

Hairpin NAT

WAN and multi-WANs supported

Pongpipat Thunyawiraphap (ppp@mikrotiktutorial.com)

www.mikrotiktutorial.com

Introduce



Ruamrudee International School
Technology Committee / Network Admin
2,400 users : Computer 1,300 Units

Live Inc. Public Company
IT Director
Broadcasting, High Availability system, Networking

Now
Network Infrastructure Consultant



Hairpin NAT on Mikrotik WIKI

http://wiki.mikrotik.com/wiki/Hairpin_NAT

MikroTik documentation

Page Discussion Read View source View history Search

Hairpin NAT

In the below network topology a web server behind a router is on private IP address space, and the router performs NAT to forward traffic to its public IP address to the web server behind it.

The NAT configuration would look like below:

```
/ip firewall nat
add chain=dstnat dst-address=1.1.1.1 protocol=tcp dst-port=80 \
    action=dst-nat to-address=192.168.1.2
add chain=srcnat out-interface=WAN action=masquerade
```

When a client out on the Internet with IP address 2.2.2.2 establishes a connection to the web server, the router performs NAT as configured.

Step 1	Source IP 2.2.2.2	Destination IP 1.1.1.1

Hairpin NAT on Mikrotik WIKI

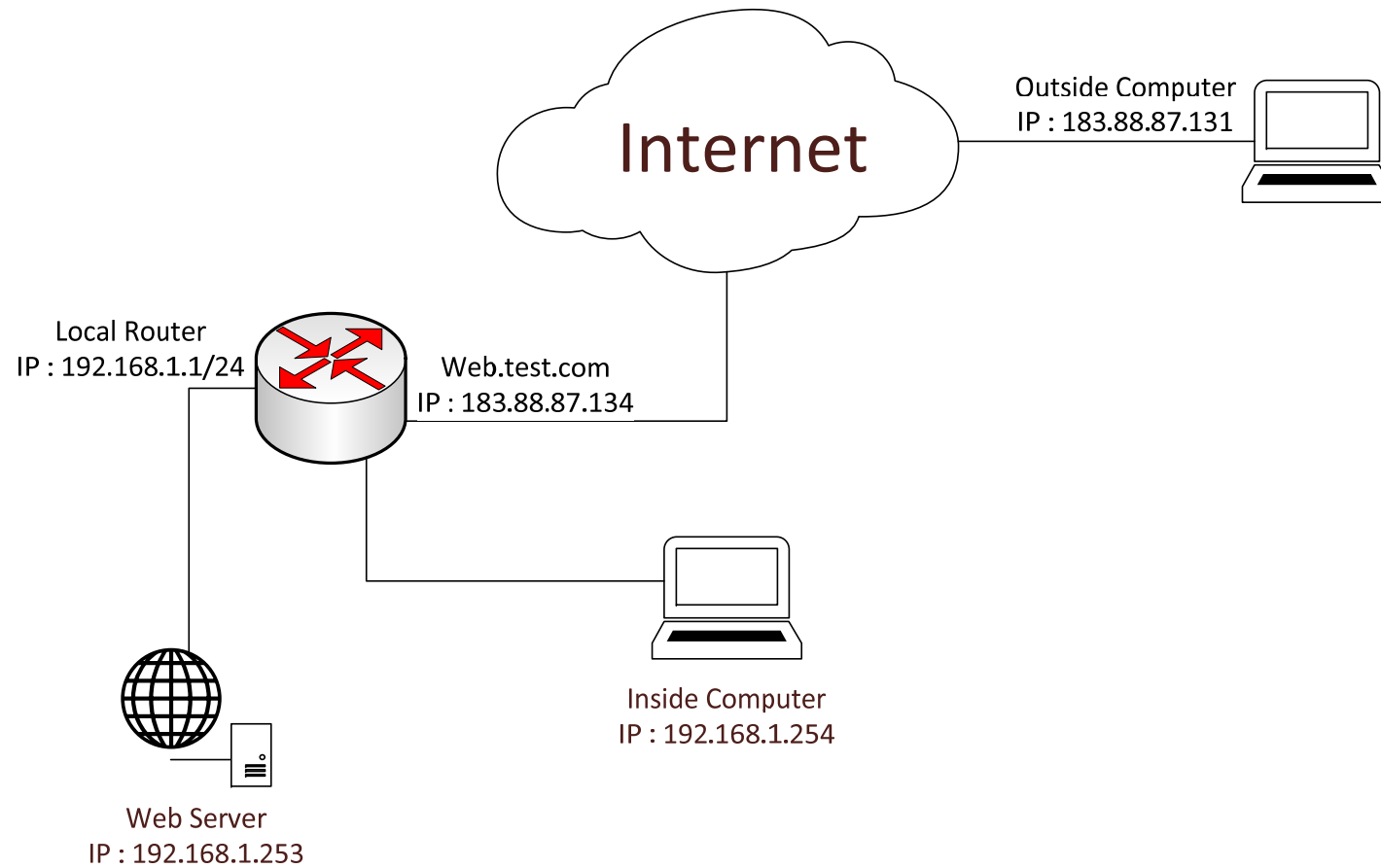
The client receives the reply packet, but it discards it because it expects a packet back from 1.1.1.1, and not from 192.168.1.2. As far as the client is concerned the packet is invalid and not related to any connection the client previously attempted to establish.

