Chapter 3
Creating Policy Lists

This chapter provides information for configuring policy lists on E-series routers. The chapter discusses the following topics:

Policy Lists Overview

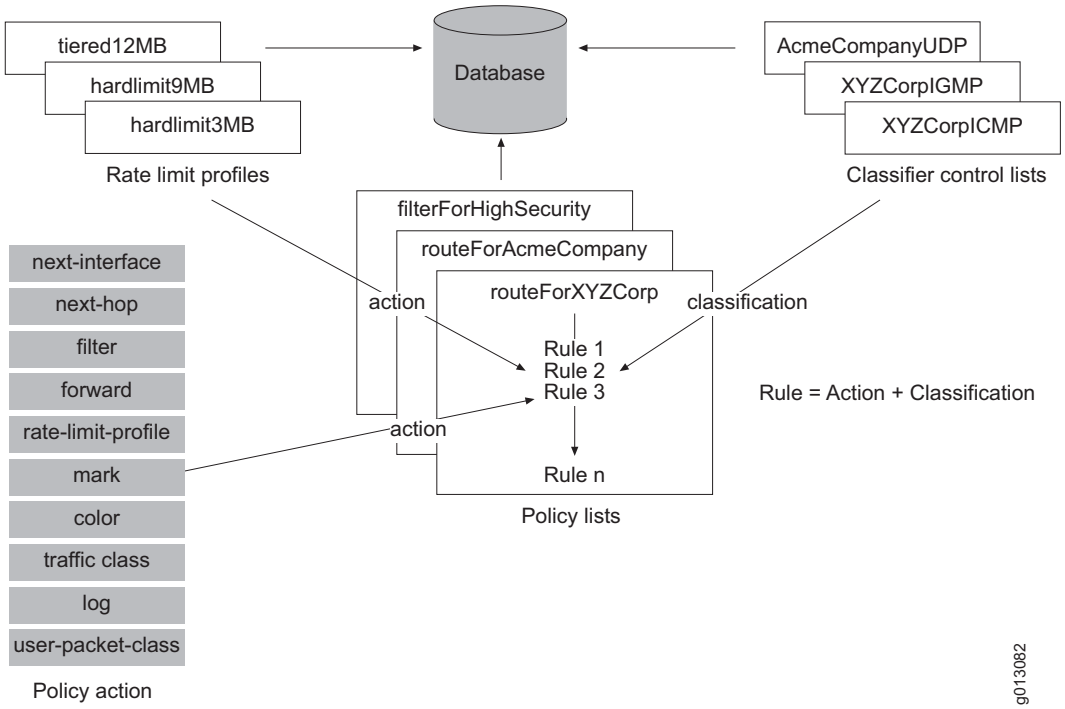
You create a policy rule by specifying a policy action within a classifier group that references a CLACL. These rules become part of a policy list that you can attach to an interface as either an input policy, secondary-input policy, or output policy. The router applies the rules in the attached policy list to the packets traversing that interface.

You can apply policy lists to packets:

- Arriving at an interface (input policy); on IP and IPv6 interfaces the packets arrive before route lookup
- Arriving at the interface, but after route lookup (secondary input policy); secondary input policies are supported only on IP and IPv6 interfaces
- Leaving an interface (output policy)

Figure 1 shows how a sample IP policy list is constructed.

Figure 1: Constructing an IP Policy List



You can create a policy list with an unlimited number of classifier groups, each containing an unlimited number of rules. These rules can reference up to 512 classifier entries.

If you enter a **policy-list** command and then enter **exit**, the router creates a policy list with no rules. If the router does not find any rules in a policy, it inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface.

NOTE: If you do not specify one of the **frame-relay**, **gre-tunnel**, **ip, ipv6, l2tp, mpls,** or **vlan** keywords, the router creates an IP policy list. This version of the command has been deprecated and may be removed in a future release.

You can create policy lists for ATM, Frame Relay, IP, IPv6, GRE tunnels, L2TP, MPLS, and VLANs.

