Security Target – syslog-ng Store Box

For CSPN evaluation

Security Target Reference

Title	One Identity syslog-ng Store Box Security Target
Revision	1.1
Publication date	20/06/2018
Author	One Identity

Table of contents

Product Identification

Editor	One Identity
Editor’s website	https://www.oneidentity.com
Commercial name of the product	syslog-ng Store Box (SSB)
Evaluated version	5.0.1
Product category	Log management

Glossary

HA	High Availability
IPMI	Intelligent Platform Management Interface
Log	Log message and its accompanying meta data
Logspace	Logstore + Index files
SNMP	Simple Network Management Protocol
SSB	syslog-ng Store Box
TLS	Transport Layer Security
TOE	Target of Evaluation. It is the product under evaluation.

References

[ADM_GUIDE]	The syslog-ng Store Box 5 LTS Administrator Guide https://www.balabit.com/documents/ssb-5.0-guides/en/ssb-guide-admin/html/index.html
[USR_GUIDE]	The syslog-ng Store Box 5 LTS User Guide https://www.balabit.com/documents/ssb-5.0-guides/en/ssb-guide-user/html/index.html
[RFC_SYSLOG]	Syslog RFC 5424 https://tools.ietf.org/html/rfc5424
[RFC_SNMP]	SNMP RFC 1157 https://tools.ietf.org/html/rfc1157
[RFC_BSD]	BSD RFC 3164 https://www.ietf.org/rfc/rfc3164.txt
[SSB_RECO]	Security checklist for configuring syslog-ng Store Box https://www.balabit.com/documents/ssb-5.0-guides/en/ssb-security-recommendations-whitepaper/html/index.html

Product Description

General description

The syslog-ng Store Box™ (SSB) is a high-performance, high-reliability log management appliance that builds on the strengths of syslog-ng Premium Edition. With SSB, you can search logs, secure sensitive information with granular access policies, generate reports to demonstrate compliance, and forward log data to 3rd party analysis tools.

It collects, processes, stores, monitors, and manages log messages. This appliance can receive system (syslog and eventlog) log messages from your network devices and computers, store them in a trusted and signed logstore, and also classify the messages using artificial ignorance.

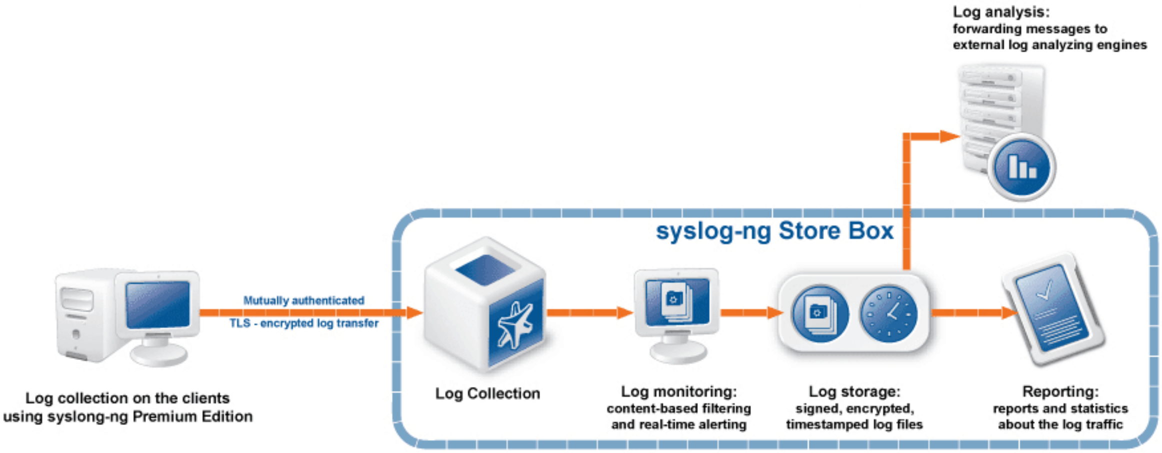

Figure 1: Syslog-ng Store Box

The most notable features of SSB are as follows:

- Secure log collection using Transport Layer Security (TLS).
- Trusted and encrypted log storage.
- Ability to collect log messages from a wide range of platforms, including Linux, Unix, BSD, Sun Solaris, HP-UX, IBM AIX, IBM System i, as well as Microsoft Windows.
- Forwards messages to log analysing engines.
- Classifies messages using customizable pattern databases for real-time log monitoring, alerting, and artificial ignorance.
- Real-time log monitoring and alerting.
- Strict, yet easily customizable access control to grant users access only to selected log messages.

