InnoMedia ESBC Application Notes

SIP Firewall Rules

Version: 2.0

Feb 2016

TABLE OF CONTENTS

1 ESBC SIP FIREWALL RULES

ESBC firewall rules (ESBC-FW) enable the operator to design and select predefined rule-sets that define all messages to be processed by the ESBC. ESBC-FW is script-based, and follows the same structure and syntax as SIP Header Manipulation Rules (SHMR). It first filters all traffic according to the firewall rules (if a firewall rule script is applied) before handling the resulting traffic that needs to be processed. Firewall rules can be applied independently on the following interfaces:

- ESBC WAN interface
- ESBC LAN interface (only for NAT-Voice ports)

SIP Firewall rules are presented in a structured manner within a script file which can be imported into the ESBC for the applicable LAN or WAN interface. Basically, the ESBC executes the rules in a top-down manner unless multiple rule-sets are defined within a script. Each rule set is defined by the designation of "sip-manipulation" at the start of each rule set in the script. At the time a script is imported, it requires

a) the identification of the rule-set that the firewall will use first (in case it has multiple rule-sets) and

b) to be applied for successful import of the script.

If there is an intention to execute other rule-sets that are defined within the script, then the next rule-set can be called within this first rule-set by the parameter "new-value" and referencing the next rule-set's "sip-manipulation" name.

On the SIP Firewall GUI page, the 'Main Rule Name' can be defined, which specifies the initial Rule Set that the ESBC will use (see Figure 2. Import Firewall Rule Set). If the Main Rule Name is left blank, the ESBC starts from the beginning of the script file.

1.1 Structure of ESBC-SIP Firewall Rules

- **sip-manipulation** (keyword)
- **name** (main rule name, case sensitive). One script file may contain multiple rule names.
- Comments (new line started with # sign)
- **description** (keyword)
- One or multiple header rules

1.2 Header Rules

Parameters	Values and descriptions
header-rule	A keyword
name	The name given to this particular header-rule
message	- **request** (sip request message type) - **reply** (sip reply message type, such as 1xx, 2xx,…) - **any** (either request or reply message types)
sip-method	SIP methods, such as: **INVITE**, **REGISTER**, **ACK**, and so on…
header-name	The name of the header to which this rule applies. The name that is entered here must match a header name.
from-ipnet	Either a Single Source IP address or a Source Subnet can be used as follows:

	- Source IP address: xxx.xxx.xxx.xxx/32 or xxx.xxx.xxx.xxx/255.255.255.255 (e.g., 192.168.3.1/32 or 192.168.3.1/255.255.255.255) - Source subnet: xxx.xxx.xxx.xxx/mask-bits (e.g., 192.168.3.0/24, or 192.168.3.0/255.255.255.0)
from-port	Source port number
to-ipnet	Either a Single Destination IP address or a Destination Subnet can be used as follows: - destination IP address: xxx.xxx.xxx.xxx/32 or xxx.xxx.xxx.xxx/255.255.255.255 (e.g., 192.168.3.1/32 or 192.168.3.1/255.255.255.255) - destination subnet: xxx.xxx.xxx.xxx/mask-bits (e.g., 192.168.3.0/24, or 192.168.3.0/255.255.255.0)
to-port	Destination port number
protocol	TCP, UDP, any
equal-value	The value to be matched with the header value. 'Regular expressions' may be used.
change-to-value	The new value to be assigned to the header value.
process	Actions to take if the rules matched. - **fw-accept**. Allow the messages to pass through ESBC. - **fw-drop.** Discard the messages. - **fw-reject**. Reject incoming SIP requests and reply with SIP error response code specified in "**change-to-value**" field. Incoming SIP responses are simply discarded. - **sip-manip.** Firewall rule set manipulation

2 BASIC FIREWALL RULE TEMPLATE

```
## ESBC SIP firewall template

sip-manipulation
name                                    rule_name
description                             SIP Firewall Rule Set A

        header-rule
                name
                message
                sip-method
                header-name
                protocol
                equal-value
                change-to-value
                process
```

