

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



documentation

Main Page
Recent changes

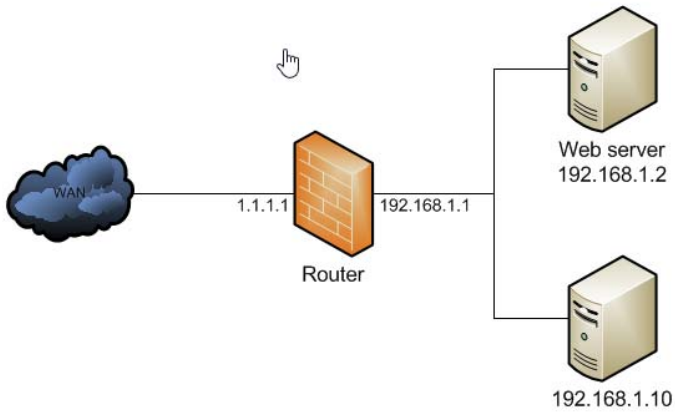
Tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Page [Discussion](#) [Read](#) [View source](#) [View history](#)

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.

Source IP	Destination IP
2.2.2.2	1.1.1.1

Step 1

Hairpin NAT on Mikrotik WIKI

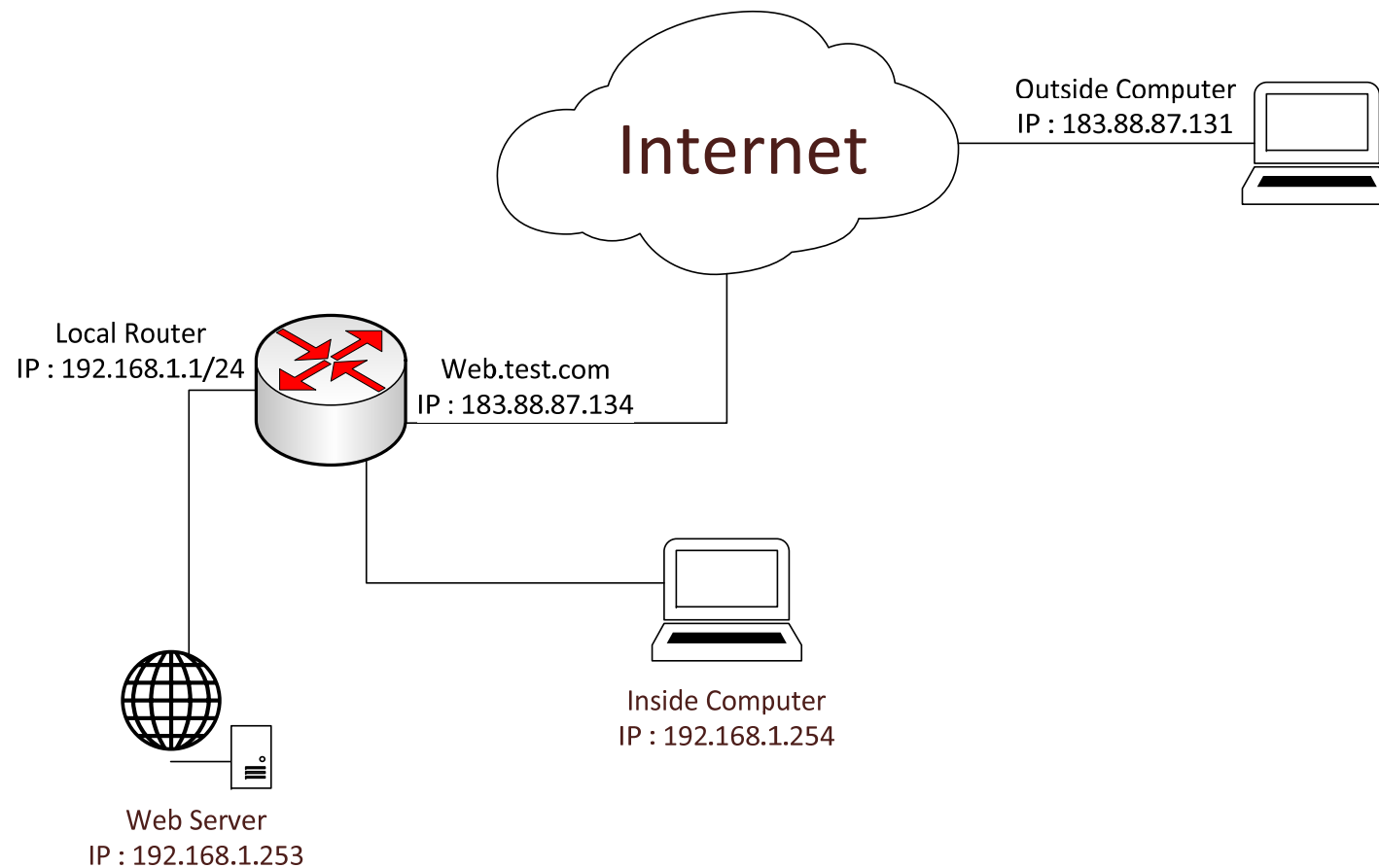
The client receives the reply packet, but it discards it because it expects a packet back from 1.1.1.1, and not from 192.168.1.2. As far as the client is concerned the packet is invalid and not related to any connection the client previously attempted to establish.

