National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10

Report Number:	**CCEVS-VR-10642-2016**
Dated:	**January 13, 2016**
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

Luke Florer
Kelly Hood
Kenneth Stutterheim

Common Criteria Testing Laboratory

Kevin Micciche

CGI IT Security Labs

Table of Contents

List of Tables

1 Executive Summary

This report documents the NIAP assessment of the evaluation of FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10 (hereafter referenced as the TOE). The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in the Network Devices Protection Profile (NDPP) v1.1 (June 8, 2013) with Errata #3 (3 November 2014) as well as the NDPP Extended Package Stateful Traffic Filter Firewall v1.0 (December 19, 2011).

It was determined that the TOE is conformant to the claimed Protection Profiles (PPs) and satisfies all of the security functional requirements stated in the ST when in the evaluated configuration. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated proprietary test report produced by the evaluation team and provided to the validation team.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the evaluators work substantiated that the product satisfies all of the security functional and assurance requirements stated in the 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 provided in the proprietary evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10
Sponsor & Developer	Fortinet, Inc. 326 Moodie Drive Ottawa, ON K2H 8G3, Canada
CCTL	CGI IT Security Labs 9700 Capitol Court Manassas, VA 20110
Completion Date	January 2016
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Network Devices Protection Profile (NDPP) v1.1, June 8, 2013, including the following optional requirements [TLS and TLS/HTTPS].* *The NDPP Extended Package Stateful Traffic Filter Firewall v1.0, December 19, 2011.* *The NDPP Errata #3, 3 November 2014*

Item	Identifier
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.
Evaluation Personnel	Kevin Micciche
Validation Personnel	Luke Florer Kelly Hood Kenneth Stutterheim

2 TOE Identification

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10 Security Target
ST Version	0.5
Publication Date	January 11, 2016
Vendor and ST Author	Fortinet, Inc.
TOE Reference	FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10
TOE Hardware Models	FortiGate-30D, FortiWiFi-30D, FortiWiFi-30D-PoE, FortiGate-60D, FortiGate-60D-PoE, FortiWiFi-60D, FortiGate-90D, FG-90D-PoE, FortiGate-100D, FortiGate-140D, FortiGate-140D-PoE, FortiGate-200D, FortiGate-240D, FortiGate-300D, FortiGate-500D, FortiGate-600C , FortiGate-800C , FortiGate-1000C, FortiGate-1000D, FortiGate-1200D, FortiGate-1240B, FortiGate-1500D, FortiGate-280D-PoE, FortiGate-3040B, FortiGate-3140B, FortiGate-3240C, FortiGate-3600C, FortiGate-3700D, FortiGate-3950B, FortiGate-3951B, FortiGate-5020 (2 Blade Slots), FortiGate-5060 (6 Blade Slots), FortiGate-5140B (14 Blade Slots), FortiGate-5001B, FortiGate-5001C, FortiGate-5001D, FortiGate-5101C, FortiSwitch-5203B
TOE Software Version	FortiOS™ 5.0 Patch Release 10
Keywords	Network Device, Firewall, FortiGate, UTM Appliance, FortiWifi

3 Architectural Information

The TOE is the referenced network appliances running version 5.0 Patch Release 10 of the FortiOS code in stand-alone mode. The TOE is designed to provide next-generation firewall services ensuring network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks. The TOE is capable of robust filtering based on information contained in IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP headers as specified by their respective RFC's. Additionally the TOE is capable of content inspection of FTP and H.323 protocols to work with the dynamic nature of these protocols.

3.1 Evaluated Configuration

The evaluated version of the TOE is FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10, as installed and configured according to the Installation Guide as well as the supporting guidance documentation identified in Section 6.

