RouterOs Firewall
Massimo Nuvoli
TRAINER #TR0368
MUM Europe 2017 Milan Italy
Massimo Nuvoli (maxnuv)

Owner of Progetto Archivio SRL and DICOBIT

System Engineer
System Architect

Please, call me Max!
First of all..

- at the last Europe MUM..
  my talk was about Switching
  and there was a request

  Please add “hardware spanning tree”
  and from 6.38...
Switch Hardware
Spanning Tree

• Make a switch (as usual)
• Add the master port to a bridge
• Then from the bridge menu IF STP is on then the STP is active on hardware
• Slave ports are shown on the bridge to show the STP status

Look documentation:

Today goals

- Know about firewall design in RouterOs
- Know where is, and what to do with
- Changes of the firewall in the last year
- Two examples
What is a “firewall?”

• Try to isolate the “less protected” outside area from the “more protected” inside area

• It's security device, but own only a firewall is not enough to be protected

• Security is a process, and firewall is only one part of

• The less secure item is between the keyboard and the chair
Cut here to activate firewall :-}
Where is “the firewall”

- L2 firewall
  Bridge → Filter
  Switch → Rule or Access List and other

- L3 (and up) firewall IPv4
  IP → Firewall and IP → Web Proxy

- L3 firewall IPv6
  IPv6 → Firewall
L2 firewall

Take the fight at L2, but not only MAC ADDRESS...

- On switch chipset with ACL (hardware)
- On bridge interface with ACL (software)
RouterOs Packet Flow 1
RouterOs Packet Flow 2

![Diagram showing the packet flow process in RouterOs firewall]

MUM EUROPE 2017 RouterOs Firewall - (c) Massimo Nuvoli
Connection Tracking

- RouterOs can “detect” the status of a connection (TCP/UDP) and try to give us a more powerful way to check packets.
- Connection state can be “new” “established” “related” but also “unknown” or “invalid”.
- Particular protocols (eg SIP and FTP) need “connection helpers” to track complex connections.

/ip firewall connection
L3 firewall IPv4 and IPv6

- Packet flow show “where firewall act”
- Each “position” is a “default chain”
- A “chain” is a set of sequential rules, the order IS important
- Check and action are different in each flow position
- You can jump and also return back on a chain
Filter table

Filter chains can be used to allow and deny connections

- Input
- Output
- Forward

/ip firewall filter
/ipv6 firewall filter
Default filter table

- With connection tracking:
  - accept established/related connections
  - drop invalid connections
  - after we have only “new” connections so no need to check the connection state
  - other rules
Nat table

In the nat chains we can change address and port of connections, only in IPv4

- src nat
- dst nat

/ip firewall nat
Mangle table

The mangle chain is useful to manage all other detail of a connection (e.g. ttl or qos)

- input
- output
- forward
- prerouting
- Postrouting

/ip firewall mangle
/ipv6 firewall mangle
New from 6.36 raw table

- only two chains
- INPUT
- OUTPUT

/ip firewall raw
/ipv6 firewall raw
How to do it better

- use “interface list” and “address list”
- use “jump” and “return”
- define new chains
- define less rules as possible

later we see...
New! “Interface Lists”

- Define a group of interfaces
- `/interface list`
- useful to simplify configuration
Interface lists
## Interface lists

<table>
<thead>
<tr>
<th>List</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan</td>
<td>ether3-lan</td>
</tr>
<tr>
<td>osp</td>
<td>vlan-200-osp</td>
</tr>
<tr>
<td>voip</td>
<td>vlan-300-voip</td>
</tr>
<tr>
<td>wan</td>
<td>pppoe-wan</td>
</tr>
<tr>
<td>wifi</td>
<td>vlan-100-wifi</td>
</tr>
</tbody>
</table>
Address Lists

- Define group of addresses
- I think MANDATORY for IPv6!!
- As “action” address can be added to address lists dynamically, also with time-out
- New from 6.36 dns names can be used in address lists!
Firewall IPv4
Firewall IPv4
Firewall IPv4

**Filter Rules**

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Src. Address</th>
<th>Dst. Address</th>
<th>Proto...</th>
<th>Src. Port</th>
<th>Dst. Port</th>
<th>In. Interface</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>✓ accept established related</td>
<td>✓ input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>✓ drop invalid</td>
<td>✓ input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓ accept icmp</td>
<td>✓ input</td>
<td></td>
<td></td>
<td>1 (ic...)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>✓ accept icmp</td>
<td>✓ input</td>
<td></td>
<td></td>
<td>6 (tcp)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✓ wan2fw</td>
<td>✓ input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NAT**