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 below 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.

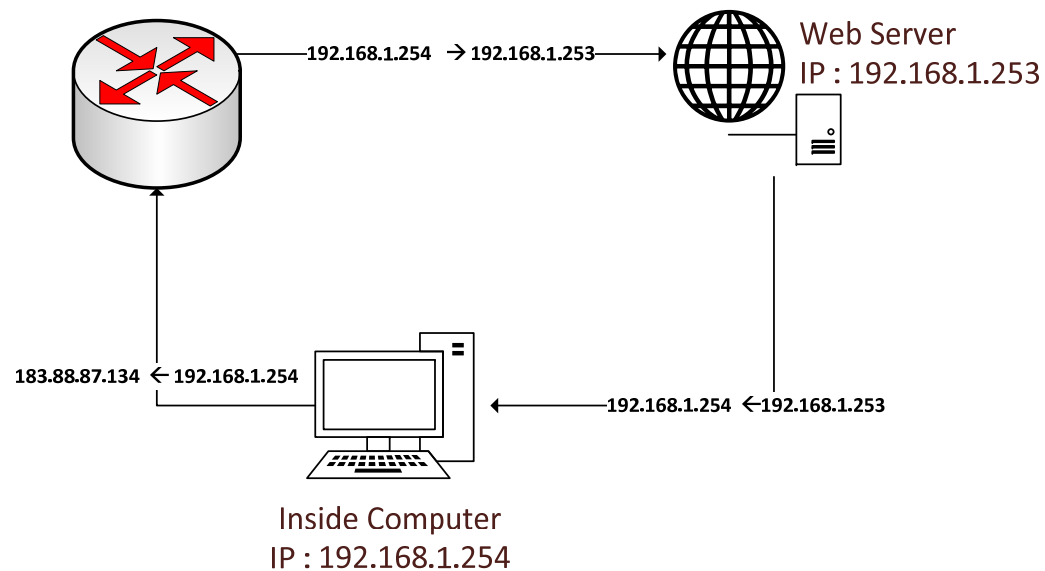
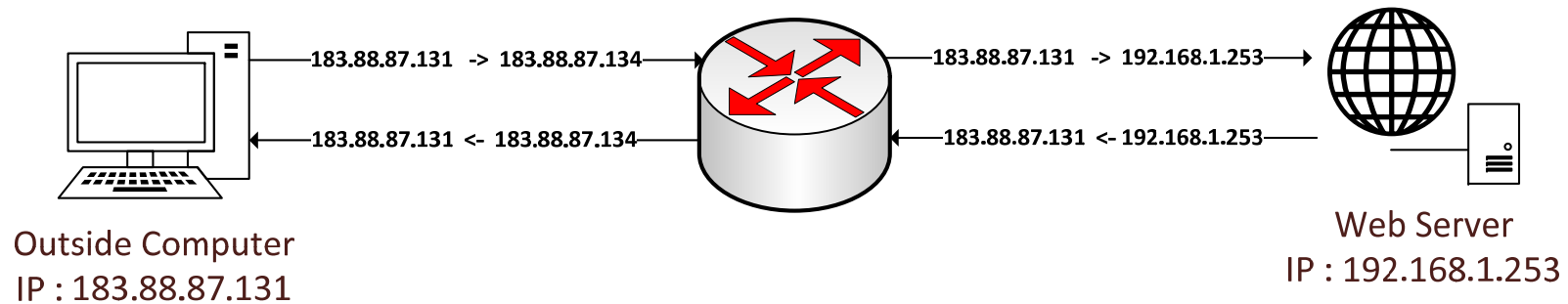
```
/ip firewall nat
add chain=srcnat src-address=192.168.1.0/24 \
    dst-address=192.168.1.2 protocol=tcp dst-port=80 \
    out-interface=LAN action=masquerade
```

