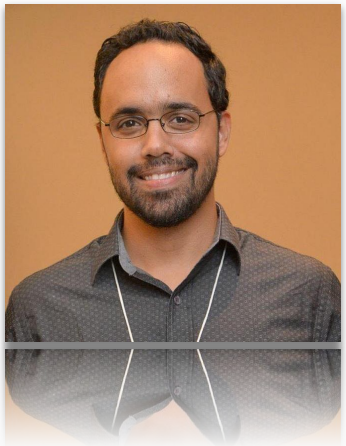
Firewall Stateful

Segurança preventiva – MikroTik routerOS

Leonardo Rosa, BRAUSER, Brasil

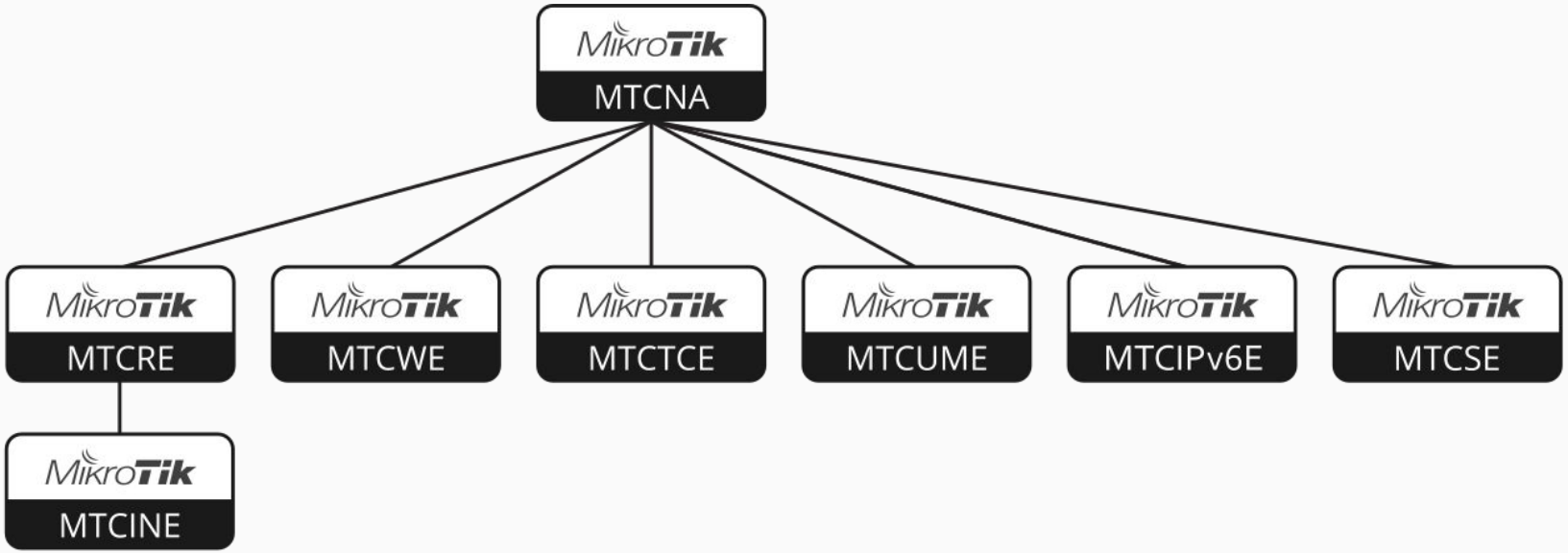
Sobre o Autor

Leonardo Rosa



- Baiano, pai de 2 meninos
- Mais de 20 anos de experiência na área
- 2006 – Consultor em Internetworking
- 2012 – Instrutor MikroTik, certificado na Polônia
- Ministra treinamentos nas certificações MTCNA, MTCRE, MTCINE, MTCWE, MTCTCE, MTCUME, MTCIPv6E e MTCSE
- Experiente em segurança e roteamento

Cursos de Certificação MikroTik



Mais informação em: mikrotik.com/training

Características do Firewall Stateful

1. Minimiza exposição e reduz **drasticamente** possibilidades de ataques, sejam vindo da Internet quanto da rede privada.
2. Consegue garantir que todo fluxo vindo da Internet seja apenas resposta de uma solicitação interna autêntica. Premissa para evitar exposição e **ataques**.
3. Permite limites e diversos recursos baseados em conexão como:
    a. Classificação de tráfego por IP, porta, protocolo, serviço geralmente usada para QoS ou políticas de segurança. Exemplos de classificação: redes sociais, VPN, acessos remotos, **jogos**.
    b. Definir perfil de acesso residencial e corporativo por volume, tanto de dados quanto de pacotes. Além de sugerir atividades suspeitas/maliciosas na rede.
4. Com recursos adicionais da **MikroTik**, é possível automatizar toda a proteção e construir padrões que simplificam a manutenção do **firewall**.

