Swedish Certification Body for IT Security

Certification Report FortiGate

Issue: 1.0, 2016-sep-30

Authorisation: Jerry Johansson, , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a boundary protection device, consisting of a hardware box and a FortiOS firmware. Some models also contain an ASIC implementing cryptographic primitives, which is placed in the TOE environment. The firmware has the version "FortiOS 5.2.7 build number b718" for all versions, and the following hardware models are included in the certification: FG-60D, FGR-60D, FWF-60D, FG-92D, FWF-92D, FG-100D, FG-140D-PoE, FG-200D, FG-300D, FG-500D, FG-600D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-3200D, FG-3700D, FG-3815D and FG-5001D. In addition, the following virtual versions (software only, installable in 3rd party hypervisors) are included in the certification: FortiGate-VM00, FortiGate-VM01, FortiGate-VM02, FortiGate-VM04, FortiGate-VM08.

The TOE provides the following functionality: firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus, antispam, intrusion prevention, content filtering, remote administration and clustering for high availability to IPv4 and IPv6 networks.

Some models of the TOE contain a hardware chip, FortiASIC, which performs cryptography on the primitive level. In accordance with SP-188 Scheme Crypto Policy this cryptographic implementation is considered outside the scope of the evaluation, but the implementation of the cryptographic function calls to the chip, and the intended effect has been verified during the evaluation. Other cryptographic implementations are within the scope of TOE.

The ST does not claim conformance to any Protection Profiles (PPs).

The evaluation has been performed by Combitech AB in Sundbyberg, Sweden, partly with the assistance of Electronic Warfare Associates-Canade Ltd. in Ottawa, Canada. A site-visit was performed in the developers premises in Vancouver, Canada.

The evaluation was completed on the 22nd of September 2016. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 4, augmented by ALC_FLR.3 Systematic flaw remediation.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

Electronic Warfare Associates-Canada Ltd. Operates as a Foreign Location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 4 + ALC_FLR.3.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

For some TOE models, the correct invocation of certain cryptographic primitives has been included in the scope of this evaluation, while correctness of the implementation of cryptographic primitives has been excluded, and their implementation is considered outside the scope of TOE.
Correctness of the implementation of the cryptographic primitives is affirmed by the vendor of the cryptographic library. Users of this product are advised to consider their acceptance of this affirmation.

2 Identification

Certification Identification

Certification ID	CSEC2015004
Name and version of the certified IT product and the TOE	Fortinet FortiGate Next Generation Firewalls and FortiOS 5.2.7 CC Compliant Firmware. Firmware: "FortiOS 5.2.7 build number b718 Hardware: FG-60D, FGR-60D, FWF-60D, FG-92D, FWF-92D, FG-100D, FG-140D-PoE, FG-200D, FG-300D, FG-500D, FG-600D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-3200D, FG-3700D, FG-3815D and FG-5001D Virtual machines: FortiGate-VM00, FortiGate-VM01, FortiGate-VM02, FortiGate-VM04, FortiGate-VM08
Security Target	Fortinet FortiGate Next Generation Firewalls and FortiOS 5.2 CC Compliant Firmware Security Target, Fortinet Incorporated, 2016-09-20, document version 1.5
Assurance level	EAL 4 + ALC_FLR.3
Sponsor	Fortinet Incorporated
Developer	Fortinet Incorporated
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2016-10-03

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- Trusted Path/Channels
- IPS Functionality
- Anti-Virus Functionality

3.1 Security Audit

The TOE generates audit records for security relevant events. An administrator may view the contents of the audit records; however, this functionality is restricted to only those users authorized to view the records.

3.2 Cryptographic Support

The TOE provides key generation, key destruction and cryptographic operation functions supported by CAVP-validated algorithms.

3.3 User Data Protection

The TOE provides interfaces to a defined set of networks and mediates information flow among these networks. The TOE supports the information flow control policies required for authenticated and unauthenticated service. Additionally, the TOE supports a VPN information flow control policy and a Web filtering information flow control policy.

