

MikroTik™
MDS 3rd Party Integration

CONTENTS

| | |
|--------------------------------|----|
| Introduction | 3 |
| Assumptions | 3 |
| What You Will Need | 4 |
| Create a Firewall Address List | 6 |
| Create Firewall Rules | 7 |
| Create the GRE Tunnel | 11 |
| Create the Tunnel Address | 12 |
| Add Default Route | 13 |
| Review IP Routes | 16 |
| Verify Traffic | 17 |
| Appendix | 18 |

INTRODUCTION

Congratulations on your sale of MyDigitalShield, using the option to configure existing device(s) to use tunneling protocol.

This guide is written specifically for the **Mikrotik RouterBOARD™ 750Gr2**. It can be used as a reference guide to configure the GRE tunnel, which will provide the connection to the MDS cloud.

This guide documents configuration of the MikroTik gateway using Winbox, which is a Microsoft Windows utility. You use Winbox to access the MikroTik gateway via IP address, or via mac-address of the gateway if you are on the local LAN segment. While there are other configuration options such as http and ssh (CLI), this document will not discuss those options.

ASSUMPTIONS

- This guide covers the configuration of the MikroTik gateway specifically for the setup of the GRE tunnel to the MDS cloud.
- MyDigitalShield certified the MikroTik gateway running RouterOS™ V6.28.
- In no way is this guide intended to be a full configuration guide for the gateway in general.
- Responsibility of the management of the gateway is not assumed by MyDigitalShield.
- The user of this guide has working knowledge of the MikroTik gateway.

WHAT YOU WILL NEED

1. A Winbox machine that can access the Mikrotik device you are configuring.
2. The following IP address information:
 - The local public IP address/subnet.
 - The local public IP GW address (your customer's default gateway address).
 - Local LAN network/subnet.
 - The MDS Cloud IP address assigned to you.
 - GRE Tunnel Network.

In general, the term "Local" refers to a configuration or IP address at your customer's site. "Cloud" refers to the MyDigitalShield node.

1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides.
2. **Local Public GW:** The gateway IP address provided by the customer's ISP.
3. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
4. **Cloud Public IP:** This is the address assigned to you by MyDigitalShield. It is the remote IP address at the MDS Node that the GRE tunnel will terminate on.
5. **GRE Tunnel Network:** This is the network that the GRE tunnel will communicate over. It is provided to you on the MDS portal when you order the service.
6. **Local GRE Tunnel IP:** This is the IP address of the Local side of the GRE tunnel.
7. **Cloud GRE Tunnel IP:** This is the IP address of the Cloud side of the GRE tunnel.

The following screen shot shows you where to obtain the IP address information on the MDS portal.



Network Setup

STEP 1

STEP 2

GRE Settings

Cloud Public IP: 69.64.177.5

Remote Public IP

104.181.238.177

Cloud Tunnel IP: 172.31.24.1

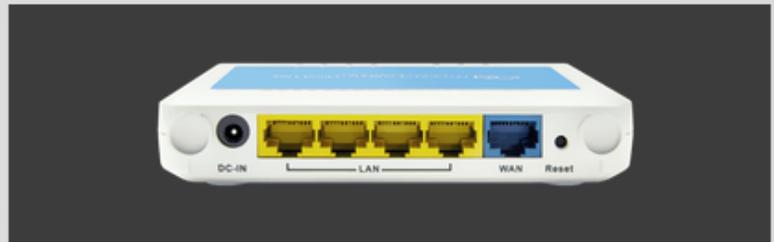
Remote Tunnel IP: 172.31.24.200

Remote LAN IP

192.168.88.1

Remote LAN Mask

255.255.255.0



Security



Firewall / NAT



Intrusion
Prevention (IPS)



Anti-Virus



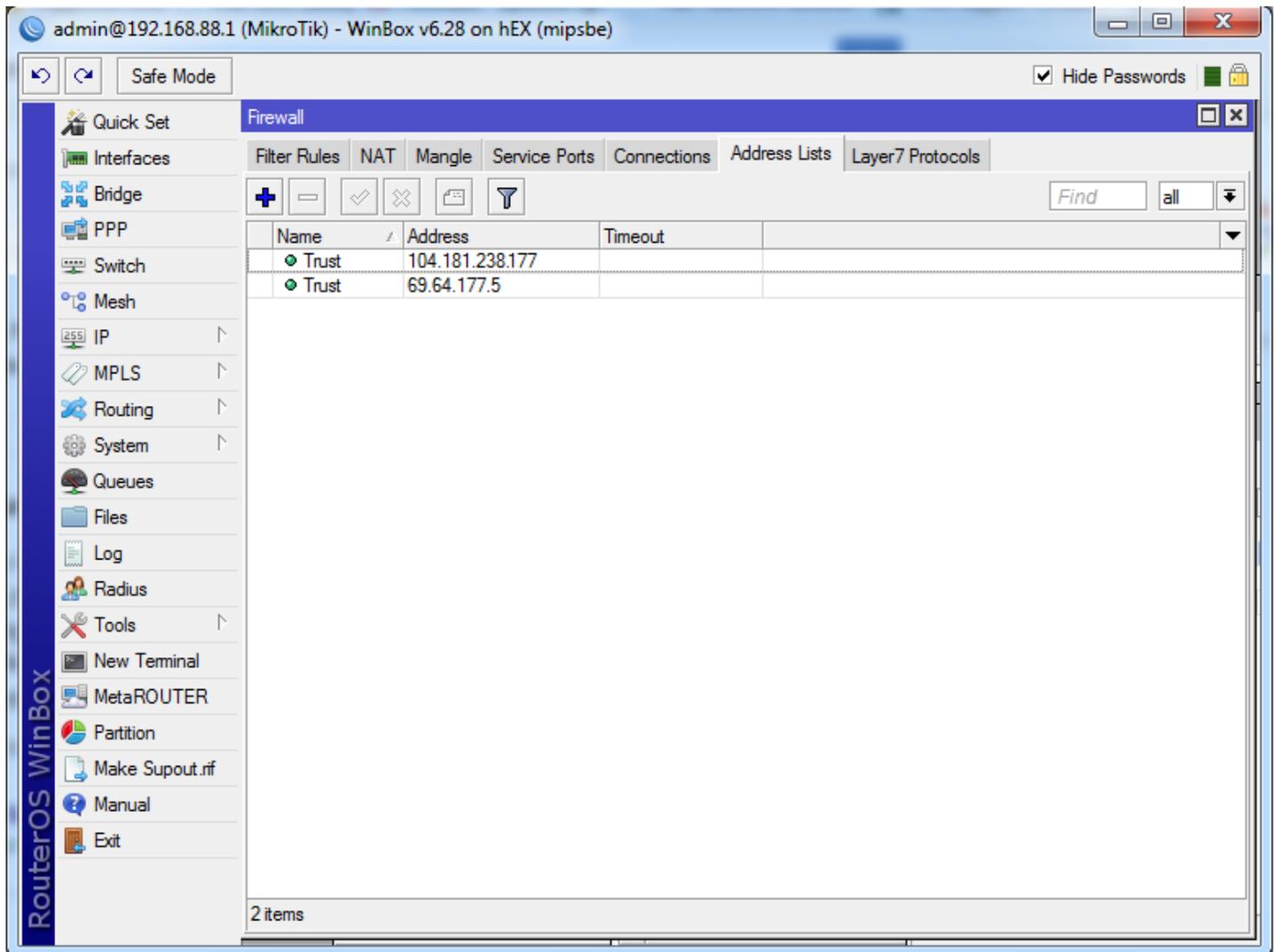
Fill in the middle column of the following table for reference throughout this guide. To map IP addresses throughout this guide, values in the “Reference Sample” column are used.

