National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

WatchGuard Fireware OS 12.6.2 on Firebox NGFWs

Report Number: CCEVS-VR-VID11051-2020
Dated: 10/01/2020
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

Validation Team

Patrick Mallett, PhD, Lead Validator
Randy Heimann, Validator
The MITRE Corporation

Kenneth Stutterheim, Senior Validator
Jerome Myers, PhD, Senior Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Austin Kimbrell
Tammy Compton
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 the WatchGuard Fireware OS version 12.6.2 on Firebox NGFWs solution provided by Watchguard. 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 October 2020. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, as summarized in the publicly available Assurance Activity Report, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020.

The Target of Evaluation (TOE) is the WatchGuard Fireware OS 12.6.2 on Firebox NGFWs.

The 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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 and provided guidance on technical issues. 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 WatchGuard Fireware OS v12.6.2 on Firebox NGFWs (NDcPP21/STFFW13/VPNGWM10) Security Target, version 0.4, October 01, 2020 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 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 Base Protection Profile to which the product is conformant.
- The PP-Configuration 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	WatchGuard Fireware OS 12.6.2 on Firebox NGFWs (Specific models identified in Section 3.1)
Protection Profile Configuration	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020
ST	WatchGuard Fireware OS v12.6.2 on Firebox NGFWs (NDcPP21/STFFW13/VPNGWM10) Security Target, version 0.4, October 01, 2020
Evaluation Technical Report	Evaluation Technical Report for WatchGuard Fireware OS 12.6.2 on Firebox NGFWs, version 0.3, October 01, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5, April 2017
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Watchguard
Developer	Watchguard
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Patrick Mallett, Randy Heimann MITRE Corporation

Item	Identifier
	Jerome Myers, Kenneth Stutterheim, Aerospace Corporation

3 Architectural Information

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

The TOE is a suite of hardware devices that provide all-in-one network and content security solutions. These devices (known as Firebox Security Appliances) are equipped with a WatchGuard proprietary operating system (OS) called Fireware v12.6.2. Most platform variants of the TOE run different images, however some families of the TOE run on the same image. Further information on the variations of the TOE included in this evaluation can be found in Section 7 (of the ST).

Firebox appliances (running the Fireware OS) separate the organization's internal networks from external network connections to decrease the risk of an external attack. It protects the internal, private networks from unauthorized users on the Internet. Traffic that enters and leaves the protected networks is examined by the Firebox appliances. They use access policies to identify and filter different types of information and can also control which policies or ports the protected computers can use on the Internet (outbound access).

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

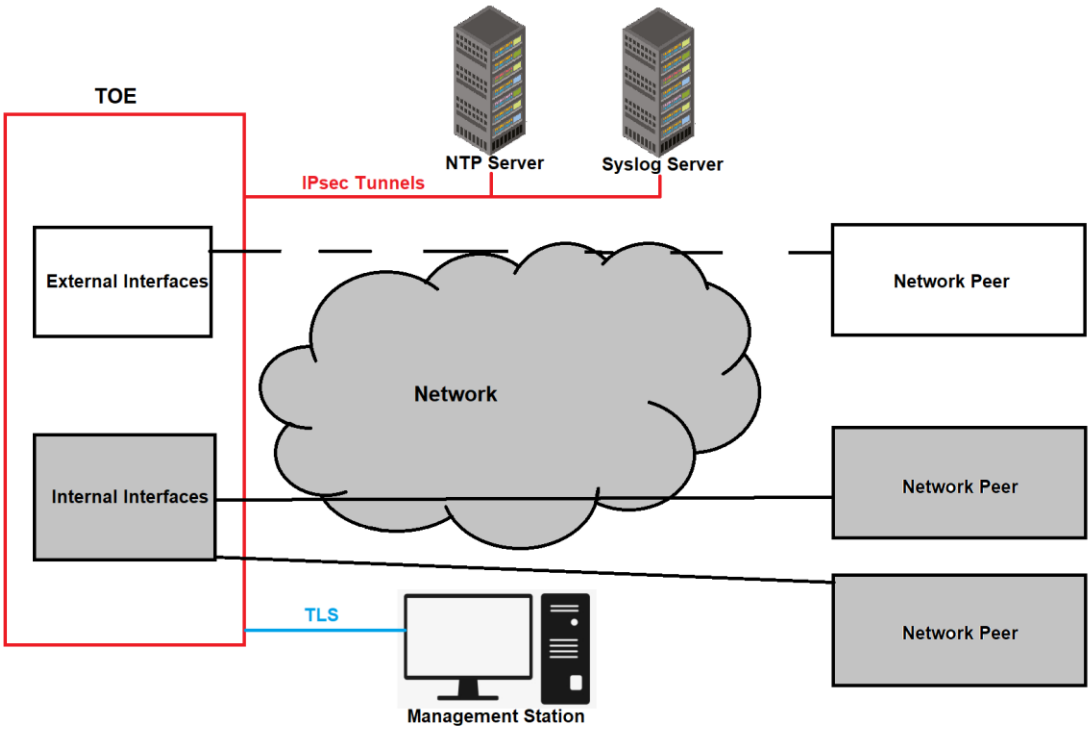
Software Version	Hardware Models	Included Expansion Modules
FirewareOS 12.6.2	T35 T40 T20 T80 T55 T70 M270 M370 M470 M570 M670 M4600 M5600	WG8592 (8x1G) WG8593 (8x1G) WG8594 (4x10G) WG8023 (2x40G)

