

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 Mic  | roTik     |
|         | / Giovanni Santela Desiró. – Assis, 2019.  |           |
|         | 45p.   |           |
|         | Trabalho de conclusão do curso (Ciência da Computação ).<br>dação Educacional do Município de Assis-FEMA | – Fun-    |
|         | 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

# 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

| Figura 1 - Estrutura Analítica do Projeto (EAP) | 17 |
|---|----|
| Figura 2 - MikroTik hEX lite                    | 19 |
| Figura 3 – Firewall                             | 21 |
| Figura 4 - Filtro de Pacotes                    | 23 |
| Figura 5 - Filtro de Pacotes com Estado         | 24 |
| Figura 6 - Proxy na Rede                        | 25 |
| Figura 7 - Logo WinBox                          |    |
| Figura 8 – Tela de Login do WinBox              |    |
| Figura 9 - Tela Inicial do WinBox               | 27 |
| Figura 10 – Interfaces                          |    |
| Figura 11 - Address List                        |    |
| Figura 12 - DHCP Server                         |    |
| Figura 13 – DNS                                 |    |
| Figura 14 - Firewall: Filter Rules              |    |
| Figura 15 - Firewall: NAT                       |    |
| Figura 16 - Processamento NAT                   |    |
| Figura 17 - Firewall: Mangle                    |    |
| Figura 18 - Firewall: Address Lists             |    |
| Figura 19 - Firewall: Layer7 Protocols          |    |
| Figura 20 - IP Pool                             |    |
| Figura 21 - Route List                          |    |
| Figura 22 - SNTP Client                         |    |
| Figura 23 - User List                           |    |
| Figura 24 - Teste de Ping com Bloqueio Ativado  | 40 |

| Figura 25 - Teste de Ping com Bloqueio Desativado  | 41 |
|--|----|
| Figura 26 - Teste de Bloqueio com Regra Ativada    | 42 |
| Figura 27 - Teste de Bloqueio com Regra Desativada | 42 |

# LISTA DE TABELAS

| Tabela 1 - Cronograma do Projeto  | 18 |
|-----------------------------------|----|
| Tabela 2 - Levantamento de Custos | 18 |

# LISTA DE ABREVIATURAS E SIGLAS

MK - MikroTik

# Sumário

| 1. | INT | RODUÇÃO                              | 15 |
|----|-----|--------------------------------------|----|
|    | 1.1 | OBJETIVO                             | 15 |
|    | 1.2 | JUSTIFICATIVA                        | 15 |
|    | 1.3 | PÚBLICO ALVO                         | 16 |
|    | 1.4 | MOTIVAÇÃO                            | 16 |
| 2. | PLA | ANEJAMENTO DO PROJETO                | 17 |
|    | 2.1 | ESTRUTURA ANALÍTICA DO PROJETO (EAP) | 17 |
|    | 2.2 | CRONOGRAMA                           | 18 |
|    | 2.3 | ORÇAMENTO                            | 18 |
|    | 2.4 | TECNOLOGIAS PREVISTAS                | 19 |
|    |     | 2.4.1 Mikrotik RouterBoard           | 19 |
| 3. | SEC | GURANÇA DA INFORMAÇÃO                | 20 |
|    | 3.1 | MECANISMOS DE SEGURANÇA              | 20 |
|    | 3.2 | FIREWALL                             | 21 |
|    | 3.3 | TIPOS DE FIREWALL                    | 22 |
|    |     | 3.3.1 Filtro de Pacotes              | 22 |
|    |     | 3.3.2 Filtro de Pacotes com Estado   | 24 |
|    |     | 3.3.3 Proxy                          | 25 |
| 4. | EXE | ECUÇÃO DO PROJETO                    | 26 |
|    | 4.1 | WINBOX                               | 26 |
|    | 4.2 | INTERFACES                           | 27 |
|    | 4.3 | IP                                   | 28 |
|    |     | 4.3.1 Address List                   | 28 |
|    |     | 4.3.2 DHCP Server                    | 29 |
|    |     | 4.3.3 DNS                            | 29 |
|    |     | 4.3.4 Firewall                       | 30 |
|    |     | 4.3.5 IP Pool                        | 35 |
|    |     | 4.3.6 Route List                     | 36 |
|    | 4.4 | SYSTEM                               | 38 |
|    |     | 4.4.1 SNTP Client                    | 38 |
|    |     | 4.4.2 User List                      | 39 |
| 5. | TES | STE DO PROJETO                       | 40 |
|    | 5.1 | TESTE DE SEGURANÇA                   | 40 |
|    | 5.2 | TESTE DE BLOQUEIO                    | 41 |

| 6. CONSIDERAÇÕES FINAIS | 43 |
|-------------------------|----|
| REFERÊNCIAS             |    |

# 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)<sup>2</sup> 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.



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).

 Aplicação
 Aplicação

 Transporte
 Transporte

 Filtro de pacotes
 (Stateless Firewall)

 Rede
 IP/ICMP/IGMP

 Interface de Rede
 Interface de Rede

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://2.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.

| WinBox v3.1  | 9 (Add             | resses)                    |                       |                       |                  | -                           |          | $\times$ |
|--|--------------------|----------------------------|-----------------------|-----------------------|------------------|-----------------------------|----------|----------|
| Connect To:<br>Login:<br>Password:                         | V Keep             | Password                   | l<br>Vindow           |                       |                  |                             |          |          |
| Managed Neigh<br>Refresh<br>MAC Address<br>6C:38:6B:D0.5F: | ibors  <br>]<br>E9 | IP Address<br>192.168.88.1 | Identity<br>Mikro Tik | Version<br>6.45.2 (st | Board<br>RB750r2 | Find<br>Uptime<br>11d 23:12 | all 2:02 |          |
|  |                    |                            |                       |                       |                  |                             |          |          |

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.

