Configuring Mikrotik router with 3CX

Presented by

Biztech Infrastructure Systems Limited
4 Emina Crescent , Off Toyin Street, Ikeja,
Lagos, Nigeria

Instructor: Ajibola Olayemi

Prepared by: Bruce Folashade

Configuring MikroTik with 3CX

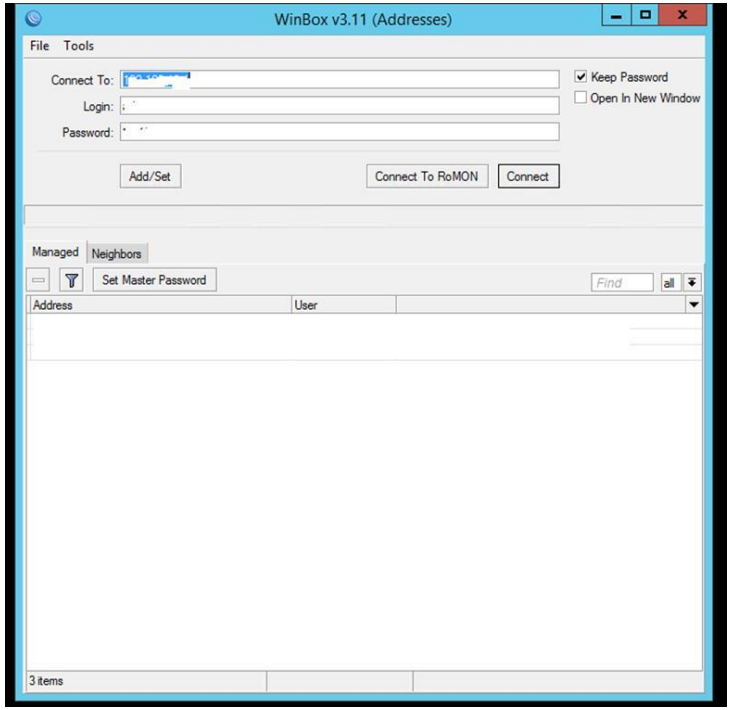
- Introduction
- Step 1: Logging into Mikrotik
- Step 2: Disable SIP ALG
- Step 3: Port Forwarding (NAT)
- Presence and Webaccess
- SIP and RTP Ports
- Tunnel Ports
- Step 4: Inbound Access List
- Questions and Answers

Introduction

This document describes the configuration of MikroTik RB2011UiAS devices for use with 3CX and should be compatible with any device of this series. Although settings can be done via ssh or the web interface, it is recommended to follow the guide via the GUI and past certain Commands into the device. The commands below need to be pasted in the router/firewall console (ssh).

Step 1: Logging into Mikrotik

We will be looking at the option and best way to do this using the WinBox. Log into the 3CX using the WinBox with the correct parameters:

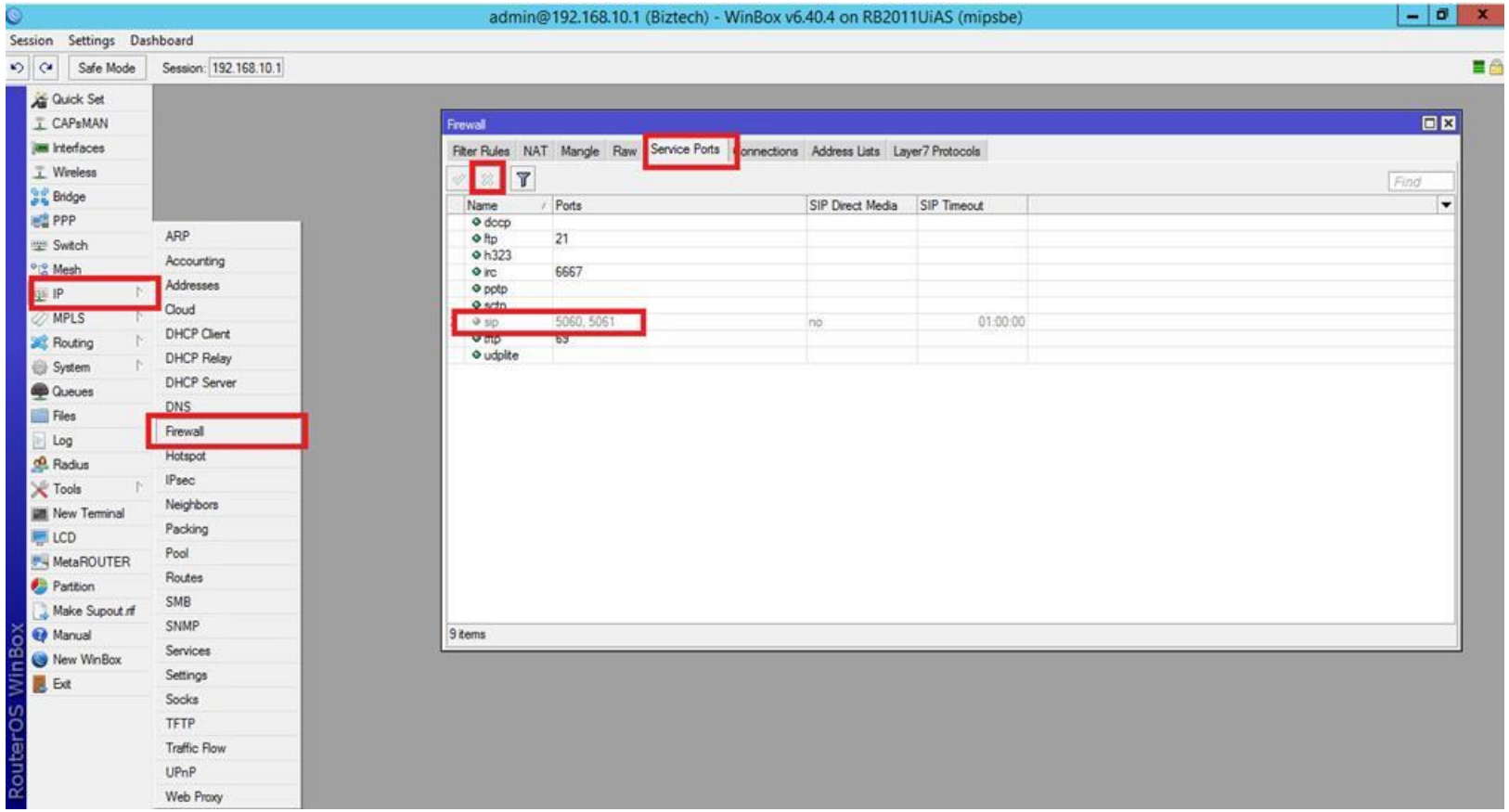


In the Connect To: type the IP address of the router or scan for the IP address. Connect with either the IP address or the MAC address of the router. Enter the username and password for the router and click connect.

Step 2: Disable SIP ALG

Within the GUI of MikroTik navigate to IP → Firewall → Service Ports → disable SIP rule.

You can just click on the “X” sign to disable. The other alternative is to use the command line from the terminal: **“ip firewall service-port disable sip”**

