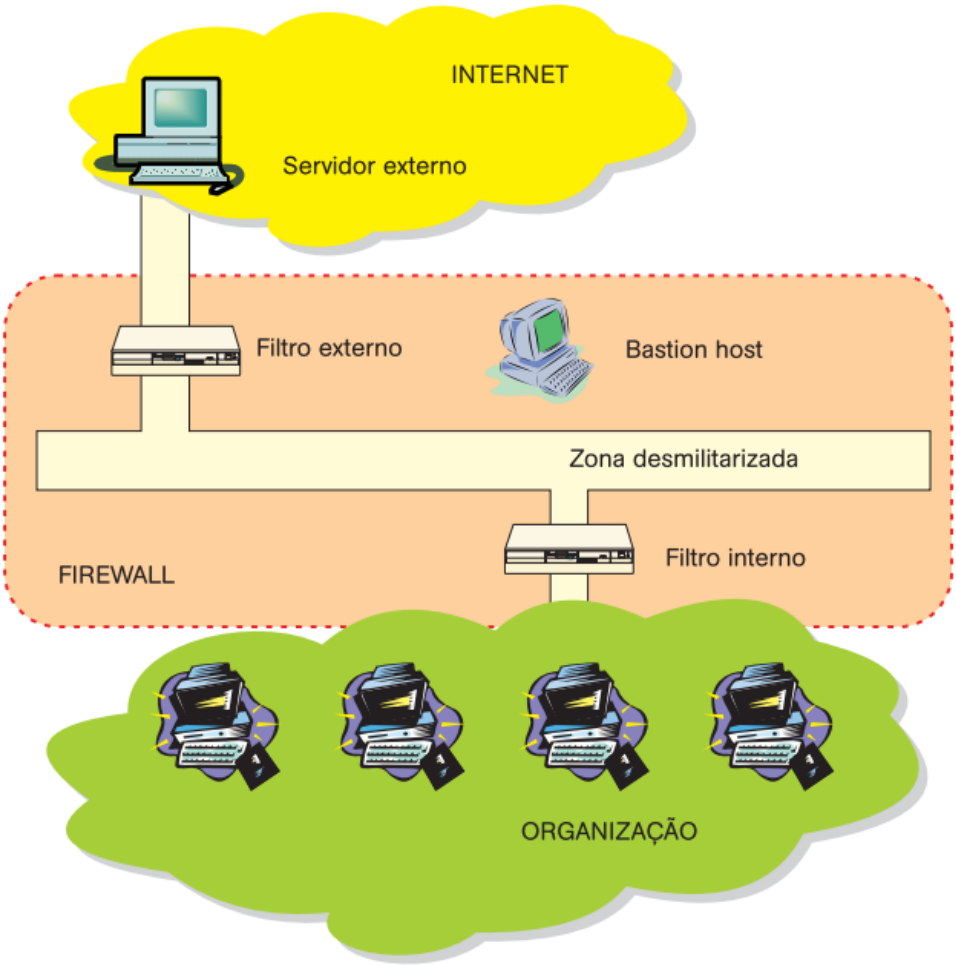

Figura 11 – Arquitetura *screened subnet*
Fonte: NAKAMURA; GEUS (2007, p. 233)

A DMZ é uma sub-rede que fica entre a rede externa e a rede interna, contém o *bastion host* proporcionando segurança a rede interna uma vez que somente a sub-rede DMZ é conhecida pela internet. Caso a rede DMZ sofra um ataque, a rede interna não será comprometida.

Nakamura e Geus (2007, p. 234) levantam um ponto importante sobre a arquitetura *screened subnet* referente a definição dos filtros internos e externos: “qualquer falha em sua definição ou implementação pode resultar em uma falsa sensação de segurança”.

Isto se dá uma vez que o filtro externo deve permitir o tráfego dos serviços disponíveis da DMZ, bem como o tráfego das requisições dos usuários internos enquanto o filtro interno deve permitir somente a passagem das requisições e respostas dos serviços permitidos para os usuários internos.

2.4 QoS - QUALIDADE DE SERVIÇOS

Qualidade de serviço (QoS) é a capacidade de melhorar os serviços trafegados na rede onde, segundo Tanenbaum (2003, p. 307), tem como características “quatro parâmetros principais: confiabilidade, retardo, flutuação e largura de banda”.

É feito um levantamento dos aplicativos que utilizam a rede e, baseado nos quatro parâmetros, é montado uma tabela de rigidez dos requisitos de qualidade de serviço (Quadro 1) e com isso definido as prioridades na implantação do QoS.

Aplicação	Confiabilidade	Retardo	Flutuação	Largura de Banda
Correio eletrônico	Alta	Baixa	Baixa	Baixa
Transferência de arquivos	Alta	Baixa	Baixa	Media
Acesso à Web	Alta	Media	Baixa	Media
***Login* remoto**	Alta	Media	Media	Baixa
Áudio por demanda	Baixa	Baixa	Alta	Media
Vídeo por demanda	Baixa	Baixa	Alta	Alta
Telefonia	Baixa	Alta	Alta	Baixa
Videoconferência	Baixa	Alta	Alta	Alta

Quadro 1 – Rigidez dos requisitos de QoS
Fonte: TANEMBAUM (2003, p.307)

A implantação é feita utilizando algoritmos e protocolos que otimizam a utilização da largura de banda das aplicações. Tanenbaum (2003, p. 308) explica que não existe “fórmula mágica” para alcançar o QoS com técnicas isoladas, mas em vez disso “foram desenvolvidas diversas técnicas, e as soluções práticas muitas vezes combinam várias dessas técnicas”.

Alguns exemplos de técnicas citados por Tanenbaum (2013) são:

- programação de pacotes;
- reserva de recursos;
- algoritmo do balde furado;
- moldagem de tráfego;
- armazenamento em buffers;
- superdimensionamento.

2.5 *HOTSPOT* E PROTOCOLO 802.1X

Hotspot é o termo utilizado para disponibilização de acesso à Internet através de uma rede sem fio com acesso temporário a visitantes, normalmente em local público e com grande movimento de pessoas, podendo ser oferecida de maneira gratuita ou paga.

Também existem aplicativos que transformam computadores, notebooks, tabletes e smartphones em servidores *hotspots* compartilhando o acesso à Internet pela interface de redes sem fio do aparelho.

O protocolo IEEE802.1x, conforme RFC 3580, é um protocolo padrão IEEE para controle de acesso de redes com base em portas envolvendo comunicação entre o requisitante, o autenticador e o servidor de autenticação.

Segundo Nakamura e Geus (2007, p. 162) "o padrão 802.1X provê um framework de arquitetura onde diferentes métodos de autenticação podem ser usados em diferentes redes, via uso do *Extensible Authentication Protocol* (EAP)".

O EAP possui alguns métodos que incluem a geração dinâmica de chaves e autenticação mútua entre clientes e pontos de acesso, na qual até mesmo certificados digitais podem ser usados.

Nakamura e Geus (2007, p. 163) citam alguns métodos EAP conhecidos:

- EAP-MD5;
- *Lighweight Extensible Authentication Protocol* (LEAP);
- EAP *Transport Layer Security* (EAP-TLS);
- EAP *Tunneled TLS* (EAP-TTLS);
- *Protected* EAP (PEAP).

3 MATERIAIS E MÉTODOS

Este capítulo apresenta o que foi utilizado e como foi feito para alcançar os objetivos do trabalho, sendo subdividido em duas seções: uma para os materiais e outra para o método.

3.1 MATERIAIS

Para desenvolvimento deste projeto foram utilizados um Routerboard modelo RB750 e um modelo RB750GL, desenvolvido pela Mikrotik com o sistema operacional RouterOS, também desenvolvido pela Mikrotik. Mikrotik é uma empresa fundada em 1996, na Letônia, que desenvolve equipamentos wireless e roteadores vendidos na maioria dos países. Em 2002, ela começou a desenvolver seu próprio hardware chamado Routerboard que é vendido com seu sistema operacional RouterOS instalado.

RouterOS é o sistema operacional baseado em Linux desenvolvido pela Mikrotik possuindo recursos como servidor de firewall, NAT, proxy, DHCP, QoS, roteamento, WDS e AP´s virtuais, *hotspot*, entre outros. Está presente nos Routerboards da Mikrotik e também pode ser instalado em microcomputadores e em outros sistemas embarcados com placas compactas SBC, sendo sua licença paga nesses casos. Neste trabalho, foi utilizada a versão 6.32.2 do RouterOS.

O Rouberboard RB750 é um roteador da Microtik que possuí 5 portas *Fast Ethernet*, um processador *single core* de 400MHz e 32MB de memória RAM. Ele é o roteador mais simples de sua família formada pelos Routerboards RB750G, RB750GL, RB750UP além do RB750. No Quadro 2, é possível verificar as maiores diferenças entre os modelos.

	RB750	**RB750G**	**RB750GL**	**RB750UP**
Processador	400 MHz	680 MHz	400 MHz	400 MHz
Memória RAM	32 MB	32 MB	64 MB	32 MB
Portas *Fast Ethernet*	5	0	0	5
Portas *Gigabit Ethernet*	0	5	5	0
Porta USB	0	0	0	1
Envia PoE	Não	Não	Não	Sim

Quadro 2 – Comparativo entre os modelos do Routerboard RB750
Fonte: Autoria própria

Foram utilizados dois links de Internet no balanceamento de carga e o link de contingência sendo o link principal uma fibra ótica de 150 Mb de *download* e 15 Mb de *upload* e como link secundário uma ADSL de 15 Mb de *download* e 1 Mb de *upload*.

O compartilhamento da rede ficou a cargo de dois *switches* da marca 3Com modelo 4200 *SuperStack* 3 com 48 portas *Fast Ethernet* e 2 portas *Gigabit Ethernet* cada. Para o compartilhamento via rede sem fio, foi utilizado um roteador marca Asus modelo RT-N56U com o seu servidor DHCP desativado para uso dos colaboradores e um roteador marca D-Link modelo DI-524 com seu servidor DHCP desativo para uso dos clientes da empresa, uma vez que todo o processo de DHCP é tratado pelo Routerboard RB750.

3.2 MÉTODO

A primeira etapa para o desenvolvimento deste trabalho foi a identificação das necessidades presentes em uma microempresa no gerenciamento de redes e o levantamento de requisitos que contemplem suas necessidades.

A segunda etapa foi o levantamento bibliográfico sobre roteamento, firewall, NAT, proxy, QoS, *hotspot* e protocolo 801.2x, através de sites e autores conhecedores dos assuntos, necessários para a implantação do projeto.

A terceira etapa foi o estudo dos equipamentos e da infraestrutura de rede bem como da quantidade de usuários e demandas de recursos utilizados pela microempresa.

A quarta etapa foi à configuração e instalação do Routerboard RB750 em um ambiente de teste dentro da microempresa.

A quinta etapa foi a implantação do projeto na microempresa, monitorando o seu funcionamento e corrigindo problemas que surgiram na implantação.

4 RESULTADOS E DISCUSSÃO

4.1 DESCRIÇÃO DA EMPRESA

A microempresa utilizada para implantação do projeto foi a Leosoft, uma empresa de desenvolvimento de softwares para cooperativas de crédito mutuo e rural, cooperativas de produção, financeiras e corretoras de seguro.

Localizada em Francisco Beltrão, no sudoeste do Estado do Paraná, a Leosoft foi fundada em 1995 e desenvolve seus sistemas nas linguagens de programação Delphi, Java e Ruby, tanto para desktop quanto para web.

Conta com quinze colaboradores, tendo uma estrutura de vinte computadores, dois servidores, impressoras, dois *switches Fast Ethernet* 48 portas, um roteador de rede sem fio e dois links de Internet, sendo um link de 150 Mb de *download* e 15 Mb de *upload* via fibra óptica e um link de 15 Mb de *download* e 5 Mb de *upload* via ADSL.

4.2 ESTRUTURA ATUAL

Os computadores de mesa e servidores se encontram conectados pela rede cabeada enquanto os notebooks utilizados pelos colaboradores estão conectados pela rede sem frio da empresa.

Internamente os servidores disponibilizam acesso a pastas compartilhadas e de teste de aplicações web, enquanto que externamente os servidores são acessados pelos clientes nos recursos de FTP e HTTP.

O link principal utilizado para conexão com a rede externa é o da fibra óptica, tendo os servidores de FTP e HTTP da empresa acessados por este link uma vez que ele está vinculado a um endereço IP global fixo.

A Internet é utilizada pelos colaboradores da empresa para envio e recebimento de código fonte no Github[6], atualização de sistemas web hospedados em servidores externos, atendimentos remotos, videoconferências e transferência de arquivos, além da navegação.

Para o acesso utilizando a rede sem fio é necessário que o endereço MAC[7] do dispositivo sem fio esteja devidamente cadastrado no roteador sem fio, além de informar uma senha para se conectar no roteador.

---

[6] Serviço de hospedagem de projetos que usam o controle de versionamento Git.
[7] Endereço físico relacionado à interface de rede sendo teoricamente único.

Essa prática gera um incomodo quando clientes visitam a empresa, uma vez que o analista de rede tem que cadastrar o endereço MAC do dispositivo do cliente e logo em seguida excluí-lo do roteador sem fio. Também tem o fato que o cliente, ao utilizar a rede sem fio, tem acesso aos servidores internos da empresa.

Todas as regras de firewall e redirecionamentos de portas bem como todo o gerenciamento da rede da empresa estão centralizadas no modem do link principal e mesmo tendo a disposição um link ADSL de 15Mb, este link secundário só é utilizado quando o link principal cai, sendo necessário o administrador de redes remover manualmente do *switch* o modem do link principal e colocar o modem do link secundário. A topologia de redes da empresa é exemplificada na Figura 12.

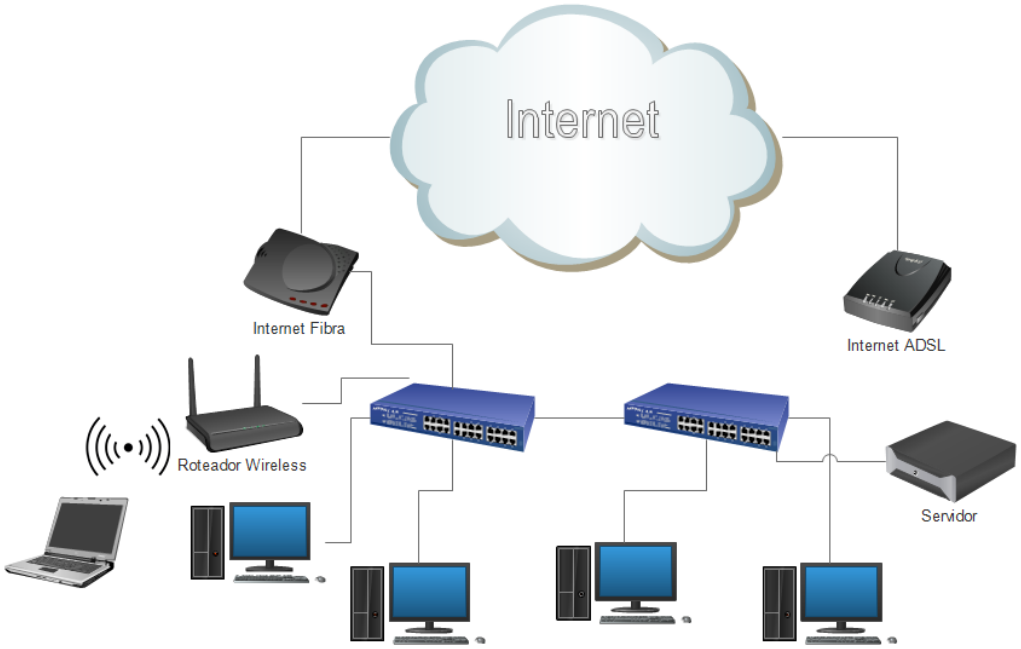

Figura 12 – Topologia atual
Fonte: Autoria própria

4.3 ESTRUTURA PROPOSTA

A proposta presente neste trabalho é remover do modem principal todo controle de rede e incorporá-lo em um roteador compacto, mais especificamente um roteador da marca Mikrotik, modelo Routerboard RB750, disponibilizado pela empresa.

O Routerboard RB750 ficará responsável pelo controle da rede fazendo o trabalho de roteamento, DHCP, firewall, NAT e proxy, sendo a topologia de rede proposta visível na Figura 13. Também será implementado QoS priorizando as videoconferências e os acessos remotos.

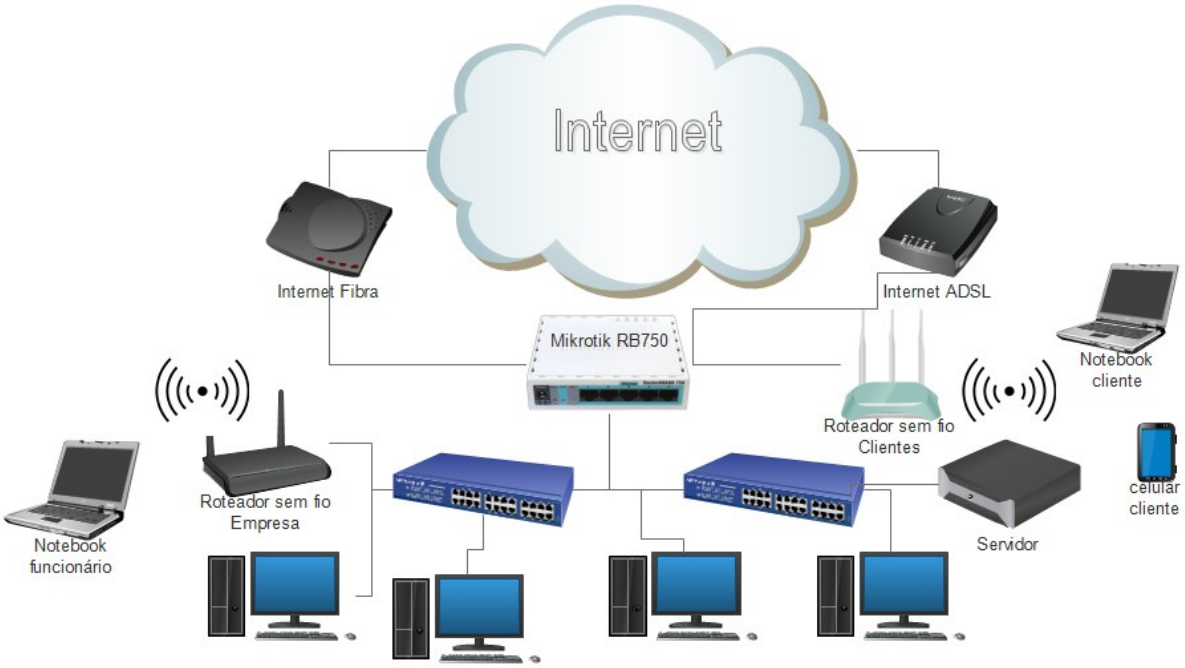

Figura 13 – Topologia proposta
Fonte: Autoria própria

Os dois links de Internet estarão conectados no Mikrotik ficando como link principal a conexão de fibra óptica e a conexão ADSL como link de *backup*, utilizada apenas quando o link principal ficar indisponível. Caso o link principal fique sobrecarregado, parte dos dados serão redirecionados para o link de backup.

