Working with Access Control Lists

IP Access Control Lists (ACLs) are filters provided to protect the SBC from attacks by blocking IP traffic that may be harmful to the network. ACLs allows user to specify rules to permit or deny packets into the SBC.

General rules:

- Only signaling and management IP traffic is subjected to IP ACL filtering. Media IP traffic (RTP) is not subject to IP ACL filtering.
- In most cases, you only need to define ACLs on the UNTRUSTED (or EXTERNAL) interface groups. These interfaces communicate with third parties, such as a trunk group to another service provider or phones from the public internet.
- Each ACL is configured with a unique precedence value between 1 and 65,535. ACLs are evaluated in the order of precedence, with 1 being the highest priority, and the first ACL evaluated. For a rule that is matched by two separate ACLs, the one that is evaluated first (lowest number= higher priority) takes precedence.
- When you define an ACL rule, it takes precedence over system-defined rules. For example, if there is a third-party management system exce eding the pre-defined rate for SNMP traffic, you can set up an ACL to Override the default rules and and allow all ("white list") traffic.

When you create a SIP Port, the system also creates an ACL that allows connection attempts to all ports on the IP address of the SIP Port. For example, SSH to the IP address is allowed. To prevent unwanted access, ACLs should be used.

Note
The maximum number of operator ACLs allowed on SBC Cores are:

- SBC 5000/7000 series: 11,231
- SBC SWe: 2,527

See Managing SBC Core System Security topic for description of ACL features.

Additional topics in this section: