Review of DHCPv6-PD on VyOS 1.3-rc1

Ray Patrick Soucy
rps@soucy.org

VyOS 1.2 made a lot of progress on IPv6 support, especially for firewalling, and while I use it at work, I haven't been able to run it for my home network due to a lack of DHCPv6-PD support. VyOS 1.3-rc1 (release candidate) is out now and one of the features it provides is DHCPv6-PD support.

It's not very well documented yet, though, and some of the configuration is unobvious, so I thought I would share a quick step-by-step guide.

First a few notes:

- DHCPv6-PD support isn't far enough along yet to provide a lot of flexibility in how you configure internal addressing, so for now if you run DHCPv6-PD on VyOS it will be limited to SLAAC addressing.

- Accepting IPv6 router advertisements is off by default on VyOS (which is appropriate for a router). Even if you use DHCPv6 and DHCPv6-PD for addressing on your WAN interface, you still need to enable receiving RA's to learn your default route.

- For DNS server information, we support RDNSS in router advertisements, but some clients only support DNS information through DHCPv6. We will configure both in our setup.

- We use Google public DNS in our example.

- My ISP doesn't use PPPoE, so I haven't tested DHCPv6-PD support with it.

Setup Details

For this project we're using a Supermicro E102-9AP-L which is a dual-core Atom E3930 1.8 GHz with two onboard Gigabit interfaces. This has been paired with an 8GB SODIMM and 250GB M.2 SATA SSD.

This isn't the latest and greatest, but the build cost came in at under $350 (USD) including shipping and it's more than enough for my cable service.

We will use port 1 (eth0) for our WAN and port 2 (eth1) for our LAN.

Part 1: Interface Configuration

NOTE: This guide assumes a basic understanding of VyOS configuration (entering configuration mode, using set and delete statements, etc.)

Before you configure DHCPv6-PD, we need to make sure that we can get an IPv6 address. In my case, this means enabling DHCP, DHCPv6, and accepting IPv6 router advertisements on the WAN interface:

```
# Use DHCP for IPv4
set interfaces ethernet eth0 address 'dhcp'

# Use DHCP for IPv6
# DHCPv6 does not provide default-gateway information, so enabling autoconf is required
set interfaces ethernet eth0 ipv6 address autoconf
set interfaces ethernet eth0 address 'dhcpv6'
```

Optionally, you can manually set your DHCPv6 client DUID. I prefer to do so using a Type 4 DUID based on `/etc/machine-id` so I always know exactly what my DUID will be. This can be generated by prefixing 0004 to the value in /etc/machine-id and adding a colon every two characters:

```
echo 0004`cat /etc/machine-id` | sed 's/../&:/g;s/:$//'
```

Example:

```
cat /etc/machine-id
ceaf52cf6bc748e49dee3e773d69bf54

echo 0004`cat /etc/machine-id`
0004ceaf52cf6bc748e49dee3e773d69bf54

echo 0004`cat /etc/machine-id` | sed 's/../&:/g;s/:$//'
```

```
00:04:ce:af:52:cf:6b:c7:48:e4:9d:ee:3e:77:3d:69:bf:54
```

The last value, is what we will configure in VyOS as our DHCPv6 client DUID:

```
set interfaces ethernet eth0 dhcpv6-options duid '00:04:ce:af:52:cf:6b:c7:48:e4:9d:ee:3e:77:3d:69:bf:54'
```

Feature Request: Add a `set interfaces ethernet eth0 dhcpv6-options duid uuid` option to do this automatically.

Upon commit, you should be able to verify IPv6 connectivity:

```
show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             67.251.8.52/21                    u/u  WAN
                 2604:6000:9cf0:9a:a57e:15f5:ee33:38a9/128
eth1             192.168.1.1/24                    u/u  LAN
lo               127.0.0.1/8                       u/u
                 ::1/128

show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* ::/0 [0/1024] via fe80::217:10ff:fe91:2d14, eth0, 00:45:37
C>* 2604:6000:9cf0:9a:a57e:15f5:ee33:38a9/128 is directly connected, eth0, 00:45:33
C * fe80::/64 is directly connected, eth1, 00:45:35
C * fe80::/64 is directly connected, eth0, 00:45:37
C>* fe80::/64 is directly connected, lo, 00:45:44
```

```
ping www.google.com count 3
PING www.google.com(lga34s15-in-x04.1e100.net (2607:f8b0:4006:811::2004)) 56 data bytes
64 bytes from lga34s15-in-x04.1e100.net (2607:f8b0:4006:811::2004): icmp_seq=1 ttl=116 time=46.3 ms
64 bytes from lga34s15-in-x04.1e100.net (2607:f8b0:4006:811::2004): icmp_seq=2 ttl=116 time=51.1 ms
64 bytes from lga34s15-in-x04.1e100.net (2607:f8b0:4006:811::2004): icmp_seq=3 ttl=116 time=39.7 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 39.671/45.693/51.129/4.702 ms
```

Next we'll configure DHCPv6-PD to request a routed IPv6 prefix that we can use for downstream networks.