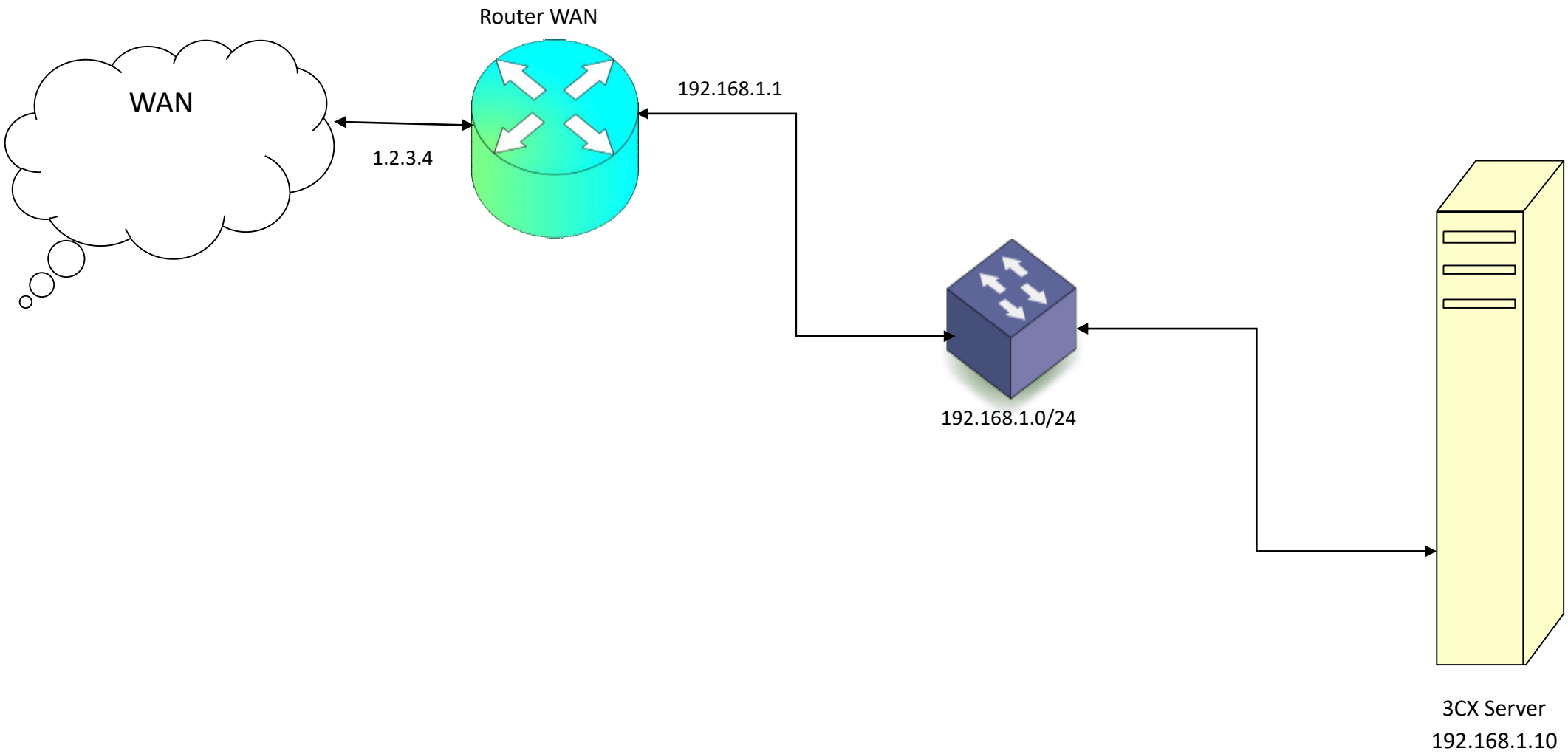


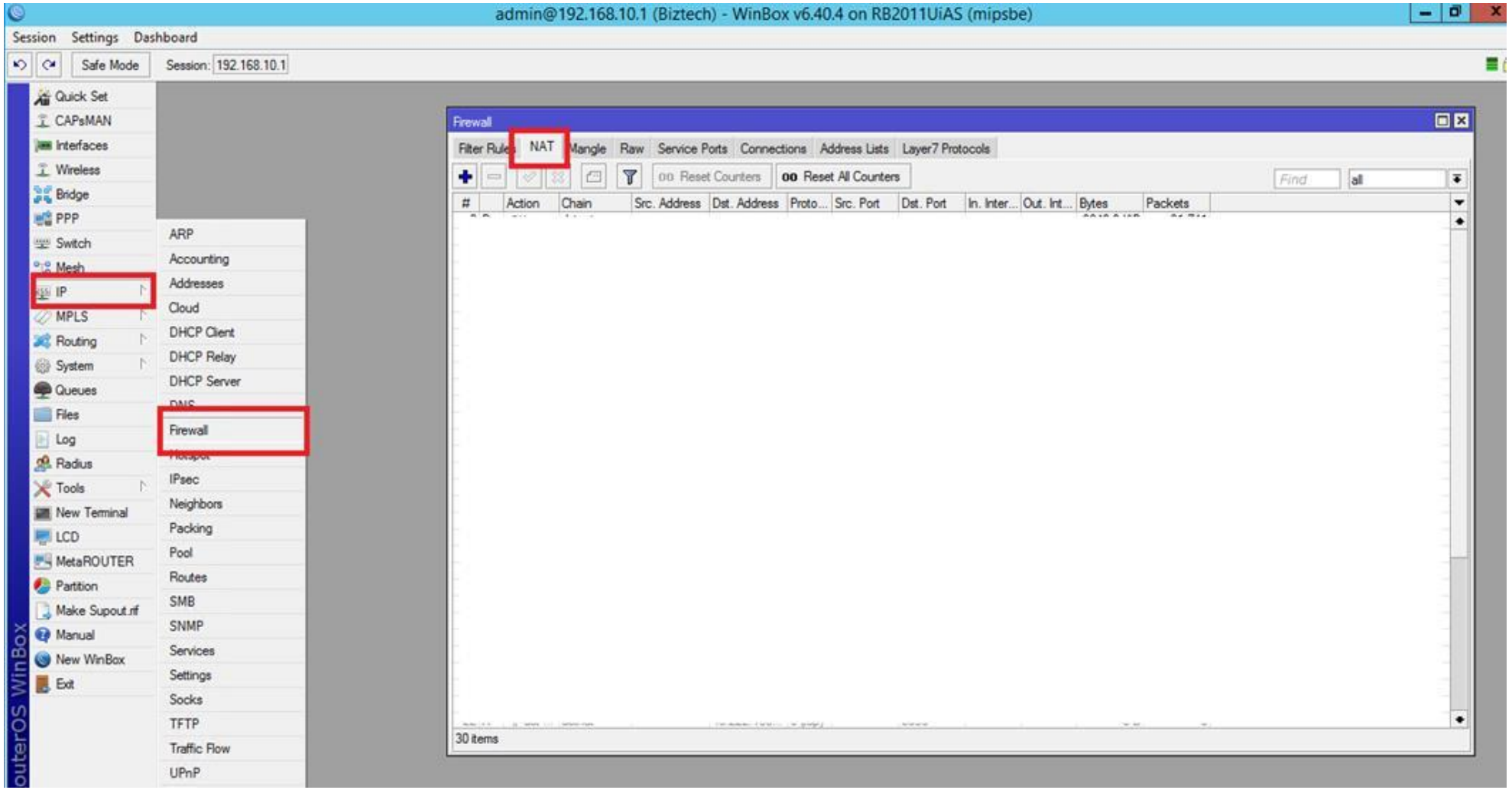
Step 3: Port Forwarding (NAT)

