



Configuring ACL

This chapter contains these sections:

- [About Access Control Lists, on page 1](#)
- [Guidelines and Limitations for VXLAN ACLs, on page 3](#)
- [VXLAN Tunnel Encapsulation Switch, on page 4](#)
- [VXLAN Tunnel Decapsulation Switch, on page 9](#)

About Access Control Lists

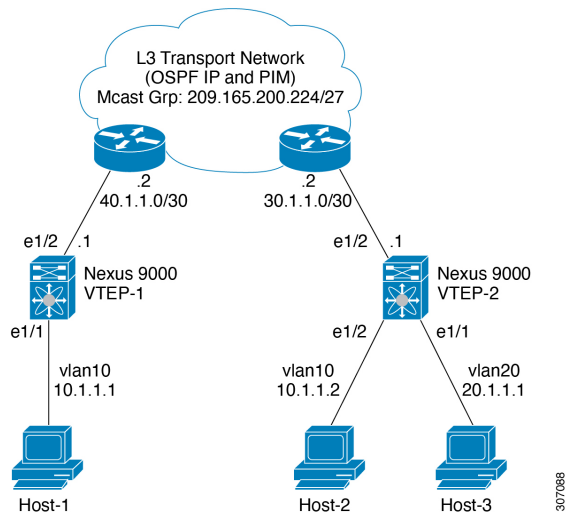
Table 1: ACL Options That Can Be Used for VXLAN Traffic on Cisco Nexus 9300-FX/FX2/FX3/GX/GX2

Scenario	ACL Direction	ACL Type	VTEP Type	Port Type	Flow Direction	Traffic Type	Supported
1	Ingress	PACL	Ingress VTEP	L2 port	Access to Network [GROUPencap direction]	Native L2 traffic [GROUPinner]	YES
2		VACL	Ingress VTEP	VLAN	Access to Network [GROUPencap direction]	Native L2 traffic [GROUPinner]	YES
3	Ingress	RACL	Ingress VTEP	Tenant L3 SVI	Access to Network [GROUPencap direction]	Native L3 traffic [GROUPinner]	YES
4	Egress	RACL	Ingress VTEP	uplink L3/L3-POSVI	Access to Network [GROUPencap direction]	VXLAN encap [GROUPouter]	NO

Scenario	ACL Direction	ACL Type	VTEP Type	Port Type	Flow Direction	Traffic Type	Supported
5	Ingress	RACL	Egress VTEP	Uplink L3/L3-PO/SVI	Network to Access [GROUP:decap direction]	VXLAN encap [GROUP:outer]	NO
6	Egress	PACL	Egress VTEP	L2 port	Network to Access [GROUP:decap direction]	Native L2 traffic [GROUP:inner]	NO
7a		VACL	Egress VTEP	VLAN	Network to Access [GROUP:decap direction]	Native L2 traffic [GROUP:inner]	YES
7b		VACL	Egress VTEP	Destination VLAN	Network to Access [GROUP:decap direction]	Native L3 traffic [GROUP:inner]	YES
8	Egress	RACL	Egress VTEP	Tenant L3 SVI	Network to Access [GROUP:decap direction]	Post-decap L3 traffic [GROUP:inner]	YES

ACL implementation for VXLAN is the same as regular IP traffic. The host traffic is not encapsulated in the ingress direction at the encapsulation switch. The implementation is a bit different for the VXLAN encapsulated traffic at the decapsulation switch as the ACL classification is based on the inner payload. The supported ACL scenarios for VXLAN are explained in the following topics and the unsupported cases are also covered for both encapsulation and decapsulation switches.

All scenarios that are mentioned in the previous table are explained with the following host details:

Figure 1: Port ACL on VXLAN Encap Switch

- Host-1: 10.1.1.1/24 VLAN-10
- Host-2: 10.1.1.2/24 VLAN-10
- Host-3: 20.1.1.1/24 VLAN-20
- Case 1: Layer 2 traffic/L2 VNI that flows between Host-1 and Host-2 on VLAN-10.
- Case 2: Layer 3 traffic/L3 VNI that flows between Host-1 and Host-3 on VLAN-10 and VLAN-20.

Guidelines and Limitations for VXLAN ACLs

VXLAN ACLs have the following guidelines and limitations:

- A router ACL (RACL) on an SVI of the incoming VLAN-10 and the uplink port (eth1/2) does not support filtering the encapsulated VXLAN traffic with outer or inner headers in an egress direction. The limitation also applies to the Layer 3 port-channel uplink interfaces.
- A router ACL (RACL) on an SVI and the Layer 3 uplink ports is not supported to filter the encapsulated VXLAN traffic with outer or inner headers in an ingress direction. This limitation also applies to the Layer 3 port-channel uplink interfaces.
- A port ACL (PACL) cannot be applied on the Layer 2 port to which a host is connected. Cisco NX-OS does not support a PACL in the egress direction.
- Beginning with Cisco NX-OS Release 10.6(2)F, PACL on Service VRF interfaces is supported.

VXLAN Tunnel Encapsulation Switch

Port ACL on the Access Port on Ingress

You can apply a port ACL (PACL) on the Layer 2 trunk or access port that a host is connected on the encapsulating switch. As the incoming traffic from access to the network is normal IP traffic. The ACL that is being applied on the Layer 2 port can filter it as it does for any IP traffic in the non-VXLAN environment.

The **ing-racl** TCAM region must be carved as follows:

SUMMARY STEPS

1. **configure terminal**
2. **hardware access-list tcam region ing-racl 256**
3. **ip access-list name**
4. **sequence-number permit ip source-address destination-address**
5. **exit**
6. **interface ethernet slot/port**
7. **ip port access-group pacl-name in**
8. **switchport**
9. **switchport mode trunk**
10. **switchport trunk allowed vlan vlan-list**
11. **no shutdown**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	hardware access-list tcam region ing-racl 256 Example: <code>switch(config)# hardware access-list tcam region ing-racl 256</code>	Attaches the UDFs to the ing-racl TCAM region, which applies to IPv4 or IPv6 port ACLs.
Step 3	ip access-list name Example: <code>switch(config)# ip access list PACL_On_Host_Port</code>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.
Step 4	sequence-number permit ip source-address destination-address Example:	Creates an ACL rule that permits or denies IPv4 traffic matching its condition.

	Command or Action	Purpose
	<code>switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32</code>	The <i>source-address destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 5	exit Example: <code>switch(config-acl)# exit</code>	Exits IP ACL configuration mode.
Step 6	interface ethernet slot/port Example: <code>switch(config)# interface ethernet1/1</code>	Enters interface configuration mode.
Step 7	ip port access-group pacl-name in Example: <code>switch(config-if)# ip port access-group PACL_On_Host_Port in</code>	Applies a Layer 2 PACL to the interface. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 8	switchport Example: <code>switch(config-if)# switchport</code>	Configures the interface as a Layer 2 interface.
Step 9	switchport mode trunk Example: <code>switch(config-if)# switchport mode trunk</code>	Configures the interface as a Layer 2 trunk port.
Step 10	switchport trunk allowed vlan vlan-list Example: <code>switch(config-if)# switchport trunk allowed vlan 10,20</code>	Sets the allowed VLANs for the trunk interface. The default is to allow all VLANs on the trunk interface, 1 through 3967 and 4048 through 4094. VLANs 3968 through 4047 are the default VLANs reserved for internal use.
Step 11	no shutdown Example: <code>switch(config-if)# no shutdown</code>	Negates the shutdown command.

VLAN ACL on the Server VLAN

A VLAN ACL (VACL) can be applied on the incoming VLAN-10 that the host is connected to on the encaps switch. As the incoming traffic from access to network is normal IP traffic, the ACL that is being applied to VLAN-10 can filter it as it does for any IP traffic in the non-VXLAN environment. For more information on VACL, see [About Access Control Lists, on page 1](#).