| Interface I | List              |          |             |            |           |               |            |           |                 |                 |       |           |           |                         |
|-------------|-------------------|----------|-------------|------------|-----------|---------------|------------|-----------|-----------------|-----------------|-------|-----------|-----------|-------------------------|
| Interface   | Interface List    | Ethernet | EoIP Tunnel | IP Tunnel  | GRE Tunne | I VLAN VRRP B | onding LTE |           |                 |                 |       |           |           |                         |
| <b>+</b> •  | • 🖉 💥 [           | - 7      | Detect Inte | met        |           |               |            |           |                 |                 |       |           |           | Find                    |
| Nan         | ne 🗵              | Туре     |             | Actual MTU | L2 MTU    | Тх            | Rx         |           | Tx Packet (p/s) | Rx Packet (p/s) | FP Tx |           | FP Rx     | FP Tx Packet (p/s) FP 🔻 |
| < >;        | ether4            | Ethernet |             | 150        | ) 1598    | 0 b           | os         | 0 bps     |                 | 0               | 0     | 0 bps     | 0 bps     | 0                       |
| <;>         | ether5            | Ethernet |             | 150        | ) 1598    | 0 b           | os         | 0 bps     |                 | 0               | 0     | 0 bps     | 0 bps     | 0                       |
| ;;; Red     | e Interna - Porta | 2        |             |            |           |               |            |           |                 |                 |       |           |           |                         |
| R 🔹         | an                | Ethernet |             | 150        | ) 1598    | 68.8 kb       | os         | 23.7 kbps | 1               | 10              | 12    | 54.4 kbps | 37.2 kbps | 8                       |
| ::: Red     | e externa 1 - Por | ta 1     |             |            |           |               |            |           |                 |                 |       |           |           |                         |
| R 4>        | wan               | Ethernet |             | 150        | ) 1598    | 18.0 kb       | os         | 3.3 kbps  |                 | 3               | 5     | 32.6 kbps | 1456 bps  | 10                      |
| ::: Red     | e externa 2 - Por | ta 3     |             |            |           |               |            |           |                 |                 |       |           |           |                         |
| 4 Þ.        | wan2              | Ethernet |             | 150        | ) 1598    | 0 b           | os         | 0 bps     |                 | 0               | 0     | 0 bps     | 0 bps     | 0                       |
|             |                   |          |             |            |           |               |            |           |                 |                 |       |           |           |                         |
| •           |                   |          |             |            |           |               |            |           |                 |                 |       |           |           | •                       |
| 5 items     |                   |          |             |            |           |               |            |           |                 |                 |       |           |           |                         |



#### 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.

| Add | ress List        |              |           |      |
|-----|------------------|--------------|-----------|------|
| ÷   |                  | T            |           | Find |
|     | Address A        | Network      | Interface |      |
|     | 177.12.54.78/24  | 177.12.54.0  | wan2      |      |
| D   | 192.168.0.101/24 | 192.168.0.0  | wan       |      |
|     | 192.168.88.1/24  | 192.168.88.0 | 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.

| DHCP S | Server   |            |           |               |            |              |        |  | ×□   |
|--------|----------|------------|-----------|---------------|------------|--------------|--------|--|------|
| DHCP   | Networks | Leases     | Options 0 | Option Sets A | Verts      |              |        |  |      |
| +      | - 🖉 🛛    | 3          | DHCP Co   | nfig DHCP     | Setup      |              |        |  | Find |
| Nam    | ne       | _∧ Interfa | ice       | Relay         | Lease Time | Address Pool | Add AR |  | -    |
| DHC    | CP_LAN   | lan        |           |               | 08:00:0    | 0 dhcp_lan   | no     |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
|        |          |            |           |               |            |              |        |  |      |
| 1 item |          |            |           |               |            |              |        |  |      |
| ritem  |          |            |           |               |            |              |        |  |      |

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.

| DNS Settings                  |                       |     |        |
|-------------------------------|-----------------------|-----|--------|
| Servers:                      | 8.8.8.8               | \$  | ОК     |
|                               | 8.8.4.4               | \$  | Cancel |
|                               | 208.67.222.222        | \$  | Apply  |
|                               | 208.67.220.220        | \$  | Static |
| Dynamic Servers:              | 192.168.0.1           |     | Cache  |
|                               | Allow Remote Requests |     |        |
| Max UDP Packet Size:          | 4096                  |     |        |
| Query Server Timeout:         | 2.000                 | s   |        |
| Query Total Timeout:          | 10.000                | s   |        |
| Max. Concurrent Queries:      | 100                   |     |        |
| Max. Concurrent TCP Sessions: | 20                    |     |        |
| Cache Size:                   | 2048                  | Kip |        |
| Cache May TTL :               | 74.00:00:00           | ND  |        |
| Cache Used:                   | 18 KiB                |     |        |
| Cache Osed.                   | 10100                 |     |        |

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.

| rewall                             |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
|------------------------------------|-------------|-------------------|-------------------|---------------|-----------|-----------|---------------|----------|-----------|----------|-------------------|---------|------------|-----------|-----|
| Filter Rules NAT Mangle Ray        | V Service P | Ports Connections | Address Lists Lay | er7 Protocols |           |           |               |          |           |          |                   |         |            |           |     |
| • - • × 🗅 🍸                        | 00 Rese     | t Counters 00 Res | et All Counters   |               |           |           |               |          |           |          |                   |         |            | Find      | all |
| # Action                           | Chain       | Src. Address      | Dst. Address      | Protocol      | Src. Port | Dst. Port | In. Interface | Out. Int | In. Inter | Out. Int | Src. Address List | Dst. Ad | Bytes      | Packets   |     |
| ::: Bloqueia ataques de login via  | FTP         |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 0 X drop                           | input       |                   |                   | 6 (tcp)       |           | 21        |               |          |           |          | ftp_blacklist     |         | 0 B        | 0         |     |
| 1 Vaccept                          | output      |                   |                   | 6 (tcp)       |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| 2 add dst to address list          | output      |                   |                   | 6 (tcp)       |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| ;;; Bloqueia ataques de login via  | SSH         |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 3 💥 drop                           | input       |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          | ssh_blacklist     |         | 104 B      | 2         |     |
| 4 add src to address list          | input       |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          | ssh_stage3        |         | 52 B       | 1         |     |
| 5 stadd src to address list        | input       |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          | ssh_stage2        |         | 156 B      | 3         |     |
| 6 add src to address list          | input       |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          | ssh_stage1        |         | 260 B      | 5         |     |
| 7 add src to address list          | input       |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          |                   |         | 364 B      | 7         |     |
| ;;; drop ssh brute downstream      |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 8 X drop                           | forward     |                   |                   | 6 (tcp)       |           | 22        |               |          |           |          | ssh_blacklist     |         | 0 B        | 0         |     |
| ::: Bloqueia conexoes invalidas    |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 9 Xdrop                            | input       |                   |                   |               |           |           |               |          |           |          |                   |         | 273.4 KiB  | 4 629     |     |
| ::: Permitir conexoes estabelecid  | as          |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 10 🗸 accept                        | input       |                   |                   |               |           |           |               |          |           |          |                   |         | 1517.5 KiB | 18 321    |     |
| ::: Permite ICMP                   |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 11 Vaccept                         | input       |                   |                   | 1 (icmp)      |           |           |               |          |           |          |                   |         | 240 B      | 4         |     |
| 12 Vaccept                         | input       | 192.168.88.0/24   |                   |               |           |           | lan           |          |           |          |                   |         | 0 B        | 0         |     |
| ::: Bloqueia todo o resto          |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 13 💥 drop                          | input       |                   |                   |               |           |           |               |          |           |          |                   |         | 298.6 MiB  | 5 437 578 |     |
| ;;; Adicionar Syn Flood IP a lista |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 14 dd src to address list          | input       |                   |                   | 6 (tcp)       |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| ;;; Drop syn flood                 |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 5 💥 drop                           | input       |                   |                   |               |           |           |               |          |           |          | Syn_Flooder       |         | 0 B        | 0         |     |
| ::: Detectar as ferramentas de P   | ort Scanner |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 16 add src to address list         | input       |                   |                   | 6 (tcp)       |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| ;;; Drop to port scan list         |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 17 💥 drop                          | input       |                   |                   |               |           |           |               |          |           |          | Port_Scanner      |         | 0 B        | 0         |     |
| ::: Jump for icmp input flow       |             |                   |                   |               |           |           |               |          |           |          | _                 |         |            |           |     |
| 8 🙉 jump                           | input       |                   |                   | 1 (icmp)      |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| ::: Accept DNS - UDP               |             |                   |                   |               |           |           |               |          |           |          |                   |         |            |           |     |
| 19 Vaccept                         | input       |                   |                   | 17 (udp)      |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| ;;; Accept DNS - TCP               |             |                   |                   | (+)           |           |           |               |          |           |          |                   |         |            |           |     |
| 20 Vaccept                         | input       |                   |                   | 6 (tcp)       |           |           |               |          |           |          |                   |         | 0 B        | 0         |     |
| Accept to established connect      | tions       |                   |                   |               |           |           |               |          |           |          |                   |         |            | _         |     |

