SIP Profile Strict Security mode

SIP Profile with Strict Security mode enabled will have SIP traffic from unregistered SIP User Agent being filtered in the IP firewall, with the exception of SIP REGISTER message. After a successful registration, source IP of the UA is whitelisted, which means future SIP traffic from this UA will bypass the firewall.

This feature can be selectively configurable for each SIP Profile. You can turn on Strict Security on external SIP Profile and leaving it disabled on all internal SIP Profiles where security is less of a concern.

Please note that this mode should be disabled on MSBG SIP profile with IP starting with 127.

SIP Trunking with Strict Security mode

All SIP messages from IPs in ACL list for inbound will bypass Strict Security. If you have Strict Security enabled and you have SIP Trunks, the SIP Trunk IP must be included in the ACL list for inbound for that SIP Profile. Otherwise, SIP OPTIONS pings will be filtered.

Limitations

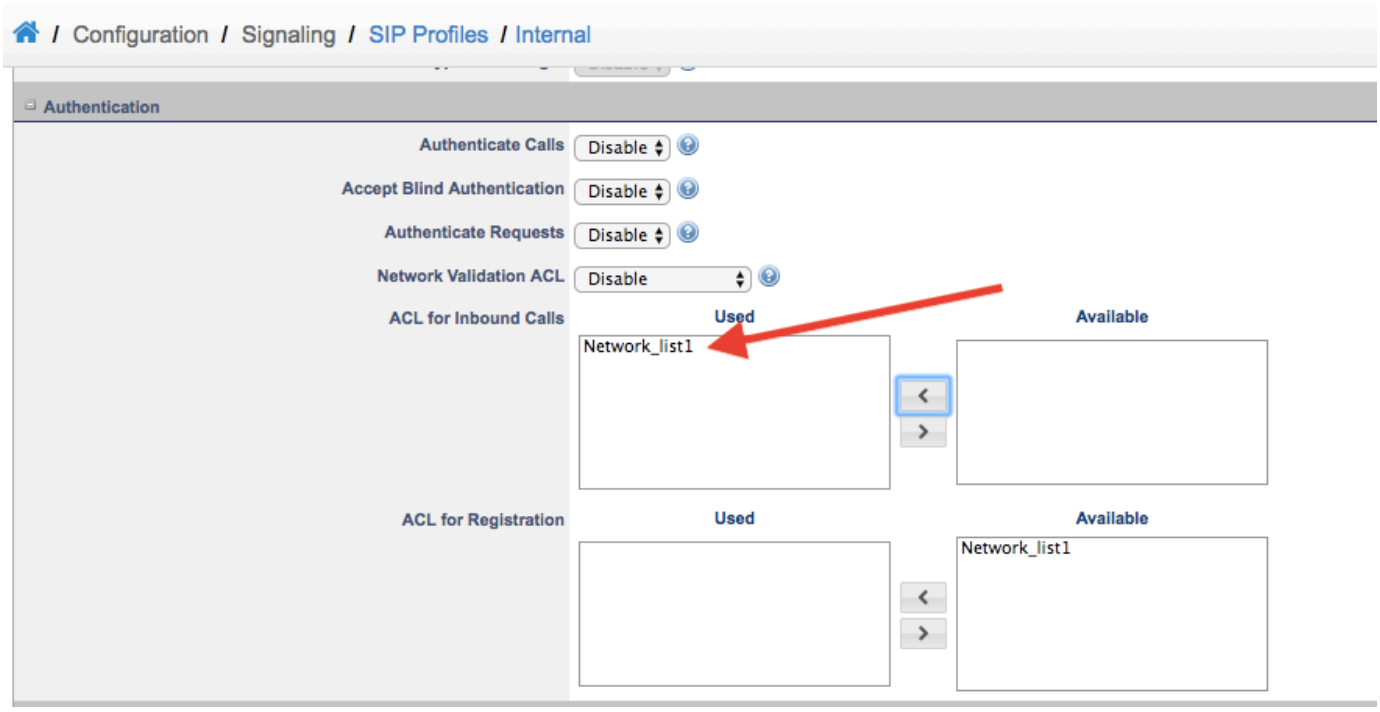
This feature has a limitation with multiple UAs using the same source IP or UAs behind NAT. These UAs use the same source IP to send SIP Messages to the SBC, as a result, we cannot individually restrict their SIP traffic flow. If Strict Security mode is enabled, the source IP for these UAs must be listed in inbound ACL to ensure normal SIP signalling operation for all these UAs.

Configuration

To enable Strict Security mode for a SIP Profile, access the following web UI page on your SBC and change Strict Security to "enable".

/SAFe/fs_sip_profile_config/edit/sip/profile/[SIP_Profile_Name]/

Existing ACL inbound will be effective for Strict Security. To modify this ACL list, go to the Authentication section in the same SIP Profile configuration page and add/Remove ACL list to "ACL for Inbound Calls".



If you want to create a new ACL list, please point your browser to /SAFe/fs_acl_config.