SUMMARY STEPS

1. configure terminal

2. **ip access-list** *name*
3. *sequence-number* **permit ip** *source-address destination-address*
4. **vlan access-map** *map-name* [*sequence-number*]
5. **match ip address** *ip-access-list*
6. **action forward**
7. **vlan access-map** *name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal</pre>	Enters global configuration mode.
Step 2	ip access-list <i>name</i> Example: <pre>switch(config)# ip access list VACL_On_Source_VLAN</pre>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.
Step 3	<i>sequence-number</i> permit ip <i>source-address destination-address</i> Example: <pre>switch(config-acl)# 10 permit ip 10.1.1.1 10.1.1.2</pre>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 4	vlan access-map <i>map-name</i> [<i>sequence-number</i>] Example: <pre>switch(config-acl)# vlan access-map VACL_on_Source_Vlan 10</pre>	Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.
Step 5	match ip address <i>ip-access-list</i> Example: <pre>switch(config-acl)# match ip address VACL_on_Source_Vlan</pre>	Specifies an ACL for the access-map entry.
Step 6	action forward Example: <pre>switch(config-acl)# action forward</pre>	Specifies the action that the device applies to traffic that matches the ACL.
Step 7	vlan access-map <i>name</i> Example:	Enters VLAN access-map configuration mode for the VLAN access map specified.

	Command or Action	Purpose
	<code>switch(config-acl)# vlan access map</code> <code>Vacl_on_Source_Vlan</code>	

Routed ACL on an SVI on Ingress

A router ACL (RACL) in the ingress direction can be applied on an SVI of the incoming VLAN-10 that the host that connects to the encapsulating switch. As the incoming traffic from access to network is normal IP traffic, the ACL that is being applied on SVI 10 can filter it as it does for any IP traffic in the non-VXLAN environment.

The **ing-racl** TCAM region must be carved as follows:

SUMMARY STEPS

1. **configure terminal**
2. **hardware access-list tcam region ing-racl 256**
3. **ip access-list** *name*
4. *sequence-number* **permit ip** *source-address destination-address*
5. **exit**
6. **interface ethernet** *slot/port*
7. **no shutdown**
8. **ip access-group** *racl-name* **in**
9. **vrf member** *vlan-number*
10. **no ip redirects**
11. **ip address** *ip-address*
12. **no ipv6 redirects**
13. **fabric forwarding mode anycast-gateway**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	hardware access-list tcam region ing-racl 256 Example: <code>switch(config)# hardware access-list tcam region</code> <code>ing-racl 256</code>	Attaches the UDFs to the ing-racl TCAM region, which applies to IPv4 or IPv6 port ACLs.
Step 3	ip access-list <i>name</i> Example: <code>switch(config)# ip access list PACL_On_Host_Port</code>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.

	Command or Action	Purpose
Step 4	<i>sequence-number</i> permit ip <i>source-address</i> <i>destination-address</i> Example: <pre>switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32</pre>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address</i> <i>destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 5	exit Example: <pre>switch(config-acl)# exit</pre>	Exits IP ACL configuration mode.
Step 6	interface ethernet <i>slot/port</i> Example: <pre>switch(config)# interface ethernet1/1</pre>	Enters interface configuration mode.
Step 7	no shutdown Example: <pre>switch(config-if)# no shutdown</pre>	Negates shutdown command.
Step 8	ip access-group <i>acl-name</i> in Example: <pre>switch(config-if)# ip port access-group RACL_On_Source_Vlan_SVI in</pre>	Applies a Layer 2 PACL to the interface. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 9	vrf member <i>vlan-number</i> Example: <pre>switch(config-if)# vrf member Cust-A</pre>	Configure SVI for host.
Step 10	no ip redirects Example: <pre>switch(config-if)# no ip redirects</pre>	Prevents the device from sending redirects.
Step 11	ip address <i>ip-address</i> Example: <pre>switch(config-if)# ip address 10.1.1.10</pre>	Configures an IP address for this interface.
Step 12	no ipv6 redirects Example: <pre>switch(config-if)# no ipv6 redirects</pre>	Disables the ICMP redirect messages on BFD-enabled interfaces.
Step 13	fabric forwarding mode anycast-gateway Example: <pre>switch(config-if)# fabric forwarding mode anycast-gateway</pre>	Configure Anycast gateway forwarding mode.