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.

| Filter Null         Margie         Name         Description         Description         Description         Filter All         Filter All <th>Firewall</th> <th></th> <th>Ξ×</th>   | Firewall          |                   |            |   |                |         |              |           |           |            |           |          |         |           |          |           |   |      |     | Ξ× |
|--|-------------------|-------------------|------------|---|----------------|---------|--------------|-----------|-----------|------------|-----------|----------|---------|-----------|----------|-----------|---|------|-----|----|
| Image       One Rest Al Courters       Find       of         #       Action       One Address       Dat. Address       Pat. Note       Dat. Not. Int.       In. Inter.       Out. Int.       In. Inter.       Out. Int.       Inter   | Filter Rules NAT  | Mangle Raw        | Service    | Ports Connection  | ns Address Lis | sts Lay | yer7 Protoco | ls        |           |            |           |          |         |           |          |           |   |      |     |    |
| H         Action         Chain         Soc. Address         Dat. Address         Proto         Soc. Pot         Dat. Pot         In. Inter         Out. Int         Soc. Ad         Dat. Add         Bytes         Packets           0         =ff masquenzde<br>scrut         scrut         Soc. Address         Dat. Address         Poto         Soc. Addres         Soc. Addres         Soc. Address <td>+ - 🖉 8</td> <td>× 🖆 🍸</td> <td>oo Re</td> <td>set Counters 00</td> <td>Reset All Cour</td> <td>nters</td> <th></th> <td></td> <td>Find</td> <td>all</td> <td>₹</td>  | + - 🖉 8           | × 🖆 🍸             | oo Re      | set Counters 00   | Reset All Cour | nters   |              |           |           |            |           |          |         |           |          |           |   | Find | all | ₹  |
| Umber Para para para para para para para par   | # Action          | Chi               | ain        | Src. Address  | Dst. Address   | Proto   | Src. Port    | Dst. Port | In. Inter | . Out. Int | In. Inter | Out. Int | Src. Ad | . Dst. Ad | Bytes    | Packets   |   |      |     | -  |
| 0         Image para an exegor as intered         wan         84.2 MB         1290.488           1         Image para an exegor as intered         wan2         0.8         0           2         Image para as cosses are solved         wan2         0.8         0           2         Image para as cosses are solved         9311.8         8           3         Image para accesses musice as cosses are solved are due as cosses are solved are due accesses musice are solved are due as cosses are solved are due as cosses musice are solved are due   | ::: Regra para na | avegar na interne | et         |   |                |         |              |           |           |            |           |          |         |           |          |           |   |      |     |    |
| ::::Regrapsa navegar avegar navegar navegar navegar navegar navegar navegar navegar navegar sendor         08         0           ::::Regra para acessar mais de um sendor na mesma rede         08         0           ::::Regra para acessar mais de um sendor na mesma rede         08         0           ::::Regra para acessar mais de um sendor na mesma rede         08         0           ::::Regra para acessar mais de um sendor na mesma rede         08         0           ::::Regra para acessar mais de um sendor na mesma rede         08         0           :::::Regra para acessar mais de um sendor na mesma rede         08         0  | 0 <b>≓l</b> masqu | uerade src        | nat        | 192.168.88.0/24   |                |         |              |           |           | wan        |           |          |         |           | 84.2 MiB | 1 290 488 |   |      |     |    |
| 1         Imaguerade         arcraft         192.168.88.0/24         understand         0           2         Imaguerade         arcraft         6 (top)         22         wan         911.8         8           2         Imaguerade         arcraft         6 (top)         22         wan         911.8         8           3         Imaguerade         arcraft         6 (top)         22         wan         0.8         0           4         Imaguerade         6 (top)         22         wan         0.8         0           4         Imaguerade         6 (top)         20         wan         0.8         0  | ;;; Regra para na | avegar na interne | et         |   |                |         |              |           |           |            |           |          |         |           |          |           |   |      |     |    |
| Implementation     Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementation       Implementation     Implementation     Implementation     Implementati   | 1 ≓ll masqu       | uerade src        | nat        | 192.168.88.0/24   |                |         |              |           |           | wan2       |           |          |         |           | 0 B      | 0         |   |      |     |    |
| 2         Image and a cost and cost and a cost and a cost and a cos | ::: Regra para ad | cessar servidor   |            |   |                | C A     |              | 22        |           |            |           |          |         |           | 011.0    |           | 1 |      |     |    |
| III regra para acessar mais de un servidor na mesma rede<br>3 Milden nat distriat 6 (top) 22 wan 0 8 0<br>4 Milden nat distriat 6 (top) 20 wan 0 8 0<br>IIII de nat distriat 6 (top) 20 wan 0 8 0  | 2 •Ilr'ast-na     | st Ost            | nat        | and the second se |                | e (tcb) |              | 22        | wan       |            |           |          |         |           | 911.8    | ő         |   |      |     |    |
| 3         In decreat         0 stop)         22         wan         0 b         0           4         In decreat         6 stop)         20         wan         0 B         0  | ;;; Hegra para ad | cessar mais de u  | m servidor | na mesma rede   |                | ( A     |              | 22        |           |            |           |          |         |           | 0.0      | 0         |   |      |     |    |
|  | J - Ustria        | st USL            | ndl        |   |                | 6 (top) |              | 22        | wan       |            |           |          |         |           | 0.0      | 0         |   |      |     |    |
|  | 4 1 031110        | st USI            | Idi        |   |                | o (ich) |              | 20        | wari      |            |           |          |         |           | 0.0      | U         |   |      |     |    |
| 5 tems   | 5 tems            |                   |            |   |                |         |              |           |           |            |           |          |         |           |          |           |   |      |     |    |

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 dstaddress=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 dstaddress=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 dstaddress=177.12.54.78 comment="Evitar Loop na Interface WAN2".