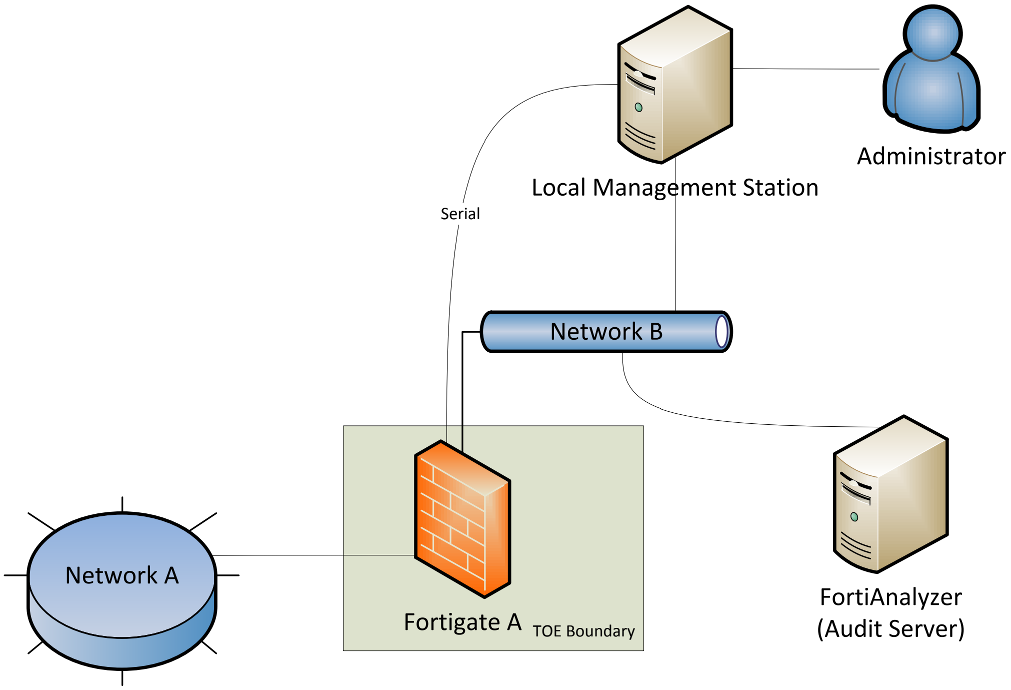

Figure 1 depicts an example of TOE deployment.

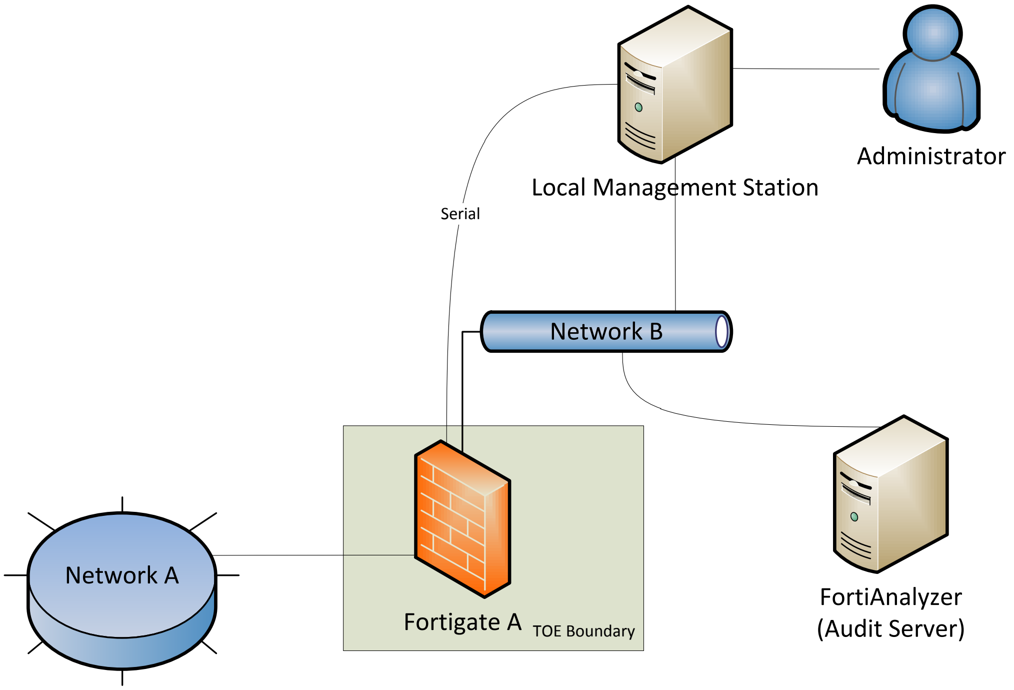

Figure 1: TOE Deployment Example

3.2 TOE Hardware

The TOE is a hardware and software solution that consists of the FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10.