Características do Firewall Stateful

5. Mapeia em memória os pacotes e os classifica em conexões. O routerOS usa quatro classificações: **new**, **established**, **related**, **invalid**.

    a. **New**: todo pacote não mapeado. É sempre o primeiro pacote de um mesmo fluxo. Se o firewall descartar esse pacote, ele sai da memória. Assim, o próximo pacote do mesmo fluxo é também classificado como **new**. Se o firewall permitir o pacote new, os próximos pacotes do fluxo são classificados como **established**.

    b. **Established**: todo pacote liberado em trânsito pelo firewall. É aqui que trafega toda a banda no router.

    c. **Related**: é também pacote não mapeado, como o **new**, e tem o mesmo comportamento deste. A única diferença é a relação que essa nova conexão tem com uma outra conexão já estabelecida (**established**).

    d. **Invalid**: firewall não consegue determinar seu estado por conter atributos IP irregulares ou por estar muito fora de ordem de seu possível fluxo. Esse tipo não sofre **NAT** e recomenda-se descartá-lo tanto em **forward** quanto em **input**.

Nosso modelo de configuração

Ordem recomendada de implantação

1. **BACKUP** (backup completo e export do firewall)
    a. `/system backup save name=antes-do-firewall`
    b. `/ip firewall export file=firewall-antigo`
2. **LISTAS** (de interface e de endereços devem ser ajustadas)
3. Connection tracking
4. **RAW**
5. Filter

Nossas listas

```
/ip firewall address-list

add list=LAN            # todo prefixo interno

add list=BOGONS         # todo prefixo inválido na Internet

add list=DNS-server     # todo servidor DNS confiável

add list=FW-OFF         # prefixos sem firewall

add list=FW-FULL        # hosts com proteção total

add list=LAN-services   # serviços de uso interno exclusivo
```

Nossas listas

```
/ip firewall address-list

add list=LAN              # todo prefixo interno
```

Contém os prefixos de uso privado (RFC1918), inclusive o de CGNAT (RFC6598), mais todo prefixo público em uso, cedido por terceiros ou de propriedade exclusiva adquiridos junto ao RIR (REGISTRO.BR). Essa lista identifica toda a rede interna.

Nossas listas

```
/ip firewall address-list

add list=BOGONS          # todo prefixo inválido na Internet
```

Contém os prefixos de uso especial listados pela IANA em IANA IPv4 Special-Purpose Address Registry. Estes prefixos não são encontrados na Internet e podem ser usados para gerar lixo na rede ou mesmo comprometer a operação da rede interna se não tratado adequadamente.

Nossas listas

```
/ip firewall address-list

add list=DNS-server     # todo servidor DNS confiável
```

Contém os servidores DNS privados, aqueles que usam endereço IP contido na lista LAN. Assim conseguimos controlar falhas relacionadas a "open recursive DNS". Esta lista também contém servidores públicos e confiáveis como os da Google, Cloudflare, Cisco.

Nossas listas

```
/ip firewall address-list

add list=FW-OFF          # prefixos sem firewall
```

Contém clientes corporativos de perfil extranet. Aqueles que prestam serviços de conectividade como acesso remoto, vpn, voip, dns etc. como redes de lojas e até ISP parceiros. Para tais clientes não existem bloqueios nem qualquer segurança. É importante deixá-los cientes disso. Essa lista deve ser a **menor** possível.

Nossas listas

```
/ip firewall address-list

add list=FW-FULL        # hosts com proteção total
```

Contém hosts que requerem nível de proteção máxima, pois qualquer acesso remoto será bloqueado por padrão. Podem ser desde sistemas com alto valor comercial ou mesmo sistemas legado que não sofrem atualizações de segurança e podem/devem ter diversas falhas conhecidas.

Nossas listas

```
/ip firewall address-list

add list=LAN-services   # serviços de uso interno exclusivo
```

Contém serviços internos com acesso completo à rede, porém ainda com proteção relativa à Internet. Exemplos são sistemas de monitoramento SNMP e hosts de gerência.

