

---

## Configuring Localized Data Policy for IPv6

This article provides procedures for configuring IPv6 localized data policy from the CLI. Localized data policy, configured on vEdge routers, lets you affect how IPv6 data traffic is sent among the vEdge routers in the network. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply mirroring and policing to IPv6 data packets.

For IPv6, you can apply access lists only to interfaces in the transport VPN, VPN 0.

---

## Configuration Components

An access list consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

To create an IPv6 access list, you include the following components in the configuration on a vEdge router:

Component	Description	Configuration Command
Mirroring and policing parameters	Parameters and rules required to configure traffic mirroring and policing. For mirroring, you configure the addresses of the source of the packets to be mirrored and the mirroring site. (You can mirror only unicast traffic.) For policing, you define transmission parameters.	<b>policy mirror</b> <b>policy policer</b>
Access list instance	Container for an access list.	<b>policy ipv6</b> <b>access-list</b>
Numbered sequences of match–action pairs	Sequences establish the order in which the policy components are applied.	<b>policy ipv6</b> <b>access-list</b> <b>sequence</b>
Match parameters	Conditions that packets must match to be considered for a data policy.	<b>policy ipv6</b> <b>access-list</b> <b>sequence</b> <b>match</b>



Component	Description	Configuration Command
Actions	Whether to accept or reject matching packets, and how to process matching items.	<b>policy ipv6 access-list sequence action</b>
Default action	Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped.	<b>policy ipv6 access-list default- action</b>
Application of access lists	For an access list to take effect, you apply it an interface.	<b>vpn 0 interface ipv6 access-list</b>

## General Configuration Procedure

Following are the high-level steps for configuring an access list:

1. Define mirroring parameters (for unicast traffic only):
 

```
vEdge(config)# policy mirror mirror-name
vEdge(config-mirror)# remote-dest ip-address source ip-address
```
3. Define policing parameters:
 

```
vEdge(config)# policy policer policer-name
vEdge(config-policer)# rate bandwidth
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action
```
4. Create an access list instance:
 

```
vEdge(config)# policy ipv6 access-list list-name
```
5. Create a series of match-action pair sequences:
 

```
vEdge(config-ipv6-access-list)# sequence number
vEdge(config-sequence)#
```

The match-action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).
6. Define match parameters for packets:
 

```
vEdge(config-sequence-number)# match match-parameter
```



7. Define actions to take when a match occurs:

```
vEdge(config-sequence) # action drop
vEdge(config-sequence) # action count counter-name
vEdge(config-sequence) # action log
vEdge(config-sequence) # action accept class class-name
vEdge(config-sequence) # action accept mirror mirror-name
vEdge(config-sequence) # action accept policer policer-name
```

8. Create additional numbered sequences of match–action pairs within the access list, as needed.

9. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:

```
vEdge(config-policy-name) # default-action accept
```

10. Apply the access list to an interface:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the access list in the inbound direction (**in**) affects packets being received on the interface. Applying it in the outbound direction (**out**) affects packets being transmitted on the interface.

---

## Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists. Each one is explained in more detail in the sections below.

```
policy
  class-map
    class class map map
  mirror mirror-name
    remote-dest ip-address source ip-address
  policer policer-name
    rate bandwidth
    burst bytes
    exceed action
policy ipv6
  access-list list-name
    sequence number
    match
      match-parameters
    action
      drop
      count counter-name
      log
      accept
        class class-name
        mirror mirror-name
        policer policer-name
    default-action
      (accept | drop)
vpn vpn-id
  interface interface-name
    ipv6 access-list list-name (in | out)
```

---

## Mirroring Parameters

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets:



```
vEdge(config)# policy mirror mirror-name
vEdge(config-mirror)# remote-dest ip-address source ip-address
```

Mirroring applied only to unicast traffic. It does not apply to multicast traffic.

---

## Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values:

```
vEdge(config)# policy policer policer-name
vEdge(config-policer)# rate bps
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action
```

**rate** is the maximum traffic rate. It can be a value from 8 through 10000000 bits per second.

**burst** is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes

**exceed** is the action to take when the burst size or traffic rate is exceeded. *action* can be **drop** (the default) or **remark**. The **drop** action is equivalent to setting the packet loss priority (PLP) bit to low. The **remark** action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

---

## Sequences

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists. You configure sequences with the **policy ipv6 access-list sequence** command.

