Defining a Layer 2 Port-Mirroring Firewall Filter

For virtual private LAN service (VPLS) traffic (family bridge or family vpls) and for Layer 2 VPNs with family ccc on MX Series routers only, you can define a firewall filter that specifies Layer 2 port mirroring as the action to be performed if a packet matches the conditions configured in the firewall filter term.

You can use a Layer 2 port-mirroring firewall filter in the following ways:

- To mirror packets received or sent on a logical interface.
- To mirror packets forwarded or flooded to a bridge domain.
- To mirror packets forwarded or flooded to a VPLS routing instance.
- To mirror tunnel interface input packets only to multiple destinations.

For a summary of the three types of Layer 2 port-mirroring you can configure on an MX Series router, see Application of Layer 2 Port Mirroring Types.

For information about configuring firewall filters in general (including in a Layer 3 environment), see Firewall Filter Overview and How Firewall Filters Are Evaluated in the *Junos Policy Framework Configuration Guide*.

To define a firewall filter with a Layer 2 port-mirroring action:

1. Enable configuration of firewall filters for Layer 2 packets that are part of a bridge domain, a Layer 2 switching cross-connect, or a virtual private LAN service (VPLS):

   ```
   [edit]
   user@host# edit firewall family family
   ```

   The value of the *family* option can be bridge, ccc, or vpls.

2. Enable configuration of a firewall filter *pm-filter-name*:

   ```
   [edit firewall family family]
   user@host# edit filter pm-filter-name
   ```

3. Enable configuration of a firewall filter term *pm-filter-term-name*:

   ```
   [edit firewall family family filter pm-filter-name]
   user@host# edit term pm-filter-term-name
   ```

   For more information about firewall filter terms in general (including in a Layer 3 environment), see Overview of Match Conditions in Firewall Filter Terms in the *Junos Policy Framework Configuration Guide*.

4. (Optional) Specify the firewall filter match conditions based on the route source address *only if* you want to mirror a subset of the sampled packets.

For information about configuring firewall filter match conditions in general (including in a Layer 3 environment), see Overview of Match Conditions in Firewall Filter Terms in the *Junos Policy Framework Configuration Guide*.

- For detailed information about Layer 2 bridging firewall filter match conditions (which are supported on MX Series routers only), see Configuring Layer 2 Bridging Match Conditions for MX Series Ethernet Services Routers.
- For detailed information about VPLS firewall filter match conditions, see Configuring VPLS Match Conditions.
- For detailed information about Layer 2 circuit cross-connect (CCC) firewall filter match conditions, see Configuring Layer 2 Circuit Cross-Connect Match Conditions.

NOTE: If you want all sampled packets to be considered to match (and be subjected to the actions specified in the then statement), then omit the from statement altogether.

5. Enable configuration of the *action* and *action-modifier* to apply to matching packets:

   [edit firewall family *family* filter *pm-filter-name* term *pm-filter-term-name*]
   user@host# **edit then**

6. Specify the actions to be taken on matching packets:

   [edit firewall family *family* filter *pm-filter-name* term *pm-filter-term-name* then]
   user@host# **set *action***

   The recommended value for the *action* is accept. If you do not specify an action, or if you omit the then statement entirely, all packets that match the conditions in the from statement are accepted.

7. Specify Layer 2 port mirroring or a next-hop group as the *action-modifier*:

   - To reference the Layer 2 port mirroring properties currently in effect for the Packet Forwarding Engine or PIC associated with the underlying physical interface, use the port-mirror statement:

     [edit firewall family *family* filter *pm-filter-name* term *pm-filter-term-name* then]
     user@host# **set port-mirror**

   - To reference the Layer 2 port mirroring properties configured in a specific named instance, use the port-mirror-instance *pm-instance-name* action modifier:

     [edit firewall family *family* filter *pm-filter-name* term *pm-filter-term-name* then]
     user@host# **set port-mirror-instance *pm-instance-name***

     If the underlying physical interface is not bound to a named instance of Layer 2 port mirroring but instead is implicitly bound to the global instance of Layer 2 port mirroring, then traffic at the logical interface is mirrored according to the properties specified in the named instance referenced by the port-mirror-instance action modifier.

- To reference a next-hop group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer), use the next-hop-group *pm-next-hop-group-name* action modifier:

  ```
  [edit firewall family family filter pm-filter-name term pm-filter-term-name then]
  user@host# set next-hop-group pm-next-hop-group-name
  ```

  For configuration information about next-hop groups, see Defining a Next-Hop Group for Layer 2 Port Mirroring. If you specify a next-hop group for Layer 2 port mirroring, the firewall filter term applies to the tunnel interface input only.

8. Verify the minimum configuration of the Layer 2 port-mirroring firewall filter:

```
[edit firewall ... ]
user@host# top
[edit]
user@host# show firewall

family (bridge | ccc | vpls) { # Type of packets to mirror
   filter pm-filter-name { # Firewall filter name
      term pm-filter-term-name {
         from { # Do not specify match conditions based on route source address
         }
         then {
            action; # Recommended action is 'accept'
            action-modifier; # Three options for Layer 2 port mirroring
         }
      }
   }
}
```

In the firewall filter term then statement, the *action-modifier* can be port-mirror, port-mirror-instance *pm-instance-name*, or next-hop-group *pm-next-hop-group-name*.

Related Topics

- Layer 2 Port Mirroring Overview
- Layer 2 Port Mirroring Firewall Filters
- Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups
- Example: Layer 2 Port Mirroring at a Logical Interface
- Example: Layer 2 Port Mirroring for a Layer 2 VPN
- Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links
- Example: Layer 2 Port Mirroring to Multiple Destinations

Published: 2010-05-11