2.1 Import the firewall script to the ESBC

1. Navigate to Telephony > ADVANCED > Firewall.
2. Choose LAN and/or WAN tab to work with

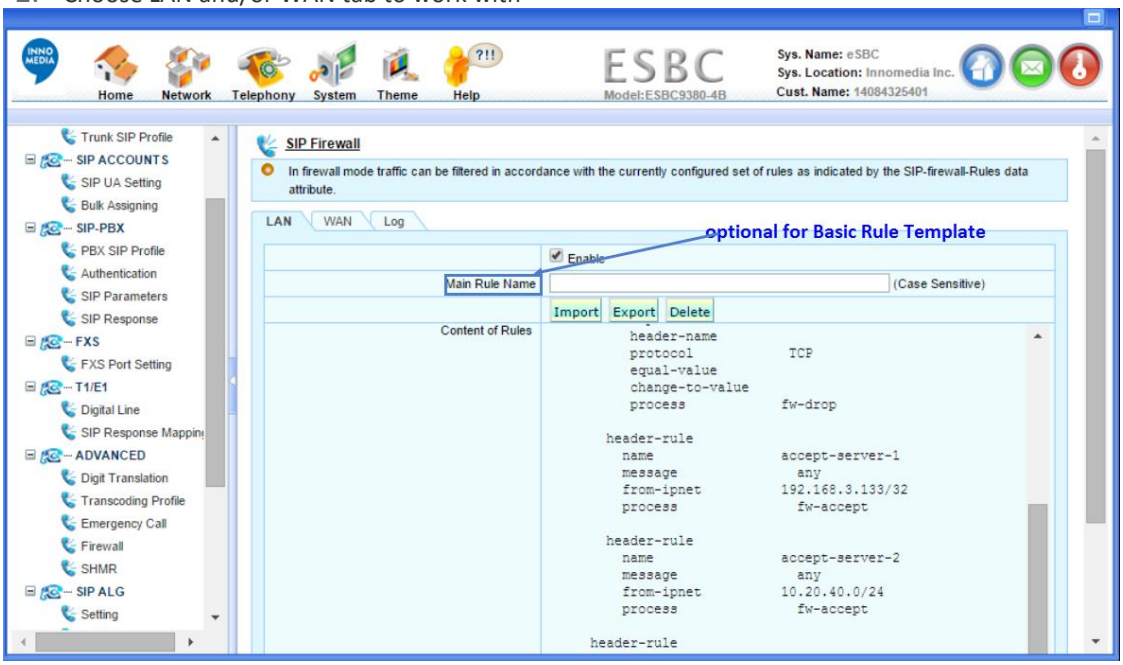

Figure 1. Import Basic Firewall Rules

2.2 Example - Basic

```
## ESBC SIP firewall
## 1. Accept SIP messages from friendly IP addresses as follows:
##    single IP: 192.168.3.133/255.255.255.255 or 192.168.3.133/32
##    subnet 10.20.40.0/255.255.255.0 or 10.20.40.0/24
##    TCP protocol only
## 2. Drop any messages from all other IP not in the friendly IP list

sip-manipulation
name                                Example-BasicSIPFirewall
description                         SIP Firewall Rule for ESBC

               header-rule
               name                 accept-server-1
               message              any
               protocol             TCP
               from-ipnet           192.168.3.133/32
               process              fw-accept

## If protocol TCP is not specified, both TCP and UDP are accepted.

       header-rule
               name                 accept-server-2
               message              any
               protocol             TCP
               from-ipnet           10.20.40.0/24
               process              fw-accept

       header-rule
               name                 drop-any
               message              any
               from-ipnet           0.0.0.0/0
               process              fw-drop
```