3.4 Identification and Authentication

All TOE administrative users must be identified and authenticated. Administration may either be performed locally using the Local Console CLI or remotely using the Network Web-based GUI. TOE users may be required to authenticate in order to access an internal or external network. The TOE blocks users after a configurable number of authentication failures, after which an administrator must intervene to allow access.

3.5 Security Management

The TOE provides administrative interfaces that permit users in administrative roles to configure and manage the TOE. In each of the two evaluated configurations (i.e., the Single-Unit Configuration and High-Availability Configuration), the TOE is connected to two or more networks and remote administration data flows from a Network Management workstation to the TOE. In each configuration there is also a Local Console, located within a Secure Area, with an interface to the TOE.

An administrator account is associated with an access profile which determines the permissions of the individual administrator. Additionally, each FortiGate unit comes with a default administrator account with all permissions, which may not be deleted.

3.6 Protection of the TOE Security Functionaity (TSF)

The TOE provides failover in support of the high availability features. Reliable time stamps are provided in support of the audit function.

3.7 Trusted Path/Channels

A trusted path communication is required for the authentication of administrators and users of TOE services that require authentication. A remote administrator's communication remains encrypted throughout the remote session.

The TOE requires an encrypted trusted channel for communication between FortiGate devices in support of the High Availability configuration.

3.8 IPS Functionality

The TOE provides IPS functionality to recognize and block potential Denial of Service attacks, and to recognize and block attacks based on known attack signatures.

3.9 Anti-Virus Functionality

The TOE supports anti-virus detection and the ability to block or quarantine suspected information. A secure mechanism is used to update virus signatures.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes one assumption on the usage of the TOE.

A.MANAGE - There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

4.2 Environmental Assumptions

Two assumptions on the environment are made in the Security Target.

A.LOCATE - The TOE hardware and software will be located within controlled access facilities and protected from unauthorized physical modification.

A.SINGEN - Information cannot flow among the internal and external networks unless it passes through the TOE.

4.3 Clarification of Scope

The Security Target [ST] contains ten threats, which have been considered during the evaluation.

T.ACCESS - An unauthorized person on an external network may attempt to bypass the information flow control policy to access protected resources on the internal network.

T.AUDACC - Persons may not be accountable for the actions that they conduct because the audit records are not created and reviewed, thus allowing an attacker to escape detection.

T.COMDIS - An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.

T.MEDIAT - An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

T.NOAUTH - An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.NOHALT - An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.

T.PRIVIL - An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.PROCOM - An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

T.REPLAY - A user may gain inappropriate access to the TOE by replaying authentication information.

T.VIRUS - A malicious agent may attempt to pass a virus through or to the TOE.

The Security Target [ST] also contains three organisational security policies:

P.ACCACT - Users of the TOE shall be accountable for their actions.

P.DETECT - All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected.

P.MANAGE - The TOE shall be manageable only by authorized administrators.

5 Architectural Information

The TOE is the boundary protection device FortiGate Next Generation Firewalls and FortiOS 5.2.7 CC Compliant Firmware (build number b0718). The TOE is a group of network appliances and a virtual machine version designed to provide firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering to provide network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks.

5.1 Hardware

The TOE appliances are delivered as both hardware and firmware, the virtual machine as one software part.

The hardware consists of several components, such as:

- Central Processing Units (CPUs)
- System Memory (RAM)
- Hard Disk
- Flash Memory
- Network Interfaces (NIs)
- Serial Port(s)
- USB port(s)
- FortiBIOS
- FortiASIC (not part of the TOE)

In the evaluated configuration, an external HW device, Fortinet Entropy Token, is used to seed the TOE with entropy at start-up and periodically at a configurable interval.

The virtual machine versions do not have any hardware parts.

5.2 Security Audit

The TOE creates audit records for administrative events, potential policy violations and information flow decisions. The TOE records the identity of the administrator or user who caused the event for which the audit record is created. The TOE applies timestamps to auditable events as they occur.

The administrator can review the audit records. The audit records are stored locally, using memory, a hard disk or FLASH memory depending on the model.

If the TOE is operating as part of an Active-Active HA cluster, the HA master logs all administrative events for the cluster. The status of each node in a clustered TOE is identified by a heartbeat. When the heartbeat response is not received from a slave node, the master node no longer routes packets to the failed node. In the event that the master fails, an existing node in the cluster will be promoted to become the master node. The HA master also logs all potential policy violations and information flow decisions that it processes. HA slaves log all potential policy violations and information flow decisions that they process. The administrator can access slave audit records through the master HA unit.

If the audit log of any node in a cluster becomes full, that node takes the action specified for the master node. If this action is to shut down the TOE interfaces the following will result:

a. If the audit log of a slave node becomes full (active-active cluster), the slave node drops out of the cluster;

b. If the audit log of a master node becomes full (active-active cluster), the master node has failed and one of the slave nodes will become the new master node; and

c. If the audit log of the master node (active-passive cluster) becomes full, the master node has failed and the backup node will take over as the master node.

Logs may be read using the CLI or the web interface on the FortiGate unit. This functionality is provided by default to the primary administrator account, and must be specifically granted to any administrator account that may be created.

5.3 Cryptographic Support

The cryptographic libraries used by the TOE are listed below:

Cryptographic Library	Version	Relevant FortiGate Models
Fortinet FortiASIC CP7	CP7	FG-60D, FGR-60D, and FWF-60D
Fortinet FortiASIC CP8	CP8	FG-100D, FG-140D-PoE, FG-200D, FG-300D, FG-500D, FG-600D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-3200D, FG-3700D, FG-3815D, and FG-5001D
Fortinet FortiOS SSL Cryptographic Library v5.2	Version 5.2.7	All evaluated FortiGate models including VMs
Fortinet FortiOS FIPS Cryptographic Library v5.2	Version 5.2.7	All evaluated FortiGate models including VMs
Fortinet FortiOS RBG Cryptographic Library	Version 5.2.7	All evaluated FortiGate models including VMs

The hardware modules CP7 and CP8 are used by certain TOE models to increase encryption speed. The implementation of these modules are considered outside the scope of TOE, and their correctness has been verified by Fortinet Incorporated.

Note that the calls to CP7 and CP8 has been verified by code review during the evaluation, and the effect of the cryptographic primitives implemented in CP7 and CP8 has been verified by testing during the evaluation.

Cryptographic support is provided using a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A. This generates cryptographic keys whose strengths are modified by available entropy. Cryptographic support is provided using a Fortinet entropy token to seed the DRBG during the boot process and to periodically reseed the DRBG. Operation of the token is based on a wide-band Gaussian white noise generator and provides a source of entropy. The default reseed period is once every 24 hours (1440 minutes). The token is connected to the Fortinet hardware device or virtual machine hardware using a standard USB interface, and must be installed to complete the boot process and to reseed of the DRBG. The entropy token is responsible for loading a minimum of 256 bits of entropy.

Each FortiGate unit is delivered with a factory installed 2048-bit RSA public/private key pair. Asymmetric keys are also generated in support of TLS functionality.

Cryptographic key destruction meets the key zeroization requirements of Key Management Security Level 1 from FIPS PUB 140-2. The TOE only stores keys in memory, either in Synchronous Dynamic Random Access Memory (SDRAM) or Flash Random Access Memory (RAM). Keys are destroyed by overwriting the key storage area with an alternating pattern at least once.

5.4 User Data Protection

The TOE operates in accordance with four information flow security functional policies:

a. The Unauthenticated Information Flow SFP allows unauthenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by an authorized administrator;

b. The Authenticated Information Flow SFP allows authenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by an authorized administrator;

c. The VPN SFP allows authenticated users to send and receive information protected using IPsec to and from the TOE; and

d. The Web Filtering SFP allows users to access only those URLs which are allowed.