To fix the issue, an additional NAT rule needs to be introduced on the router to enforce that all reply traffic flows through the router, despite the client and server being on the same subnet. The rule is very specific to only apply to the traffic that the issue could occur with - if there are many servers the issue occurs with, the rule could be made broader to save having one such exception per forwarded service.

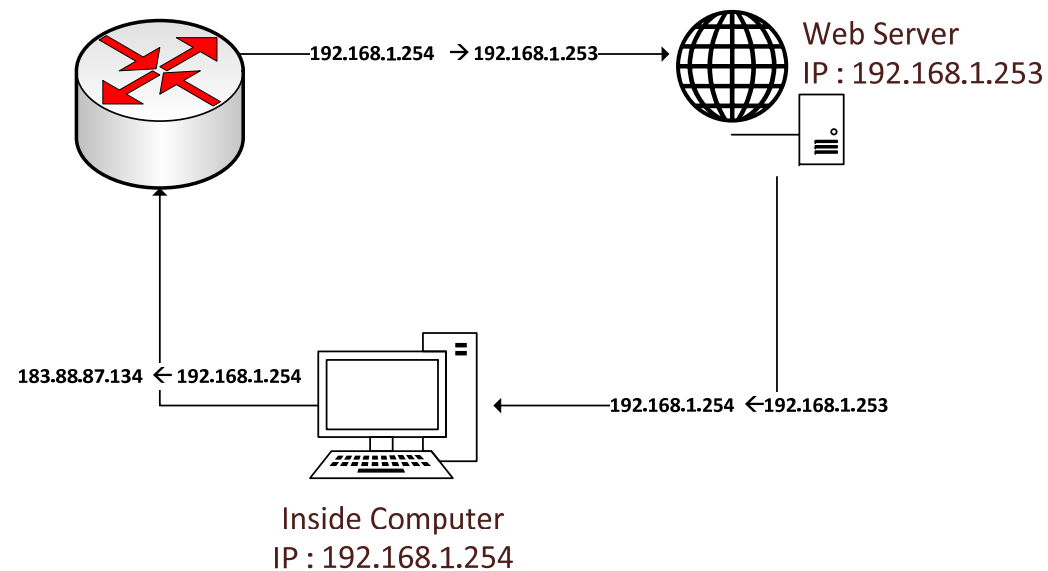
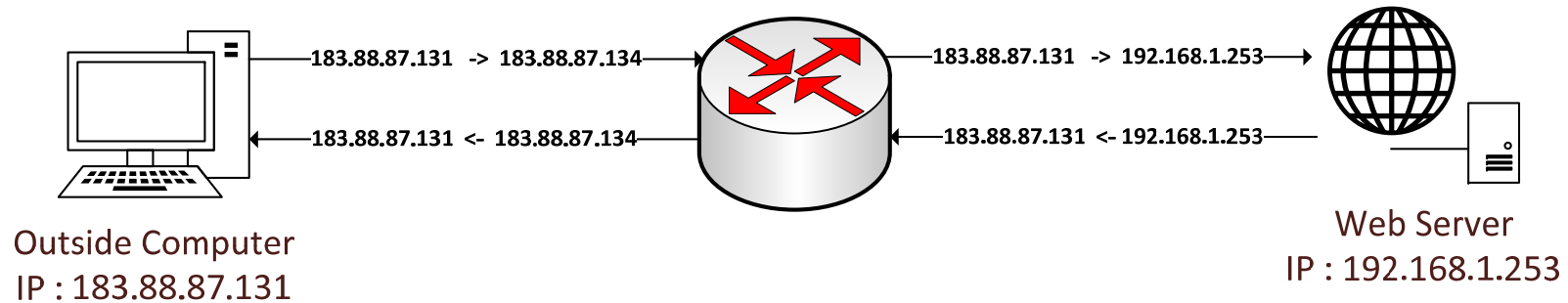
```
/ip firewall nat
add chain=srcnat src-address=192.168.1.0/24 \
dst-address=192.168.1.2 protocol=tcp dst-port=80 \
out-interface=LAN action=masquerade
```