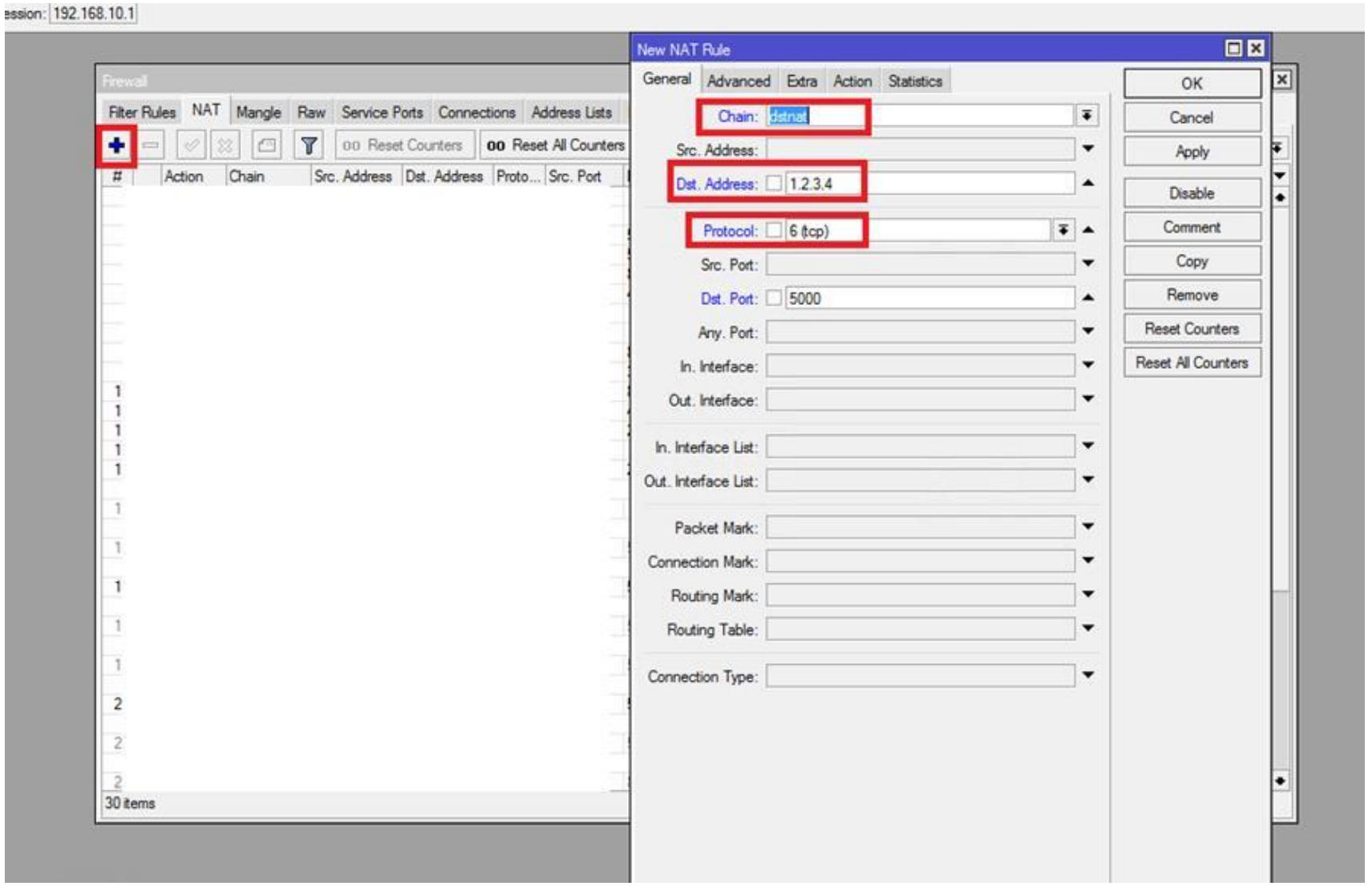
The below figure below shows how the NAT can be achieved with the WinBox. Before we do this we have to make some assumption to enable us understand the procedures.

