InnoMedia ESBC Application Notes

Security Audit Recommendations

Product Management Group, InnoMedia

Feb 2016

TABLE OF CONTENTS

ESBC Security Audit Recommendations

Target Analysis and Attacks

Network elements on unprotected networks can be vulnerable to, for instance, Fraud or Denial of Service attacks. Hackers often search for network devices with easy access. They may begin looking for vulnerabilities by scanning the platforms. Once a vulnerability has been identified, it may be used later for a larger attack.

Attacks can be further categorized into Protocol level attacks, and Application Level Attacks.

- Protocol Level Attacks. Protocol level attacks can abuse features of protocols such as ICMP and TCP/IP by flooding malformed or incomplete packets to the target.
- Application Level Attacks. These types of attacks target vulnerabilities in managerial applications and SIP signaling protocols.

ESBC Features for Security Audit

ESBC Built-in Steteful Firewall Protection

The ESBC implements a built-in stateful firewall which continually monitors all connection states. Kernel protection includes (but not limited to):

- Dropping any packets from unknown sources.
- Preventing IP spoofing attacks from the WAN interface
- Dropping non-SIP packets
- Dropping REGISTER requests from WAN interfaces

In addition to the built-in firewall protection, there are service/environment dependent security settings which must be configured properly by service providers to assure reliable and secure services.

Security Feature Configurations: Close Possible Vulnerabilities

1. Change default login password to the ESBC management console, including accounts for administrator, technician, and operator. (See Figure 1)
2. Monitor the audit log for suspicious events such as unauthorized ESBC administrative console login attempts and system operational tasks performed. (See Figure 2)
3. Disable unused applications, such as:
    a. Disable Ping from WAN interface to prevent any responses to ICMP messages on the WAN interface. (Strongly suggested. See Figure 3)
    b. SSH connection via WAN (See Figure 4)
4. Change default port number for WEB access via WAN, and enable “Only HTTPS for access WEB via WAN” interface. (See Figure 4)
5. Change SNMP community strings, if SNMP service is enabled. (See Figure 5). These strings will need to match community strings on the SNMP manager.

6. When there is a requirement for LAN hosts to access data services through the ESBC to the Internet, this access can be restricted to specific devices only (see Figure 8) Data access can be restricted according to:
   - hosts within particular IP address ranges
   - hosts within particular subnets
   - hosts with specified MAC addresses
   - ports employed by applications

   Furthermore, a schedule may be applied to restrict access to within certain time intervals only.

Security Feature Configurations: SIP Layer Protection Configurations

1. Restrict SIP trust domain (realm) configurations toward the WAN interface, i.e. the service provider network. (See Figure 6)
   a. Check the domain/host part of the To header in incoming requests
   b. Check the source IP address of incoming SIP messages
2. Restrict SIP trust domain (realm) toward the LAN interface, i.e., the enterprise network. (See Figure 7)
3. Apply SIP firewall scripts. Allow only friendly IP address to access the ESBC. (See Figure 9).

Security Feature Configurations: ACL Configurations

Access Control List Configurations, for WAN and/or LAN interfaces.

Note:

1. The following ACL rule recommendations apply to the ESBC 8xxx, ESBC 9xxx, and ESBC 10K models.
2. Please refer to the InnoMedia document "ESBC ACL Application Notes" for further details.

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	
3	TCP	IP range/mask of permitted hosts	443	443	Permit	HTTPS connections
4	TCP	0.0.0.0/0	443	443	Drop	
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 all 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	
9	TCP & UDP	IP range/mask of SIP servers	5060	5060	Permit	
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	
13	TCP & UDP	0.0.0.0/0	1	65535	Permit	

LAN Interface

ACL rules for the LAN interface are optional, and will be highly dependent on the needs of the service provider and the enterprise.