Table 3: TOE Hardware Devices

Model	CPU	ASIC	RAM	Flash	Storage
FG-1000C	Intel i5 Quad Core	CP8	8GB	8GB	128GB
FG-1000D	Intel Xeon E Series	CP8	16GB	4GB	256GB
FG-100D	Intel Atom	CP8	2GB	16GB	32GB
FG-1200D	Intel Xeon E Series	CP8	16GB	16GB	240GB
FG-1240B	Intel i5-750	CP8	8GB	8GB	128GB
FG-140D	Intel Atom	CP8	4GB	16GB	32GB
FG-140D-PoE	Intel Atom	CP8	4GB	16GB	32GB
FG-1500D	Intel Xeon E Series	CP8	16GB	32GB	480GB
FG-200D	Intel G540 (Celeron)	CP8	4GB	16GB	64GB
FG-240D	Intel Celeron	CP8	4GB	4GB	64GB
FG-280D-PoE	Intel Celeron	CP8	4GB	4GB	64GB
FG-300D	Intel i3-3220	CP8	8GB	16GB	120GB
FG-3040B	Intel Xeon E Series	CP7	12GB	8GB	64GB

Model	CPU	ASIC	RAM	Flash	Storage
FG-30D	ARM v5 Compatible (SoC2)	CP7	1GB	4GB	N/A
FG-3140B	Intel Xeon E Series	CP7	12GB	8GB	64GB
FG-3240C	Intel Xeon E5 Series	CP8	12GB	8GB	64GB
FG-3600C	Intel Xeon E Series	CP8	32GB	2GB	64GB
FG-3700D	Intel Xeon E5 Series	CP8	32GB	32GB	128GB
FG-3950B	Intel Xeon E Series	CP7	12GB	8GB	N/A
FG-3951B	Intel Xeon E Series	CP7	12GB	8GB	N/A
FG-5001B	Intel Xeon LC Series	CP7	12GB	8GB	64GB
FG-5001C	Intel Xeon E5-2658L	CP8	32GB	32GB	128GB
FG-5001D	Intel Xeon E Series	CP8	32GB	16GB	200GB
FG-500D	Intel Xeon E Series	CP8	8GB	16GB	120GB
FG-5101C	Intel Xeon LC Series	CP8	12GB	8GB	64GB
FG-600C	Intel i3-540	CP8	4GB	8GB	64GB
FG-60D	ARM v5 Compatible (SoC2)	CP7	2GB	8GB	8GB
FG-60D-PoE	ARM v5 Compatible (SoC2)	CP7	2GB	8GB	8GB
FG-800C	Intel i5-750	CP8	8GB	8GB	64GB
FG-90D	ARM v5 Compatible (SoC2)	CP7	2GB	2GB	32GB
FG-90D-PoE	ARM v5 Compatible (SoC2)	CP7	2GB	8GB	32GB
FSW-5203B	Intel Xeon 3500 Series	CP8	12GB	8GB	64GB
FWF-30D	ARM v5 Compatible (SoC2)	CP7	1GB	4GB	N/A
FWF-30D-PoE	ARM v5 Compatible (SoC2)	CP7	1GB	4GB	N/A
FWF-60D	ARM v5 Compatible (SoC2)	CP7	2GB	8GB	8GB

3.3 Clarification of Scope

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

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance based upon the successful completion of the assurance activities specified in the claimed PPs and performed by the evaluation team.
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.

4. 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. High-Availability
    b. FortiExplorer client
    c. Anti-spam
    d. Content filtering
    e. Web filtering
    f. IPSEC and SSL VPN gateway functionality
    g. Antivirus
    h. NAT
    i. Intrusion detection/prevention
    j. SSH
    k. Use of syslog
    l. FortiToken and FortiSSO Authentication
    m. Stream Control Transmission Protocol (SCTP), BGP, RIP, NTP and DHCP protocols
    n. Usage of the boot-time configuration menu to upgrade the TOE

4 Security Policy

The TOE enforces the following security policies as described in the ST.

