PLANO DE CONFIGURAÇÃO

R-MK

Descrição: unidade, setor Licenciamento

Hardware:

VM... 1.5GB RAM, 50GB, Intel core i7 8990

Nics : 1 rede Externa (“Modo Bridge”) 3 Internas (“INT-SERV”, “CLIENT”, “CLIENT1”)

Instalação:

Mikrotik RouterOs v6.49.3

Winbox 64bit

Chave de ativação: **-----BEGIN MIKROTIK SOFTWARE KEY----------**

r4YiNL2vJCLq3jdrzUsidEOqke2vD47bOCtyKyyfKPWJ

j5X7TxKFEdJKwhjDOjs83/yBCsFUVSDpOa12dfVcCA==

-----END MIKROTIK SOFTWARE KEY----------

https://mikrotik.com/download

CRIAR USUÁRIO ADMINISTRADOR:

System:

Users: Adicionar

Usuario: friendly2022

Group: full

Senha: **friendly2022H@rdw@re***

(Sair do winbox e logar. com o novo usuário e remover o usuário admin/padrão)

ADICIONAR REDE AO ROUTER:

IP:

DHCP Client: Adicionar

Interface: Wan / OK

ATUALIZAR O ROUTER:

System: Packages

Check for Updates:

Chanel: Stable

Download Install:

ATUALIZAR O FIRMWARE:

System:

RouterBORD:

Updates: OK

System:

Reboot:

NOME DO ROUTER:

System:

Identity: Friendly Hardware.

RENOMEAR INTERFACES:

Interfaces: Duplo click sobre a interface a ser renomeada

CRIAR BRIDGE:

Bridge:

Bridge: Adicionar

General:

Name: bridge-LAN

Ports: Adicionar

General:

Interfaces: ADM / INT-SERV/OPTEC/ADM

ADD IP À INTERFACE OU A BRIDGE:

CENÁRIO 1 FIREWALL

IP:

Addresses: Adicionar

Addresses: 172.30.16.1/20 – Interface INT-SRV

Addresses: 172.30.32.1/20 – Interface ADM

Addresses: 172.30.80.1/20 – Interface OPTEC

Interface: Nome da interface ou bridge que terá o IP atribuído.

DHCP Relay: Adicionar

Interface: ADM/ OPTEC

DHCP Server: 172.30.16.6

ADD IP À INTERFACE OU A BRIDGE:

CENÁRIO 2 FIREWALL

IP:

Addresses: Adicionar

Addresses: 172.30.96.1/20 – Interface RMK-PFSENSE

NAT:

IP:

Firewall:

NAT: Adicionar

General:

Chain: srcnat

Out. Interfaces: Wan

Action:

Action: masquerade

IP SERVICE PORT:

Winbox: Porta 9865

WWW: Porta 80 IP rede local 172.30.32.0/20

FIREWALL:

Regra permitir acesso Winbox:

Filter Rules: Adicionar

General:

Chain: Input

Protocol: 6 (tcp)

Dst. Port. 9865

Action: accept

Via terminal:

```
/ip firewall filter add action=accept chain=input comment="Libera acesso ao Winbox " dst-port=\
    9865 protocol=tcp
```

Identificação de PortScaner:

Filter Rules: Adicionar

General:

Chain: Input

Protocol: 6 (tcp)

Extra:

PSD: Default

Action: add src to address list

Address list: PortScan

Timeout: 2d 00:00:00

Via terminal:

```
/ip firewall filter add action=add-src-to-address-list address-list=PortScan \
   address-list-timeout=2d chain=input comment="Detecta PortScan" protocol=\
   tcp psd=21,3s,3,1
```

Identificação de PortScaner / Pé de lã:

Filter Rules: Adicionar

General:

Chain: Input

Protocol: 6 (tcp)

Dst. Port: 20-23,80,3389,53,1723

Extra:

PSD: Default

Action: add src to address list

Address list: PortScan

Timeout: 7d 00:00:00

Via terminal:

```
/ip firewall filter add action=add-src-to-address-list address-list=PortScan \
   address-list-timeout=7d chain=input comment="Pega pe de la" dst-port=\
   20-23,80,3389,53,1723 protocol=tcp
```

Bloqueio de PortScan:

Filter Rules: Adicionar

General:

Chain: Input

Advanced:

Src. Address List: PortScan

Action: drop

Via terminal:

/ip firewall filter add action=drop chain=input comment="Bloqueia PortScan" src-address-list=\

PortScan

Bloqueio Bruteforce login SSH:

Via Terminal:

/ip firewall filter

```
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \
comment="drop ssh brute forcers" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist \
address-list-timeout=10d comment="" disabled=no
```

```
add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 \
address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

PROTEÇÃO CONTRA SYN FLOOD (NEGAÇÃO DE SERVIÇO):

Identificar e adicionar Syn Flood IP a lista:

Filter Rules: Adicionar

General:

Chain: Input

Protocol: 6 (tcp)

Extra:

Connection Limit :

Limit: 30

Netmask: default

Action: add src to address list

Address list: SynFlooder

Timeout: 2d 00:00:00

Via Terminal:

```
/ip firewall filter add chain=input action=add-src-to-address-list address-list=SynFlooder address-list-timeout=2d \
comment="Identificar e adicionar Syn Flood IP a lista" connection-limit=30,32 disabled=no protocol=tcp tcp-flags=syn
```

BLOQUEIAR SYNFLOOD:

Filter Rules: Adicionar

General:

Chain: Input

Advanced:

Src. Address List: SynFlooder

Action: drop

Via Terminal:

/ip firewall filter add action=drop chain=input comment="Bloquear syn flood" disabled=no src-address-list=SynFlooder

BACKUP:

New terminal:

Export file=BkpScript

Files:

Backup:

Botão direito sobre o arquivo:

Download:

Restaurando configurações:

Files:

Backup:

Upload: importar o arquivo do backup:

New terminal:

Import file-name=Tab (será preenchido automaticamente com o nome do arquivo)

FRIENDLY HARDWARE

MikroTik

Software