Chaves ON e OFF

4 firewalls no total:

- RAW input
- RAW forward
- Filter forward
- Filter input

Para cada firewall, existe uma regra para "desligar" todas as demais. Ou seja, para "desligar" completamente este mesmo firewall.

O intuito é evitar acidentes ao desativar as regras de controle e proteção.

RAW

RAW input

```
/ip firewall raw

add action=jump chain=prerouting comment=INPUT--INICIO \
    dst-address-type=local,broadcast,multicast jump-target=input
```

Ao criarmos a chain input em RAW, conseguimos proteger o acesso ao router de maneira mais eficiente. Com isso, a proteção feita em Filter input servirá meramente como backup.

RAW input

Política Restritiva

A lógica é liberar acesso remoto a partir da LAN e a partir da Internet, se identificado com a técnica do toc-toc (knock-knock); liberar serviços cujo router pode desempenhar como cliente (consultas DNS, downloads, protocolos de roteamento etc.); somente. Tudo mais será bloqueado com um drop explícito ao final do input.

RAW forward

```
/ip firewall raw

add action=drop chain=input comment=NEGA-TUDO disabled=yes

add action=drop chain=prerouting in-interface-list=WAN \

    src-address-list=BOGONS comment=BOGON
```

Não há necessidade de criar a chain forward, contanto que usemos a chain padrão **prerouting** em regras abaixo das regras de input.

Política Permissiva

A lógica é bloquear todo lixo (segundo boas práticas conhecidas) e gerar proteção para demais serviços da rede. Aqui é importante considerar perfis diferentes de acesso, pois estes terão liberdades diferentes e volumes diferentes de tráfego. Os perfis reconhecidos em nosso firewall estão representados pelas listas (/ip firewall address-list) apresentadas anteriormente.

RAW em routers com NAT

Nenhuma política fechada pode ser aplicada ao firewall RAW quando se usa **NAT**. Ou seja, não é possível bloquear tudo no final.

Explico: todo pacote em NAT tem como endereço de origem ou destino, IP do próprio roteador, independente de o tráfego ser autêntico forward. Numa tentativa de drop final, estaremos bloqueando não apenas input mas todo prerouting em si.

Filter

Filter input

Proteção Garantida

Ao criar a chain input em RAW, conseguimos proteger o acesso ao router de maneira mais eficiente. Com isso, a proteção feita em input Filter servirá meramente como backup.

Filter forward

Política Stateful

Aqui temos recursos exclusivos para proteção complementar. A lógica continua permissiva até certo ponto: lixo extra é bloqueado, serviços locais são protegidos e todo tráfego da rede interna é garantido. O diferencial é que conseguimos identificar e limitar tráfegos suspeitos, evitando tanto a exposição quanto a exploração dos recursos da rede.

O maior benefício é poder escolher a prevenção ao invés da remediação.

Nossa configuração (rsc)

ATENÇÃO!

Devido a complexidade de elaborar configuração compatível com roteadores de borda com NAT, decidimos simplificar e criar 2 arquivos, um considerando NAT outro sem NAT.

A configuração apresentada seguir é **apenas para roteadores sem NAT**, mais completa. Em outro momento, apresentaremos a versão simplificada para aqueles que usam NAT na borda.

fw-stateful.rsc

Cabeçalho

```
# leonardorosa.com
#
#
# seu prefixo Global: 198.51.100.0/24


#[ -- PARA ROTEADORES DE BORDA *SEM* NAT -- ]


/interface list

add name=WAN
add name=LAN
```

Listas

```
/ip firewall address-list

add address=10.0.0.0/8 list=LAN
add address=172.16.0.0/12 list=LAN
add address=192.168.0.0/16 list=LAN
add address=100.64.0.0/10 list=LAN
add address=198.51.100.0/24 list=LAN comment=SeuPrefixoGlobal

add list=FW-FULL disabled=yes
add list=FW-OFF disabled=yes

add address=198.51.100.8 list=LAN-services comment=GERENCIA
add address=198.51.100.9 list=LAN-services comment=MONITORAMENTO

add address=198.51.100.1-198.51.100.4 list=DNS-server comment=Seu-DNS-local
```