A Figura 17 demonstra essas regras.

| Firewall                        |               |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     | Ξ× |
|---------------------------------|---------------|-------------------|-------------------|-----------|-----------|-----------|-----------|------------|-----------|------------|-----------------|---------|---------|------------|-----------|-----|----|
| Filter Rules NAT Mangle         | Raw Service P | Ports Connections | Address Lists Lay | er7 Proto | cols      |           |           |            |           |            |                 |         |         |            |           |     |    |
| + - 🖉 🖂 🖂                       | 7 00 Rese     | t Counters 00 Re  | eset All Counters |           |           |           |           |            |           |            |                 |         |         |            | Find      | all | ₹  |
| # Action                        | Chain         | Src. Address      | Dst. Address      | Proto     | Src. Port | Dst. Port | In. Inter | . Out. Int | In. Inter | . Out. Int | Connection Mark | Src. Ad | Dst. Ad | Bytes      | Packets   |     | -  |
| 0 smark routing                 | prerouting    |                   |                   |           |           |           |           |            |           |            |                 | wan2-ip |         | 0 B        | 0         |     |    |
| 1 s mark routing                | prerouting    |                   |                   |           |           |           |           |            |           |            |                 |         | wan2-ds | 216.6 KiB  | 675       |     |    |
| 2 2 mark routing                | prerouting    |                   |                   | 6 (tcp)   |           | 80,443    |           |            |           |            |                 |         |         | 33.3 MiB   | 454 469   |     |    |
| ;;; Evitar loop na rede interna | a (LAN)       |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     |    |
| 3 Vaccept                       | prerouting    | 192.168.88.0/24   | 192.168.88.0/24   |           |           |           |           |            |           |            |                 |         |         | 61.3 MiB   | 1 211 639 |     |    |
| ;;; Evitar loop na rede extern  | a (WAN 1)     |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     |    |
| 4 Vaccept                       | prerouting    | 192.168.88.0/24   | 192.168.0.101     |           |           |           |           |            |           |            |                 |         |         | 627 B      | 6         |     |    |
| ;;; Evitar loop na rede extern  | a (WAN 2)     |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     |    |
| 5 🗸 accept                      | prerouting    | 192.168.88.0/24   | 177.12.54.78      |           |           |           |           |            |           |            |                 |         |         | 0 B        | 0         |     |    |
| 6 and mark connection           | prerouting    |                   |                   |           |           |           | wan       |            |           |            | no-mark         |         |         | 2283.7 KiB | 17 740    |     |    |
| 7 / mark connection             | prerouting    |                   |                   |           |           |           | wan2      |            |           |            | no-mark         |         |         | 0 B        | 0         |     |    |
| 8 ark connection                | prerouting    |                   |                   |           |           |           | lan       |            |           |            | no-mark         |         |         | 32.3 MiB   | 478 457   |     |    |
| <li>9 2 mark connection</li>    | prerouting    |                   |                   |           |           |           | lan       |            |           |            | no-mark         |         |         | 29.0 MiB   | 462 657   |     |    |
| 10 A mark routing               | prerouting    |                   |                   |           |           |           | lan       |            |           |            | wan-con         |         |         | 7.0 GiB    | 6 750 856 |     |    |
| 11 A mark routing               | prerouting    |                   |                   |           |           |           | lan       |            |           |            | wan2-con        |         |         | 9.2 GiB    | 8 341 854 |     |    |
| 12 A mark routing               | output        |                   |                   |           |           |           |           |            |           |            | wan-con         |         |         | 44.3 KiB   | 292       |     |    |
| 13  mark routing                | output        |                   |                   |           |           |           |           |            |           |            | wan2-con        |         |         | 59.7 KiB   | 398       |     |    |
|                                 |               |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     |    |
| 14 items                        |               |                   |                   |           |           |           |           |            |           |            |                 |         |         |            |           |     |    |



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.

| Firewall                     |                          |  |            |
|------------------------------|--------------------------|--|------------|
| Filter Rules NAT M           | langle Raw Service Ports | Connections Address Lists Layer7 Proto | cols       |
| + - 🖉 🗱                      |                          |  | Find all F |
| Name                         | / Address                | √ Timeout Creation Time                |            |
| DNS1                         |                          |  |            |
| LIBERADOS                    | 208.67.222.222           | Jul/24/2019 20:2                       |            |
| ;;; RedeLan                  |                          |  |            |
| LIBERADOS                    | 192.168.88.0             | Jul/24/2019 20:2                       |            |
| ::: DNS1                     |                          |  |            |
| LIBERADOS                    | 8.8.8.8                  | Jul/24/2019 20:2                       |            |
| <ul> <li>SUPPORTE</li> </ul> | 192.168.88.0/24          | Jul/23/2019 20:1                       |            |
| ;;; Uol                      |                          |  |            |
| wan2-ds                      | 200.147.160.24           | Jul/28/2019 13:5                       |            |
| ;;; Youtube                  |                          |  |            |
| wan2-ds                      | 172.217.29.174           | Jul/28/2019 13:5                       |            |
| ;;; Facebook                 |                          |  |            |
| wan2-ds                      | 31.13.74.35              | Jul/28/2019 13:5                       |            |
| ;;; Separando por de         | epartamento              |  |            |
| wan2-ip                      | 192.168.88.74            | Jul/28/2019 13:1                       |            |
| wan2-ip                      | 192.168.88.73            | Jul/28/2019 13:1                       |            |
|                              |                          |  |            |
| 9 items                      |                          |  |            |
| li -                         |                          |  |            |
|                              |                          |  |            |

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:

ipfirewalllayer7-protocoladdname=torrentsitesregexp="^.\*(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.

| Frewal  | 🗆 🗙  |
|---|------|
| Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols  |      |
|   | Find |
| Name / Regexp   | ▼    |
| ofacebook     orfacebook)     ofacebook     ofacebook |      |
| ♥ google +(google). S<br>© Jammetika ^* /rottEET J threetikaaintakautopaldemanaidhii urlidhii   |      |
| Voliminiaases - (getacle ), rejonen kaneparatebayison tai ken kentanepuen kon kolobayia integrini     Varideases ^ 4-kovideases * 4   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
| 4 tems  |      |

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.

| IP Pool              |           |      |
|----------------------|-----------|------|
| Pools Used Addresses |           |      |
| +                    |           | Find |
| Name 🛛 🛆 Addresses   | Next Pool |      |
|                      | none      |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
|                      |           |      |
| 1 item               |           |      |

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".

