Fortinet FortiGate™

Next Generation Firewalls and FortiOS 5.2 CC Compliant Firmware

SECURITY TARGET

Evaluation Assurance Level (EAL): EAL4+

Document No. 1918-002-D002
Version: 1.5
20 September 2016

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

Prepared by:

EWA - Canada, Ltd.
1223 Michael St., Suite 200
Ottawa, Ontario, Canada
K1J 7T2

Enabling a More Secure Future

CONTENTS

LIST OF FIGURES

LIST OF TABLES

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, Security Target Introduction, provides the ST reference, the TOE reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Protection Profiles (PPs).

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 operational environment.

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Fortinet FortiGate™ Next Generation Firewalls and FortiOS 5.2 CC Compliant Firmware Security Target
ST Version:	1.5
ST Date:	20 September 2016

1.3 TARGET OF EVALUATION REFERENCE

TOE Identification:	FortiGate™ Next Generation Firewalls and FortiOS 5.2.7 CC Compliant Firmware
TOE Developer:	Fortinet, Inc.

TOE Type: Boundary Protection Device

The TOE components identified in Table 1 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 firmware; however, the Virtual Machine (VM) models consist only of the FortiOS.

1.3.1 Firmware Build

The firmware build for all models is FortiOS 5.2.7 build number b718.

1.3.2 Hardware Models

There is typically one major hardware revision of each model. The hardware revision is identified by the HWID (Hardware Identification). The first six characters of the HWID identify the hardware model. There are an additional six characters not shown here. They are used internally by Fortinet to identify minor changes to the Bill of Materials (BOM) that do not impact the FIPS or CC functionality.

1.3.2.1 Desktop Models

Model	HWID	QuickStart Guide
FG-60D	C1AB28	FortiGate/FortiWiFi 60D Series QuickStart
		December 10, 2013 01-502-202499-20131
FGR-60D	C1AB57	FortiGate Rugged 60D QuickStart Guide
		June 3, 2014 01-506-236464-20140603
FWF-60D	C1AB32	FortiGate/FortiWiFi 60D Series QuickStart
		December 10, 2013 01-502-202499-20131
FG-92D	C1AC34	FortiGate/FortiWiFi 92D Information Supplement
		August 11, 2015
FWF-92D	C1AC33	FortiGate/FortiWiFi 92D Information Supplement
		August 11, 2015

Table 1 – TOE Identification of Desktop Models

1.3.2.2 1U Models

Model	Hardware Model	QuickStart Guide
FG-100D	C4LL40	FortiGate-100D Information Supplement
		August 20, 2015 01-522-209622-20150820

Model	Hardware Model	QuickStart Guide
FG-140D-PoE	C1AA77	FortiGate-140D/140D-POE/140D-POE-T1 Information Supplement
		June 28 2013 01-506- 190859-20160
FG-200D	C4KV72	FortiGate 200D QuickStart Guide
		April 01, 2014 01-501-190856-20140401
FG-300D	C1AB49	FortiGate 300D QuickStart Guide
		April 18, 2016 01-506-238488-20160418
FG-500D	C1AB51	FortiGate 500D Information Supplement
		June 27, 2014
FG-600D	C1AE11	FortiGate 600D Information Supplement
		August 11, 2015 01-523-278008-2015082
FG-900D	C1AC95	FortiGate 900D Information Supplement
		July 24, 2015 01-523-279315-2015072

Table 2 – TOE Identification of 1U Models

1.3.2.3 2U Models

Model	Hardware Model	QuickStart Guides
FG-1000D	C1AB95	FortiGate 1000D QuickStart Guide
		May 28, 2014 01-503-237227-20140528
FG-1200D	C1AC57	FortiGate 1200D QuickStart Guide
		July 28, 2014 01-520-247614-20140728
FG-1500D	C1AA64	FortiGate 1500D Information Supplement
		June 4, 2015 01-523-211767-20150604
FG-3200D	C1AC28	FortiGate 3200D Information Supplement
		June 30, 2015 01-522-256537-20150630

Table 3 – TOE Identification of 2U Models

1.3.2.4 3U Models

Model	Hardware Model	QuickStart Guides

Model	Hardware Model	QuickStart Guides
FG-3700D	C1AA92	FortiGate 3700D QuickStart Guide
		December 13, 2013 01-504-214838-20131213
FG-3815D	C1AE66	FortiGate 3815D Information Supplement
		January 21, 2016 01-540-292419-20151204-M

Table 4 – TOE Identification of 3U Models

1.3.2.5 Blade Models

The FortiGate 5000 series chassis are modular enclosures for blade systems. The following blade systems are capable of running in the evaluated configuration:

- FortiGate-5020 (2 Blade Slots)
- FortiGate-5060 (6 Blade Slots)
- FortiGate-5140B (14 Blade Slots)

The FortiGate series chassis requires one or more of the hardware blades shown in Table 5.