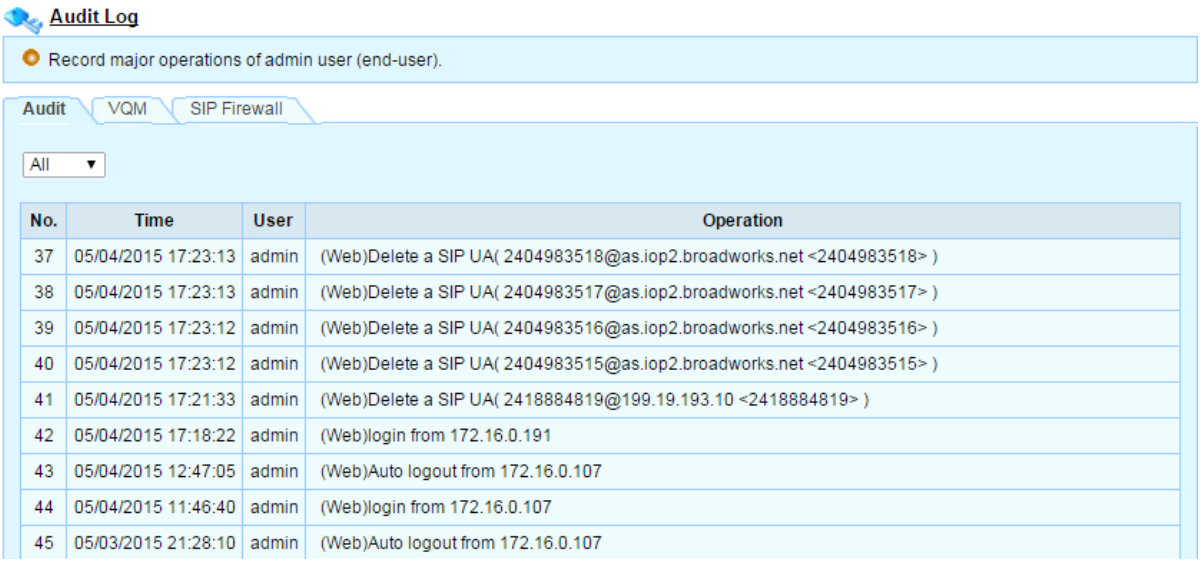
#	Protocol	Source/netmask	Starting port	Ending port	Action	Comment
1	TCP	0.0.0.0/0	22	22	Drop	Added if LAN ssh is disabled.
2	TCP	0.0.0.0/0	80	80	Drop	Added if LAN WEB console access is disabled.
3	TCP	0.0.0.0/0	443	443	Drop	
4	TCP	0.0.0.0/0	54321	54321	Drop	
5	UDP	0.0.0.0/0	53	53	Drop	
6	UDP	0.0.0.0/0	67	68	Drop	
7	UDP	0.0.0.0/0	123	123	Drop	
8	UDP	0.0.0.0/0	1900	1900	Drop	
9	UDP	0.0.0.0/0	5080	5081	Drop	Added if SIP ALG is not used.
10	TCP&UDP	0.0.0.0/0	161	162	Drop	
11	TCP&UDP	0.0.0.0/0	1	65536	Permit	

Administrator

Administrator Account Management

No.	UserID	Full Name	Contact	Admin Right	Read Only	Access Control	Action
1	admin			Admin		LAN and WAN	
2	oper			Operator		LAN and WAN	
3	tech			Technician		LAN and WAN	

Figure 1. Administrative user account settings (System>Administrator)



Audit Log

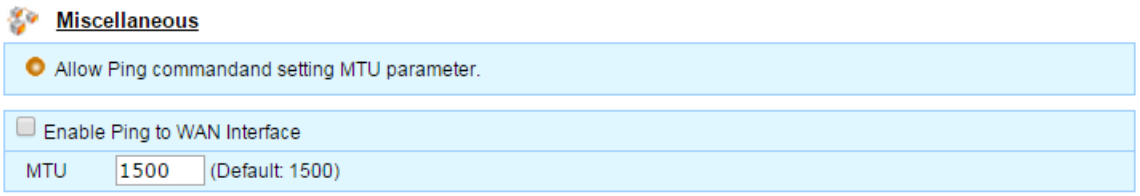
Record major operations of admin user (end-user).