Listas

```
add address=0.0.0.0/8 comment="RFC6890" list=BOGONS
add address=10.0.0.0/8 comment="RFC6890" list=BOGONS
add address=100.64.0.0/10 comment="RFC6890" list=BOGONS
add address=127.0.0.0/8 comment="RFC6890" list=BOGONS
add address=169.254.0.0/16 comment="RFC6890" list=BOGONS
add address=172.16.0.0/12 comment="RFC6890" list=BOGONS
add address=192.0.0.0/24 comment="RFC6890" list=BOGONS
add address=192.0.2.0/24 comment="RFC6890" list=BOGONS
add address=192.88.99.0/24 comment="6to4 relay Anycast RFC 3068" list=BOGONS
add address=192.168.0.0/16 comment="RFC6890" list=BOGONS
add address=198.18.0.0/15 comment="RFC6890" list=BOGONS
add address=198.51.100.0/24 comment="RFC6890" list=BOGONS
add address=203.0.113.0/24 comment="RFC6890" list=BOGONS
add address=224.0.0.0/4 comment="RFC6890" list=BOGONS
add address=240.0.0.0/4 comment="RFC6890" list=BOGONS
```

Listas

```
add address=1.1.1.1 comment=Cloudflare list=DNS-server
add address=1.0.0.1 comment=Cloudflare list=DNS-server
add address=8.8.8.8 comment=Google list=DNS-server
add address=8.8.4.4 comment=Google list=DNS-server
add address=208.67.222.222 comment=OpenDNS list=DNS-server
add address=208.67.222.123 comment=OpenDNS list=DNS-server
add address=208.67.220.220 comment=OpenDNS list=DNS-server
add address=208.67.220.123 comment=OpenDNS list=DNS-server
```

Pequeno ajuste em Tracking

```
/ip firewall connection tracking

set generic-timeout=2m tcp-established-timeout=8h
set enabled=auto
```

RAW input

```
/ip firewall raw

add action=accept chain=prerouting comment=DESLIGA--RAW_input disabled=yes \
     dst-address-type=local,broadcast,multicast
add action=accept chain=prerouting comment=DESLIGA--RAW_forward disabled=yes \
     dst-address-type=unicast

#[--INPUT--]
add action=jump chain=prerouting comment=INPUT--INICIO \
     dst-address-type=local,broadcast,multicast jump-target=input

add action=accept chain=input comment=BGP port=179 protocol=tcp
add action=notrack chain=output comment=OSPF protocol=ospf
add action=notrack chain=input comment=OSPF protocol=ospf
add action=accept chain=input comment=OSPF protocol=ospf
add action=accept chain=input comment=LAN src-address-list=LAN
```

RAW input

```
#[--router-services-as-client--]
add action=accept chain=input comment=udp-services__ajustar_leonardorosa.com \
     protocol=udp src-port=53,123,3784-3785,5678,15252
add action=accept chain=input comment=tcp-services__ajustar_leonardorosa.com \
     protocol=tcp src-port=20-23,53,80,443,587,8291

#[--toc-toc--]
add action=add-src-to-address-list address-list=toc-toc-1 address-list-timeout=15s \
     chain=input comment=toc-toc-1 dst-port=321 protocol=tcp
add action=add-src-to-address-list address-list=toc-toc-2 address-list-timeout=15s \
     chain=input comment=toc-toc-2 dst-port=4321 protocol=udp src-address-list=toc-toc-1
add action=add-src-to-address-list address-list=LAN address-list-timeout=30m chain=input \
     comment=toc-toc-3 dst-port=54321 protocol=tcp src-address-list=toc-toc-2
```

RAW input

```
#[--sessao-winbox--]
add action=add-src-to-address-list address-list=LAN address-list-timeout=10m \
     chain=input comment=suporte-sessao dst-limit=1,0,addresses-and-dst-port/1m \
     limit=1,0:packet protocol=tcp src-address-list=suporte-sessao tcp-flags=psh
add action=accept chain=output comment=suporte-sessao dst-address-list=LAN \
     protocol=tcp tcp-flags=psh
add action=add-dst-to-address-list address-list=suporte-sessao address-list-timeout=10s \
     chain=output comment=suporte-sessao dst-address-list=!LAN packet-size=200-65535 \
     dst-limit=1,0,addresses-and-dst-port/1m limit=1,0:packet protocol=tcp tcp-flags=psh

add action=log chain=input comment=NEGA-TUDO limit=1/1s,1:packet log-prefix="drop-RAW #"
add action=drop chain=input comment=NEGA-TUDO disabled=yes
```

