National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0

Report Number: CCEVS-VR-PP-0012
Dated: 1 August 2014
Version: 1.0

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

<u>Common Criteria Testing Laboratory</u>

Extended Requirements
COACT, Inc., Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 1
3 TFFWEP Description 2
4 Security Problem Description and Objectives 3
  4.1 Assumptions 3
  4.2 Threats 3
  4.3 Organizational Security Policies 3
  4.4 Security Objectives for the TOE 4
5 Requirements 4
6 Assurance Requirements 5
7 Results of the evaluation 5
8 Glossary 5
9 Bibliography 6

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, also referred to as the Traffic Filter Firewall EP (TFFWEP). It presents a summary of the TFFWEP and the evaluation results. In order to promote thoroughness and efficiency, the evaluation of the TFFWEP was performed concurrent with the first product evaluation against the PP's requirements. This evaluation addressed the firewall requirements that were extended beyond those contained in the NDPP.

The information in this report is largely derived from the Evaluation Technical Reports (ETR), written by the CCTL listed above.

The evaluation determined that the TFFWEP is both **Common Criteria Part 2 Extended and Part 3 Conformant**. The Extended Package (EP) 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 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). Because the ST contains material drawn directly from the TFFWEP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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 found that the evaluation showed that the TFFWEP meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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 Profiles containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the TFFWEP was performed concurrent with the first product evaluation against the EP. In this case the TOE for this first product was the Sourcefire 3D System 5.2.0.1 provided by Sourcefire Inc. The evaluation was performed by the COACT, Inc., Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2014.

The TFFWEP contains a set of requirements that all conformant STs must include, in addition to the base and additional requirement derived from the NDPP.

The following identifies the EP subject to the evaluation/validation.

Protection Profile Extended Package	*Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2014*
ST	Sourcefire 3D System Security Target, Version 1.0, June 12, 2014
Evaluation Technical Report	Evaluation Technical Report For Sourcefire 3D System Evaluation Technical Report, June 05, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL	COACT, Columbia, MD
Validation Body	CCEVS

3 TFFWEP Description

The TFFWEP describes security requirements for a Stateful Traffic Filter Firewall (defined to be a device that filters layers 3 and 4 (IP and TCP/UDP) network traffic optimized through the use of stateful packet inspection) and is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. The EP is not complete in itself, but rather extends the Security Requirements for Network Devices protection profile (NDPP).

Compliant TOEs will provide security functionality that addresses network devices that perform network layer 3 and 4 stateful traffic filtering. A Stateful Traffic Filter Firewall is a device composed of hardware and software that is 4 connected to two or more distinct networks and has an infrastructure role in the overall enterprise network. Compliant TOEs will also provide all the security functionality described in the NDPP.

Since this EP builds on the NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP along with the additional functionality defined in the TFFWEP in response to the threat environment discussed therein. Briefly, compliant TOEs will control the flow of information (i.e., packets) between attached networks based on configured rules based on network layer 3 and 4 traffic attributes (i.e., addresses and ports) and derived session state information potentially up to network layer 7.

In addition to the protections provided by the NDPP, compliant TOEs must protect a range of security threats related to infiltration into a protected network and exfiltration from a protected network. The term protected network is used to represent an attached network for which rules are defined to control access. As such, a given Stateful Traffic Filter Firewall could potentially have a variety of attached protected and unprotected networks simultaneously depending on its specific configuration. Also, it should be clear that all attached networks are presumed to be protectable at the discretion of an authorized administrator. Applicable threats include unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance.

4 Security Problem Description and Objectives

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These conditions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE. These conditions are in addition to those contained in the NDPP.

4.1 Assumptions

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to Stateful Traffic Filter Firewalls. However, all the organizational security policies in the NDPP apply to Stateful Traffic Filter Firewalls.

4.4 Security Objectives for the TOE

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination transport layer ports.
O.STATEFUL_INSPECTION	The TOE will determine if a network packet belongs to an allowed established connection before applying the ruleset.
O.RELATED_CONNECTION_FILTERING	For specific protocols, the TOE will dynamically permit a network packet flow in response to a connection permitted by the ruleset.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

5 Requirements

As indicated above, requirements in the TFFWEP are a set that extends those contained in the NDPP. The requirements in the TFFWEP consist of a single extended family containing one component and multiple elements.

Requirement Class	Requirement Component	Requirement Element
FFW: Firewall Traffic Filtering	FFW_RUL_EXT.1: Stateful Traffic Filtering Rules	FFW_RUL_EXT.1.1: Stateful Filtering
		FFW_RUL_EXT.1.2: Protocols
		FFW_RUL_EXT.1.3: Protocol Fields
		FFW_RUL_EXT.1.4: Filtering Operations
		FFW_RUL_EXT.1.5: Interface Filtering Rules
		FFW_RUL_EXT.1.6: Session Filtering Rules
		FFW_RUL_EXT.1.7: Additional Protocols

Requirement Class	Requirement Component	Requirement Element
		FFW_RUL_EXT.1.8: Traffic Filtering Rules
		FFW_RUL_EXT.1.9: Additional Traffic Filtering Rules
		FFW_RUL_EXT.1.10: Default Denial Rule

6 Assurance Requirements

The assurance requirements are identical to those contained in the NDPP.

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units and the listing of the ASE work units in the ETR constituted meeting each corresponding APE work unit.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.2	Pass

8 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 as interpreted by the supplemental guidance

in the NDPP Assurance Activities to determine whether or not the claims made are justified.

- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Hewlett-Packard Company A-Series Switches Part 2 (Proprietary)*, Version 2.0. April 8, 2013.

[7] Science Applications International Corporation. *Hewlett-Packard Company A-Series Switches Security Target*, Version 1.0, April 5, 2013

[8] COACT, Inc. *Haivision Makito Video Encoders Evaluation Technical Report*, May 31, 2013, Document No. F1-0613-001 (Proprietary)

[9] *Haivision Makito 2.1 Security Target*, Document Number: HVS-PD-ST-MAK211, Version 1.1, May 29, 2013

[10] *Evaluation Technical Report for Lumeta IPsonar Part 2 (Prop)*, Version 1.0, 9 October 2013 (with ECR update 19 December 2013)

[11] *Lumeta IPsonar Security Target*, Version 1.0, 7 October 2013

[12] *Security Requirements for Network Devices*, Version 1.1, 08 June 2012