Audit | VQM | SIP Firewall

All

No.	Time	User	Operation
37	05/04/2015 17:23:13	admin	(Web)Delete a SIP UA(2404983518@as.iop2.broadworks.net <2404983518>)
38	05/04/2015 17:23:13	admin	(Web)Delete a SIP UA(2404983517@as.iop2.broadworks.net <2404983517>)
39	05/04/2015 17:23:12	admin	(Web)Delete a SIP UA(2404983516@as.iop2.broadworks.net <2404983516>)
40	05/04/2015 17:23:12	admin	(Web)Delete a SIP UA(2404983515@as.iop2.broadworks.net <2404983515>)
41	05/04/2015 17:21:33	admin	(Web)Delete a SIP UA(2418884819@199.19.193.10 <2418884819>)
42	05/04/2015 17:18:22	admin	(Web)login from 172.16.0.191
43	05/04/2015 12:47:05	admin	(Web)Auto logout from 172.16.0.107
44	05/04/2015 11:46:40	admin	(Web)login from 172.16.0.107
45	05/03/2015 21:28:10	admin	(Web)Auto logout from 172.16.0.107

Figure 2. The ESBC Audit Log (System > Audit Log)



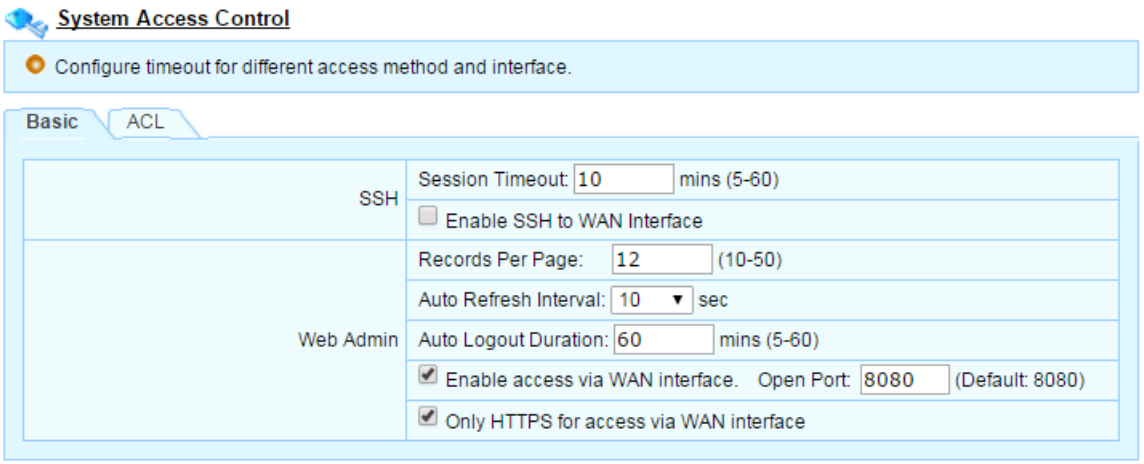
Miscellaneous

Allow Ping commandand setting MTU parameter.

Enable Ping to WAN Interface

MTU 1500 (Default: 1500)

Figure 3. Disable/Enable Ping to the ESBC WAN interface (Network > Miscellaneous)



System Access Control

Configure timeout for different access method and interface.