In my case, my ISP supports prefix hinting, so I can request a 56-bit, rather than a 64-bit, prefix allowing me to configure multiple networks. We will only configure one network for now, but it's nice to have the option to create additional networks in the future without having to change our prefix.

```
set interfaces ethernet eth0 dhcpv6-options pd 0 length '56'
set interfaces ethernet eth0 dhcpv6-options pd 0 interface eth1 sla-id '0'
set interfaces ethernet eth0 dhcpv6-options pd 0 interface eth1 address '1'
set interfaces ethernet eth0 dhcpv6-options rapid-commit
```

Here the `sla-id` is used to determine the prefix ID that will be used for the 64-bit prefix assigned to our LAN interface, and the address is the 64-bit host segment that will be used for the host address.

Note the configured value in each case is in decimal, not hex, so for a 56-bit prefix, the 8-bit sub-prefix of `00` would be configured as 0, and `FF` would be configured as 255. And for an address of `::FFFF` we would configure 65535

Feature Request: Make the configuration for `sla-id` and `address` hexadecimal and do the conversion behind the scenes.

Once configured, DHCPv6 should assign a prefix to our LAN interface upon acquiring an address:

```
show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             67.251.8.52/21                    u/u  WAN
                 2604:6000:9cf0:9a:a57e:15f5:ee33:38a9/128
eth1             192.168.1.1/24                    u/u  LAN
                 2603:7080:f440:50f0::1/64
lo               127.0.0.1/8                       u/u
                 ::1/128
```

Part 2: Router Advertisement and Host Addressing

For IPv6, either State-Less Address Auto-Configuration (SLAAC) or DHCPv6 can be used for host addressing, but both options require IPv6 router advertisements. A common misconception with DHCPv6 is that it is an alternative to router advertisements, but in fact the two are designed to work together.
The VyOS implementation of DHCPv6-PD doesn't support populating a dynamic configuration object with the assigned prefix, or other configuration such as DNS servers provided by the ISP. The result is we can't configure other services, such as DHCPv6, to use that information in a reliable way. This means our addressing method is limited to SLAAC for now.

Feature Request: Create dynamic configuration variables and network objects populated by DHCPv6-PD that can be used for service and firewall configuration.

Through router advertisements, we can provide DNS server information using RDNSS.

Not every client supports RDNSS, though. So we will also configure a stateless DHCPv6 server instance to hand out DNS information so that clients have both options.

Here is our IPv6 RA configuration for our LAN interface.

NOTE: Don't configure IPv6 RA on your WAN interface as this may cause problems for your ISP if they don't guard against it.

```
set service router-advert interface eth1 default-lifetime '300'
set service router-advert interface eth1 default-preference 'high'
set service router-advert interface eth1 hop-limit '64'
set service router-advert interface eth1 interval max '30'
set service router-advert interface eth1 link-mtu '1500'
set service router-advert interface eth1 name-server '2001:4860:4860::8888'
set service router-advert interface eth1 name-server '2001:4860:4860::8844'
```

```
set service router-advert interface eth1 other-config-flag
set service router-advert interface eth1 prefix ::/64 preferred-lifetime '300'
set service router-advert interface eth1 prefix ::/64 valid-lifetime '900'
set service router-advert interface eth1 reachable-time '900000'
set service router-advert interface eth1 retrans-timer '0'
```

The key here is to use `::/64` as our prefix. This is a special value interpreted by the RA service that means first available global scope prefix.

Feature Request: Update configuration to support `default` instead of `::/64` for `router-advert`, making it more obvious and providing help in the CLI to point users in the right direction.

The `other-config-flag` option is used to hint to hosts that DHCPv6 should be used for requesting other information. It is not needed if you don't plan to run DHCPv6 for DNS.

If you only plan to use DHCPv6 for DNS, and don't wish to use RDNSS, you can omit the `name-server` configuration here.

Next we'll configure a DHCPv6 server to provide DNS information only. The challenge here is that the DHCPv6 server needs to have at least one prefix defined in its configuration to determine which network interfaces to listen on. Since the LAN prefix is provided by DHCPv6-PD and dynamic, we don't know it ahead of time.

A work-around to this is to define an empty prefix block using the link-local address of the LAN interface as shown here:

```
set service dhcpv6-server preference '255'
set service dhcpv6-server shared-network-name LAN common-options domain-search 'lan.private'
set service dhcpv6-server shared-network-name LAN common-options name-server '2001:4860:4860::8888'
set service dhcpv6-server shared-network-name LAN common-options name-server '2001:4860:4860::8844'
set service dhcpv6-server shared-network-name LAN subnet fe80::ae1f:6bff:fe67:c1ff/128
```

Feature Request: For DHCPv6 stateless configurations support a `stateless-interface` configuration directive that configures an empty subnet block with the link-local address to make this more obvious.

With this configured, we now support both RDNSS and DHCPv6 for DNS server information. In our case we're using Google Public DNS servers.

At this point, clients should have IPv6 addresses and be able to get online.

Part 3: IPv6 Firewall Policy

IPv6 and specifically ICMPv6 are complicated, and not a lot of good documentation exists on creating firewall policy for either. As a cybersecurity engineer I take pause each time I hear someone insist that you must not block ICMPv6 under any circumstances. This is a knee-jerk reaction to people blindly blocking all ICMP traffic for IPv4 and thinking they will do the same for IPv6. Yes, there are specific messages you must not block for ICMPv6, but there are also a lot of message types that are not necessary which increase the attack surface.

Here is the IPv6 firewall policy I recommend, which filters ICMPv6 to only what is required, and goes a step further by limiting link-local ICMPv6 such as neighbor discovery, to only be permitted on-link through matching of the IPv6 Hop Limit (IPv6 equivalent of IPv4 TTL).

