

Configuração de VPN num router Mikrotik



O router que aconselhamos para utilizar nesta configuração (Mikrotik RB750UP) pode ser obtido por menos de 30€ usado, no ebay ou Wallpop. Se não tiver os conhecimentos técnicos para programar o router contacte-nos através do email info@hamnet.pt e nós ajudamos.

hamnet.pt

Depois de ter as credenciais VPN e o seu equipamento limpo de configurações (ver como fazer no guia Ponto de acesso WiFi), aplique a seguinte configuração a partir do Terminal do WinBox.

Copie o bloco de código seguinte para um editor de texto.

```
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface bridge
add name=bridge
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ip dhcp-server
add address-pool=default-dhcp disabled=no interface=bridge name=defconf
/interface bridge port
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
/ip neighbor discovery-settings
set discover-interface-list=LAN
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/ip address
add address=192.168.88.1/24 comment=defconf interface=bridge network=192.168.88.0
/ip dhcp-client
add comment=defconf disabled=no interface=ether1
/ip dhcp-server network
add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
```

```
/ip firewall filter
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-
state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment="defconf: accept to local loopback (for CAPsMAN)" dst-address=127.0.0.1
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" connection-state=established,related
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-
state=established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat
connection-state=new in-interface-list=WAN
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" ipsec-policy=out,none out-interface-
list=WAN
/system clock
set time-zone-name=Europe/Lisbon
/system identity
set name=vpn.<indicativo>
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox
set allowed-interface-list=LAN
E substitua <indicativo> pelo seu indicativo de radioamador
```

Selecione a opção do menu New Terminal e copie o texto de configuração do editor de texto para o terminal e prima ENTER.

Copie selecionando o texto e premindo o botão do rato do lado direito para aceder ao Copy e ao Paste.

Se o router não aceitar a configuração de uma só vez. Escreva o comando export no terminal para ver o que ficou configurado e copie a configuração em falta.

Para finalizar a configuração do router é necessário introduzir alguns comandos no terminal. Aplique esta configuração com a porta 1 do router Mikrotik ligado ao seu router da internet e o computador que está a utilizar para configurar numa das outras portas do Mikrotik.

Primeiro precisamos de obter o certificado do servidor VPN HamCloud.

```
/tool fetch url=https://vpn.hamnet.network/cert/hamcloud-vpn-root-ca.cer
```

E importar o certificado para o RouterOS.

```
/certificate import file-name=hamcloud-vpn-root-ca.cer passphrase=""
```

É necessário criar uma proposta IPsec própria com “pfs-group = none”.

```
/ip ipsec proposal add name=hamcloud-proposal pfs-group=none
```

É necessário adicionar esta proposta IPsec a um grupo de políticas IPsec próprio.

```
/ip ipsec policy group add name=hamcloud-policy-group
```

É necessário adicionar um modelo (template) de política IPsec.

```
/ip ipsec policy add group=hamcloud-policy-group proposal=hamcloud-proposal template=yes
```

É necessário definir o modo de operação.

```
/ip ipsec mode-config add name=hamcloud-mode-config responder=no use-responder-dns=no connection-mark=no-mark
```

É necessário definir o peer IPsec.

```
/ip ipsec peer add address=[.:resolve ikev2.vpn.hamnet.network] exchange-mode=ike2 name=hamcloud-peer
```

É necessário adicionar uma identidade IPsec. Substitua “PASSWORD” e “USERNAME” pelas suas credenciais IKEv2 da HamCloud VPN.

```
/ip ipsec identity add auth-method=eap certificate="" eap-methods=eap-mschapv2 generate-policy=port-strict mode-config=hamcloud-mode-config password=PASSWORD peer=hamcloud-peer policy-template-group=hamcloud-policy-group username=USERNAME
```

O RouterOS irá agora estabelecer uma ligação ao servidor HamCloud VPN:

IPsec							
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys							
Kill Connections							
ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	
ikev2.vpn.hamnet.network	established	192.168.8.34	192.68.17.22	0.0.0.0	initiator	00:01:15	

Ecrã de configuração IPsec

Uma vez que o peer IPsec “ikev2.vpn.hamnet.network” é resolvido apenas uma vez para um IP estático, é necessário executar periodicamente um script para verificar se o endereço IP foi alterado:

Crie o script

```
/system script add name=hamcloud-dns-lookup source="{r\
\n :local newIP ([:resolve ikev2.vpn.hamnet.network] . \"/32\")r\
\n :local oldIP [/ip ipsec peer get [/ip ipsec peer find name=\"hamcloud-peer\"] address]r\
\n :if (\$oldIP != \$newIP) do={ /ip ipsec peer set [/ip ipsec peer find name=\"hamcloud-peer\"] address=\$newIP
}}r\
\n}}r\
\n"
```

E adicione o script ao scheduler.

```
/system scheduler add name=hamcloud-sched interval=10h on-event=hamcloud-dns-lookup
```