Each sequence in an access list can contain one **match** command and one **action** command.

---

## Match Parameters

Access lists can match IP prefixes and fields in the IP headers. You configure the match parameters under the **policy access-list sequence match** command.

Each sequence in an access-list must contain one **match** command.

For access lists, you can match these parameters:

Description	Command	Value or Range
Classification map	<b>class</b> <i>class-name</i>	Name of a class defined with a <b>policy class-map</b> command.
Destination	<b>destination-</b>	0 through 65535; specify a single port number, a list of port numbers (with numbers



Description	Command	Value or Range
<a href="#">port number</a> .	<b>port</b> <i>number</i>	separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])
Next header protocol	<b>next-header</b> <i>number</i>	0 through 255, corresponding to an <a href="#">Internet Protocol number</a>
Packet length	<b>packet-length</b> <i>number</i>	Length of the packet. <i>number</i> can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])
Packet loss priority (PLP)	<b>plp</b>	( <b>high</b>   <b>low</b> ) By default, packets have a PLP value of <b>low</b> . To set the PLP value to <b>high</b> , apply a <a href="#">policer</a> that includes the <b>exceed remark</b> option.
Source <a href="#">port number</a> .	<b>source-port</b> <i>address</i>	0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])
TCP flag	<b>tcp</b> <i>flag</i>	<b>syn</b>
Traffic class	<b>traffic-class</b> <i>value</i>	0 through 63

## Action Parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets. You configure the actions parameters with the **policy access-list sequence action** command.

Each sequence in an access list can contain one **action** command.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Description	Command	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the <b>action</b> portion of the access list.	<b>accept</b>	—
Count the accepted or dropped packets.	<b>count</b> <i>counter-counter-</i>	Name of a counter. To display counter information, use the <a href="#">show ipv6 policy</a>



Description	Command	Value or Range
	<i>name</i>	<a href="#">access-lists counters</a> command on the vEdge router.
Discard the packet. This is the default action.	<b>drop</b>	—
Log the packet headers into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	<b>log</b>	To display logging information, use the <a href="#">show app log flow-all</a> and <a href="#">show app log flows</a> command on the vEdge router.

For a packet that is accepted, the following actions can be configured:

Description	Command	Value or Range
Classify the packet.	<b>class</b> <i>class-name</i>	Name of a QoS class defined with a <b>policy class-map</b> command.
Mirror the packet.	<b>mirror</b> <i>mirror-name</i>	Name of mirror defined with a <b>policy mirror</b> command.
Police the packet.	<b>police</b> <i>policer-name</i>	Name of a policer defined with a <b>policy policer</b> command.
Set the packet's DSCP value.	<b>set traffic-class</b> <i>value</i>	0 through 63.

## Default Action

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped. To modify this behavior, include the **access-list ipv6 default-action accept** command in the access list.

## Applying Access Lists

For an access list to take effect, you must apply it to a tunnel interface in VPN 0:

```
vEdge(config)# vpn 0 interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the policy in the inbound direction (**in**) affects prefixes being received on the interface. Applying it in the



outbound direction (**out**) affects prefixes being transmitted on the interface.

---

## Interaction between Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the **policy access-list** command are called *explicit* ACLs. You can apply explicit ACLs to any interface in any VPN on the router.

The router's tunnel interfaces in VPN 0 also have *implicit ACLs*, which are also referred to as *services*. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the [allow-service](#) command:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface interface-name
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# allow-service service-name
vEdge(config-tunnel-interface)# no allow-service service-name
```

On vEdge routers, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (**allow-service allow-service**) or deny (**no allow-service service-name**). Allowing a service in an implicit ACL is the same as specifying the **accept** action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the **drop** action in an explicit ACL
- Whether, in an explicit ACL, the **accept** or **deny** action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

Implicit ACL	Explicit ACL: Sequence	Explicit ACL: Default	Result
Allow (accept)	Deny (drop)	—	Deny (drop)
Allow (accept)	—	Deny (drop)	Allow (accept)
Deny (drop)	Allow (accept)	—	Allow (accept)
Deny (drop)	—	Allow (accept)	Deny (drop)

---

## Additional Information

[Configuring Localized Data Policy for IPv4](#)

[Localized Data Policy](#)