The TOE requires the following Operational Environment support which is not included in the TOE's physical boundary.

- **Administrator Workstations:** Trusted administrators access the TOE through the TLS/HTTPS protocol.
- **Syslog Server(s):** The TOE relies upon the syslog server for storage of audit records. The TOE itself stores limited amount of the audit records in its internal persistence storage. Those audit records are accessible and exportable through the Web GUI interface.
- **NTP Servers:** The TOE relies upon up to 3 NTP servers to provide reliable time**.** If the time is configured locally, the TOE will use its own reliable hardware clock to maintain time as well.

3.2 TOE Architecture

The figure below illustrates the typical deployment use case and operational environment for TOE devices.



All devices operate in the same operational environment. IPsec tunnels are used to secure the communication between the device and external servers such as NTP server, Audit log server and LDAP server. All devices offer the same HTTPS/TLS based GUI interface for device configuration and management.

3.3 Physical Boundaries

The TOE is a software and hardware TOE. It is a combination of a particular model Firebox appliance and the Fireware v12.6.2 OS software based on Linux Kernel 4.14.83. The table in Section 7 (of the ST) lists all the instances of the TOE that operate in the CC-

evaluated configuration mode along with their CPUs and Ethernet Controllers. All listed TOE instances offer the same core functionalities.

4 Security Policy

This section summarizes the security functions provided by Firebox NGFWs:

- Security audit
- Cryptographic support
- User data protection
- Stateful Traffic Filtering Firewall
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

4.1 Security Audit

The TOE generates audit logs and has the capability to store them internally and can configure the TOE to send them to an external audit server. The connection between the TOE and the remote audit server is protected with IPsec. The TOE has a disk cleanup procedure where it removes old audit logs to allow space for new ones. When disk space falls below a predefined threshold, the TOE deletes the oldest set of records so it can continue collecting audit records.

4.2 Cryptographic Support

The TOE depends on CAVP certified cryptographic algorithms as a part of the WatchGuard Crypto module. Additionally, certain platforms rely on CAVP certified cryptographic algorithms used for hardware acceleration. The TOE protects the confidentiality and integrity of all information as it passes between the TOE and the remote management workstation (via TLS) and also when it passes between the TOE and the local management workstation (via a private, direct serial connection). The TOE achieves this by using validated cryptographic algorithms to perform encryption and the decryption of data according to the TLS protocol. Additionally, all communications with external IT entities are similarly protected using the IPsec protocol.

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 Stateful Traffic Filtering Firewall

The TOE supports many protocols for packet filtering including icmpv4, icmpv6, ipv4, ipv6, tcp and udp. The firewall rules implement the SPD rules (permit, deny, bypass). Each rule can be configured to log status of packets pertaining to the rule. All codes under each protocol are implemented. The TOE supports FTP for stateful filtering.

Routed packets are forwarded to a TOE interface with the interface's MAC address as the layer-2 destination address. The TOE routes the packets using the presumed destination address in the IP header, in accordance with route tables maintained by the TOE.