| Network | IP | Reference Sample |
|---------------------------------------|----|--------------------|
| Local Public IP: (x.x.x.x/ mask) | | 104.181.238.177/22 |
| Local Public GW (x.x.x.x) | | 104.181.236.1 |
| Local LAN Network (x.x.x.x/ mask) | | 192.168.88.0/24 |
| Cloud Public IP (x.x.x.x) | | 69.64.177.5 |
| GRE Tunnel Network (x.x.x.x/ mask) | | 172.31.24.0/24 |
| Local GRE Tunnel IP (x.x.x.x) | | 172.31.24.200 |
| Cloud GRE Tunnel IP (x.x.x.x) | | 172.31.24.1 |

CREATE A FIREWALL ADDRESS LIST

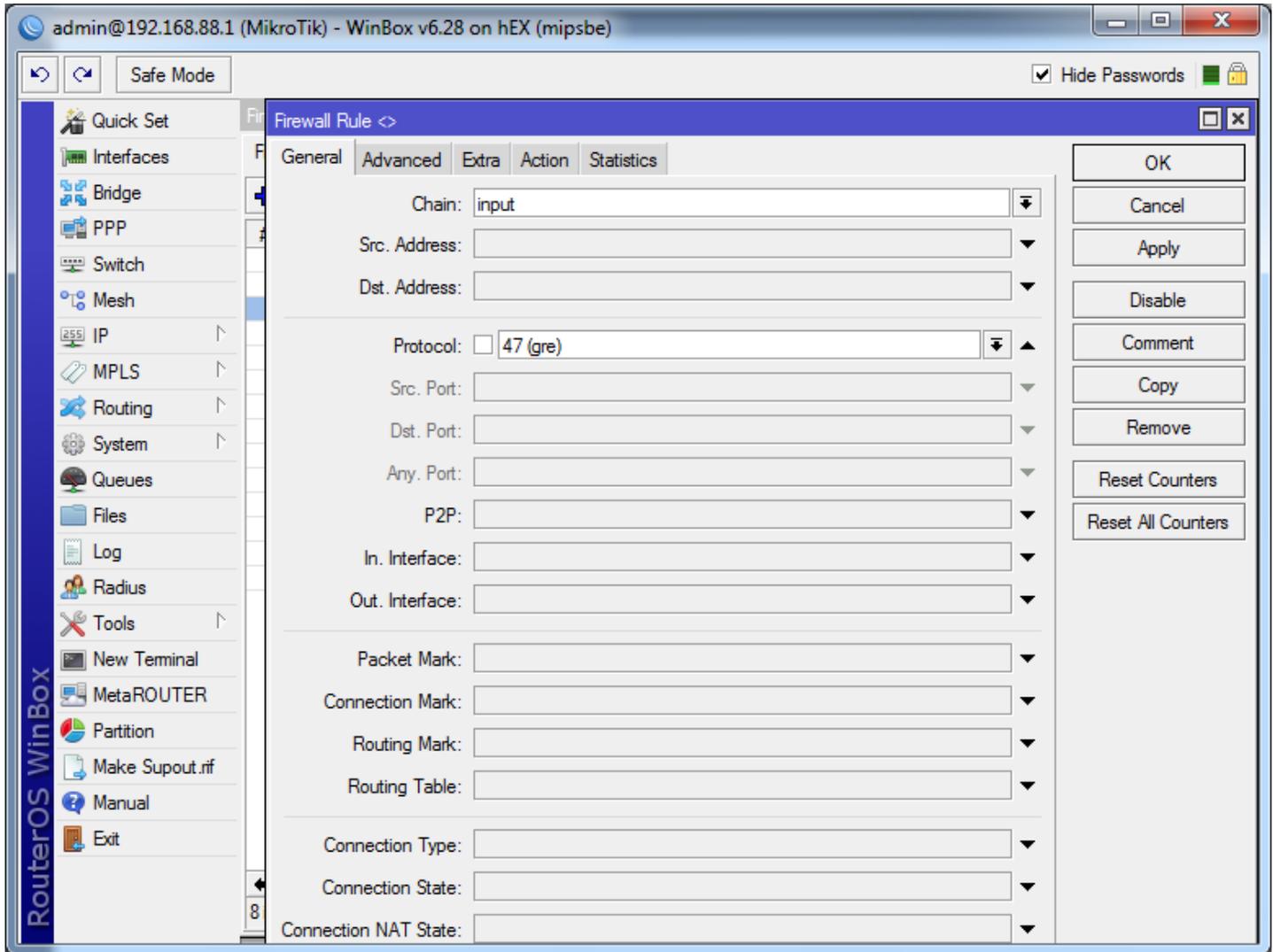
Once you are connected to the MikroTik gateway via Winbox you can follow the instructions on the following pages.

Go to **IP > Firewall** then select **Address Lists**. Click the + sign and add the two public IP's (**Local Public IP** and **Cloud Public IP**). Name both addresses "Trust."