The security functional policies are implemented as firewall rules. The rules that implement the Unauthenticated Information Flow, Authenticated Information Flow and VPN SFPs have restrictive default values and by default no information is allowed to flow, and TOE services are not available to unauthenticated users. The Web Filtering SFP has permissive default values, and does not block URLs until specifically identified. Regardless of firewall rules, packets which include parameters as specified by the security functional requirements which define the security functional policies are never permitted to pass through the TOE. Modification of the rules is restricted to an authorized administrator, and an authorized administrator may also specify alternative initial values to override the default values. The TOE allows an authorized administrator to view all information flows allowed by the information flow policy rules before the rules are applied.

The TOE mediates all information flows which pass through it. For information to pass through the TOE, it must match one of an authorized administrator specified firewall rules which permit the information flow.

The TOE ensures that all information flows provided to the TOE by external entities for transfer to other entities are subjected to the defined firewall rules and conform to them before they are allowed to proceed toward the destination entity.

The TSF immediately enforces revocation of a user's permission to use the information flow and also immediately enforces changes to the information flow policy rules when applied. The TOE also immediately enforces the disabling of a service which was available to an unauthenticated user.

The VPN functionality supports IPsec tunnel mode. An IPsec tunnel may be established between two FortiGate units, or between a client application and the FortiGate device. Authentication for IPsec services may be performed using Internet Key Exchange (IKE) pre-shared key or IKE RSA key. The IPsec VPN functionality is implemented through the Encapsulated Security Payload (ESP) protocol. When in FIPS-CC mode, TOE devices support IKEv1, as defined in RFCs 2407, 2408, 2409, RFC 4109, and RFC 4868 (for hash functions), and IKEv2 as defined in RFC 5996 (with mandatory support for NAT traversal as specified in section 2.23), RFC 4307, and RFC 4868 (for hash functions). IKEv1 Security Association (SA) lifetimes may be limited to 24 hours for Phase 1 SAs, and 8 hours for Phase 2 SAs. IKEv1 SA lifetimes may also be limited by traffic volume. This value is determined during the configuration of the Phase 2 parameters, and may be set to between 100 and 200 MB of traffic for the specified SA. Once the lifetime for the SA has been reached, the TOE device will renegotiate the SA. IKE protocols support the use of Diffie-Hellman (DH) Groups 1 (with 768-bit MODP5), 2 (with 1024-bit MODP), 5 (with 1536-bit MODP), and 14 (with 2048-bit MODP). The use of pre-shared keys is supported for authenticating IPsec peer connections. Pre-shared keys may be between 6 and 32 characters in length,

and may be composed of upper and lower case letters, numbers and special characters. Certificate based authentication may also be used.

The TOE follows a sequence of ordered steps in order to decide whether or not a requested information flow is allowed to proceed. The very first processing step performed by the FortiGate unit on incoming information is an inspection for IPS anomalies which target the TOE directly. Examples of IPS anomalies include syn floods, ping of death, source routing and port scans. If the incoming information flow is not blocked by the inspection for IPS anomalies, it is next processed against the firewall policy rules and authentication requirements. If the incoming information flow is allowed by the firewall policy rules (using the first match algorithm) and if any required authentication has been completed successfully, the incoming information flow may be subject to additional restrictions based on any Protection Profile which is associated with the firewall policy rule which allowed the information flow.

Protection Profiles are used to define additional information flow restrictions which may be based on any or all of the following types of information:

- Scheduling
- SMTP commands
- SMTP Multi-Purpose Internet Mail Extensions (MIME) types
- FTP subcommands
- HTTP request methods
- Virus signatures
- IPS signature matching

Only an authorized administrator may create, modify or delete a Protection Profile. Additionally, only an authorized administrator may associate a Protection Profile with a firewall policy rule.