Model	Hardware Model	Security System Guides
FG-5001D	P1AB76	FortiGate 5001D Security System Guide
		01-500-0242101-20151109

Table 5 – TOE Identification of Blade Models

1.3.3 Virtual Models

The following model numbers are for the TOE software VMs:

Model	Installation Guide
FortiGate-VM00	FortiOS™ Handbook VM Installation for FortiOS 5.2.0 March 4, 2015 01-520-203906-20150304
FortiGate-VM08	
FortiGate-VM04	
FortiGate-VM02	
FortiGate-VM01	

Table 6 – TOE Identification of Virtual Models

Documentation for the FortiGate Series operated in Common Criteria mode consists of the standard FortiOS version 5.2 documentation set, a Federal Information Processing Standards –Common Criteria (FIPS-CC) specific technical note, and the relevant Quickstart, Security System or Installation Guide as shown in Tables 1 to 6.

1.4 TOE OVERVIEW

The TOE is 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, Virtual Local Area Network (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 NGFW firmware. Administration of the system may be performed locally using an administrator console, or remotely via a network management station. The FortiGate NGFW can operate either alone or as part of a cluster in order to provide high availability of services. Due to having different device drivers, the models offered in the FortiGate Series have their own unique firmware image created from the same firmware build. The different models in the series provide for increased performance and additional protected ports.

All CC-evaluated FortiGate NGFW employ Fortinet’s unique FortiASIC™ processor and the powerful, secure, FortiOS™ operating system to achieve breakthrough price/performance. 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. With the 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 supports the Internet Protocol Security (IPsec) industry standard for VPN, allowing VPNs to be configured between a FortiGate model and any client or gateway/firewall that supports IPsec VPN. The FortiGate series also provides Secure Sockets Layer (SSL) VPN services.

FortiGate's firewall, web filtering, VPN, antivirus and intrusion detection/prevention security functionality are within the scope of this evaluation. The antispam, content filtering and traffic shaping features are not included in this evaluation.

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 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 configuration requirements.

Table 7 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 text-based Local Console 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.
Alerts	The FortiGate provides alert emails that announce detected security policy violations.
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.
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.

Feature	Description
Authentication (FortiToken)	The FortiGate provides an option of using a FortiToken one-time password generator for remote administrator and user authentication.
Cryptography	The FortiGate incorporates a cryptographic module[1].
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 stored in memory, written to hard disk, or written to a FLASH memory card depending on the FortiGate model.

[1] Fortinet has verified the correctness of the implementation of the cryptographic support and is currently pursuing a FIPS 140-2 validation through the Cryptographic Module Validation Program.

Feature	Description
Protection Profile[2]	Protection profiles are used to configure anti-virus protection, and IPS.
Proxies	Firewall rules may be defined that are applicable only to users who have authenticated to the firewall in order to use a proxy service. The evaluated configuration supports user authentication for the File Transfer Protocol (FTP), HTTP and Telnet protocols.
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 7 – TOE Features

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

1.5.1.1 Physical Configuration

The FortiGate (see models listed in Tables 1 to 4) are stand-alone appliances that do not require supporting hardware. The FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C and FSW-5203B are Next Generation Firewall modules (blades) that may be installed in the FortiGate-5020, 5060 or 5140B chassis, each of which is capable of holding multiple blades. The chassis supports the blades by providing mounting, power and cooling fans only. As network and management interfaces are part of the blade itself, each blade acts as an independent Next Generation Firewall. The FortiGate-VM models in Table 6 are virtual machines.

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

Each series member of the FortiGate Next Generation Firewalls, termed a FortiGate unit, consists of custom hardware and firmware with the exception of the FortiGate-VM models. The FortiGate unit consists of the following major components: FortiOS FIPS-CC compliant firmware, processor, memory, FortiASIC™, and input/output interfaces.

All models share a common software platform. All hardware modes use one of Fortinet's proprietary ASIC (FortiASIC™) models to improve performance. The FortiASIC™ is a hardware device which provides cryptographic services to a FortiGate unit. The FortiASIC™ performs security and content processing. The FortiGate-VM models consist of software only and are supported by VMware Servers.

1.5.1.2 Network Interfaces

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

- A dedicated console port is available on all models. The port is RS232 with either a DB-9 or RJ-45 connector. When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiGate unit via the CLI. This Local Console CLI 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. When connected to a Network Management Station, this port provides remote access to the Network Web-Based GUI and allows an authorized administrator to configure the FortiGate Unit, monitor its operation, and examine the audit logs that are created.
- All models are equipped with a Universal Serial Bus (USB) port that may be used by an authorized administrator to use the Fortinet token hardware entropy source. This is required for FIPS mode operation.
- On all models, an authorized administrator may configure logging information to be sent to a FortiAnalyzer unit.
- On all models, an authorized administrator may configure automatic Anti-Virus and Intrusion Prevention System (IPS) updates from the FortiGuard Distribution Server.

The 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.

1.5.1.3 TOE Boundary - 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. It also provides access to the FortiAnalyzer Server, which collects and analyzes logging information.

The Local Console, located within a Secure Area, is a terminal or general purpose computer with a standard serial interface and optional Ethernet interfaces. A serial port is required to administer the TOE via the Local Console CLI.

The Network Management Station is a terminal or general purpose computer with a standard network interface used to administer the TOE remotely using the Network Web-based GUI.

Note that the Fortinet FortiASIC CP7 Cryptographic Library and the Fortinet FortiASIC CP8 Cryptographic Library are considered to be in the operational environment.

