Certification Report

Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9

Sponsor and developer:	***Hillstone Network Corp.*** **5201 Great America Parkway, # 420,** **Santa Clara, CA 95054** **USA**
Evaluation facility:	***Secura B.V.*** **Karspeldreef 8** **1101 CJ Amsterdam** **The Netherlands**
Report number:	**NSCIB-CC-0476172-CR**
Report version:	**1**
Project number:	**0476172**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**27 September 2022**
Number of pages:	**11**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

TÜVRheinland®
Precisely Right.

CONTENTS

TÜVRheinland®
Precisely Right.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

TÜVRheinland®
Precisely Right.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9. The developer of the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9 is Hillstone Network Corp. located in Santa Clara, CA, USA. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a network security device that protects a network by controlling the traffic that comes in and out of that network, allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, the TOE can also work as a bridging device to connect a trust zone (internal network) and untrust zone (external network).

The TOE has been evaluated by Secura B.V. located in Amsterdam, The Netherlands. The evaluation was completed on 15 September 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9 from Hillstone Network Corp. located in Santa Clara, CA, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	StoneOS, build FR25098-YS-V6-r0614	5.5R9
Hardware	SG-6000-A200 SG-6000-A200W SG-6000-A1000 SG-6000-A1100 SG-6000-A2000 SG-6000-A2600 SG-6000-A2700 SG-6000-A2800 SG-6000-A3000 SG-6000-A3600 SG-6000-A3700 SG-6000-A3800 SG-6000-A5100 SG-6000-A5200 SG-6000-A5500 SG-6000-A5600 SG-6000-A5800 SG-6000-A6800 SG-6000-A7600	

In the certified configuration, the TOE supports transparent mode, routing mode and mix mode deployment running on A-Series appliances. The A-Series appliances, which is the underlying TOE hardware, is comprised of a set of different hardware models with variations in throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage as identified in the *[ST]*, chapter 1.4.

To ensure secure usage a set of guidance documents is provided, together with the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

All the hardware models share the same OS, the StoneOS 5.5R9.

The Hillstone Next Generation Firewall TOE is comprised of several security features, all implemented by StoneOS:

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channels

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The software is comprised of the operating system StoneOS with software version 5.5R9.

The StoneOS system architecture is constituted by:

- Zones, dividing network into multiple segments.
- Interface, the inlet and outlet for traffic going through security zones.
- Policy, which is used to control the traffic flow in security zones/segments.

Each instantiation of the physical TOE has two or more network interfaces and can filter IP traffic to and through those interfaces.

The TOE can optionally connect to an NTP server for clock updates, where NTP can be configured with authentication. If the StoneOS is to be remotely administered, the management station can connect using SSH or HTTPS. A syslog server can also be used to store audit records to a syslog server for UNIX or Windows, and the syslog server must support syslog over SSL/TLS. The TOE can filter connections to/from these external servers, including authentication servers, using its IP traffic filtering and can encrypt traffic where necessary using SSL/TLS and/or IPsec.

The three supported deployment scenarios for the TOE are:

1. **Transparent mode.** This is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. In this deployment mode the TOE will be used as a security device.
2. **Routing mode.** This deployment often uses the NAT function, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. The TOE in routing mode can work as a router and a security device.
3. **Mix Mode.** To configure a mix mode, it is necessary to combine the routing mode of the deployment methods with the transparent mode.

Visual depictions of these deployment scenarios are provided in *[ST]* sections 1.4.1.1 to 1.4.1.3.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Stone OS CLI User guide, dated 20 October 2021	Version 5.5R9
StoneOS Web UI User Guide, dated 20 October 2021	Version 5.5R9
Hillstone SG-6000 A-Series Hardware Reference Guide, dated 30 November 2021	Version 1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed testing on functional specification and subsystem level. The evaluator confirmed that the behaviour of all TSFI and all TSF subsystems have been demonstrated through the developer testing.

The majority of the developer testing was manual. The evaluator sampled a subset of the developer test suite, and also performed additional functional tests to further demonstrate the behaviour of the critical security functionality of the TOE.

2.6.2 Independent penetration testing

During the evaluation activities a vulnerability analysis was performed to ascertain the presence of potential vulnerabilities. Penetration testing was performed to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing was performed assuming an attack potential of Enhanced Basic.

The methodical analysis performed was conducted along the following steps:

- A public vulnerability analysis was performed that focused on:
  - Known vulnerability reports for the product and product type
  - Hardware components embedded into the device
  - Specific libraries and tools embedded into the underlying kernel.
- An independent vulnerability analysis which started with the identification of the main threat factor for the TOE was performed. Based on the environmental assumptions in the ST, the threat factor is defined as malicious known users and admin, as well as unknown users, already part of the network and organization where the TOE is deployed.
- Based on this threat factor definition, the analysis and resulted independent AVA tests are focused on deriving attacks aimed to bypass or modify the security features of the product, as defined in the ST.

The total test effort expended by the evaluators was 37 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

SG-6000-A2600 with StoneOS 5.5R9 in Routing mode was used for most of the testing. For a few test cases, the SG-6000-A1000 and SG-6000-A3800 devices were used.

The StoneOS 5.5R9 is installed in the same version on all the products in various families of the A-Series appliances with variations in throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage only. Therefore, the evaluator concluded that the testing conducted on a subset of the hardware devices is applicable across the hardware variations.

Similarly, the evaluator assessed that from a testing perspective there was no difference whether the TOE is deployed in transparent mode, routing mode or mix mode as the network plane configuration is the configuration in the environment and has no effect on the operation of the TOE itself. Thus, the test results achieved using Routing mode are considered equally applicable to Transparent mode or Mix mode.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9 build FR25098-YS-V6-r0614 running on the A-Series appliances identified in the Hardware section of the table in chapter 2.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

3 Security Target

The Common Criteria Security Target for Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9, Version 1.1, dated 09 September 2022 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NAT	Network Address Translation
NGFW	Next Generation Firewall
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SSH	Secure Shell
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report Hillstone NGFW with Stone OS 5.5R9, Version 1.2, 07 September 2022.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Common Criteria Security Target for Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9, Version 1.1, dated 09 September 2022

(This is the end of this report.)