- Ability to search log data in multiple logspaces, whether on the same SSB appliance or located on a different appliance, even in a remote location.

SSB is configured and managed from any modern web browser that supports HTTPS connections, JavaScript, and cookies.

Basic properties of SSB:

Network interfaces	• **External:** communication between SSB and the clients • **Management:** communication between SSB and auditors/administrator
Receiving logs	**Encrypted channel**: TLS-encrypted messages (default port is 6514) using the IETF-syslog protocol
Firmware	• **Boot:** provides hardware support and starts the Core firmware • **Core:** provides the web interface, receives and processes log messages, …

ToE Security features

The ToE is SSB as a software, with specified configuration.

The components of the ToE, its data handling and the relevant documentation are described below.

The following components are in the scope of the ToE:

- **Log storage**: ensured confidentiality and integrity of stored logs (stored in “logstore” files - encrypted binary files).
- **Secure management**: administration functions in order to configure the syslog-ng Store Box through web interface (configure user rights, sources, …).
- **Encrypted communication**: logs received through secure (TLS encrypted) channel.

Hardware and third-party support software (e.g. operating system, web server, DBMS) are **excluded from the scope of the ToE**.

In order to comply with the evaluated configuration, the following features must not be used:

- **Remote administration via SSH or IPMI**
- **High Availability**
- **SQL source and destination**
- **RLTP source**
- **Backup, share and archive**

- **SQL query capabilities of the user interface**
- **Remote user databases**

The following figure describes the scope of the ToE (components and data).

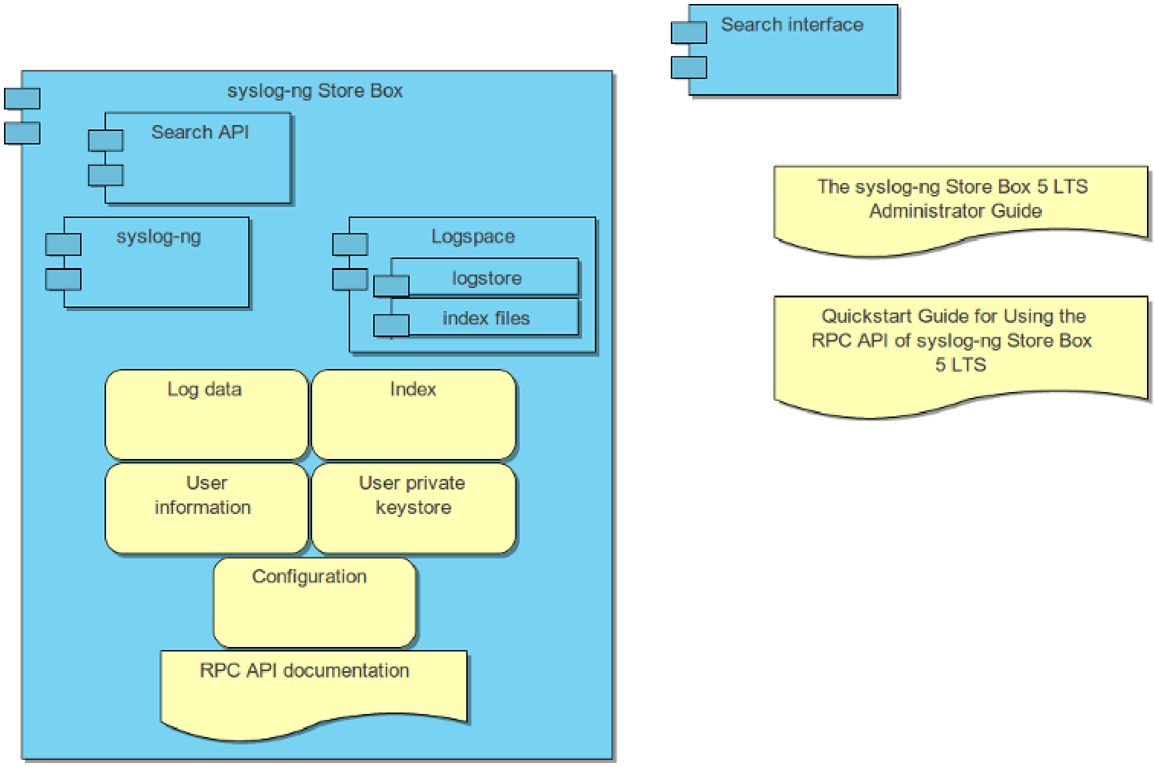

Figure 2: ToE Scope

Product usage

The following procedure illustrates the route of a log message from its source on the syslog-ng client to the syslog-ng Store Box. As previously stated, the **ToE is the server part of syslog-ng**.