IP packets are processed by the WatchGuard's FirewareOS software, which associates them with application-level connections, using the IP packet header fields: source and destination IP address and port, as well as IP protocol. Fragmented packets are reassembled before they are processed.

The TOE mediates the information flows according to an administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

The TOE's firewall and VPN capabilities are controlled by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, and whether to log the connection.

4.5 Identification and Authentication

The TOE authenticates all administrative users. The TOE requires that users associated with these accounts be identified and authenticated before permitted access to the TOE and TOE security functions. Users may authenticate using either local password authentication or remote password authentication.

4.6 Security Management

The TOE provides local management capabilities via a local serial connection and remote management capabilities via Web-Based GUI (TLS/HTTPS). Management functions allow the administrators to configure users, roles, and security policy attributes.

4.7 Packet Filtering

Please see Stateful Traffic Filtering Firewall for a description of the TOE's packet filtering mechanism.

4.8 Protection of the TSF

The TOE includes capabilities to protect itself from unwanted modification as well as protecting its persistent data.

The TOE does not store passwords in plaintext; they are obfuscated. The TOE does not support any command line capability to view any cryptographic keys generated or used by the TOE.

The TOE provides a timestamp for use with audit records, timing elements of cryptographic functions, and inactivity timeouts. The operating system clock inside the TOE can be used to provide time information, or the TOE can be configured to rely on up to three NTP servers for its time.

The TOE only allows updates after their signature is successfully verified. The TOE update mechanism uses ECDSA with SHA-512 and P-521 to verify the signature of the update package.

The TOE's FIPS executables are signed using ECDSA with SHA-512 and P-521. For all other executables a hash is computed during system installation and configuration and during updates.

During power-up the integrity of all executables is verified. If an integrity test fails in the cryptographic module, the system displays an error message and pause boot, requiring a power cycle to restart the device. Also, during power-up, algorithms are tested in the kernel and user-space. If any of these test fail, the TOE is not operational for users.

The TOE protects all communications outside of the TOE with an approved connection method. Administrative configuration is protected by HTTPS/TLS while NTP and Audit Server communications are protected by IPsec.

4.9 TOE Access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.10 Trusted Path/Channels

The TOE protects all communications outside of the physical boundary of the TOE. The TOE utilizes HTTPS/TLS for administrative configuration, while using IPsec to protect communications with Audit and NTP servers.

5 Assumptions

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

- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020
- The PP-Configuration includes the following components:

- Base-PP: Collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 (STFFW13)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019 (VPNGWM10)

That information has not been reproduced here and the NDcPP21/STFFW13/VPNGW10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21/STFFW13/VPNGW10 and supporting technical documentation as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 collaborative Protection Profile for Network Devices and the Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 2.1, dated 11 March 2019 and the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020, the Supporting Document Mandatory Technical Document Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.3, September 2019 and the Supporting Document Mandatory Technical Document PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, September 17, 2020 as performed by the evaluation team). All NIAP Technical Decisions related to the protection profile security functional requirements were considered and applied as necessary.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, 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 NDcPP21/STFFW13/VPNGW10 and applicable

Technical Decisions. 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:

- Firebox Common Criteria Deployment Guide Fireware v12.6.2, Version 1.0, 10 August 2020

Please note that any other documentation delivered with the product or that may be accessible on-line that is not listed above was not included in the scope of the evaluation nor was it used to set the product into its evaluated configuration, and therefore should not be relied upon to place the device into the compliant configuration.

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 proprietary Detailed Test Report (NDcPP21/STFFW13/VPNGW10) for WatchGuard Fireware OS v12.6.2 on Firebox NGFWs, Version 0.3, October 01, 2020 (DTR).

