BLOCKING WEBSITES & APPLICATIONS

Mikrotik Router

2025

SUBASH SUBEDI

1. Basic Network & Bridge Mode Setup

Create a Bridge for Your LAN

```
# Create a new bridge (adjust the name if desired)
 /interface bridge add name=bridge1


# Add your LAN ports to the bridge (here using 'ether2'; add additional ports as needed)
 /interface bridge port add bridge=bridge1 interface=ether2
/interface bridge port add bridge=bridge1 interface=ether3
/interface bridge port add bridge=bridge1 interface=ether4
/interface bridge port add bridge=bridge1 interface=ether5


# Assign your LAN IP (192.168.1.1/24) to the bridge
 /ip address add address=192.168.2.1/24 interface=bridge1
```

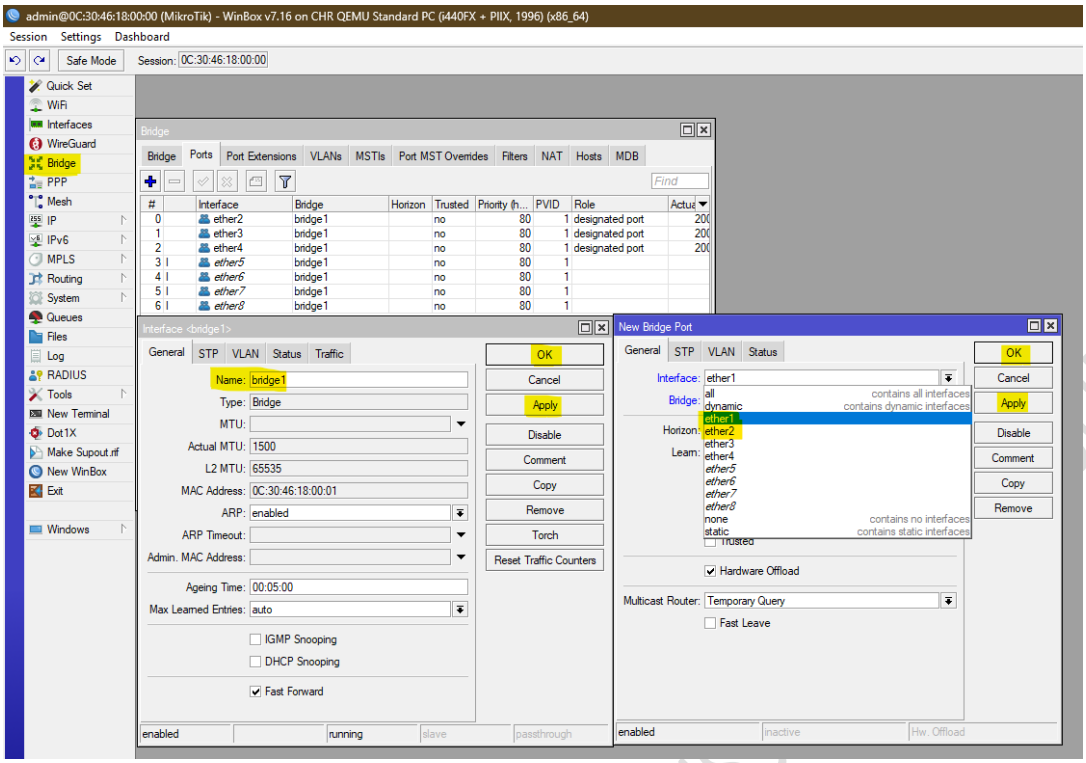

Figure 1

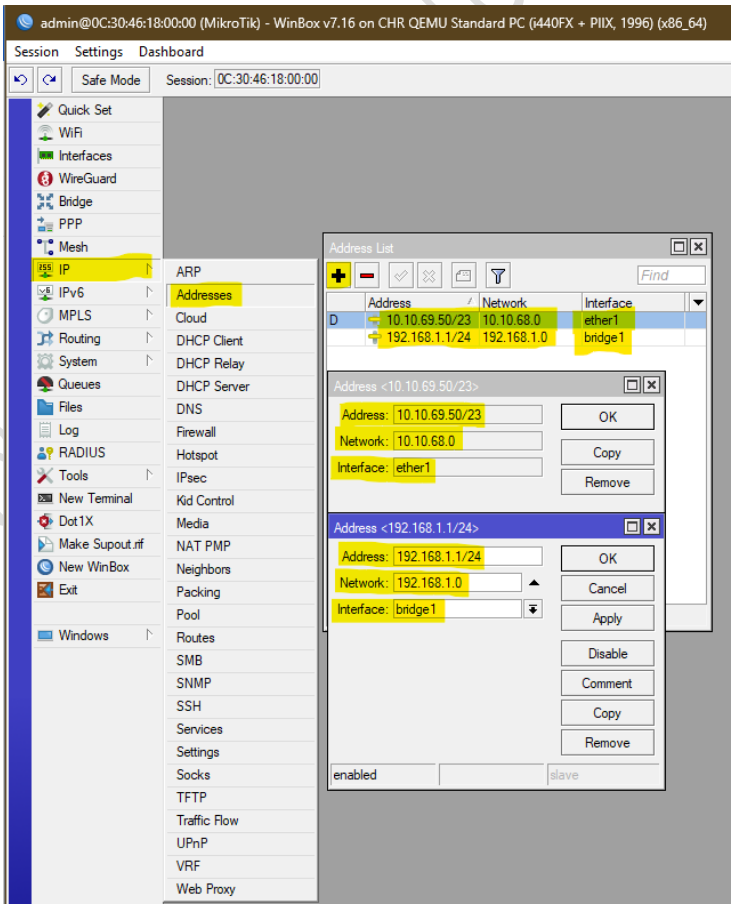

Figure 2

Configure the WAN Interface

```
# Assign your public IP (10.10.69.19/23) to the WAN port (assumed to be 'ether1')

 /ip address add address=10.10.69.19/23 interface=ether1


# Set the default gateway (replace 10.10.69.1 with your ISP's gateway if different)

 /ip route add gateway=10.10.69.1


# Set DNS servers and allow remote DNS requests

/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
```

