LAB GUIDE

Using ACLs with Aruba CX Switches

IMPORTANT!

THIS GUIDE ASSUMES THAT THE AOS-CX OVA HAS BEEN INSTALLED AND WORKS IN GNS3 OR EVE-NG. PLEASE REFER TO GNS3/EVE-NG INITIAL SETUP LABS IF REQUIRED.

AT THIS TIME, EVE-NG DOES NOT SUPPORT EXPORTING/IMPORTING AOS-CX STARTUP-CONFIG. THE LAB USER SHOULD COPY/PASTE THE AOS-CX NODE CONFIGURATION FROM THE LAB GUIDE AS DESCRIBED IN THE LAB GUIDE IF REQUIRED.

TABLE OF CONTENTS

Lab Objective

At the end of this workshop, you will be able to implement basic ACLs which can be used to add security controls to various traffic flows on Aruba CX switches.

The main traffic characteristics that ACLs can filter on are as follows:

- Protocol such as: ICMP, TCP, UDP
- Source and/or destination addresses (IPv4, IPv6, or MAC)
- Source and/or destination TCP/UDP ports (if applicable to the specified protocol)

Lab Overview

Access Control Lists (ACLs) let a network administrator permit or deny passage of traffic based on network addresses, protocols, service ports, and other packet attributes. ACLs are composed of one or more Access Control Entries (called ACEs). Each ACE defines a filter criteria and an action, either permit or deny. If the traffic matches the filter criteria, the specified action is taken. The permit action permits the traffic to continue through the switch. The deny action causes the traffic to be discarded (dropped). ACEs can also log or count matching traffic.

Three ACL types are supported; IPv4, IPv6, and MAC. Each ACL type is focused on relevant frame or packet characteristics.

ACLs must be applied (using an apply access-list command) to take effect. ACLs can be applied to interfaces (including LAGs), VLANs, or the Control Plane. Access Control Entries (ACEs) are listed according to priority by sequence number and processed in lowest to highest sequence number order. Each ACE attempts to match on one or more attributes of the particular traffic type. Attempted ACE matching ceases upon the first successful match. For a match to be considered successful, a packet must match all the criteria, qualifiers, and attributes of a particular ACE. Higher numbered ACEs are only processed if no lower-numbered ACE matches. If the traffic matches no ACE in the entire ACL, the default action deny is taken, causing the traffic to be discarded (dropped).

When defining an ACE, if the sequence number is omitted, the ACE is auto-assigned a new sequence number that is 10 greater than the existing highest ACE sequence number. The first auto-assigned sequence number is 10. If you choose to include the ACE sequence numbers, you can use any number you like, however it is suggested that you follow the practice of entering them as 10, 20, 30, and so on. Regardless of the order in which ACEs are entered, they are stored in low-to-high sequence number order. If you enter three ACEs numbered 10, 30, 20, when creating an ACL, the ACEs are stored in the ACL as 10, 20, 30.

