Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GIOVANNI SANTELA DESIRÓ

ESTUDO SOBRE SEGURANÇA DA INFORMAÇÃO COM TECNOLOGIA MIKROTIK

Assis/SP
2019

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GIOVANNI SANTELA DESIRÓ

ESTUDO SOBRE SEGURANÇA DA INFORMAÇÃO COM TECNOLOGIA MIKROTIK

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Giovanni Santela Desiró
Orientador: Fábio Eder Cardoso

Assis/SP
2019

FICHA CATALOGRÁFICA

D457e DESIRÓ, Giovanni Santela

Estudo sobre segurança da informação com tecnologia MicroTik / Giovanni Santela Desiró. – Assis, 2019.

45p.

Trabalho de conclusão do curso (Ciência da Computação). – Fundação Educacional do Município de Assis-FEMA

Orientador: Me. Fábio Eder Cardoso

1.Segurança-informação 2.Tecnologia 3.Micro Tik

CDD 005.8

ESTUDO SOBRE SEGURANÇA DA INFORMAÇÃO COM TECNOLOGIA MIKROTIK

GIOVANNI SANTELA DESIRÓ

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Fábio Eder Cardoso

Examinador: _____
Luiz Carlos Begosso

Assis/SP
2019

DEDICATÓRIA

Dedico este trabalho ao meu professor e orientador Fábio Eder Cardoso, por seus ensinamentos em sala de aula, pois isso me despertou o interesse no assunto, com isso, me fez correr atrás, estudar, aprender, elaborar e apresentar esse trabalho.

AGRADECIMENTOS

Primeiramente a Deus por ter me capacitado e dado forças para conseguir pois sem Ele, nada seria possível para superar as minhas dificuldades.

Aos meus familiares, meu pai Célio Desiró e minha mãe Sueli Santela Desiró, por estarem sempre ao meu lado, apoiando-me e conduzindo-me durante minha caminhada.

RESUMO

Nos dias atuais a segurança da informação está se tornando cada vez mais essencial. No mundo globalizado, toda informação é uma fonte de renda para uma empresa, a quebra de sigilo dessas informações, podem acarretar no fracasso da mesma, podendo ir à falência. Os altos investimentos em segurança da informação, estão se tornando cada vez mais frequentes e novos equipamentos de controle de rede estão surgindo, sempre em inovação, para frear as tentativas de *hackers* em busca dessas informações. Esse estudo tem como base apresentar uma dessas tecnologias, a Mikrotik, um equipamento que traz mais segurança e confiabilidade a rede.

Palavras-chave: Segurança da Informação, Tecnologia, Mikrotik.

ABSTRACT

Nowadays information security is becoming increasingly essential. In the globalized world, all information is a source of income, breach of confidentiality of this information may lead to the failure of the same,can go bankrupt. High investments in information security, are becoming more and more frequent and new network control equipment is emerging, always in innovation, to halt hacking attempts get this information. This study is based on presenting one of these technologies, Mikrotik, a device that brings more security and reliability to the network.

Keywords: Information Security, Technology, MikroTik.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

MK - MikroTik

Sumário

1. **INTRODUÇÃO**

Diretamente relacionada com proteção de um conjunto de dados, a segurança da informação tem por finalidade preservar esses valores de uma organização ou um indivíduo. A segurança da informação tem como características básicas a confiabilidade, disponibilidade, integridade e autenticidade. Este conceito aplica-se em todos os aspectos de proteção de dados e informações (PERES, 2018).

Falhas na segurança da informação atinge o mundo globalizado, que está cada vez mais dependente da tecnologia e da internet. Essas ameaças estão comprometendo o sucesso de muitas empresas, essas vulnerabilidades necessitam ser estudadas para impedir os riscos e impactos causados ás mesmas (CAETANO; SOUZA; COSTA, 2014).

Thiago Tristão (2017), ressalta que a segurança da informação começou a ganhar mercado e ter uma cobertura mais adequada há cerca de cinco anos, e que essa demanda está vindo, em grande parte, de empresas com uma densa base dados de pessoas físicas para atendimento ao grande público.

A empresa de segurança Trustwave, divulgou recentemente ataques que atingiram roteadores brasileiros e que modificaram o tráfego web, fornecendo um código que minera a criptomoeda Monero diretamente pelo navegador web (*browser*). O ataque teve início no Brasil, mas acreditasse que 170 mil roteadores tenham sido atacados no mundo todo (ROHR, 2018).

1.1 **OBJETIVO**

O objetivo deste trabalho é apresentar a segurança da informação usando tecnologia MikroTik, configurando roteadores, afim de restringir acesso à rede, bloquear sites impróprios, controlar o tráfego de rede, bloquear portas, para inibir ataques e invasões de hackers.

1.2 **JUSTIFICATIVA**

Atualmente pequenas empresas têm muita dificuldade em fazer altos investimentos em segurança, para proteger seus dados e integridade. Este estudo visa um método de melhorar a segurança dessas empresas, tornando o processo mais eficiente e de menor custo. A proteção dos dados vem sendo cada vez mais exigida, a alma do negócio tem grande dependência dessa base de dados, “a nova moeda digital da atualidade” (CABRAL, 2018).

1.3 **PÚBLICO ALVO**

Este projeto tem como público alvo, todos usuários que necessitam encontrar de forma rápida o número de telefone e/ou endereço de algum estabelecimento alimentício. Agilizar esse processo e dar comodidade aos usuários.

1.4 **MOTIVAÇÃO**

O mercado de segurança da informação está se tornando muito atraentes para se empreender. De acordo com o (ISC)² Management (2017) a Gartner, identificou que em 2017 houve um investimento de 84,4 bilhões de dólares, um aumento de 7% em comparação com 2016, para 2018 estimasse um investimento de 93 bilhões de dólares.

O levantamento desses dados, por empresas e fundações reconhecidas, motivou a elaboração desse projeto.

2. PLANEJAMENTO DO PROJETO

Neste capítulo, será abordado a estrutura analítica do projeto (EAP), cronograma, orçamento e tecnologias previstas para o desenvolvimento do projeto.

2.1 ESTRUTURA ANALÍTICA DO PROJETO (EAP)

A Work Breakdown Structure (WBS) ou Estrutura Analítica do Projeto (EAP), é uma maneira de organizar o desenvolvimento de um projeto, ele é usado para definir o projeto e dividi-lo em tópicos com um formato hierárquico.

A organização da WBS passa por três níveis, sendo eles nível um, onde é definido o sistema geral, nível dois, onde temos os elementos principais que compõe o sistema e no nível três, onde temos os componentes subordinados.

A Figura 1 ilustra a EAP do projeto em desenvolvimento.

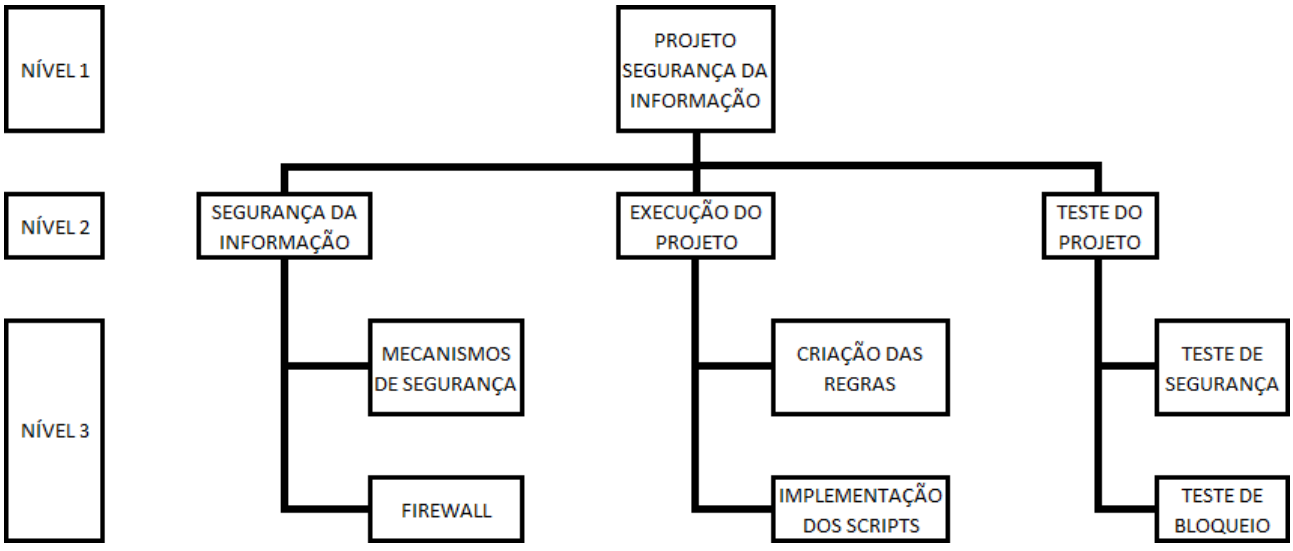

Figura 1 - Estrutura Analítica do Projeto (EAP)
Fonte - Giovanni Santela Desiró

2.2 **CRONOGRAMA**

O cronograma representa os prazos estabelecidos para o término de cada tópico presente no projeto proposto. Com os prazos estabelecidos, o desenvolvimento do projeto tornasse melhor, mais eficaz e rápido.

A Tabela 1 ilustra o Cronograma para o Desenvolvimento do projeto do Estudo Sobre Segurança Da Informação Com MikroTik.

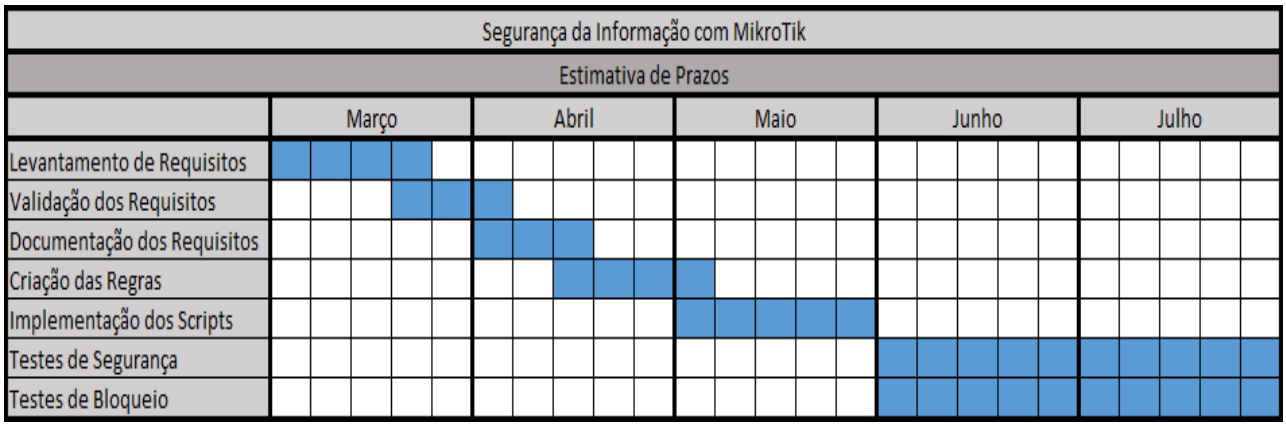

Tabela 1 - Cronograma do Projeto
Fonte - Giovanni Santela Desiró

2.3 **ORÇAMENTO**

A Tabela 2 apresenta os custos para o desenvolvimento deste projeto.

Item	Custo
Computador (Windows)	R$ 2.000,00
Mikrotik	R$ 200,00
TOTAL	R$ 2.200,00

Tabela 2 - Levantamento de Custos
Fonte - Giovanni Santela Desiró

2.4 **TECNOLOGIAS PREVISTAS**

A tecnologia estudada para a realização do projeto será: MikroTik RouterBoard.

A MikroTik é uma empresa que foi fundada na Letônia em 1996 para desenvolver roteadores e sistemas ISP (Internet Service Provider) sem fio. MikroTik agora fornece hardware e software para conectividade com a Internet na maioria dos países ao redor do mundo (SIA Mikrotīkls).

Em 1997 a MikroTik criou seu próprio sistema chamado RouterOS que fornece estabilidade extensiva, controles e flexibilidade para todos os tipos de interfaces de dados e roteamento. No ano de 2002 entra em cena a marca RouterBOARD, hardware criado pela própria MikroTik (SIA Mikrotīkls).

2.4.1 Mikrotik RouterBoard

MikroTik RouterBoard é um equipamento de gerenciamento de rede, capaz de assegurar a integridade da informação. Através de scripts de configuração é possível realizar bloqueios de sites impróprios, bloquear portas lógicas vulneráveis, controlar o tráfego dos pacotes da rede, verificar os pacotes que chegam da rede externa (internet), afim de assegurar que arquivos maliciosos não cheguem na rede interna.

O hEX Lite é um pequeno roteador ethernet de cinco portas em uma bela caixa de plástico, assim mostra a Figura 2.

Figura 2 - MikroTik hEX lite
Fonte - https://i.mt.lv/cdn/rb_images/1040_m.png

3. **SEGURANÇA DA INFORMAÇÃO**

Segundo o site Segurança da Informação (seguranca-da-informacao.info), a segurança da informação tem por finalidade a proteção de determinados dados, a fim de preservar seus respectivos valores para uma organização ou indivíduo.

Podemos entender como informação qualquer conteúdo que seja valioso para uma organização ou indivíduo que seja de utilidade ao ser humano.

Nos últimos anos, a informação digital se tornou um dos principais produtos da nossa era e consequentemente necessita ser protegida. A segurança dessas informações pode ser afetada de várias maneiras, por pessoas com o objetivo de destruir, modificar ou roubar as informações, como pelo ambiente, infraestrutura em que se encontra.

São características básicas da segurança da informação a confidencialidade, a disponibilidade e a integridade:

- Confidencialidade: informação que não pode ser divulgada para um usuário, entidade ou processo não autorizado;
- Integridade: informação não deve ser alterada ou excluída sem autorização;
- Disponibilidade: acesso aos serviços do sistema ou máquina para usuários ou entidades autorizadas;
- Autenticidade: garante que as informações provem da fonte anunciada e que não foi alvo de modificações ao longo de um processo.

A vulnerabilidade de um sistema ou computador pode representar possíveis pontos de ataque de terceiros.

3.1 **MECANISMOS DE SEGURANÇA**

Os mecanismos de segurança podem ser divididos em:

- **Controles físicos:** meios que protegem as informações limitando o contato ou acesso direto as mesmas. Tais como: portas, paredes etc.;

- **Controles lógicos:** meios que protegem as informações limitando o acesso as mesmas, todavia, ficando em exposição a alterações não autorizadas por elementos mal-intencionados. Tais como:
    - **Certificado digital e assinatura digital:** conjunto de normas e processos estabelecidos, que visam proporcionar maior segurança nas comunicações e transições eletrônicas (MACEDO, 2014);
    - **Controle de acesso:** conjunto de procedimentos com a finalidade de proteger os dados, programas e sistemas contra tentativa indevida, ou seja, não autorizada, de acesso aos dados (MACEDO, 2014);
    - **Criptografia:** técnicas que transformam a informação da sua forma original para uma forma ilegível, podendo ser conhecida apenas pelo destinatário da informação (MACEDO, 2014).

3.2 **FIREWALL**

Diego Macêdo (2012), evidencia que o firewall é um sistema de proteção de redes internas contra acesso não autorizados de redes externas (internet), ao mesmo tempo que permite o acesso controlado da rede interna à internet.

A Figura 3 traz uma representação figurada de como um firewall funciona.

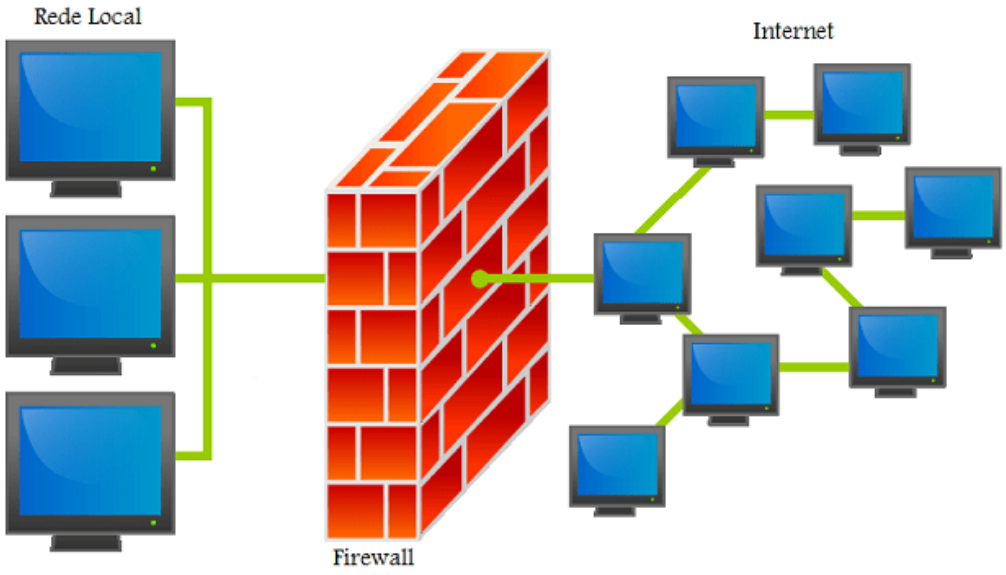

Figura 3 – Firewall
Fonte - https://i0.wp.com/www.diegomacedo.com.br/wp-content/uploads/2012/10/Firewall2.png?w=620&ssl=1

Apesar de estar geralmente relacionado a proteção contra invasões, o firewall não consegue analisar toda a extensão do protocolo, ficando geralmente restrito ao nível 4, de Transporte, da Camada OSI.

Algumas de suas características são:

- O tráfego entre a rede interna e a externa deve passar pelo Firewall;
- Apenas o tráfego autorizado passa pelo Firewall, o restante é bloqueado;
- O próprio Firewall deve ser seguro e impenetrável.

Tipos de controles realizados:

- Controle de Serviço: determinar quais tipos de serviços estarão disponíveis para acesso;
- Controle de Sentido: determinar o sentido de fluxo no qual serviços podem ser iniciados;
- Controle de Usuário: controlar o acesso baseado em qual usuário está requerendo;
- Controle de Comportamento: controla como cada serviço é usado.

3.3 **TIPOS DE FIREWALL**

Os três principais tipos de firewall são o filtro de pacotes, o filtro de pacotes com estado e o proxy.

3.3.1 Filtro de Pacotes

Este tipo de firewall controla o fluxo seletivo dos dados que chegam e saem de um segmento de rede, habilitando ou não, o bloqueio de pacotes baseando-se em regras especificadas via endereços IP, protocolos e tratamento do início da conexão (MACEDO, 2012).

A Figura 4 apresenta o filtro de pacotes na camada de rede.

Figura 4 - Filtro de Pacotes
Fonte - https://i0.wp.com/www.diegomacedo.com.br/wp-content/uploads/2012/08/Filtro-de-pacotes-no-contexto-da-pilha-TCPIP.png?w=491&ssl=1

3.3.2 Filtro de Pacotes com Estado

Este tipo de firewall realiza a mesma função que filtro de pacotes, porém ele também pode manter o estado da conexão através de máquinas de estado. Também possibilita o bloqueio de varreduras, o controle de fluxo de dados e o tratamento do cabeçalho TCP, além disso, verifica os campos do pacote, com a finalidade identificar possíveis ataques.

A Figura 5 apresenta o filtro de pacotes com estado na camada de rede e na camada de transporte.

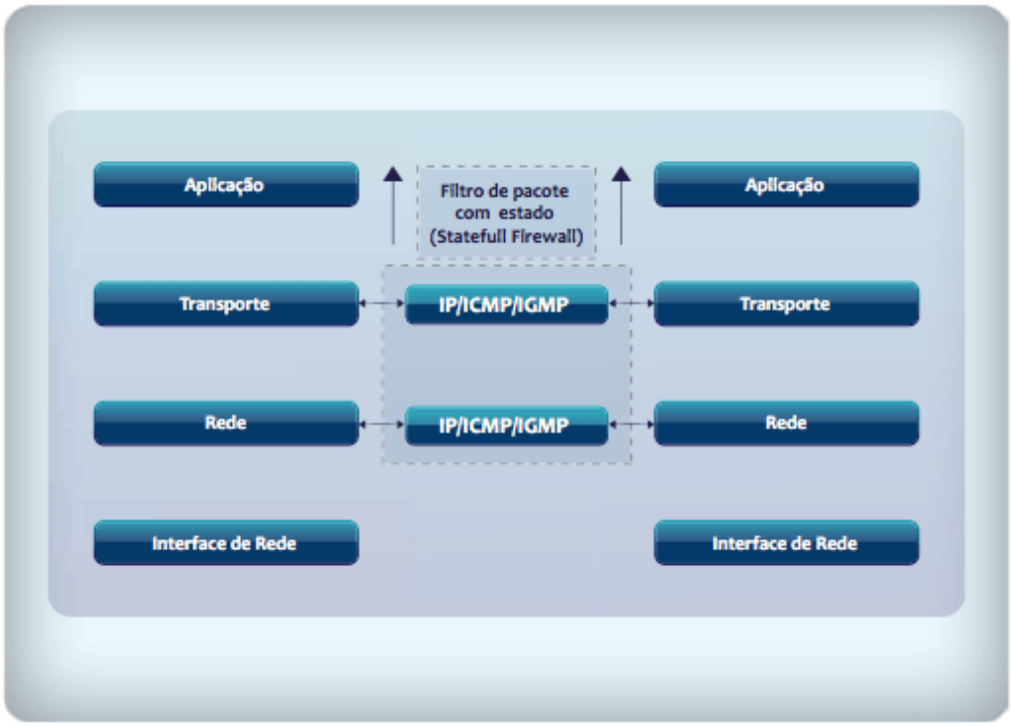

Figura 5 - Filtro de Pacotes com Estado
Fonte - https://i2.wp.com/www.diegomacedo.com.br/wp-content/uploads/2012/08/Filtro-de-pacotes-de-estados-Statefull.png?w=512&ssl=1

3.3.3 Proxy

Diego Macêdo (2012), enfatiza que o proxy é um recurso do firewall que combina o controle de acesso com a funcionalidade da camada superior. O firewall possui um proxy que atua como intermediário entre a comunicação e não permite uma conexão direta. Toda conexão realizada com sucesso resulta na criação de duas conexões separadas, uma entre o cliente e o servidor proxy e outra entre o servidor proxy e o seu verdadeiro destino, conforme apresentado na Figura 6.