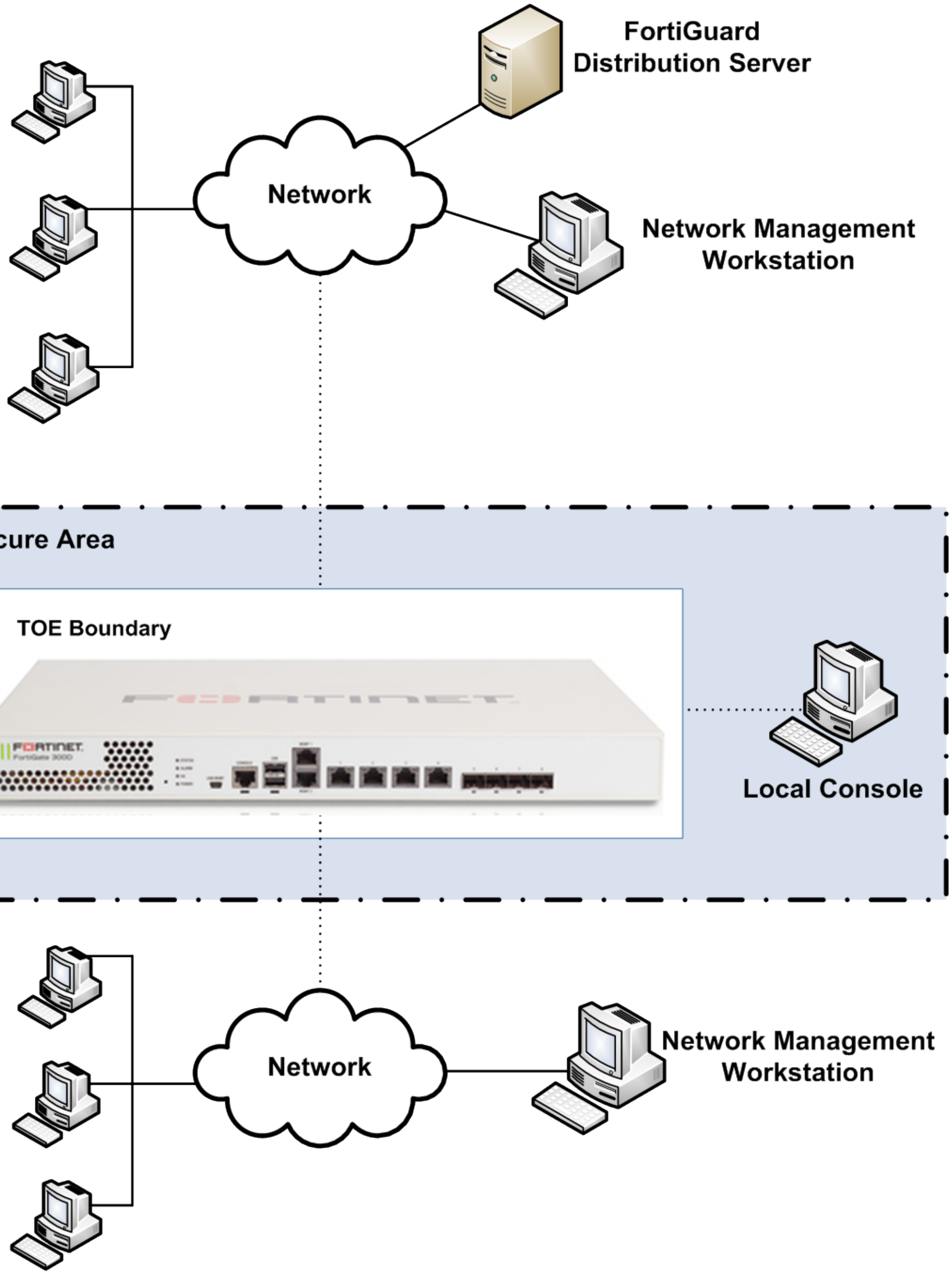

Figure 1 – Single-Unit FortiGate Next Generation Firewall Network Configuration

1.5.1.4 TOE Boundary - 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 three 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, and a FortiAnalyzer Server, which collects and analyzes logging information.

The Local Console, located within a Secure Area, is a terminal or general purpose computer with a standard serial interface and optional Ethernet interfaces. A serial port is required to administer the TOE via the Local Console CLI.

The Network Management Station is a terminal or general purpose computer with a standard network interface to administer the TOE remotely using the Network Web-based GUI.

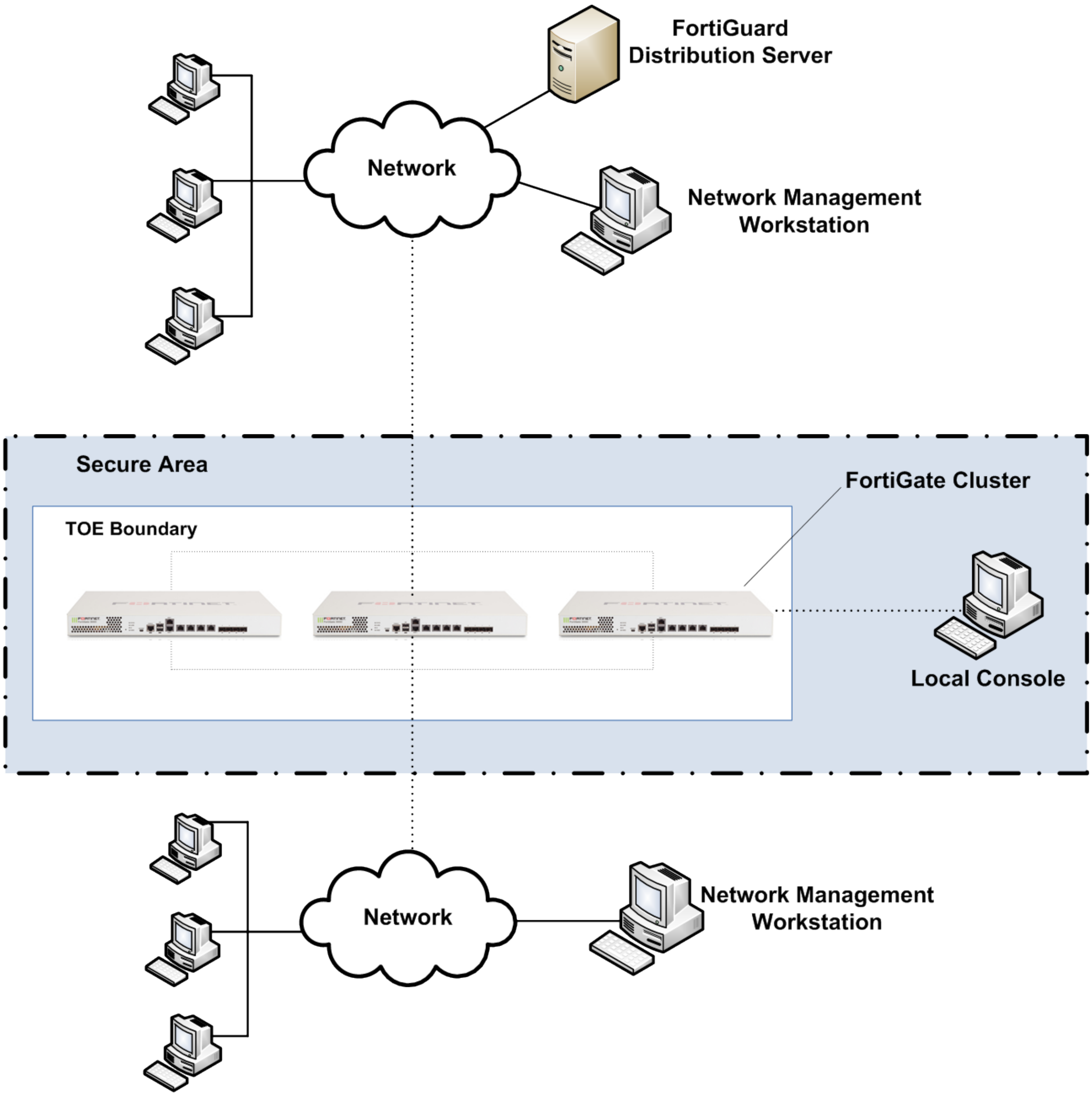

Figure 2 – High Availability FortiGate Next Generation Firewall Configuration

1.5.1.5 TOE Environment

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

Non-TOE Component	Hardware/Software Requirements
Local Management Workstation	General purpose computing platform
Remote Management Workstation	General purpose computing platform that supports the following: • Internet Explorer 11 • Transport Layer Security (TLS) (for GUI)
FortiGuard Distribution Server	Network access to a FortiGuard Distribution Server
VMware Server (for FortiGate VM models only)	VMware ESXi Server 5.5
Fortinet Entropy Token	Fortinet Entropy Token hardware

Table 8 – Non-TOE Hardware and Software

1.5.1.6 TOE Guidance Documentation

All guidance is publicly available at http://docs.fortinet.com. The following guidance documentation is an integral part of the TOE:

QuickStart, Security System and Installation Guides	The guides for hardware devices other than the hardware blades are 'Quickstart' guides; the guides for the hardware blades are called 'Security System Guides'. A list of quickstart and security system guides is provided in Tables 1 to 5. An installation guide is provided for the VM models and is referenced in Table 6.
FortiOS Guide	FortiOS Handbook Version 5.2.7

Table 9 – TOE Guidance Documentation

1.5.1.7 Features Supported but Not Included in the Evaluated Configuration

The following features were not included in the evaluated configuration of the TOE:

- The FortiGate unit is able to send log information to external log servers including FortiAnalyzer server, File Transfer Protocol (FTP), Syslog Server or Trivial File Transfer Protocol (TFTP).
- Fortinet FortiManager may be used to provide centralized management of multiple FortiGate devices.

1.5.2 Logical Scope

The logical scope of the TOE may be broken down by the security function classes. The following breakdown provides the description of the security features of the TOE, and loosely follows the security functional classes described in Section 5.1 and Section 6.2.

1.5.2.1 Security Audit

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

1.5.2.2 Cryptographic Support

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

1.5.2.3 User Data Protection

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

1.5.2.4 Identification and Authentication

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

1.5.2.5 Security Management

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

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

The terms ‘administrator’ and ‘authorized administrator’ are used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required.

1.5.2.6 Protection of the TOE Security Functionality (TSF)

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

1.5.2.7 Trusted Path / Channels

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

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

1.5.2.8 IPS Functionality

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

1.5.2.9 Anti-Virus Functionality

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

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4, September 2012.

This ST contains functional requirements based upon functional components in CC Part 2 as well as a number of extended security functional requirements. Therefore, the TOE is conformant with CC Part 2 extended.

The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 4, augmented with ALC_FLR.3 – Systematic Flaw Remediation.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

Conformance to a PP is not claimed in this ST.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS, POLICIES, AND ASSUMPTIONS

3.1.1 Threats

The threats discussed below are 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.