For this approach, we will create four rulesets, policy for local traffic on each the WAN and LAN interfaces (note they require different policy), and policy for traffic forwarded through the LAN interface in the IN and OUT direction.

This policy makes use of two IPv6 network group objects, one usually empty, as a pre-defined blacklist to quickly terminate unwanted traffic in either direction, across all policies, and another to define the list of IPv6 addresses or networks which are permitted to connect to VyOS for management, e.g. SSH.

```
set firewall group ipv6-network-group NET-6-BLACKLIST
set firewall group ipv6-network-group NET-6-MANAGEMENT
```

Next we define local policy for our WAN interface, which we will name `OUTSIDE-6-LOCAL`

```
set firewall ipv6-name OUTSIDE-6-LOCAL default-action 'drop'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 100 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 100 source group network-group 'NET-6-BLACKLIST'
```

```
set firewall ipv6-name OUTSIDE-6-LOCAL rule 101 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 101 destination group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 state established 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 state related 'enable'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 111 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 111 state invalid 'enable'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 icmpv6 type '1'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 icmpv6 type '2'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 icmpv6 type '3'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 icmpv6 type '4'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 icmpv6 type '128'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 hop-limit eq '1'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 icmpv6 type '130'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 protocol 'ipv6-icmp'
```

```
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 icmpv6 type '134'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 icmpv6 type '135'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 icmpv6 type '136'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 protocol 'ipv6-icmp'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 destination port '546'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 protocol 'udp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 source port '547'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 destination port '22'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 protocol 'tcp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 recent count '4'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 recent time '60'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 state new 'enable'

set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 destination port '22'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 protocol 'tcp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 state new 'enable'
```

```
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 log 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 protocol 'ipv6-icmp'
```

The following restrictions are in place:

- Drop any address found in the `NET-6-BLACKLIST` network object
- Allow established and related traffic, drop invalid traffic (connection state tracking)
- ICMPv6 types 1 through 4 are permitted
- ICMPv6 type 128 (echo-request) is permitted (optional but recommended)
- ICMPv6 type 130 for MLD query (multicast) is permitted, but only with a hop-limit of 1 per RFC 3810
- ICMPv6 type 134 (router-advertisement) is permitted, but only with a hop-limit of 255 to ensure on-link
    - Important Note: Type 134 will be permitted on WAN interfaces where you want VyOS to discover IPv6 routers, but type 133 will be permitted on LAN interfaces where you want VyOS to act as the router.
- ICMPv6 type 135 and 136 for neighbor discovery, but only with a hop-limit of 255 to ensure on-link
- DHCPv6 responses, UDP source port 547 and destination port 546.
- Allow SSH from addresses in the `NET-6-MANAGEMENT` group, but limit connections to 4 new connections per minute to mitigate brute-force attempts.
- Log any ICMPv6 drops so that we know about them.

Next, we create a similar policy for our LAN interface called INSIDE-6-LOCAL

```
set firewall ipv6-name INSIDE-6-LOCAL default-action 'drop'

set firewall ipv6-name INSIDE-6-LOCAL rule 100 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 100 source group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name INSIDE-6-LOCAL rule 101 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 101 destination group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name INSIDE-6-LOCAL rule 110 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 110 state established 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 110 state related 'enable'

set firewall ipv6-name INSIDE-6-LOCAL rule 111 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 111 state invalid 'enable'

set firewall ipv6-name INSIDE-6-LOCAL rule 120 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 120 icmpv6 type '1'
set firewall ipv6-name INSIDE-6-LOCAL rule 120 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 121 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 121 icmpv6 type '2'
set firewall ipv6-name INSIDE-6-LOCAL rule 121 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 122 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 122 icmpv6 type '3'
set firewall ipv6-name INSIDE-6-LOCAL rule 122 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 123 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 123 icmpv6 type '4'
set firewall ipv6-name INSIDE-6-LOCAL rule 123 protocol 'ipv6-icmp'
```

```
set firewall ipv6-name INSIDE-6-LOCAL rule 124 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 124 icmpv6 type '128'
set firewall ipv6-name INSIDE-6-LOCAL rule 124 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 125 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 hop-limit eq '1'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 icmpv6 type '143'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 126 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 hop-limit eq '255'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 icmpv6 type '133'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 127 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 hop-limit eq '255'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 icmpv6 type '135'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 128 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 hop-limit eq '255'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 icmpv6 type '136'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 protocol 'ipv6-icmp'

set firewall ipv6-name INSIDE-6-LOCAL rule 130 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 destination port '547'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 protocol 'udp'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 source port '546'

set firewall ipv6-name INSIDE-6-LOCAL rule 140 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 140 destination port '53'
set firewall ipv6-name INSIDE-6-LOCAL rule 140 protocol 'tcp_udp'
```

```
set firewall ipv6-name INSIDE-6-LOCAL rule 150 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 150 destination port '123'
set firewall ipv6-name INSIDE-6-LOCAL rule 150 protocol 'udp'

set firewall ipv6-name INSIDE-6-LOCAL rule 200 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 destination port '22'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 protocol 'tcp'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 state new 'enable'

set firewall ipv6-name INSIDE-6-LOCAL rule 800 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 800 source address 'fe80::ae1f:6bff:fe67:c1ff'

set firewall ipv6-name INSIDE-6-LOCAL rule 900 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 900 log 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 900 protocol 'ipv6-icmp'
```

This policy implements the same restrictions as our outside policy with the following changes:

- Rule 125 changes ICMPv6 type 130 to 143 for IPv6 MLDv6 listener reports
- Rule 126 changes ICMPv6 type 134 (router-advertisement) to 133 (router-solicitation), since we are the router for inside interfaces.
- Rule 130 reverses the source and destination ports for DHCPv6 since we are the server instead of the client.
- Optional exceptions for DNS (TCP and UDP port 53) and NTP (UDP port 123) are added. Only needed if you plan to point clients at the VyOS instance for these services.
- An exception is put in place at rule 800 to drop traffic sourced from the routers own link-local address to avoid excessive ICMPv6 logging generated by seeing the routers own multicast traffic.

Next, our policy for our LAN interface. A personal preference of mine is to apply forwarding firewall policy on the user-facing interface rather than the WAN interface. This allows you to filter between internal networks when you have multiple in use (for example, creating a guest network, or zero-trust network). In this model, because firewall policy is always applied to all inside interfaces, there is no need for forwarding (`in` and `out`) policy on the WAN interface.

Note that if you want to apply policy on the WAN interface instead, you would need to reverse the policy definitions to reflect the correct directions. Using policy on the LAN interface all traffic using the `in` direction is trusted, but if that were changed to the WAN interface you would need to change it to `out`.

Our LAN out policy will be named `LAN-6-OUT`

```
set firewall ipv6-name LAN-6-OUT default-action 'drop'

set firewall ipv6-name LAN-6-OUT rule 100 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 100 source group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name LAN-6-OUT rule 101 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 101 destination group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name LAN-6-OUT rule 110 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 110 state established 'enable'
set firewall ipv6-name LAN-6-OUT rule 110 state related 'enable'

set firewall ipv6-name LAN-6-OUT rule 111 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 111 state invalid 'enable'

set firewall ipv6-name LAN-6-OUT rule 120 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 120 icmpv6 type '1'
set firewall ipv6-name LAN-6-OUT rule 120 protocol 'ipv6-icmp'
```

```
set firewall ipv6-name LAN-6-OUT rule 121 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 121 icmpv6 type '2'
set firewall ipv6-name LAN-6-OUT rule 121 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-OUT rule 122 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 122 icmpv6 type '3'
set firewall ipv6-name LAN-6-OUT rule 122 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-OUT rule 123 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 123 icmpv6 type '4'
set firewall ipv6-name LAN-6-OUT rule 123 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-OUT rule 124 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 124 icmpv6 type '128'
set firewall ipv6-name LAN-6-OUT rule 124 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-OUT rule 900 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 900 log 'enable'
set firewall ipv6-name LAN-6-OUT rule 900 protocol 'ipv6-icmp'
```

This implements the following restrictions:

- Drop any address found in the `NET-6-BLACKLIST` network object
- Allow established and related traffic, drop invalid traffic (connection state tracking)
- ICMPv6 types 1 through 4 are permitted
- ICMPv6 type 128 (echo-request) is permitted (optional but recommended)
- All other ICMPv6 traffic is dropped, but logged so we know about it.

If you want to allow incoming connections into your network, for example hosting a web server, you would need to add exceptions for that traffic in this policy. By default we trust nothing.

Out policy for LAN in is named LAN-6-IN

```
set firewall ipv6-name LAN-6-IN default-action 'drop'

set firewall ipv6-name LAN-6-IN rule 100 action 'drop'
set firewall ipv6-name LAN-6-IN rule 100 source group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name LAN-6-IN rule 101 action 'drop'
set firewall ipv6-name LAN-6-IN rule 101 destination group network-group 'NET-6-BLACKLIST'

set firewall ipv6-name LAN-6-IN rule 110 action 'accept'
set firewall ipv6-name LAN-6-IN rule 110 state established 'enable'
set firewall ipv6-name LAN-6-IN rule 110 state related 'enable'

set firewall ipv6-name LAN-6-IN rule 111 action 'drop'
set firewall ipv6-name LAN-6-IN rule 111 state invalid 'enable'

set firewall ipv6-name LAN-6-IN rule 900 action 'accept'
set firewall ipv6-name LAN-6-IN rule 900 log 'enable'
set firewall ipv6-name LAN-6-IN rule 900 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-IN rule 990 action 'accept'
set firewall ipv6-name LAN-6-IN rule 990 state new 'enable'
```

This policy implements the following:

- Drop any address found in the `NET-6-BLACKLIST` network object
- Allow established and related traffic, drop invalid traffic (connection state tracking)
- Accept and log all ICMPv6
- Accept all traffic. Normally this would be scoped to the IPv6 prefix for the LAN, but because VyOS DHCPv6-PD doesn't create an object to allow for that, the source restriction is omitted.

If you wanted a more restrictive policy (such as zero-trust) you could implement restrictions on what traffic is allowed to leave your LAN here.

Remember `in` and `out` are from the perspective of the router, so out means traffic from the router to the LAN in this context.

Finally, we assign the policy to our interfaces:

```
set interfaces ethernet eth0 firewall local ipv6-name 'OUTSIDE-6-LOCAL'

set interfaces ethernet eth1 firewall local ipv6-name 'INSIDE-6-LOCAL'
set interfaces ethernet eth1 firewall in ipv6-name 'LAN-6-IN'
set interfaces ethernet eth1 firewall out ipv6-name 'LAN-6-OUT'
```

Note: take care to add addresses to the `NET-6-MANAGEMENT` group as appropriate so you don’t lock yourself out.

Appendix

Full working configuration for both IPv4 and IPv6

```
## Firewall Global Options

set firewall all-ping 'enable'
set firewall broadcast-ping 'disable'
set firewall config-trap 'disable'
set firewall ipv6-receive-redirects 'disable'
set firewall ipv6-src-route 'disable'
set firewall ip-src-route 'disable'
set firewall log-martians 'enable'
set firewall receive-redirects 'disable'
set firewall send-redirects 'disable'
set firewall source-validation 'disable'
set firewall syn-cookies 'enable'
set firewall twa-hazards-protection 'disable'

## Firewall Groups

set firewall group ipv6-network-group NET-6-BLACKLIST
set firewall group ipv6-network-group NET-6-MANAGEMENT

set firewall group network-group NET-4-BLACKLIST
set firewall group network-group NET-4-MANAGEMENT network '192.168.1.0/24'

## Firewall Policy IPv6

set firewall ipv6-name INSIDE-6-LOCAL default-action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 100 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 100 source group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name INSIDE-6-LOCAL rule 101 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 101 destination group network-group 'NET-6-BLACKLIST'
```

```
set firewall ipv6-name INSIDE-6-LOCAL rule 110 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 110 state established 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 110 state related 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 111 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 111 state invalid 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 120 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 120 icmpv6 type '1'
set firewall ipv6-name INSIDE-6-LOCAL rule 120 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 121 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 121 icmpv6 type '2'
set firewall ipv6-name INSIDE-6-LOCAL rule 121 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 122 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 122 icmpv6 type '3'
set firewall ipv6-name INSIDE-6-LOCAL rule 122 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 123 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 123 icmpv6 type '4'
set firewall ipv6-name INSIDE-6-LOCAL rule 123 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 124 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 124 icmpv6 type '128'
set firewall ipv6-name INSIDE-6-LOCAL rule 124 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 hop-limit eq '1'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 icmpv6 type '143'
set firewall ipv6-name INSIDE-6-LOCAL rule 125 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 hop-limit eq '255'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 icmpv6 type '133'
set firewall ipv6-name INSIDE-6-LOCAL rule 126 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 hop-limit eq '255'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 icmpv6 type '135'
set firewall ipv6-name INSIDE-6-LOCAL rule 127 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 hop-limit eq '255'
```

```
set firewall ipv6-name INSIDE-6-LOCAL rule 128 icmpv6 type '136'
set firewall ipv6-name INSIDE-6-LOCAL rule 128 protocol 'ipv6-icmp'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 destination port '547'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 protocol 'udp'
set firewall ipv6-name INSIDE-6-LOCAL rule 130 source port '546'
set firewall ipv6-name INSIDE-6-LOCAL rule 140 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 140 destination port '53'
set firewall ipv6-name INSIDE-6-LOCAL rule 140 protocol 'tcp_udp'
set firewall ipv6-name INSIDE-6-LOCAL rule 150 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 150 destination port '123'
set firewall ipv6-name INSIDE-6-LOCAL rule 150 protocol 'udp'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 action 'accept'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 destination port '22'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 protocol 'tcp'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name INSIDE-6-LOCAL rule 200 state new 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 800 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 800 source address 'fe80::ae1f:6bff:fe67:c1ff'
set firewall ipv6-name INSIDE-6-LOCAL rule 900 action 'drop'
set firewall ipv6-name INSIDE-6-LOCAL rule 900 log 'enable'
set firewall ipv6-name INSIDE-6-LOCAL rule 900 protocol 'ipv6-icmp'

set firewall ipv6-name LAN-6-IN default-action 'drop'
set firewall ipv6-name LAN-6-IN rule 100 action 'drop'
set firewall ipv6-name LAN-6-IN rule 100 source group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name LAN-6-IN rule 101 action 'drop'
set firewall ipv6-name LAN-6-IN rule 101 destination group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name LAN-6-IN rule 110 action 'accept'
set firewall ipv6-name LAN-6-IN rule 110 state established 'enable'
set firewall ipv6-name LAN-6-IN rule 110 state related 'enable'
set firewall ipv6-name LAN-6-IN rule 111 action 'drop'
set firewall ipv6-name LAN-6-IN rule 111 state invalid 'enable'
set firewall ipv6-name LAN-6-IN rule 900 action 'accept'
```

```
set firewall ipv6-name LAN-6-IN rule 900 log 'enable'