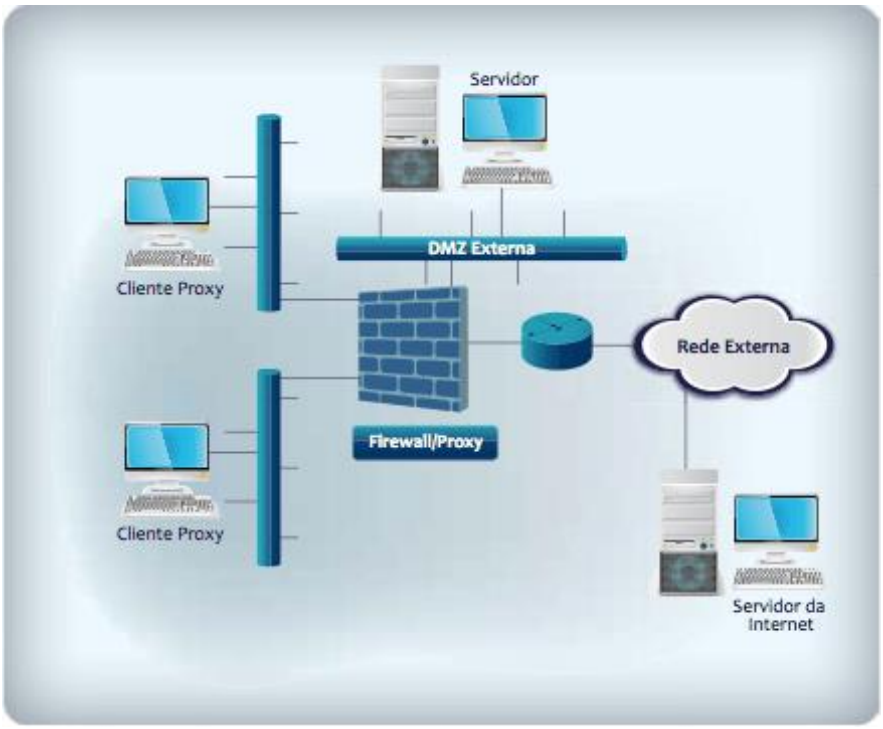

Figura 6 - Proxy na Rede
Fonte - https://i2.wp.com/www.diegomacedo.com.br/wp-content/uploads/2012/08/Proxy-na-rede.png?w=437&ssl=1

4. EXECUÇÃO DO PROJETO

Neste capítulo serão apresentadas as principais configurações da MikroTik RouterOS, detalhando o processo desse trabalho de segurança de rede.

4.1 WINBOX

WinBox é um programa executável usado para conectar e para configurar MikroTik RouterOS via terminal e interface gráfica. Na Figura 7 é apresentado o logo da WinBox.

Figura 7 - Logo WinBox
Fonte - https://whendy.net/wp-content/uploads/2017/05/winbox-310x165.png

Para acessar a MikroTik, basta realizar o login através do WinBox. Após o login, será possível acessar todos os módulos de configurações presentes na interface gráfica, para fácil configuração. A Figura 8 mostra a tela de login do WinBox e a lista de equipamentos disponíveis.

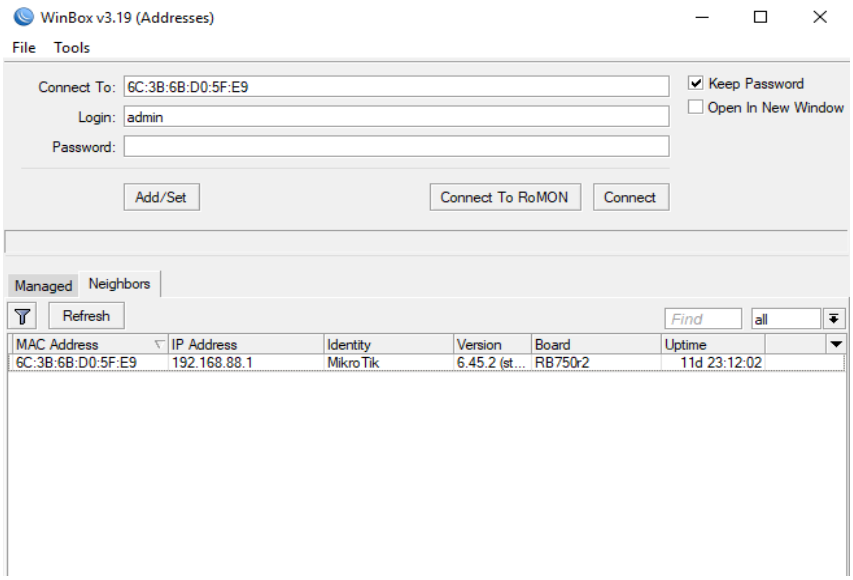

Figura 8 – Tela de Login do WinBox
Fonte - Giovanni Santela Desiró

A tela inicial do WinBox apresenta um painel, onde localiza-se todas as opções disponíveis para a configuração da MikroTik.

Para atender aos propósitos deste trabalho, foram utilizadas as configurações encontradas na categoria Interfaces, IP (Address List, DHCP Server, DNS, Firewall, IP Pool e Route List) e System (SNTP Client e User List). A Figura 9 apresenta a tela inicial do WinBox, com destaque para a lista de categorias à esquerda da tela.

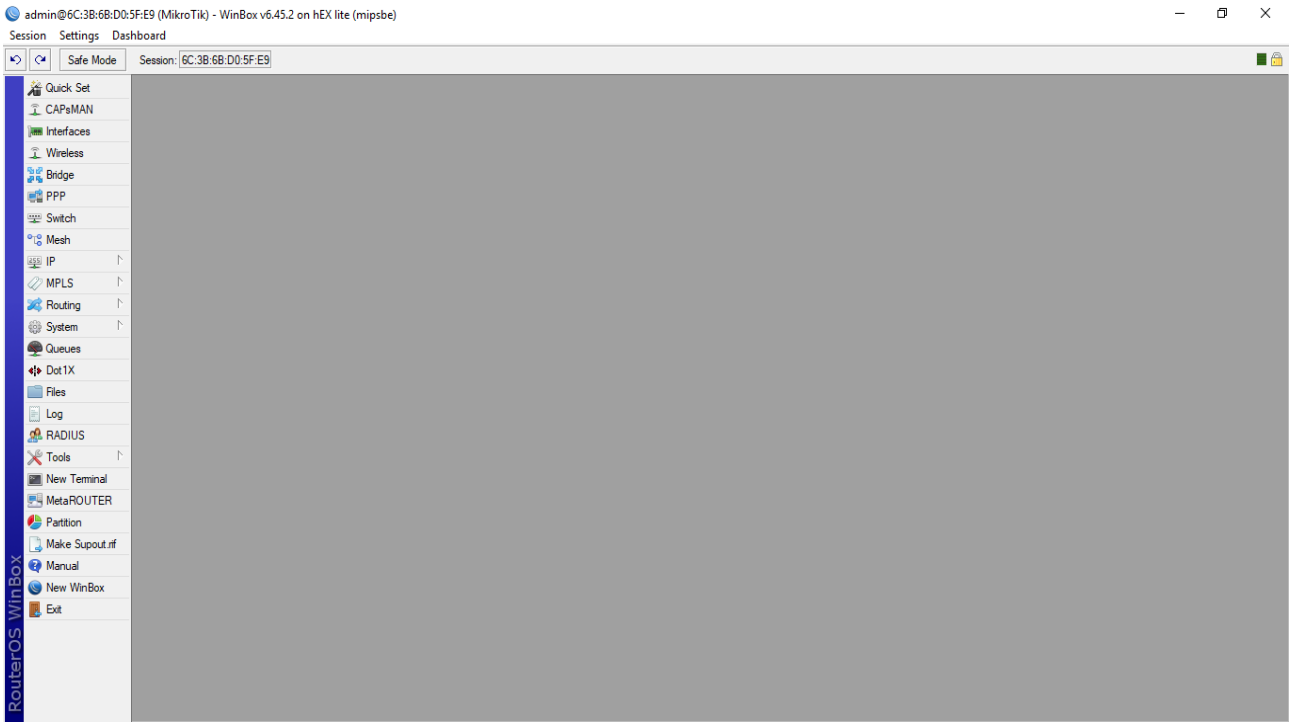

Figura 9 - Tela Inicial do WinBox
Fonte - Giovanni Santela Desiró

4.2 **INTERFACES**

A categoria Interfaces fornece as opções para a configuração das portas da MK, tanto portas WAN quanto portas LAN. Na Figura 10 é apresentado um exemplo de uma MikroTik configurada com duas interfaces WAN e uma interface LAN.

Nas Interfaces WAN são configuradas as redes externas e nas Interfaces LAN são configuradas as redes internas.

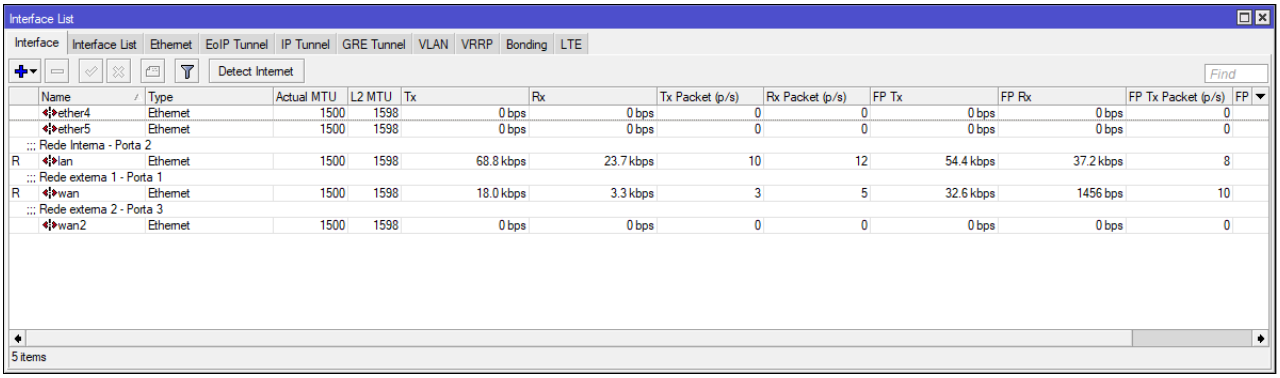

Figura 10 – Interfaces
Fonte - Giovanni Santela Desiró

4.3 **IP**

A categoria IP disponibiliza várias opções para a realização de diversas configurações, porém, foram utilizadas apenas as necessárias para cumprir o propósito deste trabalho.