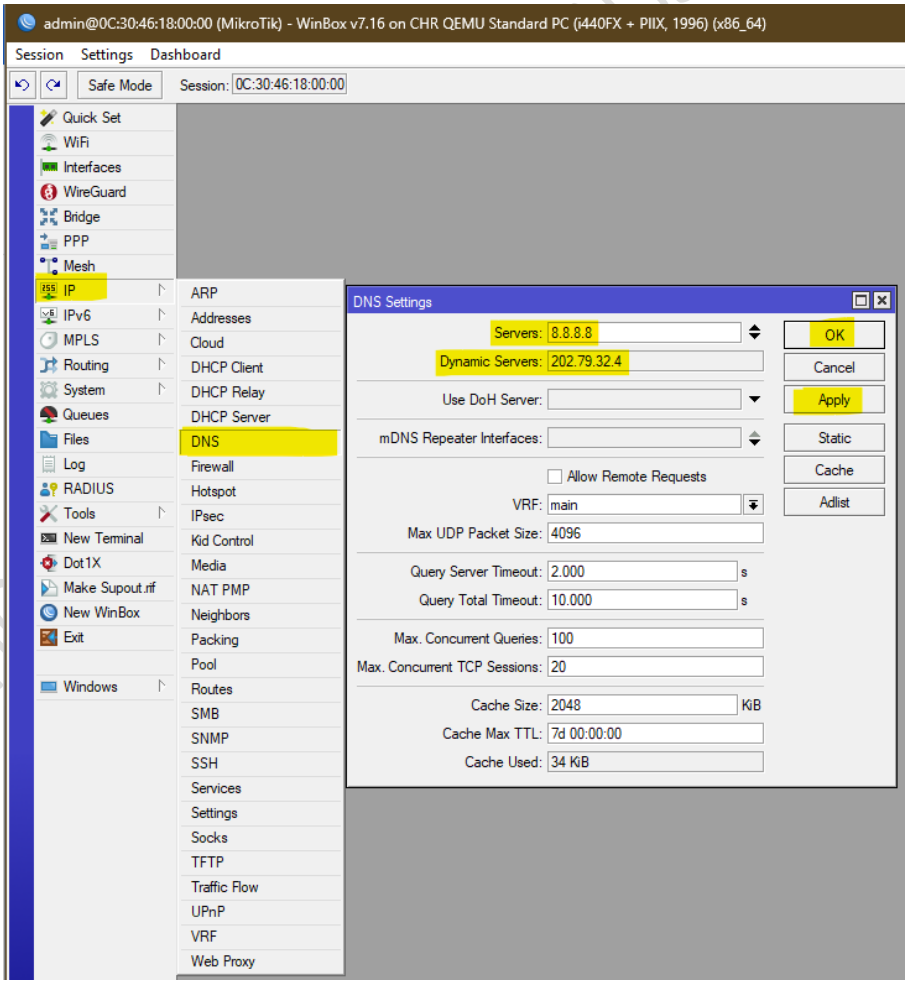

Figure 3

Enable NAT (Masquerade) for Internet Access

```
# NAT rule to masquerade LAN traffic exiting via the WAN interface

/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

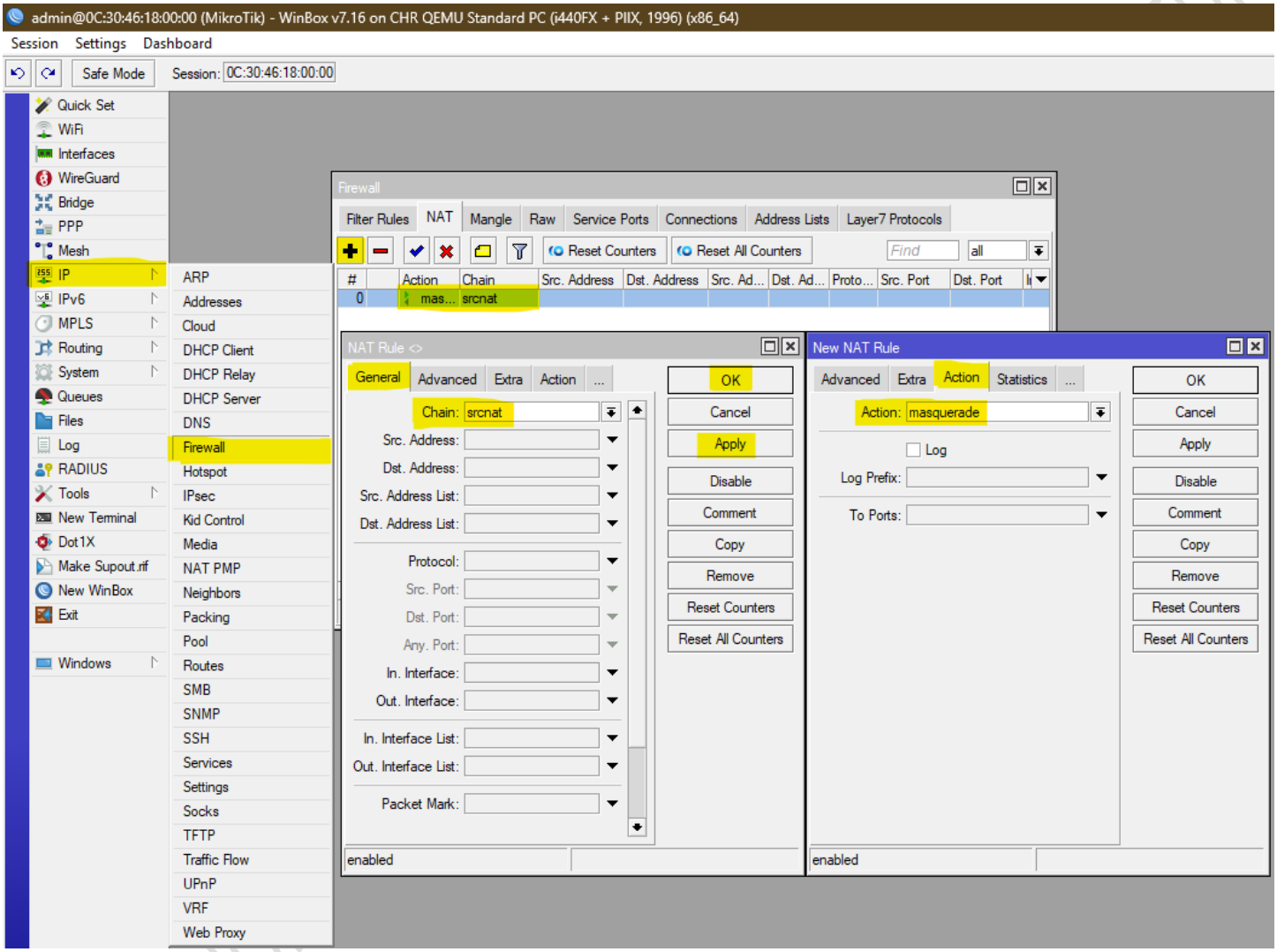

Figure 4

Create a DHCP address pool

 # Create a DHCP address pool for your LAN

/ip pool add name=dhcp_pool1 ranges=192.168.1.2-192.168.1.254

 # Add the DHCP server on the bridge interface (bridge1)

Make sure the interface matches your bridge interface name

/ip dhcp-server add name=dhcp1 interface=bridge1 address-pool=dhcp_pool1 disabled=no

 # Configure the DHCP network settings: specify the LAN network, gateway, and DNS servers

/ip dhcp-server network add address=192.168.2.0/24 gateway=192.168.1.1 dns-server=8.8.8.8,1.1.1.1

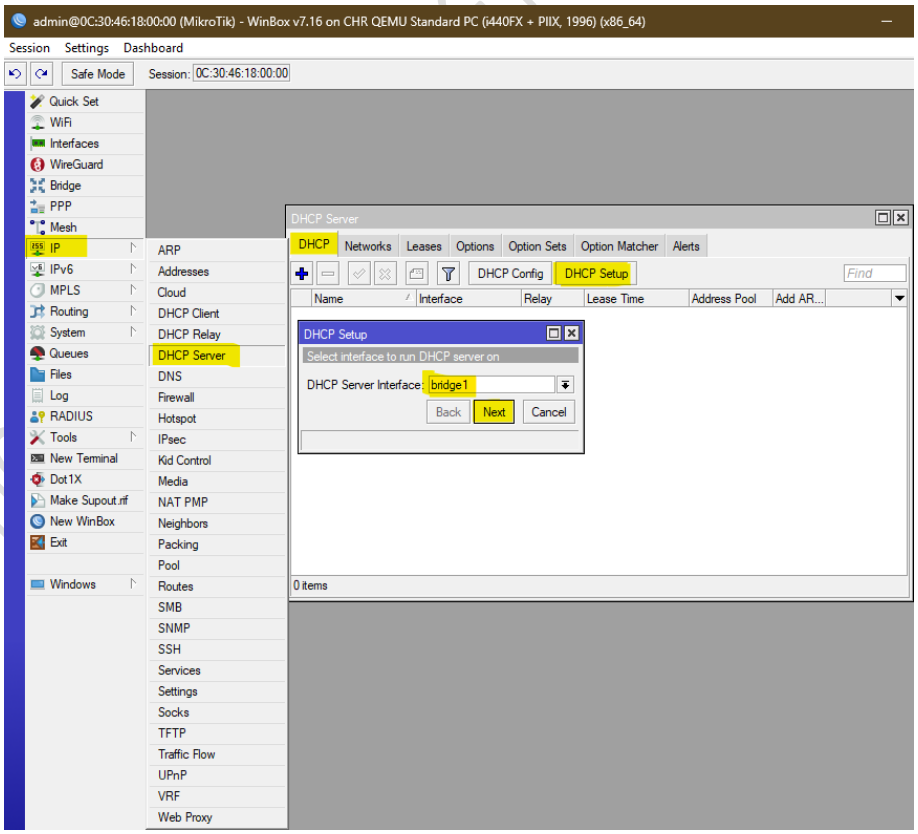

Figure 5

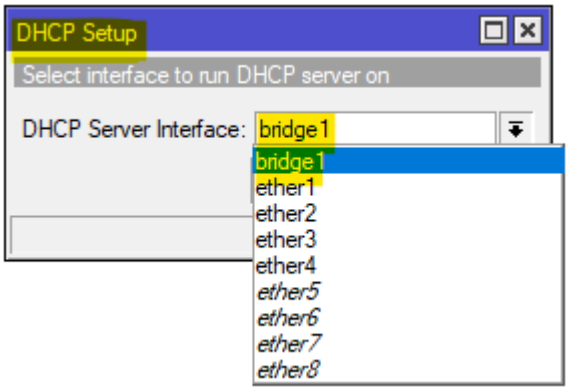

Figure 6

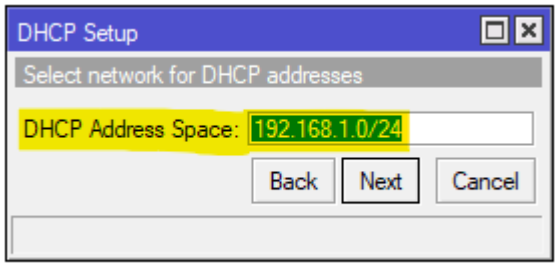

Figure 7

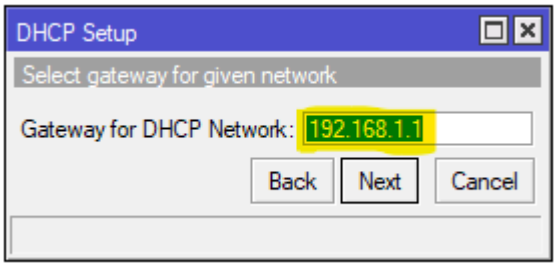

Figure 8

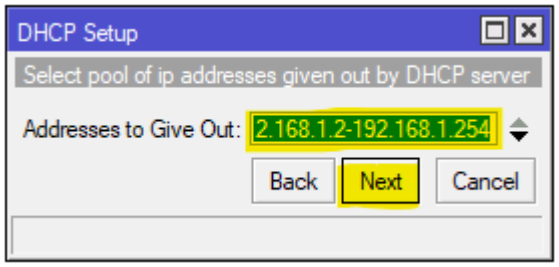

Figure 9

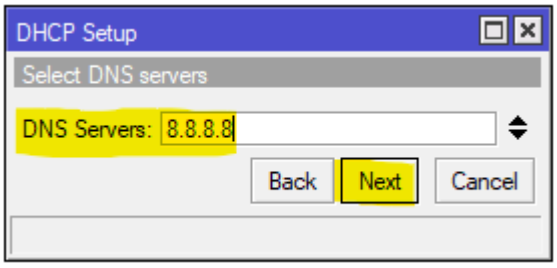

Figure 10

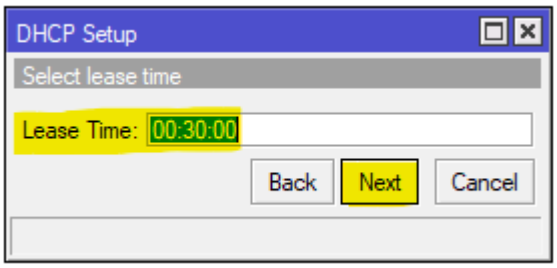

Figure 11

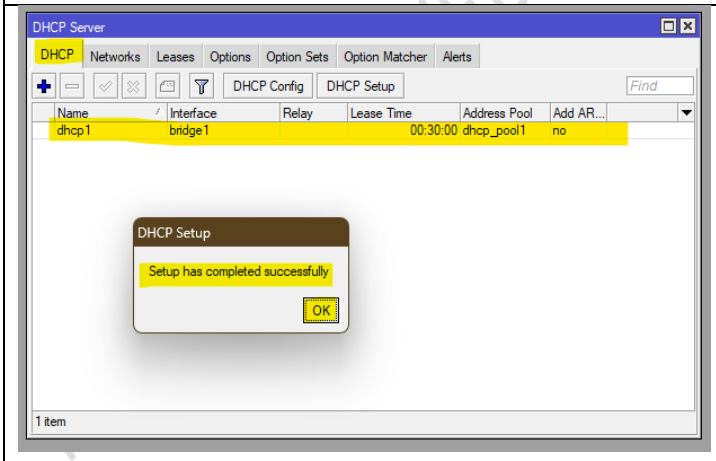

Figure 12

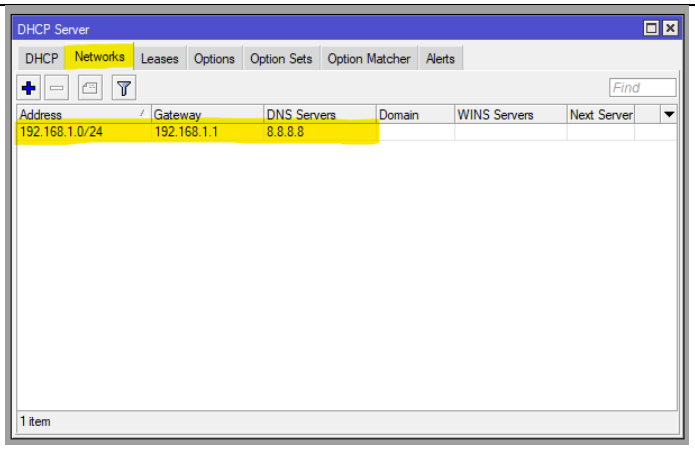

Figure 13

2. Web Filtering & Application Blocking

Let's assume you want to **block**:

TIKTOK

Step 1: Create Layer7 Protocol for TikTok