set firewall ipv6-name LAN-6-IN rule 900 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-IN rule 990 action 'accept'
set firewall ipv6-name LAN-6-IN rule 990 state new 'enable'

set firewall ipv6-name LAN-6-OUT default-action 'drop'
set firewall ipv6-name LAN-6-OUT rule 100 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 100 source group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name LAN-6-OUT rule 101 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 101 destination group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name LAN-6-OUT rule 110 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 110 state established 'enable'
set firewall ipv6-name LAN-6-OUT rule 110 state related 'enable'
set firewall ipv6-name LAN-6-OUT rule 111 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 111 state invalid 'enable'
set firewall ipv6-name LAN-6-OUT rule 120 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 120 icmpv6 type '1'
set firewall ipv6-name LAN-6-OUT rule 120 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-OUT rule 121 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 121 icmpv6 type '2'
set firewall ipv6-name LAN-6-OUT rule 121 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-OUT rule 122 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 122 icmpv6 type '3'
set firewall ipv6-name LAN-6-OUT rule 122 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-OUT rule 123 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 123 icmpv6 type '4'
set firewall ipv6-name LAN-6-OUT rule 123 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-OUT rule 124 action 'accept'
set firewall ipv6-name LAN-6-OUT rule 124 icmpv6 type '128'
set firewall ipv6-name LAN-6-OUT rule 124 protocol 'ipv6-icmp'
set firewall ipv6-name LAN-6-OUT rule 900 action 'drop'
set firewall ipv6-name LAN-6-OUT rule 900 log 'enable'
set firewall ipv6-name LAN-6-OUT rule 900 protocol 'ipv6-icmp'
```

```
set firewall ipv6-name OUTSIDE-6-LOCAL default-action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 100 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 100 source group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 101 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 101 destination group network-group 'NET-6-BLACKLIST'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 state established 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 110 state related 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 111 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 111 state invalid 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 icmpv6 type '1'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 120 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 icmpv6 type '2'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 121 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 icmpv6 type '3'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 122 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 icmpv6 type '4'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 123 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 icmpv6 type '128'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 124 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 hop-limit eq '1'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 icmpv6 type '130'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 125 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 icmpv6 type '134'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 126 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 action 'accept'
```

```
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 icmpv6 type '135'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 127 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 hop-limit eq '255'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 icmpv6 type '136'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 128 protocol 'ipv6-icmp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 destination port '546'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 protocol 'udp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 130 source port '547'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 destination port '22'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 protocol 'tcp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 recent count '4'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 recent time '60'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 140 state new 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 action 'accept'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 destination port '22'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 protocol 'tcp'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 source group network-group 'NET-6-MANAGEMENT'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 141 state new 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 action 'drop'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 log 'enable'
set firewall ipv6-name OUTSIDE-6-LOCAL rule 900 protocol 'ipv6-icmp'

## Firewall Policy IPv4

set firewall name INSIDE-4-LOCAL default-action 'drop'
set firewall name INSIDE-4-LOCAL rule 100 action 'drop'
set firewall name INSIDE-4-LOCAL rule 100 source group network-group 'NET-4-BLACKLIST'
set firewall name INSIDE-4-LOCAL rule 101 action 'drop'
set firewall name INSIDE-4-LOCAL rule 101 destination group network-group 'NET-4-BLACKLIST'
```

```
set firewall name INSIDE-4-LOCAL rule 110 action 'accept'
set firewall name INSIDE-4-LOCAL rule 110 state established 'enable'
set firewall name INSIDE-4-LOCAL rule 110 state related 'enable'