If the request is an HTTP or HTTPS, the URL may be checked against the FortiGuard Web Filtering Policy. FortiGuard Web Filtering is made up of an external service which provides category, category group and classification information for any requested website, and an internal policy that applies that information. When FortiGuard Web Filter is enabled in a web filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the TOE provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

The specific steps used by the TOE to process incoming information flows and enforce its security policy are summarized below:

1. Local IPS Anomaly protection (kernel level);
2. Firewall flow control policy enforcement: First matched policy must explicitly allow traffic to flow;
3. Authenticated flow control policies: If configured for flow-control policy, successful authentication is required for traffic to flow; and
4. Protection Profile services (if explicitly enabled):
   a. Scheduling: If scheduling is enabled, time period must be explicitly allowed,
   b. SMTP Commands: All SMTP commands permitted unless explicitly denied,
   c. MIME Types: All MIME types permitted unless explicitly denied,
   d. FTP Sub-Commands: All FTP sub-commands permitted unless explicitly denied,
   e. HTTP Request Methods: All HTTP request methods permitted unless explicitly

denied,

f. FortiGuard Web Filter: All URL requests are checked against the web filter policy to determine if they are allowed or blocked.

g. Virus protection: If content is matched against an Anti-Virus (AV) signature, the configured action is performed, and

h. IPS Signature matching: If the nature of the connection or content is matched against an IPS signature, the configured action is performed.

It must be noted that traffic is only passed to the next enforcement method if previous enforcement methods explicitly allow the traffic.

After all security policy enforcement is performed and no further security scrutiny is required, the packet data is forwarded to the network host as determined by the configuration of the egress interface and/or static route. Additionally, an authorized administrator may set a maximum quota for the amount of data received by a subject (source or destination) in a specified period of time. If a maximum quota has been set by an authorized administrator, this quota will be enforced by the TOE.

5.5 Identification and Authentication

In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access and network user access to specific services. The TOE maintains identity, role/authorization and authentication data to support this functionality. Identification and authentication is always enforced on the serial interface (local console). On the network interfaces identification and authentication is enforced for all administrator access, specific services, and VPN users. For local administrators, the identification and authentication mechanism is a username and password combination; for remote administration and user access to Telnet and FTP protocols, a FortiToken one-time password generator is required for authentication. Proxy users and administrators are presented with a system screen (configurable by an authorized administrator) prior to authentication, and must access this screen and authenticate prior to access. VPN peers authenticate using preshared keys or certificates for IPsec VPNs and certificates for SSL VPNs. The accounts are created by an authorized administrator over the serial or network interfaces.

The account of an administrative user or IT entity is disabled after a configurable number of unsuccessful authentication attempts. An authorized administrator must take action to re-enable the account before authentication may take place.

5.6 Security Management

Appropriately authorized administrators may read audit log data, acknowledge alarms and manage users, IPS policies and information flow policies. The TOE immediately enforces the revocation of a user from an administrative access profile.

The TOE provides a web-based GUI and a CLI to manage all of the security functions. The TOE allows both local and remote administration. Local administration is performed using the Local Console. Remote administration is performed using the Network web-based GUI.

An administrator account consists of an administrator's identification and authentication information, and access profile. The access profile is a set of permissions that determine which functions the administrator is allowed to access. (The term 'role' is used in FMT_SMR.1; however, the TOE uses the term access profile in its administration.) For any function, a profile may allow either read only or read-write access. When an administrator has read-only access to a feature, the administrator can access the web-based manager page for that feature but cannot make changes to the configuration. Similar permissions are enforced for the CLI.

Each FortiGate unit (and the virtual model) comes with a default administrator account with all permissions, which may not be deleted. The term 'authorized administrator' is used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required.

5.7 Protection of the TSF

The HA feature provides failover protection capability which includes configuration synchronization. The FortiGate units that make up the HA cluster exchange configuration information using a proprietary protocol (FortiGate Clustering Protocol (FGCP)). Before any information is exchanged, members of a HA cluster authenticate using information built into the FortiGate unit at the time of manufacture. Configuration information is exchanged every time the configuration of the master node in a HA cluster is updated. In this way, the slave or passive nodes in a cluster are prepared to assume the role of master node should the master node fail.