NOTE: Commands that you issue in Policy Configuration mode do not take effect until you exit from that mode.

Related Topics

- Policy Lists Overview on page 17
- *Chapter 9, Monitoring Policy Management*

Creating Policy Lists for ATM

In the following example, you create two policies: one for CBR traffic and one for UBR traffic. One policy is attached to an interface that contains CBR traffic and the other to an interface that contains UBR traffic.

1. Create a CBR policy list.

   ```
   host1(config)#atm policy-list polCbr
   host1(config-policy-list)#
   ```

2. Create the classification group and assign a strict priority traffic class and color green.

   ```
   host1(config-policy-list)#classifier-group *
   host1(config-policy-list-classifier-group)#traffic-class strict-priority
   host1(config-policy-list-classifier-group)#color green
   ```

3. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

4. Create a UBR policy that maps to the strict best-effort traffic class and color red.

   ```
   host1(config)#atm policy-list polUbr
   host1(config-policy-list)#classifier-group *
   host1(config-policy-list-classifier-group)#traffic-class best-effort
   host1(config-policy-list-classifier-group)#color red
   ```

5. Exit Policy List Configuration mode to save the configuration.

   ```
   host1(config-policy-list-classifier-group)#exit
   host1(config-policy-list)#exit
   host1(config)#
   ```

6. Attach the policies to ATM subinterfaces.

   ```
   host1(config)#interface atm 0/0.100
   host1(config-if)#atm policy input polUbr statistics enabled
   host1(config-if)#exit
   host1(config)#interface atm 0/0.101
   host1(config-if)#atm policy input polCbr statistics enabled
   host1(config-if)#exit
   ```

7. Display the policy lists.

   ```
   host1#show atm subinterface atm 0/0.100

   Circuit                  Interface
    Interface  ATM-Prot VCD VPI VCI  Type   Encap MTU  Status   Type
   ---------- -------- --- --- --- ------- ----- ---- ------ ---------
   ATM 0/0.100 RFC-1483 100   0 100 PVC     SNAP  9180 up     Static

   Auto configure status         : static
   Auto configure interface(s)   : none
   ```

```
Detected 1483 encapsulation   : none
Detected dynamic interface    : none
Interface types in lockout    : none

Assigned profile (IP)         : none assigned
Assigned profile (BridgedEnet): none assigned
Assigned profile (PPP)        : none assigned
Assigned profile (PPPoE)      : none assigned
Assigned profile (any)        : none assigned

SNMP trap link-status: disabled

InPackets:                0
InBytes:                  0
OutPackets:               0
OutBytes:                 0
InErrors:                 0
OutErrors:                0
InPacketDiscards:         0
InPacketsUnknownProtocol: 0
OutDiscards:              0
ATM policy input polUbr
  Statistics are disabled
1 interface(s) found

host1#show atm subinterface atm 0/0.101

                                  Circuit                   Interface
 Interface  ATM-Prot VCD VPI VCI  Type   Encap MTU  Status   Type
----------- -------- --- --- --- ------- ----- ---- ------ ---------
ATM 0/0.101 RFC-1483 101   0 101 PVC     SNAP  9180 up     Static

Auto configure status         : static
Auto configure interface(s)   : none
Detected 1483 encapsulation   : none
Detected dynamic interface    : none
Interface types in lockout    : none

Assigned profile (IP)         : none assigned
Assigned profile (BridgedEnet): none assigned
Assigned profile (PPP)        : none assigned
Assigned profile (PPPoE)      : none assigned
Assigned profile (any)        : none assigned

SNMP trap link-status: disabled

InPackets:                0
InBytes:                  0
OutPackets:               0
OutBytes:                 0
InErrors:                 0
OutErrors:                0
InPacketDiscards:         0
InPacketsUnknownProtocol: 0
OutDiscards:              0
ATM policy input polCbr
  classifier-group *
    3096 packets, 377678 bytes
    traffic-class best-effort
    color green
1 interface(s) found
```

Related Topics

- **atm policy-list** command

Creating Policy Lists for Frame Relay

The following example creates a Frame Relay policy that on egress marks the DE bit to 1, and on ingress colors frames with a DE bit of 1 as red.

