Managing Access Control Lists

About ACLs

Access Controls List (ACL) filter the type of traffic that is allowed or denied access to the network or portion of the network. ACLs act as packet filters based on the criteria defined in the access list. ACLs defined on the SBC 1000/2000 do not take effect until they are applied to a port.

- Access Lists can filter incoming or outgoing packets on an interface, thereby controlling access based on source addresses, destination addresses, source layer4 ports, destination layer4 ports and IP protocol.
- ACLs are composed of a sequence of rules and the order of the rules is important. If an incoming packet matches multiple rules, the first matching rule is applied.
- A port may have only one input ACL and one output ACL.

After an ACL is created, it is bound (or applied) to the following interface/ports:

On the SBC 2000:

- Ethernet ports for inbound and forwarded traffic.
- Logical interfaces for inbound/outbound/forwarded traffic.
- ASM ACLs are applied to inbound and forwarded traffic only, and they are bound on the ASM interface.

On the SBC 1000:

- ACLs are bound to logical interfaces only.

Important Things to Remember When Creating an ACL

- Because the SBC 1000/2000 stops testing conditions after the first match, the order of the conditions is critical. The same permit or deny statements specified in a different order may result in a packet being passed under one circumstance and denied in another.
- Input-ACL process packets arriving at the SBC 1000/2000 before routing to an outbound interface. An inbound access list is efficient because it saves the overhead of routing look-ups if the packet is discarded because it is denied by the filtering tests.
- Output-ACLs process packets before they leave the SBC 1000/2000.
- Forward-ACLs process packets that are forwarded from one SBC 1000/2000 port to another.

SBC Support when ACL is applied

- Pinholing and RTP-Pinholing is not supported in SBC 1000/2000.
- SBC 2000 support is as follows:
  - ACL may be applied to an Ethernet port and it takes effect for all the VLANs on that port.
  - ACL may be applied to a Logical Interface and it is equivalent to applying ACL to a VLAN (note that a VLAN may have many Ethernet ports as members).
- SBC 1000 support is as follows:
  - ACLs cannot be applied to Ethernet ports.
  - ACL may be applied to a Logical Interface and it is equivalent to applying ACL to a VLAN (note that a VLAN may have many Ethernet ports as members).

Working with Access Control List Tables

1. In the WebUI, click the Settings tab.
2. In the left navigation pane, go to Protocols > IP > Access Control Lists.
To view an Access Control List's properties:

1. Click the pop-up icon (utive) next to the entry you want to view.
2. When you are finished, close the window.

To modify an Access Control List:

1. Click the expand (utive) Icon next to the entry you wish to modify.
2. Modify the table's Description as desired
3. Click OK.

To create an Access Control List table:

1. Click the Create (utive) icon.

2. Enter a descriptive name in the Description text field.
3. Click OK.

- To delete an entry, select the checkbox next to the entry and then click the Delete (utive) icon.

- Restrictions on Deleting ACLs
  An ACL may not be deleted if it is bound to any port or logical interface. However, you may delete or modify a rule within a bound ACL. Any modification or deletion is effective immediately.

Creating and Modifying Rules for IPv4 Access Control Lists

Creating and Modifying Rules for IPv6 Access Control Lists

SWe Lite and Modifying Rules for IPv4 Access Control Lists