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

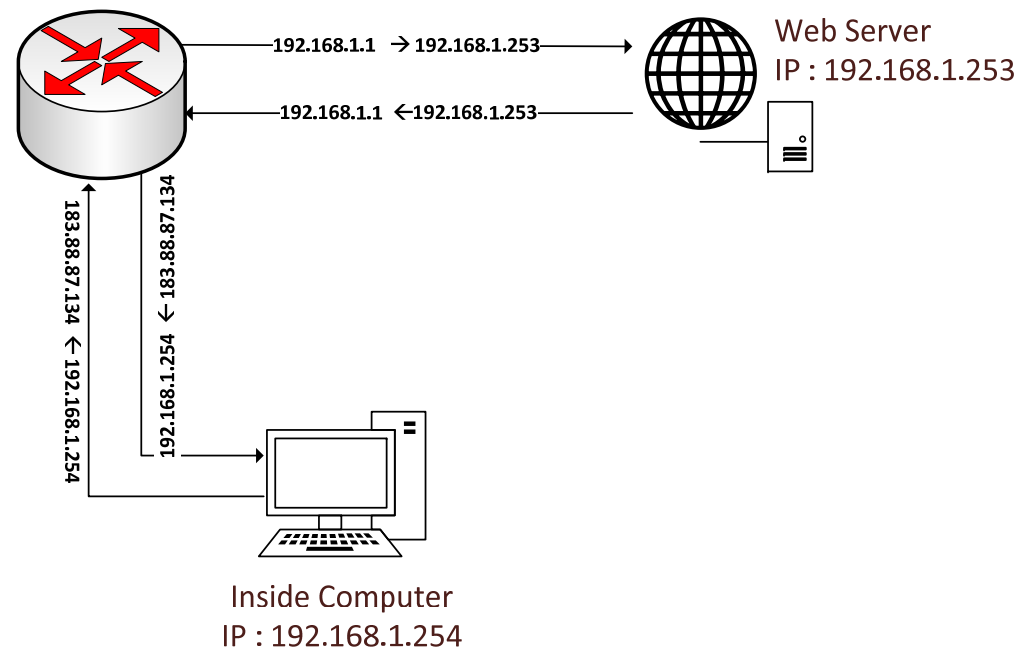
Network Topology



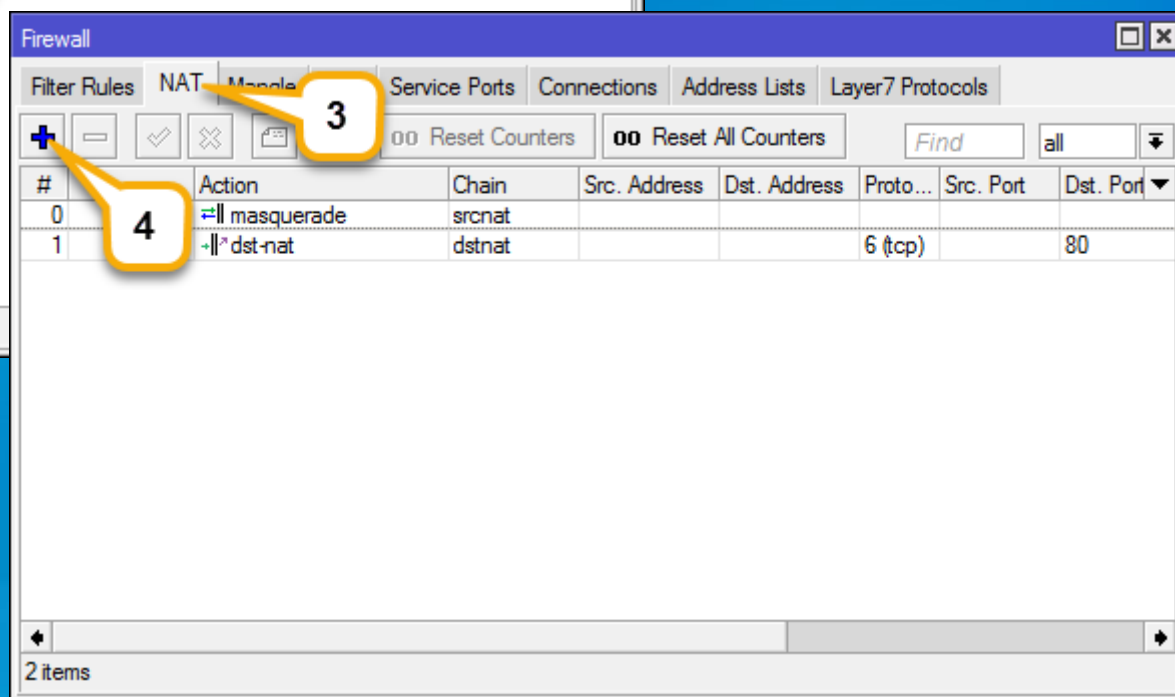
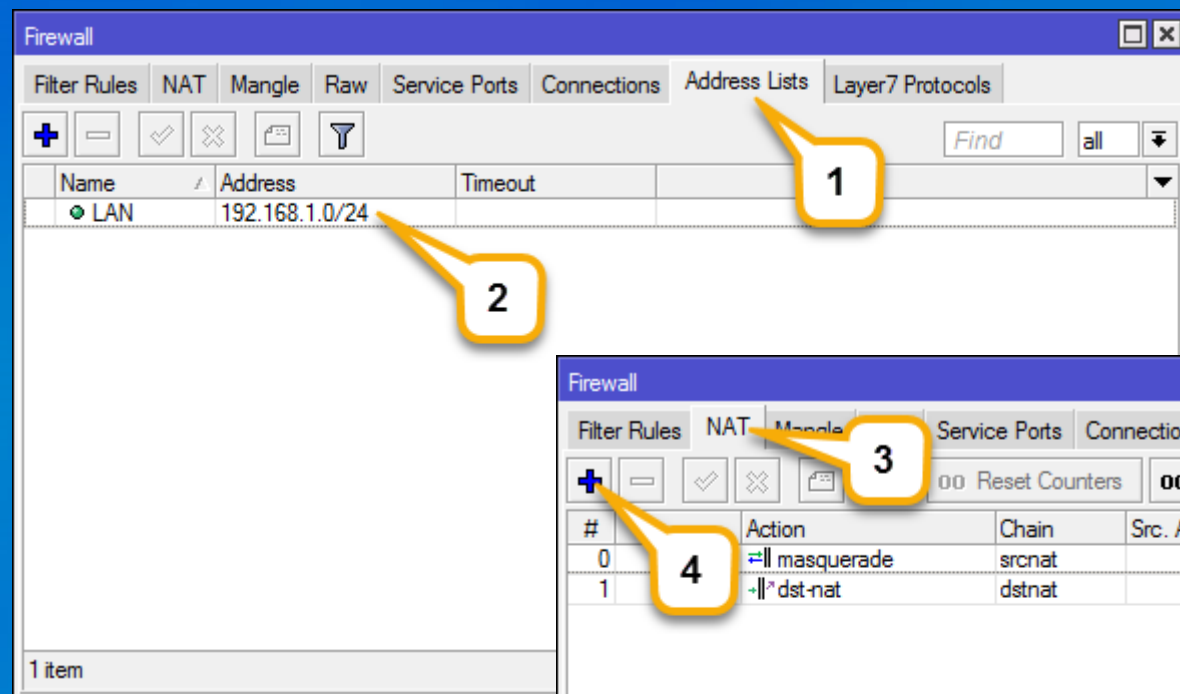
How DST-NAT work



How Hairpin NAT work



Heart of Hairpin NAT



NAT for Hairpin NAT (1)

New NAT Rule

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: LAN

In. Interface List:

Out. Interface List:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New NAT Rule

General Advanced Extra Action Statistics

Src. Address List: LAN

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New NAT Rule

General Advanced Extra Action Statistics

Action: masquerade

☐ Log

Log Prefix:

OK

Cancel

Apply

Disable

Comment

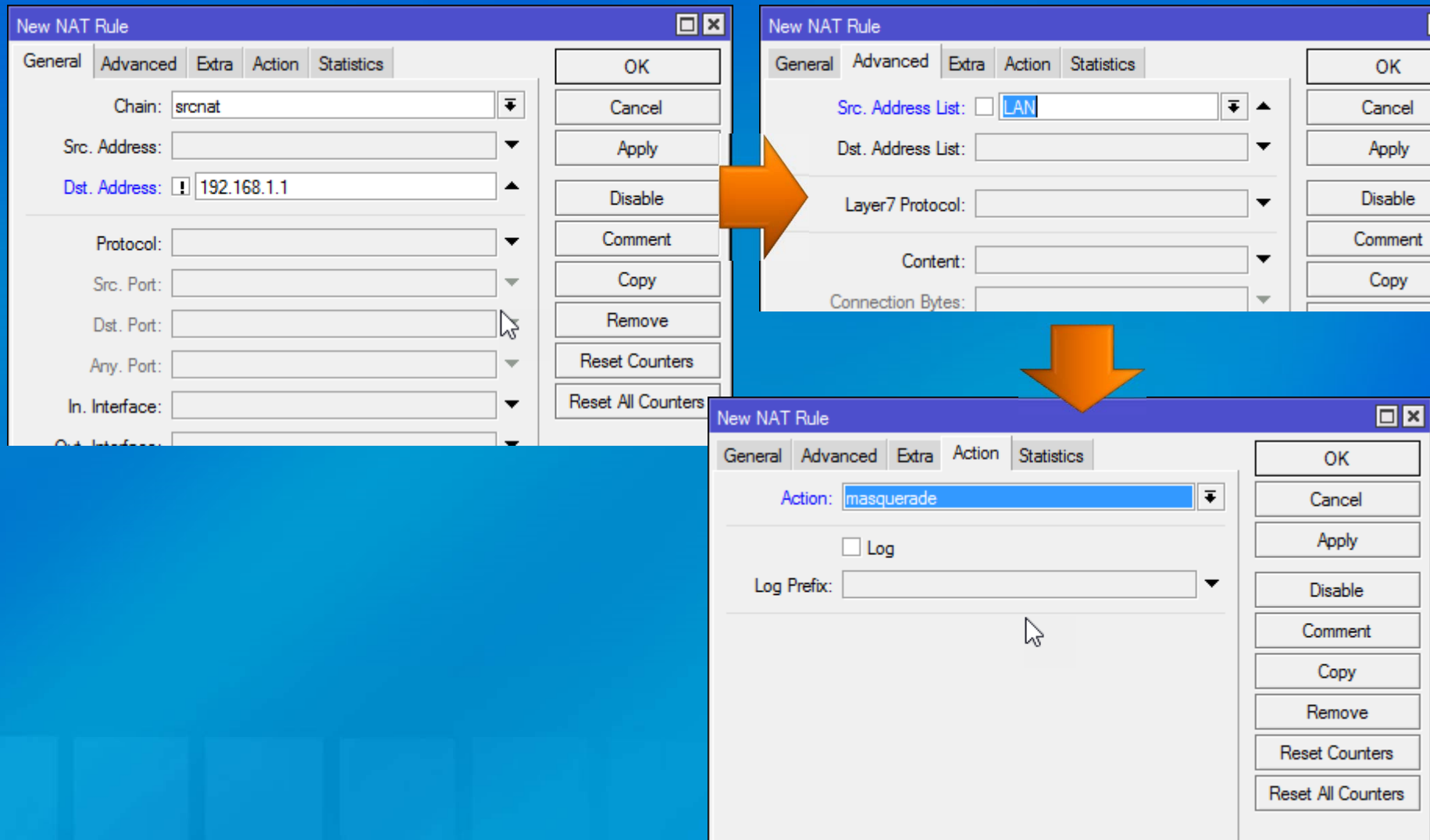
Copy

Remove

Reset Counters

Reset All Counters

NAT for Hairpin NAT (2)



NAT for Hairpin NAT (3)

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters Find 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

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:

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

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

▼ Connection Limit
▼ Limit
▼ Dst. Limit
▼ Nth
▼ Time
▼ Src. Address Type
▼ Dst. Address Type
▼ PSD
▼ Hotspot
▼ IP Fragment

Hairpin NAT

NAT Rule <80>

General Advanced Extra Action Statistics

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

▼ Connection Limit
▼ Limit
▼ Dst. Limit
▼ Nth
▼ Time
▼ Src. Address Type
▲ Dst. Address Type
Address Type: local
☐ Invert
▼ PSD
▼ Hotspot
▼ IP Fragment

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:

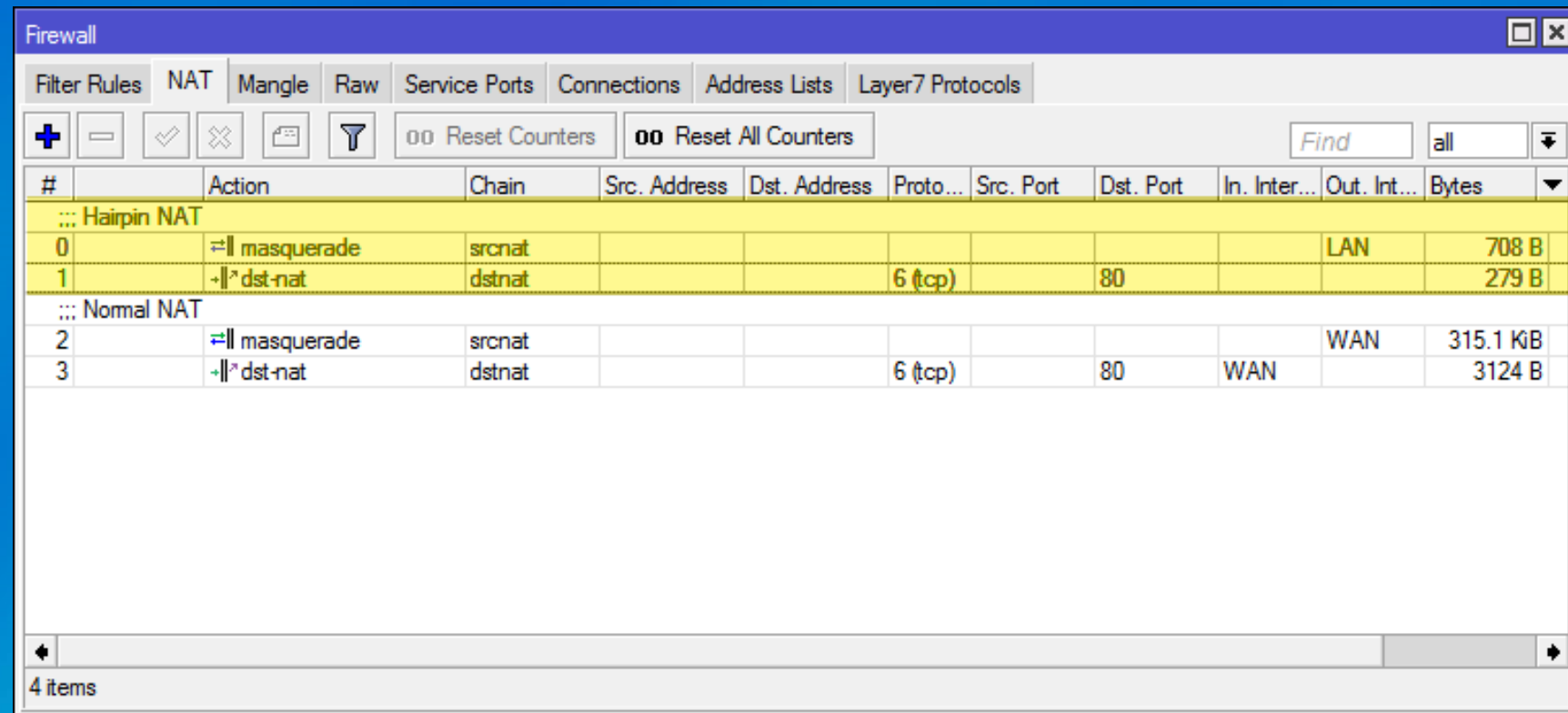
To Addresses:

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 at the top are "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "NAT" tab is selected. Below the tabs are several icons for adding, deleting, and editing rules, along with buttons for "Reset Counters" and "Reset All Counters". A search bar with the text "Find" and a dropdown menu set to "all" is also present. The main area displays a table of NAT rules. The table has columns for #, Action, Chain, Src. Address, Dst. Address, Proto..., Src. Port, Dst. Port, In. Inter..., Out. Int..., and Bytes. There are four rules listed: two under "Hairpin NAT" (rules 0 and 1) and two under "Normal NAT" (rules 2 and 3). Rule 0 is a masquerade rule for the srcnat chain. Rule 1 is a dst-nat rule for the dstnat chain, mapping port 80 to the LAN interface. Rule 2 is a masquerade rule for the srcnat chain, mapping port 80 to the WAN interface. Rule 3 is a dst-nat rule for the dstnat chain, mapping port 80 to the WAN interface. The status bar at the bottom indicates "4 items".

#	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

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