Basic | ACL

SSH	Session Timeout: 10 mins (5-60)
	Enable SSH to WAN Interface
Web Admin	Records Per Page: 12 (10-50)
	Auto Refresh Interval: 10 sec
	Auto Logout Duration: 60 mins (5-60)
	Enable access via WAN interface. Open Port: 8080 (Default: 8080)
	Only HTTPS for access via WAN interface

Figure 4. System Access Control –Basic (System > Access Control)

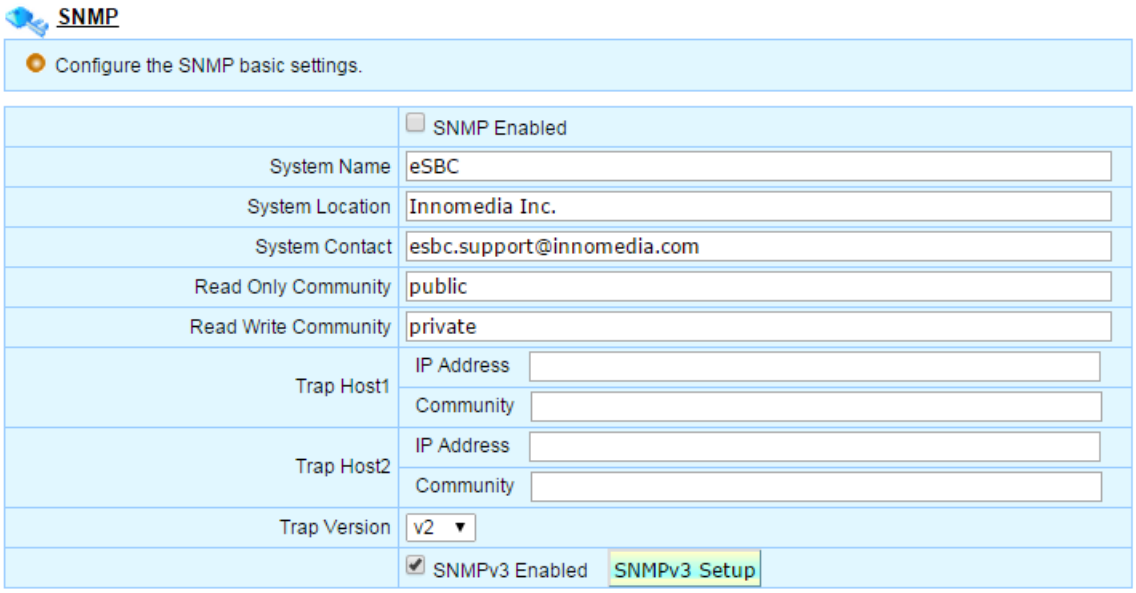


Figure 5. SNMP Community String Configurations (System > SNMP)

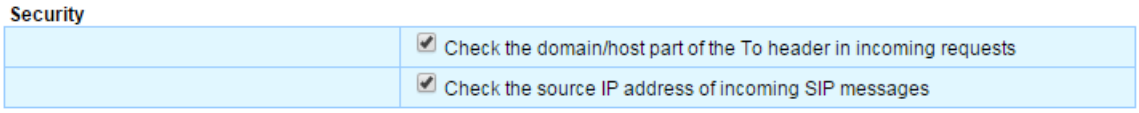


Figure 6. SIP trusted domain (realm) validation (Telephony > Trunk SIP Profile)

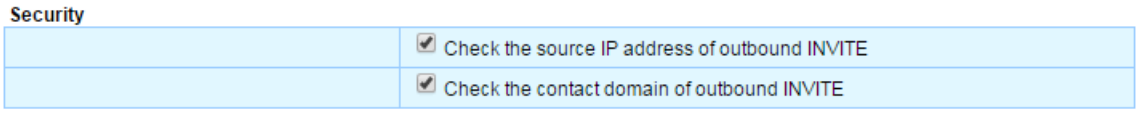


Figure 7. SIP trusted domain (realm) validation toward the LAN interface
(Telephony > SIP-PBX > PBX SIP-Profile > Target PBX model)

