InnoMedia ESBC Application Notes

Access Control List

Product Management Group, InnoMedia

Version: 1.5

June 2015

TABLE OF CONTENTS

1 THE INNOMEDIA ESBC ACCESS CONTROL LIST

An ACL (Access Control List) is required to protect the ESBC on the specified Ethernet interfaces from undesired access attempts, scans etc. It should be noted that the ACL works together with the ESBC's built-in stateful firewall protection, which independently provides its own protection against unauthorized access. This document describes how the ESBC ACL feature filters network traffic.

Note: the following ACL rule recommendations apply to the ESBC 8xxx, ESBC 9xxx, and ESBC 10K models.

1.1 ACL Rule Process:

(1) ACL rules for WAN and LAN interfaces are processed independently. That is, if the rule is configured for the WAN interface, it applies to WAN traffic only.

(2) The ESBC matches incoming UDP and TCP packets to the ACL rules and applies the appropriate filtering.

(3) Traffic that comes into the ESBC is compared to the ACL rules sequentially from the top of the list downwards. The ESBC continues to match the packet against the rules until it finds a match. If no match is found, the traffic is dropped. In other words, if the ACL feature is enabled, there is an implicit 'drop' rule that will block packets that do not match any rules for that interface.

(4) If certain application ports are only to be permitted for certain IP addresses corresponding to allowed hosts, these ports need to be configured to allow traffic from these hosts and drop packets from any other hosts.

(5) If there is no rule configured for the interface, then the ESBC behaves as if the "ACL" feature is disabled for this particular interface. For example, when ACL is enabled and there are one or more WAN-side ACL rules, but no LAN-side ACL rules, the voice LAN interface is NOT blocked.

(6) However, the existence of even a single ACL rule for a particular interface will invoke the implicit 'deny' rule at the end of the list. For example, a single 'deny' rule on the WAN interface without any 'permit' rules set up on the WAN interface will block ALL packets on the WAN interface because of the implicit 'deny'. The LAN interface will not be affected. **NOTE:** Care should be taken when configuring the ACL rules in this way since ALL traffic to the WAN interface may be inadvertently blocked, rendering the unit unreachable.

(7) ESBC initiated connections, are monitored by the rules associated with the internal firewall. The ACL rules will not block traffic which is initiated by the ESBC.

(8) ACL rules can be applied to the WAN and/or Voice LAN interfaces, but cannot be applied to management/bridge/router port.

The Access Control List entry is composed of the following fields:

- No.: Sequential number of rule
- Interface: Apply ACLs to WAN and/or LAN
- Optional protocols include 'TCP', 'UDP' and 'TCP+UDP'
- Source IP or Network /Mask: (e.g., 0.0.0.0/0.0.0.0, 192.168.1.1/255.255.255.255, 172.16.1.1/255.255.0.0, or 192.168.1.0/24)
- Service Port, indicating the TCP or UDP port numbers. A service port range can be used, for example, 'starting port' and 'ending port'.

- Action: “Permit”, “Deny” and “Drop.” “Deny” means reject a request, and “Drop” means no response for a request.

Note:

- Default SIP ports used in the ESBC.
  - B2BUA 5060 for UDP and TCP, 5061 for TLS
  - SIP ALG 5080
- RTP port range “30000-64000” (ESBC-10K), and range “62000-64000” (ESBC 9xxx/8xxx). RTP ports do not need to be explicitly entered in the permit-rule list, since those ports are handled by the ESBC’s internal firewall.
- The maximum number of rules which can be configured on the ESBC is 250.

2 SAMPLE ACL RULES

It should be noted that the WAN ACL rules specified below are recommendations only. The rules used in actual deployments will depend on customer and operator needs. Recommendations are only provided below for WAN interface ACL rules, as LAN interface rules will be highly customer-dependent.

WAN Interface

#	Protocol	Source/netmask	Starting port	Ending port	Action	Comment
1	TCP	IP range/mask of permitted hosts	8080	8080	Permit	HTTP connections
2	TCP	0.0.0.0/0	8080	8080	Drop	Drop HTTP connections from unauthorized hosts
3	TCP	IP range/mask of permitted hosts	443	443	Permit	HTTPS connections
4	TCP	0.0.0.0/0	443	443	Drop	Drop HTTPS connections from unauthorized hosts
5	TCP & UDP	IP range/mask of permitted hosts	22	22	Permit	only added if WAN ssh is enabled
6	TCP & UDP	0.0.0.0/0	22	22	Drop	Drop SSH connection requests from unauthorized hosts
7	TCP & UDP	IP range/mask of permitted hosts	161	162	Permit	SNMP connections
8	TCP & UDP	0.0.0.0/0	161	162	Drop	Drop SNMP connections from unauthorized hosts
9	TCP & UDP	IP range/mask of SIP servers	5060	5060	Permit	SIP traffic from authorized hosts
10	TCP & UDP	IP range/mask of SIP servers	5061	5061	Permit	Only added if TLS is used
11	TCP & UDP	IP range/mask of SIP servers	5080	5080	Permit	Only added if SIP-ALG mode is used
12	TCP & UDP	0.0.0.0/0	5060	5081	Drop	Drop SIP traffic from unauthorized hosts
13	TCP & UDP	0.0.0.0/0	1	65535	Permit	Final permit all rule for other traffic

3 ACL PROVISIONING TAGS

Provisioning TAG	Available Values/Examples	TAG Usage Rules	Section TAG Usage Rules
SYSTEM_ACL_ENABLED	Integer (0/1) 0: Disabled 1: Enabled	• If no TAG or TAG value blank, the ESBC uses original value	1. X =< 250 2. When SYSTEM_ACL_ENABLED = 0, the ESBC ignores all other TAGs of this Section. 3. When defining SYSTEM_ACL_ENABLED = 1, the following TAG must be present. a) SYSTEM_ACL_1 4. If any one of these rules fails, the ESBC uses original values of TAGs of this Section.
SYSTEM_ACL_X	String(length: 0-128) **Format:** Interface/Protocol/Source_IP/Source_Mask/Host_Starting_Port/Host_Ending_Port/Action Interface: lan, wan Protocol: tcp, udp, tcp+udp Action: permit, deny, drop **For example:** • SYSTEM_ACL_1 = lan/tcp/192.168.1.1/255.255.255.0/1/65535/permit • SYSTEM_ACL_2 = wan/udp/10.20.30.1/28/100/200/deny	• If "SYSTEM_ACL_1" is left blank, ESBC will delete all System ACL entries	