Como a empresa possui um endereço IP global fixo vinculado a via fibra óptica e esse endereço IP está vinculado a um endereço eletrônico utilizado pelos seus clientes, caso o link principal caia, alguns serviços como FTP e HTTP ficarão indisponíveis para acesso externo.

O compartilhamento da rede será dividido em dois roteadores sem fio, o atual utilizado exclusivamente pelos colaboradores da empresa e o novo utilizado exclusivamente para clientes.

Enquanto o roteador sem fio utilizado pelos colaboradores precisará de senha para efetuar a conexão e o endereço MAC cadastrado e terá acesso a rede interna da microempresa, o roteador usado pelos clientes só necessitará de senha para conexão e não conseguirá encontrar a rede interna.

4.4 IMPLEMENTAÇÃO

Antes de iniciar o desenvolvimento do projeto, é necessário efetuar a limpeza das configurações do Routerboard RB750, garantindo assim que não existam outras configurações além do padrão. É importante considerar que todos os procedimentos foram feitos com a versão 6.32.2 do RouterOS através do programa Winbox.

O programa Winbox é um software desenvolvido e distribuído pela Mikrotik, rodando em plataforma Windows, utilizado para configuração do Routerboard. É através desse programa que as configurações deste projeto foram executadas.

4.4.1 Winbox

Através do Winbox é possível conectar no Routerboard através do endereço de IP ou do endereço MAC da interface conectada na rede, informando esse endereço no campo "Connect To:", visível na Figura 14.

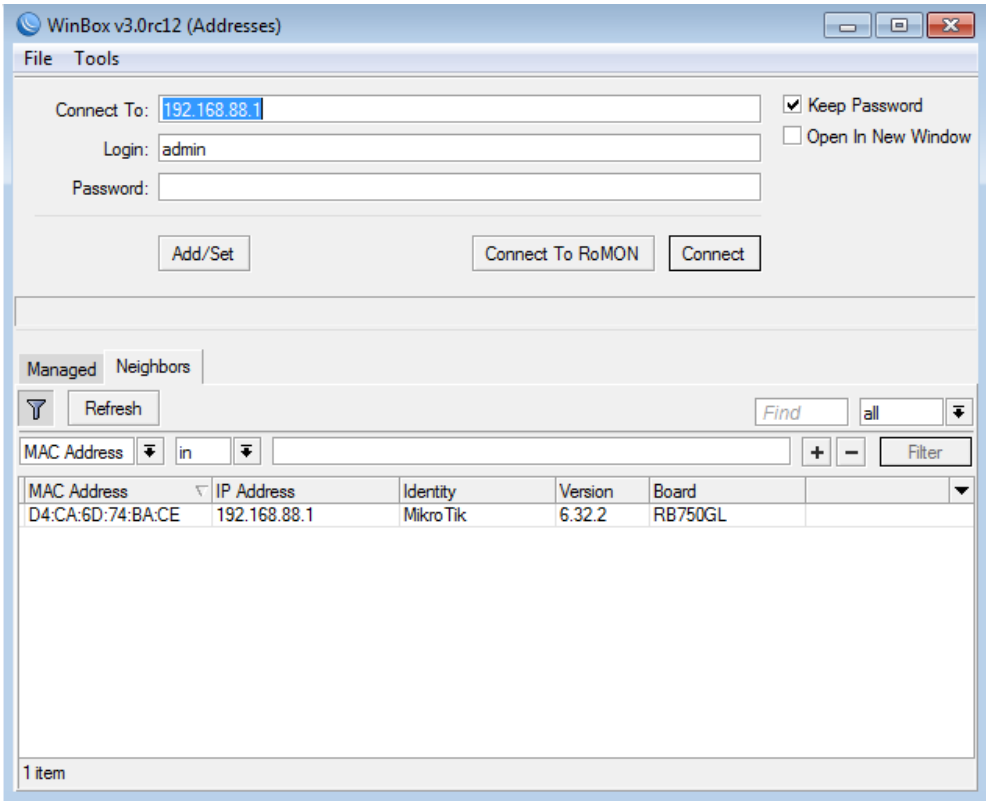

Figura 14 – Winbox
Fonte: Autoria própria

Caso o aparelho esteja configurado com usuário e senha, os mesmos devem ser informados nos campos "Login" e "Password", respectivamente. Após, deve-se clicar no

botão “Connect” e com isso o usuário terá acesso as configurações do Routerboard, conforme pode ser visto na Figura 15.

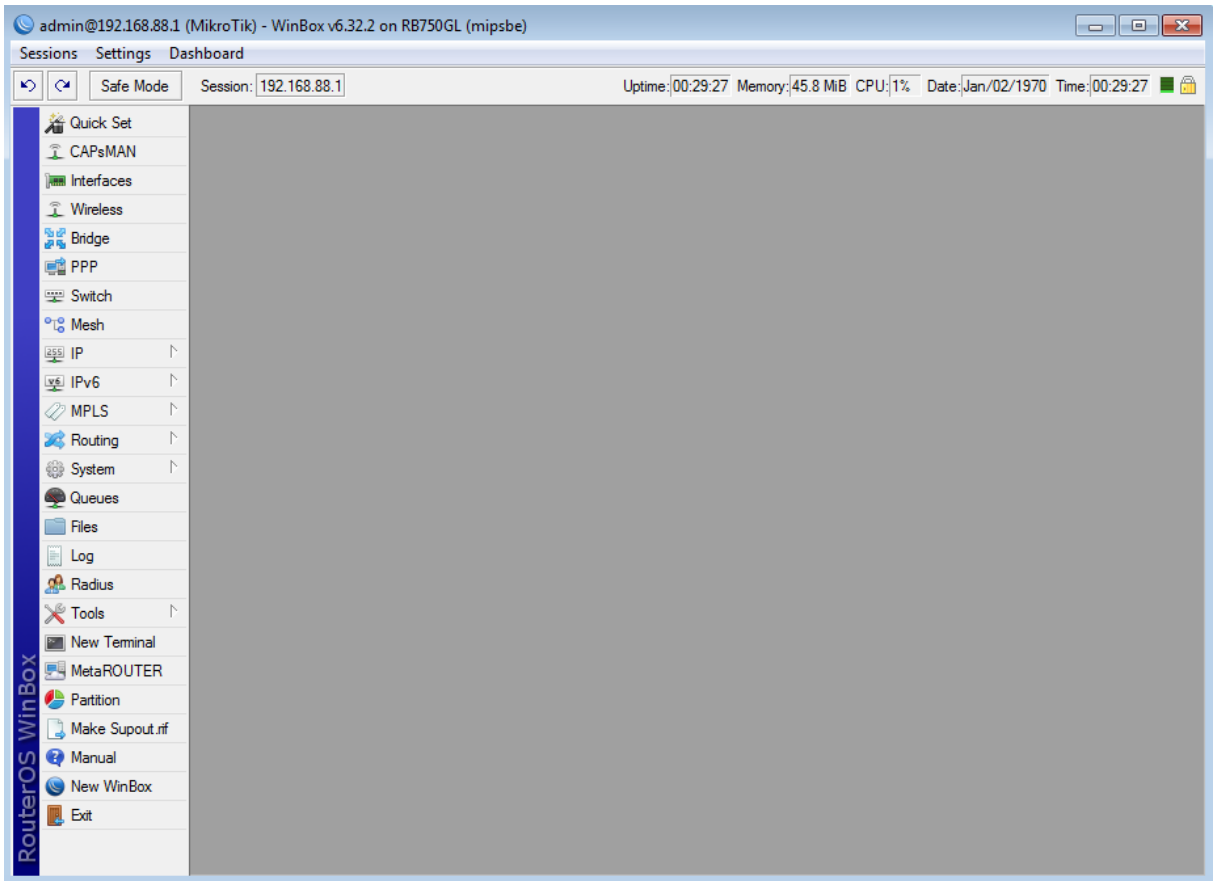

Figura 15 – Tela de configuração do Routerboard
Fonte: Autoria própria

4.4.2 Configurações Iniciais

Por padrão, o Routerboard RB750 não possuí senha para conexão e por este motivo o primeiro passo para configuração é definir uma senha padrão para acesso, aumentando assim a segurança do aparelho. O procedimento de definição de senha está descrito no Apêndice A.

Após, foram definidas a maneira que as cinco interfaces *Fast Ethernet* presentes no Routerboard RB750 irão trabalhar, conforme descrito abaixo:

- Interface 1: recebe o link principal de Internet, o link de fibra óptica, renomeada para “1_fibra”;
- Interface 2: recebe o link secundário de Internet, o link de ADSL, renomeada para “2_adsl”;
- Interface 4: conexão com o roteador sem fio que distribuirá a Internet para os clientes da empresa, renomeada para “4_LAN_Cliente”;

- Interface 5: distribuição da Internet para toda a empresa, renomeada para "5_LAN".

Na configuração padrão, o RouterOS define a interface 1 como gateway padrão, a interface 2 como interface local mestre deixando as três interfaces restantes vinculadas a interface 2. Por este motivo, deve-se desvincular as interfaces 3, 4 e 5 da interface 2 para efetuar as configurações. O procedimento de alteração dos nomes das interfaces e da desvinculação entre elas está descrito no Apêndice B.

Após a definição das interfaces, é preciso alterar o endereço IP do Routerboard uma vez que por padrão é definido como 192.168.88.1/24, vinculado à interface 2. Neste trabalho, o endereço IP foi alterado para 192.168.1.254/24 vinculado à interface 5 e adicionado o endereço IP 10.0.0.1/24 para a interface 4, sendo o procedimento explicado no Apêndice C.

Não foi preciso definir os endereços IPs das interfaces 1 e 2 uma vez que elas são adicionadas automaticamente com a configuração dos clientes DHCP no RouterOS. Foram cadastrados dois clientes DHCP, sendo um para a interface 1 e outro para interface 2, todos com as configurações padrões do RouterOS, apenas desabilitando a opção adição de rota automática, uma vez que as rotas para os links de Internet serão cadastradas manualmente. A descrição da criação de cliente DHCP pode ser encontrada no Apêndice D.

Foram cadastradas manualmente as rotas para os links de Internet, sendo uma vinculada a interface 1 e outra vinculada a interface 2 no gateway da rota, definindo como endereço IP de destino 0.0.0.0/0, fazendo assim toda navegação passar por esta rota.

A rota vinculada a interface 1 recebeu uma métrica menor se comparada a rota para a interface 2, uma vez que ela tem prioridade para navegação. O procedimento de cadastro de rota está descrito no Apêndice E.

Para finalizar as configurações básicas, foi definida duas regras no NAT do tipo *masquerade*, uma vinculada a interface 1 e outra vinculada a interface 2 para o funcionamento da Internet.

4.4.3 Servidor DHCP

Foram criados dois servidores DHCP, sendo um para a rede interna da empresa, nomeado "default" e vinculado a interface 5, e outro para a rede utilizada pelos clientes, nomeado "dhcp_externo" e vinculado a interface 4.

Cada servidor DHCP teve seu *gateway* e servidor DNS definidos como o endereço IP da sua interface bem como o endereço do servidor definido pelo endereço de rede da interface.

Por solicitação da empresa, foram definidos em ambos os servidores DHCP o tempo de vida dos endereços IP para um dia. Também foram definidas as faixas de endereço IP conforme a necessidade da empresa.

Os procedimentos de cadastro do servidor DHCP e definição da lista de endereços IP pode ser encontrado no Apêndice F.

4.4.4 Link de Contingência

Para garantir que a empresa não fique sem acesso a Internet caso o link da fibra óptica fique desligado, foram criadas algumas regras para contornar esta situação utilizando o link ADSL.

A ideia é que, caso a Internet ou o modem do link principal fique fora, o Routerboard identifique e automaticamente coloque o link de backup como ativo e quando o link principal voltar ele reverta essa configuração, de forma transparente ao usuário.

A maneira de trabalhar com esta ideia é através da alteração da métrica entre as rotas através de dois scripts, um definindo a métrica da rota para o link de backup menor que a rota para o link principal e outro script fazendo o inverso.

Para fazer tal verificação, é utilizado o recurso *netwatch* presente no RouterOS. É definido um endereço IP e o *netwatch* fica testando o endereço IP através do *ping* em tempos pré-determinados pelo usuário.

Caso não seja recebido uma resposta do ping efeuado no endereço IP, o *netwatch* considera como falha e roda o script configurado em *down*. Quando ele consegue novamente resposta do endereço IP é executado o script configurado em *Up*. Para este processo, foi utilizado o endereço IP 8.8.8.8 (DNS do Google) efetuando o *ping* a cada 10 segundos.

Por fim, foi criado uma rota estática para o endereço IP 8.8.8.8 definindo como *gateway* padrão o link principal, garantindo assim que o teste através do *ping* passe sempre pelo link principal.

O procedimento de implementação descrito neste subcapitulo estão descritos no Apêndice G.

4.4.5 Servidor DNS

Como foi definido de maneira automática os clientes DHCP, o RouterOS define de maneira automática os servidores DNS, não precisando informar manualmente. Foram definidos apenas alguns endereços HTTP que são utilizados externamente direcionados para os servidores internos da empresa, definindo esses endereços manualmente no servidor DNS, conforme pode ser visto no Apêndice H.

4.4.6 Configuração NAT e Redirecionamento de portas

Para atender as necessidades da empresa, foram redirecionadas algumas portas do link principal para alguns endereços IPs internos como serviço FTP, serviço HTTP e VNC. O procedimento de cadastro e configuração do redirecionamento de portas pode ser visto no Apêndice I.

4.4.7 Configuração QoS

Por solicitação da empresa, foram definidas prioridades para os serviços de videoconferência do programa Skype e acesso remoto RDP. A implementação foi feita utilizando filtragem do firewall na camada de aplicação, denominado no RouterOS como *Layer7 Protocols*.

Com este tipo de filtragem, o firewall identifica na camada de aplicação (camada 7 do modelo OSI) um padrão pré-determinado cadastrado no RouterOS que define qual é o serviço utilizado, diminuindo o consumo de memória RAM do Routerboard e aumentando o uso do processador. O script de configuração pode ser visto no Apêndice J.

4.4.8 Proxy

A configuração do proxy feita de maneira que todos os sites são liberados, sendo bloqueados apenas sites de pornografia e jogos. Foram definidos 40MB de cache armazenado no próprio Routerboard e o proxy é transparente ao usuário, não sendo necessário qualquer configuração no computador.

Para isso, foi adicionado uma regra no NAT do firewall onde toda saída de conexão pela porta 80 fosse redirecionada para a porta configurada do proxy 8080. O procedimento pode ser visto no Apêndice K.

4.4.9 Balanceamento de Carga

Devido a diferença entre os dois links, sendo o link principal tendo uma velocidade nominal de 150Mb de download e o link de backup uma velocidade nominal de 15Mb, a alternativa adotada para fazer o balanceamento de carga foi o de, quando o link principal estiver totalmente ocupado, o RouterOS começa a utilizar o link de backup.

4.4.10 Gráficos de Uso de Bando e Recursos

O RouterOS foi configurado para exibir o uso de banda de todas as suas interfaces como também o consumo de recursos como processamento, memória RAM e disco, acessando pelo endereço IP do Routerboard através do navegador de Internet.

Uma vez que a porta padrão para tal acesso é a porta 80, por questões de segurança, esta porta foi alterada para porta 9090 sendo também desabilitado os outros acessos ao Routerboard como FTP, SSH e Telnet. O procedimento de configuração pode ser visto no Apêndice L.

4.5 DISCUSSÃO

O levantamento feito com o referencial teórico auxiliou na escolha dos métodos e arquiteturas para implantação do projeto. O tipo de firewall utilizado foi o firewall de aplicação, uma vez que foram utilizadas regras fixas no filtro de pacotes e também o proxy em modo transparente. Já a arquitetura de firewall utilizada foi o *host dual-homed* uma vez que a empresa possui servidores simples para atualização de sistema e FTP.

Através do comando *traceroute* foi possível testar o link de contingência uma vez que os endereços IPs dos dois links de Internet são diferentes. Os testes realizados foram de desligar o modem do link principal e desativar a Internet do modem, mantendo ele ligado. Em ambos os casos, o trafego de pacotes foi redirecionado para o link de backup. Também foram efetuados através de sites que informam o endereço IP externo, sendo possível visualizar qual endereço IP estava sendo utilizado.

A implantação do Routerboard ocorreu fora do período de expediente da empresa, sendo necessário atualizar o endereço IP de todos os equipamentos conectados na rede, isto é, roteadores sem fio, impressoras, servidores, computadores e computadores portáteis.