RAW forward

```
#[--lan-services--]
add action=accept chain=prerouting comment=LAN-services dst-address-list=LAN-services \
     src-address-list=LAN
add action=accept chain=prerouting comment=LAN-services dst-address-list=LAN \
     src-address-list=LAN-services

#[--lixo--]
add action=drop chain=prerouting comment=BOGONS in-interface-list=WAN \
     src-address-list=BOGONS
add action=drop chain=prerouting comment=IP-SPOOFING dst-address-list=LAN \
     src-address-list=LAN in-interface-list=WAN log-prefix="SPOOF #"
add action=accept chain=prerouting protocol=icmp icmp-options=8:0 comment="ping"
add action=accept chain=prerouting protocol=icmp icmp-options=0:0 comment="pong"
add action=accept chain=prerouting protocol=icmp icmp-options=11:0-255 comment="traceroute"
add action=drop chain=prerouting protocol=icmp comment="bad ICMP" log-prefix="bad-icmp #"
```

RAW forward

```
#[--lixo--]
add action=drop chain=prerouting comment="bad UDP" protocol=udp \
     port=0,135-139,445,5376,10001
add action=drop chain=prerouting comment="bad UDP" protocol=udp src-port=1900 dst-port=1900
add action=drop chain=prerouting comment="bad TCP" port=0,135-139,445,25 protocol=tcp
add action=drop chain=prerouting comment="bad TCP" protocol=tcp \
     tcp-flags=!fin,!syn,!rst,!ack
add action=drop chain=prerouting comment="bad TCP" protocol=tcp tcp-flags=fin,!ack
```

RAW forward

```
#[--lixo--]
add action=drop chain=prerouting comment="bad UDP" protocol=udp \
     port=0,135-139,445,5376,10001
add action=drop chain=prerouting comment="bad UDP" protocol=udp src-port=1900 dst-port=1900
add action=drop chain=prerouting comment="bad TCP" port=0,135-139,445,25 protocol=tcp
add action=drop chain=prerouting comment="bad TCP" protocol=tcp \
     tcp-flags=!fin,!syn,!rst,!ack
add action=drop chain=prerouting comment="bad TCP" protocol=tcp tcp-flags=fin,!ack

#[--FW-OFF--]
add action=accept chain=prerouting comment=FIREWALL-OFF src-address-list=FW-OFF
add action=accept chain=prerouting comment=FIREWALL-OFF dst-address-list=FW-OFF
```

RAW forward

```
#[--limites-lan--]
add action=drop chain=prerouting comment=LAN-LOW-Ports__ajustar_leonardorosa.com \
     protocol=tcp src-address-list=LAN dst-address-list=!LAN src-port=0-1023 \
     limit=10,5:packet
add action=drop chain=prerouting comment=LAN-LOW-Ports protocol=udp src-address-list=LAN \
     dst-address-list=!LAN src-port=0-1023 dst-port=!0-1023
add action=drop chain=prerouting comment=LAN-HIGH-Ports dst-address-list=LAN \
     dst-port=8080 in-interface-list=WAN protocol=tcp
```

Filter forward

```
/ip firewall filter

add action=accept chain=input comment=DESLIGA--FILTER_input disabled=yes
add action=accept chain=forward comment=DESLIGA--FILTER_forward disabled=yes

add action=fasttrack-connection chain=forward comment=fastTrack \
     connection-state=established,related
add action=accept chain=forward comment=Estabelecidas/etc \
     connection-state=established,related,untracked

#[--lan-services--]
add action=accept chain=forward dst-address-list=LAN-services src-address-list=LAN
add action=accept chain=forward dst-address-list=LAN src-address-list=LAN-services
```

Filter forward

```
add action=drop chain=forward src-address-list=BOGONS out-interface-list=WAN comment=BOGONS
add action=drop chain=forward dst-address-list=BOGONS out-interface-list=WAN comment=BOGONS
add action=accept chain=forward comment=FIREWALL-OFF dst-address-list=FW-OFF
add action=accept chain=forward comment=FIREWALL-OFF src-address-list=FW-OFF
add action=accept chain=forward comment=LAN src-address-list=LAN
add action=accept chain=forward comment=DNS-server dst-address-list=DNS-server

add action=reject chain=forward connection-state=new src-address-list=!LAN \
     dst-address-list=LAN protocol=tcp reject-with=tcp-reset dst-port=8291 comment=WINBOX
```