A seguir são apresentadas as configurações feitas na categoria IP para a conclusão deste trabalho.

4.3.1 Address List

Na address list são configurados os endereços, as redes e em quais interfaces elas estão. A Figura 11 mostra uma lista com três endereços, sendo dois endereços de interface de rede WAN e um endereço de rede LAN.

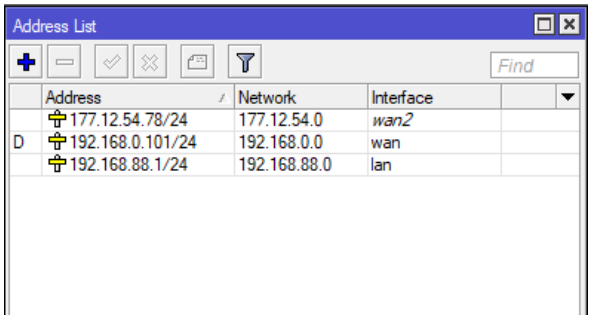

Figura 11 - Address List
Fonte - Giovanni Santela Desiró

4.3.2 DHCP Server

Na opção DHCP *Server* é declarado o nome pelo qual a rede será reconhecida, para configurações futuras em outras opções da MK, por qual interface ela trabalhará, assim como seu *lease time*, ou seja, por quanto tempo os equipamentos poderão usar determinado IP (neste caso está definido em 8 horas). A Figura 12 demonstra o DHCP Server configurado na MikroTik.

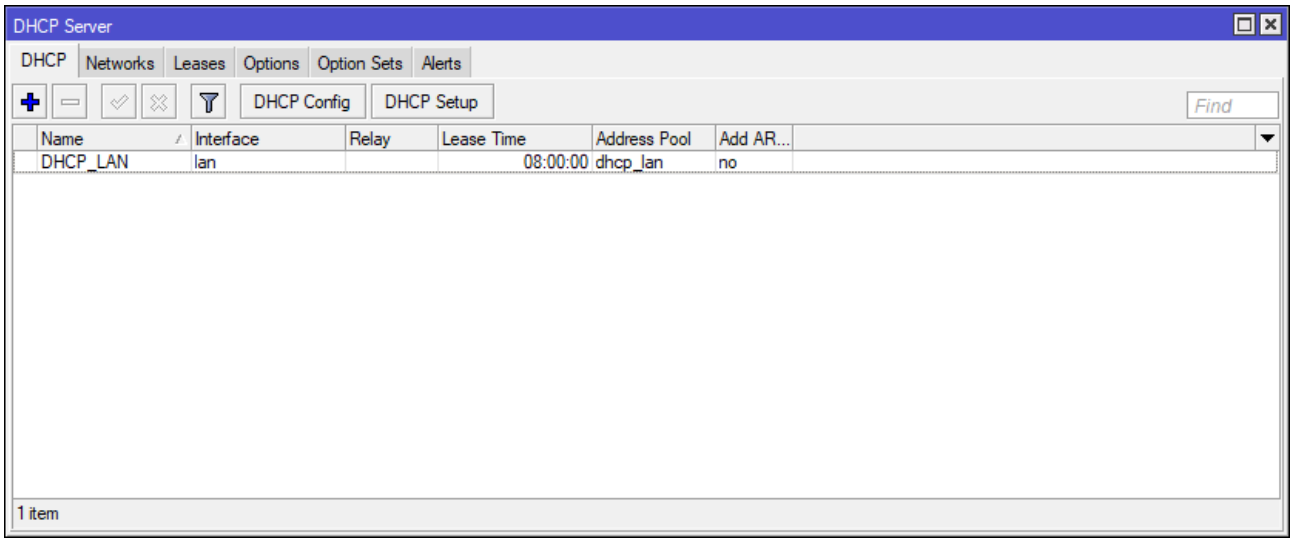

Figura 12 - DHCP Server
Fonte - Giovanni Santela Desiró

4.3.3 DNS

Na opção DNS são declarados os endereços de servidores de nomes para relacionar o endereço nominal com o endereço real, como por exemplo, o endereço real (IP) 216.58.202.174 se relaciona com o endereço nominal www.google.com, facilitando assim a memorização do mesmo. A Figura 13 apresenta alguns DNS padrões.

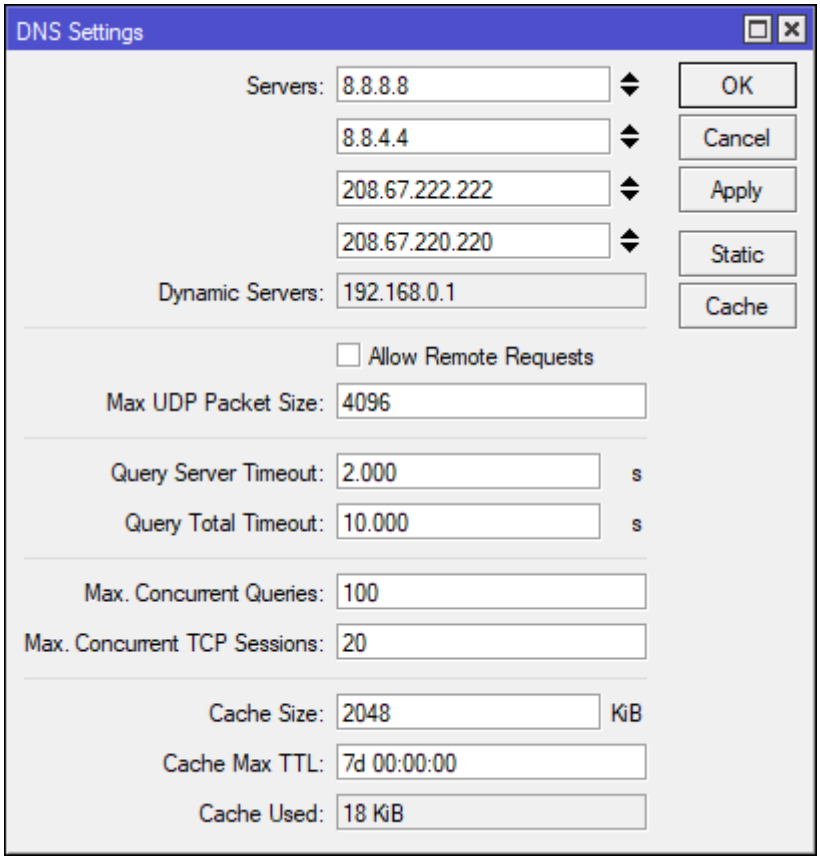

Figura 13 – DNS
Fonte - Giovanni Santela Desiró

4.3.4 Firewall

O firewall disponível no RouterOS é do tipo Stateful Firewall, ou seja, ele rastreia o estado operacional e as características das conexões de rede que passam por ele. Esse firewall funciona basicamente como *tables*, agrupando as regras em *chains* que determinam o fluxo.

São utilizadas 3 *tables*: Filter Rules, NAT e Mangle.

A *table* Filter Rules é responsável por filtrar os pacotes, ou seja, ela faz uma varredura nos pacotes, onde o *netfilter* é informado que política ele terá que adotar ao observar a passagem desse pacote e para saber o que deve ser feito com o pacote, prontamente entram as *chains* desta *table* (ODON, 2016)

A Figura 14 demonstra algumas regras configuradas na table Filter Rules.

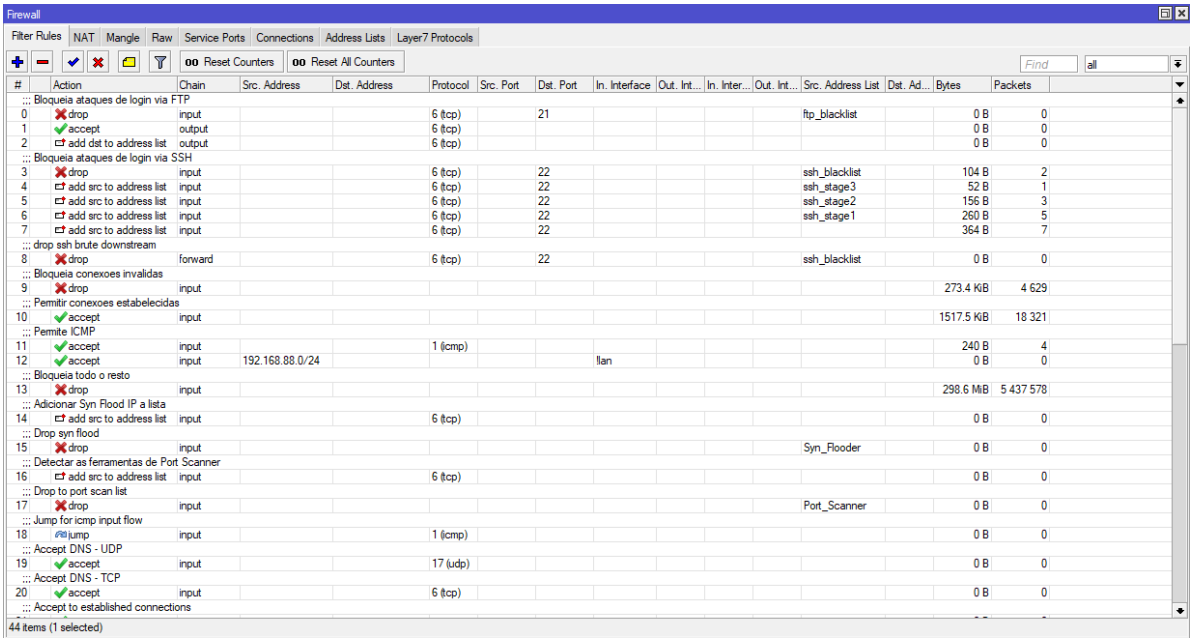

Figura 14 - Firewall: Filter Rules
Fonte - Giovanni Santela Desiró

A *table* NAT controla a tradução dos endereços que atravessam o código de roteamento. Existem três *chains* na *table* NAT: PREROUTING, OUTPUT e POSTROUTING (SCHLEMER, 2007)

Para acessar a internet deve-se criar a seguinte regra no terminal:

ip firewall nat add chain=srcnat src-address=192.168.88.0/24 out-interface=WAN action=masquerade

ip firewall nat add chain=srcnat src-address=192.168.88.0/24 out-interface="WAN 2" action=masquerade.

A Figura 15 demonstra essas regras.

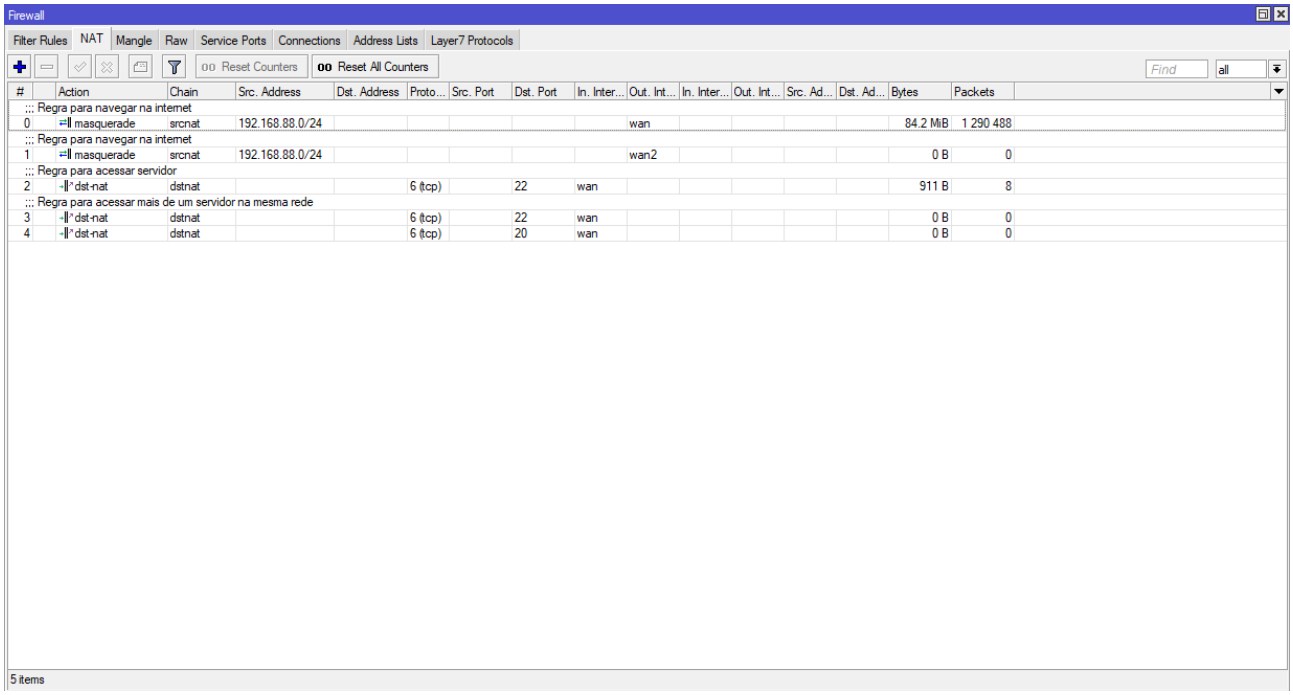

Figura 15 - Firewall: NAT
Fonte - Giovanni Santela Desiró

A *table* Mangle especifica quais ações especiais devem ser usadas para o tratamento do tráfego que atravessa as chains. Existem cinco *chains* na *table* Mangle: PREROUTING, POSTROUTING, INPUT, OUTPUT e FORWARD (GUIA DO LINUX, 2011).

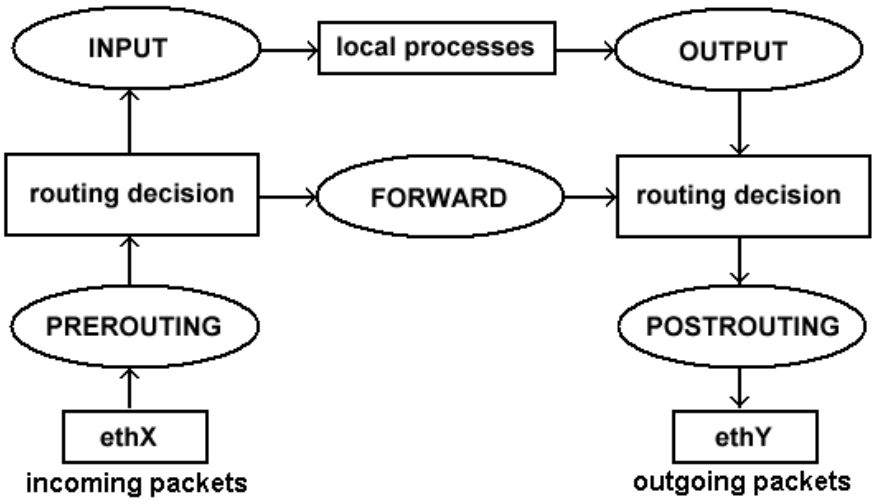

Figura 16 - Processamento NAT
Fonte - http://www.system-rescue-cd.org/images/dport-routing-02.png

Para evitar *loop* na rede interna e na rede externa cria-se as seguintes regras para a *table* Mangle:

ip firewall mangle add chain=prerouting action=accept src-address=192.168.88.0/24 dst-address=192.168.88.0/24 comment="Evitar loop na rede local"

ip firewall mangle add chain=prerouting action=accept src-address=192.168.88.0/24 dst-address=192.168.1.87/24 comment="Evitar Loop na Interface WAN"

ip firewall mangle add chain=prerouting action=accept src-address=192.168.88.0/24 dst-address=177.12.54.78 comment="Evitar Loop na Interface WAN2".

A Figura 17 demonstra essas regras.

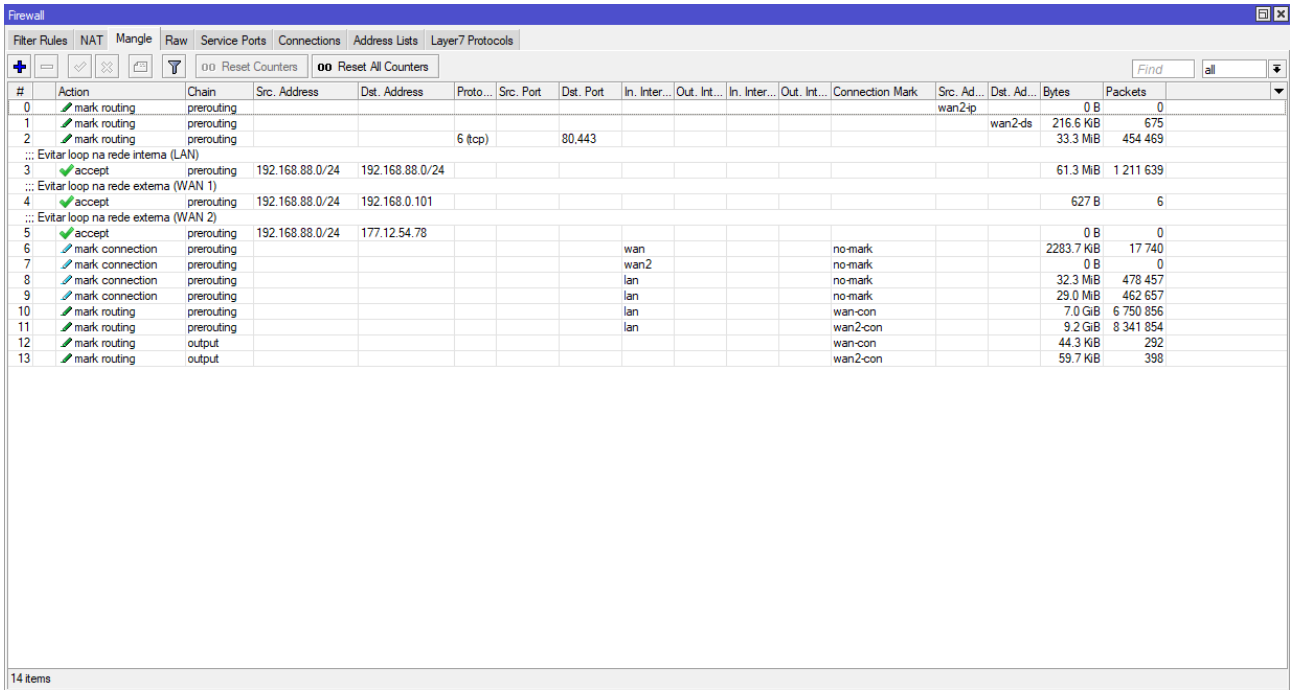

Figura 17 - Firewall: Mangle
Fonte - Giovanni Santela Desiró

Na aba Address Lists é possível criar listas de endereços IP agrupados sob um nome comum, como exemplo, um departamento de uma empresa. As regras de firewall, mangle e NAT podem utilizar essas listas de endereços para encaminhar os pacotes a eles.

Para criar regras para controlar pacotes de sites como Youtube e Facebook respectivamente, utilizam-se os seguintes comandos no terminal:

ip firewall address-list add address=216.58.202.206 list=WAN2-DST

ip firewall address-list add address=157.240.12.35 list=WAN2-DST

A Figura 18 apresenta as regras configuradas.

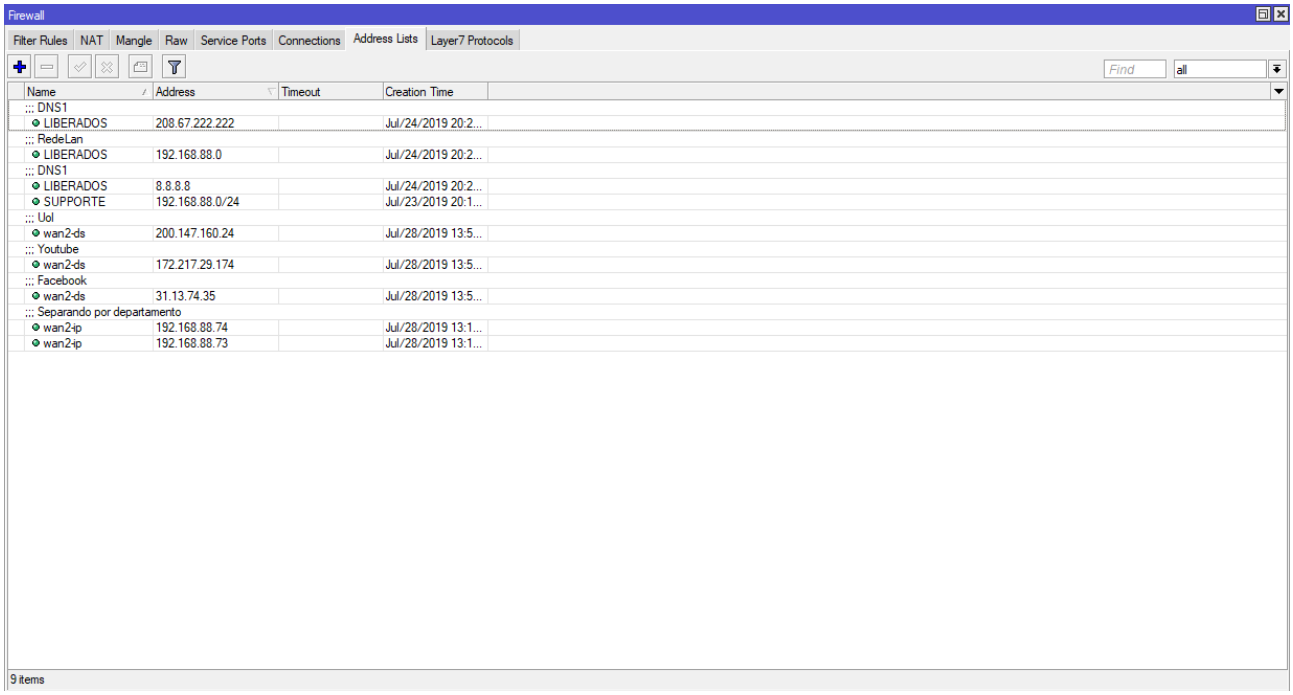

Figura 18 - Firewall: Address Lists
Fonte - Giovanni Santela Desiró

Na aba Layer7 Protocols criam-se regras específicas para bloquear pacotes de determinado site ou conjunto de sites, como sites de download para arquivos Torrents ou até mesmo para sites impróprios.