Para passar todo o acesso à Internet dos modens ao Routerboard, foi necessário informar o endereço IP do Routerboard no modem habilitando o modo DMZ e com isso redirecionando todos os pacotes para o Routerboard.

A instalação de um segundo roteador sem fio para uso dos clientes foi tranquila, ficando em uma rede separada e sem comunicação com a rede interna da empresa. Por solicitação do analista de redes, a rede interna da empresa também não acessava a rede sem fio destinada aos clientes.

Após a instalação, foram efetuados testes com os serviços implantados pelos colaboradores da empresa sendo encontrado problemas no redirecionamento de portas. O redirecionamento de portas foi feito conforme solicitado pela empresa, utiliza apenas o link principal uma vez que ele possui endereço IP fixo. O problema encontrava-se no modem do link principal que já estava com regras de redirecionamento de portas configuradas, sendo necessário a exclusão das regras no modem.

Através de sites com aplicativos de teste de velocidade de Internet como Copel e SIMET, foi detectado que a velocidade da Internet principal estava muito abaixo da nominal, em vez de chegar próximo aos 150Mb, o teste detectava a velocidade de 15Mb.

Após foram vistas todas as configurações do Routerboard não encontrando problemas relacionados a velocidade da Internet. Foi optado por testar um segundo Routerboard, modelo RB750GL com a mesma configuração do Routerboard utilizado no presente trabalho.

Antes de importar o script de configuração do Routerboard, foi efetuado no RB750GL uma limpeza geral nas configurações, incluindo a não restauração das configurações padrões. Instalado o RB750GL no lugar do RB750 e efetuado os testes, a velocidade da Internet chegou aos 100Mb.

Feito uma limpeza nas configurações do RB750 e não incluindo a restauração das configurações padrões do Routerboard e importando o script de configuração, os testes demonstraram que a velocidade da Internet subiu para 50Mb. Além disso, o consumo de memória RAM do Routerboard diminuiu.

A diferença de velocidade entre os modelos RB750 e RB750GL se devem principalmente a diferença entre as interfaces, sendo que as do modelo RB750 são *Fast Ethernet* enquanto as do modelo RB750GL são *Gigabit Ethernet*.

A diferença de performance no modelo RB750 antes e depois de efetuar a limpeza de configuração se deve a alguma configuração padrão que estava limitando a velocidade de Internet.

O modelo RB750GL não conseguiu chegar na velocidade nominal do link principal provavelmente porque os *switches* utilizados possuem apenas interfaces *Fast Ethernet* habilitadas. Infelizmente não foi possível alterar as configurações dos *switches* para utilizar a interface *Gigabit Ethernet*.

4.6 RESULTADOS

Devido a velocidade do link principal de 150Mb foi necessário a substituição do Routerboard modelo RB750 pelo modelo RB750GL que possuí as cinco portas *Gigabit Ethernet*, uma vez que os testes de velocidade através do site SIMET.NIC.BR, o modelo RB750 chegou apenas a 50Mb contra os 100Mb de velocidade apresentado pelo modelo RB750GL.

É importante ressaltar que mesmo com o modelo RB750GL implantado, devido a limitação dos *switches* presentes na empresa, não foi possível pegar a velocidade nominal do link principal de 150Mb. Entretanto, testes de velocidades efetuados dentro do Routerboard demonstraram que a conexão entre o roteador e o modem do link principal chegam na velocidade nominal.

Como resultado da implantação do presente trabalho, é possível o analista de redes acompanhar o uso da Internet, sendo que durante o uso do Routerboard não chegou a 50Mb de download o uso do link principal, mostrando que a empresa utiliza apenas um terço da sua Internet contratada no link de fibra óptica.

As informações do trafego das interfaces do Routerboard bem como o uso de processamento, memória RAM e disco podem ser acessadas pelo navegador de Internet habilitando o serviço WWW do RouterOS, não sendo necessário executar o Winbox.

Nos casos onde o link principal ficou *off-line*, o RouterOS redirecionou todo o tráfego para o link de backup de modo transparente, sem necessidade de interversão do analista de rede.

Infelizmente, não foi possível implantar o balanceamento de carga onde seria utilizado o link de backup caso o link principal ficasse 100% ocupado uma vez que todas as informações a respeito disponível no site da Mikrotik bem como nos fóruns na Internet não atendiam essa ideia. Também, a implementação do balanceamento de carga descrito nos

tutoriais impactava na metodologia utilizada no desenvolvimento do link de contingência, desabilitando a mesma.

Com a priorização de serviços de videoconferência e acesso remoto a taxa de transferência de dados manteve-se constante, mesmo com o uso da Internet pelos demais colaboradores da empresa.

Devido a implantação da metodologia de análise através da camada de aplicação, o uso do processador do Routerboard chegou a picos de 25% (antes da implementação, ficava em torno de 2%). Este custo de processamento nesse tipo de caso compensa uma vez que libera o uso de memória RAM para as demais funções do Routerboard.

Mesmo o RouterOS dando a opção de trabalhar com *Hotspot*, a empresa optou por não utilizar esse recurso e utilizar dois roteadores sem fio, sendo um para uso interno e outro para uso de seus clientes. Através de regras no firewall inseridas no RouterOS, a comunicação entre a rede interna corporativa e a rede sem fio para os clientes ficou bloqueada, impedindo assim o acesso dos clientes aos servidores e compartilhamentos da empresa.

Por fim, com o uso do proxy sites pornográficos e de jogos foram bloqueados, sem a necessidade de configuração nos computadores dos colaboradores, fazendo apenas um redirecionamento de porta no NAT do RouterOS.

5 CONCLUSÃO

É demonstrado com o desenvolvimento deste trabalho a possibilidade de utilizar um roteador compacto, de baixo custo em uma microempresa, mantendo a qualidade no serviço se comparado a softwares e hardwares com um custo mais elevado.

Com a implantação do projeto, o trabalho de contingência do link de Internet é feito de maneira automática e transparente, sem a necessidade de efetuar a troca do link manualmente como outrora ocorria.

Também existe um melhor controle nos recursos utilizados por parte de seus funcionários, já que através do proxy é possível utilizar cache de conteúdo, contudo, devido ao Routerboard RB750 ser incapaz de armazenar grandes quantidades de cache, neste trabalho foram limitados a apenas 40MB.

Entretanto, a utilização do Routerboard exige um maior grau de conhecimento por parte do analista de redes quando comparado as opções mais simples encontradas nos modems. Por este motivo, é necessária uma explicação mais detalhada ao analista de como adicionar novas rotas e opções no firewall do roteador que por ventura irão surgir.

Devido a utilização contínua na Internet por parte da microempresa e a necessidade de trocar toda classe de IP utilizada internamente, o processo de implantação foi realizado à noite, sendo necessários ajustes nos computadores portáteis dos colaboradores como também a adequação de alguns caminhos utilizados internamente na empresa.

Outro problema encontrado é que, caso utilize uma Internet com velocidade superior as suportadas pelas interfaces do aparelho, não será possível utilizar 100% dos recursos de Internet. No caso, o modelo RB750 utilizado no projeto não apresentou desempenho satisfatório, utilizando apenas um terço da velocidade do link principal.

Nestes casos, onde a velocidade da internet supera a velocidade dos 100Mb que são suportadas pelas interfaces *Fast Ethernet*, é recomendado utilizar o modelo com interfaces *Gigabit Ethernet*, como no caso do modelo RB750GL.

Como trabalhos futuros ficam a possibilidade de utilizar um segundo Routerboard RB750 como *backup* (se por ventura o roteador principal falhe o secundário inicia de modo transparente, sem a necessidade de interversão do analista de redes), a implantação de um balanceamento desigual de carga, uma alerta via e-mail da queda dos links de Internet e o desenvolvimento de uma interface gráfica para o cliente efetuar configurações básicas e pré-definidas de maneira fácil e prática.

REFERÊNCIAS

ALECRIM. Emerson. **O que é firewall?** Conceito, tipos e arquiteturas. Disponível em <http://www.infowester.com/firewall.php>. Acesso em 10/07/2015.

CANALTECH. **O que é *hotspot*?**. Disponível em <http://canaltech.com.br/o-que-e/internet/O-que-e-hotspot/>. Acesso em 06/07/2015.

JCVIRTUAL. **Firewall** – Conceito e Principais Tipos. Disponível em <http://www.jcvirtual.com.br/index.php/2011-12-29-12-54-04/130-firewall-conceito-e-principais-tipos>. Acesso em 10/07/2015.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**: Uma Abordagem Top-Down. 5. ed. São Paulo: Pearson Addison-Wesley, 2010.

MACÊDO, Diego. **Tipos de Firewall**. Disponível em **<**http://www.diegomacedo.com.br/tipos-de-firewall>. Acesso em 10/07/2015.

MIKROTIK. Página oficial da fabricante Mikrotik. Disponível em <http://www.mikrotik.com/>. Acesso em 10/08/2015.

MORIMOTO, Carlos E. **Servidores Linux, guia prático**. 2. ed. Porto Alegre: Sul Editores, 2010.

NAKAMURA, Emilio T.; GEUS, Paulo L. de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

NETDEEP. **Inspeção profunda de pacotes** (DPI). Disponível em <http://www.netdeep.com.br/blog/seguranca-da-informacao/inspecao-profunda-de-pacotes-dpi.html>. Acesso em 10/07/2015.

ROUTERBOARD. Página oficial sobre equipamentos da Mikrotik. Disponível em <http://routerboard.com/>. Acesso em 25/08/2015.

SIGNIFICADOS. **Significado de Hotspot Wifi**. Disponível em <http://www.significados.com.br/hotspot-wifi/>. Acesso em 06/07/2015.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores** – Princípios e Práticas. 2. ed. Rio de Janeiro: Elsevier, 2014.

TANEMBAUM, Andrew. **Rede de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

UFRJ. **Firewall:** Proxy de Aplicação. Disponível em <http://www.gta.ufrj.br/grad/07_1/firewall/index_files/Page480.htm>. Acesso em 10/08/2015.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. **Building Internet Firewalls**. 2. ed. Sebastopol: O'Reilly Media, 2000.

APÊNDICE A – Definição de senha de usuário no Routerboard

Para definir, ou alterar, a senha de um usuário deve-se acessar o menu *System* →*Users*, conforme exibido pela Figura 16, para entrar na tela de lista de usuários.

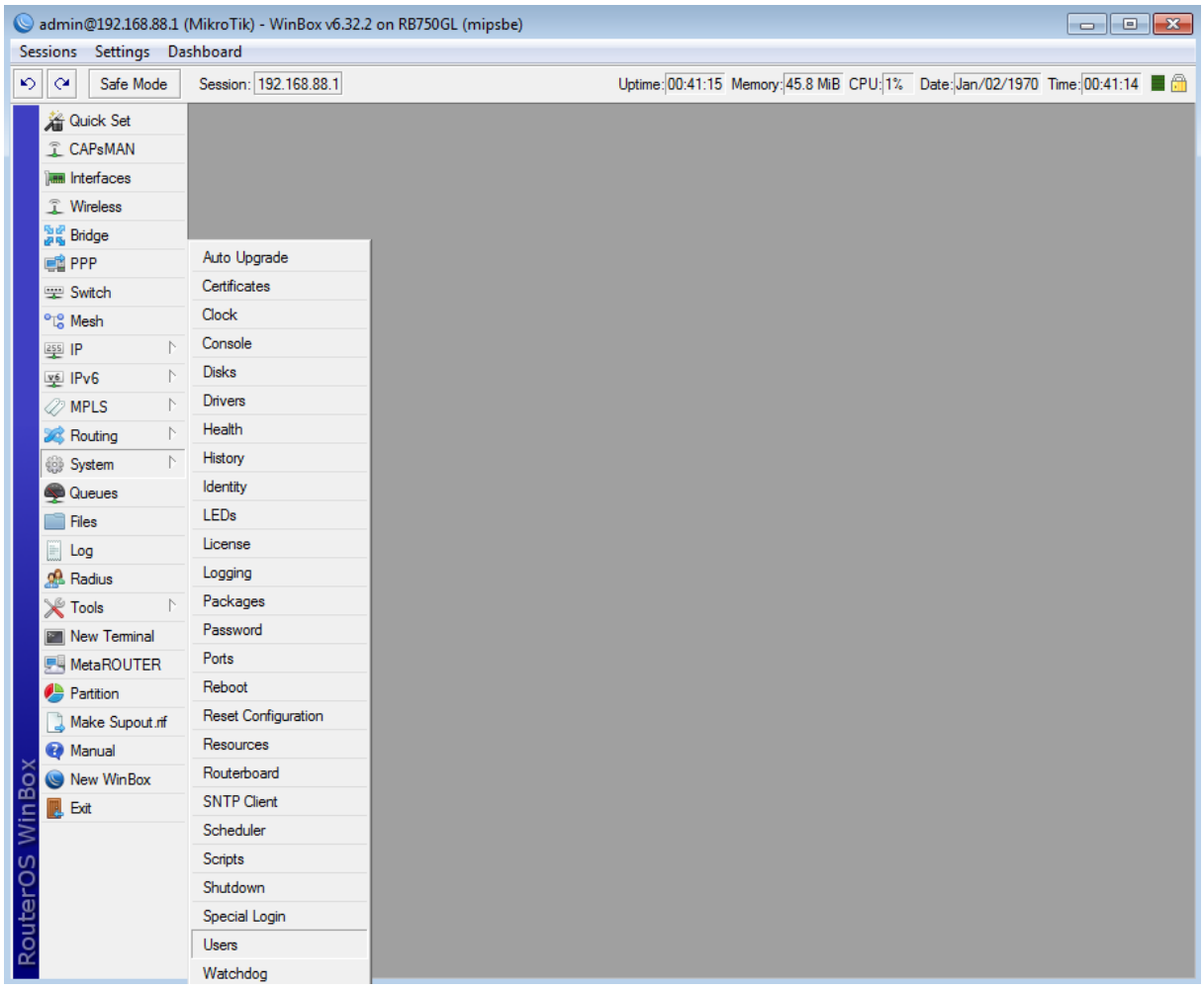

Figura 16 – Menu para alteração de usuário.
Fonte: Autoria própria

A Figura 17 mostra a tela "User List", sendo necessário ir na aba "Users" para exibir os usuários cadastrados no RouterOS.

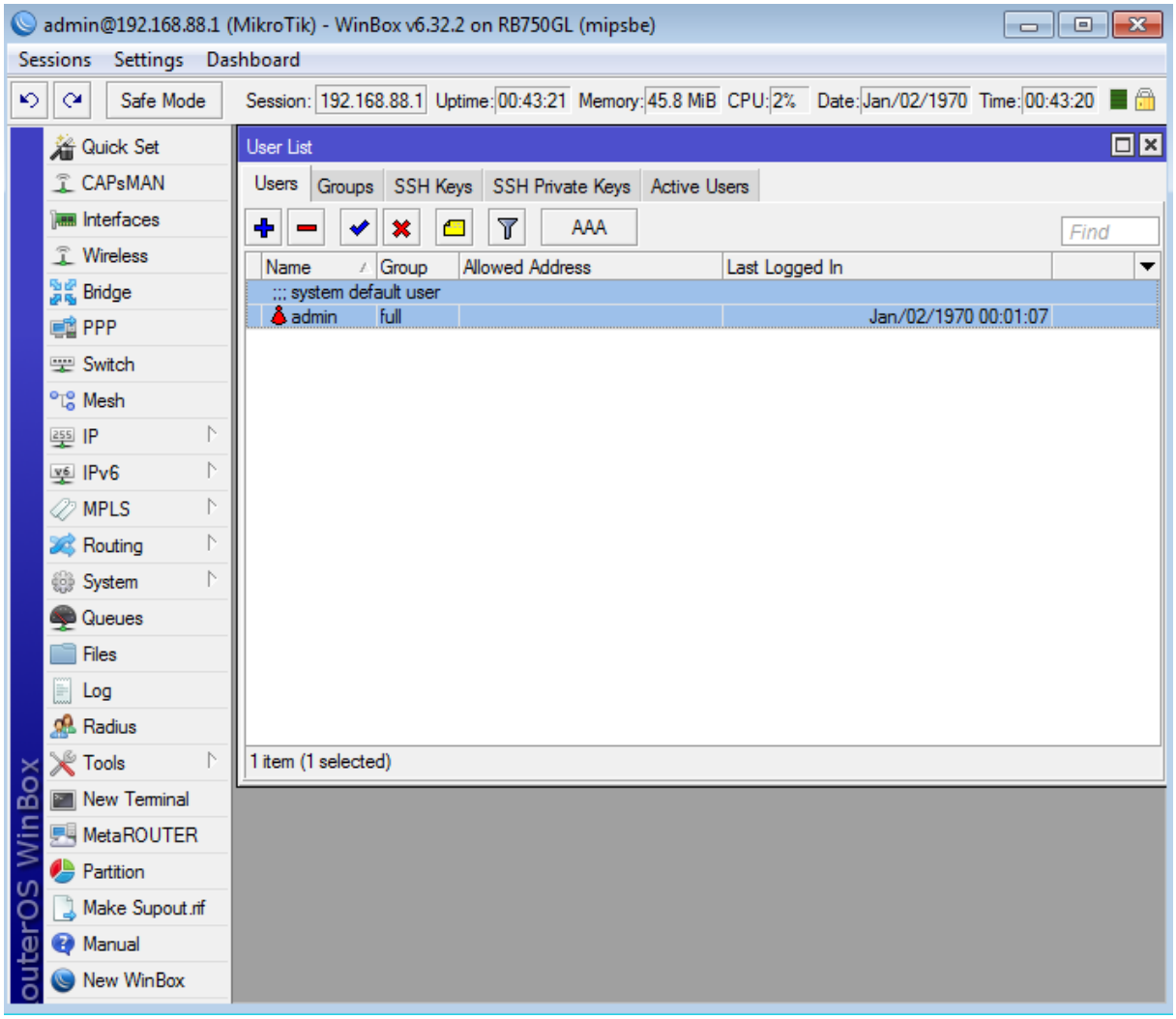

Figura 17 – Tela listando os usuários do RouterOS
Fonte: Autoria própria

O usuário padrão “admin” será exibido sendo necessário clicar duas vezes nele para abrir a janela de edição do usuário. Conforme Figura 18, é exibido algumas informações para edição do usuário como “name” (nome), “group” (grupo) e “allowed address” (endereço de rede onde se pode utilizar o usuário).