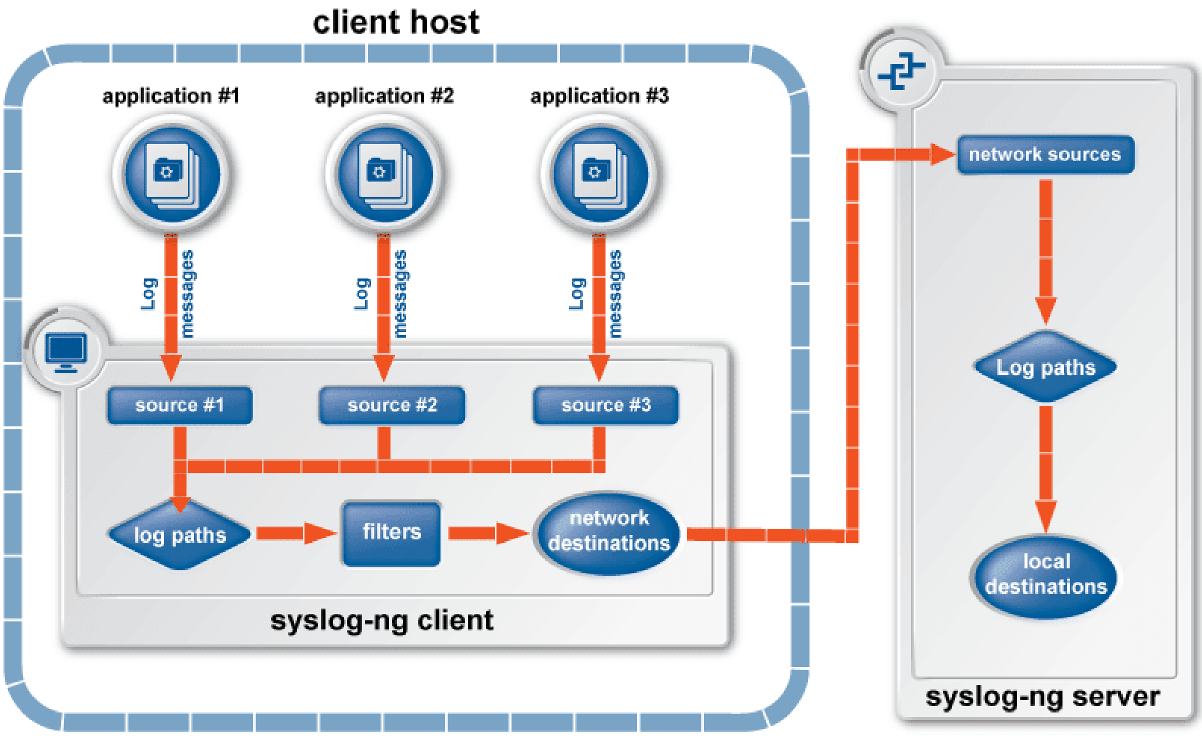

Figure 3: The route of a log message

Steps:

1. A device or application sends a log message to a source on the syslog-ng client. For example, an Apache web server running on Linux enters a message into the /var/log/apache file.
2. The syslog-ng client running on the web server reads the message from its /var/log/apache source.
3. The syslog-ng client processes the first log statement that includes the /var/log/apache source.
4. The syslog-ng client performs optional operations on the message, for example, it rewrites parts of the message or compares the message to the filters of the log statement (if any). If the message complies with all filter rules, syslog-ng sends the message to the destinations set in the log statement, for example, to the remote syslog-ng server.
5. After that, the syslog-ng client processes the next log statement that includes the /var/log/apache source, repeating Steps 3-4.
6. The message sent by the syslog-ng client arrives to a source set on the syslog-ng Store Box.
7. The syslog-ng Store Box reads the message from its source and processes the first log path that includes that source.