Lab Network Layout

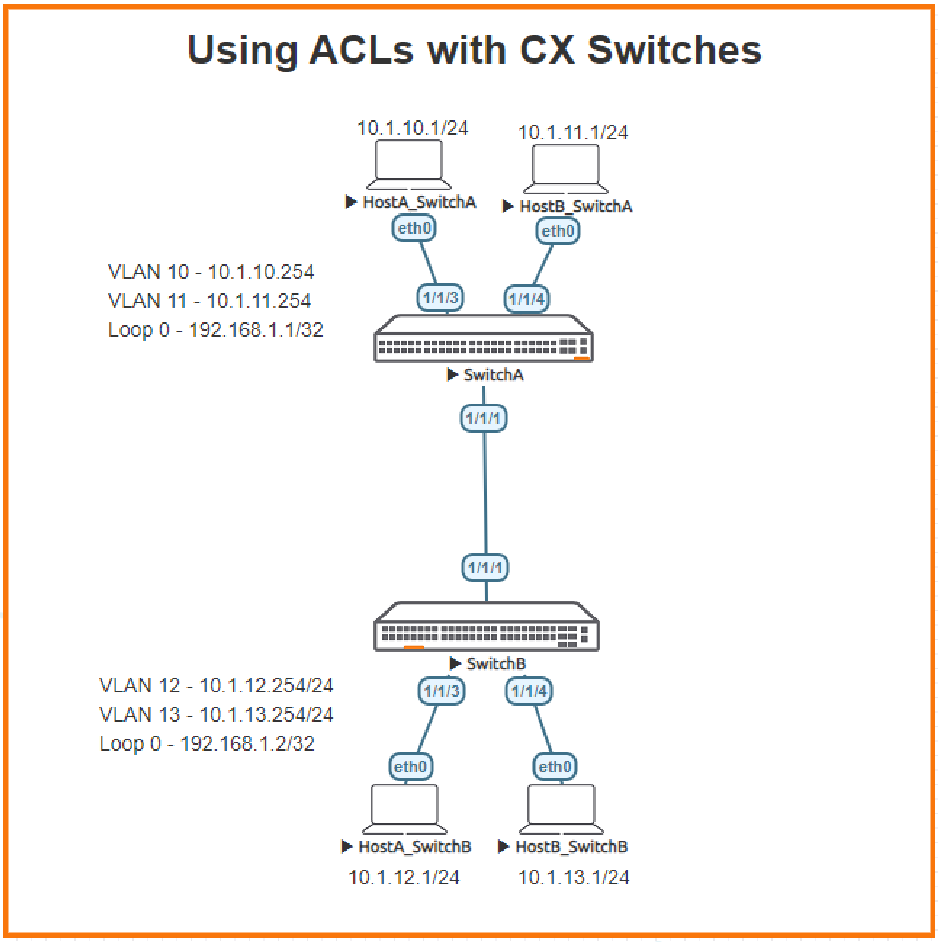

Figure 1. Lab topology and addresses

Lab Tasks

Task 1 - Lab setup

For this lab refer to Figure 1 for topology and IP address details.

- Start all the devices, including host and client
- Open each switch console and log in with user “admin” and no password
- Change all hostnames as shown in the topology:

```
hostname …
```

- On all devices, bring up required ports:

```
int 1/1/1
  no shutdown
int 1/1/3-1/1/4
  no shutdown
```

- Validate LLDP neighbors appear as expected

```
show lldp neighbor
```

SwitchA

```
LLDP Neighbor Information
=========================

Total Neighbor Entries          : 1
Total Neighbor Entries Deleted  : 0
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 0

LOCAL-PORT  CHASSIS-ID         PORT-ID          PORT-DESC                TTL      SYS-NAME
------------------------------------------------------------------------------------------
1/1/1       08:00:09:16:7b:7e  1/1/1            To SwitchA               120      SwitchB
```

Task 2 - Configure HostA_SwitchA, HostB_SwitchA, HostA_SwitchB, and HostB_SwitchB

- Apply the proper IP address and gateway to both Host_A and Host_B

HostA_SwitchA

```
ip 10.1.10.1/24 10.1.10.254
```

HostB_SwitchA

```
ip 10.1.11.1/24 10.1.11.254
```

HostA_SwitchB

```
ip 10.1.12.1/24 10.1.12.254
```

HostB_SwitchB

```
ip 10.1.13.1/24 10.1.13.254
```

- Verify with show ip

```
show ip
```

HostA

```
NAME         : VPCS[1]
IP/MASK      : 10.1.10.1/24
GATEWAY      : 10.1.10.254
DNS          :
MAC          : 00:50:79:66:68:07
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```

Task 3 - Configure switch interfaces/VLANs, routing, and verify direct connectivity between all Hosts

- Configure switch interfaces and ensure direct connectivity works
- Apply proper IPv4 addresses to switch to switch interfaces
- Configure loopback 0
- On Switch A and B:
  - Create Host facing VLAN/Interface
  - Apply proper access VLAN to host facing interface
- Enable routing and ensure direct connectivity works between each host

SwitchA

```
vlan 10
    description HostA_SwitchA
vlan 11
    description HostB_SwitchA
interface 1/1/1
    no shutdown
    description To SwitchB
    ip address 192.168.3.0/31
interface 1/1/3
    no shutdown
    description To HostA_SwitchA
    no routing
    vlan access 10
interface 1/1/4
    no shutdown
    description To HostB_SwitchA
    no routing
    vlan access 114
interface loopback 0
    ip address 192.168.1.1/32
interface vlan 10
    description To HostA_SwitchA
    ip address 10.1.10.254/24
interface vlan 11
    description To HostB_SwitchA
    ip address 10.1.11.254/24
ip route 0.0.0.0/0 192.168.3.1
```

SwitchB

```
vlan 12
    description HostA_SwitchB
vlan 13
    description HostB_SwitchB
interface 1/1/1
    no shutdown
    description To SwitchA
    ip address 192.168.3.1/31
interface 1/1/3
    no shutdown
    description To HostA_SwitchA
    no routing
    vlan access 12
interface 1/1/4
    no shutdown
    description To HostB_SwitchA
    no routing
    vlan access 13
interface loopback 0
    ip address 192.168.1.2/32
interface vlan 12
    description To HostA_SwitchB
    ip address 10.1.12.254/24
interface vlan 13
    description To HostB_SwitchB
    ip address 10.1.13.254/24
ip route 0.0.0.0/0 192.168.3.0
```

SwitchA

```
SwitchA(config)# ping 10.1.12.1
PING 10.1.12.1 (10.1.12.1) 100(128) bytes of data.
108 bytes from 10.1.12.1: icmp_seq=1 ttl=63 time=11.8 ms
108 bytes from 10.1.12.1: icmp_seq=2 ttl=63 time=2.21 ms
108 bytes from 10.1.12.1: icmp_seq=3 ttl=63 time=1.91 ms
108 bytes from 10.1.12.1: icmp_seq=4 ttl=63 time=1.65 ms
108 bytes from 10.1.12.1: icmp_seq=5 ttl=63 time=2.21 ms
--- 10.1.12.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.659/3.977/11.889/3.961 ms

SwitchA(config)# ping 10.1.13.1
PING 10.1.13.1 (10.1.13.1) 100(128) bytes of data.
108 bytes from 10.1.13.1: icmp_seq=1 ttl=63 time=2.29 ms
108 bytes from 10.1.13.1: icmp_seq=2 ttl=63 time=2.33 ms
108 bytes from 10.1.13.1: icmp_seq=3 ttl=63 time=2.05 ms
108 bytes from 10.1.13.1: icmp_seq=4 ttl=63 time=2.32 ms
108 bytes from 10.1.13.1: icmp_seq=5 ttl=63 time=2.65 ms
--- 10.1.13.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.055/2.333/2.659/0.194 ms
```

SwitchB

```
SwitchB# ping 10.1.10.1
PING 10.1.10.1 (10.1.10.1) 100(128) bytes of data.
108 bytes from 10.1.10.1: icmp_seq=1 ttl=63 time=9.95 ms
108 bytes from 10.1.10.1: icmp_seq=2 ttl=63 time=2.04 ms
108 bytes from 10.1.10.1: icmp_seq=3 ttl=63 time=1.75 ms
108 bytes from 10.1.10.1: icmp_seq=4 ttl=63 time=1.92 ms
108 bytes from 10.1.10.1: icmp_seq=5 ttl=63 time=2.10 ms
--- 10.1.10.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.750/3.554/9.954/3.202 ms

SwitchB# ping 10.1.11.1
PING 10.1.11.1 (10.1.11.1) 100(128) bytes of data.
108 bytes from 10.1.11.1: icmp_seq=1 ttl=63 time=11.8 ms
108 bytes from 10.1.11.1: icmp_seq=2 ttl=63 time=2.05 ms
108 bytes from 10.1.11.1: icmp_seq=3 ttl=63 time=1.91 ms
108 bytes from 10.1.11.1: icmp_seq=4 ttl=63 time=2.10 ms
108 bytes from 10.1.11.1: icmp_seq=5 ttl=63 time=1.86 ms
--- 10.1.11.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.868/3.959/11.858/3.950 ms
```

Task 4 - Finish by adding a layer of security which blocks unwanted communication.

- In these examples –
    - Create an access-list to block HostA_SwitchA from connecting to other hosts
    - Create an access-list to block HostB_SwitchB from connecting to other hosts
- Once completed, you will be able to control which host is able to communicate, or not.

SwitchA

```
access-list ip ACL-IPv4-1
    10 comment Block pings from HostA_SwitchA
    20 deny icmp 10.1.10.1 any count
int 1/1/3
    apply access-list ip ACL-IPv4-1 in
```

HostA_SwitchA

```
VPCS> ping 10.1.11.1

10.1.11.1 icmp_seq=1 timeout
10.1.11.1 icmp_seq=2 timeout
10.1.11.1 icmp_seq=3 timeout
10.1.11.1 icmp_seq=4 timeout
10.1.11.1 icmp_seq=5 timeout

VPCS> ping 10.1.12.1

10.1.12.1 icmp_seq=1 timeout
10.1.12.1 icmp_seq=2 timeout
10.1.12.1 icmp_seq=3 timeout
10.1.12.1 icmp_seq=4 timeout
10.1.12.1 icmp_seq=5 timeout
```

SwitchB

```
access-list ip ACL-IPv4-1
    10 comment Block pings from HostB_SwitchB
    20 deny icmp 10.1.13.1 any count
int 1/1/4
    apply access-list ip ACL-IPv4-1 in
```

HostB_SwitchB

