Mikrotik Configurations

1. **Speed Queues(CLI)**  
   “:for i from=201 t=250 do={/queue simple add name="Invozone-23-II-$i" max-limit=10M/10M target="192.168.23.$i"}”  
   “:for i from=51 t=250 do={/queue simple add name="Guest-$i" max-limit=5M/5M target="10.10.20.$i"}”  
   :for i from=51 t=255 do={/queue simple add name="vlan20-20.$i" max-limit=10M/10M target="10.10.20.$i"}
2. :for i from=1 t=200 do={/queue simple add name="vlan20-21.$i" max-limit=10M/10M target="10.10.21.$i"}
3. **L2TP/IPSec VPN(GUI)**  
   S1:IP>IPSec>Proposal>default>sha1✔>sha256✔>3des✔>des✔>aes128cbc✔>apply>ok  
   S2:IPSec>profiles>default>3des✔>aes128✔>modp1024✔>modp2048✘>apply>Ok  
   S3:IP>pool>+>Name:”VPN”>Addresses”192.168.1.98/27”(local ip range network for vpn clients)>apply>ok  
   S4:PPP>profiles>+>Name:”l2tp-vpn”>Local-Address:”192.168.1.1(LAN Gateway)”>Remote-Address:”VPN-poo”(lan IP range for vpn clients)>DNS-Server:”8.8.8.8”>Limit>session-Timeout:”10.00.00”>idle-timeout:”id 00:00:00”>apply>ok.  
   S5:PPP>Interface>L2TP-server>Enable✔>>Default-profile:’l2tp-vpn’>chap✔>mschap1✔>mschap2✔>pap✔>use-IPsec:’Yes’>ipsec-Secret:”password”(pre-shared-key)>apply>ok  
   S5:PPP>scret>+>Name:”user-name”>Password:”user-pass”>service:’l2tp’>profile:’L2tp-vpn’>apply>ok.  
   S6:Add and dail vpn from client.
4. **Get configuration commands (CLI)**  
   S1:[admin@Microtik] > export file=config.txt  
   S2:drag and drop from ‘Files’>open in notepad.
5. Auto-Backup

/tools email  
server: 74.125.141.108, port: 587, Start TLS:yes, VRF: main, From: “email” , User: “Email” Passwd:

/system scheduler  
+, Name: AutoBackup, date, time, Interval, Owner: admin, Policy: all yes except dude, ON.Event: “/system backup save name=RouterIdentity.backup”  
+, Name:AutoMail, date, time, Interval, owner, policy, On.Event:” /tool e-mail send to=from-email/aqib.shahzad@gamil.com subject=([/system identity get name] . "backup") file=Router-identity.backup”

1. Load Balancing GUI process

Ether1=WAN1,IP add=192.168.20.0/24

Ether2=WAN2, IP add=192.168.2.0/24

/IP firewall nat

+ >genera:chain='input', int-interface='ehter1' >Action:Action=mark-connection ,new-routing-mark="WAN1-Connection"

+ >genera:chain='input', int-interface='ehter2' >Action:Action=mark-connection ,new-routing-mark="WAN2-Connection"

+ >general:chain='output', connection-mark='WAN1-Connection' >Action:Action='mark-routing', New-routing-mark="To-WAN1"

+ >general:chain='output', connection-mark='WAN2-Connection' >Action:Action='mark-routing', New-routing-mark="To-WAN2"

+ >general:chain='prerouting', Dst.-add="192.168.20.0/24", In.Interface='LAN-Bridge/LAN' >Action:Action='accept'

+ >general:chain='prerouting', Dst.-add="192.168.2.0/24", In.Interface='LAN-Bridge/LAN' >Action:Action='accept'

+ >general:chain='prerouting', In.Interface='LAN-Bridge/LAN' >Advanced:per-connection-classifier='both-address-and-ports'2(no of wans)/0 >Extra:Dst.Address-Tyes:address-type='local',invert=yes >Action:Action='mark-connection', New-Connection-mark='WAN1-Connection', passthrough=yes

+ >general:chain='prerouting', In.Interface='LAN-Bridge/LAN' >Advanced:per-connection-classifier='both-address-and-ports'2(no of wans)/1(previous.No+1) >Extra:Dst.Address-Tyes:address-type='local',invert=yes >Action:Action='mark-connection', New-Connection-mark='WAN2-Connection', passthrough=yes

+ >general:chain='prerouting', In.Interface='LAN-Bridge/LAN', connection-mark='WAN1-connection' >Action:Action='mark-routing', New-routing-mark='To-WAN1'

+ >general:chain='prerouting', In.Interface='LAN-Bridge/LAN', connection-mark='WAN2-connection' >Action:Action='mark-routing', New-routing-mark='To-WAN2'

/ip routes

+ >general:Gatway="192.168.20.1", Routing-mark=To-WAN1

+ >general:Gatway="192.168.2.1", Routing-mark=To-WAN2