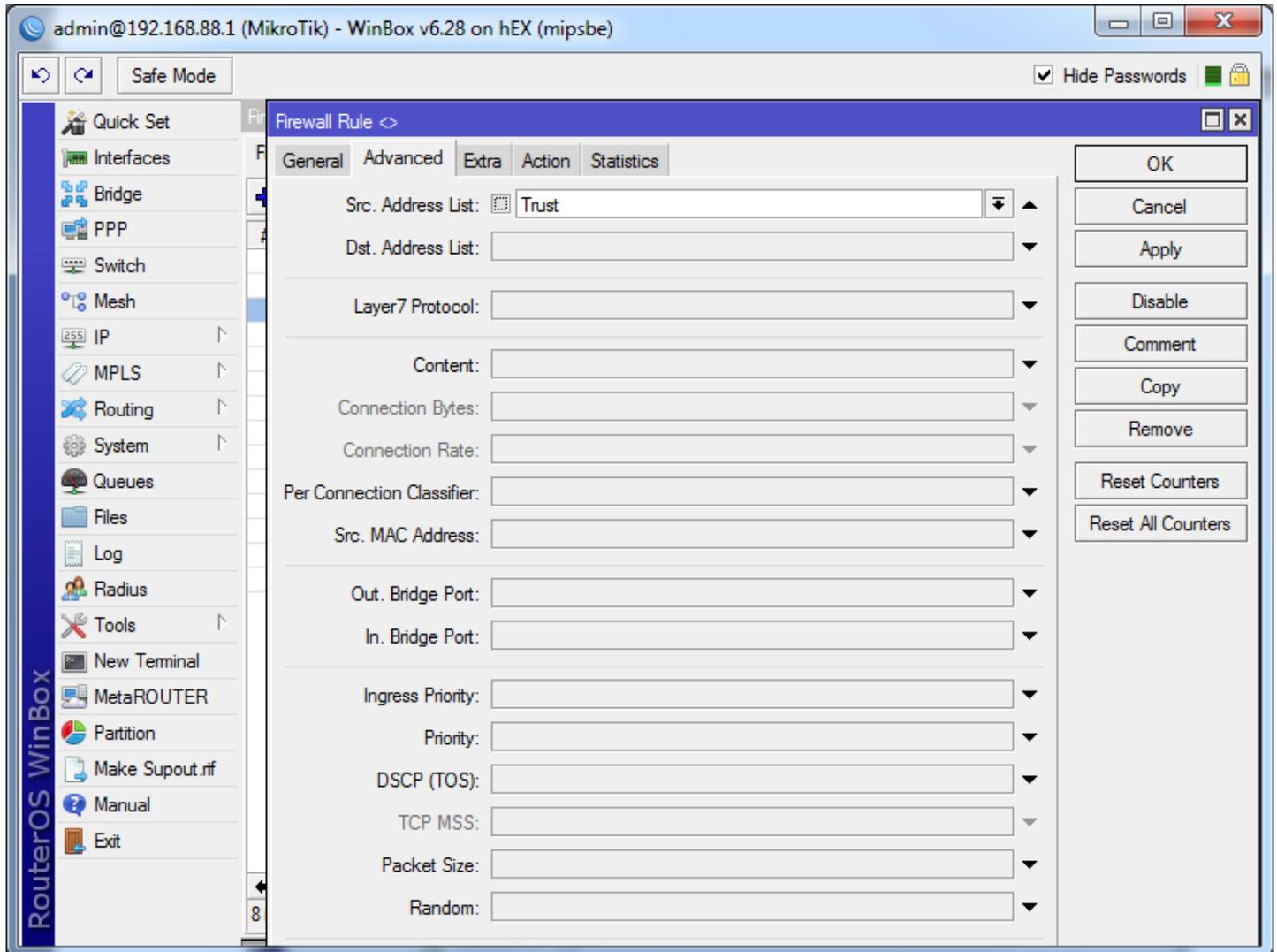


CREATE FIREWALL RULES

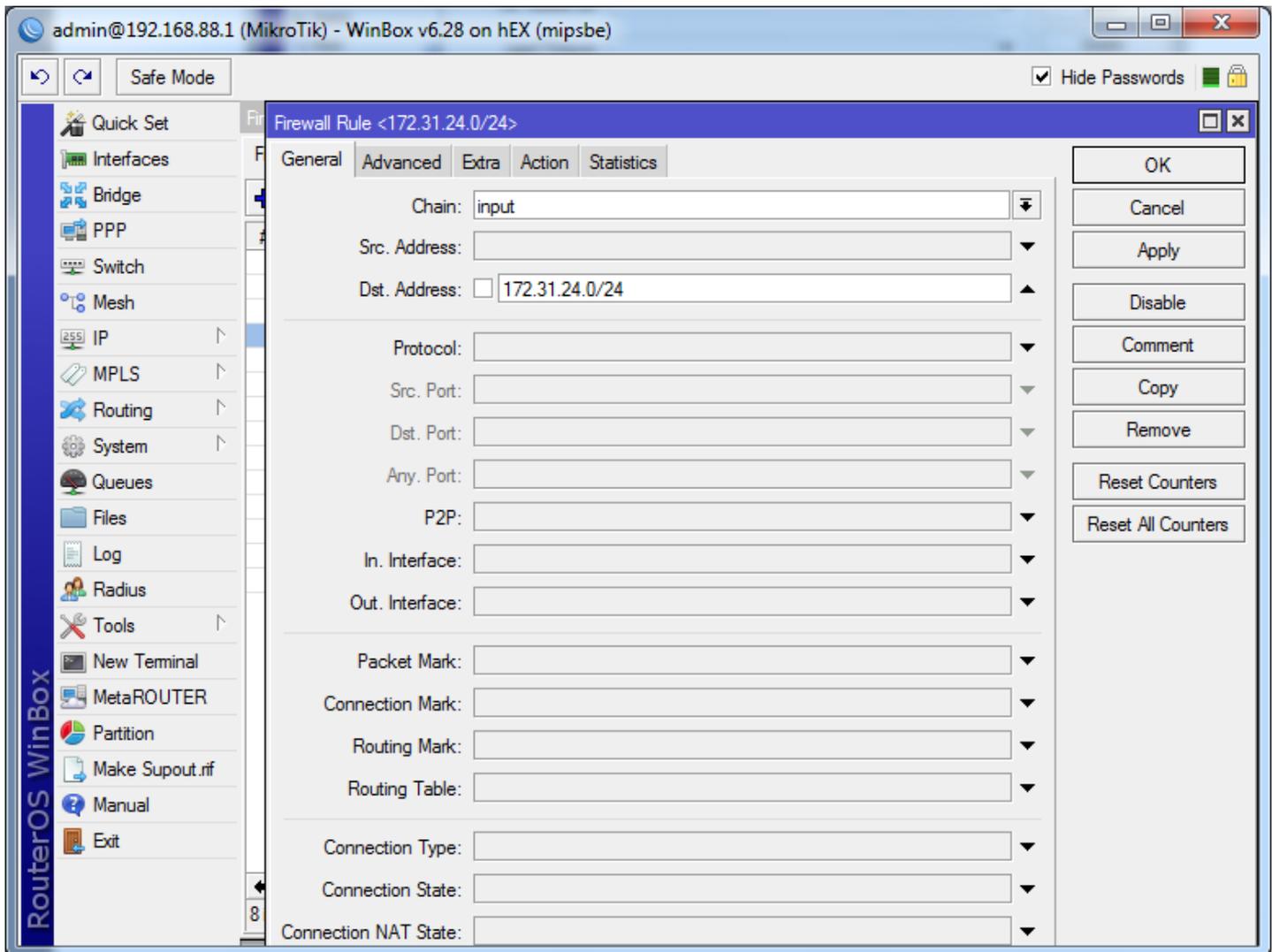
Add a firewall rule to include the “Trust” addresses with GRE protocol. To do this go to **IP > Firewall** and click the + symbol. Select **input** for Chain and use **gre** for Protocol.



