Fortinet FortiGate™

Next Generation Firewalls with FortiOS 6.2 Compliant Firmware

Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 2173-000-D102
Version: 1.10
12 October 2021

Fortinet, Incorporated
899 Kifer Road
Sunnyvale, California, USA
94086

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

Section 9, Annex A, identifies the TOE hardware models, guides, and entropy sources.

1.2 SECURITY TARGET REFERENCE

ST Title:	Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2 Compliant Firmware Security Target
ST Version:	1.10
ST Date:	12 October 2021

1.3 TOE REFERENCE

TOE Identification:	Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7 (Build # 5081)
TOE Developer:	Fortinet, Incorporated
TOE Type:	Boundary Protection Device

1.4 TOE OVERVIEW

The TOE is any one of a group of network appliances 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.

The FortiGate Family of Next Generation Firewalls span the full range of network environments, from the remote office and branch office (ROBO) to service provider, offering cost-effective systems for any size of application. They are hardware security systems designed to protect computer networks from abuse. They reside between the network they are protecting and an external network, such as the Internet, restricting the information flow between them permitted by policies (set of rules) defined by an authorized administrator. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, and intrusions in real-time, without degrading network performance. In addition to providing application-level protection, the FortiGate series uses dedicated, easily managed platforms to deliver a full range of network-level services including: VPN, VLAN, Network Address Translation (NAT), intrusion protection, web filtering, antivirus, antispam, and traffic shaping.

Each FortiGate unit consists of a hardware box and the FortiOS™ custom Next Generation Firewall (NGFW) firmware. FortiOS may also be deployed as a virtual machine running on VMware ESXi. Administration of the system may be performed locally using an administrator console, or remotely via a network management workstation. Each FortiGate NGFW can operate either standalone or as part of a cluster in order to provide high availability of services. The different models in the series provide for increased performance and additional protected ports.

With the exception of the entry level and virtual models, all CC-evaluated FortiGate NGFW employ Fortinet's unique FortiASIC™ processor and FortiOS™ operating system. The Application-Specific Integrated Circuit (ASIC) processors accelerate network security in Fortinet platforms. The purpose-built, high-performance network and content processors use intelligent and proprietary digital engines to accelerate compute-intensive security services. Combined with FortiOS, they provide a critical layer of real-time, network-based antivirus protection that

complements host-based antivirus software and supports "defence-in-depth" strategies without compromising performance or cost. They can be deployed to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, VLAN, and related devices, or to provide complete network protection.

The FortiGate series support the Internet Protocol Security (IPsec) industry standard for VPN, allowing VPNs to be configured between a FortiGate model and any gateway/firewall that supports IPsec VPN. The FortiGate series also provide Secure Sockets Layer (SSL) VPN services, allowing VPNs to be configured between a FortiGate unit and any VPN client supporting TLSv1.1 or TLSv1.2.

The TOE components identified in Table 18 are collectively termed the FortiGate™ Series or FortiGate™ Family of Next Generation Firewalls (NGFW). They are uniquely referenced by product name, firmware build number, and hardware version. The TOE consists of hardware and the FortiOS software; however, the Virtual Machine (VM) models identified in Table 19 consist only of the FortiOS.

1.4.1 TOE Features

The function of the FortiGate Series is to isolate two or more networks from each other and arbitrate the information transfers between these networks. Arbitration is based on a set of policies (rules) that are established by an authorized administrator and applied to each data packet that flows through the system. The TOE arbitrates all data that travels through it from one network to another.

The FortiGate has a FIPS-CC Mode of operation which, when enabled by an authorized administrator, provides the capability claimed in this ST. FIPS-CC Mode provides initial default values and enforces the FIPS-CC configuration requirements.

The following table summarizes the most security-relevant FortiGate features.

Feature	Description
Access Control	FortiGate Next Generation Firewalls provide a role-based access control capability to ensure that only authorized administrators are able to administer the FortiGate unit.
Administration (Local Console CLI)	The FortiGate provides management capabilities via the text-based Local Console Command Line Interface (CLI).
Administration (Network Web-Based GUI)	The FortiGate provides a Network Web-based Graphical User Interface (GUI), accessed via HyperText Transfer Protocol Secure (HTTPS), for system management and configuration.
Administration (SSH)	The FortiGate provides remote administration services over Secure Shell (SSH) for system management and configuration.
Anti-Virus	The FortiGate Series provides anti-virus protection for HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post-Office Protocol Version 3 (POP3), and Internet Message Access Protocol (IMAP) Web content as it passes through the FortiGate unit.
Authentication	The FortiGate implements a username and password mechanism for identification and authentication.

Feature	Description
Authentication (Firewall Policy Authentication)	The FortiGate Firewall Policy may be configured to require authentication by the user before the information flow is enabled for that user.
Cryptography	The FortiGate incorporates cryptographic operations for protecting communication channels.
Firewall (Information Flow Control)	FortiGate Next Generation Firewalls implement a stateful traffic filtering firewall. Information flow is restricted to that permitted by a policy (set of rules) defined by an authorized administrator. The default policy is restrictive (i.e., no traffic flows without administrator action to configure policy).
FortiGuard Web Filtering	When a request for a web page appears in traffic controlled by the FortiGate unit, the Universal Resource Locator (URL) is sent to a FortiGuard server and the URL category is returned. The FortiGate unit determines if the URL should be allowed or blocked based on the category and the implemented policy.
High Availability (FortiGate Cluster)	The FortiGate Series provides a high availability capability between two or more identical units communicating via the FortiGate clustering protocol. Two modes of operation are supported: active-passive for failover protection and active-active for failover protection and load balancing.
Intrusion Prevention System	FortiGate units use signatures to detect and prevent attacks to the data passing through them. The IPS attack signatures may be updated manually or the FortiGate unit may be configured to automatically download updates. The TOE also includes local anomaly detection to protect itself from direct attacks such as denial of service (DoS) attacks.
IPv6	Both an IPv4 and an IPv6 address may be assigned to any interface on a FortiGate unit. The interface functions as two interfaces; one for IPv4-addressed packets and another for IPv6-addressed packets. The FortiGate series supports static routing, periodic router advertisements, and tunnelling of IPv6-addressed traffic over an IPv4-addressed network. All relevant security claims apply to IPv4 and IPv6.
Logging (management)	The FortiGate supports management activities for configuration and management of logging.
Logging (recording)	Logging is performed and data is transferred to a FortiAnalyzer server in the environment.
Protection Profile[1]	Protection profiles are used to configure anti-virus protection, and IPS.

[1] The term 'Protection Profile' is the name given to a set of Fortinet security rules and should not be confused with Common Criteria PPs.

Feature	Description
Static Routing	Static routes are configured by defining the destination IP address and netmask of packets that the FortiGate unit is intended to intercept, and specifying a (gateway) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.
Time	The FortiGate maintains internal time on a system clock, settable by an authorized administrator. This clock is used when time stamps are generated.
VLAN	The FortiGate supports VLAN as a sub interface attached to a physical interface port. The firewall rules detailed herein may be applied to VLANs.
VPN	The FortiGate supports VPN using SSL or IPsec to provide a secure connection between widely separated office networks or to securely link telecommuters or travellers to an office network.

Table 1 - TOE Features

1.4.2 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Management Workstation	Windows 10 supporting a web browser and terminal application	General Purpose Computer Hardware
FortiGuard Distribution Server	N/A	General Purpose Computer Hardware
VMware Server (for FortiGate VM Models)	ESXi 6.7	General Purpose Computer Hardware (see list of virtual models in Table 19)
VPN Client	Windows 10 with VPN client supporting the TLSv1.1 or TLSv1.2 protocols	General Purpose Computer Hardware
Entropy Token	N/A	Araneus Alea II True Random Number Generator (TRNG) Hardware Token
FortiAnalyzer Server	v6.2.7-build1398 201118 (GA)	General Purpose Computer Hardware

Table 2 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The FortiOS 6.2.7 software is deployed on a stand-alone FortiGate NGFW appliance (see models listed in Annex A) or as a VM running on ESXi. Each

FortiGate NGFW consists of custom hardware and firmware, with the exception of the FortiGate-VM models, which does not include the hardware. The FortiGate unit consists of the following major components: FortiOS FIPS-CC compliant firmware, processor, memory, FortiASIC™, and input/output interfaces.