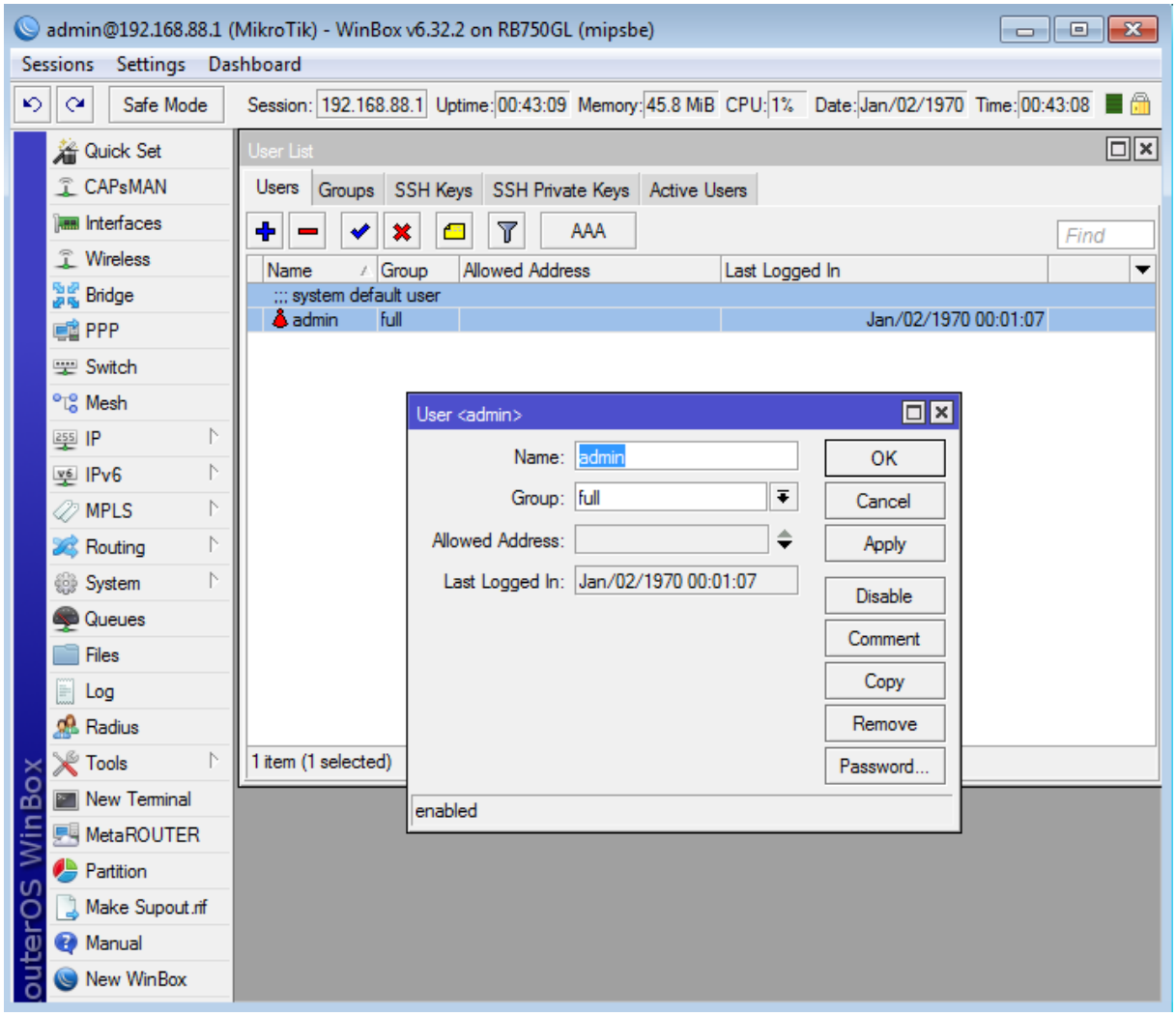

Figura 18 – Tela de configuração do Routerboard
Fonte: Autoria própria

Ao clicar no botão “Password...” será exibido uma nova janela com nome “Change Password” solicitando a nova senha (“New Password”) e a confirmação da nova senha (“Confirm Password”), visto na Figura 19.

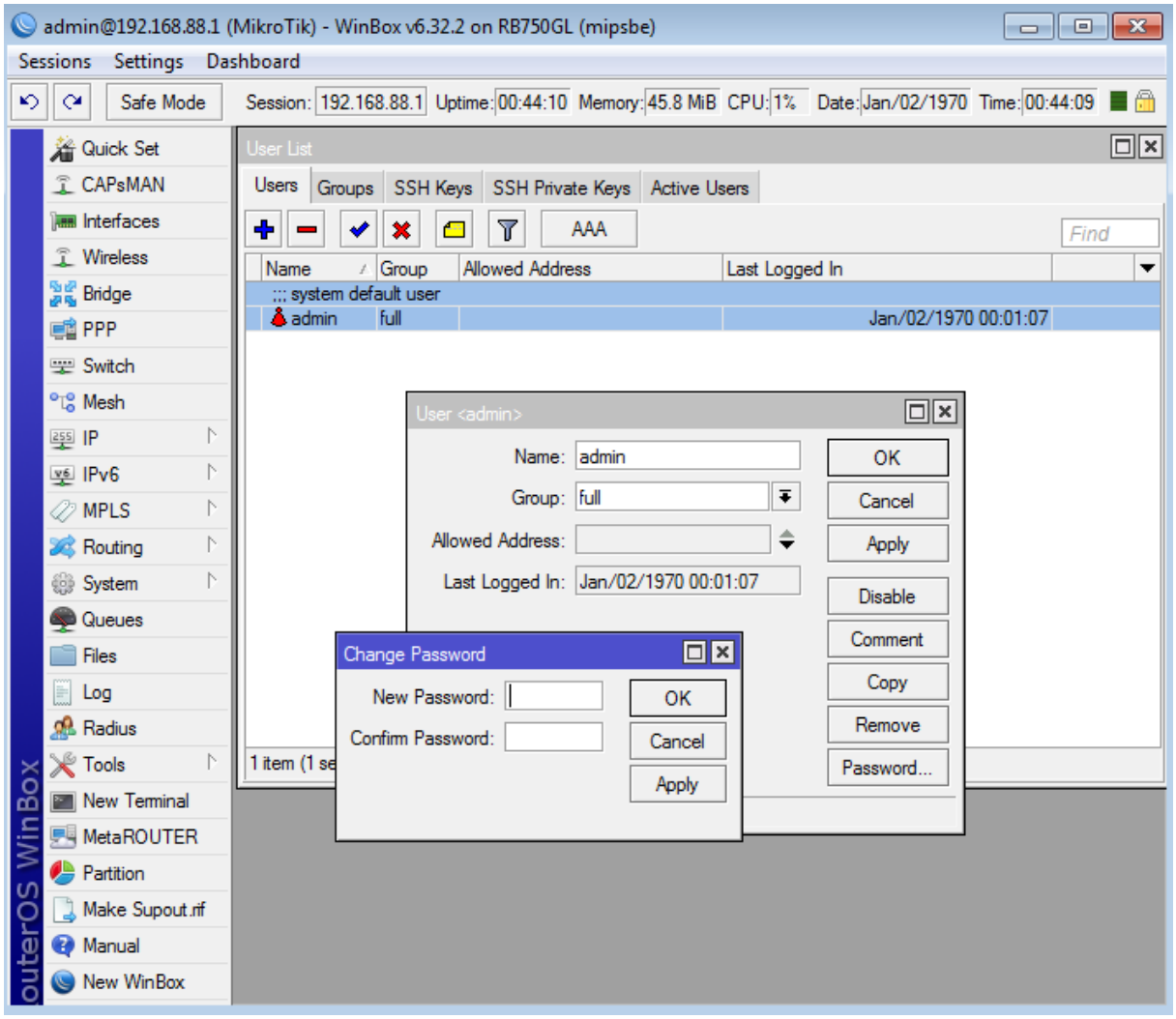

Figura 19 – Tela de definição de nova senha de usuário
Fonte: Autoria própria

Depois de informar a nova senha, basta clicar no botão “Ok” da janela “Change Password” e clicar no botão “Ok” ou “Apply” da tela “User <admin>”. Com isso será cadastrado uma nova senha para o usuário padrão do RouterOS sendo que no próximo acesso ao Routerbord pelo Winbox já será necessário informar a senha.

APÊNDICE B – Configuração das Interfaces

As configurações das interfaces são feitas através do menu *Interfaces*. Ao clicar no menu, abrirá uma janela com o nome “Interface List”, conforme pode ser visto na Figura 20.

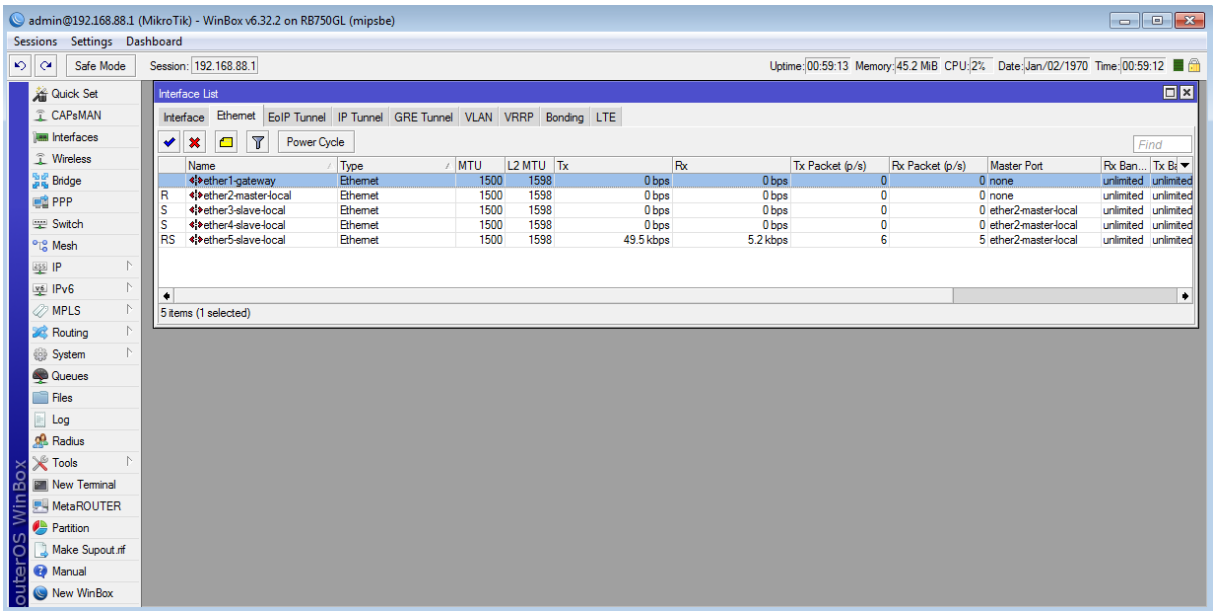

Figura 20 – Janela de Interfaces.
Fonte: Autoria própria

Na aba “Interface” é listada todas as interfaces cadastradas no RouterOS. É possível desativar a interface selecionando-a e clicando no botão “X” sendo que para ativa-la novamente basta seleciona-la e clicar no botão “✔”.

Ao dar dois cliques em uma das interfaces será aberta uma nova janela exibindo os dados da interface, conforme pode ser visto a Figura 21.

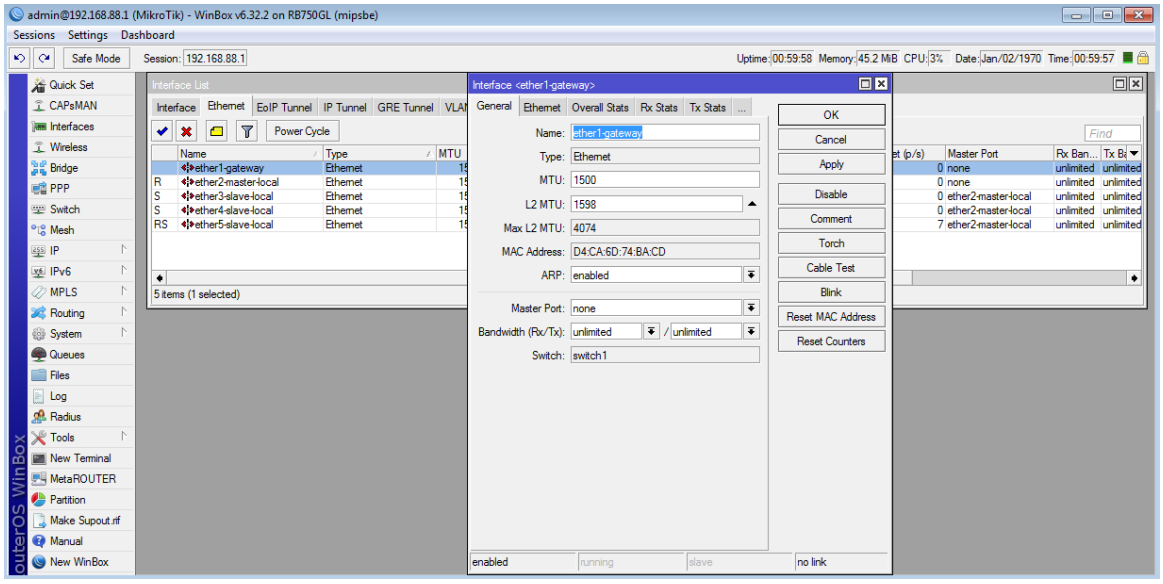

Figura 21 – Janela de edição de Interfaces.
Fonte: Autoria própria

Indo na aba “General” é possível editar, entre outros campos, o campo “Name” que altera o nome da interface e o campo “Master Port” que define qual é interface mestre da interface que está sendo editada.

Assim como mostra a Figura 22, o campo “Master Port” exibe as interfaces disponíveis para vinculo como também a opção “none” que define a interface sem vinculo. Só é possível selecionar interfaces sem vinculo (isto é, interface com a opção “Master Port” *none*) no campo “Master Port”.

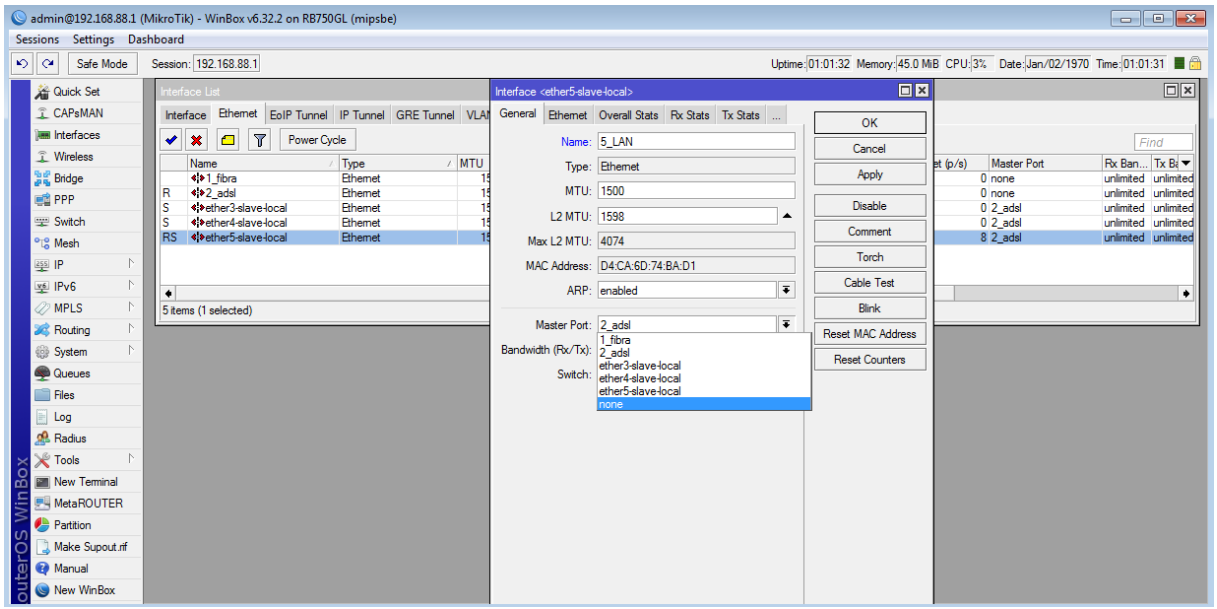

Figura 22 – Lista de opções do campo *Master Port*.
Fonte: Autoria própria

Após efetuar as alterações, basta clicar no botão “OK” ou “Apply”. Caso a interface alterada seja a que esteja sendo utilizada para conexão com Winbox a conexão irá cair sendo necessário reconectar pelo programa e, em alguns casos, usando o endereço MAC.

APÊNDICE C – Adição e alteração de endereço IPs

Para adição ou alteração de endereço IP no RouterOS, deve-se ir no menu IP → *Addresses*, conforme mostrado na Figura 23.