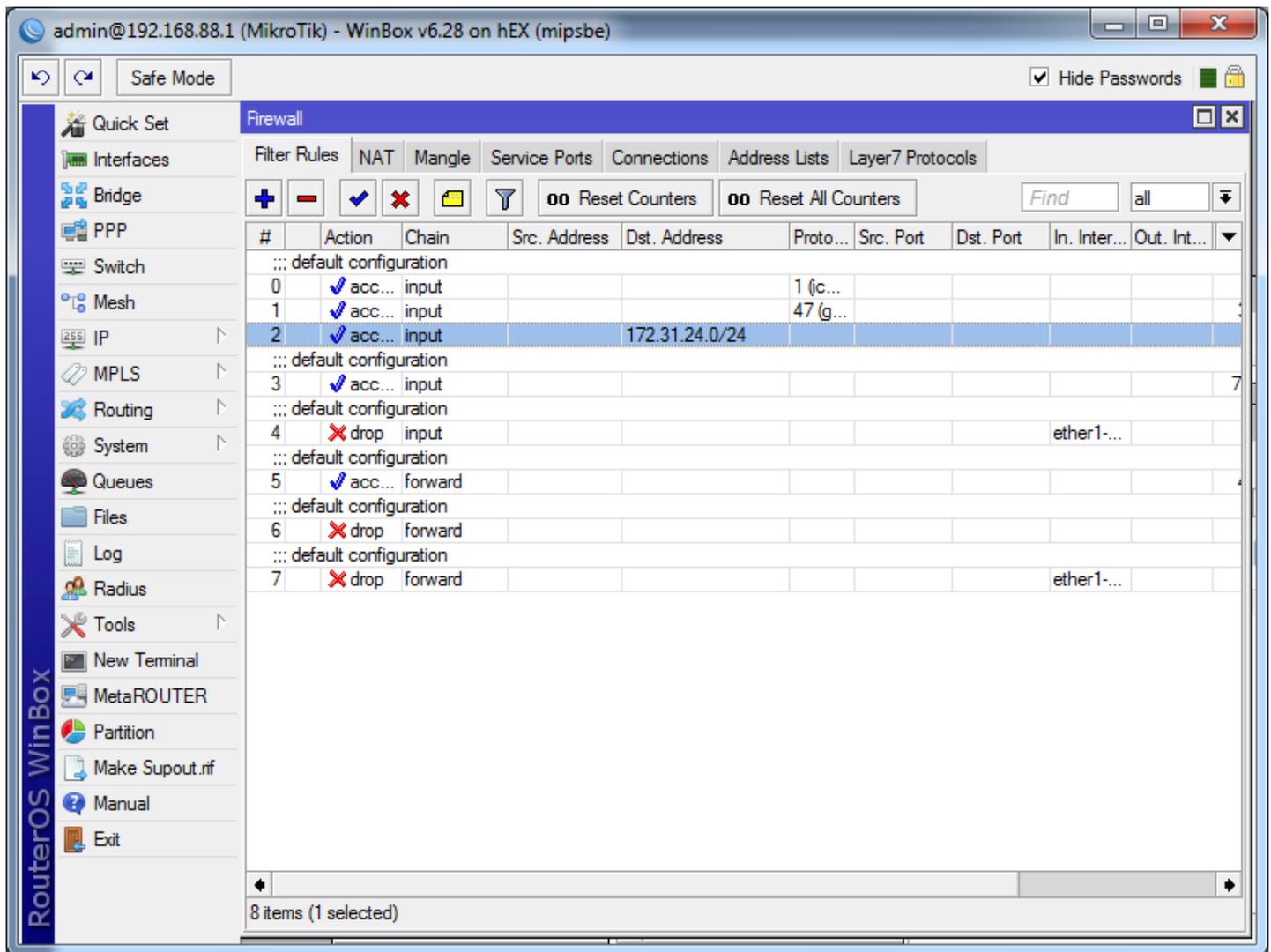
Go to the **Advanced** tab and select **“Trust”** as the Src. Address List.



Add a second rule. Under the General tab, select **input** for Chain. Use the **GRE Tunnel Network** as Dst. Address.

