National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Forcepoint LLC

10900-A Stonelake Blvd.

Austin, TX USA 78759

Forcepoint™ Stonesoft Next Generation Firewall Version 5.10

Report Number: CCEVS-VR-10669-2016
Dated: March 3, 2016
Version: 0.3

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Tony Chew
Rob Heald
Meredith Hennan
Jerome Myers
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Ed Morris
Catherine Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of ForcepointTM Stonesoft Next Generation Firewall solution provided by Forcepoint LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in February 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is the ForcepointTM Stonesoft Next Generation Firewall Version 5.10. The Stonesoft Next Generation Firewall (NGFW) is a stateful packet filtering firewall. Being a stateful packet filtering firewall, the NGFW filters network traffic optimized through the use of stateful packet inspection. The NGFW is intended to be used as a network perimeter security gateway that provides a controlled connection. The NGFW is centrally managed and generates audit records for security critical events.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Stonesoft Next Generation Firewall (NDPP11e3/STFFEP10) Security Target, Version 0.7, February 29, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	ForcepointTM Stonesoft Next Generation Firewall Version 5.10 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 and Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (including the optional TLS requirements)
ST:	Stonesoft Next Generation Firewall (NDPP11e3/STFFEP10) Security Target, Version 0.7, February 29, 2016
Evaluation Technical Report	Evaluation Technical Report for ForcepointTM Stonesoft Next Generation Firewall Version 5.10, Version 0.3, March 1, 2016.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forcepoint LLC
Developer	Forcepoint LLC

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Tony Chew, Rob Heald, Meredith Hennan, and Jerome Myers of The Aerospace Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Stonesoft Next Generation Firewall (NGFW) is a stateful packet filtering firewall. The Stonesoft Next Generation Firewall (NGFW) system is composed of two physical appliances: the NGFW engine and the Security Management Center (SMC) Appliance. The NGFW engine controls connectivity and information flow between internal and external connected networks. The SMC Appliance provides administrative functionality supporting the configuration and operation of one or more NGFW engines. Throughout the remainder of this document, references to the NGFW engine are meant to reference the firewall engine as a TOE component, while references to the NGFW are meant to refer to the TOE as a whole.

The NGFW engine controls connectivity and information flow between internal and external connected networks. Being a stateful packet filtering firewall, the NGFW filters network traffic optimized through the use of stateful packet inspection. The NGFW engine also provides a means to keep the internal host's IP-address private from external users. The NGFW engine is intended to be used as a network perimeter security gateway that provides a controlled connection. The NGFW is centrally managed and generates audit records for security critical events.

The NGFW is assumed to be installed and operated within a physically protected environment, administered by trusted and trained administrators over a trusted and separate management network. Multiple installations of the NGFW engine may be used in combination to provide a company with an overall network topology.

The NGFW engine runs on a hardened Linux operating system that is shipped with the product. The software (which is also part of the NGFW engine product) runs on a single or multi-processor Forcepoint platform.

The SMC appliance – a management system comprising a Management Server, Log Server and McAfee Linux Operating System (MLOS) to support the management and operation of the firewall – is included as part of the product. The MLOS that is used for the management server is the same underlying OS that is used in several other evaluated security products and has undergone prior evaluation as part of those products.

The Target of Evaluation (TOE) is Stonesoft Next Generation Firewall (NGFW) version 5.10.

3.1 TOE Evaluated Configuration

Forcepoint™ Stonesoft Next Generation Firewall is composed of the NGFW Engine (version 5.10.1) and Security Management Center (SMC) Appliance (version 5.10.0 with SMC Appliance patch 5.10.0P001). The NGFW Engine is evaluated on the following models:

Firewall Appliances:

Rack Mounted Firewall models

- 1035
- 1065
- 1401
- 1402
- 3202 (2U)
- 3207 (2U)
- 3206 (2U)
- 3301 (2U)
- 5206 (3U)

Desktop Firewall models

- 320X-C1
- 321-C2
- 325-C2

3.2 TOE Architecture

The Stonesoft Next Generation Firewall (NGFW) system is composed of two physical appliances: the NGFW engine and the Security Management Center (SMC) Appliance. The NGFW engine is an appliance composed of firewall functionality, an Engine OpenSSL Library and a Linux operating system. The SMC Appliance is composed of two custom built Java applications called the Management Server and the Log Server, running on the McAfee Linux Operating System (MLOS) with support from OpenSSL and a Java runtime environment.

The NGFW engine (a.k.a., the engine) is responsible for performing all firewall packet handling, analysis and filtering that is provided by the NGFW system.

The Management server on the SMC appliance provides the majority of the administrative capabilities in the NGFW system. A very limited console interface is provided on the SMC appliance by the MLOS and used to verify and update TOE software.

Given that this Security Target conforms to the NDPP and STFFEP, the security claims focus on the TOE as a secure network infrastructure device with stateful traffic filtering firewall capabilities and do not focus on other key functions provided by the TOE, such as virtual private networking. However, those functions can be freely used without affecting

the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE is composed of two physical components: the NGFW engine appliance and the SMC appliance. Each of these appliances have physical network connections to its environment to facilitate communication between TOE components as well as to position the TOE to monitor and filter network traffic. All management of the TOE occurs through the SMC appliance, while all firewall packet filtering occurs through the NGFW engine.

