Treinamento SixCore MTCNA - Configuração de Firewall Mikrotik

Em desenvolvimento

1 - Paulo Patrick Rodrigues da Silva
2 - Controllar Sistemas de Segurança e Acesso

Fonte: https://wallpaperaccess.com/mikrotik

1 - Introdução

A função de um firewall é proteger a rede, o qual pode abranger desde regras simples e genéricas a complexas e específicas. O roteador Mikrotik possui um sistema firewall integrado que trabalha baseado em filtragem de pacotes utilizando estados de conexões (novas, estabelecidas, relacionadas e inválidas), assim como o uso do protocolo de tradução de endereços NAT para redirecionamentos (srcnat, dstnat, masquerade), bloqueio de endereços cujas ações sejam suspeitas, entre outras atuações.

O firewall integrado ao Mikrotik é denominado “Firewall de Filtro de Pacotes com Inspeção de Estado, do ingês SPI, assim não sendo um “Next Generation Firewall – NGFW”. Essa classificação é para equipamentos dedicados à proteção da rede como, por exemplos, FortiGate, Palo Alto e Sophos, os quais detém maiores capacidades defensivas; não significa que seja necessária sua instalação em um ambiente de produção.

O uso de um equipamento firewall dedicado é, usualmente, instalado em grandes empresas com altas taxas de acesso, na casa dos milhares, havendo um alto custo na compra, instalação e manutenção. Para ambientes menores um mikrotik com SPI é suficiente.

2 - Proposta

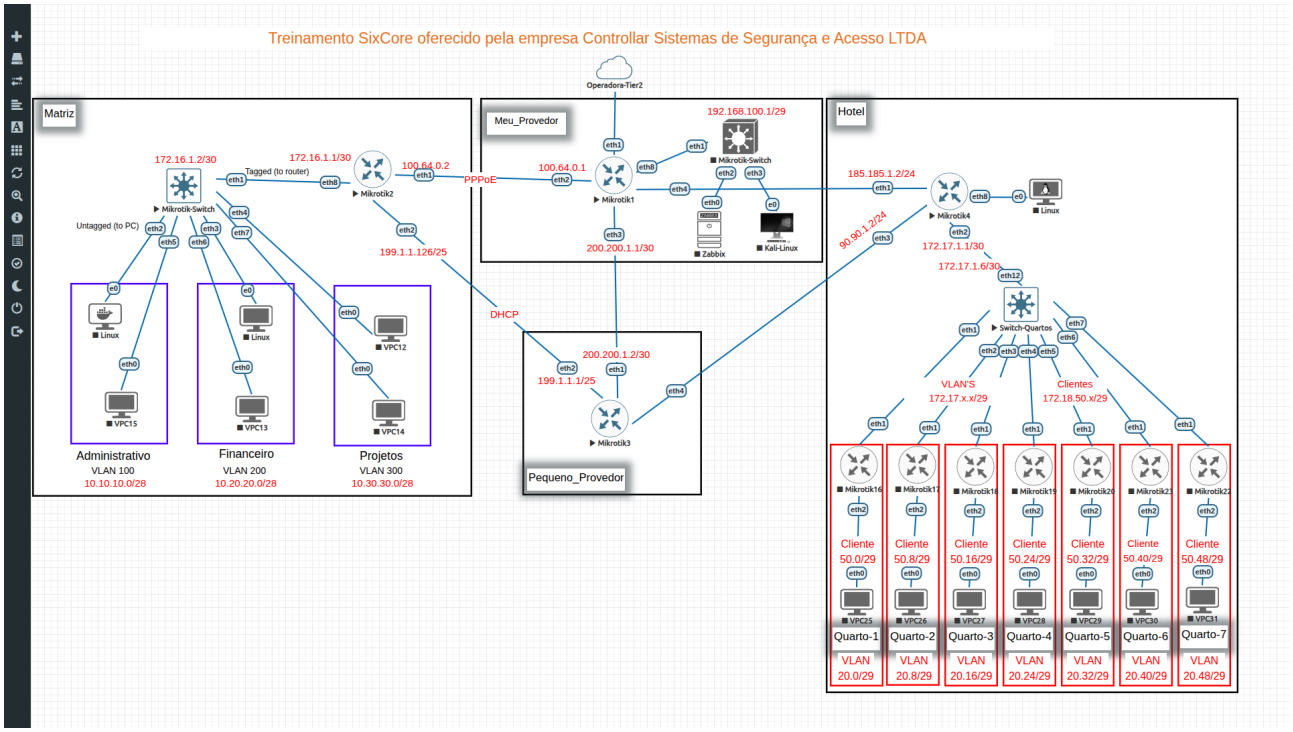
Um ambiente simulado no emulador EVE-NG abordando um provedor de internet Tier 2 (Cloud0-Management) que vende um link de internet a um provedor menor, enquanto esse revende o link para demais empresas, inclusive micro provedores sem acesso às empresas Tier 2.