Routed ACL on the Uplink on Egress

A RACL on an SVI of the incoming VLAN-10 and the uplink port (eth1/2) is not supported to filter the encapsulated VXLAN traffic with an outer or inner header in an egress direction. This limitation also applies to the Layer 3 port-channel uplink interfaces.

VXLAN Tunnel Decapsulation Switch

Routed ACL on the Uplink on Ingress

A RACL on a SVI and the Layer 3 uplink ports is not supported to filter the encapsulated VXLAN traffic with outer or inner header in an ingress direction. This limitation also applies to the Layer 3 port-channel uplink interfaces.

Port ACL on the Access Port on Egress

Do not apply a PACL on the Layer 2 port to which a host is connected. Cisco Nexus 9000 Series switches do not support a PACL in the egress direction.

VLAN ACL for the Layer 2 VNI Traffic

A VLAN ACL (VACL) can be applied on VLAN-10 to filter with the inner header when the Layer 2 VNI traffic is flowing from Host-1 to Host-2. For more information on VACL, see [About Access Control Lists, on page 1](#).

The VACL TCAM region must be carved as follows:

SUMMARY STEPS

1. **configure terminal**
2. **hardware access-list tcam region vACL 256**
3. **ip access-list *name***
4. **statistics per-entry**
5. *sequence-number* **permit ip** *source-address destination-address*
6. *sequence-number* **permit protocol** *source-address destination-address*
7. **exit**
8. **vlan access-map *map-name* [*sequence-number*]**
9. **match ip address *list-name***

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	hardware access-list tcam region vACL 256 Example: <code>switch(config)# hardware access-list tcam region vACL 256</code>	Changes the ACL TCAM region size.
Step 3	ip access-list name Example: <code>switch(config)# ip access list VXLAN-L2-VNI</code>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.
Step 4	statistics per-entry Example: <code>switch(config-acl)# statistics per-entry</code>	Specifies that the device maintains global statistics for packets that match the rules in the VACL.
Step 5	sequence-number permit ip source-address destination-address Example: <code>switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32</code>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 6	sequence-number permit protocol source-address destination-address Example: <code>switch(config-acl)# 20 permit tcp 10.1.1.2/32 10.1.1.1/32</code>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 7	exit Example: <code>switch(config-acl)# exit</code>	Exit ACL configuration mode.
Step 8	vlan access-map map-name [sequence-number] Example: <code>switch(config)# vlan access-map VXLAN-L2-VNI 10</code>	Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.

	Command or Action	Purpose
Step 9	match ip address <i>list-name</i> Example: <code>switch(config-access-map) # match ip VLAN-L2-VNI</code>	Configure the IP list name.

VLAN ACL for the Layer 3 VNI Traffic

A VLAN ACL (VACL) can be applied on the destination VLAN-20 to filter with the inner header when the Layer 3 VNI traffic is flowing from Host-1 to Host-3. It slightly differs from the previous case as the VACL for the Layer 3 traffic is accounted on the egress on the system. The keyword **output** must be used while dumping the VACL entries for the Layer 3 VNI traffic. For more information on VACL, see [About Access Control Lists, on page 1](#).

The VACL TCAM region must be carved as follows.

SUMMARY STEPS

1. **configure terminal**
2. **hardware access-list tcam region vACL 256**
3. **ip access-list** *name*
4. **statistics per-entry**
5. *sequence-number* **permit ip** *source-address destination-address*
6. *sequence-number* **permit protocol** *source-address destination-address*
7. **vlan access-map** *map-name* [*sequence-number*]
8. **action forward**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	hardware access-list tcam region vACL 256 Example: <code>switch(config) # hardware access-list tcam region vACL 256</code>	Changes the ACL TCAM region size.
Step 3	ip access-list <i>name</i> Example: <code>switch(config) # ip access list VLAN-L3-VNI</code>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.

