This article describes security access control lists (ACLs) in the ACE, how to configure them, and troubleshooting steps to follow if you encounter problems with ACLs.

Guide Contents
Main Article
Overview of ACE Troubleshooting
Understanding the ACE Module Architecture and Traffic Flow
Preliminary ACE Troubleshooting
Troubleshooting ACE Boot Issues
Troubleshooting with ACE Logging
Troubleshooting Connectivity
Troubleshooting ACE Appliance Ethernet Ports
Troubleshooting Remote Access
Troubleshooting Access Control Lists
Troubleshooting Network Address Translation
Troubleshooting ACE Health Monitoring
Troubleshooting Layer 4 Load Balancing
Troubleshooting Layer 7 Load Balancing
Troubleshooting Redundancy
Troubleshooting SSL
Troubleshooting Compression
Troubleshooting Performance Issues
ACE Resource Limits
Managing ACE Resources
Show Counter Reference

Contents

Overview of Security Access Control Lists

An ACL consists of a series of statements called ACL entries that define the network traffic profile. Each entry permits or denies network traffic (inbound and outbound) from and to the parts of your network specified in the entry. Each entry also contains a filter element that is based on criteria such as the source address, the destination address, the protocol, and protocol-specific parameters such as ports and so on.

An implicit deny-all entry exists at the end of each ACL, so you must configure an ACL on each interface that you want to permit connections. Otherwise, the ACE denies all traffic on the interface.

ACLs allow you to control network connection setups rather than processing each packet. Such ACLs are commonly referred to as security ACLs. You can configure ACLs as parts of other features (for example, security, Network Address Translation (NAT), server load balancing (SLB), and so on). The ACE merges these individual ACLs into one large ACL called a merged ACL. The ACL compiler then parses the merged ACL and generates the ACL lookup mechanisms. A match on this merged ACL can result in multiple actions.

Note: You can apply only one extended ACL to each direction (inbound or outbound) of an interface. You can also apply the same ACL on multiple interfaces. You can apply EtherType ACLs only in the inbound direction and only on Layer 2 interfaces.

ACL Types and Uses

You can configure the following two types of ACLs in the ACE:

- Extended?Control network access for IP traffic (Layer 3 and Layer 4)
- EtherType?Control network access for non-IP traffic on Layer 2 interfaces

The ACE does not explicitly support standard ACLs. To configure a standard ACL, specify the destination address as any and do not specify ports in an extended ACL. For details about configuring an extended ACL, see the ?Configuring an Extended ACL? section.

ACL Configuration Guidelines

This section describes the guidelines to observe when you configure and use ACLs in your network. It contains the following topics:

- ACL Entry Order
- ACL Implicit Deny
- Maximum Number of ACL Entries

ACL Entry Order

An ACL consists of one or more entries. Depending on the ACL type, you can specify the source and destination addresses, the protocol, the ports (for TCP or UDP), the ICMP type, the ICMP code, or the EtherType as the match criteria. By default, the ACE appends each ACL entry at the end of the ACL. You can also indicate the location of each entry within an ACL by specifying a line number.

The order of the entries is important. When the ACE decides whether to accept or refuse a connection, the ACE tests the packet against each ACL entry in the order in which the entries are listed. After it finds a match, the ACE does not check any more entries. For example, if you create an entry at the beginning of an ACL that explicitly permits all traffic, the ACE does not check any other statements in the ACL.

Note: If there is a deny statement for packets coming to the Control Plane (CP), then the ACE skips to the next ACL entry.

ACL Implicit Deny

All ACLs have an implicit deny entry at the end of the ACL, so, unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the ACE except for those users with particular IP addresses, then you must deny the particular IP addresses in one entry and permit all other IP addresses in another entry.

Maximum Number of ACL Entries

ACLs are used in ACE as conventional access-groups, and also for use in class maps. The ACLs are converted into trees of different data structures called nodes, which are merged into a single tree instance that consists of nodes of one type called Policy Action Nodes (PANs). This merged tree is then transferred to the dataplane. A tree is created for each instance, and an instance is defined as a VLAN interface in either the input or output direction. Therefore, all ACLs that are applied to a given VLAN and a given direction contribute to the node usage for that instance.