Threat ID	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 and reviewed, thus allowing an attacker to escape detection.
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information.
T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.

Table 10 – Security Threats

3.1.2 Organizational Security Policies

The TOE must address the organizational security policies described in Table 11.

Policy ID	Security Description
P.ACCACT	Users of the TOE shall be accountable for their actions.
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected.
P.MANAGE	The TOE shall be manageable only by authorized administrators.

Table 11 – Organizational Security Policies

3.1.3 Assumptions

The following specific conditions are assumed to exist in the TOE environment.

Assumption ID	Assumption Description
A.LOCATE	The TOE hardware and software 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 12 – TOE Environment Assumptions

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operational Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). The mapping of security objectives to assumptions, threats and organizational security policies along with the rationale for this mapping is found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE.

Objective ID	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 and view a readable audit trail of security-related events, with accurate dates and times.
O.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, or between TOE devices using cryptographic functions.
O.IDAUTH	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.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROTCT	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.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.
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 13 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

Objective ID	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.PHYCAL	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 14 – 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.MEDIAT	T.NOAUTH	T.NOHALT	T.PRIVIL	T.PROCOM	T.REPLAY	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.ENCRYP					X			X								
O.IDAUTH			X		X	X	X				X		X			
O.MEDIAT	X			X												
O.PROTCT			X			X	X						X			
O.REUSE									X							
O.TIME											X	X				
O.VIRUS										X						
OE.ADMIN													X		X	
OE.PHYCAL														X		
OE.SINGEN																X

Table 15 – Mapping Between Objectives and Threats, Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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.MEDIAT	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.MEDIAT 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 and reviewed, 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 and view a readable audit trail of security-related events, with accurate dates and times.
Rationale:	O.ADMIN provides for security management functionality, including the functionality for reviewing the audit trail. 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.IDAUTH	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.PROTCT	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.IDAUTH 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.PROTCT objective addresses this threat by providing TOE self-protection.	

Threat: T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.	
Objectives:	O.MEDIAT	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.MEDIAT 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.ENCRYP	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, or between TOE devices using cryptographic functions.
	O.IDAUTH	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.IDAUTH requires that users be uniquely identified before accessing the TOE. O.ENCRYP ensures the confidentiality and integrity a data passed between the TOE and the authorized administrator for management purposes.

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.IDAUTH	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.PROTCT	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.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by requiring the TOE to protect itself against bypass, or to deny access to legitimate users.	

Threat: T.PRIVIL	An unauthorized user may 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.IDAUTH	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.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.

Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT 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.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
Rationale:	O.ENCRYP requires that an authorized administrator uses encryption when performing administrative functions on the TOE remotely.	

Threat: T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information.	
Objectives:	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.
Rationale:	The O.REUSE objective ensures that the TOE provides a means to prevent the reuse of authentication data, providing a means to mitigate the threat of a user replaying authentication information.	

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 Policies

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 and view a readable audit trail of security-related events, with accurate dates and times.
	O.IDAUTH	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.IDAUTH 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 and view a readable 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.IDAUTH	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.PROTCT	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.IDAUTH supports this policy by ensuring that administrators must be identified and authenticated prior to being granted access to TOE security management functions. O.PROTCT 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

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

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

This section specifies the extended Security Functional Requirements (SFR)s used in this ST.

5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 16 identifies all extended SFRs implemented by the TOE.

Name	Description
FAV_ACT_EXT.1	Anti-Virus action requirements
FIP_DOS_EXT.1	Denial of service
FIP_SIG_EXT.1	Signature protection

Table 16 – Extended TOE Security Functional Requirements

5.1.1 Anti-Virus Action Requirements (FAV)

5.1.1.1 FAV_ACT_EXT.1

This extended requirement was explicitly created because the CC does not provide a means to specify Anti-Virus detection and blocking capabilities. A new class is explicitly created and it has a family of FAV_ACT_EXT. The Anti-Virus class and family were modelled after FPT_PHP TSF physical protection, and FAV_ACT_EXT.1 was loosely modelled after FPT_PHP.1 Passive detection of physical attack. Component levelling is shown in Figure 3.