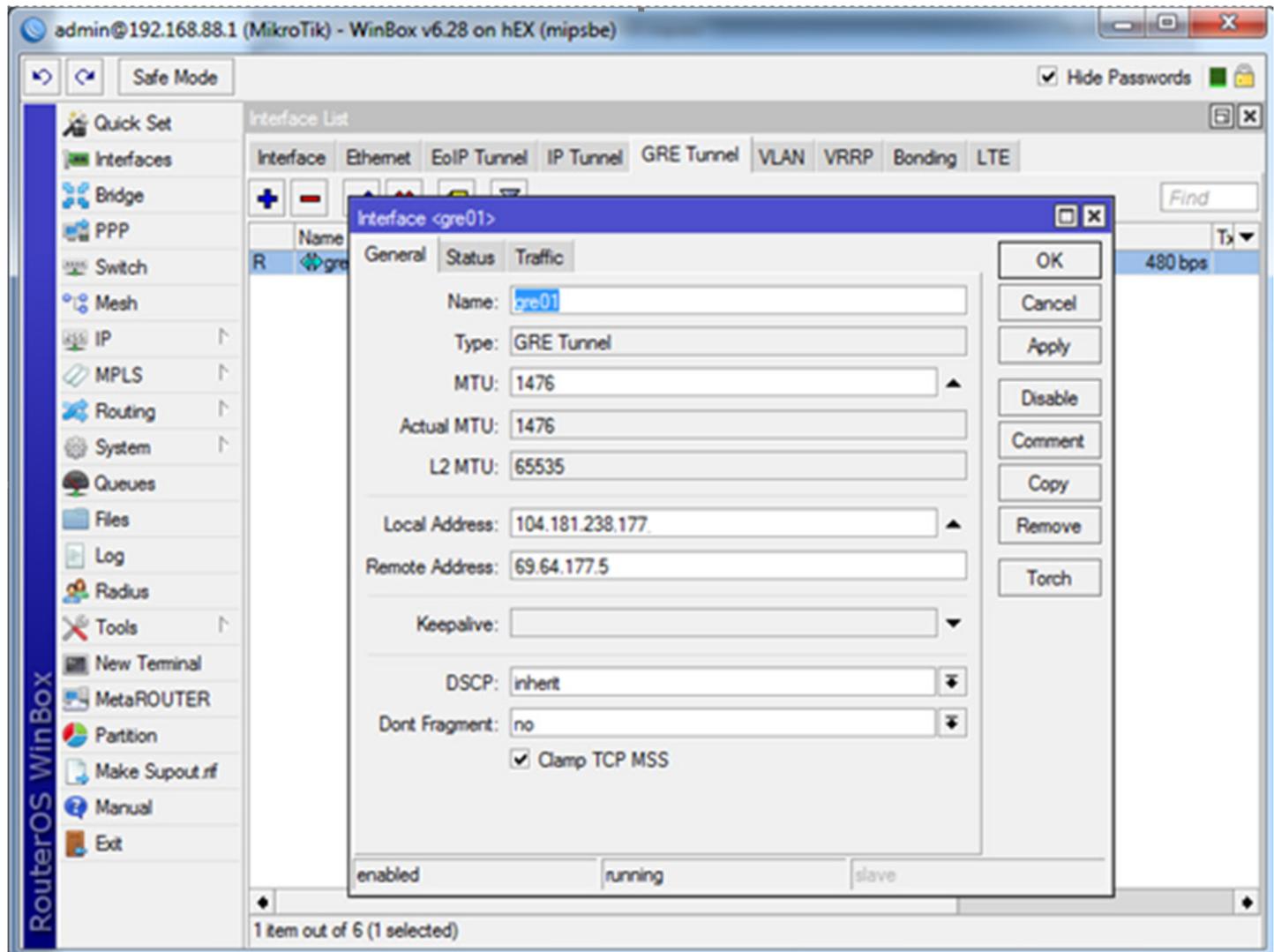


Drag the 2 rules you created so they appear below rule 0. This is to ensure that gre traffic and tunnel are allowed.



CREATE THE GRE TUNNEL

Go to Interface > GRE Tunnel. Click “+” to add the interface.



CREATE THE TUNNEL ADDRESS

Go to IP > Address List. Click + to add a new address.

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.88.1 (MikroTik) - WinBox v6.28 on hEX (mipsbe)". The left sidebar contains a menu with options: Quick Set, Interfaces, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.nf, Manual, and Exit. The "IP" menu is expanded, and the "Address List" window is open. The "Address List" window has a toolbar with a plus sign (+) for adding a new address, a minus sign (-) for deleting, a checkmark for enabling, a red X for disabling, a folder icon, and a filter icon. A "Find" search box is also present. The main area of the "Address List" window displays a table with columns: Address, Network, and Interface. The table contains three entries: 1. Address: 104.181.238.4/24, Network: 104.181.236.0, Interface: ether1-gateway. 2. Address: 172.31.24.200/24, Network: 172.31.24.0, Interface: gre01. 3. Address: 192.168.88.1/24, Network: 192.168.88.0, Interface: ether2-master-lo... The second entry is selected. Below the table, there is a section for "default configuration" with a plus sign (+) icon. A modal dialog box titled "Address <172.31.24.200/24>" is open over the table. It contains fields for "Address:" (172.31.24.200/24), "Network:" (172.31.24.0), and "Interface:" (gre01). The dialog has buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove". The status "enabled" is shown at the bottom of the dialog.