The ACE supports a maximum of 256,000 Policy Action Nodes (PANs) entries. Some ACLs use more memory than others, such as an ACL that uses large port number ranges or overlapping networks (for example, one entry specifies 10.0.0.0/8 and another entry specifies 10.1.1.0/24). Depending on the type of ACL, the actual limit that the ACE can support may be less than 256,000 PANs entries.

If you use object groups in ACL entries, you enter fewer actual ACL entries, but the same number of expanded ACL entries as you did when you entered entries without object groups. Expanded ACL entries count toward the system limit. To view the number of expanded ACL entries in an ACL, use the **show access-list name** command.

If you exceed the memory limitations of the ACE, it generates a syslog message and increments the Download Failures counter in the output of the **show interface vlan** *number* command. The configuration remains in the running-config file and the interface stays enabled. The ACL entries stay the same as they were before the failing configuration was attempted.

For example, if you add a new ACL with ten entries, but the addition of the sixth entry fails because the ACE runs out of memory, the ACE removes the five entries that you successfully entered.

Note: You must allocate sufficient ACL memory resources for each virtual context in the ACE. The ACE does not generate a syslog if you exceed the maximum number of ACL entries.

Configuring ACLs

You can configure ACLs in one of two ways:

- Using the **access-list** command in configuration mode
- Using the **match access-list** command in a Layer 3 and Layer 4 class map

You can permit or deny network connections based on the IP protocol, source and destination IP addresses, and TCP or UDP ports. To configure a non-ICMP extended ACL, enter the following command:

access-list *name* [*line number*] **extended** {**deny** | **permit**} {**protocol** {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port1* [*port2*]] {**any** | *host dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port3* [*port4*]]} | {**object-group** *service_obj_grp_name*} {**any** | *host src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | *host dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

You can also permit or deny network connections based on the ICMP type (for example, echo, echo-reply, unreachable, and so on). To configure an ICMP extended ACL, enter the following command:

access-list *name* [*line number*] **extended** {**deny** | **permit**} {**icmp** {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | *host dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*} [*icmp-type* **code** [*operator code1* [*code2*]]]} | {**object-group** *service_obj_grp_name*} {**any** | *host src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | *host dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

You can configure an ACL that controls traffic based on its EtherType. An EtherType is a subprotocol identifier. EtherType ACLs support Ethernet V2 frames; they do not do not support 802.3-formatted frames. To configure an Ethertype ACL, enter the following command:

access-list *name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **ipv6** | **mpls**}

Note: You can configure an EtherType ACL on a Layer 2 interface in the inbound direction only. If you are operating the ACE in bridge mode, be sure to configure an ACL on all interfaces that permit BPDUs. Otherwise, a bridge loop may result.

For example, to configure an extended ACL to permit all IP traffic from any source IP address and that is destined to any IP address on interface VLAN 200, enter the following commands:

```
ACE_module5/Admin(config)# access-list ACL1 extended permit ip any any
ACE_module5/Admin(config)# interface vlan 200
ACE_module5/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
ACE_module5/Admin(config)# access-group input ACL1
```

You can apply an ACL to all interfaces in a context at once, subject to the following conditions:

- No interface in the context has an ACL applied to it.
- You can globally apply one Layer 2 and one Layer 3 ACL in the inbound direction only.
- On Layer 2 bridged-group virtual interfaces (BVIs), you can apply both Layer 3 and Layer 2 ACLs.
- On Layer 3 virtual LAN (VLAN) interfaces, you can apply only Layer 3 ACLs.
- In a redundant configuration, the ACE does not apply a global ACL to the FT VLAN.

For example, to apply ACL1 to all interfaces in the Admin context, enter the following command in configuration mode:

```
ACE_module5/Admin(config)# access-group input ACL1
```

The syntax of the **match access-list** command is as follows:

match access-list *acl_name*

To configure an ACL match statement in a class map, enter the following commands:

```
ACE_module5/Admin(config)# class-map match-any L4_CLASS
ACE_module5/Admin(config-cmap)# match access-list ACL1
ACE_module5/Admin(config-cmap)# exit
ACE_module5/Admin(config)# policy-map multi-match L4_POLICY
ACE_module5/Admin(config-pmap)# class L4_CLASS
ACE_module5/Admin(config-pmap-c)#
```

For more details about ACLs and how to configure them, see the Cisco Application Control Engine Module Security Configuration Guide.