1.5.2 TOE Interfaces

FortiGate units may be securely administered over the external or internal networks, or locally within the secure area. FortiGate units provide the following administration options:

- A dedicated RS-232 console port is available on all models, with a DB-9 connector. When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiGate unit via the Local Console CLI. This permits an authorized administrator to configure the FortiGate unit, monitor its operation, and examine the audit logs that are created.
- Remote administration may be performed on all models through any network port that has been configured by an authorized administrator to allow HTTPS for the Network Web-Based GUI.
- Remote administration may be performed on all models using Secure Shell (SSH) on port 22.
- All models are equipped with a Universal Serial Bus (USB) port that may be used by an authorized administrator to connect the hardware entropy source.
- On all models, an authorized administrator may configure automatic Anti-Virus and Intrusion Prevention System (IPS) updates from the FortiGuard Distribution Server.

FortiGate units are designed to be installed and used in an environment that is configured and controlled in accordance with the administrator guidance that is supplied with the product.

1.5.3 Single-Unit Configuration

In the single-unit configuration, which is supported by all of the FortiGate series, the TOE consists of a single FortiGate unit. The FortiGate unit controls network access by implementing classic firewall concepts, in which the firewall is linked to two or more networks and controls the transfer of data between them. The configuration supports additional networks, each of which is physically connected to one of the included network interfaces. Figure 1 shows an example of a single FortiGate unit mediating information flow between two networks. One of the networks provides access to the FortiGuard Distribution Server, which permits Anti-Virus and IPS updates to be downloaded and facilitates access to Web filtering data.

The Management Workstation is a general-purpose computer with a standard network interface used to administer the TOE remotely using the Network Web-based GUI or over SSH. A standard serial interface may also be used to administer the TOE locally.

The TOE accesses the FortiGuard Distribution Server, which permits Anti-Virus and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) updates to be downloaded by the TOE.

The TOE acts as a secure gateway for remote clients through an SSL VPN tunnel. All traffic between the user and the FortiGate unit is encrypted using TLS. The TOE may also operate in a gateway-to-gateway configuration creating an IPsec VPN tunnel between two separate private networks.

Note: The gateway to gateway configuration is not depicted in Figure 1.

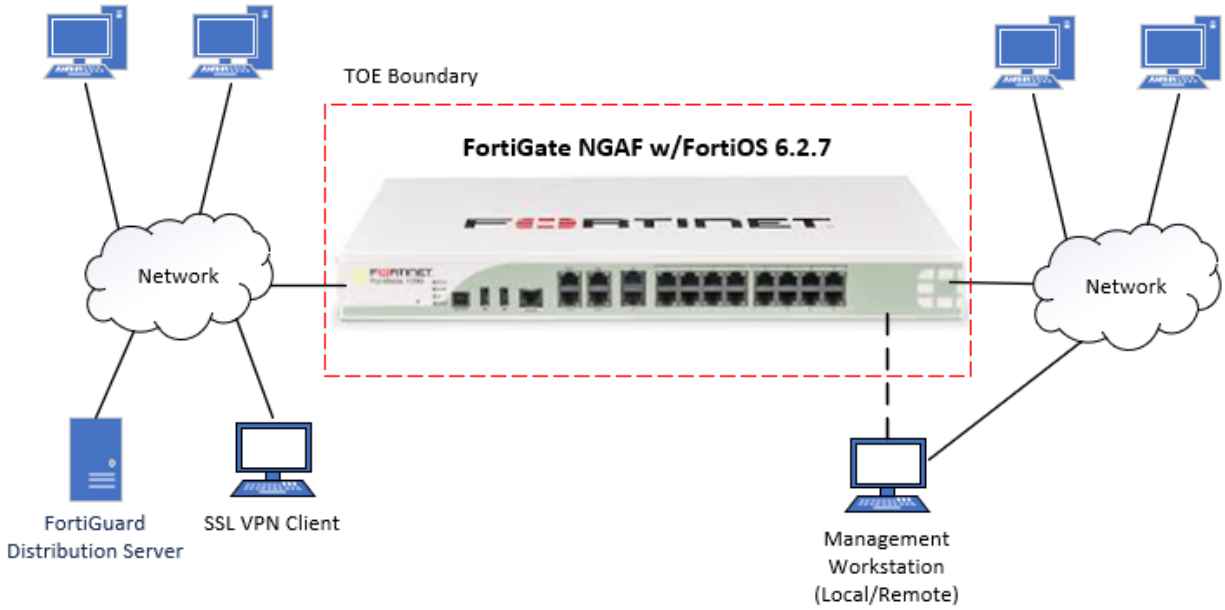

Figure 1 – Single-Unit Configuration

1.5.4 High-Availability Configuration

In the High Availability (HA) configuration, which is supported by all FortiGate units, the TOE consists of two or more FortiGate units interconnected to form a FortiGate Cluster. The FortiGate Cluster controls network access by implementing classic firewall concepts, in which the firewall is linked to two or more networks and controls the transfer of data between them. The configuration supports additional networks, each of which is physically connected to one of the included network interfaces.

Figure 2 shows two FortiGate units of the same type configured in HA mode to form a FortiGate Cluster. A FortiGate Cluster may be configured to work in active-passive mode for failover protection, or in active-active mode for failover protection and load balancing. Both active-passive mode and active-active mode are part of the evaluated configuration of the TOE. The cluster units share state and configuration information over a dedicated High Availability Link. The TOE accesses the FortiGuard Distribution Server, which permits Anti-Virus and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) updates to be downloaded.

The Management Workstation is present as per the single-unit configuration.

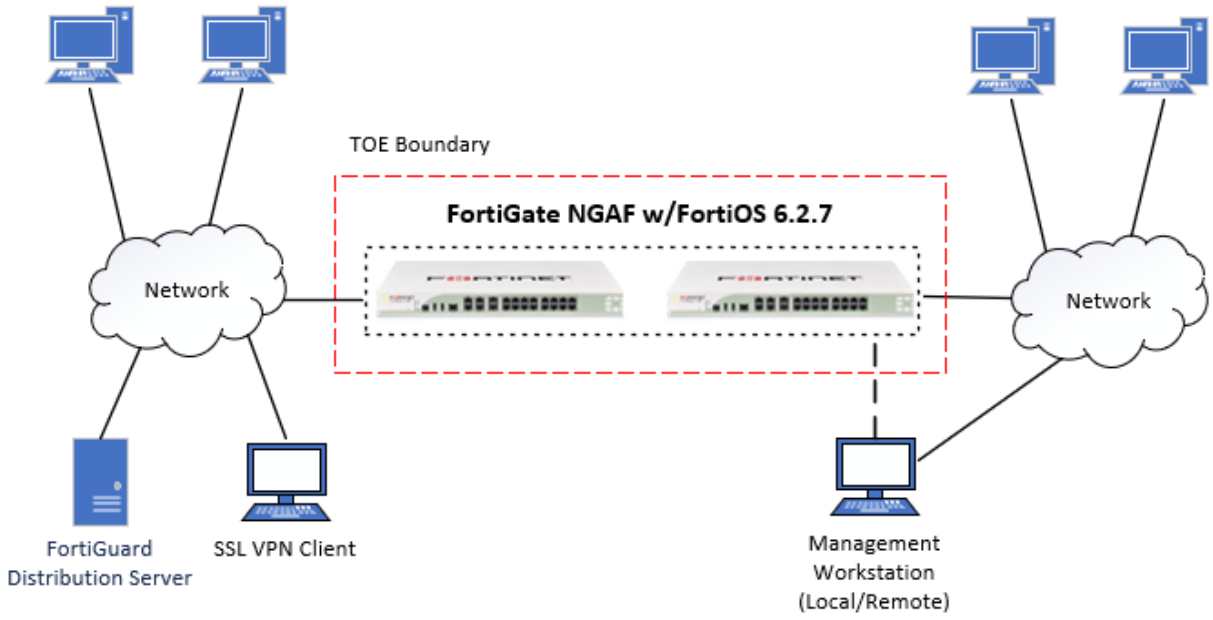

Figure 2 - HA Configuration

1.5.5 TOE Delivery

FortiGate units are shipped directly to customers, but the certified FortiOS image is not preinstalled. Customers can download the correct version by logging in to the Fortinet Customer Support website (https://support.fortinet.com [support.fortinet.com]) and navigating to **Download** > **Firmware Images.**

Due to having different device drivers, each model offered in the FortiGate Series has its own unique firmware image created from the same common firmware build. For each series, the hardware model identifier changes (e.g. *301E*).

Customers can download the image based on their FortiGate hardware model. The images are provided to customers as a .out file. An example of a filename is as follows:

- *FGT_301E-v6-build1190-FORTINET.out*

1.5.5.1 TOE Guidance

All guidance documentation is available for download in Portable Document Format (PDF) format at: https://docs.fortinet.com/product/FortiGate/6.2.