| Route List                       |                           |          |              |               |   |
|----------------------------------|---------------------------|----------|--------------|---------------|---|
| Routes Nexthops Rules VRF        |                           |          |              |               |   |
| +- ~ ~ 🕾 🍸                       |                           |          | Find         | all           | ₹ |
| Dst. Address                     | Gateway                   | Distance | Routing Mark | Pref. Source  | • |
| S > 0.0.0/0                      | 192.168.0.1 reachable wan | 1        |              |               |   |
| S > 0.0.0.0/0                    | wan2 unreachable          | 1        | rota-wan2    |               |   |
| DAS 0.0.0.0/0                    | 192.168.0.1 reachable wan | 1        |              |               |   |
| ;;; Link Primario                |                           |          |              |               |   |
| AS 0.0.0.0/24                    | wan reachable             | 1        |              |               |   |
| ;;; Link Secundario              |                           |          |              |               |   |
| S > 0.0.0.0/24                   | wan2 unreachable          | 2        |              |               |   |
|                                  |                           |          |              |               |   |
| S > 0.0.0.0/24                   | wan reachable             | 1        |              |               |   |
| S > 0.0.0/24                     | wan2 unreachable          | 2        |              |               |   |
| AS 0.0.0/24                      | wan reachable             | 1        | rota-wan     |               |   |
| S > 0.0.0.0/24                   | wan2 unreachable          | 1        | rota-wan2    |               |   |
| ;;; Rota para a rede 172.16.0.0/ | 24                        |          |              |               |   |
| AS 172.16.0.0/24                 | lan reachable             | 1        |              |               |   |
| DC 177.12.54.0/24                | wan2 unreachable          | 255      |              | 177.12.54.78  |   |
| DAC 192.168.0.0/24               | wan reachable             | 0        |              | 192.168.0.101 |   |
| DAC 192.168.88.0/24              | lan reachable             | 0        |              | 192.168.88.1  |   |
|                                  |                           |          |              |               |   |
| 13 items                         |                           |          |              |               |   |

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 secondaryntp= 201.49.148.135

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

| SNTP Client             |                |        |
|-------------------------|----------------|--------|
|                         |                | OK     |
| Mode:                   | unicast        | Cancel |
| Primary NTP Server:     | 200.160.7.186  | Apply  |
| Secondary NTP Server:   | 201.49.148.135 |        |
| Server DNS Names:       | \$             |        |
| Dynamic Servers:        |                |        |
| Poll Interval:          | 512 s          |        |
| Active Server:          | 200.160.7.186  |        |
| Last Update From:       | 200.160.7.186  |        |
| Last Update:            | 00:03:44 ago   |        |
| Last Adjustment:        | 5 277 us       |        |
| Last Bad Packet From:   |                |        |
| Last Bad Packet:        |                |        |
| Last Bad Packet Reason: |                |        |



#### 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.

| User List |           |           |                   |             |                |                      |      |
|-----------|-----------|-----------|-------------------|-------------|----------------|----------------------|------|
| Users     | Groups    | SSH Key   | vs SSH Private Ke | ys Active L | lsers          |                      |      |
| + -       |           | × C       | AAA               |             |                |                      | Find |
| Name      | Δ.        | Group     | Allowed Address   |             | Last Logged In |                      |      |
| ::: sys   | stem defa | ault user |                   |             |                |                      |      |
| 💧 🍐 adı   | min       | full      |                   |             |                | Aug/02/2019 21:04:59 |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |
|           |           |           |                   |             |                |                      |      |

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.

| Sadmin@6C:3B:6B:D    | 0:5F:E9 (MikroTik) - WinBox v6.45. | .2 on hEX lite | (mipsbe)           |                   | - 🗆             | ×         | C:\WINDOWS\system32\cmd.exe                                   | × |
|----------------------|------------------------------------|----------------|--------------------|-------------------|-----------------|-----------|---|---|
| Session Settings Da  | shboard                            |                |                    |                   |                 |           | Microsoft Windows [versão 10.0.17134.885]                     |   |
| Safe Mode            | Session: 6C:3B:6B:D0:5F:E9         |                |                    |                   |                 |           | (c) 2018 Microsoft Corporation. Todos os direitos reservados. |   |
| Auick Set            | Firewall                           |                |                    |                   |                 |           | C:\Users\giova>ping youtube.com                               |   |
| CAP <sub>8</sub> MAN | Filter Rules NAT Mangle Ray        | v Service Po   | rts Connections    | Address Lists La  | aver7 Protocols |           | Disperande vertube cam [216 50 202 206] cam 22 hutas de dadas |   |
|                      |                                    |                | C                  | 1410              |                 |           | Esgotado o tempo limite do pedido                             |   |
| minineraces          |                                    | UU Heset       | Counters UU Re     | eset All Counters | Find            | all       | Esgotado o tempo limite do pedido.                            |   |
| vvreiess             | # Action                           | Chain          | Src. Address       | Dst. Address      | Protocol        | Src. Port | Esgotado o tempo limite do pedido.                            |   |
| Sig Bridge           | 21 V drop                          | forward        | 192 168 88 0/24    |                   |                 |           | Esgotado o tempo limite do pedido.                            |   |
| 📑 PPP                | ::: drop DNS                       | Torward        | 132.100.00.0/24    |                   |                 |           |   |   |
| 🛫 Switch             | 25 Xdrop                           | forward        | 192.168.88.0/24    |                   | 17 (udp)        |           | Estatisticas do Ping para 216.58.202.206:                     |   |
| ere Mesh             | ;;; keyword_drop                   |                |                    |                   |                 |           | nerda)  |   |
|                      | 26 X drop                          | forward        | 192.168.88.0/24    |                   |                 |           | per ud / ;  |   |
| ∰ P                  | 27 Version drop                    | forward        | 192 168 88 0/24    |                   |                 |           | C:\Users\giova>   |   |
| 🧷 MPLS 🗈 🗅           | :::trackers drop                   | Tormara        | 132.100.00.0/24    |                   |                 |           |   |   |
| 🐹 Routing 🛛 🗅        | 28 Xdrop                           | forward        | 192.168.88.0/24    |                   |                 |           |   |   |
| 68 System            | ::: get_peers_drop                 |                |                    |                   |                 |           |   |   |
|                      | 29 🗙 drop                          | forward        | 192.168.88.0/24    |                   |                 |           |   |   |
| gueues               | ::: info_hash_drop                 | forward        | 102 100 00 00 0/24 |                   |                 |           |   |   |
| Dot1X                | ::: Bloqueio por Brute Force       | Ioiwaiu        | 132.100.00.0/24    |                   |                 |           |   |   |
| 📄 Files              | 31 add src to address list         | input          |                    |                   | 6 (tcp)         |           |   |   |
| 🖹 Log                | ::: Bloqueio por Brute Force       |                |                    |                   |                 |           |   |   |
|                      | 32 dd src to address list          | input          |                    |                   | 6 (tcp)         |           |   |   |
| M RADIUS             | 33 X drop                          | input          |                    |                   | 6 (tcp)         |           |   |   |
| 🗙 Tools 🛛 🗈          | ···· ataque de SYN Flood           | riput          |                    |                   | r (icmp)        |           |   |   |
| New Terminal         | 35 @iump                           | forward        |                    |                   | 6 (tcp)         |           |   |   |
| RetaBOUTER           | ;;; Ping da Morte                  |                |                    |                   | - (             |           |   |   |
| Destiling            | 36 <i>i</i> ump                    | forward        |                    |                   | 1 (icmp)        |           |   |   |
| Martition            | 37 Vaccept                         | Protect-SYN    |                    |                   | 6 (tcp)         |           |   |   |
| 🗙 🛄 Make Supout.rif  | 38 Xdrop                           | Protect-SYN    |                    |                   | 6 (tcp)         |           |   |   |
| 🔗 😧 Manual           | 40 X drop                          | PINGOED        |                    |                   | 1 (icmp)        |           |   |   |
| New WinBox           | ::: Facebook                       | 1 11001 0      |                    |                   | r (cmp)         |           |   |   |
| S                    | 41 Xdrop                           | forward        |                    |                   |                 |           |   |   |
|                      | ::: Google                         |                |                    |                   |                 |           |   |   |
| ö                    | 42 X X drop                        | forward        |                    |                   |                 |           |   |   |
| <b>D</b>             | ::: Xvideos                        | forward        |                    |                   |                 |           |   |   |
| nt                   | 45 <b>A</b> grop                   | rorward        |                    |                   |                 |           |   |   |
| ō                    | •                                  |                |                    |                   |                 |           |   |   |
| <u>ш</u>             | 44 items (5 selected)              |                |                    |                   |                 |           |   |   |