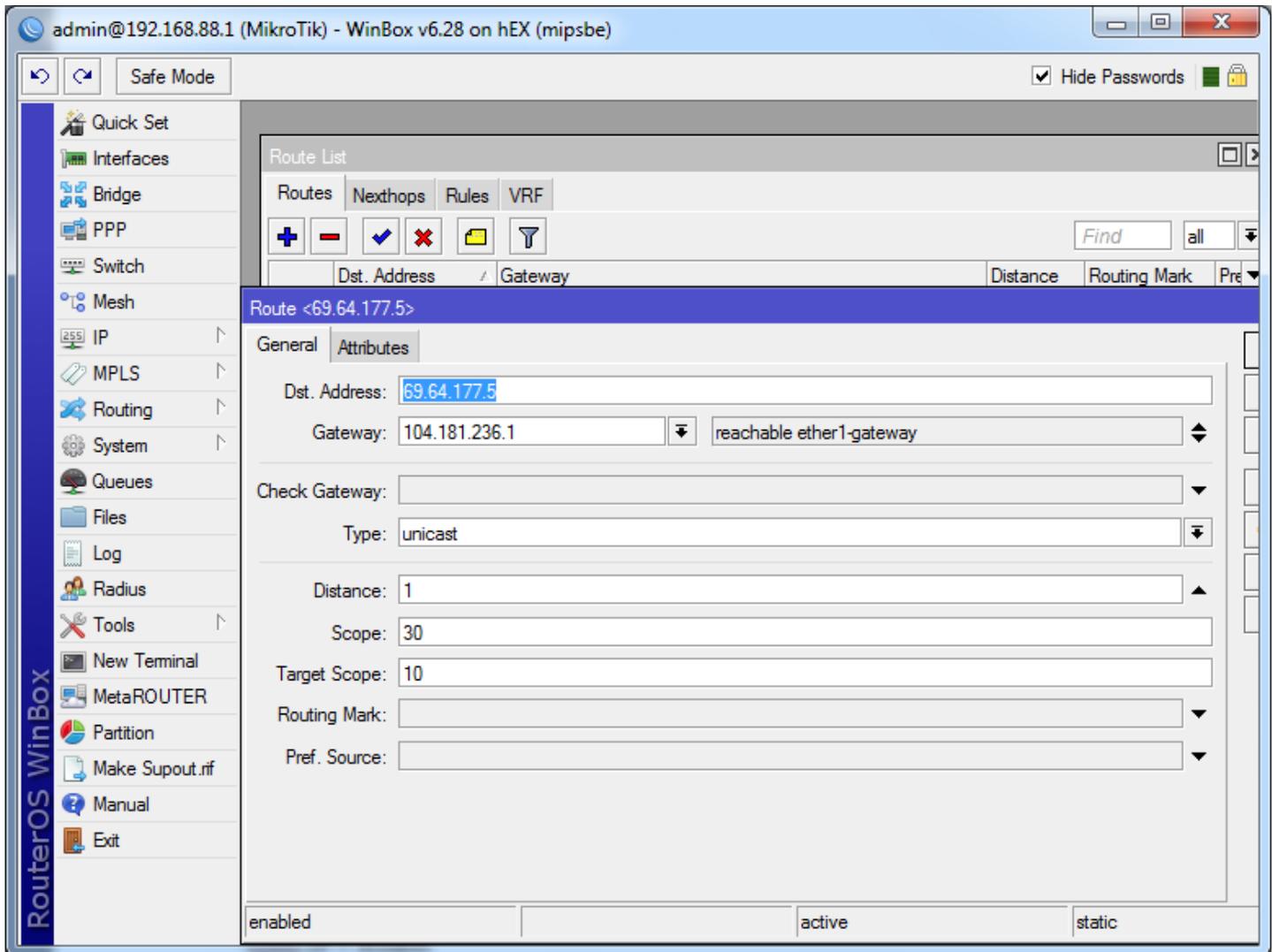
| Address | Network | Interface |
|------------------|---------------|---------------------|
| 104.181.238.4/24 | 104.181.236.0 | ether1-gateway |
| 172.31.24.200/24 | 172.31.24.0 | gre01 |
| 192.168.88.1/24 | 192.168.88.0 | ether2-master-lo... |

ADD DEFAULT ROUTE

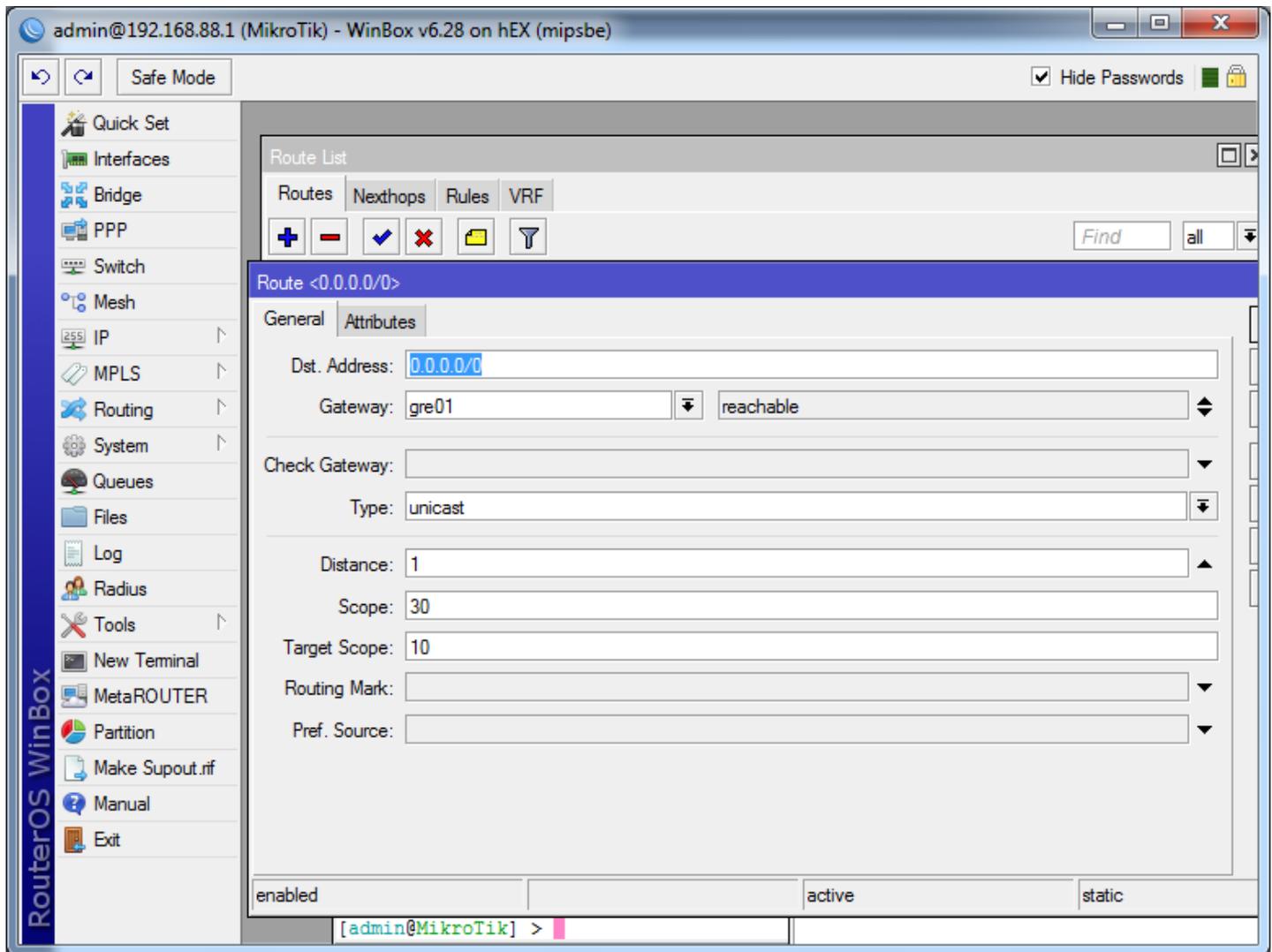
This step is critical!