set firewall name INSIDE-4-LOCAL rule 111 action 'drop'
set firewall name INSIDE-4-LOCAL rule 111 state invalid 'enable'
set firewall name INSIDE-4-LOCAL rule 120 action 'accept'
set firewall name INSIDE-4-LOCAL rule 120 icmp type-name 'echo-request'
set firewall name INSIDE-4-LOCAL rule 120 protocol 'icmp'
set firewall name INSIDE-4-LOCAL rule 120 state new 'enable'
set firewall name INSIDE-4-LOCAL rule 129 action 'accept'
set firewall name INSIDE-4-LOCAL rule 129 protocol 'igmp'
set firewall name INSIDE-4-LOCAL rule 130 action 'accept'
set firewall name INSIDE-4-LOCAL rule 130 destination port '67'
set firewall name INSIDE-4-LOCAL rule 130 protocol 'udp'
set firewall name INSIDE-4-LOCAL rule 130 state new 'enable'
set firewall name INSIDE-4-LOCAL rule 140 action 'accept'
set firewall name INSIDE-4-LOCAL rule 140 destination port '53'
set firewall name INSIDE-4-LOCAL rule 140 protocol 'tcp_udp'
set firewall name INSIDE-4-LOCAL rule 140 state new 'enable'
set firewall name INSIDE-4-LOCAL rule 150 action 'accept'
set firewall name INSIDE-4-LOCAL rule 150 destination port '123'
set firewall name INSIDE-4-LOCAL rule 150 protocol 'udp'
set firewall name INSIDE-4-LOCAL rule 150 state new 'enable'
set firewall name INSIDE-4-LOCAL rule 200 action 'accept'
set firewall name INSIDE-4-LOCAL rule 200 destination port '22'
set firewall name INSIDE-4-LOCAL rule 200 protocol 'tcp'
set firewall name INSIDE-4-LOCAL rule 200 source group network-group 'NET-4-MANAGEMENT'
set firewall name INSIDE-4-LOCAL rule 200 state new 'enable'

set firewall name LAN-4-IN default-action 'drop'
set firewall name LAN-4-IN rule 100 action 'drop'
set firewall name LAN-4-IN rule 100 source group network-group 'NET-4-BLACKLIST'
set firewall name LAN-4-IN rule 101 action 'drop'
set firewall name LAN-4-IN rule 101 destination group network-group 'NET-4-BLACKLIST'
```

```
set firewall name LAN-4-IN rule 110 action 'accept'
set firewall name LAN-4-IN rule 110 state established 'enable'
set firewall name LAN-4-IN rule 110 state related 'enable'
set firewall name LAN-4-IN rule 111 action 'drop'
set firewall name LAN-4-IN rule 111 state invalid 'enable'
set firewall name LAN-4-IN rule 120 action 'accept'
set firewall name LAN-4-IN rule 120 icmp type-name 'echo-request'
set firewall name LAN-4-IN rule 120 protocol 'icmp'
set firewall name LAN-4-IN rule 120 state new 'enable'
set firewall name LAN-4-IN rule 990 action 'accept'
set firewall name LAN-4-IN rule 990 state new 'enable'

set firewall name LAN-4-OUT default-action 'drop'
set firewall name LAN-4-OUT rule 100 action 'drop'
set firewall name LAN-4-OUT rule 100 source group network-group 'NET-4-BLACKLIST'
set firewall name LAN-4-OUT rule 101 action 'drop'
set firewall name LAN-4-OUT rule 101 destination group network-group 'NET-4-BLACKLIST'
set firewall name LAN-4-OUT rule 110 action 'accept'
set firewall name LAN-4-OUT rule 110 state established 'enable'
set firewall name LAN-4-OUT rule 110 state related 'enable'
set firewall name LAN-4-OUT rule 111 action 'drop'
set firewall name LAN-4-OUT rule 111 state invalid 'enable'
set firewall name LAN-4-OUT rule 120 action 'accept'
set firewall name LAN-4-OUT rule 120 icmp type-name 'echo-request'
set firewall name LAN-4-OUT rule 120 protocol 'icmp'
set firewall name LAN-4-OUT rule 120 state new 'enable'

set firewall name OUTSIDE-4-LOCAL default-action 'drop'
set firewall name OUTSIDE-4-LOCAL rule 100 action 'drop'
set firewall name OUTSIDE-4-LOCAL rule 100 source group network-group 'NET-4-BLACKLIST'
set firewall name OUTSIDE-4-LOCAL rule 101 action 'drop'
set firewall name OUTSIDE-4-LOCAL rule 101 destination group network-group 'NET-4-BLACKLIST'
set firewall name OUTSIDE-4-LOCAL rule 110 action 'accept'
set firewall name OUTSIDE-4-LOCAL rule 110 state established 'enable'
```

```
set firewall name OUTSIDE-4-LOCAL rule 110 state related 'enable'
set firewall name OUTSIDE-4-LOCAL rule 111 action 'drop'
set firewall name OUTSIDE-4-LOCAL rule 111 state invalid 'enable'
set firewall name OUTSIDE-4-LOCAL rule 120 action 'accept'
set firewall name OUTSIDE-4-LOCAL rule 120 icmp type-name 'echo-request'
set firewall name OUTSIDE-4-LOCAL rule 120 protocol 'icmp'
set firewall name OUTSIDE-4-LOCAL rule 120 state new 'enable'
set firewall name OUTSIDE-4-LOCAL rule 130 action 'accept'
set firewall name OUTSIDE-4-LOCAL rule 130 destination port '68'
set firewall name OUTSIDE-4-LOCAL rule 130 protocol 'udp'
set firewall name OUTSIDE-4-LOCAL rule 130 source port '67'
set firewall name OUTSIDE-4-LOCAL rule 130 state new 'enable'
set firewall name OUTSIDE-4-LOCAL rule 140 action 'drop'
set firewall name OUTSIDE-4-LOCAL rule 140 destination port '22'
set firewall name OUTSIDE-4-LOCAL rule 140 protocol 'tcp'
set firewall name OUTSIDE-4-LOCAL rule 140 recent count '4'
set firewall name OUTSIDE-4-LOCAL rule 140 recent time '60'
set firewall name OUTSIDE-4-LOCAL rule 140 source group network-group 'NET-4-MANAGEMENT'
set firewall name OUTSIDE-4-LOCAL rule 140 state new 'enable'
set firewall name OUTSIDE-4-LOCAL rule 141 action 'accept'
set firewall name OUTSIDE-4-LOCAL rule 141 destination port '22'
set firewall name OUTSIDE-4-LOCAL rule 141 protocol 'tcp'
set firewall name OUTSIDE-4-LOCAL rule 141 source group network-group 'NET-4-MANAGEMENT'
set firewall name OUTSIDE-4-LOCAL rule 141 state new 'enable'

## FQ-CODEL traffic shaping on WAN interface upload (20M limit) and
## LAN interface download (400M limit) to mitigate bufferbloat
## tuned for cable modem service

set traffic-policy shaper SHAPE-LAN-OUT bandwidth '400mbit'
set traffic-policy shaper SHAPE-LAN-OUT default bandwidth '100%'
set traffic-policy shaper SHAPE-LAN-OUT default burst '4k'