Time is provided by the TSF and can only be changed by an authorized administrator. The TOE hardware devices include a hardware clock which is used to generate reliable time stamps which in turn are used for audit records and to provide scheduling features for flow control policies. The hardware clock does not rely upon any external factors in order to function correctly. The time setting of the hardware clock may only be modified by an authorized administrator and all such modifications are recorded in the audit log. For the virtual device, time information is provided to the TOE from the underlying hardware.

5.8 Trusted Path/Channel

The TOE provides trusted paths and trusted channels, protected by encryption to guard against disclosure and protected by cryptographic signature to detect modifications. The trusted paths and trusted channels are logically distinct from other communication paths and provide assured identification of their end points.

The trusted paths are used to protect remote administrator authentication, all remote administrator actions, Proxy User authentication, VPN user authentication, and all VPN user actions. Remote administration sessions apply to the Network Web-Based GUI.

The Network Web-Based GUI uses the HTTPS protocol for secure administrator communications. With respect to the TOE implementation of HTTPS, TLS version 1.1 (RFC4346) and TLS 1.2 (RFC 5246) are used to encrypt and authenticate administration sessions between the remote browser and TOE. The TOE supports the following ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA (RFC 4346)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC 5246)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (RFC 5246)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (RFC 4346, RFC 5246)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA2 56 (RFC 4346, RFC 5246)

Use of these ciphersuites requires that the keying material be determined when the session is established through a Diffie-Hellman (DH) exchange which consists of the following steps:

• The server sends the 2048-bit RSA public certificate56 (RFC 4346, RFC 5246)

• The server generates, signs (RSA PKCS#1) and sends DH parameters and the DH public value

• The client generates and sends the DH public value. The keying material is then used to encrypt/decrypt (using AES128 or AES256) and authenticate (using HMAC-SHA1 or HMAC-SHA256) the data exchange.

By default, HTTPS connections to the TOE are disabled and must be explicitly enabled before an administrator may use the Network Web-Based GUI. SHA1 is supported in order to maintain compatibility with older browser versions, and compliance with RFC 4346 and RFC 5246.

When a connection is first established, the server presents the 2048-bit RSA certificate to the connecting web browser. The administrator can examine the certificate to validate the identity of the TOE and then choose to continue with the connection if the certificate conforms to the expected values. Only after the certificate has been explicitly accepted as valid will the administrator be presented with the login page, where the user and password credentials can be submitted for authentication. Only local administrator account credentials can be used to successfully authenticate to the TOE via the Network Web-Based GUI.

The trusted channels provide communication between the TOE and other TOE devices in support of the HA cluster configuration, when implemented. This channel is logically distinct from other communication channels and provides assured identification of the end points and protection of the channel data from disclosure. HA heartbeat encryption and authentication is enabled to encrypt and authenticate HA heartbeat packets. This ensures that the cluster password and changes to the cluster configuration are not exposed allowing an attacker to sniff HA packets to get cluster information. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster. HA heartbeat encryption and authentication are disabled by default, and must be enabled in the evaluated configuration. HA authentication and encryption uses AES-128 for encryption and SHA-1 for authentication.

5.9 Intrusion Prevention

The TOE provides an Intrusion Prevention System that examines network traffic arriving on its interfaces for evidence of intrusion attempts.

Ingress packets received on a FortiGate interface are passed to the Denial of Service sensors, which determine if it is a valid information request or not. Detection of any potential attack is recorded in the IPS or packet logs. If the packet is allowed to pass based on the information flow policy (based on the Fortinet Protection Profile), it is examined against IPS signatures known to indicate potential attacks. If evidence of an attack is found, the TOE records the event in the IPS or packet logs. These logs are made available only to authorized administrators, and is provided in a manner suitable for the administrators to interpret the information.

