Loopback Interfaces

Feature history for loopback interfaces

Table 1: Feature History

Feature Name	Release Information	Description
Implicit ACL on Loopback Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	When a loopback TLOC interface has its own implicit ACL, ACL rules are applied on the traffic destined for the interface. With implicit ACL enabled on the loopback TLOC interface, only limited services can be allowed, thereby enhancing your network security. When a loopback TLOC interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device, the physical interface is treated like a physical TLOC interface.

Loopback interfaces

A loopback interface is a network interface that

- enables data traffic exchange across private WANs such as MPLS or metro Ethernet networks,
- allows routers behind private networks to communicate directly with other edge routers over the private WAN, and
- is configured as a tunnel interface instead of using a physical WAN interface.

Implicit ACLs on loopback interfaces

Implicit ACLs on loopback interfaces are access control mechanism that

- consist of default rules applied to traffic destined for loopback interfaces,
- can be present by default or enabled through configuration to limit or permit traffic, and
- is applied to traffic destined for loopback interfaces configured with a Transport Location (TLOC) in both bind mode (bound to a physical interface) and unbind mode (not bound to any physical interface) on Cisco IOS XE Catalyst SD-WAN devices.

Benefits

Implicit ACL on a loopback TLOC interface protects against denial of service (DoS) attacks by allowing only limited services. This enhances your network security.

Loopback TLOC interface bound to a physical WAN interface

When a loopback interface is a TLOC and is bound to a physical WAN interface, the corresponding implicit ACL rules are applied based on where the traffic is destined:

- If the traffic that is destined to the loopback TLOC interface is received on a physical WAN interface, the implicit ACL rules configured on the loopback TLOC interface is applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured with a TLOC, then routing decisions apply.
  - Forwarded or passthrough packets are dropped when a loopback TLOC interface is bound to a physical WAN interface—the same behavior as when a physical interface is configured as a TLOC. Therefore, an explicit ACL must be configured on the bound physical interface to forward packets.
- An explicit ACL is necessary to allow passthrough packets in the following sample scenarios:
  - Branch edge routers accessing controllers hosted in on-premises data centers: This scenario presumes that the branch edge routers access the controllers through the data center hub, which is configured with a loopback interface bound to a physical WAN interface.

- Branch routers accessing cloud-hosted controllers through data center internet circuits: This scenario presumes that the branch routers are connected to the data center edge using an MPLS network. Such branch routers then access the cloud-hosted controllers through the data canter edge router, which is configured with a loopback interface bound to a physical WAN interface.

- If a physical WAN interface is configured with TLOC, implicit ACL rules of the physical TLOC interface apply. In both these scenarios explicit ACLs on the bound physical WAN interface are necessary to allow passthrough traffic.

Note When a loopback interface with a public IP address is configured as a TLOC and bound to a NAT-enabled physical WAN interface, DIA forwarding works. However, strict color-based exit selection using centralized data policy local-tloc or local-tloc-list is not supported if the bound physical WAN interface is not itself configured as a TLOC.

Loopback TLOC interface not bound to a physical WAN interface

When a loopback interface is a TLOC, and is not bound to a physical WAN interface, implicit ACL rules are applied based on where the traffic is destined for:

- If the traffic that is destined for the loopback TLOC interface is received on a physical WAN interface, implicit ACL rules of the loopback TLOC are applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the input physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured for TLOC, then routing decisions apply.
  - If the physical WAN interface is configured for TLOC, the configured implicit ACL rules apply.

Bind mode and unbind mode

The difference between the bind mode and the unbind mode for loopback TLOC is that in a bind mode the passthrough traffic is dropped because the bound physical interface is treated as a TLOC by itself. In an unbind mode, the passthrough traffic is allowed.

Bind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 and Loopback2 configured as TLOCs and bound to the physical interface GigabitEthernet1. The device also has another interface, Loopback3, which is not configured as a TLOC.

Physical interface GigabitEthernet1 will be treated as a TLOC interface for incoming VPN 0.