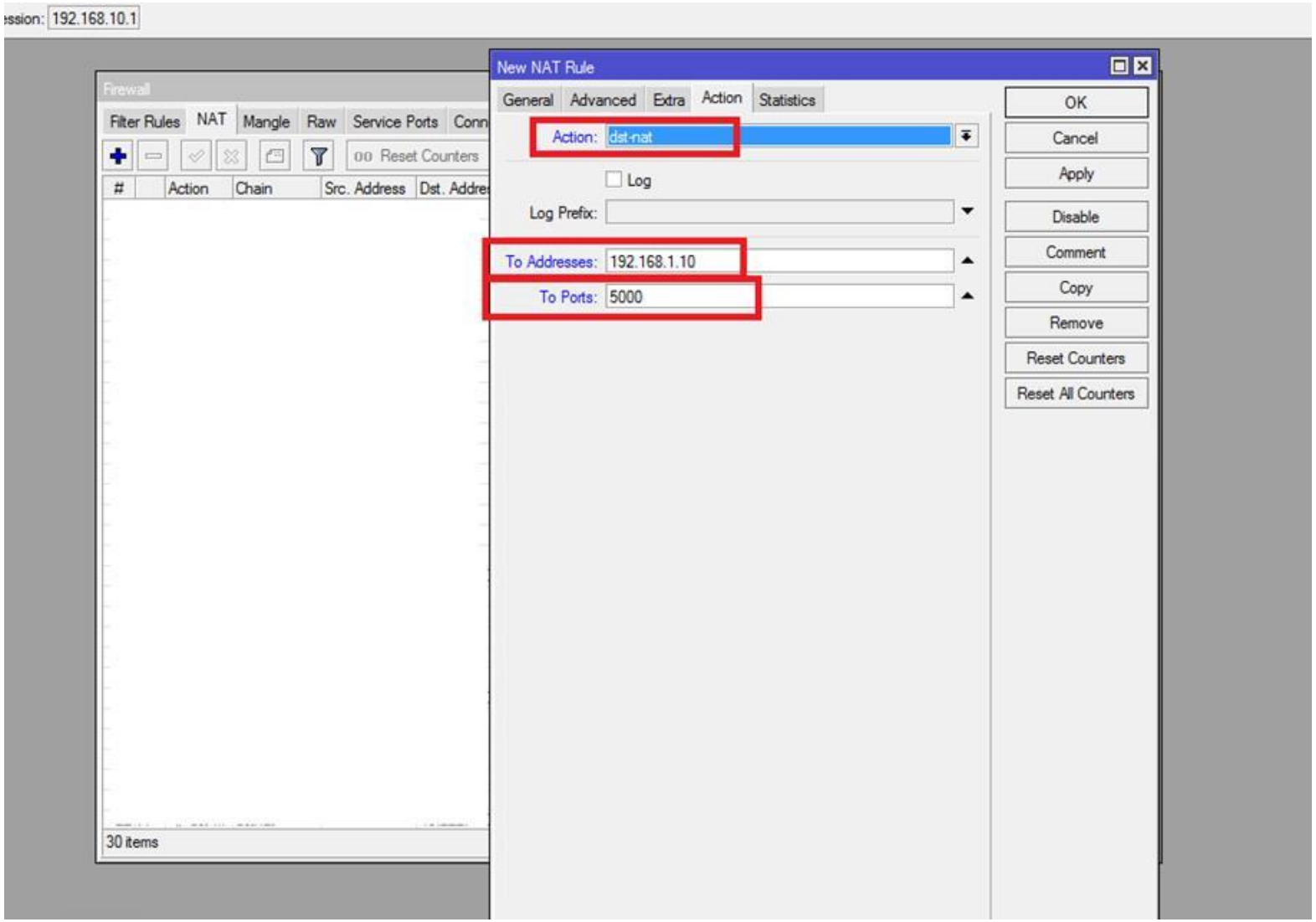
Let us assume that the IP address for the 3CX Server is 192.168.1.10, The LAN IP address is 192.168.1.0/24, the LAN interface on the Mikrotik Router is 192.168.1.1 and the WAN interface on the Mikrotik Router is 1.2.3.4.