3 ADVANCED FIREWALL TEMPLATE (RULE-SET)

If subroutines are to be defined and the execution of the firewall script should start from a main rule, an advanced firewall template as shown below can be used as a starting point for the rule-sets that need to be applied to the ESBC.

```
## Advanced ESBC SIP firewall template
## Script execution starting point: RuleSetMAIN

sip-manipulation
name                                    RuleSetA
description                             SIP Firewall Rule Set A

        header-rule
                name
                message
                sip-method
                header-name
                equal-value
                change-to-value
                process

sip-manipulation
name                                    RuleSetMAIN
description                             SIP Firewall Rule Set B

        header-rule
                name
                message
                from-ipnet
                change-to-value
                process                 sip-manip
```

3.1 Import the advanced firewall script to the ESBC

When the rule-sets are applied, it is necessary to input the rule name, the entry point of script execution into the “Main Rule Name” text box.

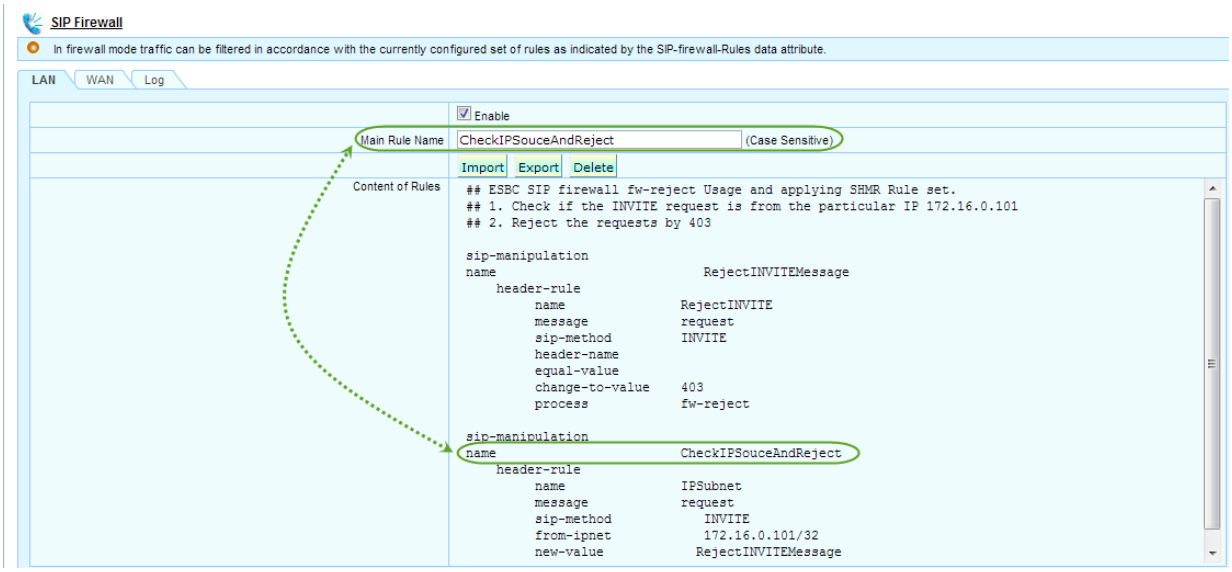

Figure 2. Import Firewall Rule Set

3.2 Example -Advanced: ESBC Firewall Rule Set

```
## ESBC SIP firewall fw-reject Usage and applying SHMR Rule set
## 1. Check if the INVITE request is from the particular IP 172.16.0.101
## 2. Reject its INVITE requests by 403

sip-manipulation
name                                    RejectINVITEMessage
        header-rule
                name                    RejectINVITE
                message                 request
                sip-method              INVITE
                header-name
                equal-value
                change-to-value         403
                process                 fw-reject

sip-manipulation
name                                    CheckIPSouceAndReject
        header-rule
                name                    IPSubnet
                message                 request
                sip-method              INVITE
                from-ipnet              172.16.0.101/32
                new-value               RejectINVITEMessage
                process                 sip-manip
```