8.1 Developer Testing

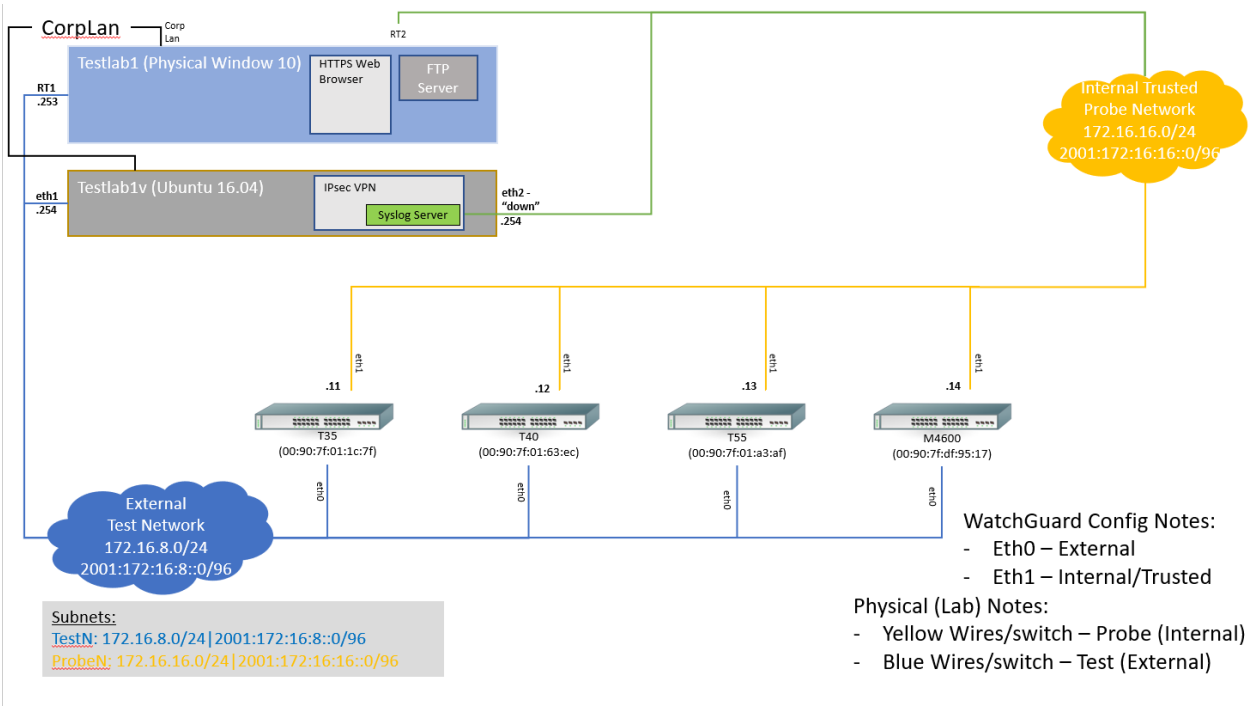
No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

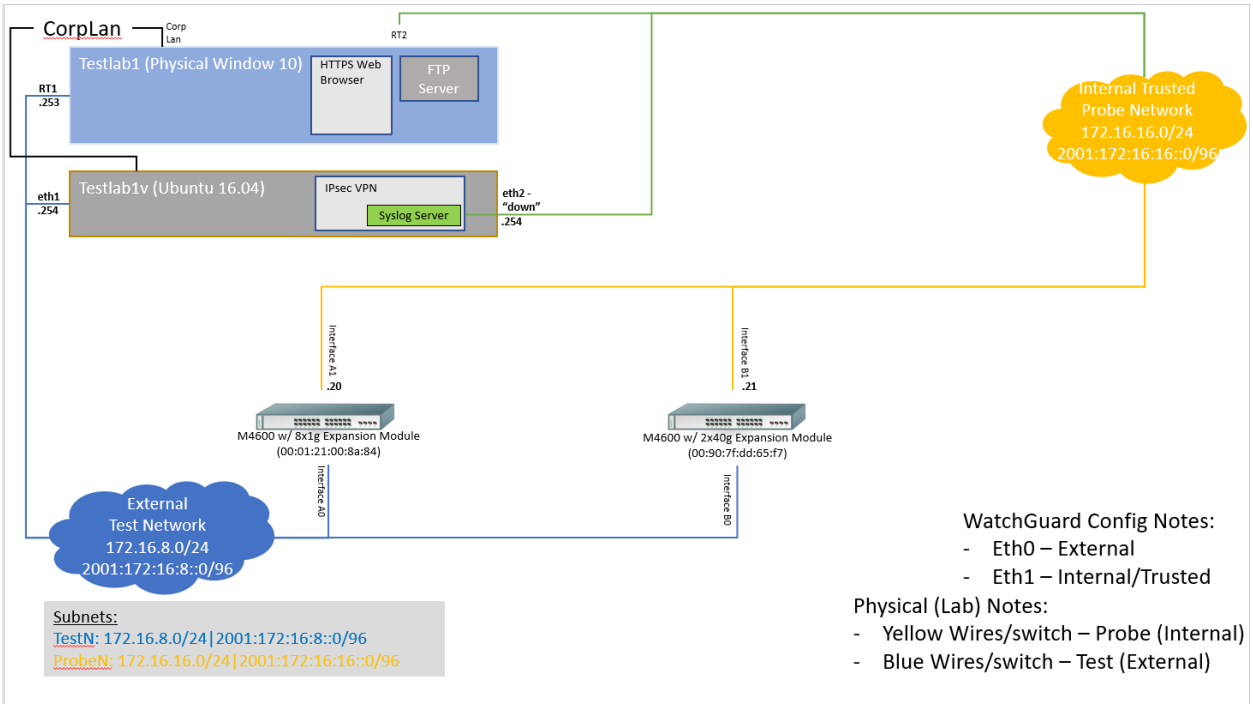
The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP21/STFFW13/VPNGW10 including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in AAR Section 3.4.