```
/ip firewall layer7-protocol add name=tiktok regexp="(tiktok\\.com|tiktokcdn\\.com|tiktokv\\.com|musical\\.ly|snssdk123\\.com|.*\\.ttfdata\\.com|.*\\.tiktok\\.akamaized\\.net|.*\\.tiktok\\.cdn\\.cloudflare\\.net)" comment="Block TIKTOK layer 7"
```

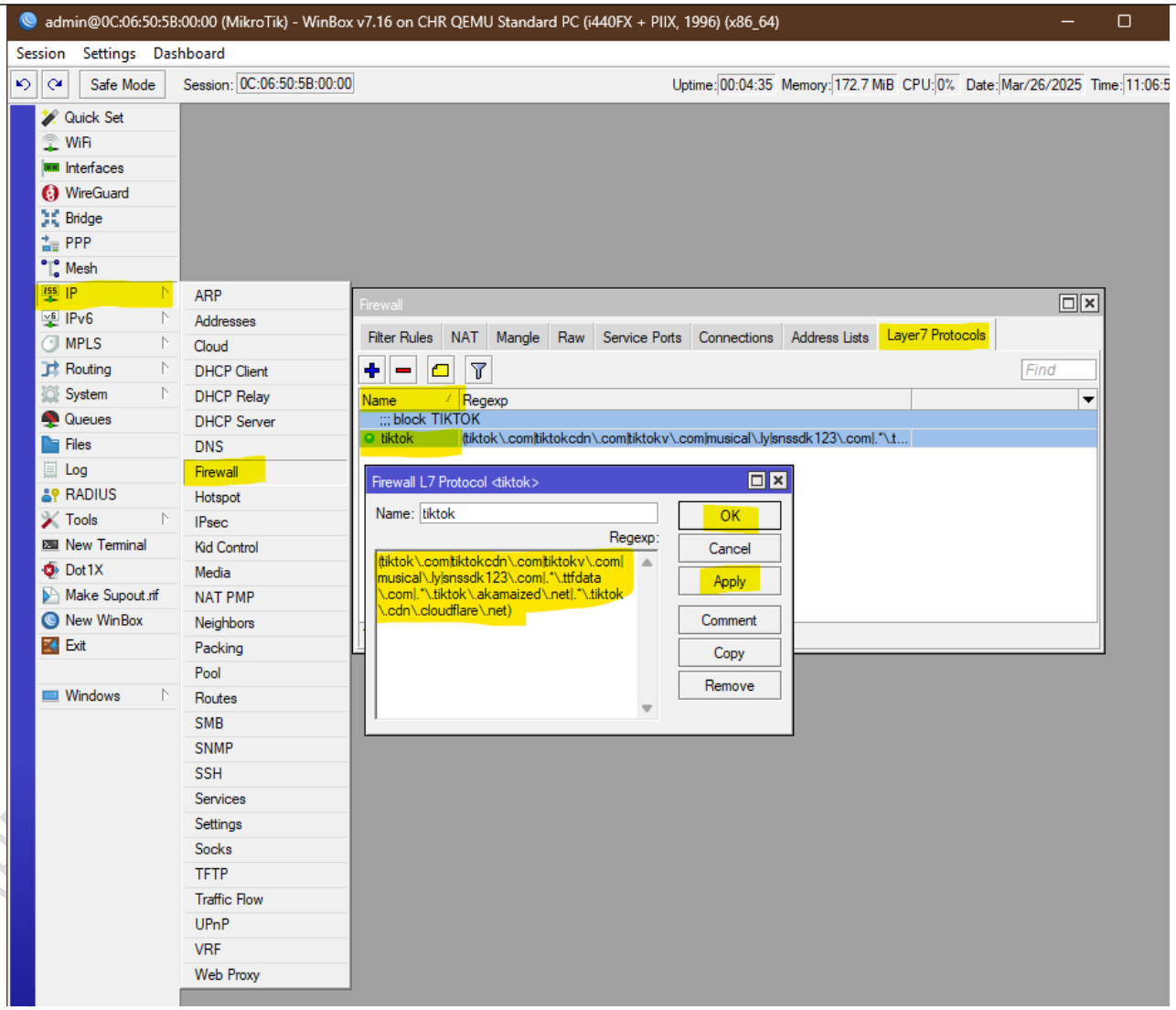

Figure 14

Step 2: Block TikTok Traffic

```
/ip firewall filter

# Block TikTok via Layer7

add chain=forward layer7-protocol=tiktok action=drop comment="Block TikTok Traffic (Layer7)"



# Block IPv6 TikTok traffic (if applicable)

add chain=forward layer7-protocol=tiktok action=drop comment="Block TikTok IPv6" ipv6=yes

/
```

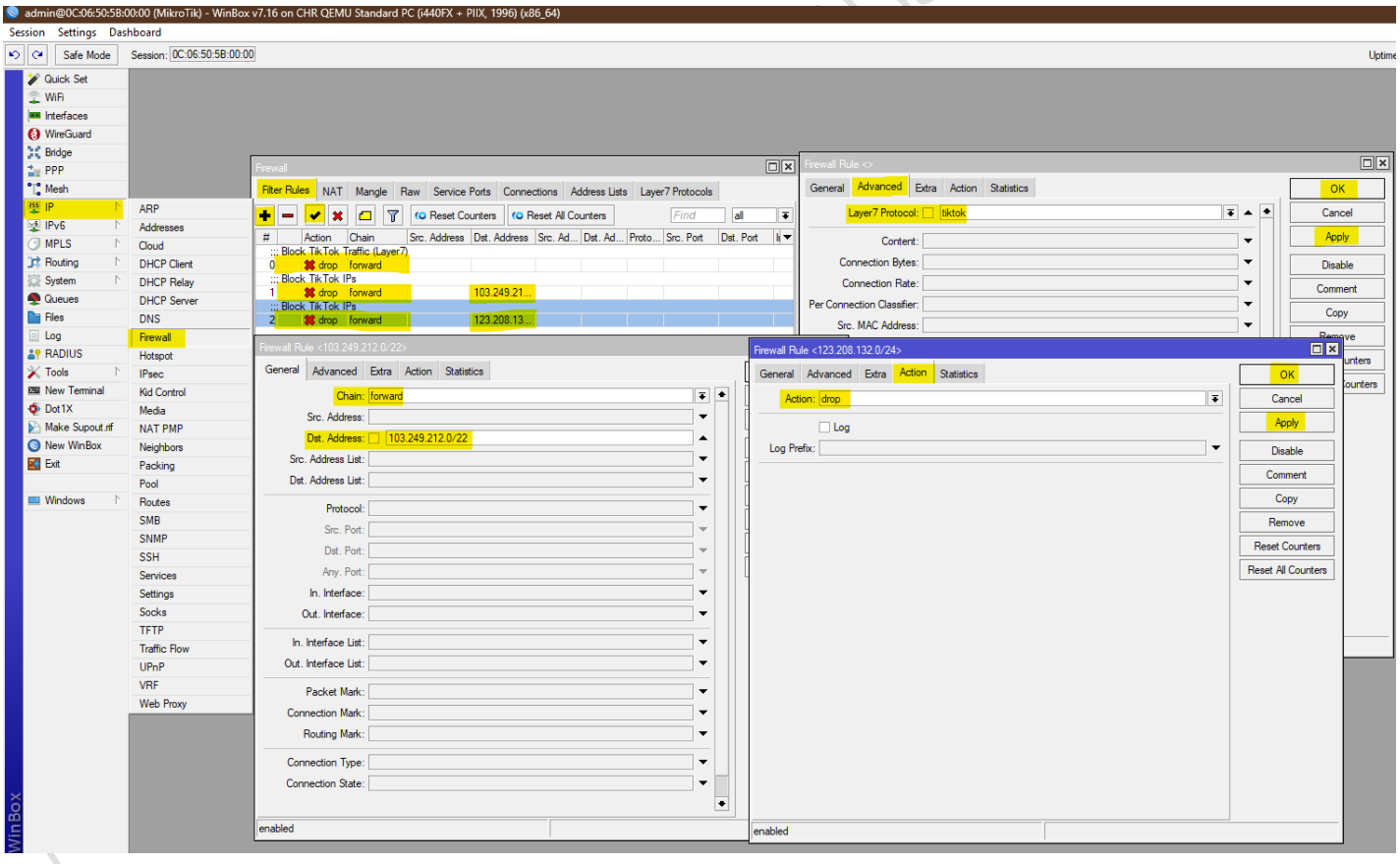

Figure 15

Block Known TikTok IP Ranges

```
/ip firewall address-list add list=Blocked_TikTok address=123.123.123.0/24 comment="TikTok IP Range 1"

/ip firewall address-list add list=Blocked_TikTok address=234.234.234.0/24 comment="TikTok IP Range 2"