O foco do projeto será um roteador de borda de uma empresa (Matriz + Hotel). O equipamento simulado é uma Cloud Hosted Router (CHR) versão 7.20.6 sob a licença P1 fornecida no treinamento SixCore, a qual limita a velocidade de transmissão de dados em 1 GB no cenário simulado. A configuração abrangerá todas as etapas estudadas no treinamento, com maior atenção ao firewall, o que não implica menor atenção às outras ferramentas do equipamento como, por exemplo, controle de banda dos clientes.

1 – Estudante de Defesa Cibernética (Estácio), treinando para certificação MTCNA com a SixCore.
2 – Empresa patrocinadora do treinamento.

3 - Simulação no EVE-NG (em desenvolvimento)

Imagem 1 – Ambiente simulado no emulador EVE-NG



Fonte: Autoria própria

4 – Configurações

4.1 – As configurações iniciais no ambiente iniciaram no provedor de internet que recebe link da operadora Tier 2, nomeado como “Meu_Provedor” no EVE-NG.

Nota:

Os provedores de serviço de internet (ISP’s) são classificados em três níveis – Tier 1, Tier 2 e Tier 3 – com base em sua infraestrutura, alcance global e como se conectam à internet.

- Tier 1 – São os provedores responsáveis pela espinha dorsal da internet global. Possuem redes próprias interligadas sem que haja processo de compra de links entre si, mas sim acordos de peering gratuito. Exemplos de provedores nesta categoria são AT&T, NTT e Verizon.

- Tier 2 – Operadores de internet regionais e nacionais que compram link de internet de provedores Tier 1, mas também fazem acordos peering com outros Tier 2 para redução de custos. Exemplos de empresas categorizadas como Tier 2 são a Comcast e Vodafone.

- Tier 3 – Provedores locais e de última milha que alugam links de internet de provedores Tier 2 para revender aos consumidores locais (residenciais e empresariais). Não possuem infraestrutura global e dependem de provedores de categoria superior. Exemplos de empresas Tier 1 são ISP’s locaos e operadoras regionais.

4.2 – Segue para configuração do micro provedor que revende o link adquirido do provedor “Meu_Provedor”, nomeado “Pequeno_Provedor” no EVE-NG.

...

4.3 – Configuração do roteador da empresa – Matriz

4.3.1 – Configuração do Firewall

O Mikrotik possui 4 tabelas para atribuições de regras de firewall – Filter Rules, NAT, Mangle e Raw, sendo cada uma dessas responsável por certas funções.

- **Filter Rules** → Controle de tráfego. Permite e bloqueia a passagem de pacotes, tanto em direção ao interior do roteador (input) quanto partindo dele (output), assim como os dados que apenas passam pelo roteador (forward) por estar no meio do caminho (PC → Roteador → Internet).

- **NAT** → Trata-se do protocolo de tradução de endereços (NAT, do inglês) que converte os endereços de IP privados a públicos, além de traduzir também portas de acesso; realiza direcionamentos.

- **Mangle** → Marca e manipula pacotes como, por exemplo, priorizar tráfego de VoIP (Qualidade de Serviço, do inglês QoS).

- **RAW** → Filtragem de pacotes antes de ocorrer o processo de roteamento no roteador, muito utilizado para impedir tráfego malicioso.

Regras básicas:

❯ IMPORTANTE → Antes de validar a regra “Drop Geral”, aplicar todos os serviços aceitos antes, porque caso faça primeiro, poderá **perder o acesso** ao roteador.

1 – **Aceitar conexões estabelecidas ou relacionadas** (até então não há uso do protocolo OSPF para roteamento dinâmico, logo não é necessário marcar a opção “untracked”).

- Chain: input
- Connection Type: established related
- Action: Accept

2 – **Aceita os serviços WinBox, SSH e Webfig** com portas alteradas.

As redes de computadores funcionam com base no protocolo TCP/IP via portas de acesso, como as exemplificadas abaixo. É de boa prática alterar as portas a serem utilizadas por motivos de segurança, afinal as padronizadas são frequentemente escaneadas, atacadas.

Serviço	Porta(s) padrão	Porta(s) adotada(s)
WinBox	8291	47511
SSH	22	15748
Webfig	80, 443	26423, 36589

Caminho: IP → Services (IP Services List).

3 – **Aceita a rede virtual privada (do inglês, VPN)** Wireguard

- Chain: input
- Protocolo: UDP
- Dst. Port: 55056

4 – **Recusa de pacotes inválidos** (Origem desconhecida)
- Chain: input
- In. Interface List: WAN (Lista com as interfaces que recebe link de internet).
- Connection Type: Invalid
- Action: Drop

5 – Regra **PortScan Detective**

As redes de computadores funcionam com base no protocolo TCP/IP via portas de acesso, como as exemplificadas anteriormente. Há algumas portas publicamente conhecidas como “well-known-ports” por serem críticas, com graus elevados de privilégio, ou seja, devem receber maior atenção – protegidas com rigor.