set traffic-policy shaper SHAPE-LAN-OUT default codel-quantum '300'
set traffic-policy shaper SHAPE-LAN-OUT default queue-type 'fq-codel'
```

```
set traffic-policy shaper SHAPE-LAN-OUT default target '30'

set traffic-policy shaper SHAPE-WAN-OUT bandwidth '20mbit'
set traffic-policy shaper SHAPE-WAN-OUT default bandwidth '100%'
set traffic-policy shaper SHAPE-WAN-OUT default burst '4k'
set traffic-policy shaper SHAPE-WAN-OUT default codel-quantum '300'
set traffic-policy shaper SHAPE-WAN-OUT default queue-type 'fq-codel'
set traffic-policy shaper SHAPE-WAN-OUT default target '30'

## Interface Configuration

set interfaces ethernet eth0 address 'dhcp'
set interfaces ethernet eth0 address 'dhcpv6'
set interfaces ethernet eth0 description 'WAN'
set interfaces ethernet eth0 dhcpv6-options duid '00:04:ce:af:52:cf:6b:c7:48:e4:9d:ee:3e:77:3d:69:bf:56'
set interfaces ethernet eth0 dhcpv6-options pd 0 interface eth1 address '1'
set interfaces ethernet eth0 dhcpv6-options pd 0 interface eth1 sla-id '1'
set interfaces ethernet eth0 dhcpv6-options pd 0 length '56'
set interfaces ethernet eth0 dhcpv6-options rapid-commit
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 firewall local ipv6-name 'OUTSIDE-6-LOCAL'
set interfaces ethernet eth0 firewall local name 'OUTSIDE-4-LOCAL'
set interfaces ethernet eth0 hw-id 'ac:1f:6b:67:c1:fe'
set interfaces ethernet eth0 ipv6 address autoconf
set interfaces ethernet eth0 ring-buffer rx '4096'
set interfaces ethernet eth0 ring-buffer tx '4096'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth0 traffic-policy out 'SHAPE-WAN-OUT'

set interfaces ethernet eth1 address '192.168.1.1/24'
set interfaces ethernet eth1 description 'LAN'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 firewall in ipv6-name 'LAN-6-IN'
set interfaces ethernet eth1 firewall in name 'LAN-4-IN'
```

```
set interfaces ethernet eth1 firewall local ipv6-name 'INSIDE-6-LOCAL'
set interfaces ethernet eth1 firewall local name 'INSIDE-4-LOCAL'
set interfaces ethernet eth1 firewall out ipv6-name 'LAN-6-OUT'
set interfaces ethernet eth1 firewall out name 'LAN-4-OUT'
set interfaces ethernet eth1 hw-id 'ac:1f:6b:67:c1:ff'
set interfaces ethernet eth1 ring-buffer rx '4096'
set interfaces ethernet eth1 ring-buffer tx '4096'
set interfaces ethernet eth1 speed 'auto'
set interfaces ethernet eth1 traffic-policy out 'SHAPE-LAN-OUT'

set interfaces loopback lo

## NAT configuration

set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.1.0/24'
set nat source rule 100 translation address 'masquerade'
## IGMPv3 querier (no MLD supported yet)

set protocols igmp interface eth1 query-interval '125'
set protocols igmp interface eth1 version '3'

## DHCP server

set service dhcp-server shared-network-name LAN authoritative
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 default-router '192.168.1.1'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 dns-server '8.8.8.8'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 dns-server '8.8.4.4'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 domain-name 'lan.private'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 lease '43200'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range LAN-POOL start '192.168.1.100'
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 range LAN-POOL stop '192.168.1.199'

## DHCPv6 server
```

```
set service dhcpv6-server preference '255'
set service dhcpv6-server shared-network-name LAN common-options domain-search 'lan.private'
set service dhcpv6-server shared-network-name LAN common-options name-server '2001:4860:4860::8888'
set service dhcpv6-server shared-network-name LAN common-options name-server '2001:4860:4860::8844'
set service dhcpv6-server shared-network-name LAN subnet fe80::ae1f:6bff:fe67:c1ff/128

## IPv6 Router Advertisements

set service router-advert interface eth1 default-lifetime '300'
set service router-advert interface eth1 default-preference 'high'
set service router-advert interface eth1 hop-limit '64'
set service router-advert interface eth1 interval max '30'
set service router-advert interface eth1 link-mtu '1500'
set service router-advert interface eth1 name-server '2001:4860:4860::8888'
set service router-advert interface eth1 name-server '2001:4860:4860::8844'
set service router-advert interface eth1 other-config-flag
set service router-advert interface eth1 prefix ::/64 preferred-lifetime '300'
set service router-advert interface eth1 prefix ::/64 valid-lifetime '900'
set service router-advert interface eth1 reachable-time '900000'
set service router-advert interface eth1 retrans-timer '0'

# Enable SSH

set service ssh port '22'

# Conntrack Tuning 1M

set system config-management commit-revisions '10'
set system conntrack expect-table-size '100000'
set system conntrack hash-size '1000000'
set system conntrack modules nfs disable
set system conntrack modules sip disable
set system conntrack modules sqlnet disable
```

```
set system conntrack table-size '1000000'

# System Configuration

set system console device ttyS0 speed '9600'
set system domain-name 'wan.private'
set system host-name 'gateway'
# set system login user <redacted> authentication encrypted-password <redacted>
set system name-server '8.8.8.8'
set system name-server '8.8.4.4'
set system name-server '2001:4860:4860::8888'
set system name-server '2001:4860:4860::8844'
set system ntp server time1.google.com
set system ntp server time2.google.com
set system ntp server time3.google.com
set system ntp server time4.google.com
set system option performance 'latency'
set system syslog global facility all level 'info'
set system syslog global facility protocols level 'debug'
set system time-zone 'UTC'
```