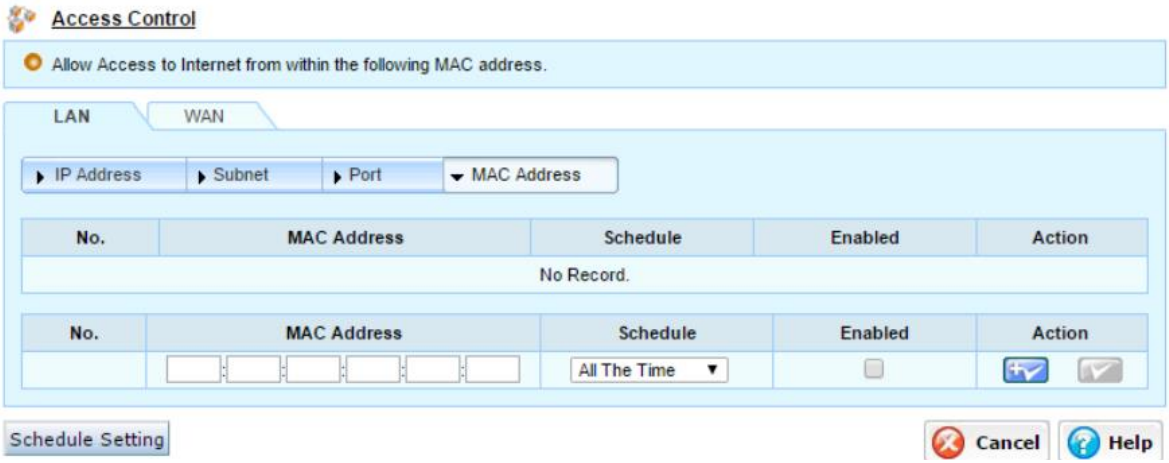


Figure 8. Specifying and Controlling LAN hosts for Data Access
(Network > Advanced > Access Control)

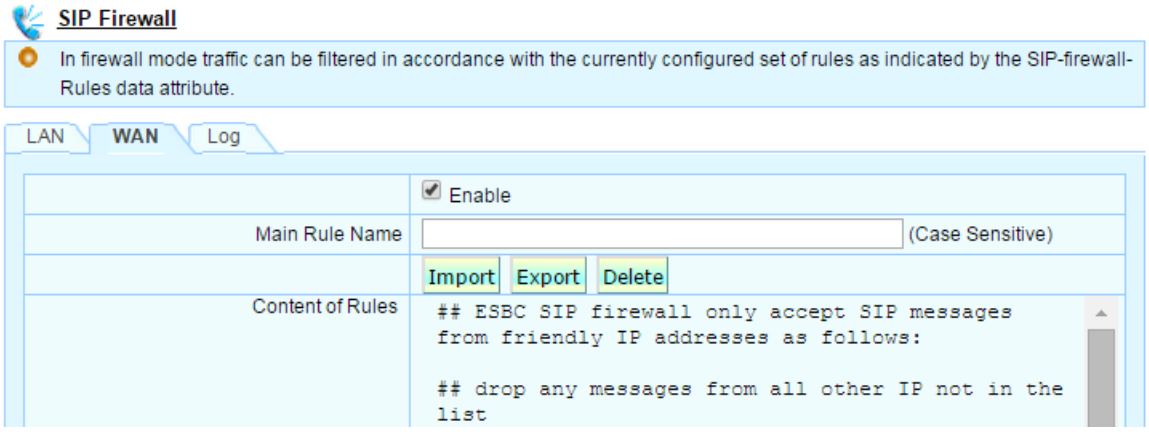


Figure 9. Enabling SIP Firewall Protection

Note:

1. GUI access:
    a. SIP Trunk Service: Telephony > Advanced > Firewall
    b. Hosted Voice Service: Telephony > SIP ALG > Firewall
2. Firewall script programming, refer to the document: ESBC SIP Firewall Rules.