8. The syslog-ng Store Box processes the message and performs the following operations. Note that most of these operations are optional, but the order of the processing steps is fixed.
    a. Parse the message as a syslog message (unless message parsing is explicitly disabled for the source).
    b. Classify the message using a pattern database.
    c. Modify the message using rewrite rules (before filtering).
    d. Filter the messages, for example, based on sender hostname or message content. If the message does not match the configured filter, SSB will not send it to the destination.
    e. Parse the text of the message (that is, the ${MESSAGE} part) using a key-value parser.
    f. Modify the message using rewrite rules (after filtering and other parsing).
    g. SSB sends the message to the destinations set in the log path. The destinations are local, optionally encrypted files on SSB, or remote servers, receiving TLS-encrypted messages using the IETF-syslog protocol.
9. SSB processes the next log statement, repeating Steps 6-8.

The syslog-ng Store Box appliance receives logs through the network from Log Source Hosts and forwards them to the central SSB server, a relay, or another network destination.

The syslog-ng Store Box appliance can act as a central log-collecting server that receives messages through a network connection, and stores them locally, or forwards them to other destinations or external systems (for example, a SIEM). The SSB appliance requires a license file. This license file determines the number of Log Source Hosts (LSHs) that can send log messages to the SSB server.

Note that the number of source hosts is important, not the number of hosts that directly sends messages to SSB: every host that send messages to the server (directly or using a relay) counts as a Log Source Host.

Evaluation platform

The test platform is the following:

- Operating system: BalabitOS (Ubuntu based) version 6.0
- Required packages:

angularjs	1.6.7-1
gnupg	1.4.20-1ubuntu3.1
iptables	1.6.0-2ubuntu3

jquery	3.2.1-2
openjdk-8	8u151-b12-0ubuntu0.16.04.2
openssl	1.0.2g-1ubuntu4.10, 1.0.2m-1.syslogng60.1
php7.0	7.0.25-0ubuntu0.16.04.1bb1

- Two test agents will be used: Windows and Linux

Operating environment

The configuration and the operational mode of the ToE for the evaluation are:

- SSB is receiving and optionally sending logs through an encrypted TLS channel
- Use of encrypted logstores (logs are stored encrypted in SSB)
- SSB is configured to send an alert if the free space on the disks of SSB is low

The following features are not used in the ToE:

- **Remote administration via SSH or IPMI**
- **High Availability**
- **SQL source and destination**
- **RLTP source**
- **Backup, share and archive**
- **SQL query capabilities** of the user interface
- **Remote user databases**

Security Parameters

Users

The users that may interact with the ToE are the following:

- **Administrator**: user that has all privileges (modify settings, group management, local users, access control of groups).
- **Restricted administrator**: user with limited privileges in the remote administration interfaces depending on their group (define what they can view and configure).
- **Client source**: user on the syslog-ng client that can send logs to SSB.

Assumptions

The following assumptions are considered:

- **Proper administrator**: The administrator is not careless, wilfully negligent or hostile, and manages the ToE and its technical environment according to its documentation, within compliance of the applied enterprise security policy.
- **External PKI**: The management of cryptographic keys are secure; they are not compromised before uploading them to or after downloading them from the ToE.
- **Proper configuration**: The entire configuration of the referenced [SSB_RECO] security checklist is applied on SSB.
- **Protected environment**: The ToE relies upon a protected IT environment consisting of a trustworthy computing platform and a protected network environment for its execution. This underlying platform and network environment are out of scope of this ST, and the computing platform is protected from physical access. The external services used by SSB (e.g. DNS, NTP, etc.) are available and provide accurate information.
- **Residual data**: The platform elements containing sensitive data (e.g. hard disks) are properly cleared from data or destroyed after use.
- **Deactivated services**: Services of the ToE which are not covered by the evaluation are disabled in the operational configuration (see section Operating environment)

Critical Assets

Critical assets of the environment

The critical assets of the environment are the following:

- **Logspaces**: Contains logstore and index files. Log messages are sent from a source and stored in the ToE in binary logstore files and indexed in binary index files. Logstore files must be protected in confidentiality, integrity and availability. Index files must be protected in availability. The administrator can define who can access which logspaces, and what logs are encrypted by which keys.
- **Log communication**: Communications with the ToE must be protected in confidentiality, integrity and authenticity (collecting and sending logs). When receiving logs from a source, input must be validated and protected in integrity.
- **Web communication**: Communications with the ToE must be protected in confidentiality and integrity (using web interface).