The TOE includes the following guidance documentation:

- FortiOS – CLI Reference, Version 6.2.7, February 9, 2021
  - *FortiOS-6.2.7-CLI_Reference.pdf*
- FortiOS - Log Reference, Version 6.2.7, December 17, 2020
  - *FortiOS_6.2.7_Log_Reference.pdf*
- FortiOS - Cookbook, Version 6.2.7, February 10, 2021
  - *FortiOS-6.2.7-Cookbook.pdf*
- FortiOS – Handbook, Version 6.0, June 17, 2020

- *FortiOS-6.0-Handbook.pdf*

In addition to the above, a series of Information Supplement, QuickStart, Security System and Installation guides are included as part of the TOE. Each of these guides is specific to the hardware model it references. A list of these guides is provided in Table 18 (for hardware models) and Table 19 (for virtual models).

The following FIPS and Common Criteria Guidance Supplement is also available to customers, in Portable Document Format (PDF) format, upon request:

- FortiOS 6.2 and FortiGate NGFW Appliances, EAL4 Common Criteria Technote, May 25, 2021
  - *FOS 62 Technote – NGFW EAL4.pdf*

1.5.6 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	The TOE generates audit records for security relevant events.
Cryptographic Support	Cryptographic functionality is provided to protect communications for remote administration, VPN, and peer-to-peer connections within a cluster.
User Data Protection	The TOE provides interfaces to a defined set of networks and mediates information flow among these networks. The TOE supports firewall and web filtering policies.
Identification and Authentication	All TOE administrative users must be identified and authenticated. Administration may be performed locally using the Local Console CLI, remotely using the Network Web-based GUI, or remotely over SSH. 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.
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. The terms 'administrator' and 'authorized administrator' are used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required.

Functional Classes	Description
Protection of the TSF	The TOE provides failover in support of the high availability features. Reliable time stamps are provided in support of the audit function.
Trusted Path/Channel	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 VPN peers (client or gateway) and TLS connections (FortiAnalyzer). The TOE requires an encrypted trusted channel for communication between FortiGate devices in support of the High Availability configuration.
Anti-Virus Actions	The TOE supports anti-virus detection and the ability to block or quarantine suspected information. A secure mechanism is used to update virus signatures.
Intrusion Prevention	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.

Table 3 – Logical Scope of the TOE

1.5.7 Functionality Excluded from the Evaluated Configuration

1.5.7.1 Excluded Features

The following TOE features are excluded from this evaluation:

- Centralized management of the TOE by FortiManager servers
- The TOE's antispam, content filtering and traffic shaping features
- The ICMP, SNMP, LDAP, Windows AD, NTP, Radius and Routing protocols
- The FortiGate REST API (not used in the evaluated configuration)
- FortiGuard-Antispam, Endpoint Control, and FortiSandbox services
- The TOE's DHCP, DDNS, or DNS server capabilities
- Traffic offloading to the FortiASIC NPx network processors

1.5.7.2 Disabled Features

The following TOE features are disabled by default and are excluded from the scope of this evaluation:

- HTTP GUI
- The TOE acting as a telnet client or server
- The TOE acting as a TFTP client.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 4 augmented with ALC_FLR.3 Systematic Flaw Remediation.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are unauthorized persons or external IT entities not authorized to use the TOE itself. The threat agents are assumed to have a low to moderate attack potential and are assumed to have a moderate level of resources and access to all publicly available information about the TOE and potential methods of attacking the TOE. It is expected that the FortiGate units will be protected to the extent necessary to ensure that they remain connected to the networks they protect.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
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, 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.MEDIATE	An unauthorized person may attempt to send impermissible information through the TOE, which could result 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.PRIVILEGE	An unauthorized user may attempt to 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, between VPN peers and the TOE, or between TOE devices.
T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

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

OSP	Description
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.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.LOCATE	The hardware appliances will be located within controlled access facilities and protected from unauthorized physical modification.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security operational environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the operational environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow only authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions by providing a means to record an audit trail of security-related events, with accurate dates and times.
O.ENCRYPT	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, between itself and VPN peers, or between TOE devices using cryptographic functions.
O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROTECT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
O.TIME	The TOE shall provide reliable time stamps.
O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.AUDACC	T.COMDIS	T.MEDIATE	T.NOAUTH	T.NOHALT	T.PRIVILEGE	T.PROCOM	T.VIRUS	P.ACCACT	P.DETECT	P.MANAGE	A.LOCATE	A.MANAGE	A.SINGEN
O.ACCESS			X			X	X					X			
O.ADMIN		X										X			
O.AUDIT		X								X	X				
O.ENCRYPT					X			X							
O.IDENTAUTH			X		X	X	X			X		X			
O.MEDIATE	X			X											
O.PROTECT			X			X	X					X			
O.TIME										X	X				
O.VIRUS									X						
OE.ADMIN												X		X	
OE.PHYSICAL													X		
OE.SINGEN															X

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: 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.	
Objectives:	O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
Rationale:	O.MEDIATE mitigates this threat by ensuring that all information	

	between clients and servers located on internal and external networks is mediated by the TOE.	

Threat: T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not created, thus allowing an attacker to escape detection.	
Objectives:	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.AUDIT	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions by providing a means to record an audit trail of security-related events, with accurate dates and times.
Rationale:	O.ADMIN provides for security management functionality. O.AUDIT requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.	

Threat: T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.	
Objectives:	O.ACCESS	The TOE must allow only authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.
	O.PROTECT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
Rationale:	The O.IDENTAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTECT objective addresses this threat by providing TOE self-protection.	

Threat: T.MEDIATE	An unauthorized person may attempt to send impermissible information through the TOE, which could result in the exploitation of resources on the internal network.	
Objectives:	O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
Rationale:	O.MEDIATE requires that all information that passes through the networks is mediated by the TOE, blocking unauthorized users, and impermissible information.	

Threat: 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.

Objectives:	O.ENCRYPT	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, between itself and VPN peers, or between TOE devices using cryptographic functions.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.
Rationale:	O.IDENTAUTH requires that users be uniquely identified before accessing the TOE. O.ENCRYPT ensures the confidentiality and integrity of data passed between the TOE and the authorized administrator, between itself and VPN peers, and between TOE devices.	

Threat: T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.
	O.PROTECT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
Rationale:	The O.IDENTAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this threat by requiring the TOE to protect itself against bypass, or to deny access to legitimate users.	

Threat: T.PRIVILEGE	An unauthorized user may attempt to gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IENTDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IENTDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this threat by providing TOE self-protection.	

Threat: 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, between VPN peers and the TOE, or between TOE devices.	
Objectives:	O.ENCRYPT	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, between itself and VPN peers, or between TOE devices using cryptographic functions.
Rationale:	O.ENCRYPT requires encryption for remote administration of the TOE, VPN use, and communications between TOE devices.	

Threat: T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.	
Objectives:	O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.
Rationale:	The O.VIRUS objective ensures that the TOE detects and blocks viruses which are contained in any information flow which reaches one of the TOE network interfaces.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE.

Policy: P.ACCACT	Users of the TOE shall be accountable for their actions.	
Objectives:	O.AUDIT	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions by providing a means to record an audit trail of security-related events, with accurate dates and times.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
Rationale:	The O.AUDIT objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. O.TIME supports the audit trail with reliable time stamps.	

Policy: P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected.	
Objectives:	O.AUDIT	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions by providing a means to record an audit trail of security-related events, with accurate dates and times.
	O.TIME	The TOE shall provide reliable time stamps.
Rationale:	The O.AUDIT objective supports this policy by ensuring the collection of data on security relevant events.	

	O.TIME supports this policy by ensuring that the audit functionality is able to include reliable timestamps.

Policy: P.MANAGE	The TOE shall be manageable only by authorized administrators.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
	O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.
	O.PROTECT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.
	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	The O.ACCESS objective supports this policy by ensuring that authorized administrators have appropriate access to manage the TOE. O.ADMIN supports this policy by ensuring that the TOE provides the appropriate security management functionality to authorized administrators. O.IDENTAUTH supports this policy by ensuring that administrators must be identified and authenticated prior to being granted access to TOE security management functions. O.PROTECT supports this policy by ensuring that the TOE security functions may not be bypassed to allow unauthorized access. OE.ADMIN supports this policy by ensuring that only competent, trained administrators have access to the TOE security functions.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: A.LOCATE	The hardware appliances will be located within controlled access facilities and protected from unauthorized physical modification.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
Rationale:	The OE.PHYSICAL objective supports this assumption by ensuring the physical protection of the hardware appliances.	