ACL-Related syslogs

When a packet matches an ACL entry, a syslog message is generated based on the following rules:

- All ACL deny entries generate a syslog message unless logging is explicitly disabled using the **no logging enable** command in configuration mode.
- An ACL permit entry generates a syslog message only if logging is enabled using the **logging enable** command in configuration mode.
- All implicit deny entries generate the default deny syslog (%ACE-4-106023).

To minimize syslog message generation, the ACE uses the flow cache as follows:

1. For the first packet hit on an ACL entry, the ACE generates a syslog and caches the flow (5-tuple) in the connection table.
2. For subsequent hits on the same ACL entry, the ACE checks the cache. If it finds the flow in the cache, the ACE increments a hit counter for this entry in the cache and does *not* generate a syslog.
3. After some time (the default is 300 seconds, which is configurable in the ACL entry definition in the CLI as the *interval_secs* option), the ACE generates a syslog and sets the hit count to 0.
4. However, if at the expiry of the above time, the hit count is 0, the ACE deletes the cache entry silently. So by default, a cache entry is aged out 600 seconds after the last hit.

Troubleshooting ACLs

Many ACL issues manifest themselves by all traffic or only certain traffic being denied or permitted access to the ACE or out of the ACE. Remember that, initially, all traffic to the ACE is denied until you permit traffic using an ACL. Every ACL contains an implicit deny at the end of it, so only traffic that you explicitly permit will have access to the ACE. To troubleshoot ACLs, follow these steps:

1. Verify that your ACL configuration is correct for your network application. Make any required changes to the running-config file, and then test the configuration. If it is satisfactory, save it to the startup-config file using the **copy runnning-config startup-config** command.

For example, to display the ACLs that you have configured in your ACE, enter the following command:

```
ACE_module5/Admin# show running-config access-list
Generating configuration....

access-list ACL1 remark This ACL permits any IP traffic from any source going to any destination e
 192.168.12.15 255.255.255.192.
access-list ACL1 line 8 extended permit ip any any
access-list ACL1 line 10 extended deny icmp 192.168.12.15 255.255.255.192 any echo code range 1 1
access-list ANYONE line 8 extended permit ip any any
```

To verify that the configured ACLs are applied to the correct interfaces and in the right directions (input or output), enter the following command:

```
ACE_module5/Admin# show running-config interface
Generating configuration....

interface vlan 100
  ip address 10.2.1.1 255.255.255.0
  access-group input ANYONE
  access-group output ANYONE
  no shutdown
interface vlan 200
  ip address 192.168.1.1 255.255.255.0
  access-group input ACL1
  service-policy input MGMT_POLICY
  no shutdown
```

2. Verify that you have allocated sufficient resources for ACLs. To display the allocated resources in your ACE, enter the following command:

```
ACE_module5/Admin# show resource usage
                                          Allocation
        Resource          Current       Peak        Min         Max       Denied
-------------------------------------------------------------------------------
Context: Admin
  conc-connections             10         18          0     8000000          0
  mgmt-connections              2         10          0      100000          0
  proxy-connections           584        590          0     1048574          0
  xlates                        0          0          0     1048574          0
  bandwidth                   880      16194          0   625000000          0
    throughput                880      12606          0   500000000          0
    mgmt-traffic rate           0       3588          0   125000000          0
  connection rate               1         21          0     1000000          0
  ssl-connections rate          0          0          0        5000          0
  mac-miss rate                 0         16          0        2000          0
  inspect-conn rate             0          0          0        6000          0
  acl-memory                33448      33448    7858944    70749384          0 <------- ACL memory
  sticky                        0          0          0           0          0
  regexp                        0          0          0     1048576          0
  syslog buffer            188416     188416          0     4194304          0
  syslog rate                   0          9          0      100000          0
Context: C1
  conc-connections              0          0          0     8000000          0
  mgmt-connections              0          0          0      100000          0
  proxy-connections             0          0          0     1048574          0
  xlates                        0          0          0     1048574          0
  bandwidth                     0          0          0   625000000          0
    throughput                  0          0          0   500000000          0
```

```
    mgmt-traffic rate           0          0          0  125000000          0
  connection rate               0          0          0    1000000          0
  ssl-connections rate          0          0          0       5000          0
  mac-miss rate                 0          0          0       2000          0
  inspect-conn rate             0          0          0       6000          0
  acl-memory                    0          0    7858944   70749384          0
  sticky                        0          0          0          0          0
  regexp                        0          0          0    1048576          0
  syslog buffer                 0          0          0    4194304          0
  syslog rate                   0          0          0     100000          0
```