Go to IP > Routes.

Use the **Cloud Public IP** as Dst. Address. Use the **Local Public GW** address as Gateway. The tunnel will not establish if this is not added.

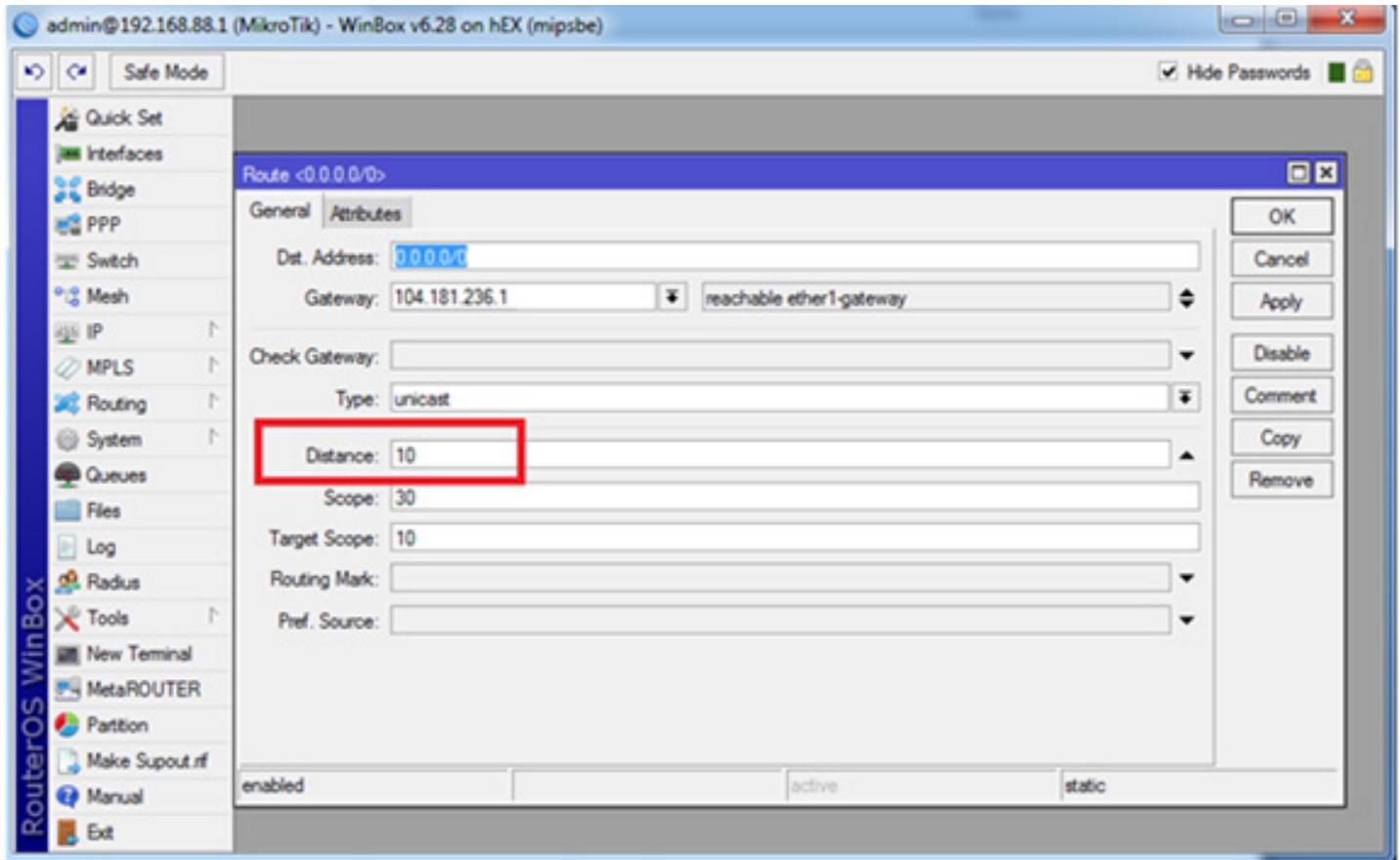


Point the default route to the GRE tunnel you created above using Distance 1.