Para criar regras para controlar esses pacotes, utiliza-se o seguinte comando no terminal:

ip firewall layer7-protocol add name=torrentsites regexp="^.*(get|GET).+(torrent|thepiratebay|isohunt|entertane|demonoid|btjunkie|mininova|flixflux|torrentz|vertor|h33t|btscene|bitunity|bittoxic|thunderbytes|entertane|zoozle|vcdq|bitnova|bitsoup|meganova|fulldls|btbot|flixflux|seedpeer|fenopy|gpirate|commonbits).*\$\ ".

A Figura 19 demonstra esse tipo de bloqueio.

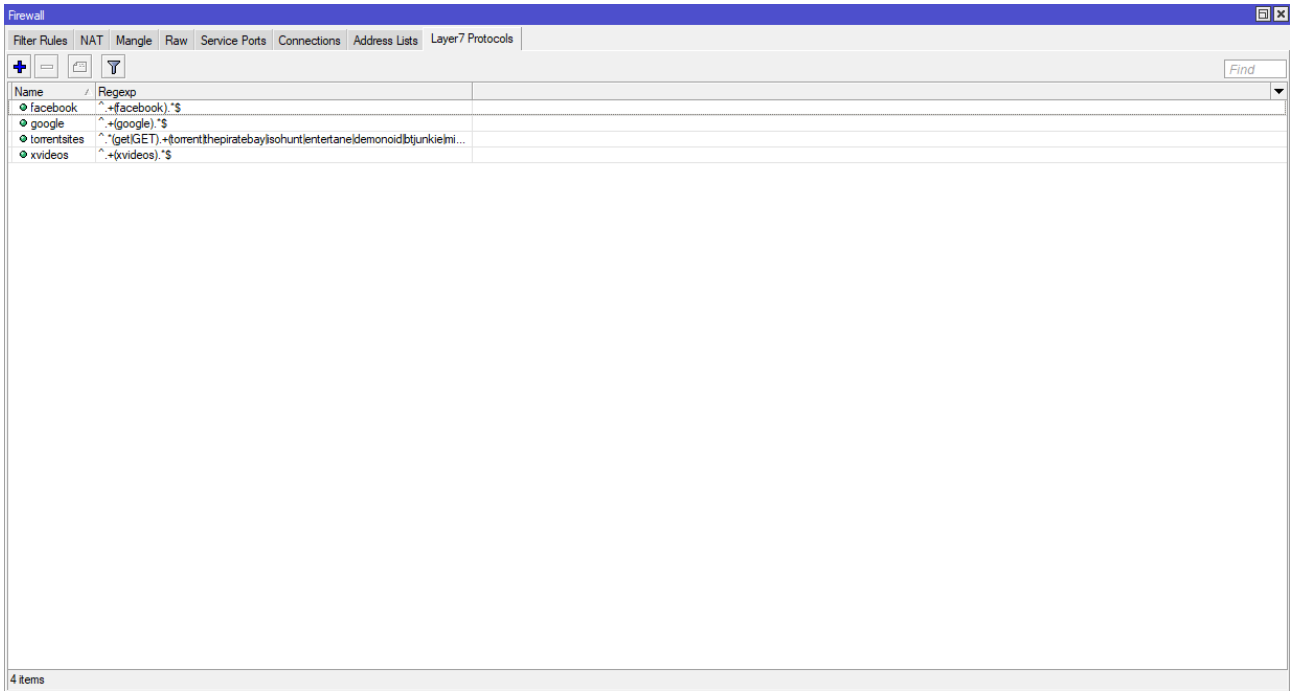

Figura 19 - Firewall: Layer7 Protocols
Fonte - Giovanni Santela Desiró

4.3.5 IP Pool

Na opção IP Pool é definido o *range* da rede, ou seja, quais IPs estarão disponíveis na rede, para conexões dos dispositivos, como computadores, notebooks e celulares. Através do terminal utiliza-se o comando:

ip pool add name=dhcp_lan ranges=192.168.88.2-192.168.88.250.

Na Figura 19 é apresentado o *pool* configurado para a rede interna.

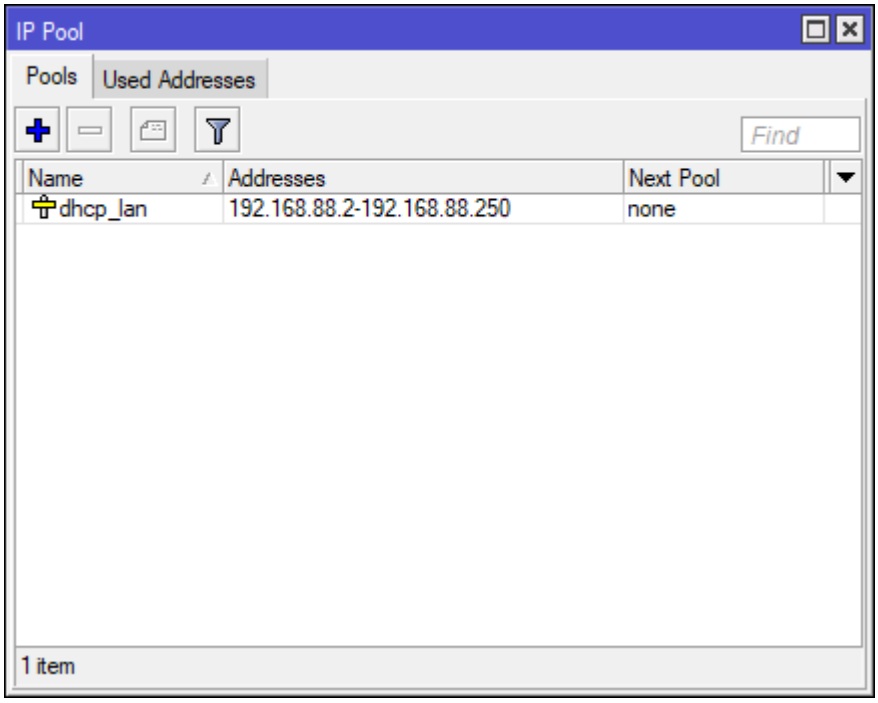

Figura 20 - IP Pool
Fonte - Giovanni Santela Desiró

4.3.6 Route List

Na opção Routes são criadas as rotas estáticas, que podem trabalhar com balanceamento tanto pela origem quanto pelo destino, ou até mesmo balanceamento de links, ou seja, com diferentes internets, como demonstrado na Figura 21 através do “Link Primário” e “Link Secundário”.

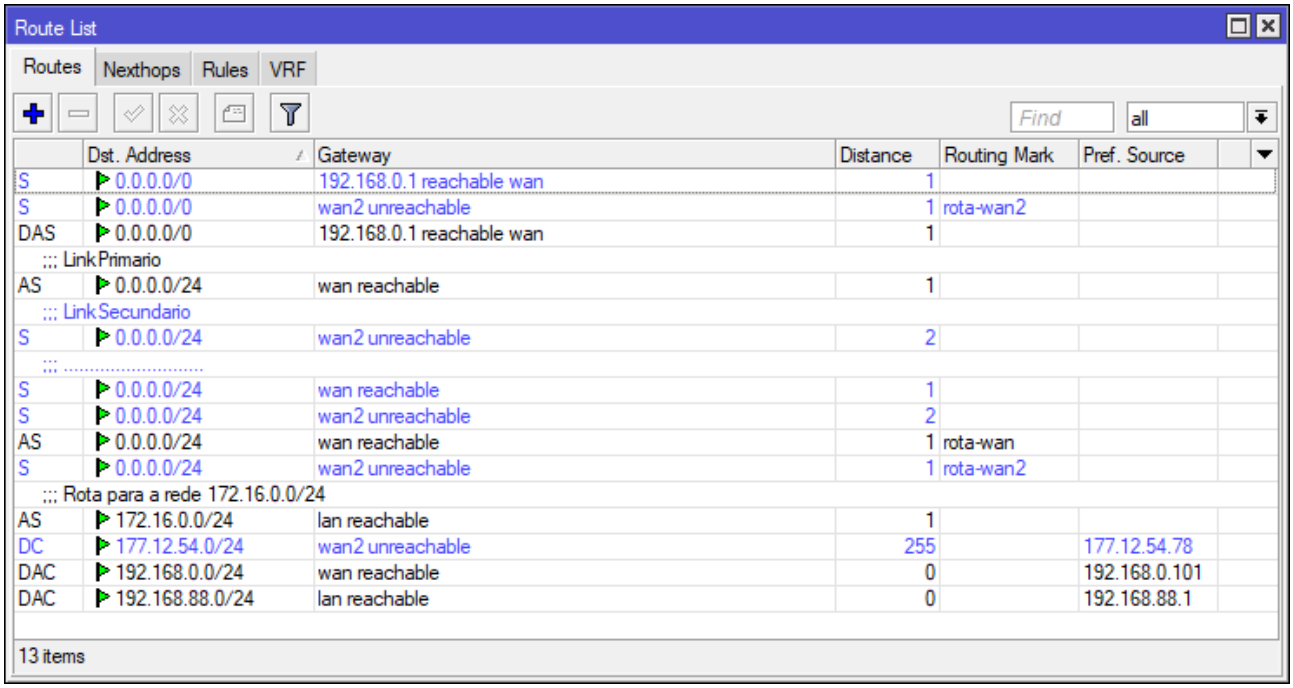

Figura 21 - Route List
Fonte - Giovanni Santela Desiró

Para criar uma rota estática através do terminal usa-se os comandos:

ip route add dst-address=172.16.0.0/24 gateway=LAN.

Para criar o balanceamento, primeiro é necessário preparar o ambiente da MK, com os seguintes comandos:

ip firewall nat add chain=srcnat src-address=192.168.88.0/24 out-interface=WAN action=masquerade

ip firewall nat add chain=srcnat src-address=192.168.88.0/24 out-interface="WAN 2" action=masquerade

ip route add dst-address=0.0.0.0/24 gateway=WAN distance=1;

ip route add dst-address=0.0.0.0/24 gateway=”WAN 2” distance=2.

Depois de preparar o ambiente da MikroTik, pode-se criar o balanceamento de links, com os seguintes comandos:

ip route add dst-address=0.0.0.0/24 gateway=WAN distance=1

ip route add dst-address=0.0.0.0/24 gateway="WAN 2" distance=2

ip route add dst-address=0.0.0.0/24 gateway=WAN distance=1 routing-mark=Rota-WAN

ip route add dst-address=0.0.0.0/24 gateway="WAN 2" distance=1 routing-mark=Rota-WAN2.

Finalizando com esses comandos, a rede estará balanceada com dois links de internet, ou seja, dois provedores diferentes.

4.4 **SYSTEM**

Na categoria System pode-se alterar várias opções do sistema da MK, como o relógio, histórico de modificações que são realizadas em suas configurações e ativar e desativar os LEDs de cada Interface.