For port forwarding to be possible we need to be able to re direct all traffic meant for the 3CX Server on specific ports to the 3CX server from the Public IP address (WAN).


Router WAN
WAN
1.2.3.4
192.168.1.1
192.168.1.0/24
3CX Server
192.168.1.10


admin@192.168.10.1 (Biztech) - WinBox v6.40.4 on RB2011UiAS (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 192.168.10.1
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
Firewall
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
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 Proto... Src. Port Dst. Port In. Inter... Out. Int... Bytes Packets
30 items
RouterOS WinBox


ession: 192.168.10.1
Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Reset Counters
Reset All Counters
#
Action
Chain
Src. Address
Dst. Address
Proto...
Src. Port
30 items
New NAT Rule
General
Advanced
Extra
Action
Statistics
Chain: dstnat
Src. Address:
Dst. Address: 1.2.3.4
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 5000
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


ession: 192.168.10.1
Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Reset Counters
#
Action
Chain
Src. Address
30 items
New NAT Rule
General
Advanced
Extra
Action
Statistics
Action: dst-nat
Log
Log Prefix:
To Addresses: 192.168.1.10
To Ports: 5000
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

The following commands will enable the port forwarding from your WAN interface to 3CX. We assume that there is a static IP on the WAN interface. However, if the router deals with a dynamic public IP then you must omit in each of the following commands the part **“dst-address=1.2.3.4”** which will be highlighted in bold.

Presence and Webaccess

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5001 protocol=tcp **“dst-address=1.2.3.4”** dst-port=5001 comment="3CX Presence and Provisioning HTTPS"

SIP and RTP Ports

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5060 protocol=udp **“dst-address=1.2.3.4”** dst-port=5060 comment="3CX SIP UDP"

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5060 protocol=tcp **“dst-address=1.2.3.4”** dst-port=5060 comment="3CX SIP TCP"

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5061 protocol=tcp **“dst-address=1.2.3.4”** dst-port=5061 comment="3CX SIP TLS"

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=9000-9500 protocol=udp **“dst-address=1.2.3.4”** dst-port=9000-9500 comment="3CX Media UDP"

Tunnel ports

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5090 protocol=tcp **“dst-address=1.2.3.4”** dst-port=5090 comment="3CX Tunnel TCP"

ip firewall nat add chain=dstnat action=dst-nat to-addresses=10.7.7.2 to-ports=5090 protocol=udp **“dst-address=1.2.3.4”** dst-port=5090 comment="3CX Tunnel UDP"

Step 4: Inbound Access List

When creating port forwarding rules the router adds the filter rule behind the scenes and do not have to be created as ACL. However, you might need to validate the general firewall filters. The following commands will DROP all the traffic getting to the Internet interface of the router. Keep in mind, that the additional rules allow traffic from connections already established like traffic coming back from a connections initialized by a local computer.

```
ip firewall filter add chain=input action=accept connection-state=established
ip firewall filter add chain=input action=accept connection-state=related
ip firewall filter add chain=forward action=accept connection-state=established
ip firewall filter add chain=forward action=accept connection-state=related
ip firewall filter add chain=forward action=drop connection-state=invalid
ip firewall filter add chain=input action=drop in-interface=ether1
```

Questions & Answers

Thanks