**Documentação da Configuração da MikroTik RB750Gr3 - Gateway do Home Lab**

**📌 Visão Geral**

Este documento descreve a configuração e as decisões técnicas tomadas na implementação da MikroTik RB750Gr3 (modelo hEX) como gateway principal do ambiente de Home Lab. A solução visa prover conectividade, segurança e controle avançado para uma rede doméstica com múltiplos serviços virtuais e dispositivos físicos.

**🧩 Topologia Resumida**

* **ether1**: WAN - Conexão com o provedor via PPPoE
* **ether2**: AP do laboratório (Wi-Fi dedicado ao Home Lab)
* **ether3**: PC de administração da rede
* **ether4**: Proxmox Hypervisor
* **ether5**: AP da sala de estar
* **bridge1**: Agrega ether2–ether5, atuando como switch e interface LAN

**📐 Endereçamento e Rede Local**

* **Faixa de IP**: 10.100.0.0/16
* **Gateway padrão**: 10.100.0.1 (IP atribuído à bridge)
* **Servidor DHCP ativo**:
  + **Range**: 10.100.10.10 – 10.100.255.254
  + **Interface**: bridge1
  + **Reservas de IP e lease fixo** para dispositivos críticos (ex: PC de admin)

🔎 **Decisão técnica**: O uso de uma máscara /16 permite amplo espaço de endereçamento interno, facilitando a separação lógica futura por sub-redes ou VLANs, sem mudanças drásticas na estrutura IP.

**🌐 Conectividade WAN**

* **Interface WAN**: ether1
* **Cliente PPPoE configurado** com credenciais do provedor de internet
* IP dinâmico recebido via PPPoE
* DNS forwarding habilitado

**🧾 Segurança e Hardening**

**1. Usuários e Autenticação**

* Criado novo usuário com grupo full e senha forte
* **Usuário padrão admin foi removido**

🔐 **Racional**: Minimiza risco de ataque via dicionário/brute-force usando credenciais default.

**2. Serviços IP**

* Acesso aos serviços (Winbox, Web, API, etc.) restrito apenas à sub-rede local
* Serviços desnecessários foram desabilitados

**3. IP Neighbors Discovery**

* Discovery desabilitado para interfaces WAN
* Habilitado apenas na bridge local

**4. Firewall**

**🔸 Port Knocking**

Implementado port knocking em duas etapas:

| **Porta** | **Função** | **Timeout** |
| --- | --- | --- |
| 3366 | Primeira etapa (pré-admin) | 3 segundos |
| 6699 | Segunda etapa (rede-admin liberada) | 5 horas |

* Regras criam endereço de lista (address list) temporária para liberar o acesso remoto à RB
* IP local do PC de administração já está com **IP fixo liberado**, não exigindo knocking

**🔸 FastTrack**

* Regra para **FastTrack de conexões estabelecidas e relacionadas**
* Melhoria significativa no throughput e desempenho de NAT

**🔸 Controle ICMP**

* Regras para limitar **ping flood (ICMP rate-limit)**
* Evita ataques de negação de serviço simples (DoS)

**🔸 SNMP para Monitoramento**

* Regras específicas para liberar SNMP **apenas para o IP do servidor Zabbix** local

**🔸 Regra de Drop Final**

* Implementada **regra de drop all no final da cadeia** para eliminar qualquer tráfego não permitido explicitamente

**⚙️ Scripts e Otimizações**

* Criação de listas dinâmicas no firewall (address-list) para controlar acesso remoto
* IP fixo atribuído ao PC do administrador via lease DHCP estático
* Logging ativado para eventos de acesso indevido ou tentativas falhas de port knocking

**🔒 Considerações Finais**

Esta configuração estabelece uma base segura, performática e escalável para o Home Lab, mantendo o controle detalhado sobre acessos e a flexibilidade necessária para expansão futura. O uso de port knocking e regras refinadas de firewall permite acesso remoto seguro sem comprometer a superfície de ataque.