Assumption: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	The OE.ADMIN objective supports the assumption by ensuring that all authorized administrators are qualified and trained to manage the TOE.	

Assumption: A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	
Objectives:	OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
Rationale:	This objective supports the assumption by requiring that the information flow subject to security policy is made to pass through the TOE.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFR)s used in this ST. Three extended SFRs have been created to address additional security features of the TOE. They are:

a. Anti-Virus Actions (FAV_ACT_EXT.1);

b. Denial of Service (FIP_DOS_EXT.1); and

c. Signature Protection (FIP_SIG_EXT.1).

5.2 CLASS FAV: ANTI-VIRUS ACTION REQUIREMENTS

A new class, FAV, was created to address the detection and blocking of malware. FPT: Protection of the TSF, was used as a model for creating these requirements. The purpose of this class of requirements is to address the Anti-Virus functionality provided by the TOE. This new class has a single family – FAV_ACT_EXT. FAV_ACT_EXT.1 was loosely modelled after FPT_TEE.1: Testing of external entities.

5.2.1 FAV_ACT_EXT Anti-Virus Actions

Family Behaviour

This family defines the requirements for virus detection and blocking. This family may be used to specify anti-virus detection and blocking capabilities.

Component Levelling

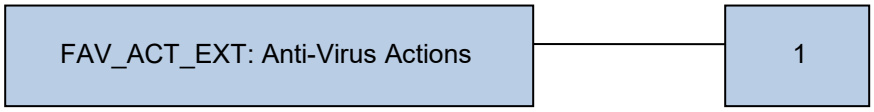

Figure 3 – FAV_ACT_EXT: Anti-Virus Actions Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a) The management of actions on the information flow when a virus is detected;

b) The management of actions on virus signatures.

Audit

The following actions should be auditable:

a) Minimal: actions taken on the information flow when virus is detected.

FAV_ACT_EXT.1 Anti-Virus Actions

Hierarchical to: No other components.

Dependencies: No dependencies

FAV_ACT_EXT.1.1 The TSF shall provide an authorized administrator the capability to select one or more of the following actions: [selection: quarantine the

content of the information flow, remove the content of the information flow, [*assignment: other action*]] to be taken on detection of a virus in an information flow.

FAV_ACT_EXT.1.2 The TSF shall provide a secure mechanism to update the virus signatures used by the TSF.

Application Note: Virus signature updates consist of updates to both the virus signature database and the processing engine for the detection of virus attacks. The TOE provides specific guidance to administrators noting that in the evaluated configuration of the TOE, only the virus signature database updates may be applied to the TOE.

5.3 CLASS FIP: INTRUSION PREVENTION

A class of FIP requirements was created to address the intrusion prevention functionality provided by the TOE. FPT: Protection of the TSF, was used as a model for creating these requirements. The purpose of this class of requirements is to address the Denial of Service (DoS) and signature-based protection functionality provided by the TOE. This class of requirements has two families – FIP_DOS_EXT and FIP_SIG_EXT. FIP_DOS_EXT.1 and FIP_SIG_EXT.1 were loosely modelled after FPT_TEE.1: Testing of external entities.

5.3.1 FIP_DOS_EXT Denial of Service Prevention

Family Behaviour

This family defines the requirements for detection and blocking of potential Denial of Service attacks. This family may be used to specify the use of DoS capabilities.

Component Levelling

Figure 4 – FIP_DOS_EXT: Denial of Service Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a. Basic: Configuring of DoS policy.

Audit

The following actions should be auditable:

a. Basic: Detection of a possible DoS attack.

FIP_DOS_EXT.1 Denial of Service

Hierarchical to:	No other components.
Dependencies:	No dependencies
FIP_DOS_EXT.1.1	The TSF shall be able to recognize and block potential Denial of Service attacks.

5.3.2 FIP_SIG_EXT Signature Protection

Family Behaviour

This family defines the requirements for detection and blocking of potential IPS attacks. This family may be used to specify the IPS policies and signatures.

Component Levelling

Figure 5 – FIP_SIG_EXT: Signature Protection Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a. Configuring of IPS policies; and

b. Update of IPS signatures.

Audit

The following actions should be auditable:

b. Basic: Detection of a possible attack incident; and

c. Basic: Update of the signature protection profile.

FIP_SIG_EXT.1 Signature Protection

Hierarchical to:	No other components.
Dependencies:	No dependencies
FIP_SIG_EXT.1.1	The TSF shall detect and block potential attacks based on similarities to known attack signatures.

5.4 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Symmetric Keys)
	FCS_CKM.1(2)	Cryptographic key generation (RSA Keys)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1(1)	Subset information flow control (Firewall SFP)
	FDP_IFC.1(2)	Subset information flow control (Web Filtering SFP)
	FDP_IFF.1(1)	Simple security attributes (Firewall SFP)
	FDP_IFF.1(2)	Simple security attributes (Web Filtering SFP)
Identification and	FIA_AFL.1	Authentication failure handling

Class	Identifier	Name
Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Firewall SFP)
	FMT_MSA.1(2)	Management of security attributes (Web Filtering SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Firewall SFP)
	FMT_MSA.3(2)	Static attribute initialisation (Web Filtering SFP)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Intrusion Prevention (FIP)	FIP_DOS_EXT.1	Denial of service
	FIP_SIG_EXT.1	Signature protection
Anti-Virus Action Requirements (FAV)	FAV_ACT_EXT.1	Anti-Virus Actions

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*All auditable events listed in* Table 11].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in* Table 11].

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1(1) FCS_CKM.1(2)	Success or failure of the activity	
FDP_IFF.1(1) FDP_IFF.1(2)	Decisions to permit/deny information flows	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and action taken	Identity of the unsuccessfully authenticated user
FIA_UAU.2	All uses of the authentication mechanism	
FIA_UAU.5	Decision of the authentication mechanism	Claimed identity of the user attempting to authenticate
FIA_UID.2	Unsuccessful use of the user identification mechanism	Claimed identity of the user using the identification mechanism
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	The identity of the administrator performing the function
FMT_MSA.1(1) FMT_MSA.1(2)	Modification of the security attributes	The identity of the administrator performing the function
FMT_MSA.3(1) FMT_MSA.3(2)	Modification to the default settings or initial values of security attributes	
FMT_SMF.1	Use of management functions	The identity of the administrator performing the function
FMT_SMR.1	Modifications to the group of users that are part of a role	User identification of the administrator performing modification, and the user whose role is modified
FPT_FLS.1	Failure of a unit within a cluster	
FPT_STM.1	Changes to the time	The identity of the administrator performing the operation
FAV_ACT_EXT	Actions taken on the information flow when virus is detected	
FIP_DOS_EXT.1	Detection of a potential Denial of Service	
FIP_SIG_EXT.1	Triggering of a match to a known signature	

Table 11 - Auditable Events

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1(1) Cryptographic key generation (symmetric keys)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*CTR DRBG (Advanced Encryption Standard (AES))*] and specified cryptographic key sizes [*128, 256 bit*] that meet the following: [*National Institute of Standards and Technology (NIST) Special Publication 800-90A*].

6.2.2.2 FCS_CKM.1(2) Cryptographic key generation (RSA keys)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Rivest Shamir Adleman (RSA)*] and specified cryptographic key sizes [*2048, 3072 bit*] that meet the following: [*FIPS 186-4*].

6.2.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in* Table 12] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in* Table 12] and cryptographic key sizes [*cryptographic key sizes specified in* Table 12] that meet the following: [*standards listed in* Table 12].