Test Environment

Default Devices



Devices w/ Expansion Module



9 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured with the documentation specified in Section 7.

- Fireware v12.6.2 OS
- Firebox Firewall Appliance: T35, T40, T20, T80, T55, T70, M270, M370, M470, M570, M670, M4600, and M5600
- Expansion Modules: WG8592 (8x1G), WG8593 (8x1G), WG8594 (4x10G), and WG8023 (2x40G).

10 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 5 and CEM version 3.1 rev 5. The evaluation determined the CyberFence 3e-636 Series Network Security Devices TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21/STFFW13/VPNGW10.

10.1 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 WatchGuard Fireware OS 12.6.2 on Firebox NGFWs that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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.

10.2 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 NDcPP21/STFFW13/VPNGW10 related to the examination of the information contained in the TSS.

The validators 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.

10.3 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 validators 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.

10.4 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 validators 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.

10.5 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 NDcPP21/STFFW13/VPNGW10 and recorded the results in a Test Report; summarized in the AAR.

The validators 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database

(http://www.kb.cert.org/vuls/) on 09/28/2020 with the following search terms: "T35", "T20", "T40", "T55", "T70", "T80", "m270", "m370", "m470", "m570", "m670", "m4600", "m5600", "Linux Kernel 4.14", "Firebox", "Fireware OS 12.6.2", "OpenSSL", "Jitterentropy", "Watchguard", "TCP", "Firewall", "IPsec", "TLS", "UDP", "IPv4 ", "IPv6". Based on the results, no vulnerabilities existed in the TOE at the time of the evaluation that were exploitable.

The validators 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.

10.7 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.

11 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Firebox Common Criteria Deployment Guide Fireware v12.6.2, Version 1.0, 10 August 2020 document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *WatchGuard Fireware OS v12.6.2 on Firebox NGFWs (NDcPP21/STFFW13/VPNGWM10) Security Target, Version 0.4, October 01, 2020.*

14 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.

15 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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019

[5] Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 2.1, 11 March 2019

[6] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4, 27 September 2019

[7] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019

[8] PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020

[9] WatchGuard Fireware OS v12.6.2 on Firebox NGFWs (NDcPP21/STFFW13/VPNGWM10) Security Target, version 0.4, October 01, 2020 (ST)

[10] Assurance Activity Report (NDcPP21/STFFW13/VPNGW10) for WatchGuard Fireware OS v12.6.2 on Firebox NGFWs, version 0.3, October 01, 2020 (AAR)

[11] Detailed Test Report (NDcPP21/STFFW13/VPNGW10) for WatchGuard Fireware OS v12.6.2 on Firebox NGFWs, version 0.3, October 01, 2020 (DTR) <Evaluation Sensitive>

[12] Evaluation Technical Report for (NDcPP21/STFFW13/VPNGW10) for WatchGuard Fireware OS v12.6.2 on Firebox NGFWs, version 0.3, October 01, 2020 (ETR)

[13] Firebox Common Criteria Deployment Guide, Version 1.0, 10 August 2020 (AGD)