1. Create the policy list used to mark egress traffic, then create the classifier group for packets conforming to CLACL frMatchDeSet. Add a rule that marks the DE bit as 1.

   host1(config)#**frame-relay policy-list frOutputPolicy**
   host1(config-policy-list)#**classifier-group frMatchDeSet**
   host1(config-policy-list-classifier-group)#**mark-de 1**
   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**

2. Create the policy list used for the ingress traffic. and create the classifier group conforming to CLACL frMatchDeSet. Add a rule that colors the ingress traffic.

   host1(config)#**frame-relay policy-list frInputPolicy**
   host1(config-policy-list)#**classifier-group frGroupA**
   host1(config-policy-list-classifier-group)#**color red**
   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**

3. Apply the policy lists.

   host1(config)#**interface serial 5/0:1/1.1**
   host1(config-subif)#**frame-relay policy output frOutputPolicy statistics enabled**
   host1(config-subif)#**ip address 10.0.0.1 255.255.255.0**
   host1(config-subif)#**exit**
   host1(config)#**interface serial 5/1:1/1.1**
   host1(config-subif)#**frame-relay policy input frInputPolicy statistics enabled**
   host1(config-subif)#**exit**

4. Display interface information to view the applied policies.

```
host1#show frame-relay subinterface

Frame relay sub-interface SERIAL5/0:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:04:59
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy output frOutputPolicy
  classifier-group frGroupA entry 1
     5 packets, 640 bytes
     mark-de 1
Frame relay sub-interface SERIAL5/1:1/1.1, status is up
Number of sub-interface down transitions is 0
Time since last status change 03:05:09
```

```
No baseline has been set
  In bytes: 660                    Out bytes: 660
  In frames: 5                     Out frames: 5
  In errors: 0                     Out errors: 0
  In discards: 0                   Out discards: 0
  In unknown protos: 0
Frame relay policy input frInputPolicy
  classifier-group frMatchDeSet entry 1
     5 packets, 660 bytes
     color red
```

5. Display the classifier list.

```
host1#show classifier-list detailed

                        Classifier Control List Table
                        ---------- ------- ---- -----
Frame relay Classifier Control List frMatchDeSet
   Reference count:      1
   Entry count:          1

   Classifier-List frMatchDeSet Entry 1
      DE Bit:                    1
```

6. Display the policy lists.

```
host1#show policy-list

                                  Policy Table
                                  ------ -----

Frame relay Policy frOutputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frMatchDeSet, precedence 100
      mark-de 1

Frame relay Policy frInputPolicy
   Administrative state: enable
   Reference count:      0
   Classifier control list: frGroupA, precedence 100
     color red
```

Related Topics

- **frame-relay policy-list** command

Creating Policy Lists for GRE Tunnels

The following example creates a GRE tunnel policy list named routeGre50. For information about creating the CLACL used in this example, see the previous sections.

1. Create the policy list routeGre50.

   host1(config)#**gre-tunnel policy-list routeGre50**

2. Create the classification group for the CLACL named gre8 and assign a precedence of 150 to it.

   host1(config-policy-list)#**classifier-group gre8 precedence 150**
   host1(config-policy-list-classifier-group)#

3. Add two rules for traffic based on the CLACL named gre8: one rule to color packets as red, and a second rule that specifies the ToS DS field value to be assigned to the packets.

   host1(config-policy-list-classifier-group)#**color red**
   host1(config-policy-list-classifier-group)#**mark dsfield 20**
   host1(config-policy-list-classifier-group)#

4. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**
   host1(config)#

5. Display the policy list.

```
host1#show policy-list routeGre50

                                  Policy Table
                                  ------ -----
GRE Tunnel Policy routeGre50
   Administrative state: enable
   Reference count:      0
   Classifier control list: gre8, precedence 150
      color red
      mark dsfield 20
```

Related Topics

- **gre-tunnel policy-list** command

Creating Policy Lists for IP

The following example creates an IP policy list named routeForABCCorp. For information about creating the CLACLs and rate-limit profile used in this example, see the previous sections.