Filter forward

```
#[--STATEFULL--]
add action=accept chain=forward comment=ACK__ajustar_leonardorosa.com protocol=tcp \
     dst-limit=100,100,addresses-and-dst-port/1m tcp-flags=ack
add action=jump chain=forward comment=FW-PARCIAL__ajustar_leonardorosa.com \
     connection-state=new dst-address-list=LAN dst-limit=100,5,addresses-and-dst-port/1m \
     jump-target=fw-parcial dst-port=!0-1023 protocol=udp
add action=jump chain=forward comment=FW-PARCIAL__ajustar_leonardorosa.com \
     connection-state=new dst-address-list=LAN dst-limit=100,5,addresses-and-dst-port/1m \
     jump-target=fw-parcial dst-port=!0-1023 protocol=tcp
add action=jump chain=forward comment=FW-PARCIAL__ajustar_leonardorosa.com \
     connection-state=new dst-address-list=LAN dst-limit=100,5,addresses-and-dst-port/1m \
     jump-target=fw-parcial

add chain=fw-parcial comment=FW-PARCIAL action=drop dst-address-list=FW-FULL
add chain=fw-parcial comment=FW-PARCIAL action=accept
add chain=forward comment=FIREWALL-FULL action=drop disabled=yes
```

Filter input

```
add action=accept chain=input comment=estabelecidas/etc \
     connection-state=established,related,untracked
add action=drop chain=input comment=invalidas connection-state=invalid
add action=accept chain=input comment=BGP port=179 protocol=tcp
add action=accept chain=input comment=OSPF  protocol=ospf
add action=accept chain=input src-address-list=LAN comment=LAN
add action=accept chain=input comment=udp-services protocol=udp \
     src-port=53,123,3784-3785,5678,15252
add action=accept chain=input comment=tcp-services protocol=tcp \
     src-port=20-23,53,80,443,587,8291
```

Filter input

```
#[--toc-toc--]
add action=add-src-to-address-list address-list=toc-toc-1 address-list-timeout=15s \
     chain=input comment=toc-toc-1 dst-port=321 protocol=tcp
add action=add-src-to-address-list address-list=toc-toc-2 address-list-timeout=15s \
     chain=input comment=toc-toc-2 dst-port=4321 protocol=tcp src-address-list=toc-toc-1
add action=add-src-to-address-list address-list=LAN address-list-timeout=30m chain=input \
     comment=toc-toc-3 dst-port=54321 protocol=tcp src-address-list=toc-toc-2

add action=log chain=input comment=nega-tudo disabled=yes limit=1/1m,1:packet
add action=drop chain=input comment=nega-tudo disabled=yes
```

BÔNUS

As regras a seguir identificam clientes usando DNS desconhecidos ou não confiáveis e redireciona toda requisição DNS para o próprio router. Com isso estes clientes usarão os servidores configurados em **IP** > **DNS**.

É recurso interessante, totalmente opcional. Para que tenha o efeito desejado, é necessário habilitar a seguinte função:

```
/ip dns set allow-remote-requests=yes
```

NAT (bônus)

```
/ip firewall nat

add action=accept chain=dstnat comment=FW-OFF dst-port=53 protocol=udp \
     src-address-list=FW-OFF place-before=0
add action=accept chain=dstnat comment=FW-OFF dst-port=53 protocol=tcp \
     src-address-list=FW-OFF place-before=0
add action=redirect chain=dstnat comment=DNS-bogus dst-address-list=!DNS-server \
     dst-port=53 protocol=udp src-address-list=bogus-dns place-before=0
add action=redirect chain=dstnat comment=DNS-bogus dst-address-list=!DNS-server \
     dst-port=53 protocol=tcp src-address-list=bogus-dns place-before=0
add action=add-src-to-address-list address-list=bogus-dns address-list-timeout=30m \
     chain=dstnat comment=DNS-bogus dst-address-list=!DNS-server dst-port=53 \
     protocol=udp src-address-list=LAN place-before=0
add action=add-src-to-address-list address-list=bogus-dns address-list-timeout=30m \
     chain=dstnat comment=DNS-bogus dst-address-list=!DNS-server dst-port=53 \
     protocol=tcp src-address-list=LAN place-before=0
```

siga o mestre e saiba mais!

Leonardo Rosa

contato@leonardorosa.com

19 | 3090 3600 | WhatsApp

https://leonardorosa.com

https://www.youtube.com/c/LeonardoRosa

https://www.linkedin.com/in/leonardorosa

BRAUSER

MikroTik TRAINING CENTER