```
VPCS> ping 10.1.10.1

10.1.10.1 icmp_seq=1 timeout
10.1.10.1 icmp_seq=2 timeout
10.1.10.1 icmp_seq=3 timeout
10.1.10.1 icmp_seq=4 timeout
10.1.10.1 icmp_seq=5 timeout

VPCS> ping 10.1.12.1

10.1.12.1 icmp_seq=1 timeout
10.1.12.1 icmp_seq=2 timeout
10.1.12.1 icmp_seq=3 timeout
10.1.12.1 icmp_seq=4 timeout
10.1.12.1 icmp_seq=5 timeout
```

Appendix – Complete Configurations

SwitchA

```
SwitchA(config)# show run
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname SwitchA
user admin group administrators password ciphertext
AQBapWj7mDkCMP8rhH/OWg9vrInunZHSaT8gB78Rf/0FYNqpYgAAAMQl0Fq94J040Pwq4V
KbfOfxRL2qLpNxBJTxhZpkesF5oUSY2YjxEOJdFAiI2XcBGSMULGEfGELEPWEBoHlOcSvVeFj+27tmZ8G3MYsNFZHt030Js
DtwxobyVUhk3XSHg/2F
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
ssh server vrf mgmt
access-list ip ACL-IPv4-1
    10 comment Block Pings From HostA_SwitchA
    20 deny icmp 10.1.10.1 any count
vlan 1
vlan 10
    description HostA_SwitchA
vlan 11
    description HostB_SwitchA
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    description To SwitchB
    ip address 192.168.3.0/31
interface 1/1/3
    no shutdown
    description To HostA_SwitchA
    no routing
    vlan access 10
    apply access-list ip ACL-IPv4-1 in
interface 1/1/4
    no shutdown
    description To HostB_SwitchA
    no routing
    vlan access 11
interface loopback 0
    ip address 192.168.1.1/32
interface vlan 10
    description To HostA_SwitchA
    ip address 10.1.10.254/24
interface vlan 11
    description To HostB_SwitchA
    ip address 10.1.11.254/24
ip route 0.0.0.0/0 192.168.3.1
!
!
!
!
!
https-server vrf mgmt
```

SwitchB

```
SwitchB(config)# show run
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname SwitchB
user admin group administrators password ciphertext
AQBapaKszhG9P2egaDYa6VrR5UaGAfWKJZ178xtWd36nSwjWYgAAACCsEodK1eDIrhuAIcbfWully
2GqriNMT3HWLeIWo5cv/mZw14gNZ0fwFTSVAe0Hy0L7nSVSfdPIXVS7C5F8PeVk5oUl/kNls2XXOxdrlb6uz7l+/1EVb3St
L9QdDwsLSIKt
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
ssh server vrf mgmt
access-list ip ACL-IPv4-1
    10 comment Block Pings From HostB_SwitchB
    20 deny icmp 10.1.13.1 any count
vlan 1
vlan 12
    description HostA_SwitchB
vlan 13
    description HostB_SwitchB
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    description To SwitchA
    ip address 192.168.3.1/31
interface 1/1/3
    no shutdown
    description To HostA_SwitchB
    no routing
    vlan access 12
interface 1/1/4
    no shutdown
    description To HostB_SwitchB
    no routing
    vlan access 13
    apply access-list ip ACL-IPv4-1 in
interface loopback 0
    ip address 192.168.1.2/32
interface vlan 12
    description To HostA_SwitchB
    ip address 10.1.12.254/24
interface vlan 13
    description To HostB_SwitchB
    ip address 10.1.13.254/24
ip route 0.0.0.0/0 192.168.3.0
!
!
!
!
!
https-server vrf mgmt
```

HostA_SwitchA

```
VPCS> sh ip

NAME        : VPCS[1]
```

```
IP/MASK      : 10.1.10.1/24
GATEWAY      : 10.1.10.254
DNS          :
MAC          : 00:50:79:66:68:07
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```

HostB SwitchA

```
VPCS> sho ip

NAME         : VPCS[1]
IP/MASK      : 10.1.11.1/24
GATEWAY      : 10.1.11.254
DNS          :
MAC          : 00:50:79:66:68:06
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```

HostA SwitchB

```
VPCS> sho ip

NAME         : VPCS[1]
IP/MASK      : 10.1.12.1/24
GATEWAY      : 10.1.12.254
DNS          :
MAC          : 00:50:79:66:68:08
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```

HostB SwitchB

```
VPCS> sho ip

NAME         : VPCS[1]
IP/MASK      : 10.1.13.1/24
GATEWAY      : 10.1.13.254
DNS          :
MAC          : 00:50:79:66:68:05
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```