/ip firewall filter add chain=forward dst-address-list=Blocked_TikTok action=drop comment="Drop TikTok Traffic"
```

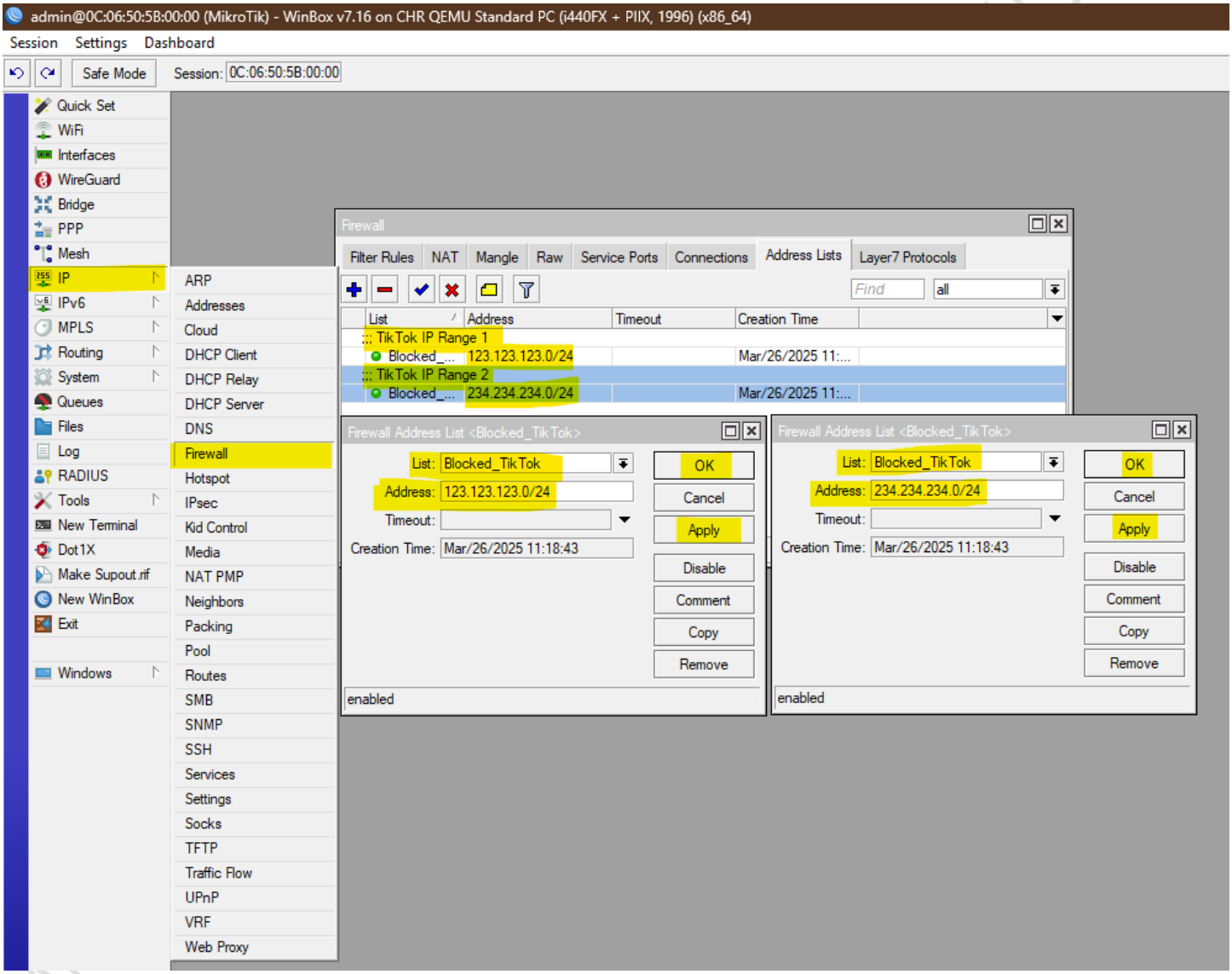

Figure 16

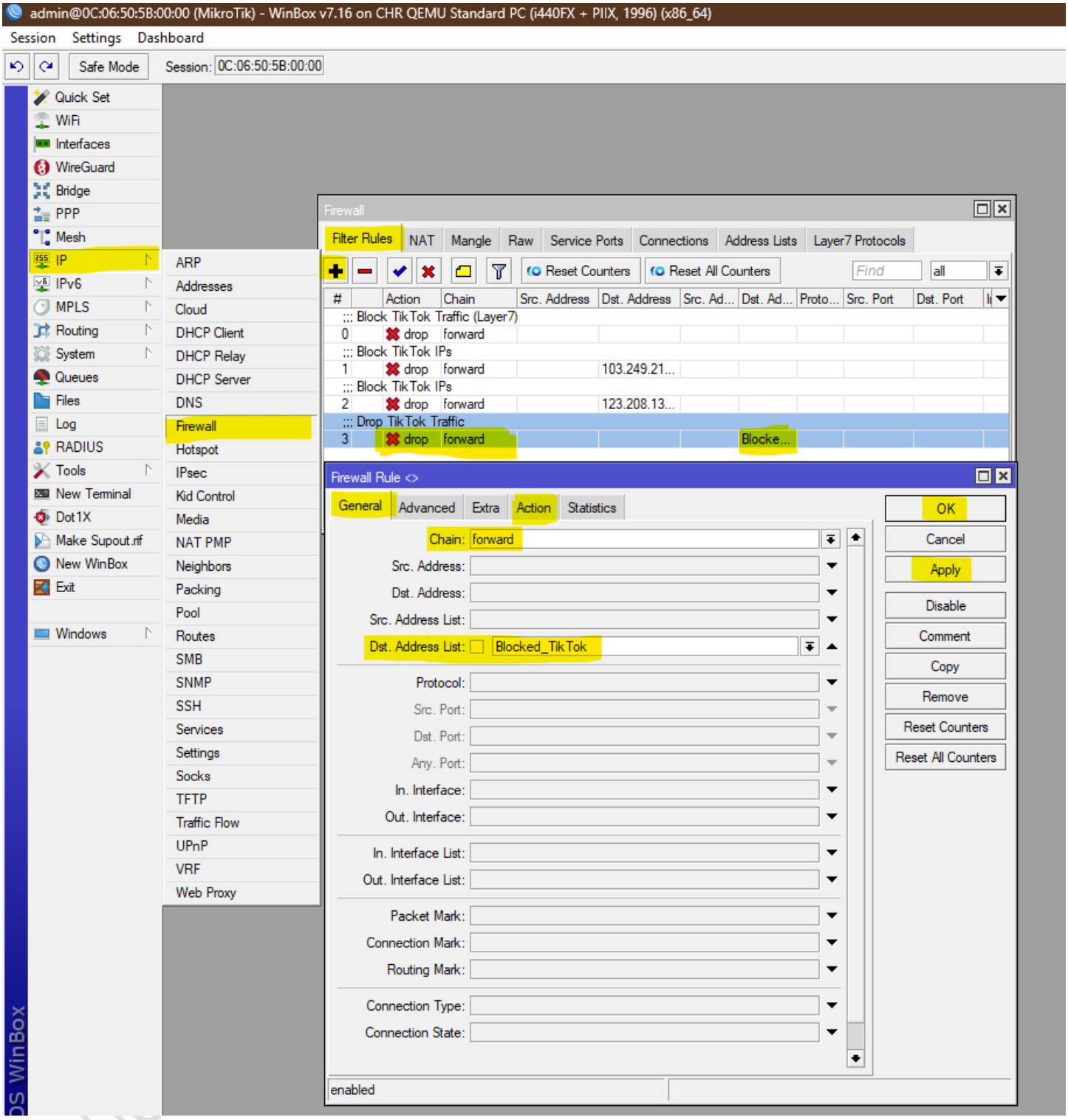
admin@0C:06:50:5B:00:00 (MikroTik) - WinBox v7.16 on CHR QEMU Standard PC (i440FX + PIIX, 1996) (x86_64)
Session Settings Dashboard
Safe Mode
Session: 0C:06:50:5B:00:00
Quick Set
WiFi
Interfaces
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Make Supout.rif
New WinBox
Exit
Windows
ARP
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Media
NAT PMP
Neighbors
Packing
Pool
Routes
SMB
SNMP
SSH
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
VRF
Web Proxy
Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Src. Ad... Dst. Ad... Proto... Src. Port Dst. Port
;;; Block TikTok Traffic (Layer7)
0 drop forward
;;; Block TikTok IPs
1 drop forward 103.249.21...
;;; Block TikTok IPs
2 drop forward 123.208.13...
;;; Drop TikTok Traffic
3 drop forward Blocke...
Firewall Rule <>
General
Advanced
Extra
Action
Statistics
Chain: forward
Src. Address:
Dst. Address:
Src. Address List:
Dst. Address List: Blocked_TikTok
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Connection Type:
Connection State:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled

Figure 17

Step 3: DNS Filtering (Force DNS & Static Entries)

Force DNS requests to the router:

"NOTE: If you used this cmd dns problem will come so be carefull"