4.1 Security Audit

The TOE is capable of generating and securely transmitting Security Audit logs to a remote, trusted FortiAnalyzer server for further processing and review. The TOE will generate auditable events as specified in the NDPP which may help indicate a number of potential security concerns including resonance, password guessing and tampering with the trusted paths and channels. For all auditable events the TOE will associate a user (either IP address or with administrative credentials) to the session and use this identifier for all logging to the audit server. The TOE can generate audit logs for a variety of security events. These include basic events such as hits against firewall rules and will include information which is tracked by the TOE and exported for later analysis and review via a trusted channel. This information includes information such as source, destination, port and protocol as required by the Firewall EP.

4.2 Cryptographic Support

The TOE's cryptographic modules are FIPS PUB 140-2 validated and meet Security Level 1 overall. In addition, several devices have achieved Security Level 2. The certificates for those specific devices can be found in the Security Target. The TOE is capable of generating cryptographic keys using a NIST SP 800-90B compliant random bit generator seeded with a minimum of 256 bits of entropy by the dedicated hardware based noise source. These keys are created, managed and destroyed to provide cryptographic services to the network. The TOE is also capable of importing cryptographic keys and certificates from outside the TOE boundary. Cryptographic keys and CSPs are zeroized by the FIPS compliant modules when no longer required and the TOE offers a function to zeroize this data on demand.

4.3 User Data Protection

The TOE ensures that no information from previously processed information flows is transferred to subsequent information flows. This applies both to information that is input to the TOE from an external source and to information (e.g., padding bits) that might be added by the TOE during processing of the information from the external source. For instance, packets that are not the required length uses a series of repeating byte patterns to meet the packet length. This ensures that no data reuse occurs during packet processing. The removal of any previous residual information is done through the zeroization of data when the memory structure is initially created and strict bounds checking on the data prior to it being assigned in memory.

4.4 Identification and Authentication

All administration requires authentication by user identification and password mechanism. Administration may either be performed locally using the Local Console CLI or remotely using the Network Web-Based GUI. The TOE supports complex configurable password rules and supports complex character sets. Any individual attempting to log on for an interactive session will be shown a warning message that they must accept prior to being presented with a prompt to attempt their authentication.

4.5 Security Management

The TOE provides remote and local administrative interfaces that permit the administrator to configure and manage the TOE. In the evaluated configuration, the TOE is connected to two or more networks and remote administration request data flows from a Network Management Station to the TOE. On the TOE hardware model in each configuration there is also a Local Console, located within the physically secured area described within the NDPP which has a physical serial interface to the TOE. Administrator accounts are associated with an access profile, which determines the permissions of the individual administrator.

4.6 Protection of the TSF

Inter-TSF communications are protected to ensure availability, confidentiality and detection of modification. This is accomplished through the usage of cryptographic communications for any and all communications with remote IT entities, other components of the TOE and remote administrators. By default the detection of modification and audit logging is enabled on TLS connections. The TOE prevents the reading of all administrator passwords, pre-shared keys, symmetric keys and private keys through encryption with AES-128 prior to storing them into the TOE configuration file. Certificates cannot be viewed through any interface once loaded into the TOE. The TOE maintains its own timestamp which is free from outside interference. This timestamp is used for the purposes of generating audit logs and other time-sensitive operations on the TOE including cryptographic key regeneration intervals.

4.7 TOE Access

The TOE is capable of terminating both local and remote administrative sessions upon the detection of an administrator configurable period of inactivity being exceeded. The TOE is also capable of terminating a remote session upon request from a remote administrator. The TOE provides administrators with a configurable warning banner which appears prior to initiating any interactive session with the administrator.

4.8 Trusted Path/Channels

A cryptographically protected trusted communications channel is required for all communications with the FortiAnalyzer audit server. For the purposes of auditing the TOE is capable of securing its audit server communications via TLS. The use of this secure channel ensures that the TOE will protect from disclosure the credentials contained in the authentication request and raise an audit log entry should the TOE detect modification in transit. The TOE or the remote peer may initiate this cryptographically protected channel. The TOE will ensure that cryptographically protected sessions to the HTTPS GUI are used to establish a trusted path between the TOE and the trusted remote administrator. This path will be used for both the initial administrator authentication and all remote administration requests and can be terminated upon session timeout or an explicit request from the administrator.