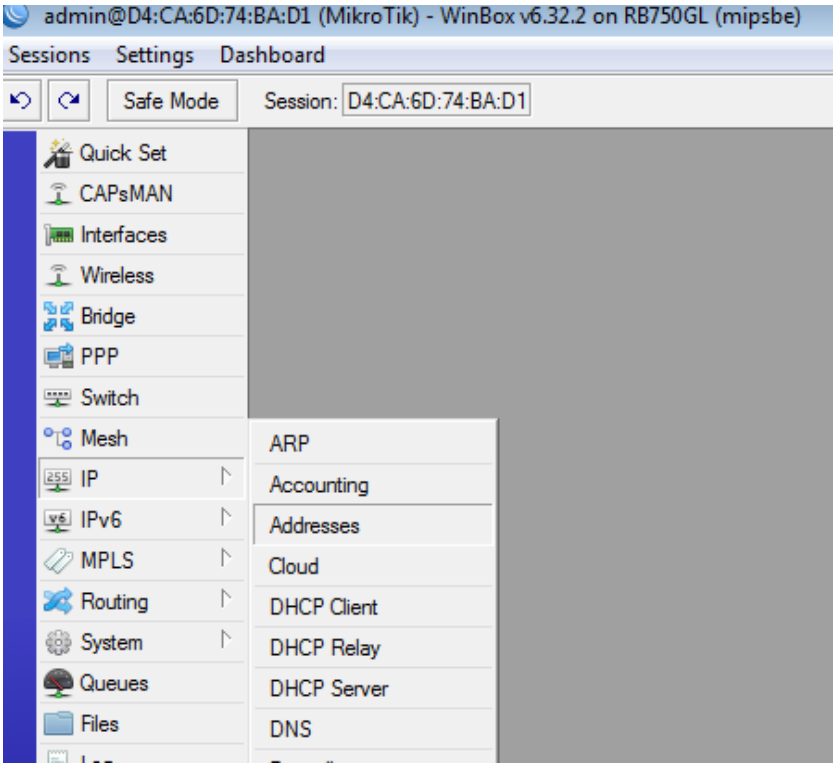

Figura 23 – Menu para adição ou alteração de IPs
Fonte: Autoria própria

A janela "Address List" mostra todos os endereços IPs cadastrados no RouterOS. Para adicionar um novo endereço IP basta clicar no botão "+" que será aberto uma nova janela contendo as informações de endereço IP ("Address"), endereço de rede ("Network") e seleção de interface, conforme mostra a Figura 24.

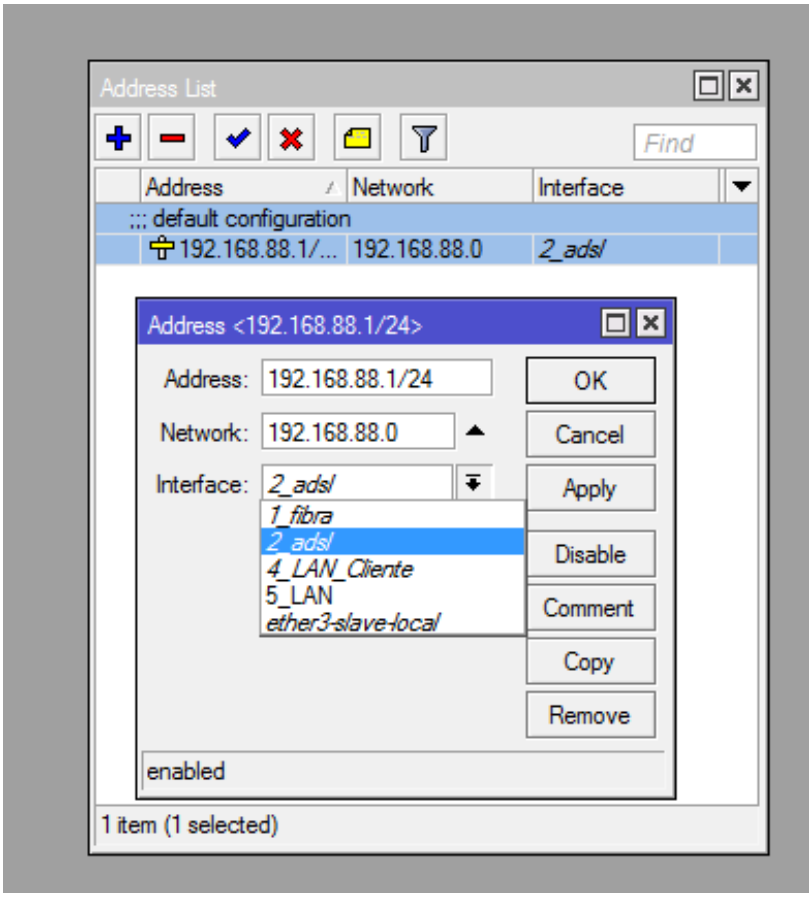

Figura 24 – Janela de Interfaces.
Fonte: Autoria própria

No campo “Address” deve-se informar o endereço IP da interface, informando também a máscara no formato CIDR, no campo “Network” deve-se informar o endereço de rede e no campo “Interface” deve-se escolher a qual interface pertence o endereço IP atribuído. Por fim, basta clicar no botão “OK” ou “Apply” para finalizar o procedimento.

APÊNDICE D – Cadastro de Clientes DHCP

Para adição ou alteração de clientes DHCP no RouterOS, deve-se ir no menu IP → *DHCP Client*, e clicar no botão + para cadastrar um novo cliente DHCP, conforme mostra a Figura 25.

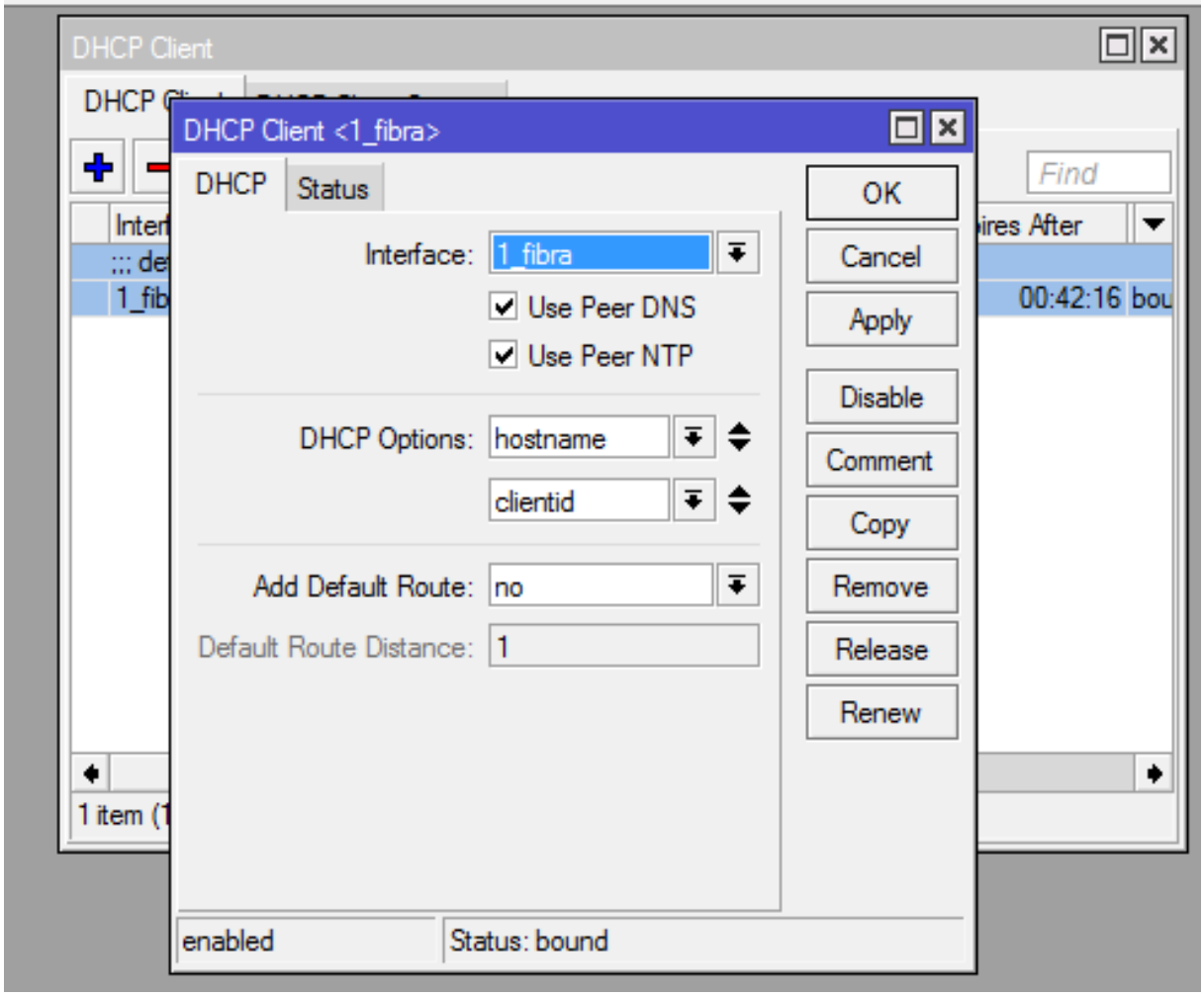

Figura 25 – Janela para adição ou alteração de cliente DHCP
Fonte: Autoria própria

No campo "Interface" deve-se selecionar a interface do Routerboard que receberá a Internet, deixando as demais configurações iguais a da Figura 25. Por fim, basta clicar no botão "OK" ou "Apply" para finalizar o procedimento.

Vale lembrar que o campo "Add Default Route" está com a opção "no" pois a rota para esse link será definida manualmente. Caso a opção fique em "yes", a rota para o link é adicionada automaticamente, contudo, atrapalhará o desenvolvimento deste trabalho.

APÊNDICE E – Cadastro de Rotas

Para adição ou alteração de rotas no RouterOS, deve-se ir no menu IP → *Routes*, na aba "Routes", clicando no botão +, conforme mostrado na Figura 26.

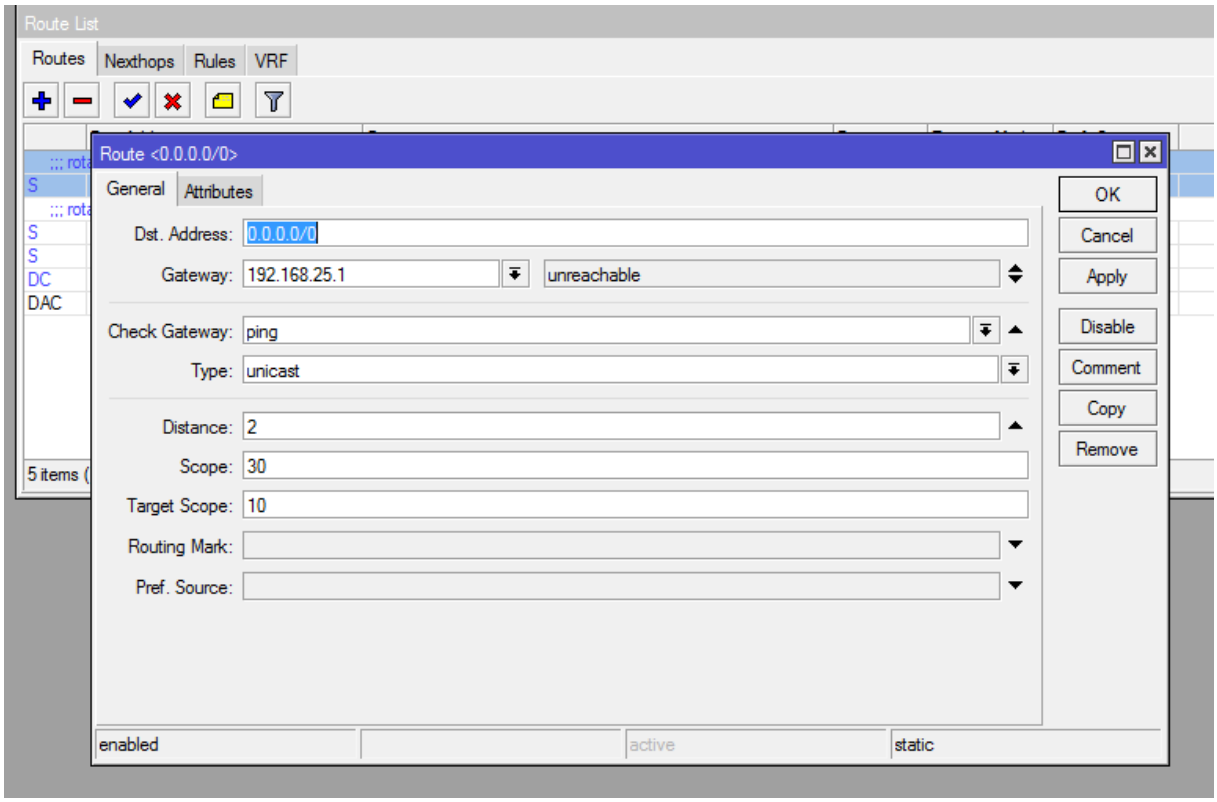

Figura 26 – Janela para adição ou alteração de rotas
Fonte: Autoria própria

No campo "Dst. Address" deve-se informar o endereço IP de destino, informando também a máscara no formato CIDR. No cadastro das rotas padrões para acesso a Internet, é informado o endereço IP 0.0.0.0/0.

No campo "Gateway" deve-se informar o endereço IP do modem com acesso a Internet sendo possível também escolher a interface no campo ao lado. O campo "Check Gateway" serve para definir de que forma o RouterOS testará o endereço IP informado no campo "Gateway".

O campo "Distance" define qual será a métrica definida para aquela rota, lembrando que quando menor o valor definido neste campo, mais prioritário ele será quando comparado a outras rotas cadastradas.

Os demais campos podem ser informados conforme mostra na Figura 26. Bastando clicar no botão "OK" ou "Apply" para finalizar o procedimento.

APÊNDICE F – Cadastro e configuração de Servidor DHCP

Antes de criar o servidor DHCP é preciso definir a faixa de endereços IPs que o servidor irá entregar de maneira automática, para isso deve-se ir no menu IP → Pool, e clicar no botão +, abrindo a janela mostrada pela Figura 27.

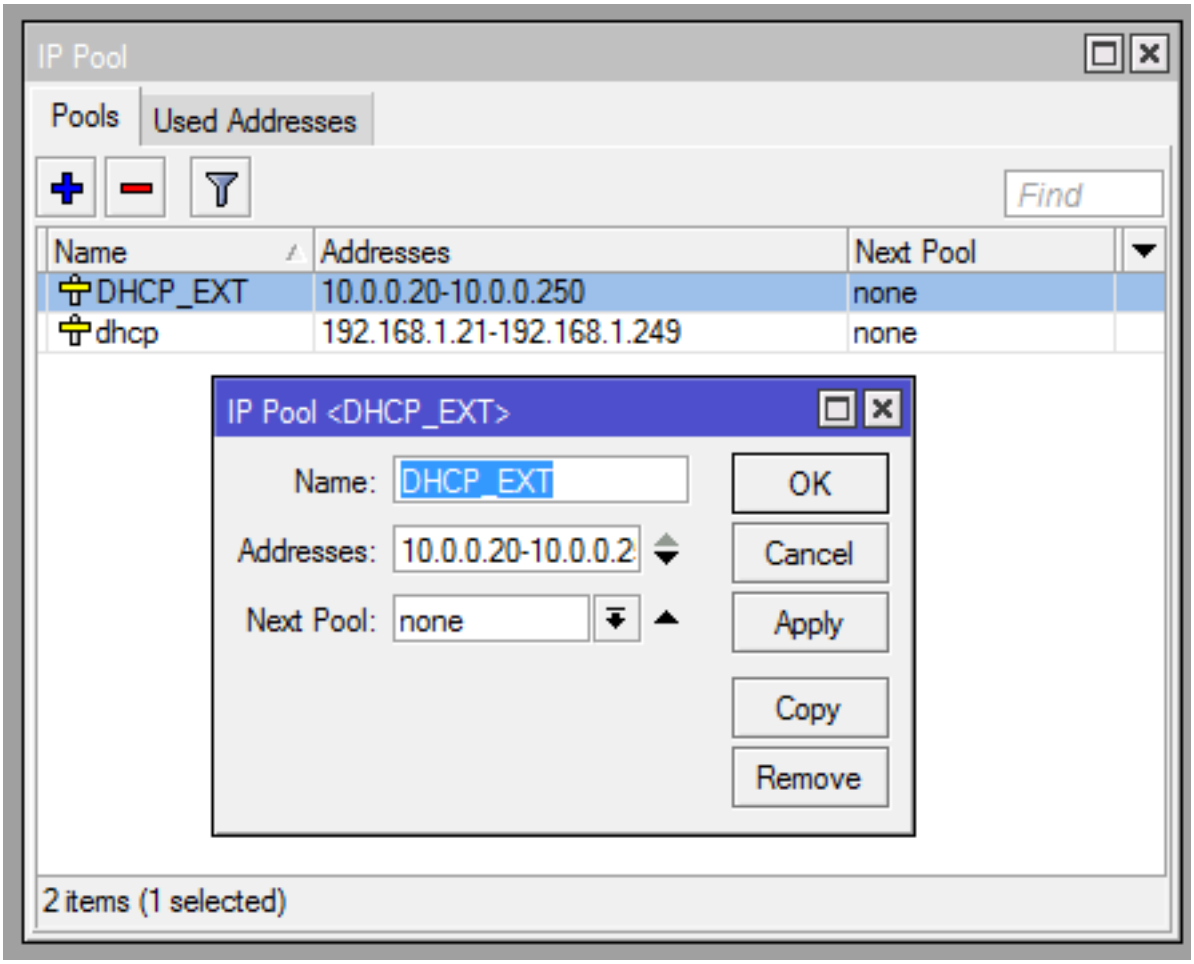

Figura 27 – Janela para adição ou alteração de faixa de endereços de IP
Fonte: Autoria própria

No campo "Name" deve-se informar o nome que será identificado a faixa de endereços IPs, no campo "Addresses" deve-se informar a faixa de endereços IP, sendo separados por – e sem espaço entre os endereços. Caso seja necessário cadastrar mais faixas de endereço IP, basta clicar no botão "▼" para adicionar mais campos. Por fim, basta clicar no botão "OK" ou "Apply" para finalizar o procedimento.