Operation	Algorithm	Key Size or Digest (bits)	Standard	CAVP Cert Number
Encryption and Decryption	AES (CBC mode only or CBC and GCM modes)	128, 256	FIPS PUB 197 (AES) and NIST SP 800-38A	C1549 C1575 C1576 C1578 C1797 C1798 C2140 C2197 C2199 C2200 C2201 A1187 A1339 A1349
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS1-v1_5 using SHA-256)	2048, 3072	PKCS #1.5	C1576 C1578 C1797 C1798 C2199 C2201 A1187
	Elliptic Curve Digital Signature Algorithm (ECDSA)	P-256, P-384, P-521	FIPS 186-4 (Digital Signature Standard)	C1575 C1576 C1578 C1798 C2197 C2199 C2200 C2201 A1187 A1349
Key agreement	Key Agreement Schemes (KAS) and Key Confirmation	2048, 3072	NIST SP800-56A	C1575 C1576 C1578 C1798 C2197 C2199 C2200 C2201 A1187 A1349 A1253
	EC DH	P-256, P-384		
Hashing	SHA-1	160	FIPS PUB 180-3	C1575 C1576 C1578
	SHA-256	256		

Operation	Algorithm	Key Size or Digest (bits)	Standard	CAVP Cert Number
	SHA-384	384		C1797 C1798 C2197 C2200 C2201 A1187 A1349
Keyed Hash	HMAC-SHA-1	160 key 160 digest	FIPS PUB 198	C1575 C1576 C1578 C1797 C1798 C2197 C2199 C2200 C2201 A1187 A1349
	HMAC-SHA-256	256 key 256 digest		
	HMAC-SHA-384	384 key 384 digest		
Random Bit Generation	CTR_DRBG	N/A	NIST SP800-90A	C1573 C2195 C2198 A1348

Table 12 - Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1(1) Subset information flow control (Firewall SFP)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [*Firewall SFP*] on:

[*Subjects: users and IT entities*[2]*;*

Information: network traffic[3]*;*

Operations: pass information].

6.2.3.2 FDP_IFC.1(2) Subset information flow control (Web Filtering SFP)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [*Web Filtering SFP*] on:

[2] Users and IT entities that exchange information via the TOE

[3] Any network traffic sent through the TOE from one subject to another

[*Subjects: users*

Information: web pages

Operations: HTTP and HTTPS].

6.2.3.3 FDP_IFF.1(1) Simple security attributes (Firewall SFP)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(1) The TSF shall enforce the [*Firewall SFP*] based on at least the following types of subject and information security attributes:

[*Subjects: users and external entities*

Subject security attributes:

- *presumed address;*
- *user identity;*
- *user group.*

Information: network traffic

Information security attributes:

- *presumed address of source subject;*
- *presumed address of destination subject;*
- *TOE interface on which the traffic arrives and departs;*
- *service (protocol);*
- *schedule*].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[*Subjects can cause information to flow through the TOE to another connected network if all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes*].

FDP_IFF.1.3(1) The TSF shall enforce the [*none*].

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.2.3.4 FDP_IFF.1(2) Simple security attributes (Web Filtering SFP)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(2) The TSF shall enforce the [*Web Filtering SFP*] based on at least the following types of subject and information security attributes:

[*Subjects: users*

Subject security attributes:

- *optional user ID;*
- *optional user group.*

Information: web pages

Information security attributes:

- *URL;*
- *category assigned by FortiGuard web filtering service based on the website content;*
- *local category, if applicable;*
- *override, if applicable.*]

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) The policy for the category to which the URL has been assigned by the FortiGuard web filtering service is set to 'allow';

b) The local category, if used, is set to 'allow'].

FDP_IFF.1.3(2) The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [

a) *An override has been set for the URL*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Application Note: The FortiGuard web filtering service assigns all websites to a category based on content. Those not assigned to other categories are assigned to the 'Unrated' category. For example, the cached content classification indicates that the site caches content, but provides no indication of the content type.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an ~~administrator configurable positive integer within~~ **administrator configured number between** *1 and 10*] unsuccessful authentication attempts occur related to [*authorized TOE administrator access*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [*lock out the application TCP session for a configurable period of time*].

Application Note: This feature is not applicable to console login or public key authentication.

6.2.4.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) identity;

b) role;

c) authentication data].

6.2.4.3 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*password, one time passcode, pre-shared key, public key, and X.509 certificate based authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*the following rules:*

a) administrators authenticate to the console, CLI or web interface via username and password;

b) administrators may authenticate via username and password or RSA public key for remote SSH connections;

c) users authenticate to the TOE using a username and password;

d) x.509 certificates are used to authenticate IPsec and SSL VPN peers;

e) pre-shared keys are used to authenticate IPsec VPN peers; and

f) x.509 certificates are used to authenticate FortiAnalyzer to the TOE].

6.2.4.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [enable, disable, modify the behaviour of] the functions [

a) *Denial of Service (DOS) detection policy implementation; and*

b) *Signature based protection policy implementation*]

to [*an authorized administrator*].

6.2.5.2 FMT_MSA.1(1) Management of security attributes (Firewall SFP)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(1) The TSF shall enforce the [*Firewall SFP*] to restrict the ability to [*delete attributes from a rule, modify attributes in a rule, add attributes to a*

rule] the security attributes [*user identity user group, source address, destination address, service, schedule*] to [*the authorized administrator*].

6.2.5.3 FMT_MSA.1(2) Management of security attributes (Web Filtering SFP)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [Web Filtering *SFP*] to restrict the ability to [query, modify, delete] the security attributes [*user ID, user group, URL, category, and override setting*] to [*the authorized administrator*].

6.2.5.4 FMT_MSA.3(1) Static attribute initialisation (Firewall SFP)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Firewall SFP*] to provide [restrictive] default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*authorized administrator*] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1(1) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

6.2.5.5 FMT_MSA.3(2) Static attribute initialisation (Web Filtering SFP)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*Web Filtering SFP*] to provide [permissive] default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*authorized administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) administer firewall policy rules;

b) administer web filtering functionality;

c) administer VPN rules;

d) administer security audit functionality;

e) administer user account information;

f) administer authentication mechanisms and authentication failure handling policy;

g) administer DoS and signature based protection policy implementation].

6.2.5.7 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*administrator*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*failure of a unit in a FortiGate cluster is detected*].

Application Note: The FPT_FLS.1 requirement is only implemented in the High Availability configuration of the TOE.

6.2.6.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*High Availability Cluster communication, IPsec VPN services (gateway-to-gateway), SSL VPN services (client-to-gateway) and SSL TLS services (TOE-to-FortiAnalyzer)*].

6.2.7.2 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*remote administration*].

6.2.8 Intrusion Prevention (FIP)

6.2.8.1 FIP_DOS_EXT.1 Denial of Service

Hierarchical to: No other components.

Dependencies: No dependencies.

FIP_DOS_EXT.1.1 The TSF shall be able to recognize and block potential Denial of Service attacks.

6.2.8.2 FIP_SIG_EXT.1 Signature Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FIP_SIG_EXT.1.1 The TSF shall detect and block potential attacks based on similarities to known attack signatures.

6.2.9 Anti-Virus Requirements (FAV)

6.2.9.1 FAV_ACT_EXT.1 Anti-Virus Actions (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

FAV_ACT_EXT.1.1 The TSF shall provide an authorized administrator the capability to select one or more of the following actions:[quarantine the content of

the information flow, remove the content of the information flow, [*monitor the content of the information flow*]] to be taken on detection of a virus in an information flow.

FAV_ACT_EXT.1.2 The TSF shall provide a secure mechanism to update the virus signatures used by the TSF.

Application Note: Virus signature updates consist of updates to both the virus signature database and the processing engine for the detection of virus attacks. The TOE provides specific guidance to administrators noting that in the evaluated configuration of the TOE, only the virus signature database updates may be applied to the TOE.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in the following table.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools

Assurance Class	Assurance Components	
	Identifier	**Name**
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.3	Focused vulnerability analysis

Table 13 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.MEDIATE	O.PROTECT	O.REUSE	O.TIME	O.VIRUS
FAU_GEN.1			X							
FAU_GEN.2			X							
FCS_CKM.1(1)				X						
FCS_CKM.1(2)				X						
FCS_CKM.4				X						
FCS_COP.1				X						
FDP_IFC.1(1)						X				
FDP_IFC.1(2)						X				
FDP_IFF.1(1)						X				
FDP_IFF.1(2)						X				
FIA_AFL.1							X			
FIA_ATD.1					X					
FIA_UAU.2	X				X			X		

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYPT	O.IDENTAUTH	O.MEDIATE	O.PROTECT	O.REUSE	O.TIME	O.VIRUS
FIA_UAU.4					X			X		
FIA_UAU.5					X					
FIA_UID.2	X				X					
FMT_MOF.1	X	X					X			
FMT_MSA.1(1)	X	X					X			
FMT_MSA.1(2)	X	X					X			
FMT_MSA.3(1)		X					X			
FMT_MSA.3(2)		X					X			
FMT_SMF.1		X					X			
FMT_SMR.1					X		X			
FPT_FLS.1							X			
FPT_STM.1									X	
FTP_ITC.1				X						
FTP_TRP.1				X						
FIP_DOS_EXT.1						X	X			
FIP_SIG_EXT.1						X	X			
FAV_ACT_EXT.1						X				X

Table 14 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Firewall SFP)
	FMT_MSA.1(2)	Management of security attributes (Web Filtering SFP)
Rationale:	FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated prior to being allowed access to TOE security management functionality. FMT_MOF.1 ensures that only authorized administrators have access to IPS security management functions. FMT_MSA.1(1) and FMT_MSA.1(2) ensure that only authorized administrators have access to the security attributes associated with the firewall and web filtering security functional policies.	