```
# Redirect all DNS requests to router

/ip firewall nat

add chain=dstnat protocol=udp dst-port=53 action=dst-nat to-addresses=192.168.2.1 to-ports=53 comment="Force DNS to Router (UDP)"

add chain=dstnat protocol=tcp dst-port=53 action=dst-nat to-addresses=192.168.2.1 to-ports=53 comment="Force DNS to Router (TCP)"

/
```

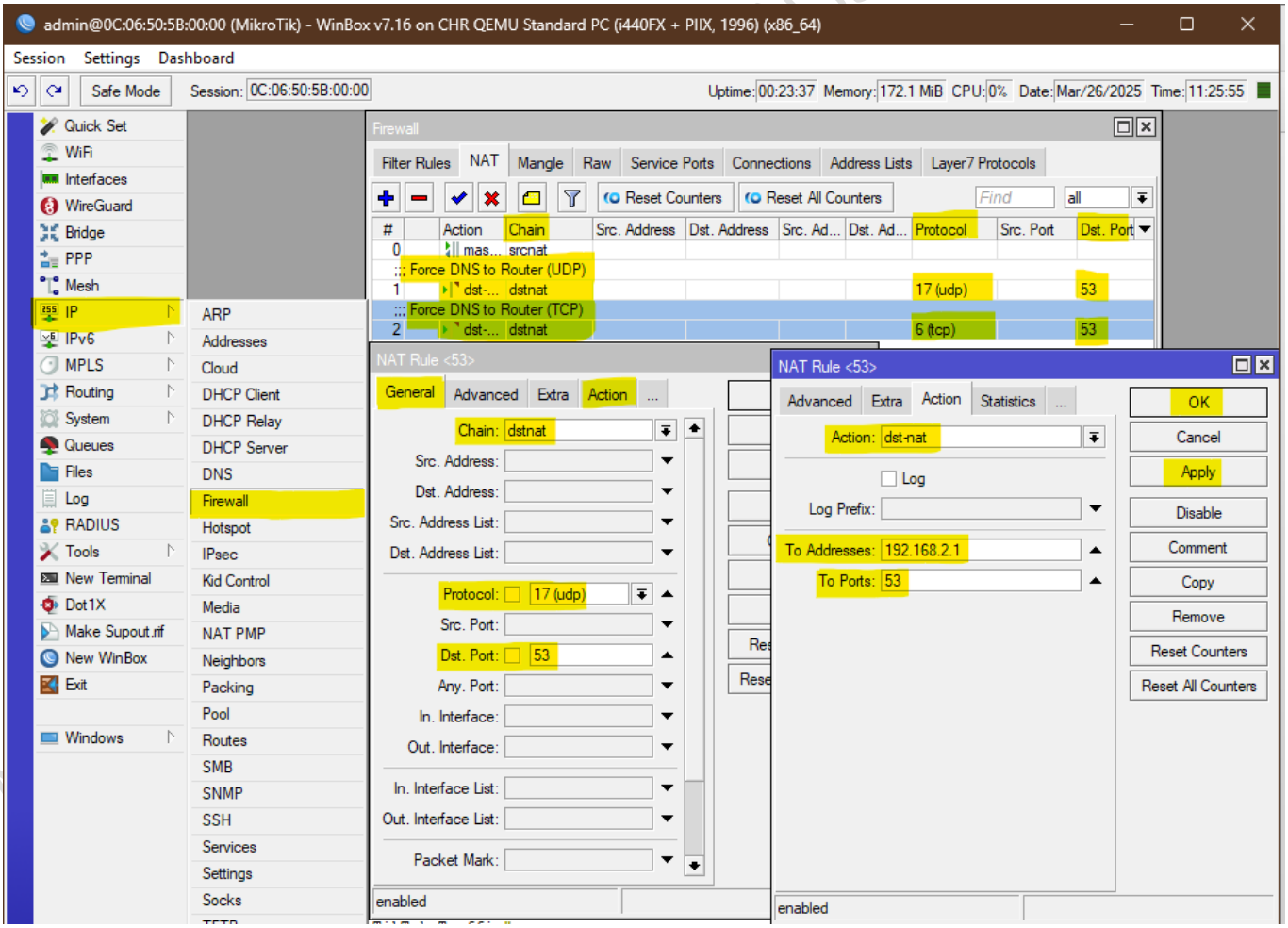

Figure 18

Adjust Firewall Rules to Allow DNS Traffic:

```
# Block external DNS bypass

/ip firewall filter

add chain=forward protocol=udp dst-port=53 action=drop comment="Block External DNS (UDP)"

add chain=forward protocol=tcp dst-port=53 action=drop comment="Block External DNS (TCP)"

/
```

IMP: Flush the DNS Cache:

```
/ip dns cache flush
```

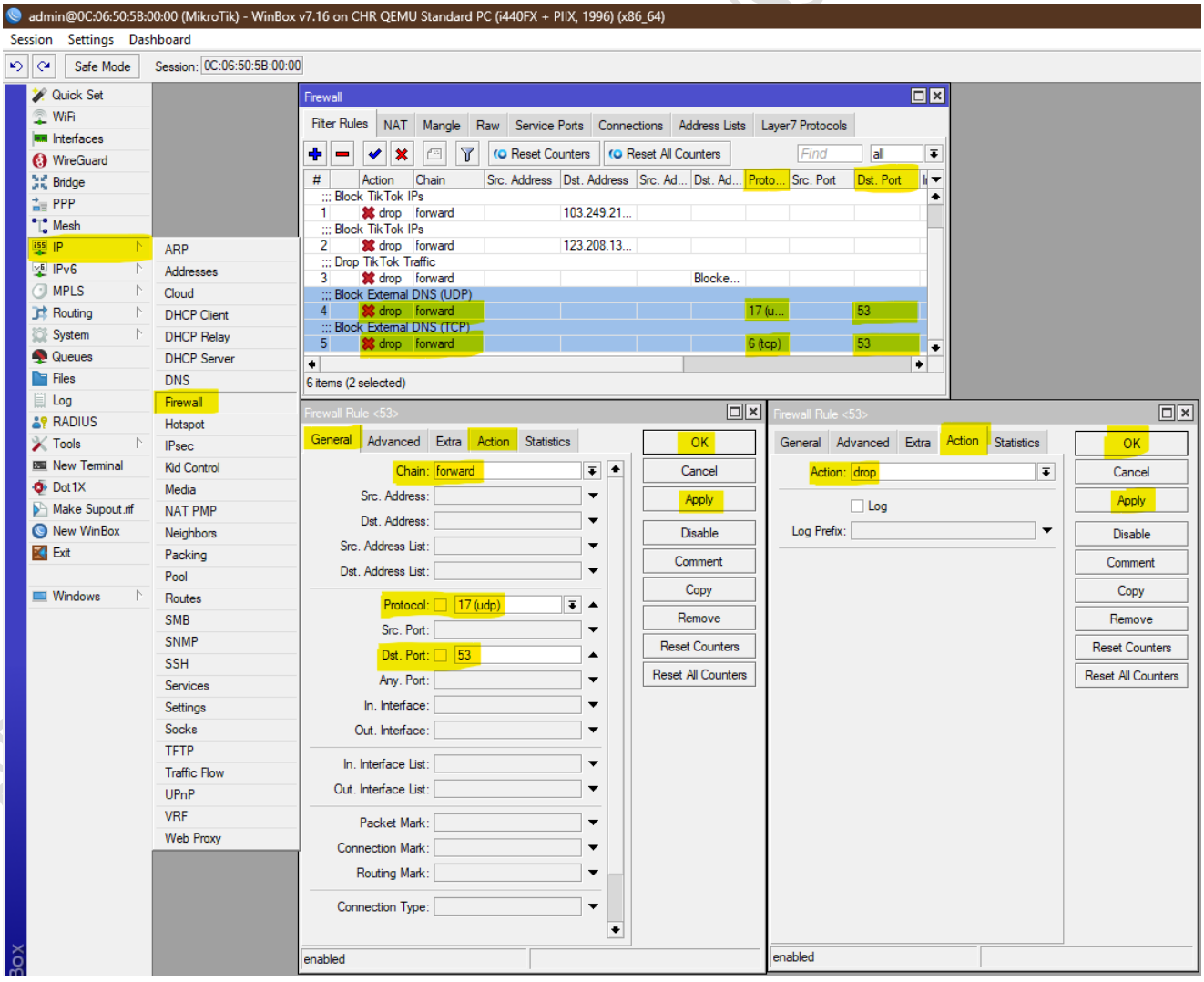

Figure 19

Step 4: Poison TikTok DNS Responses

Create static DNS entries for TikTok domains:

```
# DNS will resolve blocked TikTok domains to 127.0.0.1

/ip dns static add name="tiktok.com" address=127.0.0.1

/ip dns static add name="tiktokcdn.com" address=127.0.0.1

/ip dns static add name="tiktokv.com" address=127.0.0.1

/ip dns static add name="musical.ly" address=127.0.0.1

/ip dns static add name="muscdn.com" address=127.0.0.1
```

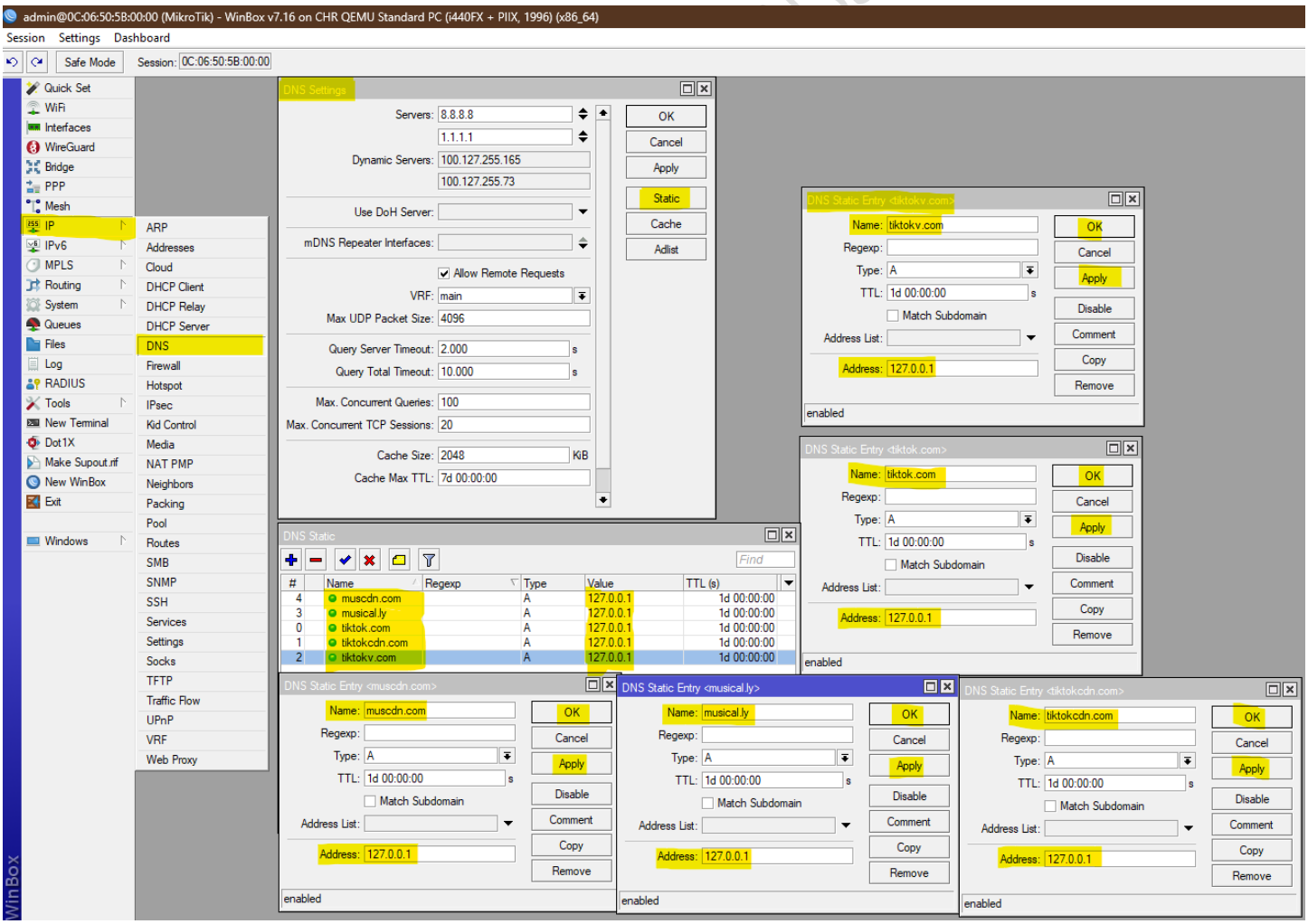

Figure 20

Step 5: Automate IP Blocklist Updates

```
# Fetch TikTok IP ranges daily

/system scheduler

add name="Update TikTok IPs" interval=1d on-event="/tool fetch url=https://raw.githubusercontent.com/example/tiktok-ips/main/list.txt dst-path=tiktok-ips.txt;\

    /import file-name=tiktok-ips.txt"