Após o cadastro dos faixas de endereço IP, para adição ou alteração do servidor DHCP no RouterOS, deve-se ir no menu IP → *DHCP Server*, abrindo a janela demonstrada na Figura 28.

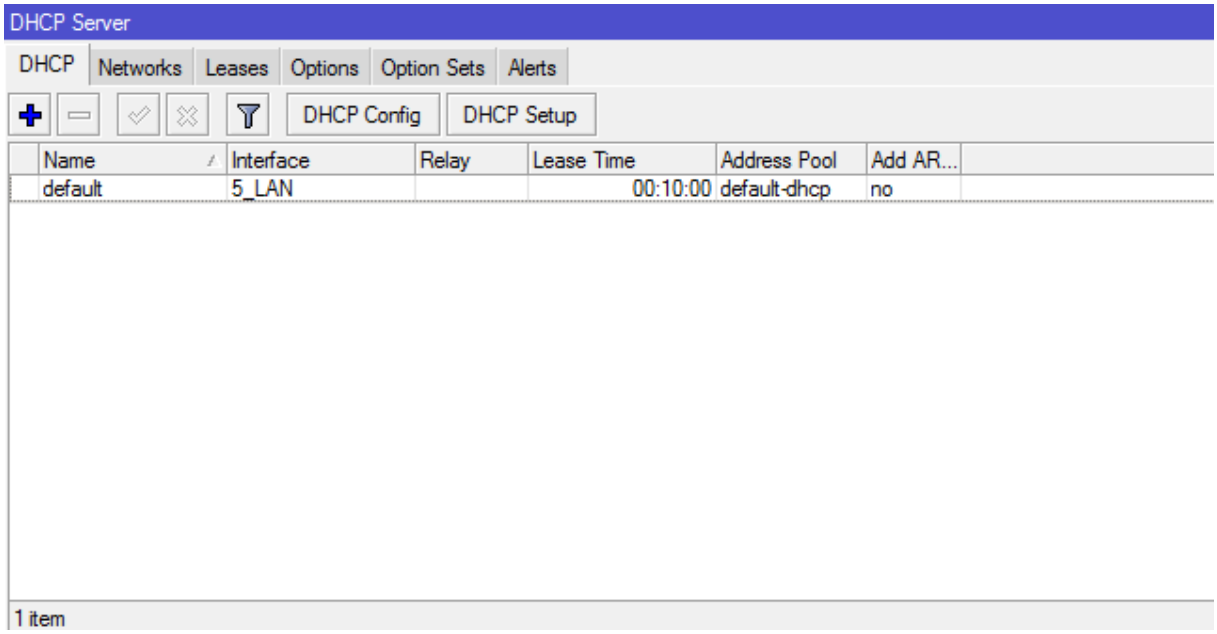

Figura 28 – Janela para configuração de servidor DHCP
Fonte: Autoria própria

É possível criar um servidor DHCP clicando no botão + na aba "DHCP", abrindo assim uma nova janela, conforme pode ser visto na Figura 29.

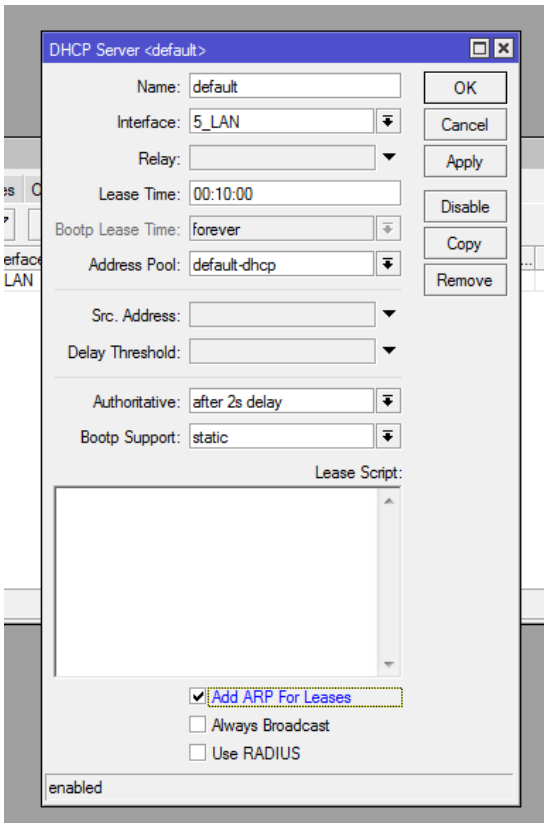

Figura 29 – Janela para adição ou alteração de servidor DHCP
Fonte: Autoria própria

No campo “Name” deve-se informar o nome de exibição do servidor DHCP, no campo “Interface” deve-se informar qual interface o servidor DHCP ficará responsável, no campo “Lease Time” é definido o tempo que o endereço IP ficará vinculado ao endereço MAC do dispositivo conectado e o campo “Address Pool” define qual é a faixa de endereço IP que o servidor DHCP irá trabalhar, exibindo na lista as faixas cadastradas na janela “Pool”. Por fim, basta clicar no botão “OK” ou “Apply” para finalizar o procedimento.

Feito o cadastramento do servidor DHCP é necessário ir na aba “Networks” para informar o endereço do servidor DHCP e demais informações de rede que serão repassados para os clientes, conforme exibido na Figura 30.

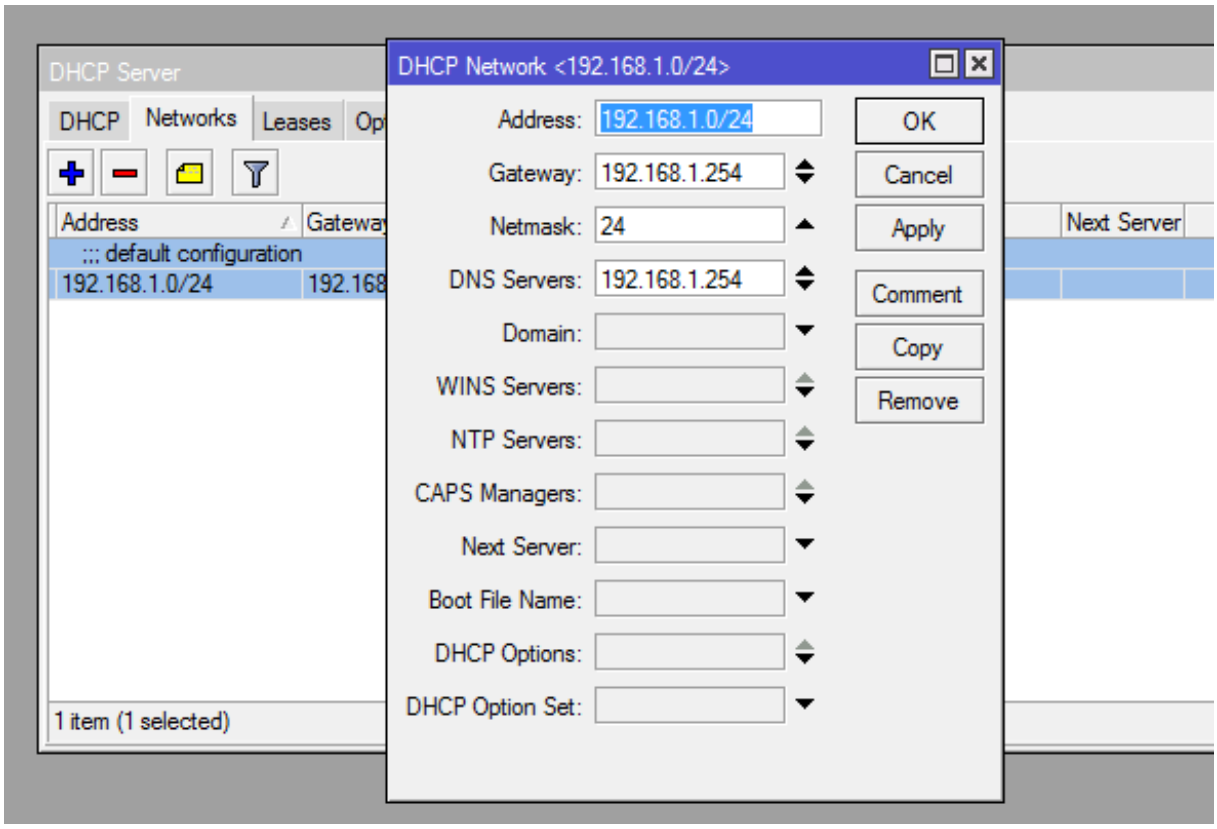

Figura 30 – Janela para adição ou alteração de rede do servidor DHCP
Fonte: Autoria própria

No campo “Address” deve-se informar o endereço de Rede informando também a máscara no formato CIDR, no campo “Gateway” deve-se informar o endereço IP do servidor Gateway, no campo “Netmask” deve-se informar a máscara de rede e no campo “DNS Servers” os endereços IPs dos servidores DNS.

Como os servidores DNS e Gateway dos modens estão cadastrados de maneira automática, nos campos “Gateway” e “DNS Servers” basta informar o mesmo endereço IP da interface do Routerboard vinculada ao servidor DHCP. Por fim, basta clicar no botão “OK” ou “Apply” para finalizar o procedimento.

APÊNDICE G – Script de configuração de Link de Contingência

Segue abaixo o script de configuração para o link de contingência.

```
/system script
add name=ativa_fibra owner=admin policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive source="/ip rou\
    te set [/ip route find comment=rota_fibra] distance=1\r\
    \n\r\
    \n/ip route set [/ip route find comment=rota_adsl] distance=2\r\
    \n"
add name=ativa_adsl owner=admin policy=reboot,read,write,test source="/ip rout\
    e set [/ip route find comment=rota_fibra] distance=2\r\
    \n\r\
    \n/ip route set [/ip route find comment=rota_adsl] distance=1\r\
    \n"

/tool netwatch
add comment=verifica_rotas down-script=ativa_adsl host=8.8.8.8 interval=10s up-
script=ativa_fibra

/ip route
add distance=1 dst-address=8.8.8.8/32 gateway=192.168.25.1
```

APÊNDICE H – Configuração de DNS Estático

Para adição ou alteração endereço DNS estático no RouterOS, deve-se ir no menu IP → *DNS*, clicar no botão "Static" e após clicar no botão +, conforme mostra na Figura 31.

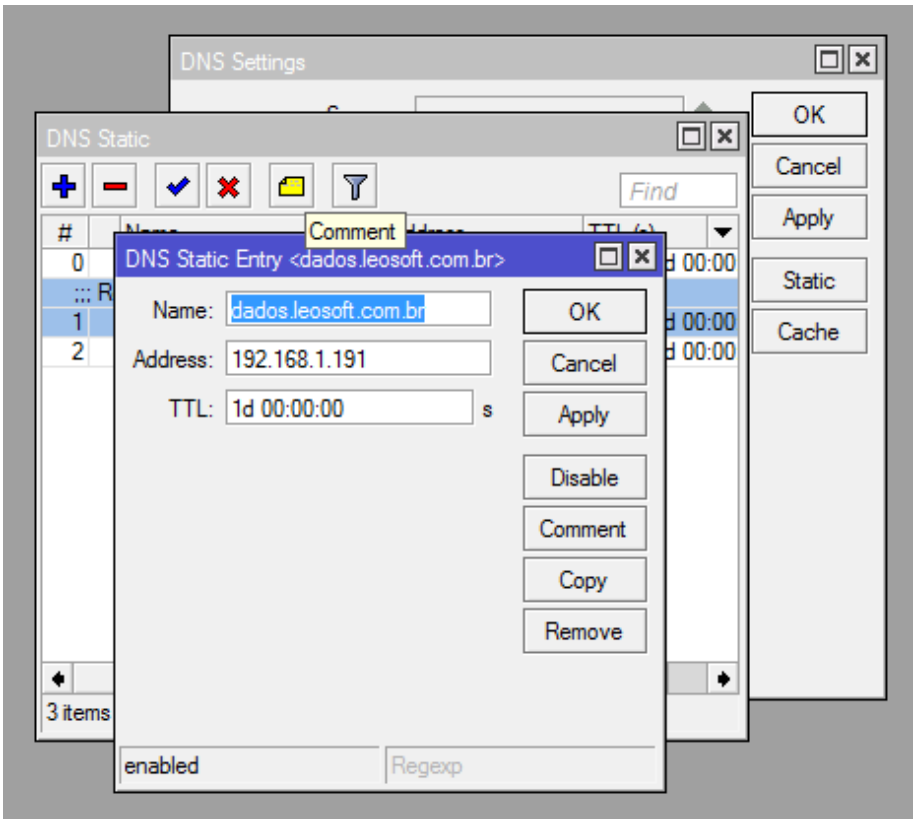

Figura 31 – Janela para adição ou alteração de DNS estático
Fonte: Autoria própria

No campo "Name" deve-se informar o endereço HTTP e no campo "Address" o endereço IP que será usado para redirecionar o endereço HTTP. Por fim, basta clicar no botão "OK" ou "Apply" para finalizar o procedimento.

APÊNDICE I – Redirecionamento de Portas

Para adição ou alteração de redirecionamento de portas no RouterOS, deve-se ir no menu IP → *Firewall*, aba "NAT" e clicar no botão +, conforme mostra na Figura 32, sendo necessário configurar em duas partes.

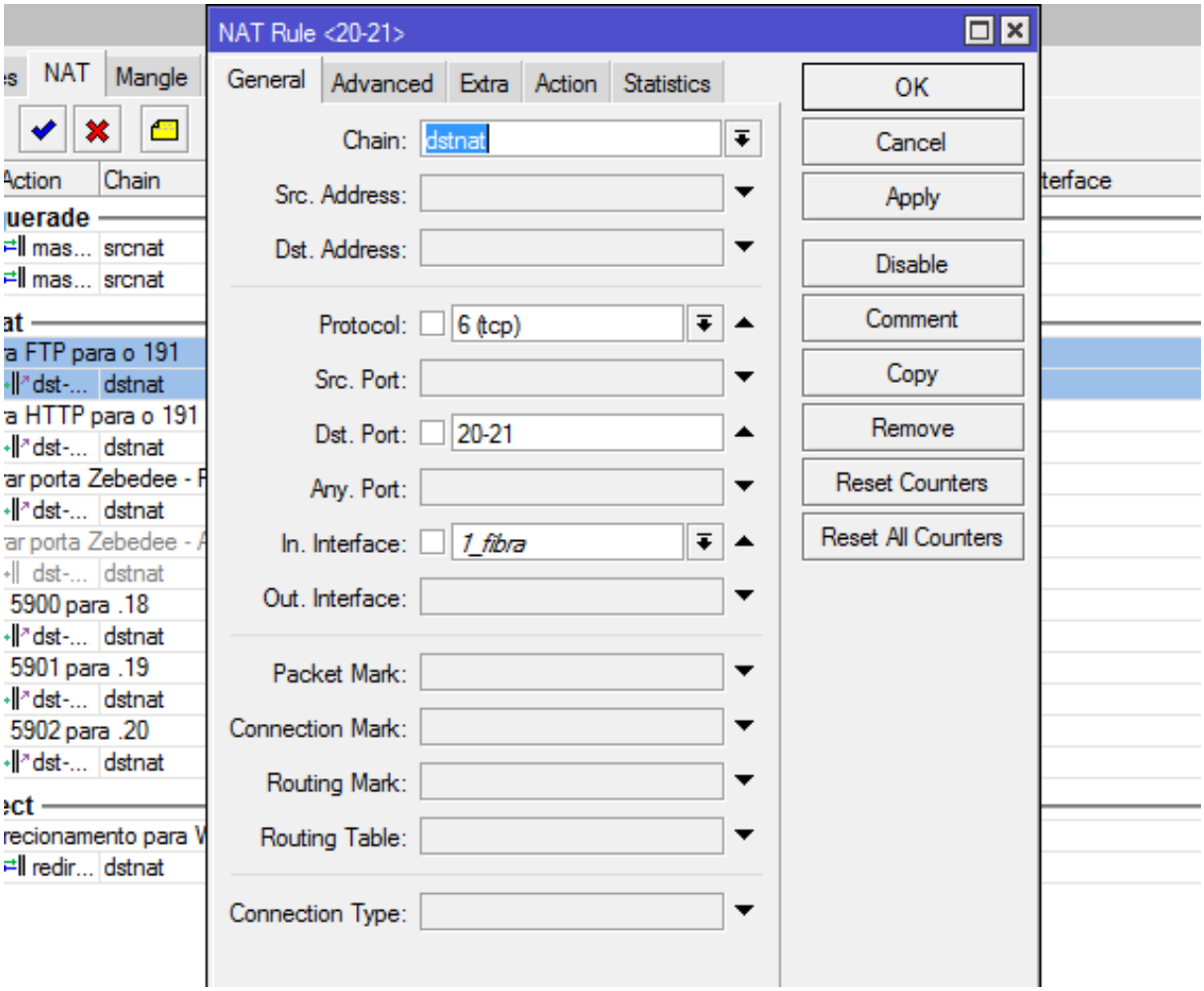

Figura 32 – Janela para adição ou alteração de redirecionamento de portas
Fonte: Autoria própria

Primeiramente, na aba "General", deve-se definir no campo "Chain" a opção "dstnat" definindo no campo "Protocol" qual protocolo será utilizado para o redirecionamento.

No campo "Dst. Port" são informadas as portas que a rede externa irá utilizar para conectar na rede interna, sendo possível informar um intervalo de portas colocando um – entre os números das portas, sem espaço. No campo "In. Interface" deve-se informar de qual interface virá a solicitação.

Após, deve-se ir na aba "Action" para informar para que endereço IP será redirecionado a solicitação externa, exibido pela Figura 33.