Objective: O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	
Security Functional Requirements:	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Firewall SFP)
	FMT_MSA.1(2)	Management of security attributes (Web Filtering SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Firewall SFP)
	FMT_MSA.3(2)	Static attribute initialisation (Web Filtering SFP)
	FMT_SMF.1	Specification of Management Functions
Rationale:	FMT_MOF.1 meets this objective by providing functionality to manage the behaviour of the Denial of Service and signature based protection features of the TOE. FMT_MSA.1(1) and FMT_MSA.1(2) meet the objective by providing the functionality to manage the parameters associated with the firewall and web filtering security functional policies. FMT_MSA.3(1) and FMT_MSA.3(2) meet the objective by providing the initial values required to manage the firewall and web filtering security functional policies. FMT_SMF.1 meets the objective by providing the management functions supporting the specific security management claims.	

Objective: O.AUDIT	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions by providing a means to record an audit trail of security-related events, with accurate dates and times.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
Rationale:	FAU_GEN.1 supports the objective by detailing the set of events that the	

	TOE must be capable of recording, ensuring that any security relevant event that takes place in the TOE is audited. FAU_GEN.2 supports the objective by ensuring that the audit records associate a user identity with the auditable event.

Objective: O.ENCRYPT	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, between itself and VPN peers, or between TOE devices using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1(1)	Cryptographic key generation (Symmetric keys)
	FCS_CKM.1(2)	Cryptographic key generation (RSA keys)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Rationale:	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4, and FCS_COP.1 support the objective by providing the cryptographic functionality required to support trusted links. FTP_ITC.1 and FTP_TRP.1 support the objective by specifying the use of cryptography between trusted VPN clients and peer devices, and between the TOE and the remote administrator.	

Objective: O.IDENTAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE security management functions or, if required, to a connected network.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
	FMT_SMR.1	Security roles
Rationale:	FIA_ATD.1 supports this objective by ensuring that the data required to identify and authenticate users is maintained by the TOE. FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated prior to being granted access to TOE security management functions, or to a connected network. FIA_UAU.4 supports the objective by providing a single use authentication mechanism. FIA_UAU.5 provides multiple possible authentication mechanisms that may be used to support the objective. FMT_SMR.1 supports the objective by providing roles which are used to provide users access to TOE security functionality.	

Objective: O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.	
Security Functional Requirements:	FDP_IFC.1(1)	Subset information flow control (Firewall SFP)
	FDP_IFC.1(2)	Subset information flow control (Web Filtering SFP)
	FDP_IFF.1(1)	Simple security attributes (Firewall SFP)

	FDP_IFF.1(2)	Simple security attributes (Web Filtering SFP)
	FAV_ACT_EXT.1	Anti-Virus Actions
	FIP_DOS_EXT.1	Denial of Service Prevention
	FIP_SIG_EXT.1	Signature Protection
Rationale:	FDP_IFC.1(1) and FDP_IFF.1(1) support the objective by detailing how the TOE mediates the flow of information for the firewall policy. FDP_IFC.1(2) and FDP_IFF.1(2) support the objective by detailing how the TOE mediates the flow of information for the web filtering policy. FIP_DOS_EXT.1 and FIP_SIG_EXT.1 support the objective by detecting and preventing denial of service attacks and attacks with known signatures present in the information flow. FAV_ACT_EXT.1 supports the objective by taking specific actions when a virus is detected in the flow of information.	

Objective: O.PROTECT	The TOE must protect itself and the designated network against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions in such a way as to cause unauthorized access to its functions and data, or to deny access to legitimate users.	
Security Functional Requirements:	FIA_AFL.1	Authentication failure handling
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Firewall SFP)
	FMT_MSA.1(2)	Management of security attributes (Web Filtering SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Firewall SFP)
	FMT_MSA.3(2)	Static attribute initialisation (Web Filtering SFP)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FPT_FLS.1	Failure with preservation of secure state
	FIP_DOS_EXT.1	Denial of service
	FIP_SIG_EXT.1	Signature protection
Rationale:	The security management SFRs, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1 and FMT_SMR.1 support the objective by ensuring that access to TOE security functions is limited to authorized users. FIA_AFL.1 supports the objective by ensuring that unauthorized users are locked out following a configurable number of unsuccessful authentication attempts, thereby thwarting a brute force attack on the TOE. FPT_FLS.1 supports the objective by ensuring that the TOE, in a high availability configuration, remains secure and operational in the case of a unit failure. FIP_DOS_EXT.1 and FIP_SIG_EXT.1 support the objective by preventing denial of service attacks and attacks identifiable by their unique signatures.	

Objective: O.REUSE	The TOE must provide a means to prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	
Security Functional	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms

Requirements:		
Rationale:	FIA_UAU.2 and FIA_UAU.4 support this objective by providing a single use authentication mechanism and requiring users to be authenticated prior to gaining access.	

Objective: **O.TIME**	The TOE shall provide reliable time stamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 supports this objective by requiring that the TOE be able to provide reliable time stamps.	

Objective: **O.VIRUS**	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.	
Security Functional Requirements:	FAV_ACT_EXT.1	Anti-virus actions
Rationale:	FAV_ACT_EXT.1 supports this objective by ensuring that the TOE can detect and block information that may contain a virus.	

6.4.3 Dependency Rationale

Table 15 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1.
	FCS_CKM.4	✓	
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1.
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1.
	FCS_CKM.4	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FDP_IFC.1(1)	FDP_IFF.1	✓	Satisfied by FDP_IFF.1(1).
FDP_IFC.1(2)	FDP_IFF.1	✓	Satisfied by FDP_IFF.1(2).
FDP_IFF.1(1)	FDP_IFC.1	✓	Satisfied by FDP_IFC.1(1).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1).
FDP_IFF.1(2)	FDP_IFC.1	✓	Satisfied by FDP_IFC.1(2).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2).
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.4	None	N/A	
FIA_UAU.5	None	N/A	
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1(1).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1(2).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1).
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2).
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_FLS.1	None	N/A	
FTP_ITC.1	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FTP_TRP.1	None	N/A	
FAV_ACT_EXT.1	None	N/A	
FIP_DOS_EXT.1	None	N/A	
FIP_SIG_EXT.1	None	N/A	

Table 15 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.3). EAL 4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.3 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 4.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 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.

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. If 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.

All audit records are transferred to the FortiAnalyzer servers where they can be reviewed in real-time.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2.

7.2 CRYPTOGRAPHIC SUPPORT

The TOE includes the FortiOS FIPS-validated cryptographic module (CMVP certificate #3814). The cryptographic module is used in support of the TLS, SSH, and IPsec protocols. Asymmetric keys are also generated in support of TLS functionality.

Models deployed with the FortiASIC™ Content Processor 8 (CP8) and those that do no contain a FortiASIC™ (including all virtual models) rely on the Araneus Alea II hardware token as their entropy source. Models deployed with the FortiASIC CP9, CP9lite or CP9Xlite rely on the processor. The entropy source for each hardware model can be found in Table 18 (hardware models) and Table 19 (virtual models).

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.

Cryptographic operations are performed in accordance with the detail provided in Table 12.

The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

TOE Security Functional Requirements addressed: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

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

a. The Firewall SFP allows authenticated and unauthenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by an authorized administrator. Separate policies may be defined for unauthenticated and authenticated users;

b. 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 Firewall SFP have restrictive default values and by default no information is allowed to flow. The Web Filtering SFP has permissive default values, and does not block URLs until specifically identified. 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 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 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 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 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. First matched policy must explicitly allow traffic to flow;
3. If configured, 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.

TOE Security Functional Requirements addressed: FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FMT_MSA.3(1), FMT_MSA.3(2).

7.4 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 are 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 and users, the identification and authentication mechanism are a username and password combination. Local users and administrators are presented with a system screen (configurable by an authorized administrator) prior to authentication. For remote SSH administration, a username and password combination or SSH-RSA public key authentication are used. VPN peers authenticate using pre-shared keys or certificates for IPsec VPNs (gateway-to-gateway) and SSL VPNs (client-to-gateway or TOE-to-FortiAnalyzer). The accounts are created by an authorized administrator over the serial or network interfaces.

All certificate-based authentication is performed against a CA certificate held inside a trust store maintained by the TOE.