**Mangle**

**Raw**

**Service Ports**

**Connections**

**Address Lists**

**Layer7 Protocols**
Firewall IPv4
New! “Address Lists”
New! “Address Lists”

Firewall Address List <cedip>

Name: cedip
Address: 192.167.8.0/24
Timeout: 
Creation Time: Mar/27/2017 20:58:42

Options: OK, Cancel, Apply, Disable, Comment, Copy, Remove

enabled
New! “Address Lists”

![Address Lists](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Timeout</th>
<th>Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>cedip</td>
<td>192.167.8.0/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lanip</td>
<td>192.168.7.0/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>myresolvedip</td>
<td>coolname3.mum.it</td>
<td>Mar/27/2017 19:1:13</td>
<td></td>
</tr>
<tr>
<td>; ; ; ; coolname3.mum.it</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>myresolve... 192.168.77.3</td>
<td>Mar/27/2017 22:1:13</td>
<td></td>
</tr>
</tbody>
</table>
New! “Address Lists”

Name: myresolvedip
Address: 192.168.77.3
Timeout:
Creation Time: Mar/27/2017 22:10:58

Dynamic: checked
Enabled: checked
Firewall IPv6
Firewall IPv6
### Firewall IPv6

**IPv6 Firewall**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>✔️ acc...</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>✗ drop</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✔️ acc...</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>⚪️ jump</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>⚪️ jump</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Reset Counters**: Reset counters for selected rules.
- **Reset All Counters**: Reset all counters for all rules.

*Note: The image shows a screenshot of the RouterOS firewall configuration interface, focusing on IPv6 rules.*
Firewall IPv6
Where we can use “lists”? 

- Today only the “check”, not action
Interface Lists
Address Lists
And... improved firewall

- faster “connection-limit”
- raw filter
- interface list
- address list with dns names
- limit (connections, packets, bits)

check the wiki... all there..
Example: routeback
Example: routeback
Goal

- PC with private address C need to talk to the server with private address D
- The server is on DNAT from the address A on the wan side of the router
- Use “dns name” of the server
Routeback!

- First a dnat on the public ip address, and the packet is routed back to the lan
- Then i need a source nat, as the packet must route back to the router and then to the pc
- But... if the public ip address is dynamic?
Address list!

- Configure the “cloud” option, so we have a dns address name with the public ip address
- Configure one address list with this dns name, then use the address list on the destination nat rule!
/ip firewall address-list
add address=coolname3.mum.it list=myresolvedip
/ip firewall filter
add action=accept chain=input comment="accept established related" connection-state=\
established,related
add action=drop chain=input comment="drop invalid" connection-state=invalid
add action=accept chain=input protocol=icmp
add action=drop chain=input comment="drop all from wan" in-interface=pppoe-wan
Sample code part 2

/ip firewall nat
add action=masquerade chain=srcnat comment="normal masq" out-interface=pppoe-wan
add action=dst-nat chain=dstnat comment="nat to 192.168.7.2" dst-address-list=myresolvedip \
to-addresses=192.168.7.2
add action=src-nat chain=srcnat comment="routeback from 192.168.90.0/24 to lan (eq lan to lan)" \
out-interface=ether3-lan src-address=192.168.7.0/24 to-addresses=192.168.7.1
A complex firewall

- One wan
- More than one lan
- Define and update frequently all rules
- Avoid to hard code all
All code here...
address list