For example, to allocate a 10 percent minimum and a maximum of unlimited resources for ACL memory in the Admin virtual context, enter the following commands:

```
ACE_module5/Admin(config)# resource myclass
ACE_module5/Admin(config-resource)# limit-resource acl-memory minimum 10 maximum unlimited
ACE_module5/Admin(config-resource)# exit
ACE_module5/Admin(config)# context Admin
ACE_module5/Admin(config-context)# member myclass
```

3. Display the details of an individual ACL by using the **show access-list** *acl_name* **detail** command. This command displays every entry in the specified ACL, the hit counts for each entry, and a 32-bit hexadecimal MD5-hash value that the ACE computes from the **access-list** command immediately when you configure an ACL. The ACE includes this hash value in deny syslog messages (106023) to help you identify the ACL entry that caused the deny syslog. For example to display the details of the ACL1 access control list, enter the following command:

```
ACE_module5/Admin# show access-list ACL1 detail

access-list:ACL1, elements: 2, status: ACTIVE
  remark : This ACL permits any IP traffic from any source going to any destination except for ICM
access-list ACL1 line 8 extended permit ip any any (hitcount=9) [0x894c1008] <------- 32-bit hexad
access-list ACL1 line 10 extended deny icmp 192.168.12.15 255.255.255.192 any echo code range 1 1
```

The format of the deny syslog message is as follows:

```
%ACE-4-106023: Deny protocol number | name src incoming-interface:src-ip dst outgoing-interface:ds
An IP packet was denied by the ACL.
```

> **Explanation:** This message displays even if you do not have the log option enabled for an ACL. If a packet hits an input ACL, the outgoing interface will not be known. In this case, the ACE prints the outgoing interface as undetermined. The source IP and destination IP addresses are the unmapped and mapped addresses for the input and output ACLs, respectively, when used with NAT.
>
> **Recommended Action:** If messages persist from the same source address, messages may indicate a foot-printing or port-scanning attempt. Contact the remote host administrators.

An ACL merged list is a large ACL that the CP compiles from multiple security ACL entries and policies. When the ACE executes an ACL merged list, it performs multiple actions on a flow that matches the merged list.

4. Display the actions that the ACE will perform on a flow by entering the **show acl-merge merged-list** command. For example, to display the merged list for VLAN 100, enter the following command:

```
ACE_module5/Admin# show acl-merge merged-list vlan 100 in non-redundant
```

```
All ACEs in merged list 2 Total:18 Non-redundant:12

Priority:1000, Lineno:0, ACE-id:211 Action:PERMIT, Path-id:0x81/0x0/0x0:6/0[6/0]
[6/0]
Pmap:0x5, Log:FALSE/FALSE[FALSE][FALSE], Interval:0/0[0][0]
Hash1:0x0 Hash2:0x0
Generated:TRUE, need-to-add-in-comp:NO_ACT_NEEDED, redundant:FALSE
Parent:: feature:SECURITY ace-lineno:5 ACL priority:0[G:0,P:0,C:0,ACL:0]
Parent:: feature:TO CP ace-lineno:2 ACL priority:16779265[G:0,P:1,C:8,ACL:1]
Feature:SECURITY Policy:1[1][1] sec-level:0x0 Intratype:SKIP
Feature:TO CP Policy:1[1][1] sec-level:0x0 Intratype:TERMINATE
Intertype:TERMINATE
IP address SRC:161.44.0.0/255.255.0.0 DST:10.86.215.134/255.255.255.255
Ports SRC:RANGE 0 65535 DST:RANGE 22 22
Protocol:6
Hit Count:0 Active:TRUE Timerange:0
.
.
.
Feature:SECURITY Policy:0[0] sec-level:0x0 Intratype:TERMINATE
.
.
.
Feature:SLB Policy:14[14] sec-level:0x0 Intratype:TERMINATE
.
.
.
Feature:SRC NAT Policy:2[2] sec-level:0x0 Intratype:TERMINATE
.
.
.
```

