Software ACL

This document describes how to optimize security and CPU utilization using software ACL in VRF traffic management.

Optimizing security and CPU utilization using software ACL in VRF traffic management

Table 1: Feature History

Feature Name	Release Information	Description
Optimizing security and CPU utilization using software ACL in VRF traffic management	Cisco IOS XE 17.15.3b	The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU. The software ACLs enhances reliable and secure VRF-based services in enterprise networks and service provider networks. Command introduced:**platform sw_acl enable** ***interface*** **{icmp | ssh | telnet}**

Software ACL

The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU.

Note This feature is applicable for the RSP2 module.

Key Features

- **Default State**—The feature is disabled by default and activates only when at least one interface is explicitly configured with SW ACL.

  You can configure a maximum of 100 interfaces with SW ACL.

- **Targeted Traffic Control**—Applies exclusively to VRF traffic, specifically ICMP, Telnet, and SSH, without impacting other protocol packets.

- **Non-VRF Traffic Exclusion**—Non-VRF traffic remains unaffected by this feature.

- **Selective Traffic Permission**—When enabled, only traffic to the VRF IP (primary or secondary) or within the same subnet is permitted. All other VRF ICMP, SSH, and Telnet traffic is dropped.

- **Interface Configuration Dependency**—If there are changes in interface configuration, ensure that you must remove and reapply the **platform sw_acl enable** CLI.

  Secondary IP Support:—Supports only one secondary IP, which must be configured before enabling SW ACL

Benefits of using software ACL

- **Enhanced Security**—Prevents unauthorized traffic from reaching the CPU, reducing the risk of attacks.

- **Optimized CPU Utilization**—Ensures that only necessary traffic is processed by the CPU, improving overall system performance.

- **Scalability**—Supports up to 100 interfaces, making it suitable for large-scale deployments, especially in enterprise networks and service provider networks.

Enable software ACL on an interface

1. Configure the interface explicitly to activate the software AC using the **`platform sw_acl enable`** ***`interface`*** **`{icmp | ssh | telnet}`** command.

   For example, if an interface A is enabled with SW ACL to allow ICMP, only pings to that VRF IP (or within the same subnet) are allowed. SSH or telnet to interface A and ICMP, SSH, or Telnet to other VRF interfaces are dropped.

2. Reapply the configuration using the **`platform sw_acl enable`** ***`interface`*** command on the interface.

Verify software ACL applied on the interface

- Use the **`show ip access-lists`** command to verify the applied ACLs and their match counts.

- Ensure that the ACL is applied correctly to the intended interfaces and that traffic is being filtered as expected