/ip firewall address-list
add address=coolname3.mum.it list=myresolvedip
add address=192.168.7.0/24 list=lanip
add address=192.167.8.0/24 list=cedip
/ip firewall filter
add action=accept chain=input comment="accept established related" \ connection-state=established,related
add action=drop chain=input comment="drop invalid" connection-state=invalid
add action=accept chain=input comment="accept icmp" protocol=icmp
add action=accept chain=input port=8291 protocol=tcp
add action=jump chain=input comment=wan2fw in-interface-list=wan jump-target=\ wan2fw
add action=jump chain=input comment=wifi2fw in-interface-list=wifi jump-target=\ wifi2fw
add action=jump chain=input comment=osp2fw in-interface-list=osp jump-target=\ osp2fw
add action=jump chain=input comment=voip2fw in-interface-list=voip jump-target=\ voip2fw
add action=accept chain=forward comment="accept established related" \ 
    connection-state=established,related
add action=drop chain=forward comment="drop invalid" \ 
    connection-state=invalid
add action=jump chain=forward comment="filtro icmp" \ 
    jump-target=accept-icmp protocol=icmp
add action=jump chain=forward comment="lan (ip) to wan" disabled=yes \ 
    in-interface-list=lan jump-target=lan out-interface-list=wan \ 
    src-address-list=lanip
add action=jump chain=forward comment="ced (ip) to wan" disabled=yes \ 
    in-interface-list=lan jump-target=lan out-interface-list=wan \ 
    src-address-list=cedip
add action=jump chain=forward in-interface-list=lan jump-target=lan2wan \           out-interface-list=wan
add action=jump chain=forward in-interface-list=lan jump-target=lan2voip \           out-interface-list=voip
add action=jump chain=forward in-interface-list=lan jump-target=lan2osp \           out-interface-list=osp
add action=jump chain=forward in-interface-list=osp jump-target=osp2wan \           out-interface-list=wan
add action=jump chain=forward in-interface-list=voip jump-target=voip2wan \           out-interface-list=wan
add action=jump chain=forward in-interface-list=voip jump-target=voip2lan \           out-interface-list=lan
add action=jump chain=forward in-interface-list=wan jump-target=wan2lan \           out-interface-list=lan
All code here...
zone to zone

add action=drop chain=lan2osp comment="default drop"
add action=drop chain=lan2voip comment="default drop"
add action=drop chain=forward comment="default drop all2all"
add action=drop chain=input comment="drop all2fw" log-prefix=all2fw
add action=drop chain=voip2fw comment="default drop"
add action=drop chain=voip2lan comment="default drop"
add action=drop chain=voip2wan comment="default drop"
add action=drop chain=wan2lan comment="default drop"
add action=jump chain=wifi2fw comment="accept dns" jump-target=accept-dns
add action=drop chain=wifi2fw comment="default drop"
add action=jump chain=lan2wan jump-target=accept-dns
add action=drop chain=lan2wan comment="default drop"
add action=jump chain=wlan2fw comment="protect ssh" jump-target=ssh
add action=drop chain=wlan2fw comment="drop all from wan"
All code here...

dns check

add action=accept chain=accept-dns dst-port=53 protocol=udp

add action=accept chain=accept-dns dst-port=53 protocol=tcp

add action=return chain=accept-dns
add action=accept chain=accept-icmp comment="echo reply" icmp-options=0:0 protocol=icmp
add action=accept chain=accept-icmp comment="net unreachable" icmp-options=3:0 protocol=icmp
add action=accept chain=accept-icmp comment="host unreachable" icmp-options=3:1 protocol=icmp
add action=accept chain=accept-icmp comment="host unreachable fragmentation required" icmp-options=3:4 protocol=icmp
add action=accept chain=accept-icmp comment="allow source quench" icmp-options=4:0 protocol=icmp
add action=accept chain=accept-icmp comment="allow echo request" icmp-options=8:0 protocol=icmp
add action=accept chain=accept-icmp comment="allow time exceed" icmp-options=11:0 protocol=icmp
add action=accept chain=accept-icmp icmp-options=12:0 protocol=icmp
add action=drop chain=accept-icmp comment="deny all other types"
add action=drop chain=ssh comment="drop ssh brute forcers" dst-port=22 protocol=tcp src-address-list=badip

add action=add-src-to-address-list address-list=badip address-list-timeout=1w3d chain=ssh dst-port=22 protocol=tcp src-address-list=ssh_stage3

add action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m chain=ssh dst-port=22 protocol=tcp src-address-list=ssh_stage2

add action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m chain=ssh dst-port=22 protocol=tcp src-address-list=ssh_stage1

add action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m chain=ssh dst-port=22 protocol=tcp

add action=return chain=ssh
All code here...

icmp check

/ip firewall nat

add action=masquerade chain=srcnat out-interface=pppoe-wan

/ip firewall raw

add action=drop chain=prerouting comment="drop bad ip" in-interface-list=wan \ 
src-address-list=badip
What you've seen

- Compex firewall
- And configuration can be exported and imported to another routerboard, with NO ERROR
- And all “specific” configuration is on the “interface lists” and “address lists”
- Recycle firewall rules
This year request

- Complete IPv6 firewall
- Please add some kind of “global” generic constant values like objects
- IP addresses
- Ports
Questions?
Thank you!

massimo@dicobit.it