Step 1	Source IP 192.168.1.10	Destination IP 1.1.1.1
Step 2	Source IP 192.168.1.1	Destination IP 192.168.1.2
Step 3	Source IP 192.168.1.2	Destination IP 192.168.1.1
Step 4	Source IP 1.1.1.1	Destination IP 192.168.1.10

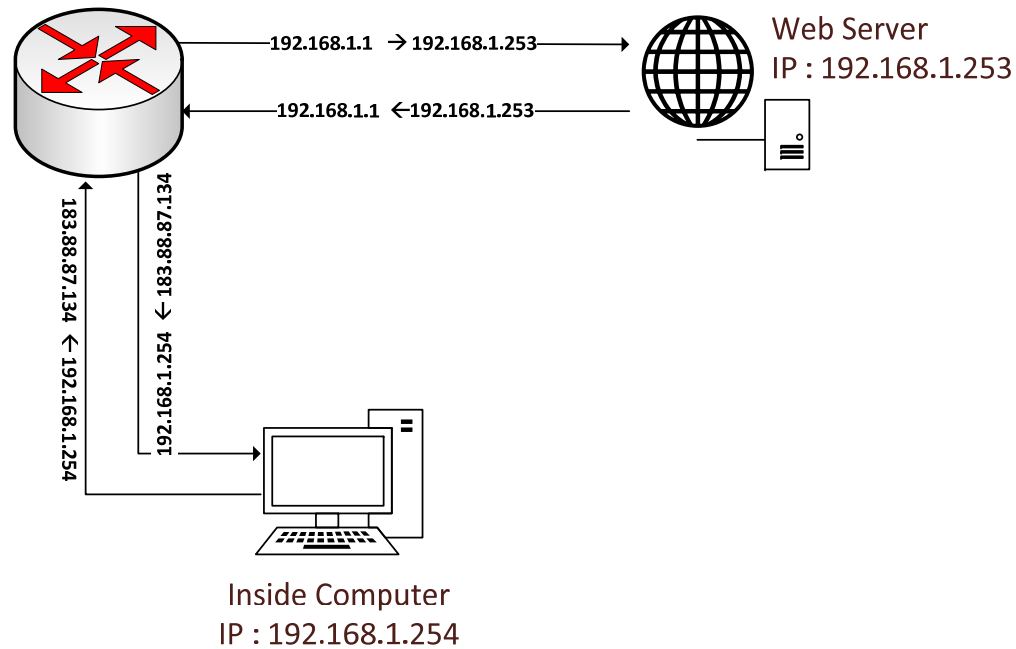
Network Topology



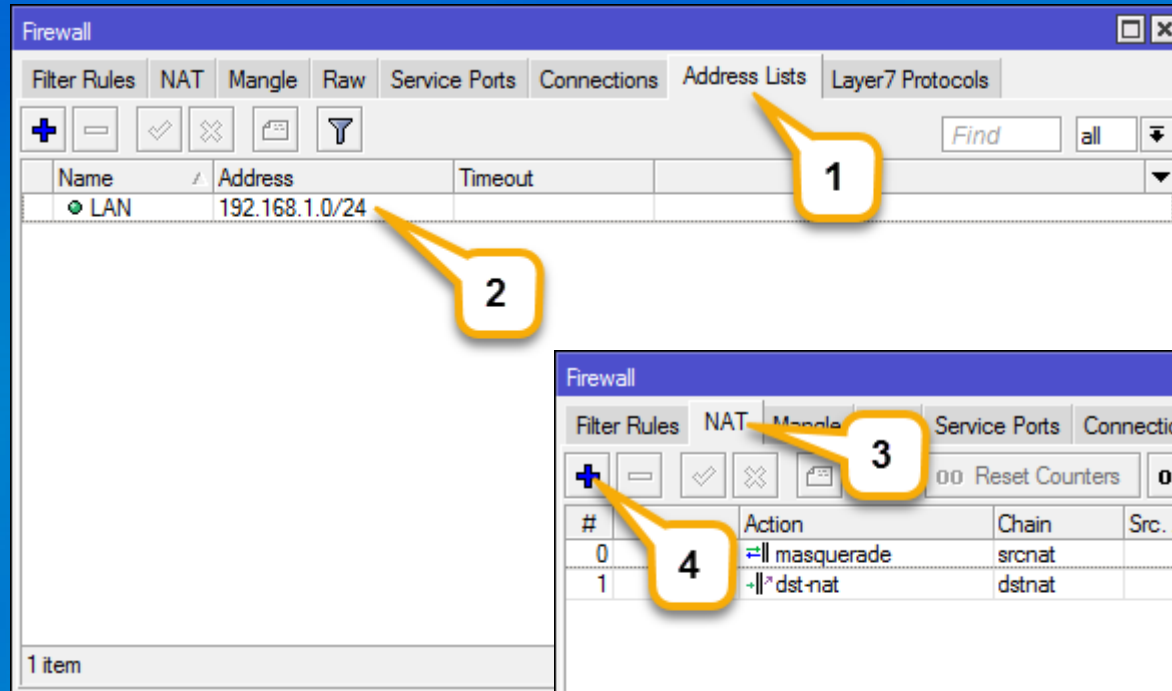
How DST-NAT work



How Hairpin NAT work