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.

| Sadmin@6C:3B:6B:D0                      | :5F:E9 (MikroTik) - WinBox v6.45. | 2 on hEX lite (mipsbe) |                        | - 🗆            | ×         | C:\WINDOWS\system32\cmd.exe                                    | - | Х      |
|---|-----------------------------------|------------------------|------------------------|----------------|-----------|--|---|--------|
| Session Settings Das                    | hboard                            |                        |                        |                |           | Microsoft Windows [versão 10.0.17134.885]                      |   | ^      |
| 🖒 🗘 Safe Mode                           | Session: 6C:3B:6B:D0:5F:E9        |                        |                        |                | •         | (c) 2018 Microsoft Corporation. Todos os direitos reservados.  |   |        |
| Quick Set                               | Firewall                          |                        |                        |                |           | C:\Users\giova>ping youtube.com                                |   |        |
| T CAPSMAN                               | Filter Rules NAT Mangle Raw       | V Service Ports Conne  | tions Address Lists La | ver7 Protocols |           | Disperende voutube cam [216 EQ 202 206] cam 22 butes de dedes  |   |        |
|   |                                   | 00 Poset Countern      | 00 Peact All Countern  |                |           | Esgotado o tempo limite do pedido.                             |   |        |
| 7 Wireless                              |                                   |                        |                        | Find           | al        | Esgotado o tempo limite do pedido.                             |   |        |
| Sug Del                                 | # Action                          | Chain Src. Addr        | ss Ust. Address        | Protocol       | Src. Port | Esgotado o tempo limite do pedido.                             |   |        |
| andge                                   | 24 X drop                         | forward 192.168.8      | 8.0/24                 |                |           | Esgotado o tempo limite do pedido.                             |   |        |
| E PPP                                   | ::: dropDNS                       |                        |                        |                |           | Estatísticas de Ding para 216 ER 202 206                       |   |        |
| 🛫 Switch                                | 25 💥 drop                         | forward 192.168.8      | 8.0/24                 | 17 (udp)       |           | Decetes: Enviados - A. Perebidos - A. Dendidos - A (190% de    |   |        |
| ere Mesh                                | ::: keyword_drop                  |                        |                        |                |           | nerda).  |   |        |
|   | 26 X drop                         | forward 192.168.8      | 8.0/24                 |                |           | μεί αθ/;   |   |        |
| - · · · · · · · · · · · · · · · · · · · | ::: announce_peers_drop           | forward 102,100 0      | NC/04                  |                |           | C:\Users\giova>ping voutube.com                                |   |        |
| 🧷 MPLS 🗈 🗈                              | trackers drop                     | 101walu 132.100.0      | 0.0/24                 |                |           |  |   |        |
| 🔀 Routing 🗈                             | 28 Xdrop                          | forward 192.168.8      | 8.0/24                 |                |           | Disparando youtube.com [216.58.202.206] com 32 bytes de dados: |   |        |
| 18 Suntam                               | ;;; get_peers_drop                |                        |                        |                |           | Resposta de 216.58.202.206: bytes=32 tempo=15ms TTL=52         |   |        |
| sgr System                              | 29 💥 drop                         | forward 192.168.8      | 8.0/24                 |                |           | Resposta de 216.58.202.206: bytes=32 tempo=14ms TTL=52         |   |        |
| 👳 Queues                                | ::: info_hash_drop                |                        |                        |                |           | Resposta de 216.58.202.206: bytes=32 tempo=14ms TTL=52         |   |        |
| Dot1X                                   | 30 Xdrop                          | forward 192.168.8      | 8.0/24                 |                |           | Resposta de 216.58.202.206: bytes=32 tempo=14ms TTL=52         |   |        |
| Files                                   | 21 Bioqueio por Brute Force       | ine d                  |                        | C Arra)        |           |  |   |        |
|   | ··· Bloqueio por Brite Force      | input                  |                        | o (icp)        |           | Estatisticas do Ping para 216.58.202.206:                      |   |        |
| Log                                     | 32 add src to address list        | input                  |                        | 6 (tcp)        |           | Pacotes: Enviados = 4, Recepidos = 4, Perdidos = 0 (0% de      |   |        |
| 🥵 RADIUS                                | 33 💥 drop                         | input                  |                        | 6 (tcp)        |           | perda),  |   |        |
| 🖌 Tools                                 | 34 💥 drop                         | input                  |                        | 1 (icmp)       |           | Aproximar um numero redondo de vezes em milissegundos:         |   |        |
| Man Tamiral                             | ::: ataque de SYN Flood           |                        |                        |                |           | Pillino = 14ms, Paximo = 15ms, Pedia = 14ms                    |   |        |
|   | 35 @iump                          | forward                |                        | 6 (tcp)        | _         | C:\Users\giova>  |   |        |
| MetaROUTER                              | Hing da Morte                     | Forward                |                        | 1 (omr)        |           |  |   |        |
| 🦺 Partition                             | 37 X Paccent                      | Protect-SYN            |                        | 6 (tcn)        |           |  |   |        |
| Make Supout rif                         | 38 X X drop                       | Protect-SYN            |                        | 6 (tcp)        |           |  |   |        |
| A Marke Supportin                       | 39 X 💥 drop                       | PINGOFD                |                        | 1 (icmp)       |           |  |   |        |
| Manual                                  | 40 X 💥 drop                       | PINGOFD                |                        | 1 (icmp)       |           |  |   |        |
| 들 🕓 New WinBox                          | ::: Facebook                      |                        |                        |                |           |  |   |        |
| S 📕 Exit                                | 41 Xdrop                          | forward                |                        |                |           |  |   |        |
| S                                       | ::: Google                        | ferrored.              |                        |                |           |  |   |        |
| 0                                       | 4∠ ∧ J K drop                     | rorward                |                        |                |           |  |   |        |
| <u>e</u>                                | 43 X drop                         | forward                |                        |                |           |  |   |        |
| ut                                      |                                   |                        |                        |                | _         |  |   |        |
| 8                                       | •                                 |                        |                        |                |           |  |   |        |
| <u> </u>                                | 44 items (5 selected)             |                        |                        |                |           |  |   | $\sim$ |