5. If the acl-memory Denied counter in the output of the **show resource usage** command is incrementing and the Peak (ACL) memory counter has not exceeded the Max Allocated ACL memory counter, the problem may lie with one of the nodes in the ACL merge tree. The ACL merge tree contains several different kinds of nodes (see the example output below), each of a different size and each with a maximum limit. If you allocate a minimum of 10 percent of the ACE resources to ACL memory, the ACE will guarantee 10% of the maximum number of each node. If your configuration causes the ACE to exceed the maximum value of one of these nodes, the ACL resource allocation will fail and the acl-memory Denied counter will increment.

To monitor the ACL merge tree node usage in the ACE, enter the following command:

```
ACE_module5/Admin# show np 1 access-list resource

ACL Tree Statistics for Context ID: Admin
=========================================
ACL memory max-limit: None
ACL memory guarantee: 10.00 %
MTrie nodes(used/guaranteed/max-limit):
        43 / 26214 / 262143 (compressed) <-------|
        3 / 2199 / 21999 (uncompressed) <--------|
Leaf Head nodes (used/guaranteed/max-limit):     |
        39 / 26214 / 262143 <--------------------|---- Maximum number of available nodes in the AC
Leaf Parameter nodes (used/guaranteed/max-limit):|
        594 / 52428 / 524288 <-------------------|
Policy action nodes used: 153
memory consumed: 23776 bytes resource-limited 4896 bytes other 28672 bytes total
.
min-guarantee: 7861043 bytes total, 0 % consumed.
max-limit: 78610432 bytes total, 0 % consumed.

ACL Tree Statistics for the linecard
```

```
===================================
MTrie nodes(used): 43 (compressed) 3 (uncompressed) <--------------|
           (shared): 235929 (compressed) 19800 (uncompressed)      |
Leaf Head nodes (used/shared): 39 / 235929 <-----------------------|---- Number of used nodes in t
Leaf Parameter nodes (used/shared): 594 / 471860 <-----------------|
Policy action nodes (used/shared): 153 / 261990 <------------------|
```

You can calculate the percentage of use for each node type by dividing the used nodes value by the maximum number of nodes and multiplying the result by 100. If any of these percentages exceeds the maximum value of allocated ACL memory for the context, increase the **max** value of allocated ACL memory using the **limit-resource acl-memory** command in resource class configuration mode so that that value is greater than or equal to the highest used nodes percentage that you calculated. Alternatively, if you are approaching the limits of ACL resource capacity, you may consider consolidating your ACL configuration.

If the ACL nodes are depleted while the ACE is downloading ACL configurations for an interface, the complete ACL merged list for that interface is deleted and no traffic flows through that interface. The ACE increments the download failure counter in the output of the **show interface** command and the ACE logs a system message from the configuration manager.

6. To trace a packet through a specific ACL, enter the following command:

```
ACE_module5/Admin# show np 1 access-list trace vlan 130 in protocol 1 source 172.27.16.23 2000 des

Root 0x2c01b00
Src Mtrie (0) offset 1 curr 0x2c01b00 child 0x0 leaf 0x10a840
   Dst Mtrie (0) offset 2 curr 0x10a840 child 0x0 leaf 0x3c01330
        proto ICMP head node 0x4004880
            proto node 0x4004880
            src op range port 0/65535
            dst op range port 0/65535 lineno 112000
    inner match line#:112000
inner match line#: 112000

packet matched priority 112000

action node 0x4c02460
Action Leaf-node
version+aceid 0x99 (version 0 ace_id 153 dirty no)
action_flag 0x10 (permit no log no punt_to_cp no capture no bridge yes)
path ID 0x0
src nat 0x0 dst nat 0x0 vserver 0x0 fixup 0x0
TCP conn 0x0 AAA 0x0 Websense 0x0 QOS Policer 0x0
Syslog Info 0
Hitcount 130426
Syslog info:
  idx:[153:0] name_idx:[0:0] hash1:0x0 hash2:0x0 name_len:0 invalid

Number of DRAM access: 6 (2 mtrie 4 non-mtrie)
```