Asset	Availability	Confidentiality	Integrity	Authenticity
Logstore	X	X	X	
Index files	X		X	
Log communication		X	X	X
Web communication		X	X	

ToE critical assets

The critical assets of the ToE are the following:

- **Configuration**: The configuration of the ToE must be protected in confidentiality, integrity and availability. The attacker must not be able to discover the configuration of the ToE by any other means than using the ToE.
- **User credentials**: Credentials that are used for authentication must be protected in confidentiality and integrity.
- **Cryptographic keys**: Keys used for securely store logs and securely communicate with source and destinations must be protected in confidentiality and integrity.
- **User access policy**: Users profiles and associated permissions are stored in the ToE. This information must be protected in integrity.

Asset	Availability	Confidentiality	Integrity	Authenticity
Configuration	X	X	X	
User credentials		X	X	
Cryptographic keys		X	X	
User access policy			X	

Threat Model

Attackers

The following attackers are considered:

- **Remote attacker**: An attacker intercepting log messages in traffic, reading and/or modifying them.
- **Local attacker**: An attacker having access to administration interface but having no valid credentials for the ToE.

Threats

The following threats are considered:

- **Flow compromise**: The attacker manages to fetch data by intercepting exchanges between the ToE and a source, a destination, or a user and the administrative web interface.
- **Flow alteration**: The attacker manages to corrupt exchanges between the ToE and a source, a destination, or a user and the administrative web interface.
- **Denial of service**: During a DoS attack, it is not possible to login to SSB.
- **Log loss**: Loss of log, for example due to:
  - Stop or inadequate speed of log gathering functionality;
  - Removal of the log.
- **Log tampering**: The log is tampered with.
- **Log compromise**: The attacker manages to illegally read logs.
- **Dangerous data**: A source is sending dangerous data on SSB.
- **Configuration alteration**: The attacker manages to modify, temporarily or permanently, the ToE configuration. Writing configuration settings exceeding the account privileges is also considered under this threat.
- **Configuration compromise**: The attacker manages to illegally obtain some parts of the ToE configuration. Reading configuration settings exceeding the account privileges is also considered under this threat.
- **Credentials theft**: The attacker manages to steal user credentials from the product.
- **Authentication violation**: The attacker successfully bypasses authentication on the administration interface.
- **Access control violation**: The attacker manages to obtain permissions which he does not have normally.

Security Functions

Security functions list

The following security functions are deduced from the above assets, assumptions and threats; therefore the ToE ensures the following:

1. **Secure log storage**: Confidentiality and integrity of stored logs.
2. **Secure communications**: Secure (confidentiality and integrity) communication both between a client and server, and between a user/administrator and the server (web interface).
3. **Secret storage**: Confidentiality of the stored cryptographic secrets (keys) and credentials.
4. **Secure management**: The ToE includes administration/management functions in order to configure the syslog-ng Store Box server (web interface).
5. **Access control policy**: SSB offers an access control policy based on user profiles and associated rights. The policy allows authorization of specific tasks (i.e. add/delete users, define log filtering policy, modify configuration, …).
   The implementation of such policy permits the definition of various profiles with detailed specific access rights.
6. **Log input validation**: SSB properly validates the logs arriving on the log interfaces.
7. **Authentication of actors**: TLS communication (for log communication) use mutual authentication. Authentication on the web interface is performed with credentials (login-password).

Rationale

Security functions and Assumptions vs Threats

	Flow compromise	Flow alteration	Denial of service	Log loss	Log tampering	Log compromise	Dangerous data	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation
Security functions												
Secure log storage				X	X	X						
Secure communication	X	X			X	X				X		
Secrets storage	X	X			X	X			X	X		
Secure management			X	X		X		X	X			
Access control policy					X	X		X	X	X	X	X
Log input validation							X					
Authentication of actors											X	X
Assumptions												
Proper administrator			X	X		X		X	X			
External PKI	X	X			X	X		X	X			
Protected environment			X	X							X	
Residual data						X			X	X		
Deactivated services			X									

Threats vs Assets

	Flow compromise	Flow alteration	Denial of service	Log loss	Log tampering	Log compromise	Dangerous data	Configuration alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation
Assets												
Logspaces			X	X	X	X						
Log communication	X	X			X	X	X					
Web communication	X	X								X		
Configuration								X	X			
User credentials										X		
Cryptographic keys	X	X			X	X		X	X	X		
User access policy						X			X		X	X