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".

| Service Setting Dec  | ):5F:E9 (MikroTik) - WinBox v6.45 | .2 on hEX lite (mij | psbe)         |                   | - 🗆            | ×         | U www.fa      | cebook.co | m ×                    | +  |   | - | -  |       | × |
|--|-----------------------------------|---------------------|---------------|-------------------|----------------|-----------|---------------|-----------|------------------------|--|---|---|----|-------|---|
| Session Settings Das   | hboard                            |                     |               |                   |                |           |               | ~ ^       | A https://www          | w facebook com                                       | × | • | 0  | 18    |   |
| Safe Mode  | Session: 6C:3B:6B:D0:5F:E9        |                     |               |                   |                |           |               | ^ U       | Inteps://www           | W.Iacebook.com                                       | Ж | 0 | Ψ. | All A | • |
| 🖌 🔏 Quick Set  | Firewall                          |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| CAPsMAN  | Filter Rules NAT Mangle Ray       | w Service Ports     | Connections   | Address Lists Lag | ver7 Protocols |           |               |           |                        |  |   |   |    |       |   |
| Interfaces   | + - <b>* x</b> 🗆 T                | 00 Reset Cour       | ters 00 Res   | set All Counters  | Find           | all       |               |           |                        |  |   |   |    |       |   |
| 🔔 Wireless   | # Action                          | Chain Sro           | . Address     | Dst. Address      | Protocol       | Src. Port |               |           |                        |  |   |   |    |       |   |
| St Bridge  | ;;; torrentsites                  |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| PPP  | 24 🗙 drop                         | forward 19          | 2.168.88.0/24 |                   |                |           |               |           | ΓP4                    |  |   |   |    |       |   |
| Carlo Carlo  | ::: dropDNS                       | forward 10          | 2 160 00 0/24 |                   | 17 (uda)       |           |               |           |                        |  |   |   |    |       |   |
| Switch   | ::: keyword drop                  | Ioiwaid 15          | 2.100.00.0/24 |                   | 17 (uup)       |           |               |           |                        |  |   |   |    |       |   |
| °℃ Mesh  | 26 🗙 drop                         | forward 19          | 2.168.88.0/24 |                   |                |           |               |           | Não é possíve          | a acessar esse site                                  |   |   |    |       |   |
| 이 말 P 🛛 🖓  | ::: announce_peers_drop           |                     |               |                   |                |           |               |           | Nuo e possíve          | accisal cise site                                    |   |   |    |       |   |
| 🖉 MPLS 🗈 🗈   | 2/ Kdrop                          | forward 19.         | 2.168.88.0/24 |                   |                |           |               |           | Não foi possível encon | ntrar o endereço IP do servidor de www.facebook.com. |   |   |    |       |   |
| 😹 Routing 🗈 🗈  | 28 Xdrop                          | forward 19          | 2.168.88.0/24 |                   |                |           |               |           | Tente executar o Diagr | nóstico de Rede do Windows.                          |   |   |    |       |   |
| illi Svetem  | ::: get_peers_drop                |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| Concerned to the second | 29 Xdrop                          | forward 19          | 2.168.88.0/24 |                   |                |           |               |           | DNS_PROBE_FINISHED_NXD | DOMAIN   |   |   |    |       |   |
| ulleues  | :::into_nasn_drop                 | forward 19          | 2 169 99 0/24 |                   |                |           |               |           |                        |  |   |   |    |       |   |
| Dot1X  | ;;; Bloqueio por Brute Force      | Iorward 15          | 2.100.00.0/24 |                   |                |           |               |           | Recarregar             |  |   |   |    |       |   |
| Files  | 31 🖬 add src to address list      | input               |               |                   | 6 (tcp)        |           |               |           |                        |  |   |   |    |       |   |
| 📄 Log  | ::: Bloqueio por Brute Force      |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| A RADIUS   | 32 add src to address list        | input               |               |                   | 6 (tcp)        |           |               |           |                        |  |   |   |    |       |   |
| Si Taala   | 34 X drop                         | input               |               |                   | 1 (icmp)       |           |               |           |                        |  |   |   |    |       |   |
| Tools .  | ;;; ataque de SYN Flood           |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| Mew Terminal   | 35 🕫 jump                         | forward             |               |                   | 6 (tcp)        |           |               |           |                        |  |   |   |    |       |   |
| MetaROUTER   | ::: Ping da Morte                 | forward             |               |                   | 1 (inmo)       |           |               |           |                        |  |   |   |    |       |   |
| b Partition  | 37 Jaccept                        | Protect-SYN         |               |                   | 6 (tcp)        |           |               |           |                        |  |   |   |    |       |   |
| 🔍 🗋 Make Supout.rif  | 38 🗙 drop                         | Protect-SYN         |               |                   | 6 (tcp)        |           | 1             |           |                        |  |   |   |    |       |   |
| Q Manual   | 39 Xdrop                          | PINGOFD             |               |                   | 1 (icmp)       |           |               |           |                        |  |   |   |    |       |   |
| Now WinPer   | 40 K drop                         | PINGOFD             |               |                   | 1 (icmp)       |           |               |           |                        |  |   |   |    |       |   |
|  | 41 Xdrop                          | forward             |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| Exit   | ::: Google                        |                     |               |                   |                |           | 1             |           |                        |  |   |   |    |       |   |
| ö  | 42 X X drop                       | forward             |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| 0  | ::: Xvideos                       | forward             |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
| nt   | 40 💊 unb                          | Torward             |               |                   |                | _         |               |           |                        |  |   |   |    |       |   |
| 8  | •                                 |                     |               |                   |                |           |               |           |                        |  |   |   |    |       |   |
|  | 44 items (1 selected)             |                     |               |                   |                |           | Resolvendo ho | st        |                        |  |   |   |    |       |   |

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.