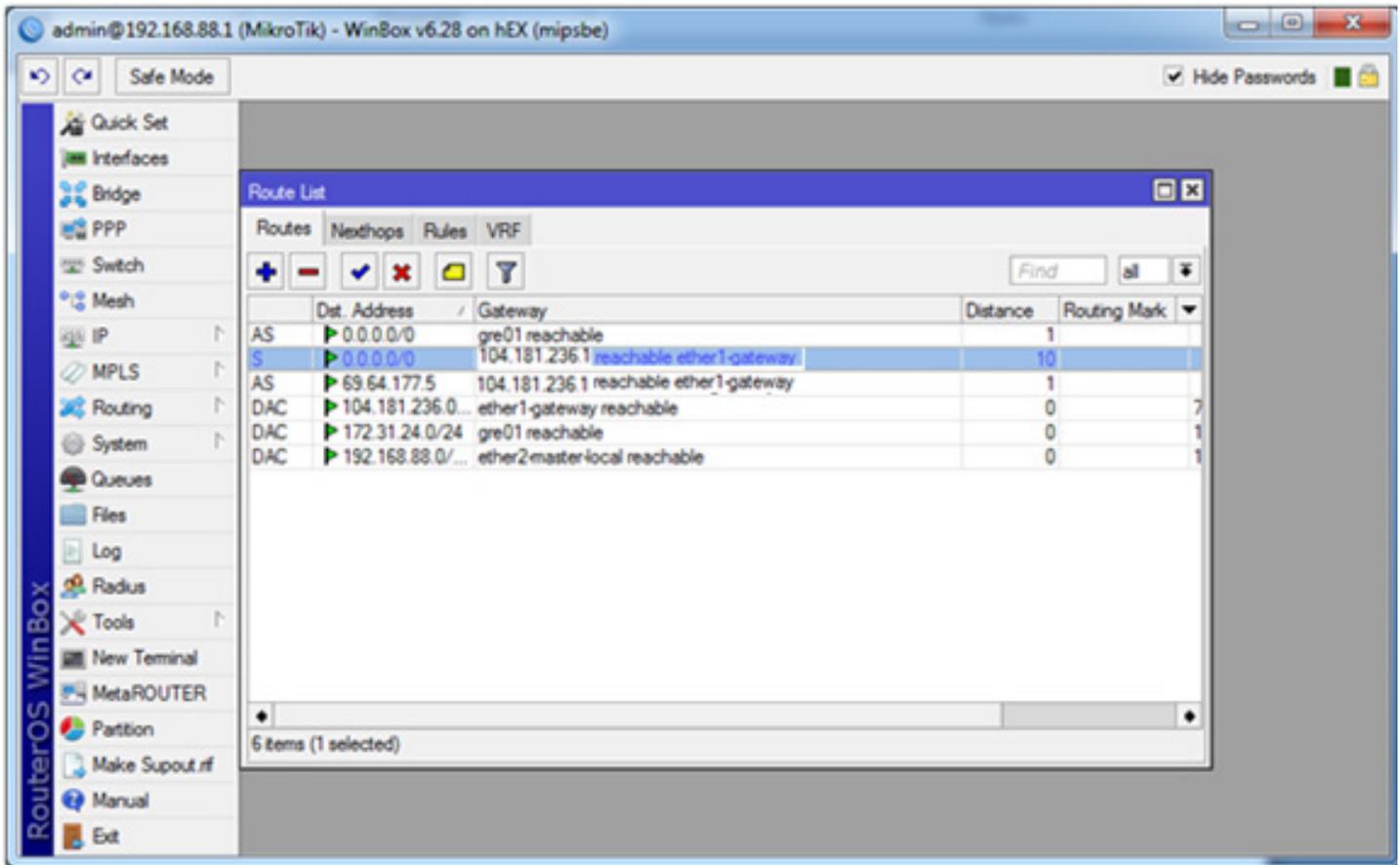
Assuming the MikroTik is currently being used as a gateway device, there is likely a default route that currently exists.

Open the rule and change the distance to 10.



REVIEW IP ROUTES

Go to IP > Routes.



Once the routes are verified, the tunnel should be up and you should be able to pass traffic to the MDS cloud.

VERIFY TRAFFIC

This step verifies that Internet traffic is exiting via the MDS cloud.

Open a browser from the local LAN and attempt to browse to ipchicken.com. The IP address should be the address of the **Cloud Public IP**.



Current IP Address

69.64.177.5

[Add to Favorites](#)

Advanced

- Name Address: 5-177-64-69-available.ilandcloud.com
- Remote Port: 52050
- Browser: Mozilla/5.0 (Windows NT 6.1; rv:42.0) Gecko/20100101 Firefox/42.0

APPENDIX

This is the cli export of the configuration. All the changes documented above can be accomplished by using the CLI if you are an advanced user.

```
CLI configuration: [admin@MikroTik] > export
# feb/04/2016 00:40:18 by RouterOS 6.28
# software id = 8QBA-5ILV
#
/interface ethernet
set [ find default-name=ether1 ] name=ether1-gateway
set [ find default-name=ether2 ] name=ether2-master-local
set [ find default-name=ether3 ] master-port=ether2-master-local name=\
ether3-slave-local
set [ find default-name=ether4 ] master-port=ether2-master-local name=\
ether4-slave-local
set [ find default-name=ether5 ] master-port=ether2-master-local name=\
ether5-slave-local
/interface gre
add !keepalive local-address=104.181.238.177 mtu=1476 name=gre01 \
remote-address=69.64.177.5
/ip neighbor discovery
set ether1-gateway discover=no
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ipdhcp-server
add address-pool=default-dhcp disabled=no interface=ether2-master-local name=\
default
/ip address
add address=192.168.88.1/24 comment="default configuration" interface=\
ether2-master-local network=192.168.88.0
add address=172.31.24.200/24 interface=gre01 network=172.31.24.0
/ipdhcp-client
add comment="default configuration" dhcp-options=hostname,clientid disabled=\
no interface=ether1-gateway
/ipdhcp-server network
add address=192.168.88.0/24 comment="default configuration" gateway=\
192.168.88.1
/ipdns
set allow-remote-requests=yes
/ipdns static
add address=192.168.88.1 name=router
/ip firewall address-list
add address=104.181.238.177 list=Trust
add address=69.64.177.5 list=Trust
/ip firewall filter
add chain=input comment="default configuration" protocol=icmp
add chain=input protocol=gresrc-address-list=Trust
add chain=input dst-address=172.31.24.0/24
```

```
add chain=input comment="default configuration" connection-state=\
established,related
add action=drop chain=input comment="default configuration" in-interface=\
ether1-gateway
add chain=forward comment="default configuration" connection-state=\
established,related
add action=drop chain=forward comment="default configuration" \
connection-state=invalid
add action=drop chain=forward comment="default configuration" \
connection-nat-state=!dstnat connection-state=new in-interface=\
ether1-gateway
/ip firewall nat
add action=masquerade chain=srcnat comment="default configuration" \
out-interface=ether1-gateway
/ip route
add distance=1 gateway=gre01
add distance=1 gateway=104.181.236.1
add distance=1 dst-address=69.64.177.5/32 gateway=104.181.236.1
/romon port
add disabled=no
/system clock
set time-zone-name=America/Chicago
/system routerboard settings
set cpu-frequency=720MHz protected-routerboot=disabled
/tool mac-server
set [ find default=yes ] disabled=yes
add interface=ether2-master-local
add interface=ether3-slave-local
add interface=ether4-slave-local
add interface=ether5-slave-local
/tool mac-server mac-winbox
set [ find default=yes ] disabled=yes
add interface=ether2-master-local
add interface=ether3-slave-local
add interface=ether4-slave-local
add interface=ether5-slave-local
[admin@MikroTik] >
```