1. Create the policy list routeForABCCorp.

   host1(config)#**ip policy-list routeForABCCorp**
   host1(config-policy-list)#

2. Create the classification group for the CLACL named ipCLACL10 and assign the precedence to the classification group.

   host1(config-policy-list)#**classifier-group ipCLACL10 precedence 75**
   host1(config-policy-list-classifier-group)#

3. Add a rule that specifies a group of forwarding solutions based on classifier list ipCLACL10.

   host1(config-policy-list-classifier-group)#**forward next-hop 192.0.2.12 order 10**
   host1(config-policy-list-classifier-group)#**forward next-hop 192.0.100.109 order 20**
   host1(config-policy-list-classifier-group)#**forward next-hop 192.120.17.5 order 30**
   host1(config-policy-list-classifier-group)#**forward interface ip 3/1 order 40**

4. Add a rule that sets a ToS byte value of 125 for packets based on classifier list ipCLACL10.

   host1(config-policy-list-classifier-group)#**mark tos 125**

5. Add a rule that uses rate-limit profile ipRLP25.

   host1(config-policy-list-classifier-group)#**rate-limit-profile ipRLP25**

6. Exit Classifier Group Configuration mode for ipCLACL10, then create a new classification group for classifier list ipCLACL20. Add a rule that filters packets based on classifier list ipCLACL20.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**classifier-group ipCLACL20 precedence 125**
   host1(config-policy-list-classifier-group)#**filter**

7. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**
   host1(config)#

8. Display the policy list.

```
host1#show policy-list routeForABCCorp

                                    Policy Table
                                    ------ -----
IP Policy routeForABCCorp
   Administrative state: enable
   Reference count:      0
   Classifier control list: ipCLACL10, precedence 75
      forward
         Virtual-router: default
         List:
           next-hop 192.0.2.12, order 10, rule 2 (active)
           next-hop 192.0.100.109, order 20, rule 3 (reachable)
           next-hop 192.120.17.5, order 30, rule 4 (reachable)
           interface ip3/1, order 40, rule 5
      mark tos 125
      rate-limit-profile ipRLP25
   Classifier control list: ipCLACL20, precedence 125
      filter
```

Related Topics

- **ip policy-list** command

Creating Policy Lists for IPv6

The following example creates an IPv6 policy list named routeForIPv6. For information about creating the CLACL used in this example, see the previous sections.

1. Create the policy list routeForIPv6.

```
host1(config)#ipv6 policy-list routeForIPv6
host1(config-policy-list)#
```

2. Create the classification group for the CLACL named ipv6tc67 and assign the precedence to the classification group.

```
host1(config-policy-list)#classifier-group ipv6tc67 precedence 75
host1(config-policy-list-classifier-group)#
```

3. Add a rule to color packets as red, and a second rule that sets the traffic class field of the packets to 7.

```
host1(config-policy-list-classifier-group)#color red
host1(config-policy-list-classifier-group)#mark tcfield 7
```

4. Exit Policy List Configuration mode to save the configuration.

```
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

5. Display the policy list.

```
host1#show policy-list routeForIPv6

                                  Policy Table
                                  ------ -----
IPv6 Policy routeForIPv6
   Administrative state: enable
   Reference count:      0
   Classifier control list: ipv6tc67, precedence 75
      color red
      mark tc-precedence 7
```

Related Topics

- **ipv6 policy-list** command

Creating Policy Lists for L2TP

The following example creates an L2TP policy list.

1. Create the policy list routeForl2tp.

```
host1(config)#l2tp policy-list routeForl2tp
host1(config-policy-list)#
```

2. Create the classification group to match all packets.