| 😵 admin@6C:3B:6B:D0:5F:E9 (MikroTik) - WinBox v6.45.2 on hEX lite (mipsbe) — 🗆 🗙 |  |                            |                 |              |               | ×    | Facebook – entre ou cadastre-se × +  | - 🗆 X   |  |  |
|--|--|----------------------------|-----------------|--------------|---------------|------|--|---|--|--|
| Session Settings Dashboard   |  |                            |                 |              |               |      |  |   |  |  |
| Safe Mode  | Session: 6C:3B:6B:D0:5F:E9   |                            |                 |              |               |      | ← → C ☆ 🏻 https://www.facebook.com   | ९ 🕁 🚺 🕡 👹 :   |  |  |
| Quick Set  | Firewall   |                            |                 |              |               |      |  | Email ou telefone Senha   |  |  |
| 2 CAPsMAN  | Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols |                            |                 |              |               |      | facebook   | Entrar  |  |  |
| 🕅 Interfaces   | + - V X C V OO Reset Counters OO Reset All Counters Find all                         |                            |                 |              |               | -    |  |   |  |  |
| 🚊 Wireless   | # Action   | Chain                      | Src. Address    | Dst. Address | Protocol Src. | Port | O Facebook siuda vosê a sa sanastar a  | Abra uma conta  |  |  |
| 📲 🖁 Bridge   | ;;; torrentsites   |                            | 100 100 00 0 00 |              |               |      | compartilhar com as possoas que fazon parte  | É gratuite o compre corá  |  |  |
| est PPP  | 24 K drop  | forward                    | 192.168.88.0/24 |              |               | _    | da sua vida  | L gratuto e sempre sera.  |  |  |
| 💬 Switch   | 25 X drop  | forward                    | 192.168.88.0/24 |              | 17 (udp)      |      | ua sua viua.   | Nome  |  |  |
| 91º Mash   | ::: keyword_drop   |                            |                 |              |               |      | and an and a second and a second and a second as a   | From Continuing   |  |  |
|  | 26 X drop  | forward                    | 192.168.88.0/24 |              |               | _    |  | Celular ou email  |  |  |
| 9 P  | 27 X drop  | forward                    | 192 168 88 0/24 |              |               |      |  |   |  |  |
| MPLS P   | ::: trackers_drop  |                            |                 |              |               |      | I I Data   | Nova senha  |  |  |
| 🍂 Routing 🗈  | 28 💥 drop  | forward                    | 192.168.88.0/24 |              |               |      |  | Data de nascimento  |  |  |
| 🌐 🛞 System 🗈   | 29 drop  | forward                    | 192 168 88 0/24 |              |               | -    |  |   |  |  |
| 🙊 Queues   | ;;; info_hash_drop   | loindid                    | 132.100.00.0/24 |              |               |      |  |   |  |  |
| Dot1X  | 30 💥 drop  | forward                    | 192.168.88.0/24 |              |               |      |  | Gënero  |  |  |
| - Files  | ::: Bloqueio por Brute Force   | 1                          |                 |              | ( A)          | _    |  | Feminino O Masculino O Personalizado  |  |  |
| E Lee  | Bloqueio por Brute Force   | nput                       |                 |              | 6 (tcp)       |      |  | 0   |  |  |
| Log  | 32 dd src to address list  | input                      |                 |              | 6 (tcp)       |      |  | Ao cicar em inscreva-se, voce concorta com nossos termos,<br>Política de Dados e Política de Cookies. Você pode receber |  |  |
| RADIUS   | 33 X drop  | input                      |                 |              | 6 (tcp)       |      |  | noncações por aixa e pose cancelar são quanto quiser.   |  |  |
| 🗙 Tools 🗈  | 34 K drop  | input                      |                 |              | I (icmp)      | -    |  | Inscreva-se   |  |  |
| New Terminal   | 35 @jump   | forward                    |                 |              | 6 (tcp)       |      |  |   |  |  |
| MetaROUTER   | ::: Ping da Morte  |                            |                 |              |               |      |  | Criar uma Página para uma celebridade, banda ou empresa.  |  |  |
| Partition  | 36 🕫 jump  | forward                    |                 |              | 1 (icmp)      | _    |  |   |  |  |
| Malua Curavit at   | 3/ Vaccept   | Protect-SYN<br>Protect-SYN |                 |              | 6 (tcp)       | _    |  |   |  |  |
| Make Supour.n  | 39 X drop  | PINGOFD                    |                 |              | 1 (icmp)      |      | Portuguiar (Brazel) English (18) English Erangeir (Erange) Italiano Deuterh (11) 1871 877  |   |  |  |
| Manual   | 40 💥 drop  | PINGOFD                    |                 |              | 1 (icmp)      |      | Totogona (onum) English (Od) Explanat Thingka (Tranca) manana Boarach 72 il 19 T (2017) 2018 T   |   |  |  |
| 들 💿 New WinBox   | ::: Facebook   |                            |                 |              |               |      | teorova se Entre Messenger Facebook Lie Pessoas Perfis Páginas Categorias de Página Locais Japos Locais Markeplace Grupos<br>Instagram Locai Compenhas de anterdados de Indrod Serviços Satze Cairaránicio Ciar Página Desenvolvedores Cameiras Pinacidade Cookies<br>Opções de animisióp - Termos Segurança da conta Ajuda para login Ajuda |   |  |  |
| S 📃 Exit   | ··· Google   | IOIWald                    |                 |              |               |      |  |   |  |  |
| SC   | 42 X 💥 drop  | forward                    |                 |              |               |      | Facebook @ 2019  |   |  |  |
| Br (   | ::: Xvideos  |                            |                 |              |               |      |  |   |  |  |
| lte  | 43 💥 drop  | torward                    |                 |              |               | -    |  |   |  |  |
| ō  |  |                            |                 |              |               |      |  |   |  |  |
| LLC.   |  |                            |                 |              |               |      | Aguardando www.google.com  | ·   |  |  |

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 <a href="http://acqnotes.com/acqnote/careerfields/work-breakdown-structure">http://acqnotes.com/acqnote/careerfields/work-breakdown-structure</a>. 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-daatualidade/>. 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: <a href="https://pt.wikibooks.org/wiki/Guia\_do\_Linux/Avan%C3%A7ado/Firewall\_iptables/A\_tabela\_mangle">https://pt.wikibooks.org/wiki/Guia\_do\_Linux/Avan%C3%A7ado/Firewall\_iptables/A\_tabela\_mangle</a>>. Acesso em: 02/08/2019.

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

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

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

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 MinerarCriptomoedasNaWeb.Disponívelem:<https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2018/08/02/hackers-<br/>atacam-roteadores-mikrotik-no-brasil-para-minerar-criptomoedas-na-web.ghtml>. Acesso<br/>em: 05/11/2018.

SEGURANCA-DA-INFORMACAO.INFO. **Segurança da Informação**. Disponível em: <a href="http://seguranca-da-informacao.info/>">http://seguranca-da-informacao.info/></a>. 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/artigosseguranca/07/06/2017/o-desafio-de-seguranca-da-informacao-numa-sociedadeconectada-pelas-coisas/>. Acesso em: 21/10/2018.