Exemplos de portas sensíveis – as ditas “Portas Baixas”:

- Acesso Remoto / Administração:

Porta	Protocolo	Serviço	Risco
22	TCP	SSH	Brute Force
23	TCP	Telnet	Senha em texto puro
3389	TCP	RDP	Brute Force
5900	TCP	VNC	Acesso Remoto

- Serviços de rede essenciais:

Porta	Protocolo	Serviço
21	TCP	FTP
25	TCP	SMTP
53	TCP/UDP	DNS
80	TCP	HTTP
443	TCP	HTTPS

- Infraestrutura / Baixo nível:

Porta	Serviço
67/68	DHCP
123	NTP
161	SNMP

445	SMB

Sabendo que existem diversas portas críticas na rede, é de boa prática a sua proteção. A regra de firewall a ser configurada para barrar os endereços oriundos da internet pode seguir a seguinte forma:

- Chain: input
- Protocolo: TCP
- In. Interface List: WAN
- Extra → PSD
- Action: add src to address list
- Address List: PortScan

A ação “add src to address list” capta o endereço IP de quem tentou acesso à porta e o guarda em uma lista denominada “PortScan” por um período determinado. O número de tentativas de acesso à porta é padronizado por peso na configuração da regra, na aba “extra” → PSD (PortScan Detection).

- Weight Threshold: 21
- Delay Threshold: 00:00:03
- Low Port Weight: 3
- Hight Port Weight: 1

Caso haja múltiplas tentativas de acesso às portas altas e baixas em um período inferior a 3 segundos, existindo para cada tipo de porta um peso (alta: 3, baixa: 1), soma-se os pesos das portas em questão e, caso alcance a pontuação de 21, a conexão passa a ser considerada suspeita e é detida pela regra de firewall.

Seguindo a mesma linha de raciocínio, uma regra para impedir quem tentar diversos acessos ao roteador com foco em portas ainda mais sensíveis, como exemplo a 22 (SSH – Acesso Remoto), pode ser reforçada a segurança com mais uma regra, mais específica para estes casos:

- Chain: input
- Protocolo: TCP
- Dst. Ports: 20-25, 3389, 5900
- Action: add src to address list
- Address List: PortScan
- Timeout: 7d 00:00:00

Para que os endereços IP alocados na lista de PortScan sejam barrados em novas tentativas de conexões, é na aba Raw que se cria uma regra de prerouting. Nessa área de regras são escritas àquelas que serão avaliadas antes de a conexão chegar ao centro do roteador e ser processada, gastar CPU.

- Chain: prerouting
- Src. Address List: PortScan
- Action: Drop

EM DESENVOLVIMENTO…

4.2 – Controle de Banda

Quando o tema é controle de qualidade da internet, há no Mikrotik o menu Queues onde são criadas regras enumeradas, assim como no firewall. Neste campo é configurada a velocidade máxima que determinados dispositivos em uma rede pode atingir.

Supondo que a velocidade contratada pela empresa (Matriz) seja de 100 Mb; a equipe de TI pode configurar no roteador Mikrotik na aba Queues o quanto desse limite será distribuído em todos os dispositivos, em todas as VLAN's. Podem ser criadas regras (Simple Queues) que limitam a banda fornecida com base, por exemplo, no dia e hora da semana, no consumo de um cliente, citando alguém que aproveita a rede wi-fi para baixar um arquivo grande – neste caso para não utilizar toda a banda contratada de 100 Mb, pode ser controlada a banda fornecida aos outros cliente utilizando garantias (targets de upload e download), impedindo assim de um prejudicar o outro.

4.2.1 – Configuração de Controle de Banda

A configuração de controle de banda no roteador da empresa (Matriz) foi considerando a velocidade em que os computadores alcançaram em simulação no emulador EVE-NG – aproximadamente 50 Mb. Atribuídos 2 Simple Queues nomeadas "LINK – Dedicado" e "LINK – CGNAT" com os respectivos Target Upload e Target Download travados em 50 Mb, considerando o Target como 0.0.0.0/0, em conformidade com o treinamento.

Cada VLAN configurada no roteador recebeu uma Simple Queue com seu limite de velocidade – Max Limit – igual a 20 Mb, em ambos os Targets (upload e download). A garantia de banda – Limit At – adotada foi de 15 Mb sem prioridade (Priority = 8) para nenhum cliente, com o devido controle de banda entre usuários – Queue Type padronizado em PCQ = 0 – o que implica uma divisão igualitária do total da banda disponível entre todas a VLAN's.

E visando um bom relacionamento com o cliente, é atribuído um boost de velocidade de 30 Mb para os primeiros momentos de conexão – o que transmite sensação de maior velocidade ao iniciar downloads (exemplo: o carregamento inicial de um vídeo no YouTube ser mais rápido).