4.9 Stateful Traffic Filtering

The TOE implements a stateful firewall which is compliant with the NDPP EP for stateful firewall inspection. Each packet that arrives on an interface is subject to the enforcement of the stateful traffic filtering. This filtering verifies if the connection is part of an established session or if it is a new connection. If the security attributes of the incoming connection request match those already present for an entry in the state table of the TOE the information flow is automatically allowed. Otherwise this is considered a new connection attempt.

The TOE can create firewall rules based on a number of security attributes located in the header information of traffic arriving on a specific interface. Rules can be created based on a number of traffic protocols including the RFC's for ICMPv4, ICMPv6, IPv4, IPv6, TCP and UDP. Attributes of these protocols such as IP address, transport protocol, type, code and port can be used to provide more granular access control policies. The TOE also supports advanced protocols including FTP and H.323 which have non-static ports during their negotiation. The TOE is capable of inspecting this traffic to understand what is expected during these information flows.

4.10 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server.

5 Documentation

The following documents were available with the TOE for evaluation:

- FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10, March 20, 2015
- FortiOS™ Handbook for FortiOS 5.0 01-5010-99686-20150219 February 19, 2015
- FortiGate™ Log Message Reference v5.0 Patch Release 10 01-510-112804-20150313 March 13, 2015
- FortiOS™ CLI Reference for FortiOS 5.0 01-509-99686-20150226 February 26, 2015
- FIPS 140-2 and Common Criteria Compliant Operation for FortiOS™ 5.0.10 01-510-267768-20150206 March 20, 2015
- FortiAnalyzer v5.0 Patch Release 9 Administration Guide 05-509-187572-20141020 October 20, 2014
- FortiGate Appliances with FortiOS 5.0 (NDPP Compliant) Product Architectural Description 0.3 February 6, 2015

The Security Target used is:

- FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10 Security Target, Version 0.5, January 11, 2016

6 Independent Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Independent Test Plan for Fortigate UTM appliances running FortiOS 5.0 Patch Release 10, Version 1.1, December 30, 2015

The evaluation lab generated the test results from the manual tests and confirmed the actual results matched those of the expected results. The testing activities were conducted as specified in the Protection Profile for NDPP, Version 1.1, with Errata #3 as well as the TFFWEP v1.0. Testing was completed at the CGI Facility in December of 2015.

7 Results of the Evaluation

The evaluation was conducted in accordance with the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 with Errata #3 and in the NDPP Extended Package Stateful Traffic Filter Firewall v1.0, December 19, 2011, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST. A team of validators, on behalf of the CCEVS Validation Body reviewed the submission of evidence by the evaluation lab and the evaluation completed in January 2016.

8 Validator Comments/Recommendations

Please note that all the devices require the use of the FortiGate proprietary hardware entropy noise source (FTR-ENT1 – entropy token) to seed the cryptographic system.

To place the device(s) into the evaluated configuration for FIPS140-2 and Common Criteria compliant operation, the administrators must follow the guidance set forth by the vendor in the *Fortinet FIPS 140-2 and Common Criteria Compliant Operation for FortiOS 5.0.10*, dated March 20, 2015. As well, attention should be paid to Section 3.3, Item 5 of this document which lists the specific product capabilities that are excluded from use in the evaluated configuration.

9 Annexes

Not applicable.

10 Security Target

FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10 Security Target, Version 0.5, January 11, 2016

11 Acronyms

Table 4: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCCS	Canadian Common Criteria Scheme
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameters
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
FSSO	Fortinet Single Sign-On
HMAC	Keyed-Hash Message Authentication Code
NDPP	Network Device Protection Profile
OFB	Output Feedback
OSP	Organizational Security Policy
PP	Protection Profile
RBG	Random Bit Generator
SA	Security Association
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

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

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

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, 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 2012.

[4] FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10 Security Target, Version 0.5, January 11, 2016

[5] Assurance Activities Report for FortiGate™ UTM appliances running FortiOS™ 5.0 Patch Release 10, Version 0.4, January 11, 2016