Para atingir o propósito deste trabalho, foram utilizadas nesta categoria as opções SNTP Client e User List, que são detalhadas a seguir.

4.4.1 SNTP Client

O protocolo NTP é baseado no protocolo UDP na porta 123. Sua função é manter o relógio dos computadores que estão na rede sendo gerenciados pela MK sempre atualizados e corretos. A configuração desta opção através do terminal é realizada pelo seguinte comando:

system ntp client set enabled=yes mode=unicast primary-ntp=200.160.7.186 secondary-ntp= 201.49.148.135

A Figura 22 demostra a configuração por meio da interface gráfica.

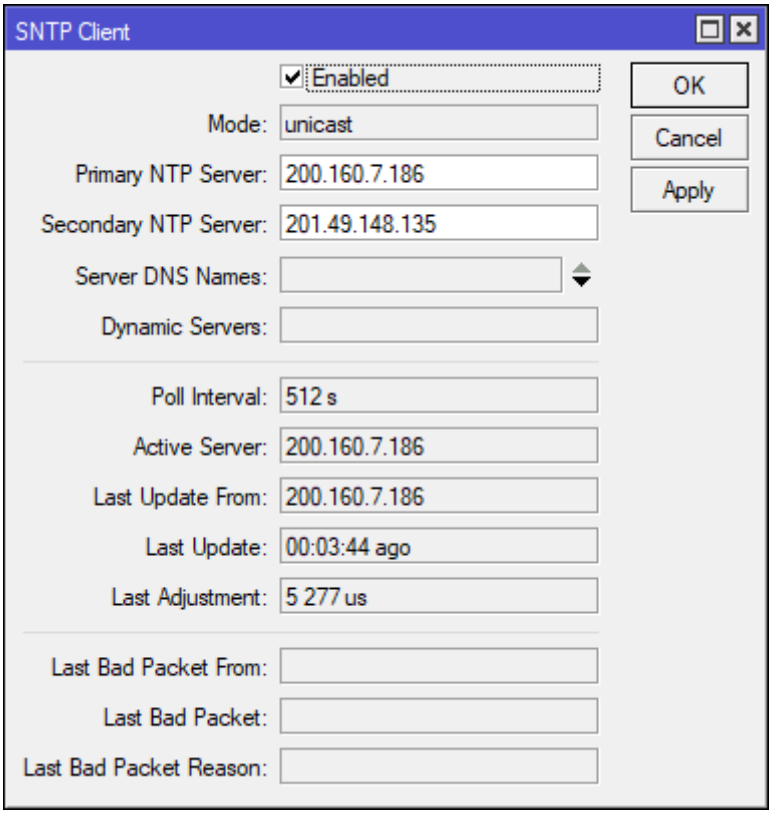

Figura 22 - SNTP Client
Fonte - Giovanni Santela Desiró

4.4.2 User List

Na opção User List podem ser configurados novos usuários, além do administrador, restringir acesso para que usuários comuns tenham acesso, porém não consigam alterar nenhuma configuração, excluir usuários, alterar senhas. A Figura 23 demostra o usuário “admin” criado com acesso a todas as configurações.

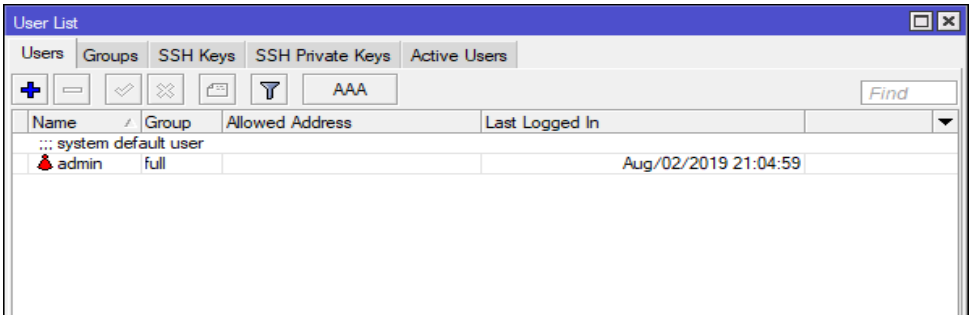

Figura 23 - User List
Fonte - Giovanni Santela Desiró

5. TESTE DO PROJETO

Neste capítulo será apresentado os testes do projeto, sendo eles teste de segurança e teste de bloqueio.

5.1 TESTE DE SEGURANÇA

O teste de segurança tem por finalidade o bloqueio de ping da rede interna para a rede externa e vice-versa.

A Figura 24 apresenta o teste de ping para o site www.youtube.com com o bloqueio (demarcado no lado esquerdo) ativo, tendo como resposta “Esgotado o tempo limite do tempo”, pois não está acessível.

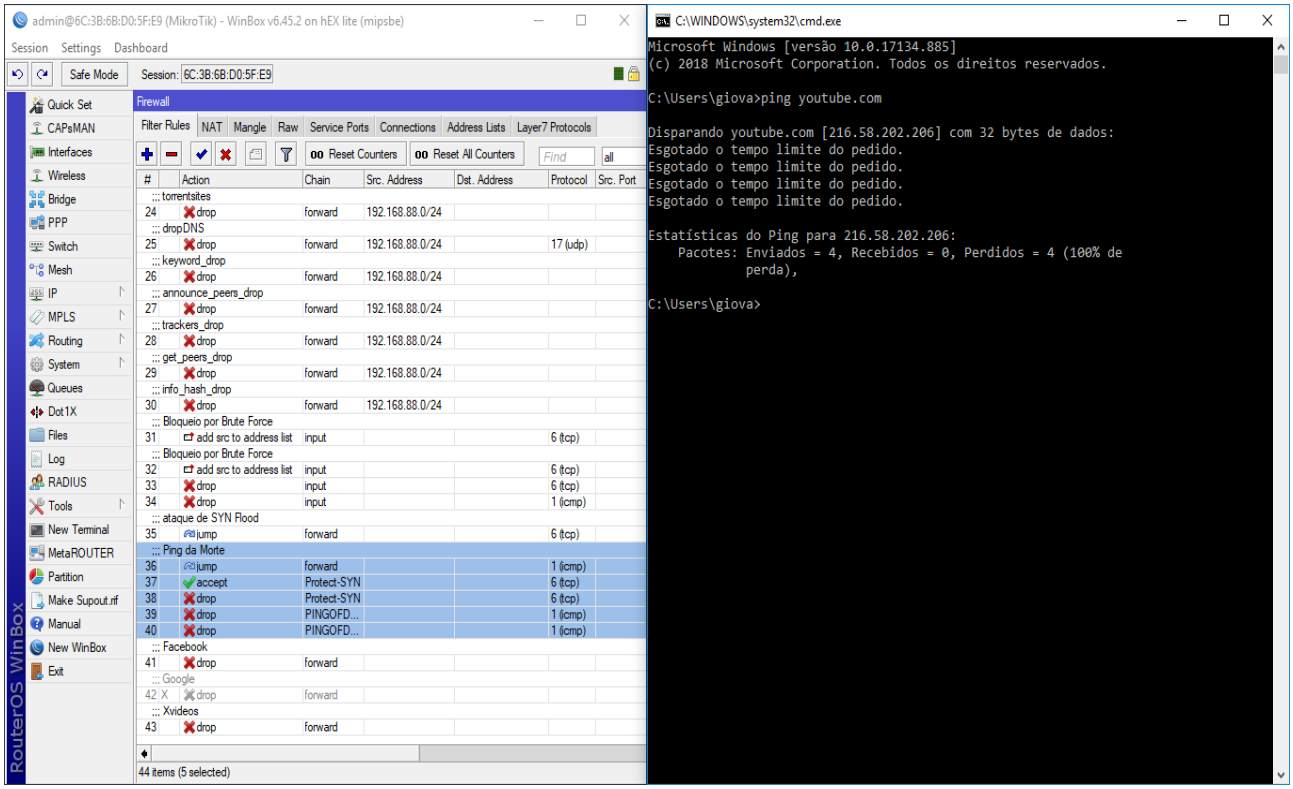

Figura 24 - Teste de Ping com Bloqueio Ativado
Fonte - Giovanni Santela Desiró

A Figura 25 apresenta o teste de ping para o site www.youtube.com com o bloqueio (demarcado no lado esquerdo) desativado, tendo a resposta dos pacotes disparados.

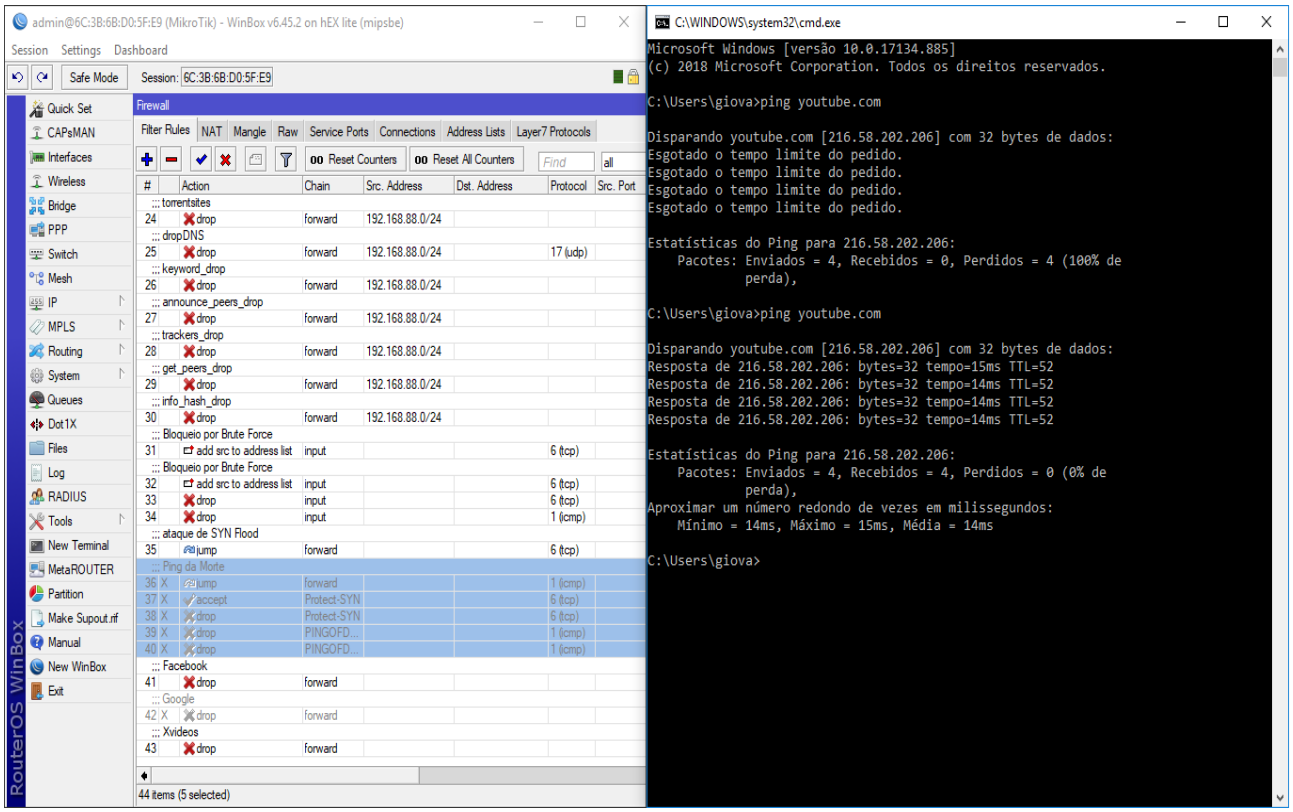

Figura 25 - Teste de Ping com Bloqueio Desativado
Fonte - Giovanni Santela Desiró

5.2 **TESTE DE BLOQUEIO**

O teste de bloqueio tem por finalidade o bloqueio de sites impróprios, sites onde o ambiente não permita acessar, como acessar o site www.facebook.com no ambiente de trabalho.