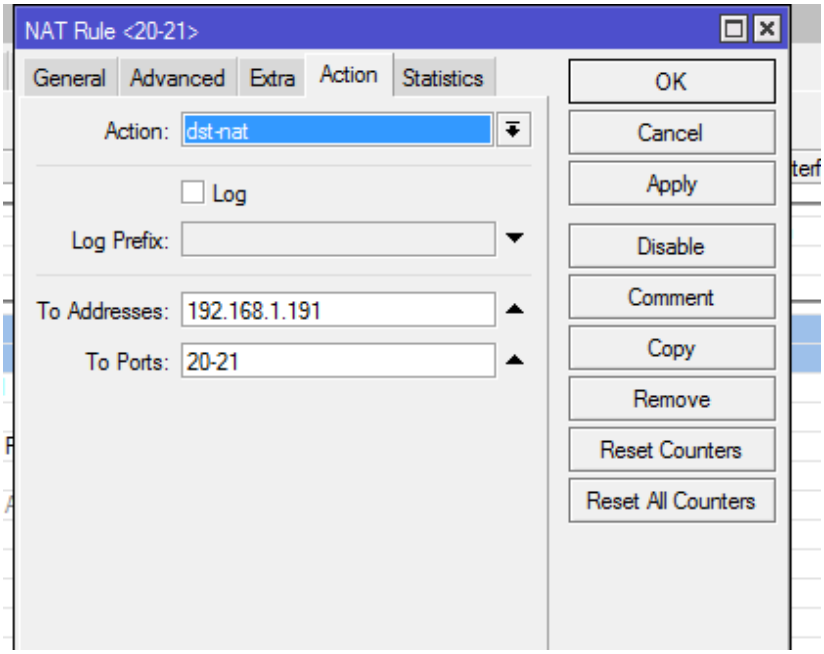

Figura 33 – Aba *Action* para redirecionamento de portas
Fonte: Autoria própria

No campo “Action” deve-se selecionar a opção “dst-nat”, no campo “To Addresses” deve-se informar o endereço IP que irá receber a solicitação e no campo “To Ports” deve-se informar a porta para conexão do endereço IP informado no campo anterior. Por fim, basta clicar no botão “OK” ou “Apply” para finalizar o procedimento.

APÊNDICE J – Script para QoS

O script utilizado para configuração de priorização para utilização do Skype em videoconferência e também da área de trabalho remota que deve ser executado no terminal:

```
/ip firewall layer7-protocol
add name=skypetoskype regexp="^..\02....."
add name=rdp regexp="rdpdr.*cliprdr.*rdpsnd"

/ip firewall mangle
add action=set-priority chain=forward comment="Prioridade Voip - skypetoskype" layer7-protocol=skypetoskype new-priority=7
add action=set-priority chain=forward comment="Prioridade Area de trabalho remota" layer7-protocol=rdp new-priority=7
```

APÊNDICE K – Configuração do Servidor Proxy

Para configuração do servidor Proxy no RouterOS, deve-se ir no menu IP → *Web Proxy*, conforme mostra a Figura 34.

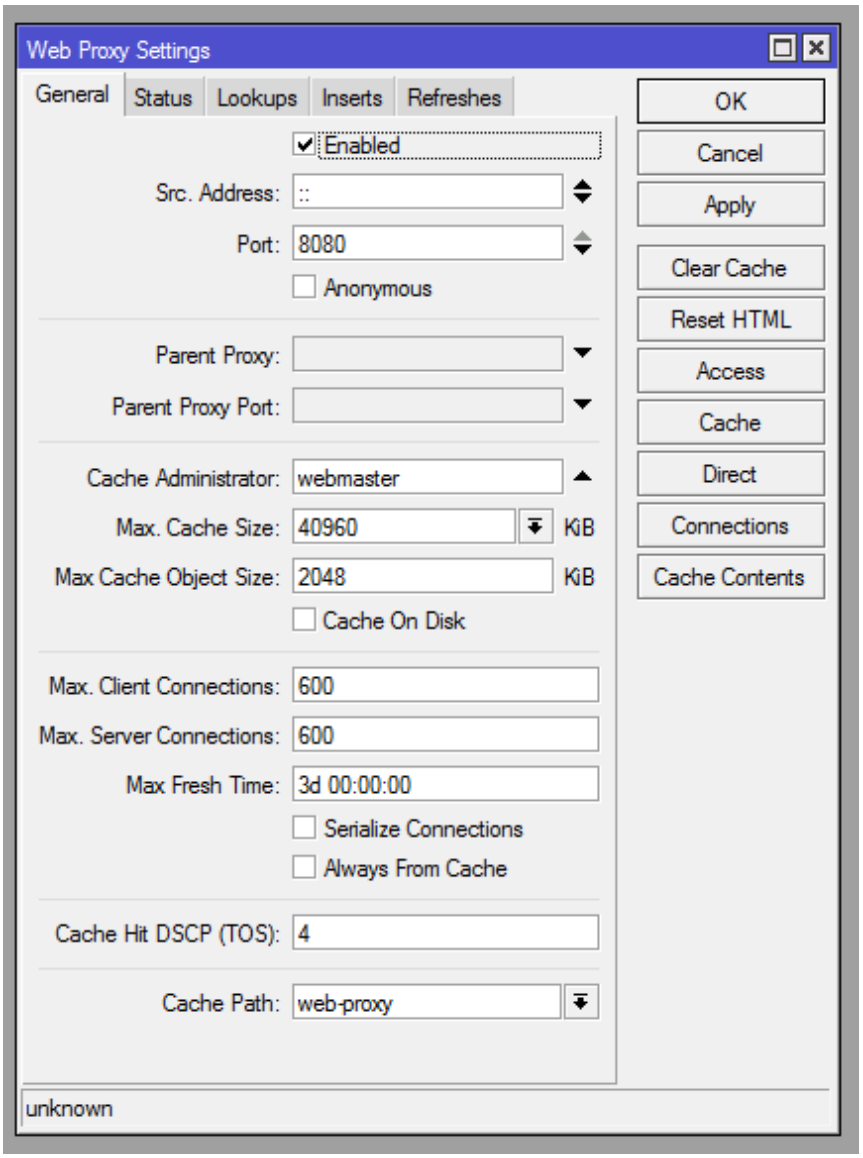

Figura 34 – Janela para configuração do Proxy
Fonte: Autoria própria

As configurações devem ser definidas conforme exibido na Figura 34, sendo possível alterar o campo “Port” para outra porta.

Para definir o bloqueio ou acesso a sites, deve-se clicar no botão “Access” que abrirá uma nova janela, exibida pela Figura 35. Nesta janela, deve-se clicar no botão + para adição de nova regra.

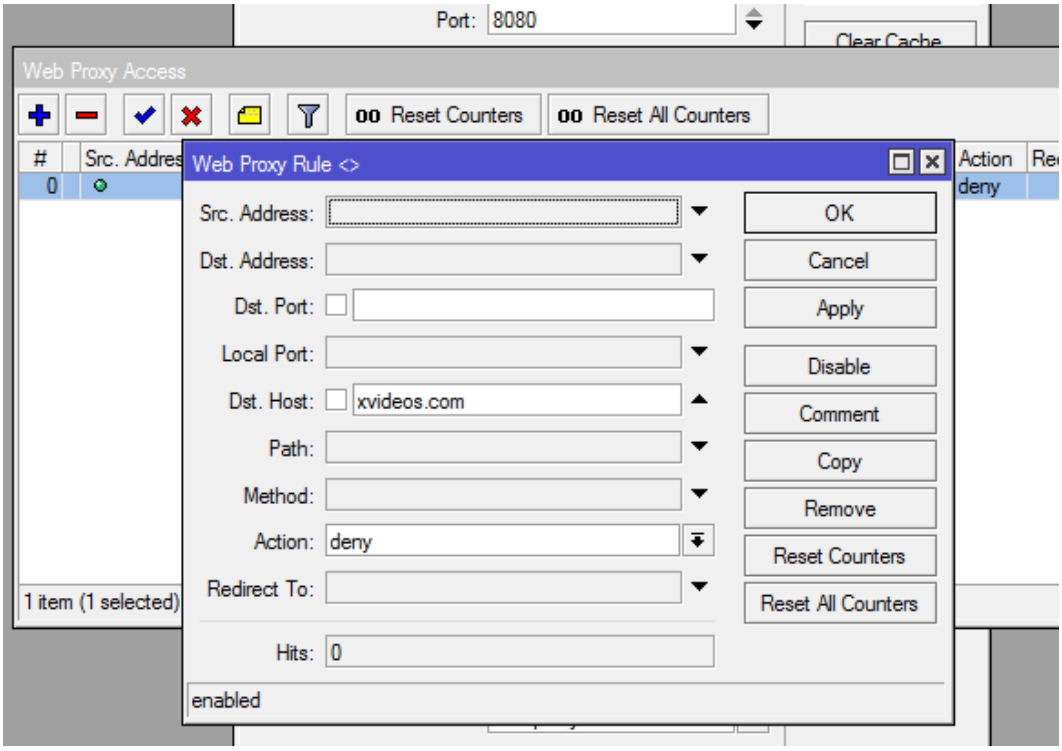

Figura 35 – Janela para bloqueio ou liberação de sites no Proxy
Fonte: Autoria própria

No campo “Dst. Address” pode informar o endereço IP do site que será acessado sendo possível também informar a porta no campo “Dst. Port”. Para controlar por endereço Host, deve-se informar o endereço no campo “Dst. Host” e no campo “Action” é definido se a regra irá bloquear ou liberar o acesso, escolhendo as opções “deny” ou “allow”, respectivamente.

Por fim, para deixar o servidor proxy transparente para o usuário, é definido uma regra no NAT do firewall redirecionado todo o trafego da porta 80 que entra pela interface 4 ou 5 para a porta definida no servidor proxy, selecionando como ação o tipo “redirect”. As Figuras 36 e 37 demonstram esta configuração.

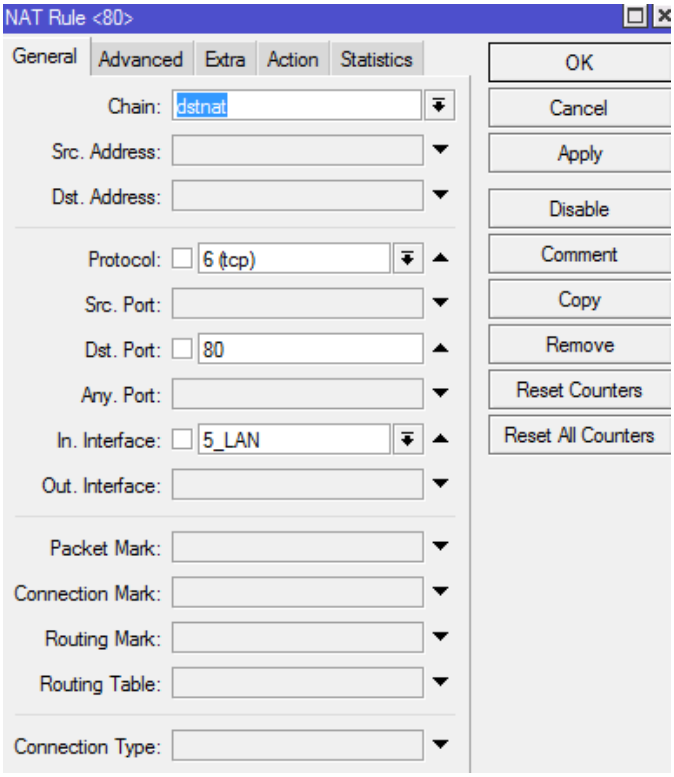

Figura 36 – Janela para regra de direcionamento para o Proxy
Fonte: Autoria própria

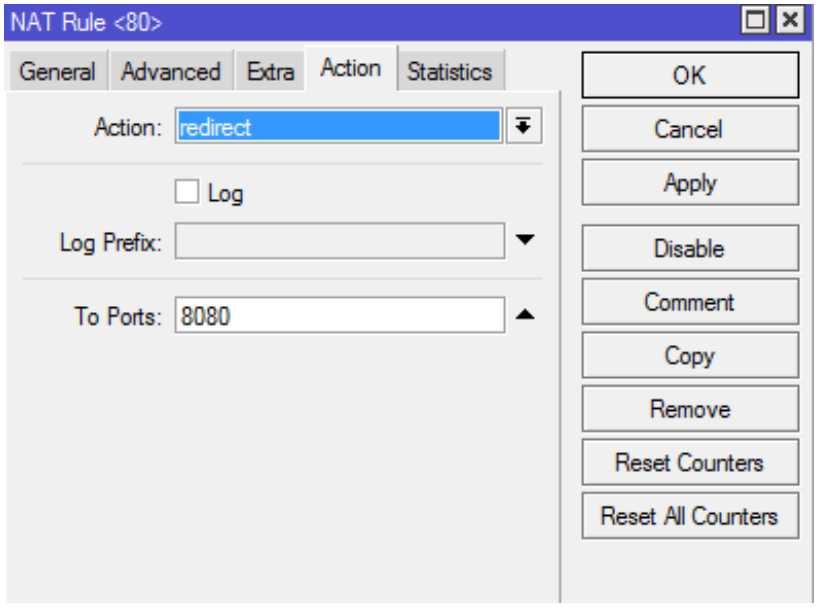

Figura 37 – Aba *Action* da regra de redirecionamento para o Proxy
Fonte: Autoria própria

APÊNDICE L – Configuração para Exibição de Gráficos.

Primeiramente, através do menu IP → Services, deve-se entrar na janela "IP Service List" que exibirá todos os serviços habilitados para acesso ao Routerboard, conforme pode ser visto na Figura 38.

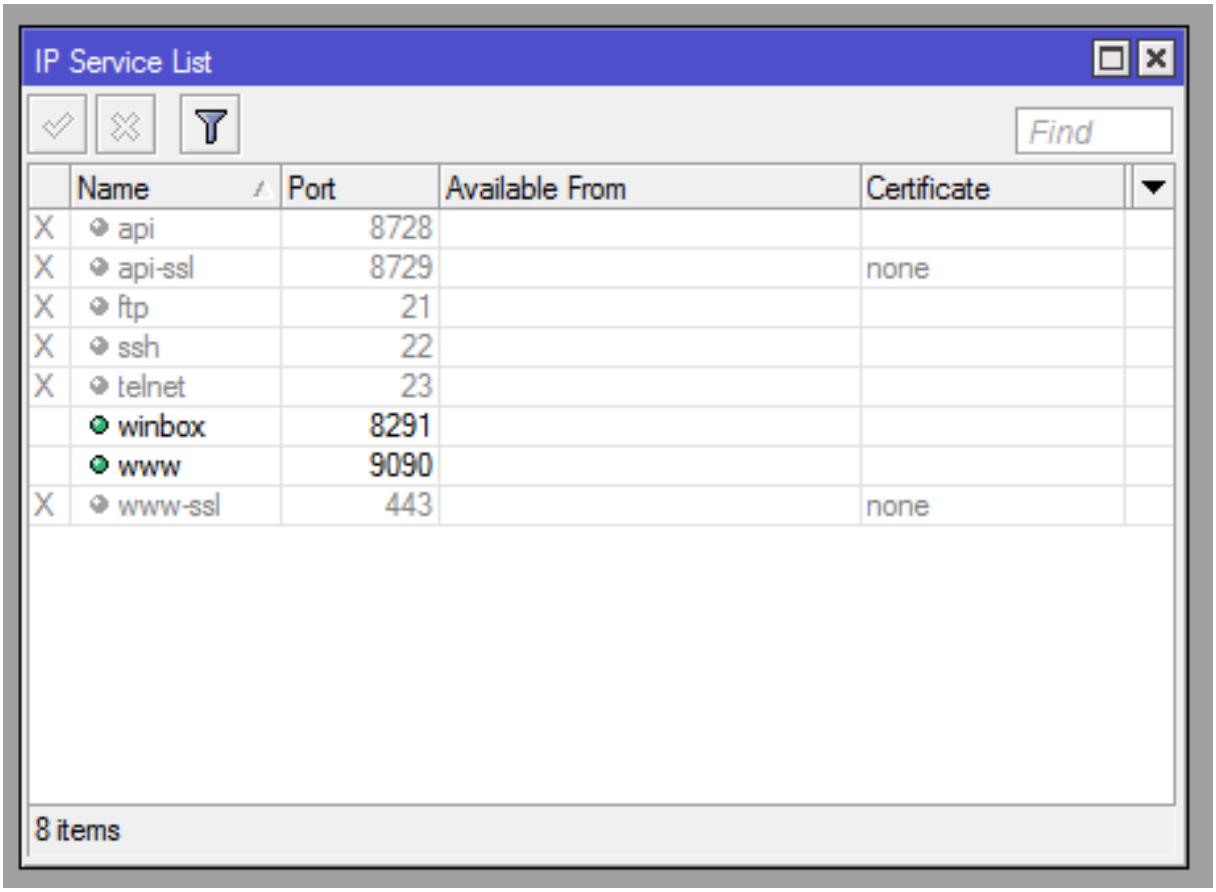

Figura 38 – Janela para configuração de serviços do Routerboard
Fonte: Autoria própria

Nesta tela, é possível desabilitar os serviços de acesso selecionando na lista e clicando no botão "X". Os serviços são pré-definidos e não é possível excluí-los ou adicioná-los, apenas alterar a porta de acesso e definir qual endereço IP poderá ter acesso pelo serviço.

Para alterar as configurações de um serviço, basta dar dois cliques em cima do serviço desejado, abrindo assim uma janela de edição, conforme pode ser visto pela Figura 39.