/
```

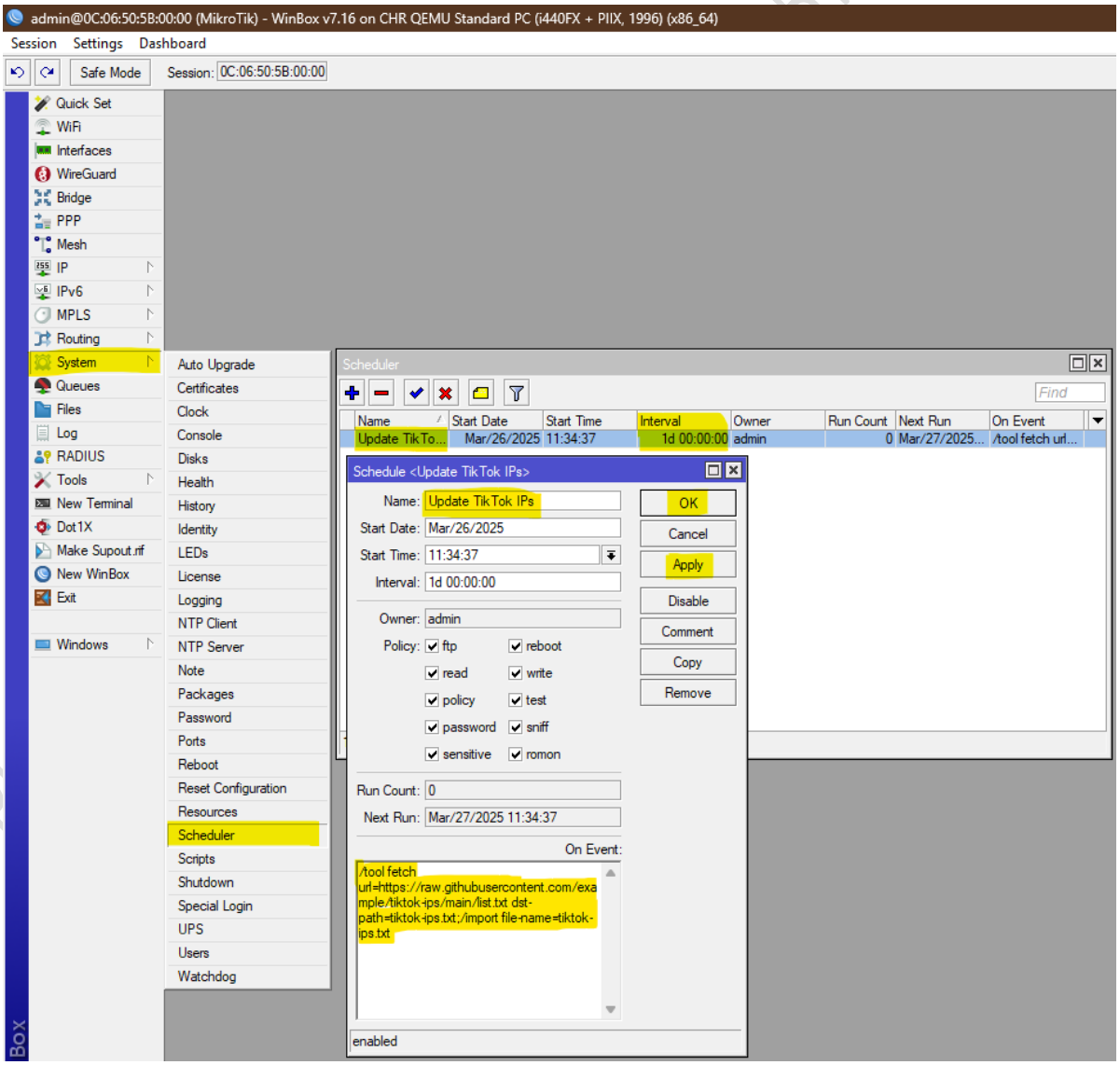

Figure 21

Step 6: Block VPN Protocols

```
/ip firewall filter

# Block UDP port 443 used by QUIC (which may be used by some VPN or proxy services)

add chain=forward protocol=tcp dst-port=443 content="vpn" action=drop comment="Block VPN"


# Block UDP ports commonly used by VPN protocols

/ip firewall filter add chain=forward protocol=udp dst-port=1194 action=drop comment="Block OpenVPN UDP 1194"

/ip firewall filter add chain=forward protocol=udp dst-port=500 action=drop comment="Block IPSec UDP 500"

/ip firewall filter add chain=forward protocol=udp dst-port=4500 action=drop comment="Block IPSec UDP 4500"

/ip firewall filter add chain=forward protocol=tcp dst-port=1723 action=drop comment="Block PPTP TCP 1723"

/ip firewall filter add chain=forward protocol=udp dst-port=1701 action=drop comment="Block L2TP UDP 1701"
```

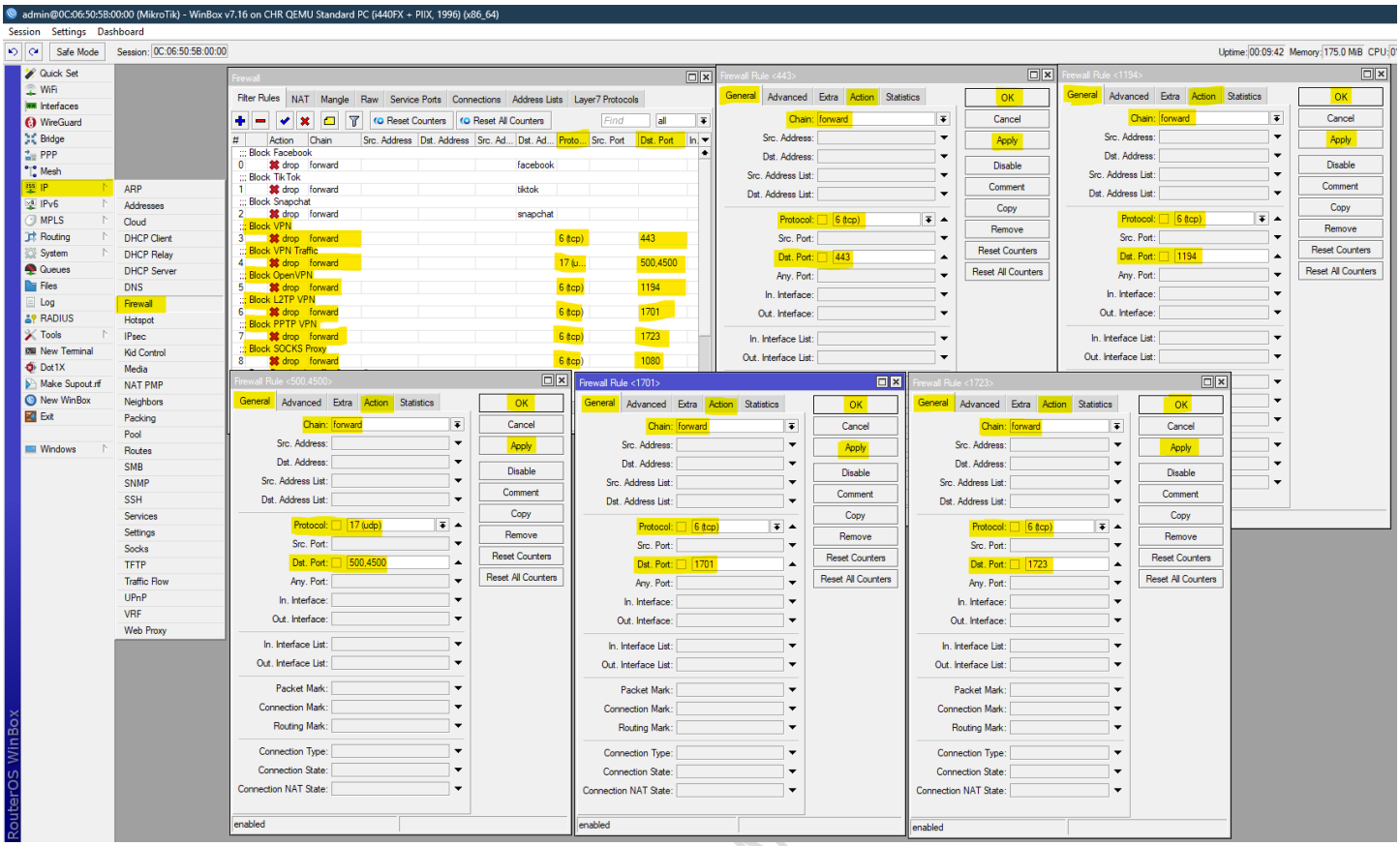

Figure 22