After a configurable number of unsuccessful authentication attempts, administrators are prevented from attempting to login from the same IP session for a preconfigured amount of time.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2.

7.5 SECURITY MANAGEMENT

Appropriately authorized administrators may manage security function behaviour, 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 local Console CLI for administrators to manage all of the security functions.

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.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_SMF.1, FMT_SMR.1.

7.6 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 appliances 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.

TOE Security Functional Requirements addressed: FPT_FLS.1, FPT_STM.1.

7.7 TRUSTED PATH / CHANNELS

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 and all remote administrator actions.

The VPN functionality supports IPsec and SSL tunnel modes. 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. TOE devices support IKEv1 and IKEv2.

In the evaluated configuration, IKE protocols support the use of Diffie-Hellman (DH) 15 (with 3072 MODP). Certificate based authentication may be used, as well as pre-shared key based authentication for IPsec peer connections.

In SSL tunnel mode, remote clients connect to the FortiGate unit that acts as a secure HTTPS gateway and authenticates remote users as members of a user group. Each user must have a unique user certificate installed on their PC that is checked against the CA certificate during the authentication process. When the user initiates a VPN connection with the FortiGate unit through the SSL VPN client. The FortiGate unit then assigns the client a virtual IP address from a range of reserved addresses. The client uses the assigned IP address as its source address for the duration of the connection. After the tunnel has been established, the user can access the network behind the FortiGate unit.

The TOE acts as the client for SSL tunnels between the TOE and the FortiAnalyzer. The FortiAnalyzer server has the X.509 certificate verified by the TOE using a trusted CA certificate.

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 (RFC 4346) and TLS 1.2 (RFC 5246) are used to encrypt and authenticate administration sessions between the remote browser and TOE. When a connection is first established, the server presents the public key 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. Local administrator account credentials can be used to successfully authenticate to the TOE via the Network Web-Based GUI.

SSH is used to protect remote connections to the CLI. Administrators use password based or SSH-RSA public key authentication.

The trusted channels provide communication between the TOE and other TOE devices in support of the HA cluster configuration. This channel is logically distinct from other communication channels. The channel is encrypted with AES-128. 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.

TOE Security Functional Requirements addressed: FTP_ITC.1 and FTP_TRP.1

7.8 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 can 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.

TOE Security Functional Requirements addressed: FIP_DOS_EXT.1, FIP_SIG_EXT.1.

7.9 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.

TOE Security Functional Requirements addressed: FAV_ACT_EXT.1

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Firewall Rules	Firewall rules are configuration parameters set by an authorized administrator that allow or deny data flow through the TOE. These rules may optionally include the use of a firewall Protection Profile that enforces AV and IPS configuration parameters.
FortiGate Clustering Protocol	A proprietary protocol used to exchange data to configure and synchronize the FortiGate units that form a High Availability cluster.
Local Console	A management console (may be a computer workstation or VT100 type terminal) connected directly to the TOE. It is located in the same physical location as the TOE and therefore is provided with the same physical protection as is provided for the TOE.
Network Management Station	A computer located remotely from the TOE but which is able to establish a network connection to the TOE. The Network Management Station falls outside the TOE Boundary.
Presumed Address	The TOE can make no claim as to the real address of any source or destination subject; the TOE can only suppose that these addresses are accurate. Therefore, a 'presumed address' is used to identify source and destination addresses.
Protection Profile	Both the Common Criteria and Fortinet use the term Protection Profile. Within this ST, the context generally makes it clear which usage is appropriate. However, for clarity, the CC usage is generally noted by the abbreviation PP while the Fortinet usage is always denoted by spelling out the complete term.

Table 16 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
ASIC	Application-specific Integrated Circuit
AV	Anti-Virus
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CTR	Counter-mode
DH	Diffie-Hellman
DoS	Denial of Service
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Protocol
FGCP	FortiGate Clustering Protocol
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability
HMAC	Keyed Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IFC	Integer Factorization Cryptography
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
Ipv4, Ipv6	Internet Protocol version 4, Internet Protocol version 6
IT	Information Technology
MIME	Multi-Purpose Internet Mail Extensions
MODP	Modular Exponential
NAT	Network Address Translation
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology

Acronym	Definition
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PoE	Power over Ethernet
POP3	Post-Office Protocol Version 3
PP	Common Criteria Protection Profile
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comments
ROBO	Remote Office and Branch Office
RSA	Rivest, Shamir and Adleman
RSASSA-PKCS1-v1_5	RSA Signature Scheme with Appendix PKCS1
SA	Security Association
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TDEA	Triple Data Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
URL	Universal Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

Table 17 – Acronyms

9 ANNEX A – FORTIGATE MODELS, GUIDES AND ENTROPY SOURCE

9.1 HARDWARE MODELS

Model	QuickStart/ Information Supplement/Security Guide/Security System Guide	ASIC	Entropy
FG-30E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	N/A	Token
FWF-30E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	N/A	Token
FG-40F	Guide: FortiGate/FortiWifi 40F & 60F Series QuickStart Guide File: FG-FWF-40F-60F-Series-QSG.pdf	CP9Xlite	CP9Xlite
FG-40F-3G4G	Guide: FortiGate/FortiWifi 40F & 60F Series QuickStart Guide File: FG-FWF-40F-60F-Series-QSG.pdf	CP9Xlite	CP9Xlite
FG-50E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	CP9lite	CP9lite
FWF-50E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	CP9lite	CP9lite
FG-51E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	CP9lite	CP9lite
FWF-51E	Guide: FortiGate/FortiWifi 30E/50E/51E Information Supplement File: FG-FWF-30E-50E-51E-Supplement.pdf	CP9lite	CP9lite
FG-52E	Guide: FortiGate 52E Information Supplement File: FG-52E-Supplement_-_BSMI.pdf	CP9lite	CP9lite
FG-60E	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9lite	CP9lite
FG-60E-DSL	Guide: FortiGate/FortiWifi 60E-DSL Information Supplement File: FG-FWF-60E-DSL.pdf	CP9lite	CP9lite
FG-60E-PoE	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9lite	CP9lite
FWF-60E	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9lite	CP9lite
FWF-60E-DSL	Guide: FortiGate/FortiWifi 60E-DSL Information Supplement File: FG-FWF-60E-DSL.pdf	CP9lite	CP9lite
FG-60F	Guide: FortiGate/FortiWifi 40F & 60F Series QuickStart Guide File: FG-FWF-40F-60F-Series-QSG.pdf	CP9Xlite	CP9Xlite
FG-60F-3G4G	Guide: FortiGate/FortiWifi 40F & 60F Series QuickStart Guide File: FG-FWF-40F-60F-Series-QSG.pdf	CP9Xlite	CP9Xlite
FG-61E	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9lite	CP9lite
FG-61F	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9Xlite	CP9Xlite
FWF-60F	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9Xlite	CP9Xlite

Model	QuickStart/ Information Supplement/Security Guide/Security System Guide	ASIC	Entropy
FWF-61E	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9lite	CP9lite
FWF-61F	Guide: FortiGate/FortiWifi 60E/61E Information Supplement File: FG-FWF-60E-61E-POE-Supplement.pdf	CP9Xlite	CP9Xlite
FG-80E	Guide: FortiGate 80E/81 Information Supplement File: FortiGate-80E-81E-Supplement.pdf	CP9lite	CP9lite
FG-80E-PoE	Guide: FortiGate 80E/81EPOE Information Supplement File: FortiGate-80E-81E-POE-Supplement.pdf	CP9lite	CP9lite
FG-81E	Guide: FortiGate 80E/81E Information Supplement File: FortiGate-80E-81E-Supplement.pdf	CP9lite	CP9lite
FG-81E-PoE	Guide: FortiGate 80E/81EPOE Information Supplement File: FortiGate-80E-81E-POE-Supplement.pdf	CP9lite	CP9lite
FG-100E	Guide: FortiGate 100E/101E Information Supplement File: FortiGate-100E-101E-Supplement_BSMI.pdf	CP9lite	CP9lite
FG-100EF	Guide: FortiGate 100EF Information Supplement File: FortiGate-100EF-Supplement_BSMI.pdf	CP9lite	CP9lite
FG-100F	Guide: FortiGate 100F/101F QuickStart Guide File: FG-100F-101F-QSG.pdf	CP9Xlite	CP9Xlite
FG-101E	Guide: FortiGate 100E/101E Information Supplement File: FortiGate-100E-101E-Supplement_BSMI.pdf	CP9lite	CP9lite
FG-101F	Guide: FortiGate 100F/101F QuickStart Guide File: FG-100F-101F-QSG.pdf	CP9Xlite	CP9Xlite
FG-140E	Guide: FortiGate 140E Series Information Supplement File: FortiGate-140E-Series-Supplement.pdf	CP9lite	CP9lite
FG-140E-PoE	Guide: FortiGate 140E Series Information Supplement File: FortiGate-140E-Series-Supplement.pdf	CP9lite	CP9lite
FG-200E	Guide: FortiGate 200E/201E Information Supplement File: FortiGate-200E-201E-Supplement-20190912.pdf	CP9	CP9
FG-201E	Guide: FortiGate 200E/201E Information Supplement File: FortiGate-200E-201E-Supplement-20190912.pdf	CP9	CP9
FG-300D	Guide: FortiGate 300D Information Supplement File: FortiGate-300D-Supplement-BSMI.pdf	CP8	Token
FG-300E	Guide: FortiGate 300E/301E Information Supplement File: FortiGate_300E-301E_Supplement.pdf	CP9	CP9
FG-301E	Guide: FortiGate 300E/301E Information Supplement File: FortiGate_300E-301E_Supplement.pdf	CP9	CP9
FG-400D	Guide: FortiGate 400D Information Supplement File: FortiGate-400D-Supplement-BSMI.pdf	CP8	Token
FG-400E	Guide: FortiGate 400E/401E Information Supplement File: FortiGate_400E-401E_Supplement-20190814-ONLINE.pdf	CP9	CP9
FG-401E	Guide: FortiGate 400E/401E Information Supplement File: FortiGate_400E-401E_Supplement-20190814-ONLINE.pdf	CP9	CP9
FG-500D	Guide: FortiGate 500D Information Supplement File: FG-500D-Supplement.pdf	CP8	Token