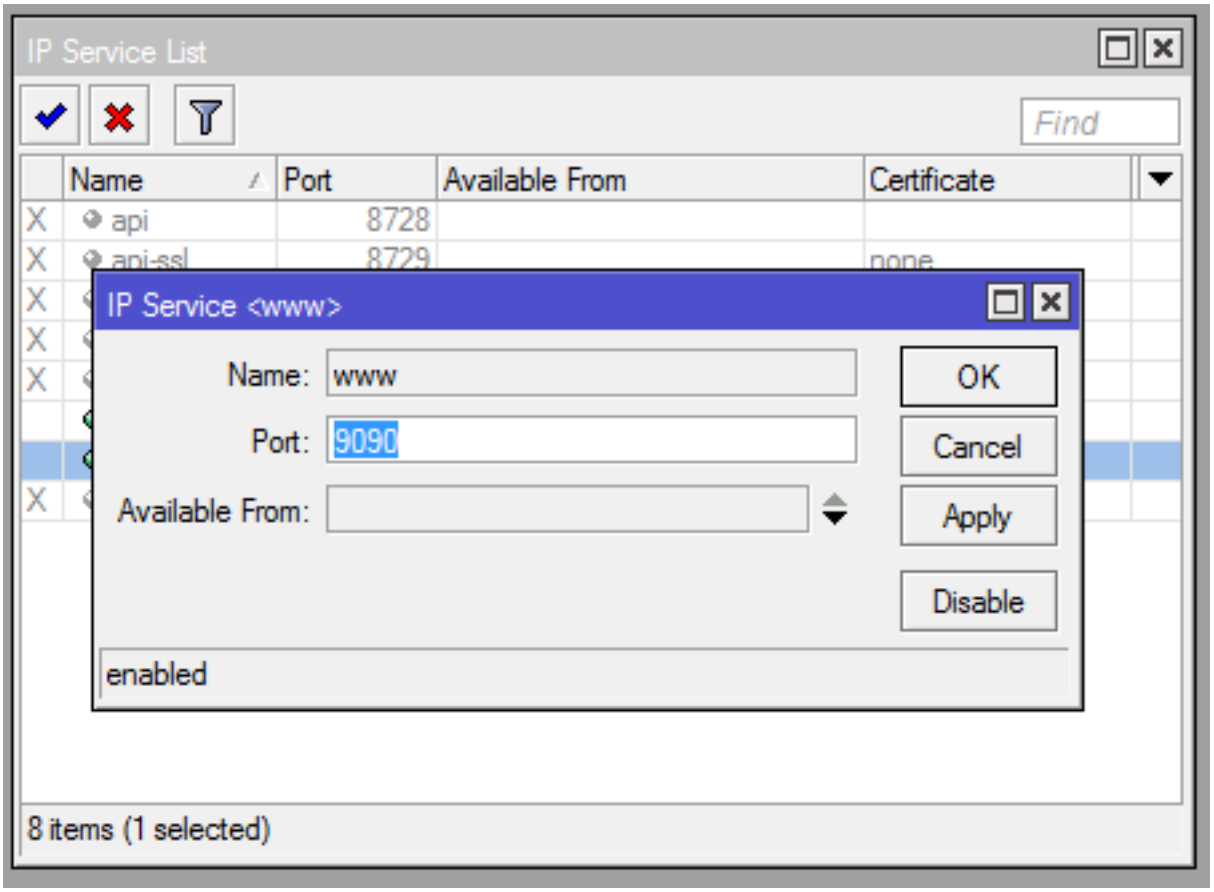

Figura 39 – Janela para alteração de serviços do Routerboard
Fonte: Autoria própria

No campo “Port” é definido a porta que será utilizada para acessar o serviço e no campo “Available From” o endereço IP que terá acesso liberado para o serviço. Por fim, basta clicar no botão “OK” ou “Apply” para finalizar o procedimento.

Após a definição dos serviços ativos no RouterOS, deve-se ir no menu Tools → Graphing para habilitar a exibição dos gráficos das interfaces e também dos recursos do aparelho, abrindo a janela “Graphing”.

Na aba “Interfaces Rules” é possível adicionar as interfaces que serão monitoras clicando no botão “+” e assim abrindo a tela de adição, conforme mostra a Figura 40.

No campo “Interface” é selecionado a interface que deseja monitorar e no campo “Allow Address” é informado qual endereço IP será monitorado na interface. A configuração utilizada neste projeto exibirá os dados de todas as interfaces com todos os endereços IP, conforme mostrado na Figura 40.

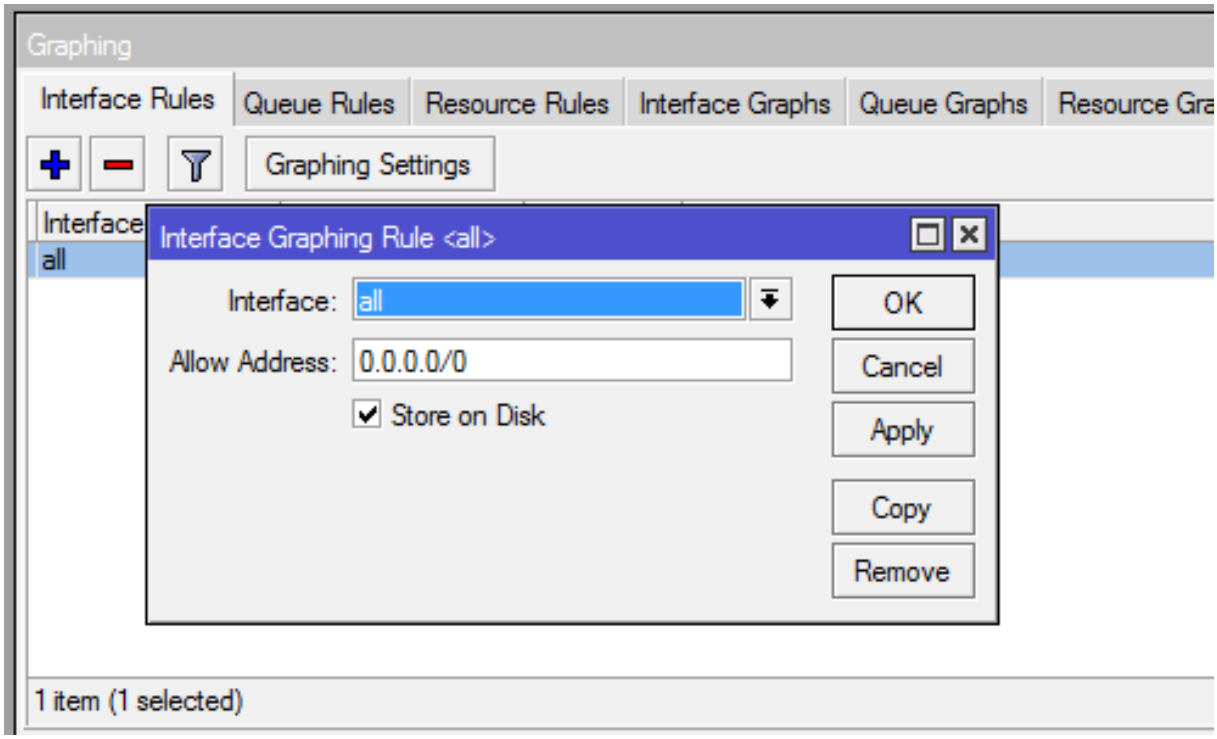

Figura 40 – Janela para adição de Gráficos das Interfaces
Fonte: Autoria própria

Na aba "Resource Rules", clicando no botão "+", é possível adicionar o monitoramento dos recursos do Routerboard, isto é, processamento, memória e disco, fazendo a configuração exibida na Figura 41.

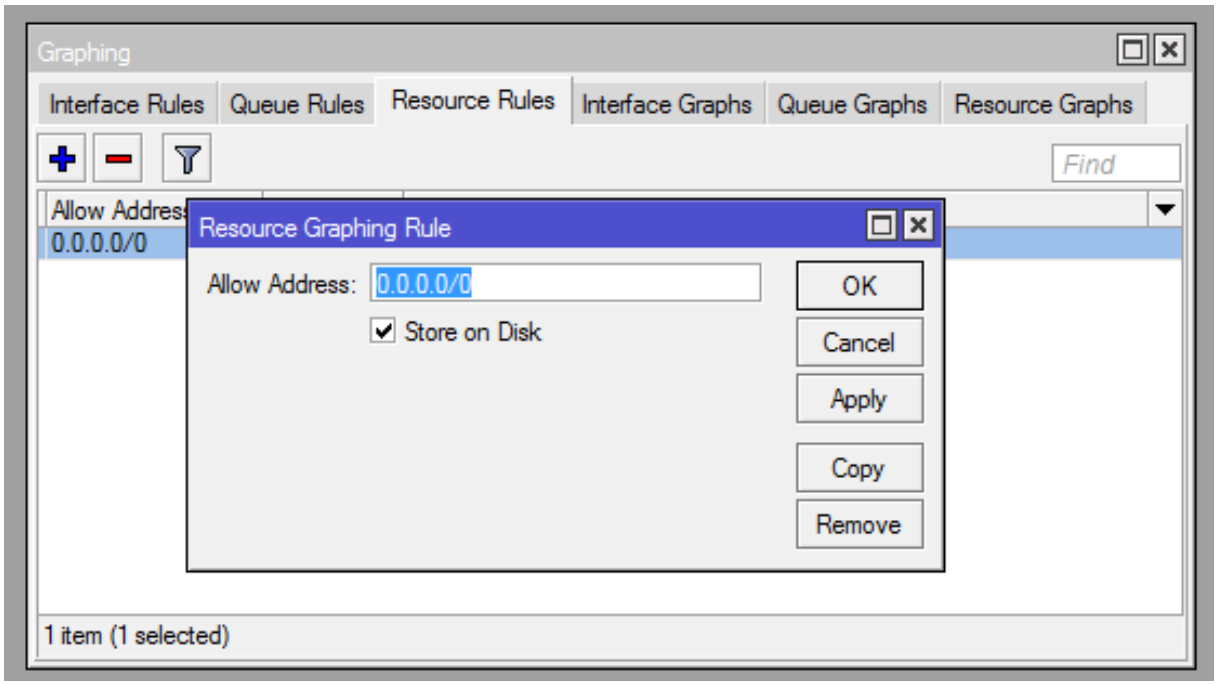

Figura 41 – Janela para adição de Gráfico para Recursos do Routerboard
Fonte: Autoria própria

Depois de efetuar todas essas configurações, basta acessar o Routerboard via navegador, informando o seu endereço IP com a porta configurada para o serviço WWW. Com isso será exibido uma tela conforme a Figura 42.

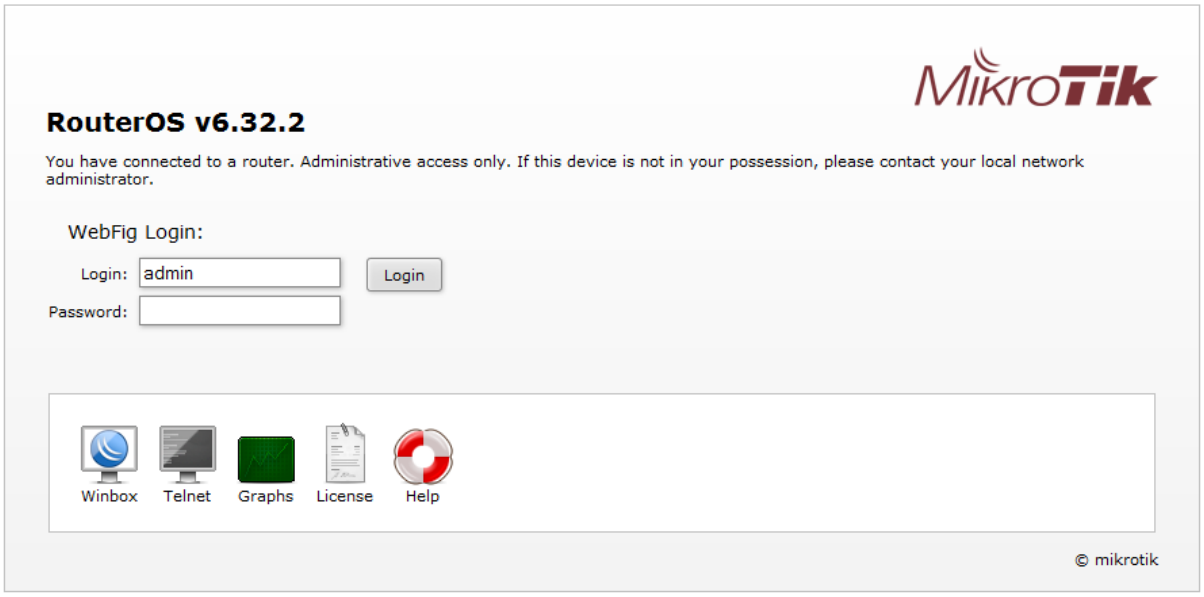

Figura 42 – Janela para acesso de gráficos do Routerboard
Fonte: Autoria própria

Nesta tela, basta clicar no ícone escrito “Graphs”, sem necessidade de informar usuário ou senha para acesso. Com isso será exibido uma tela conforme pode ser visto na Figura 43, exibindo os gráficos cadastrados no RouterOS.

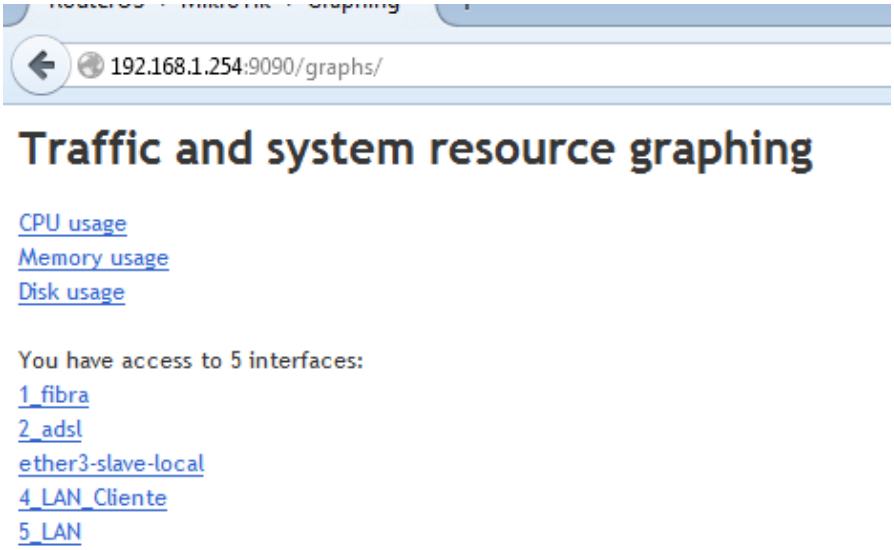

Figura 43 – Janela dos gráficos do Routerboard
Fonte: Autoria própria

A opção “CPU usage” exibe os gráficos de uso do processador enquanto a opção “Memory usage” exibe o gráfico de uso de memória e o “Disk usage” exibe o gráfico de uso de disco do Routerboard. As opções de gráfico para cada interface são exibidas conforme os nomes definidos no RouterOS para cada interface.

Os gráficos são exibidos em quatro categorias diferentes: diário, semanal, mensal e anual. Cada categoria tem um intervalo pré-definido de atualização, conforme pode ser visto na Figura 44.

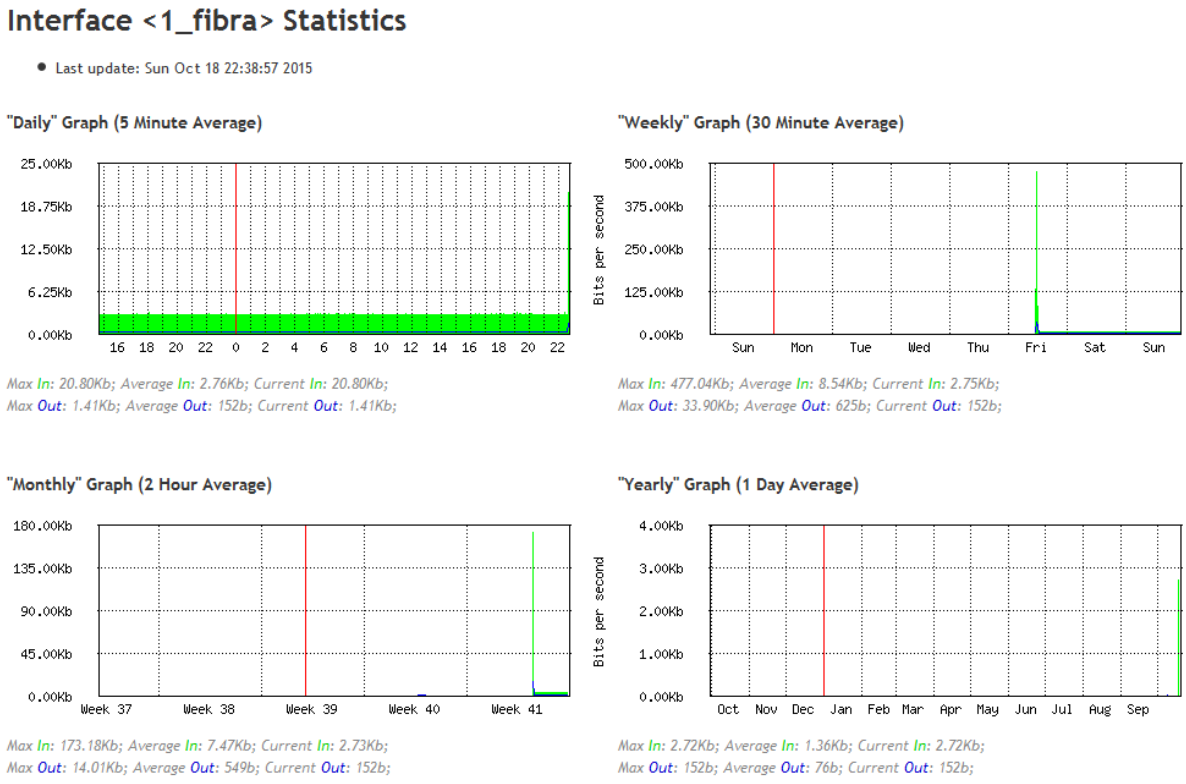

Figura 44 – Janela dos gráficos de uma interface
Fonte: Autoria própria

No caso dos gráficos das interfaces, são exibidos em cor verde o tráfego de entrada enquanto o tráfego de saía é exibido na cor azul.