In this example:

- If the traffic is destined for Loopback1, implicit ACL rules of Loopback1 are applied.
- If the traffic is destined for Loopback2, implicit ACL rules of Loopback2 are applied.

- If the traffic is destined for Loopback3 on GigabitEthernet1, traffic is allowed.
- If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the bound interface, GigabitEthernet1, is also configured as a TLOC, the traffic to Loopback3 will be subjected to implicit ACL rules on GigabitEthernet1.

Unbind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 configured as a TLOC and is in unbind mode. Loopback2 is not configured as a TLOC. The device also has GigabitEthernet1 interface, which is configured as a TLOC, and GigabitEthernet4 interface, which is not configured as a TLOC.

In this example:

- If the traffic destined for Loopback1 arrives at GigabitEthernet1, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied.
- If the traffic destined for Loopback1 arrives at GigabitEthernet4, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet4, traffic is allowed.
- If the traffic destined for Loopback2 arrives on GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied. If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the traffic is destined for another device passing through GigabitEthernet4, the traffic is forwarded.

Configure implicit ACL on loopback interfaces using CLI commands

You can configure implicit ACL on loopback interfaces using a feature template or using a CLI Add-on template in Cisco SD-WAN Manager.

To configure implicit ACL on loopback interfaces using a feature template, see *Configure VPN Ethernet Interface*.

For information on using the CLI Add-On template, see *Create a CLI Add-On Feature Template*.

Procedure

Step 1 Configure a loopback interface that emulates an interface that is always up.

Example:

```
Device(config)# sdwan
Device(config)# interface Loopback100
```

Use the interface name format **loopback** *string*, where *string* can be any alphanumeric value and may include underscores (_) and hyphens (–). The total interface name, including **loopback**, can be up to 16 characters long. Because of the flexibility of interface naming in the CLI, interfaces such as **lo0** and **loopback0** are parsed as different strings and are

not interchangeable. For the CLI to recognize an interface as a loopback interface, its name must begin with the full string **loopback**.

Step 2 Configure an interface as a secure transport connection.

Example:

```
Device(config)# tunnel-interface
```

Step 3 Permit or deny a service.

- To permit all the services, use the **allow-service** *all* command.
- To permit a specific service, use the **allow-service** *service name* command.
- To deny a service, use the **no allow-service** *service name* command.

Example:

```
Device(config)# no allow-service bgp
Device(config)# allow-service dhcp
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, configuring the **allow-service** *all* command on Cisco SD-WAN Controller is only applicable for the following services **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**.

Step 4 Enable implicit ACL protection on a physical interface for incoming VPN 0 traffic.

Example:

```
Device(config)# implicit-acl-on-bind-intf
```

Use this command to enable implicit ACL protection on a physical interface in cases where a physical interface is not configured with a TLOC and bound to the loopback TLOC interface.

The following example shows implicit ACL configured on a loopback interface.

```
sdwan interface Loopback100
  tunnel-interface
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

Examples of implicit ACL configurations on loopback interfaces

Configuration Examples for Implicit ACL Configured on a Loopback Interface

Configuration Examples for Implicit ACL Configured on a Loopback Interface in Bind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in bind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Configuration Examples for Implicit ACL Configured on a Loopback Interface in unbind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in unbind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Verify implicit ACL configurations on loopback interfaces

This section provides example for verifing implicit ACL configurations on loopback interfaces

Use the **show platform hardware qfp active statistics drop** command to verify implicit ACL configuration on loopback interfaces. The **show platform hardware qfp active statistics drop** command displays drop statistics that help identify implicit ACL activity on loopback interfaces.

The following is a sample output from the **show platform hardware qfp active statistics drop** command:

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


------------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
------------------------------------------------------------------------------
Disabled                                         4                    266
Ipv4EgressIntfEnforce                           15                  10968
Ipv6NoRoute                                      6                    336
Nat64v6tov4                                      6                    480
SVIInputInvalidMac                             244                  15886
SdwanImplicitAclDrop                           160                  27163
UnconfiguredIpv4Fia                         942525               58524580
UnconfiguredIpv6Fia                          77521                9587636
```