5.10 Anti-Virus Actions

The TOE detects and prevents virus attacks contained within information flows which arrive at any of its network interfaces. An authorized administrator may configure the TOE to block and or quarantine a virus which is detected in an information flow. The TOE may also be configured to monitor the information flow and make a record of any virus found, but perform no other action. The TOE provides a secure mechanism for the update of virus signatures used by the TSF.

6 Documentation

The following documents are included in the scope of the TOE:

FortiGate/FortiWiFi 60D Series QuickStart, December 10, 2013
FortiGate Rugged 60D QuickStart Guide, June 3, 2014
FortiGate/FortiWiFi 92D Information Supplement, August 11, 2015
FortiGate-100D Information Supplement, August 20, 2015
FortiGate-140D/140D-POE/140D-POE-T1 Information Supplement, June 28, 2013
FortiGate-200D QuickStart Guide, April 01, 2014
FortiGate-300D QuickStart Guide, April 18, 2016
FortiGate-500D Information Supplement, June 27, 2014
FortiGate-600D Information Supplement, August 11, 2015,
FortiGate-900D Information Supplement, July 24, 2015
FortiGate-1000D QuickStart Guide, May 28, 2014
FortiGate-1200D QuickStart Guide, July 28, 2014
FortiGate-1500D Information Supplement, June 4, 2015
FortiGate-3200D Information Supplement, June 30, 2015
FortiGate-3700D QuickStart Guide, December 13, 2013
FortiGate-3815D Information Supplement, January 21, 2016
FortiGate-5001D Security System Guide, November 9, 2015

FortiOS Handbook VM Installation for FortiOS 5.2.0 March 4, 2015,

FortiOS Handbook 5.2.8, August 18, 2016 (covers 5.2.7)

Common Criteria Compliant Operation for FortiOS, 5.2.7, 2016-05-17,
document version 0.5

7 IT Product Testing

7.1 Developer Testing

The developer's testing covers all TSFIs and their security functional behaviour as well as the interaction between subsystems and the interfaces of the SFR-enforcing modules.

The developer tested all hardware models within the scope of the evaluation, and two configurations of the virtual models FortiGate-VM04, FortiGate-VM02. The virtual models listed in [ST], section 1.3.3, are considered equal, the same binary is used for all, they only differ in number of virtual cores and virtual memory allowed through a licensing procedure.

7.2 Evaluator Testing

The evaluator's independent testing focussed on the following hardware models:

- FortiWiFi-60D
- FortiGate-60D
- FortiGate-300D (two firewalls put in high availability clustering mode)
- FortiGate-1500D
- FortiGate-3700D

The evaluators repeated a sample of developer tests, and added independent test cases, which were applied to all the five TOE configurations listed above.

7.3 Evaluator Penetration Testing

Both internal and external interfaces were port scanned and vulnerability scanned, using Nmap, Nessus, and Core Impact.

It was also tested that the entropy token is required during boot and when reseeding.

The FortiGate backdoor (FortiDoor) attack was tested using a publicly published exploit.

The penetration tests did not reveal any vulnerability in the TOE.

8 Evaluated Configuration

The TOE shall be configured in accordance with "Common Criteria Compliant Operation for FortiOS™ 5.2.7", 2016-05-17, document version 0.5.

Both single and cluster configurations are covered by the evaluation.

The virtual models have been tested on VMware ESXi Server 5.5 during the evaluation but are installable on most hypervisors.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.4	PASS
Implementation Representation	ADV_IMP.1	PASS
TOE Design	ADV_TDS.3	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.4	PASS
CM Scope	ALC_CMS.4	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Tools and Techniques	ALC_TAT.1	PASS
Flaw Remediation	ALC_FLR.3	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