```
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#
```

3. Add a rule to color packets as red, and a second rule that uses the rate-limit profile l2tpRLP10.

```
host1(config-policy-list-classifier-group)#color red
host1(config-policy-list-classifier-group)#rate-limit-profile l2tpRLP10
```

4. Exit Policy List Configuration mode to save the configuration.

```
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

5. Display the policy list.

```
host1#show policy-list routeForl2tp

                                  Policy Table
                                  ------ -----
L2TP Policy routeForl2tp
   Administrative state: enable
   Reference count:      0
   Classifier control list: *, precedence 100
      color red
      rate-limit-profile l2tpRLP20
```

Related Topics

- **l2tp policy-list** command

Creating Policy Lists for MPLS

The following example creates an MPLS policy list.

1. Create the policy list routeForMpls.

   host1(config)#**mpls policy-list routeForMpls**
   host1(config-policy-list)#

2. Create the classification group.

   host1(config-policy-list)#**classifier-group * precedence 200**
   host1(config-policy-list-classifier-group)#

3. Add one rule that sets the EXP bits for all packets to 2, and a second rule that uses the rate-limit profile mplsRLP5.

   host1(config-policy-list-classifier-group)#**mark-exp 2**
   host1(config-policy-list-classifier-group)#**rate-limit-profile mplsRLP5**

4. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**
   host1(config)#

5. Display the policy list.

```
host1#show policy-list routeForMpls

                                  Policy Table
                                  ------ -----
MPLS Policy routeForMpls
   Administrative state: enable
   Reference count:      0
   Classifier control list: *, precedence 200
      mark-exp 2 mask 7
      rate-limit-profile mplsRLP5
```

Related Topics

- **mpls policy-list** command

Creating Policy Lists for VLANs

The following example creates a VLAN policy list named routeForVlan. The classifier group lowLatencyLowDrop uses the default precedence of 100.

1. Create the policy list routeForVlan.

   host1(config)#**vlan policy-list routeForVlan**
   host1(config-policy-list)#

2. Create the classification group.

   host1(config-policy-list)#**classifier-group lowLatencyLowDrop**
   host1(config-policy-list-classifier-group)#

3. Create a rule that adds the lowLatencyLowDrop traffic class for all packets that fall into the lowLatencyLowDrop classification.

   host1(config-policy-list-classifier-group)#**traffic-class lowLatencyLowDrop**

4. Add a rule that sets the drop precedence for all packets that fall into the lowLatencyLowDrop classification to green.

   host1(config-policy-list-classifier-group)#**color green**

5. Add a rule that sets the user-priority bits for all packets that fall into the lowLatencyLowDrop classification to 7.

   host1(config-policy-list-classifier-group)#**mark-user-priority 7**

6. Exit to Policy List Configuration mode, then add traffic class rules for packets that conform to different CLACLs.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**classifier-group lowLatency**
   host1(config-policy-list-classifier-group)#**traffic-class lowLatency**
   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**classifier-group excellentEffort**
   host1(config-policy-list-classifier-group)#**traffic-class excellentEffort**
   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**classifier-group bestEffort**
   host1(config-policy-list-classifier-group)#**traffic-class bestEffort**

7. Exit Policy List Configuration mode to save the configuration.

   host1(config-policy-list-classifier-group)#**exit**
   host1(config-policy-list)#**exit**
   host1(config)#

8. Display the policy list.

```
host1#show policy-list routeForVlan

                                  Policy Table
                                  ------ -----
VLAN Policy routeForVlan
   Administrative state: enable
   Reference count:      0
   Classifier control list: lowLatencyLowDrop, precedence 100
      traffic-class lowLatencyLowDrop
      color green
      mark-user-priority 7
   Classifier control list: lowLatency, precedence 100
      traffic-class lowLatency
   Classifier control list: excellentEffort, precedence 100
      traffic-class excellentEffort
   Classifier control list: bestEffort, precedence 100
      traffic-class bestEffort
```

Related Topics

- **vlan policy-list** command