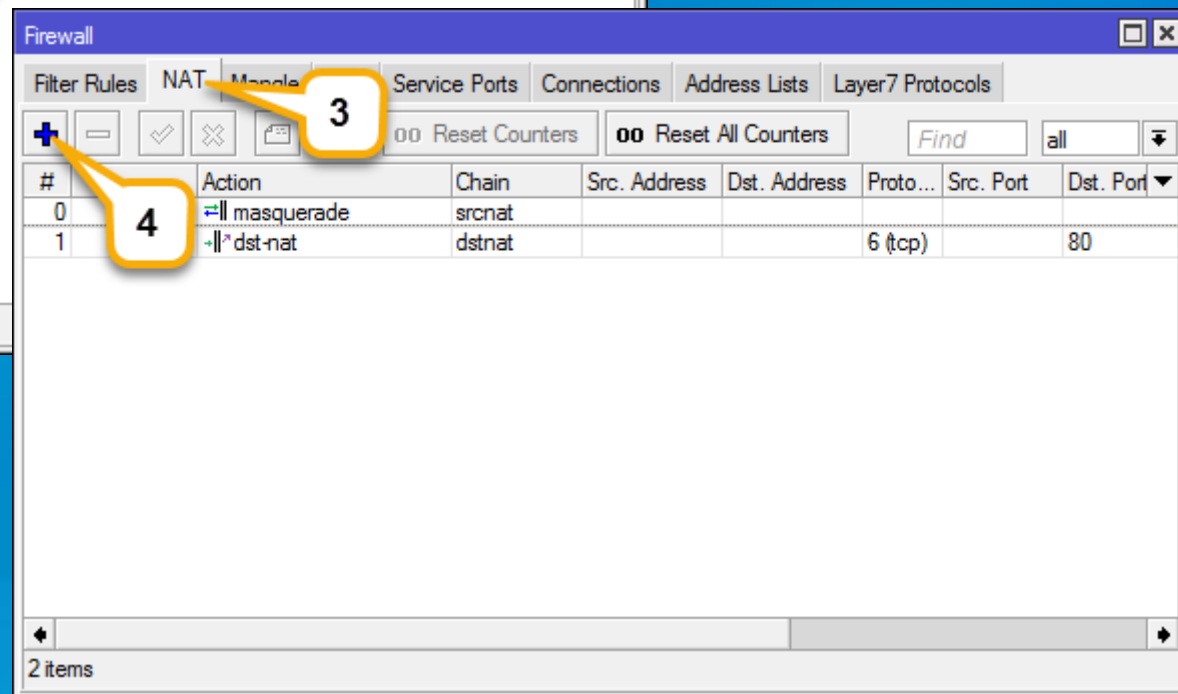


Heart of Hairpin NAT



The screenshot shows the Mikrotik WinBox Firewall configuration window with the 'Address Lists' tab selected. A table lists address lists, with one entry highlighted. A callout box labeled '1' points to the 'Address Lists' tab, and another callout box labeled '2' points to the highlighted entry.