	Command or Action	Purpose
Step 4	statistics per-entry Example: <pre>switch(config)# statistics per-entry</pre>	Specifies that the device maintains global statistics for packets that match the rules in the VACL.
Step 5	<i>sequence-number</i> permit ip <i>source-address</i> <i>destination-address</i> Example: <pre>switch(config-acl)# 10 permit ip 10.1.1.1/32 20.1.1.1/32</pre>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address</i> <i>destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 6	<i>sequence-number</i> permit protocol <i>source-address</i> <i>destination-address</i> Example: <pre>switch(config-acl)# 20 permit tcp 20.1.1.1/32 10.1.1.1/32</pre>	Configures the ACL to redirect-specific HTTP methods to a server.
Step 7	vlan access-map <i>map-name</i> [<i>sequence-number</i>] Example: <pre>switch(config-acl)# vlan access-map VXLAN-L3-VNI 10</pre>	Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.
Step 8	action forward Example: <pre>switch(config-acl)# action forward</pre>	Specifies the action that the device applies to traffic that matches the ACL.

Routed ACL on an SVI on Egress

A router ACL (RACL) on the egress direction can be applied on an SVI of the destination VLAN-20 that Host-3 is connected to on the decap switch to filter with the inner header for traffic flows from the network to access which is normal post-decapsulated IP traffic post. The ACL that is being applied on SVI 20 can filter it as it does for any IP traffic in the non-VXLAN environment. For more information on ACL, see [About Access Control Lists, on page 1](#).

The egr-racl TCAM region must be carved as follows:

SUMMARY STEPS

1. **configure terminal**
2. **hardware access-list tcam region egr-racl 256**
3. **ip access-list** *name*
4. *sequence-number* **permit ip** *source-address* *destination-address*
5. **interface vlan** *vlan-id*
6. **no shutdown**

7. **ip access-group** *access-list out*
8. **vrf member** *vlan-number*
9. **no ip redirects**
10. **ip address** *ip-address/length*
11. **no ipv6 redirects**
12. **fabric forwarding mode anycast-gateway**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal</pre>	Enters global configuration mode.
Step 2	hardware access-list tcam region egr-racl 256 Example: <pre>switch(config)# hardware access-list tcam region egr-racl 256</pre>	Changes the ACL TCAM region size.
Step 3	ip access-list name Example: <pre>switch(config)# ip access-list Racl_on_Source_Vlan_SVI</pre>	Creates an IPv4 ACL and enters IP ACL configuration mode. The name arguments can be up to 64 characters.
Step 4	<i>sequence-number permit ip source-address destination-address</i> Example: <pre>switch(config-acl)# 10 permit ip 10.1.1.1/32 20.1.1.1/32</pre>	Creates an ACL rule that permits or denies IPv4 traffic matching its condition. The <i>source-address destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, and any to designate any address.
Step 5	interface vlan vlan-id Example: <pre>switch(config-acl)# interface vlan vlan20</pre>	Enters interface configuration mode, where <i>vlan-id</i> is the ID of the VLAN that you want to configure with a DHCP server IP address.
Step 6	no shutdown Example: <pre>switch(config-if)# no shutdown</pre>	Negate the shutdown command.
Step 7	ip access-group access-list out Example: <pre>switch(config-if)# ip access-group Racl_On_Detination_Vlan_SVI out</pre>	Applies an IPv4 or IPv6 ACL to the Layer 3 interfaces for traffic flowing in the direction specified. You can apply one router ACL per direction.

	Command or Action	Purpose
Step 8	vrf member <i>vlan-number</i> Example: switch(config-if) # vrf member Cust-A	Configure SVI for host.
Step 9	no ip redirects Example: switch(config-if) # no ip redirects	Prevents the device from sending redirects.
Step 10	ip address <i>ip-address/length</i> Example: switch(config-if) # ip address 20.1.1.10/24	Configures an IP address for this interface.
Step 11	no ipv6 redirects Example: switch(config-if) # no ipv6 redirects	Disables the ICMP redirect messages on BFD-enabled interfaces.
Step 12	fabric forwarding mode anycast-gateway Example: switch(config-if) # fabric forwarding mode anycast-gateway	Configure Anycast gateway forwarding mode.