Model	QuickStart/ Information Supplement/Security Guide/Security System Guide	ASIC	Entropy
FG-500E	Guide: FortiGate 500E/501E Information Supplement File: FortiGate_500E-501E_Supplement.pdf	CP9	CP9
FG-501E	Guide: FortiGate 500E/501E Information Supplement File: FortiGate_500E-501E_Supplement.pdf	CP9	CP9
FG-600D	Guide: FortiGate 600D Information Supplement File: FortiGate-600D-Supplement_BSMI.pdf	CP8	Token
FG-600E	Guide: FortiGate 600E/601E Information Supplement File: FortiGate_600E-601E_Supplement-20190814-ONLINE.pdf	CP9	CP9
FG-601E	Guide: FortiGate 600E/601E Information Supplement File: FortiGate_600E-601E_Supplement-20190814-ONLINE.pdf	CP9	CP9
FG-900D	Guide: FortiGate 900D Information Supplement File: FortiGate-900D-Supplement.pdf	CP8	Token
FG-1000D	Guide: FortiGate 1000D Information Supplement File: FortiGate-1000D-Supplement.pdf	CP8	Token
FG-1100E	Guide: FortiGate 1100E/1101E AC DC Information Supplement File: FortiGate-1100E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-1100E-DC	Guide: FortiGate 1100E/1101E AC DC Information Supplement File: FortiGate-1100E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-1101E	Guide: FortiGate 1100E/1101E AC DC Information Supplement File: FortiGate-1100E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-1200D	Guide: FortiGate 1200D Information Supplement File: FortiGate-1200D-Supplement-ONLINE-20190613.pdf	CP8	Token
FG-1500D	Guide: FortiGate 1500D Information Supplement File: FortiGate-1500D-Supplement-20190715-ONLINE.pdf	CP8	Token
FG-1500DT	Guide: FortiGate 1500DT Information Supplement File: FortiGate-1500DT-Supplement-ONLINE-20190613.pdf	CP8	Token
FG-1500D-DC	Guide: FortiGate 1500D Information Supplement File: FortiGate-1500D-Supplement-20190715-ONLINE.pdf	CP8	Token
FG-2000E	Guide: FortiGate 2000E/2500E Information Supplement File: FortiGate-2000E-2500E-Supplement_BSMI.pdf	CP9	CP9
FG-2200E	Guide: FortiGate 2200E/2201E Information Supplement File: FortiGate_2200E_Series_Supplement.pdf	CP9	CP9
FG-2201E	Guide: FortiGate 2200E/2201E Information Supplement File: FortiGate_2200E_Series_Supplement.pdf	CP9	CP9
FG2500E	Guide: FortiGate 2000E/2500E Information Supplement File: FortiGate-2000E-2500E-Supplement_BSMI.pdf	CP9	CP9
FG-3000D	Guide: FortiGate 3000D Information Supplement File: FortiGate-3000D-Supplement-BSMI.pdf	CP8	Token
FG-3100D	Guide: FortiGate 3100D Information Supplement File: FortiGate-3100D-Supplement.pdf	CP8	Token
FG-3200D	Guide: FortiGate 3200D Information Supplement File: FortiGate-3200D-Supplement.pdf	CP8	Token
FG-3300E	Guide: FortiGate 3300E/3301E Information Supplement File: FortiGate_3300E_Series_Supplement.pdf	CP9	CP9

Model	QuickStart/ Information Supplement/Security Guide/Security System Guide	ASIC	Entropy
FG-3301E	Guide: FortiGate 3300E/3301E Information Supplement File: FortiGate_3300E_Series_Supplement.pdf	CP9	CP9
FG-3400E	Guide: FortiGate 3400E/3401E Series AC DC Information Supplement File: FortiGate-3400E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-3401E	Guide: FortiGate 3400E/3401E Series AC DC Information Supplement File: FortiGate-3400E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-3600E	Guide: FortiGate 3600E/3601E AC DC Information Supplement File: FortiGate-3600E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-3601E	Guide: FortiGate 3600E/3601E AC DC Information Supplement File: FortiGate-3600E-Series-ACDC-Supplement.pdf	CP9	CP9
FG-3700D	Guide: FortiGate 3700D Information Supplement File: FortiGate-3700D-Supplement.pdf	CP8	Token
FG-3800D	Guide: FortiGate 3800D Information Supplement File: FortiGate-3800D-Supplement-20190828-ONLINE.pdf	CP8	Token
FG-3810D	Guide: FortiGate 3810D Information Supplement File: FortiGate-3810D-M-Supplement_-_BSMI.pdf	CP8	Token
FG-3815D	Guide: FortiGate 3815D Information Supplement File: FortiGate-3815D-M-Supplement_-_BSMI.pdf	CP8	Token
FG-3960E	Guide: FortiGate 3960E/3980E Information Supplement File: FortiGate-3960E-3980E_Supplement.pdf	CP9	CP9
FG-3980E	Guide: FortiGate 3960E/3980E Information Supplement File: FortiGate-3960E-3980E_Supplement.pdf	CP9	CP9
FG-5001D	Guide: FortiGate-5001D Security System Guide File: FortiGate-5001D-security-system-guide.pdf	CP8	Token
FG-5001E	Guide: FortiGate-5001E and FortiGate-5001E1 Security System Guide File: FortiGate-5001E-security-system-guide.pdf	CP9	CP9
FG-5001E1	Guide: FortiGate-5001E and FortiGate-5001E1 Security System Guide File: FortiGate-5001E-security-system-guide.pdf	CP9	CP9
FG-6301F	Guide: FortiGate-6000F System Guide, FortiGate-6000F Series File: FortiGate-6000F-system-guide.pdf	CP9	CP9/Token
FG-6501F	Guide: FortiGate-6000F System Guide, FortiGate-6000F Series File: FortiGate-6000F-system-guide.pdf	CP9	CP9/Token
FGR-30D	Guide: FortiGate Rugged 30D Information Supplement File: FortiGateRugged-30D-Supplement-20190828-ONLINE.pdf	N/A	Token
FGR-60F	Guide: FortiGate Rugged 60F QuickStart Guide File: FGR-60F-QSG.pdf	CP9lite	CP9lite
FGR-60F-3G4G	Guide: FortiGate Rugged 60F QuickStart Guide File: FGR-60F-QSG.pdf	CP9lite	CP9lite

Table 18 - Hardware Models, Guides and Entropy Source

9.2 VIRTUAL MODELS

Model	Installation Guide	Entropy
FortiGate-VM00	Guide: FortiSandbox VM – Install Guide for VMware File: `FortiSandbox-3.1-VMware-VM-Install-Guide.pdf`	Token
FortiGate-VM01		
FortiGate-VM02		
FortiGate-VM04		
FortiGate-VM08		
FortiGate-VM16		
FortiGate-VM32		
FortiGate-VMUL		

Table 19 - Virtual Models, Guides and Entropy Source