**Policy Based Routing**

A policy-based routing rule is an ACL that can forward traffic as normal, or route traffic over a VPN tunnel

specified by an IPsec map, routed to a nexthop router on a nexthop list, or redirected over an L3 GRE tunnel or

tunnel group.

A Policy Based Routing rule does not become active until it is applied to a VLAN interface or user role.

To associate a policy based routing rule with a managed device:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Interfaces > IP Routes**.

2. Expand the **Policy-Based Routing** menu.

3. Click **+** below the **Policies** table to create a new policy. When you add a new policy, the **Add Policy** window

appears and prompts you to name the new policy. The policy type (route) is predefined in this window.

4. Select the policy in the **Policies** table. The **Policies > (policy name)** table appears.

5. Click **+** to add a new policy.

6. The **New Rule** window opens. Select a rule type

n Access Control: Applies the rule to all traffic, or traffic using a specific service, protocol, or TCP/UDP port

or range of ports.

n Application: Applies a rule to an traffic for an application or application category.

7. Configure the rule parameters.

**Table 46:** *Policy Based Routing ACL Rule Parameters*





**Targets for PBR Rules**

Use the command routing-policy-map to associate a routing ACL with a specific user role on a managed device.

n If you selected the VLAN type, click the **Target** drop-down list and select a VLAN ID to apply the rule to

inbound traffic on the VLAN interface.