A Figura 26 apresenta o teste de bloqueio para o site www.facebook.com com o bloqueio (demarcado no lado esquerdo) ativado, tendo como resposta “Não é possível acessar esse site”.

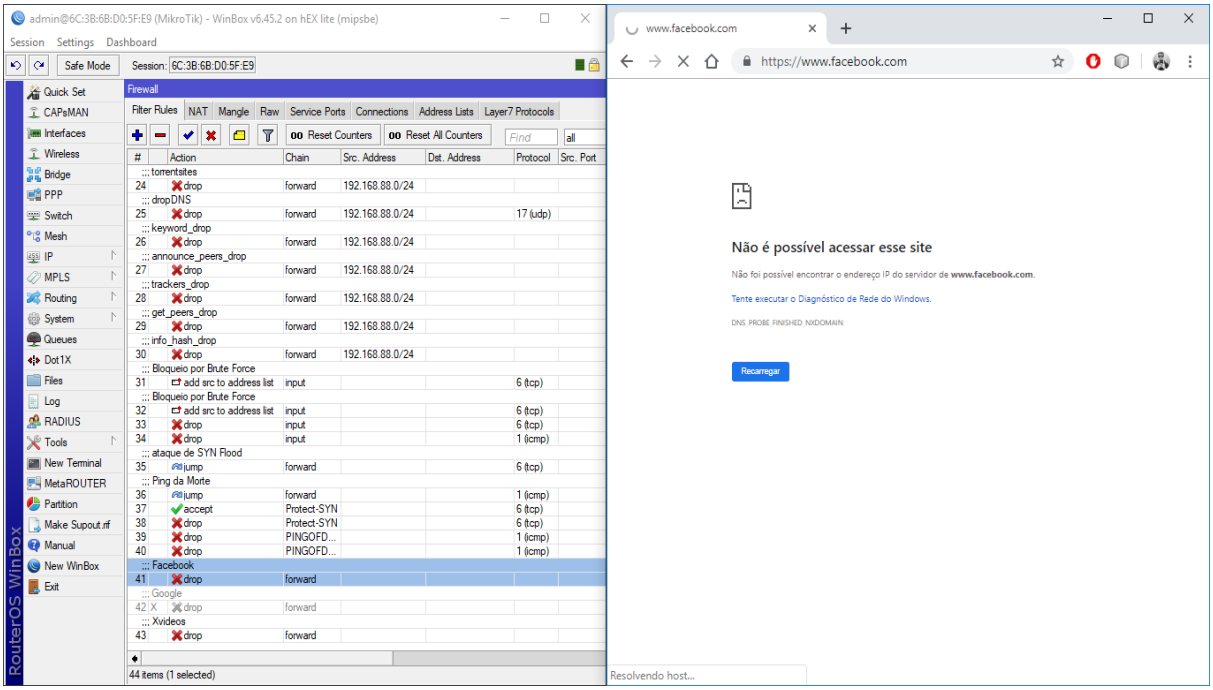

Figura 26 - Teste de Bloqueio com Regra Ativada
Fonte - Giovanni Santela Desiró

A Figura 27 apresenta o teste de bloqueio para o site www.facebook.com com o bloqueio (demarcado no lado esquerdo) desativado, sendo possível acessar o site.

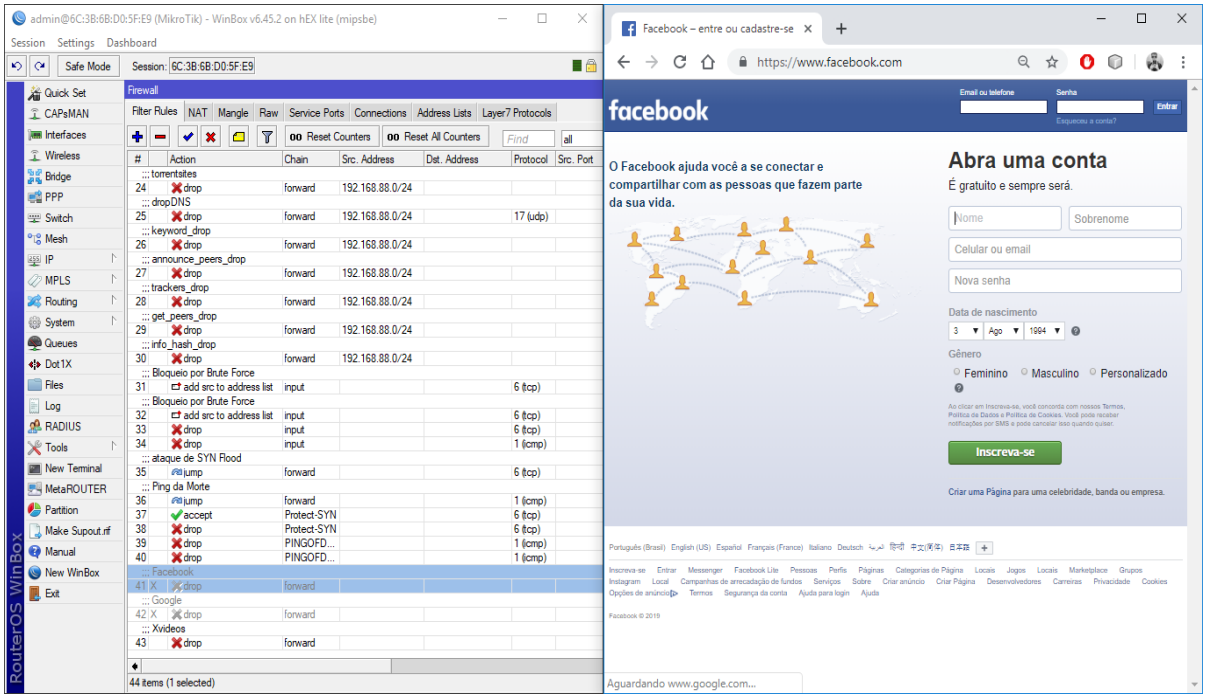

Figura 27 - Teste de Bloqueio com Regra Desativada
Fonte - Giovanni Santela Desiró

6. **CONSIDERAÇÕES FINAIS**

O estudo para a configuração do sistema de segurança da informação foi finalizado com grande êxito. O equipamento MikroTik RouterBoard foi configurado, testado e aprovado. O intuito deste trabalho foi demonstrar sobre essa tecnologia, suas configurações, sua segurança, inspirar futuros alunos, para que eles possam despertar interesse pela segurança da informação. Para trabalhos futuros prevê a configuração mais avançada do roteador MikroTik, inserindo ao mesmo proxy, vpn e IDS/IPS, deixando a segurança ainda mais segura.

REFERÊNCIAS

ACQNOTES. **Work Breakdown Structure**. Acqnotes.com. Disponível em <http://acqnotes.com/acqnote/careerfields/work-breakdown-structure>. Acesso em: 16/03/2018.

CABRAL, WALLISSON. **Os Dados São A Nova Moeda Digital Da Atualidade!** Disponível em: <guiarnet.com.br/2018/02/14/os-dados-sao-a-nova-moeda-digital-da-atualidade/>. Acesso em: 04/11/2018.

CAETANO, GECILEIA; SOUZA, MARTA; COSTA, HELDER. **Segurança Da Informação: Um Estudo A Partir Dos Crimes Virtuais**. Disponível em: <revistapensar.com.br/tecnologia/artigo/no=a78.pdf>. Acesso em: 28/10/2018.

GUIA DO LINUX. **A Tabela Mangle**. Disponível em: <https://pt.wikibooks.org/wiki/Guia_do_Linux/Avan%C3%A7ado/Firewall_iptables/A_tabela_mangle>. Acesso em: 02/08/2019.

(ISC)² MANAGEMENT. **Gartner Expects $93 Billion In Security Spend, But What's Missing?** Disponível em: <https://blog.isc2.org/isc2_blog/2017/08/gartner-expects-93-billion-in-security-spend-but-whats-missing.html >. Acesso em: 10/11/2018.

MACEDO, DIEGO. **Conceito De Filtragem De Pacotes E Firewall**. Disponível em: <https://www.diegomacedo.com.br/conceito-de-filtragem-de-pacotes-e-firewall/>. Acesso em: 16/03/2019.

MACEDO, DIEGO. **Modelos E Mecanismos De Segurança Da Informação**. Disponível em: <https://www.diegomacedo.com.br/modelos-e-mecanismos-de-seguranca-da-informacao/>. Acesso em: 15/03/2019.

MACEDO, DIEGO. **Tipos De Firewall**. Disponível em: < https://www.diegomacedo.com.br/tipos-de-firewall/>. Acesso em: 16/03/2019.

ODON, BRUNO. **Um Passeio Pelas Chains Da Tabela Filter (INPUT)**. Disponível em: < https://www.mundotibrasil.com.br/iptables-artigo-110-um-passeio-pelas-chains-da-tabela-filter-input/>. Acesso em: 02/08/2019.

PERES, FERNANDO. **Segurança da Informação**. Disponível em: <www.peres.adv.br/atuacao/seguranca-da-informacao/>. Acesso em: 03/11/2018.

ROHR, ALTIERES. **Hackers Atacam Roteadores MikroTik No Brasil Para Minerar Criptomoedas Na Web**. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2018/08/02/hackers-atacam-roteadores-mikrotik-no-brasil-para-minerar-criptomoedas-na-web.ghtml>. Acesso em: 05/11/2018.

SEGURANCA-DA-INFORMACAO.INFO. **Segurança da Informação**. Disponível em: <http://seguranca-da-informacao.info/>. Acesso em: 15/03/2019.

SCHLEMER, ELGIO. **Estrutura do IPTables 2: A Tabela NAT**. Disponível em: < https://www.vivaolinux.com.br/artigo/Estrutura-do-IPTables-2-a-tabela-nat>. Acesso em: 02/08/2019.

SIA MIKROTĪKLS. **About Us**. Disponível em: <https://mikrotik.com/aboutus>. Acesso em: 14/03/2019.

TRISTÃO, THIAGO. **O Desafio De Segurança Da Informação Numa Sociedade Conectada Pelas "Coisas"**. Disponível em: <tiinside.com.br/tiinside/segurança/artigos-seguranca/07/06/2017/o-desafio-de-seguranca-da-informacao-numa-sociedade-conectada-pelas-coisas/>. Acesso em: 21/10/2018.