AES	Advanced Encryption Standard
AH	Authentication Header (IPsec)
CBC	Cipher Block Chaining
CIFS	Common Internet File System
CRV	Constrained Random Verification
CTS	Cipher Text Stealing
DNS	Domain Name System
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
FTP	File Transfer Protocol
HCD	Hardcopy Device
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IKE	Internet Key Exchange (IPsec)
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MFP	Multifunction printer
NTP	Network Time Protocol
OXP	Open Extensibility Platform
OXPd	OXP device layer
PIN	Personal Identification Number
PJL	Printer Job Language
PML	Printer Management Language
PRF	Pseudo-random Function
PSTN	Public Switched Telephone Network
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TOE	Target of Evaluation
USB	Universal Serial Bus
WINS	Windows Internet Name Service
XML	Extensible Markup Language

12 Bibliography

ST	Fortinet FortiGate Next Generation Firewalls and FortiOS 5.2 CC Compliant Firmware, Fortinet Incorporated, 2016-09-20, document version 1.5
Guide60	FortiGate/FortiWiFi 60D Series QuickStart, Fortinet Inc. 2013-10-10
Guide60r	FortiGate Rugged 60D QuickStart Guide, Fortinet Inc. 2014-06-03
Guide92	FortiGate/FortiWiFi 92D Information Supplement, Fortinet Inc. 2015-08-11
Guide100	FortiGate-100D Information Supplement, Fortinet Inc. 2015-08-20
Guide140	FortiGate-140D/140D-POE/140D-POE-T1 Information Supplement, Fortinet Inc. 2013-06-28
Guide200	FortiGate-200D QuickStart Guide Fortinet Inc. 2014-04-01
Guide300	FortiGate-300D QuickStart Guide Fortinet Inc. 2016-04-18
Guide500	FortiGate-500D Information Supplement Fortinet Inc. 2014-06-27
Guide600	FortiGate-600D Information Supplement Fortinet Inc. 2015-08-11
Guide900	FortiGate-900D Information Supplement Fortinet Inc. 2015-07-24
Guide1000	FortiGate-1000D QuickStart Guide Fortinet Inc. 2014-05-28
Guide1200	FortiGate-1200D QuickStart Guide Fortinet Inc. 2014-07-28
Guide1500	FortiGate-1500D Information Supplement Fortinet Inc. 2015-06-04
Guide3200	FortiGate-3200D Information Supplement Fortinet Inc. 2015-06-30
Guide3700	FortiGate-3700D QuickStart Guide Fortinet Inc. 2013-12-13
Guide3815	FortiGate-3815D Information Supplement Fortinet Inc. 2016-01-21
Guide5001	FortiGate-5001D Security System Guide Fortinet Inc.2015-11-09
VMguide	FortiOS Handbook VM Installation for FortiOS 5.2.0, Fortinet Incorporated, 2015-03-04, docuent version 01-520-203906-20150304
Handbook	FortiOS Handbook 5.2.8, Fortinet Incorporated, August 18, 2016
CCcfg	Common Criteria Compliant Operation for FortiOS 5.2.7, Fortinet Incorporated, 2016-05-17, document version 0.5
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 4, CCMB-2012-09-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-002
CCpart3	Common Criteria for Information Technology Security Evaluation,

Part 3, version 3.1 revision 4, CCMB-2012-09-003

CC — CCpart1 + CCpart2 + CCpart3

CEM — Common Methodology for Information Technology Security Evaluation, version 3.1 revision 4, CCMB-2012-09-004

SP-002 — SP-002 Evaluation and Certification, CSEC, 2016-04-28, document version 23.0

SP-188 — SP-188 Scheme Crypto Policy, CSEC, 2016-01-13, document version 5.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2015-05-05:

QMS 1.17.3 valid from 2015-01-29

QMS 1.18 valid from 2015-06-18

QMS 1.18.1 valid from 2015-08-21

QMS 1.19 valid from 2016-02-05

QMS 1.19.1 valid from 2016-03-07

QMS 1.19.2 valid from 2016-04-28

QMS 1.19.3 valid from 2016-06-02

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.17.3”, “Ändringslista CSEC QMS 1.18.1”, and “Ändringslista CSEC QMS 1.19.3”.

The certifier concluded that, from QMS 1.17.3 to the current QMS 1.19.3, there are no changes with impact on the result of the certification.