The TOE is accessed and managed from a PC in the environment which is expected to have a communication pathway to the SMC appliance.

The TOE can be configured to forward its audit records to an external syslog server in the environment. All audit records sent to the external syslog server, are sent from the SMC appliance. The NGFW engine does not send audit data directly to an external syslog server. Instead, the NGFW engine passes all of its audit data to the Logging server on the SMC appliance, which forwards the data to the external syslog server.

The TOE can be configured to synchronize it internal clock using an NTP server in the operational environment. The SMC appliance synchronizes with the external NTP server, then configures the NGFW engine's time to be in synch with itself. The NGFW engine does not synchronize to the external NTP server itself.

The NGFW engine utilizes the **Error! Reference source not found.** to support the NGFW engine's use of TLS to protect Internal-TOE-transfers. The SMC appliance uses RSA's Crypto-J Library to provide TLS, which protects Internal-TOE-transfers, the trusted channel mechanism and the trusted path mechanism.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Stateful Traffic Filtering Firewall
5. Identification and authentication
6. Security Management
7. Protection of the TSF
8. TOE access

9. Trusted path/channels

4.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message MSG contents into an encapsulating syslog record.

4.2 Cryptographic support

Because the TOE is distributed into two physically distinct parts, each physical component of the TOE must be considered when discussing the TOE cryptographic support. Both components of the TOE utilize cryptography to support its use of the TLS protocol to protect network communication and to support verification of TOE updates.

4.3 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner and performing firewall packet filtering operations. The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user.

4.5 Security management

Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. Administrators access the TOE remotely using a TLS protected communication channel between the Management server and the Client GUI (which runs on a workstation in the IT environment).

4.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE and a hardware clock to ensure reliable timestamps. The TOE protects sensitive data such

as stored passwords and cryptographic keys so that they are not accessible through the TOE, even to an authorized administrator. The TOE also utilizes the TLS protocol to protect communication between distributed parts of the TOE.

4.7 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using TLS for GUI access, ensuring both integrity and disclosure protection. If the negotiation of an encrypted session fails the attempted connection will not be established.

The TOE protects communication with network peers, such as an external syslog server, using TLS connections to prevent unintended disclosure or modification of logs.

The TOE also protects internal communication between components of the TOE using TLS connections which prevent unintended disclosure and modification of TSF communications.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3) with the following two extended packages:
- Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (STFFEP10)

That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PP and EP and performed by the evaluation team.
- This evaluation covers only the specific device models and software version identified in this document.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDPP11e3/STFFEP10. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Intel Security Product Guide, McAfee Next Generation Firewall 5. 10, Revision A
- Intel Security Installation Guide, McAfee Next Generation Firewall 5.10, Revision B
- Intel Security Common Criteria Evaluated Configuration Guide, McAfee Next Generation Firewall 5.10.1, Revision F
- McAfee Security Management Center Appliance Hardware Guide, Revision B
- Hardware Guide, Revision D, McAfee Next Generation Firewall, Models 321, 325, 1035, 1065, 1401, 1402
- Hardware Guide, Revision D, McAfee Next Generation Firewall, Models 3201, 3202, 3205, 3206, 3207, 3301
- Hardware Guide, Revision B, McAfee Next Generation Firewall, Models 5201, 5205, 5206
- Hardware Guide, Revision B, McAfee Next Generation Firewall, Model 320X

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (NDPP11e3/STFFEP10) for Stonesoft Next Generation Firewall, Version 0.6, February 29, 2016, and summarized in the Assurance Activity Report (NDPP11e3/STFFEP10) for Stonesoft Next Generation Firewall, Version 0.5, March 1, 2016 (AAR), which is publically available.

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDPP and STFFEP including the tests associated with optional requirements.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Stonesoft Next Generation Firewall Version 5.10 TOE to be Part 2 extended, and to meet the SARs contained in the NDPP and STFFEP.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Stonesoft Next Generation Firewall Version 5.10 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP and STFFEP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and STFFEP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

During the evaluation, the vendor provided a minimal patch to the SMC component of the TOE. This patch was tested for efficacy and is not deemed to affect the TOE security functionality, however, regression testing of the TOE as a whole was not performed.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Stonesoft Next Generation Firewall (NDPP11e3/STFFEP10) Security Target, Version 0.7,* February 29, 2016.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3)

[5] Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (STFFEP10)

[6] Stonesoft Next Generation Firewall (NDPP11e3/STFFEP10) Security Target, Version 0.7, February 29, 2016 (ST)

[7] Assurance Activity Report (NDPP11e3/STFFEP10) for Stonesoft Next Generation Firewall, Version 0.5, March 1, 2016 (AAR)

[8] Detailed Test Report (NDPP11e3/STFFEP10) for Stonesoft Next Generation Firewall, Version 0.6, February 29, 2016 (DTR)