Name	Address	Timeout
LAN	192.168.1.0/24	



The screenshot shows the Mikrotik WinBox Firewall configuration window with the 'NAT' tab selected. A table lists NAT rules. Callout boxes are present: '3' points to the 'NAT' tab, and '4' points to the first rule in the table.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
0	masquerade	srcnat					
1	dst-nat	dstnat			6 (tcp)		80

NAT for Hairpin NAT (1)

The image illustrates the configuration of a NAT rule in Mikrotik WinBox, specifically for Hairpin NAT. It consists of three sequential screenshots of the 'New NAT Rule' dialog box, connected by orange arrows indicating the flow of configuration.

First Screenshot (Left): The 'General' tab is active. The 'Chain' is set to 'srcnat'. The 'Out. Interface' is set to 'LAN'. The 'Action' tab is visible but not yet selected.

Second Screenshot (Top Right): The 'General' tab is still active. The 'Src. Address List' is set to 'LAN'. The 'Action' tab is now selected, and the 'Action' is set to 'masquerade'. The 'Log' checkbox is unchecked.

Third Screenshot (Bottom Right): The 'Action' tab is still active. The 'Log Prefix' field is visible. The 'Log' checkbox is now checked.

NAT for Hairpin NAT (2)

The image illustrates the configuration of a NAT rule for Hairpin NAT in Mikrotik WinBox, shown in three sequential screenshots:

- Top Left Screenshot:** The 'General' tab is active. The 'Chain' is set to 'srcnat' and the 'Dst. Address' is '192.168.1.1'. The 'Action' tab is highlighted in blue, indicating the next step.
- Top Right Screenshot:** The 'Advanced' tab is active. The 'Src. Address List' is set to 'LAN'. The 'Action' tab is highlighted in blue.
- Bottom Screenshot:** The 'Action' tab is active. The 'Action' is set to 'masquerade'. The 'Log' checkbox is unchecked, and the 'Log Prefix' field is empty.

Orange arrows indicate the flow from the General tab to the Advanced tab, and then to the Action tab.

NAT for Hairpin NAT (3)

The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the NAT tab. The window title is "Firewall". The tabs include "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "NAT" tab is active. Below the tabs are several control buttons: a plus sign, a minus sign, a checkmark, a cross, a folder icon, a funnel icon, "00 Reset Counters", "00 Reset All Counters", a "Find" search box, and a dropdown menu set to "all".

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
::: Hairpin NAT							
0	= masquerade	srcnat					
::: Normal NAT							
1	= masquerade	srcnat					
2	+ dst-nat	dstnat			6 (tcp)		80

At the bottom of the window, there is a scroll bar and a status bar that reads "3 items (1 selected)".

What still missing? (1)

NAT

NAT Rule <80>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

In. Interface: WAN

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

Hairpin NAT

NAT Rule <80>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

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

What still missing? (2)

NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy:

Ingress Priority:

Priority:

DSCP (TOS):

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Hairpin NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Src. Address List: LAN

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy:

Ingress Priority:

Priority:

DSCP (TOS):

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

What still missing? (3)

NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Hotspot

IP Fragment

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Hairpin NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

▲ Dst. Address Type

Address Type: local

Invert

PSD

Hotspot

IP Fragment

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

What still missing? (4)

NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

To Addresses:

To Ports:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Hairpin NAT

NAT Rule <80>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

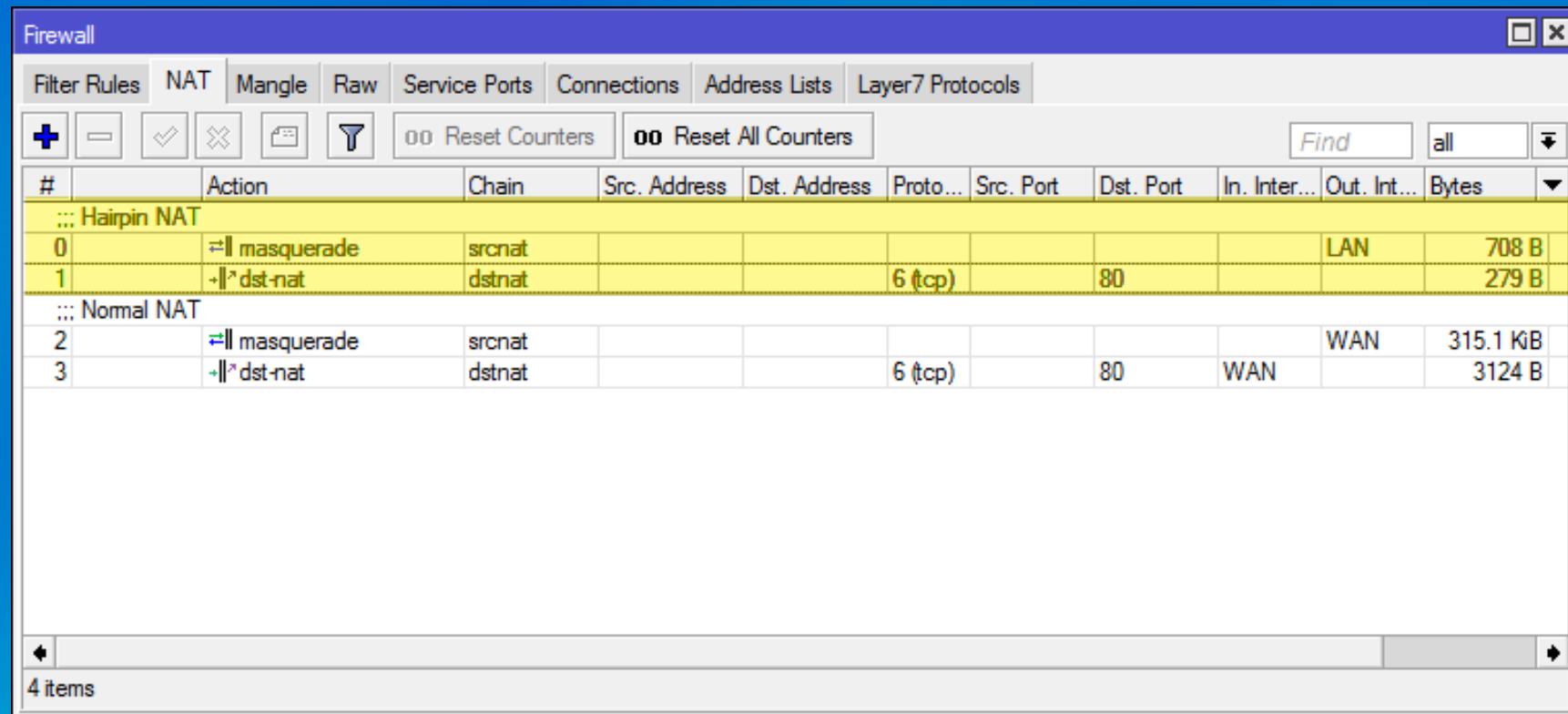
To Addresses:

To Ports:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

What still missing? (5)

Hairpin NAT rules



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the NAT tab. The window title is "Firewall". The tabs include "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "NAT" tab is active. The interface includes a toolbar with icons for adding, deleting, and saving rules, along with buttons for "Reset Counters" and "Reset All Counters". A search bar is present with the text "Find" and a dropdown menu set to "all".

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes
::: Hairpin NAT										
0	masquerade	srcnat							LAN	708 B
1	dst-nat	dstnat			6 (tcp)		80			279 B
::: Normal NAT										
2	masquerade	srcnat							WAN	315.1 KB
3	dst-nat	dstnat			6 (tcp)		80	WAN		3124 B

4 items

Conclusion

/ip firewall nat

**(1)add action=masquerade chain=srcnat comment=Solution1 out-interface=LAN
src-address-list=LAN**

**(2)add action=masquerade chain=srcnat comment=Solution2 dst-address=!192.168.1.1
src-address-list=LAN**

**add action=dst-nat chain=dstnat dst-address-type=local dst-port=80 protocol=tcp src-
address-list=LAN to-addresses=192.168.1.253 to-ports=80**

**add action=masquerade chain=srcnat out-interface=WAN src-address-list=LAN
add action=dst-nat chain=dstnat dst-port=80 in-interface=WAN protocol=tcp to-
addresses=192.168.1.253 to-ports=80**

Black = regular rules.

Green = Hairpin NAT, Choose one between (1) or (2).

Orange = Hairpin NAT, a must.

Purple = vary to environment.

Question &

Answer

Thank you

www.mikrotiktutorial.com