###### IP ACL

* Access Control List – also called Access Flows on 10x.
  + Access flows (ACLs) are intended to control the type of traffic on the network.
  + Prior to SAOS 10.5, access flows are intended for ingress filtering and classifying on a flow point. The filtered and/or classified traffic based on access flow rules on the flow point will follow the filter actions Deny or Allow or may be re-directed to another flow point (which may or may not be on the same FD). Access flows attached to a flow point are used to filter traffic on the flow point.
  + As of SAOS 10.5, in addition to access flows, **access profiles** are introduced. Access profiles contain a list of **embedded access flows**. The access profile attaches to an IP interface. The IP interface will classify and filter traffic according to the access profile rules.
* Supported on 514x, 516x, 517x
* **Classifiers supported for access profiles:**
  + SrcIPV4
  + SrcIPv6
  + DestIPV4
  + DestIPV6
  + IPProtocol
  + IPFragment
  + DSCP (IPv4)
  + L4SrcPort (IPv4, IPv6)
  + L4DstPort (IPv4, IPv6)
  + TCPFlags
  + ICMP message type (request, reply, router advertisement, router solicitation etc..)

Access profiles have global action of deny or allow (default is allow). Each of the embedded access flows will have an individual designation of deny or allow.

**IP ACL Supports:**

* + Access profile is attached to an IP interface  IP ACL
  + Access flow is attached to a flow point  Flow Point Access flow
  + Stats-collection on the Access Profile is not supported
  + Access profile can be attached to the remote management interface
  + Access profile on mgmtbr0 interface is NOT supported in SAOS 10.5.

Creation of Access Profiles

**Access profiles are added to a port or an IP interface**

***Topology:***



***Objective:***

Objective is to create and verify access profile. Below example replicates access profile supporting Source ip address classifiers.

***Procedure:***

* Go to the configuration terminal
  + config
* Enter the following command

diag@5170-209# access-profiles access-profile deny\_srcip diag@5170-209(access-profile)# stats-collection on diag@5170-209(access-profile)# type IP-interface diag@5170-209(access-profile)# access-flow deny\_srcip diag@5170-209(access-flow)# filter-action deny

diag@5170-209(access-flow)# classifier srcip1 filter-entry source-ip source-address 172.16.2.121/30

diag@5170-209(access-flow)# exit Applying 1 edit

diag@5170-209(access-profile)# exit

diag@5170-209(access-profiles)# exit

diag@5170-209# oc-if:interfaces interface intf12 config access-profile deny\_srcip

* Go back out of configuration terminal

# exit

* Check the access profile definition

You should see something like the following:

5170-209> sh access-profiles access-profile deny\_srcip

+ ACCESS PROFILE +

| KEY | VALUE |

+ + +

| Name | deny\_srcip |

| Type | IP-interface |

| Access Flow | |

| Name | deny\_srcip |

| Filter Action | deny |

| Classifier List | |

| Name | srcip1 |

| Filter Entry | |

| Filter Parameter | ciena-mef-classifier:source-ip |

| IP Source Address | 172.16.2.121/30 |

+ + +

With no IP ACL, ping from 5170-210 to interface 172.16.2.121 is successful

5170\*> file ping 172.16.2.121

PING 172.16.2.121 (172.16.2.121): 56 data bytes

64 bytes from 172.16.2.121: seq=0 ttl=64 time=0.293 ms

64 bytes from 172.16.2.121: seq=1 ttl=64 time=0.277 ms

64 bytes from 172.16.2.121: seq=2 ttl=64 time=0.320 ms

--- 172.16.2.121 ping statistics ---

3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max = 0.277/0.296/0.320 ms

After attaching IP ACL, ping from 5170-210 to interface 172.16.2.121 is denied

5170\*> file ping 172.16.2.121

PING 172.16.2.121 (172.16.2.121): 56 data bytes

--- 172.16.2.121 ping statistics ---

3 packets transmitted, 0 packets received, 100% packet loss

Test Case Results:

Passed: Yes No Verified by Date/Time Comments