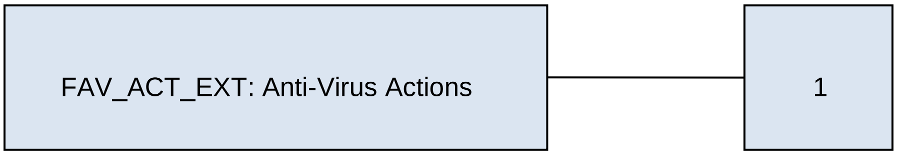

Figure 3 – FAV_ACT_EXT Component Levelling

Management: FAV_ACT_EXT.1

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

- The management of actions on the information flow when virus is detected;
- The management of actions on virus signatures.

Audit: FAV_ACT_EXT.1

The following actions should be auditable:

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

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.

5.1.2 Intrusion Prevention (IPS) Class

A class of FIP requirements was created to address the intrusion prevention functionality provided by the TOE. The FPT Protection of the TSF class 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 and FIP_SIG. These requirements have no dependencies; the stated requirements embody all the necessary security functions. Component levelling is shown in Figure 4.

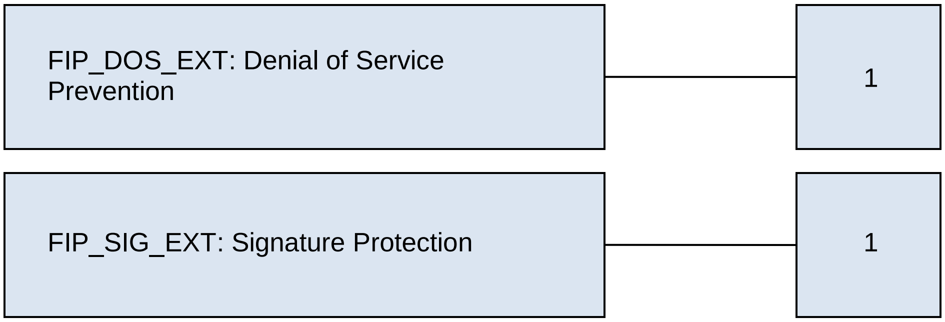
FIP_DOS_EXT: Denial of Service Prevention
1
FIP_SIG_EXT: Signature Protection
1

Figure 4 – IPS Component Levelling

5.1.2.1 FIP_DOS_EXT Denial of Service

Management: FIP_DOS_EXT.1

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

- Configuration of DoS policy.

Audit: FIP_DOS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Detection of a possible DoS attack.

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.

5.1.2.2 FIP_ SIG_EXT.1 Signature Protection

Management: FIP_SIG_EXT.1

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

- Configuration of IPS policies
- Update of IPS signatures

Audit: FIP_SIG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Detection of a possible attack incident
- Basic: Update of the signature protection file.

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.

5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS

There are no extended TOE Security Assurance components associated with this evaluation.

6 SECURITY REQUIREMENTS

This section provides the 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 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]. To improve readability selections of [none] are generally not shown.
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability, assignments of [*none*] may not be shown.
- Refinement: Refined components are identified by using **bold** 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 TOE 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.

Component	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
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
FDP_IFC.1(1)	Subset information flow control (unauthenticated policy)
FDP_IFC.1(2)	Subset information flow control (authenticated policy)

Component	Description
FDP_IFC.1(3)	Subset information flow control (VPN policy)
FDP_IFC.1(4)	Subset information flow control (web filtering policy)
FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)
FDP_IFF.1(2)	Simple security attributes (authenticated policy)
FDP_IFF.1(3)	Simple security attributes (VPN policy)
FDP_IFF.1(4)	Simple security attributes (web filtering policy)
FIA_AFL.1	Authentication failure handling
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_MOF.1	Management of security functions behaviour (IPS Functions)
FMT_MSA.1(1)	Management of security attributes (Unauthenticated SFP)
FMT_MSA.1(2)	Management of security attributes (Authenticated SFP)
FMT_MSA.1(3)	Management of security attributes (VPN)
FMT_MSA.1(4)	Management of security attributes (Web Filtering)
FMT_MSA.3(1)	Static attribute initialisation (authenticated, unauthenticated, VPN)
FMT_MSA.3(2)	Static attribute initialisation (Web filtering)
FMT_SMF.1	Specification of management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_STM.1	Reliable time stamps
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path
FIP_DOS_EXT.1	Denial of service
FIP_SIG_EXT.1	Signature protection
FAV_ACT_EXT.1	Anti-virus actions

Table 17 – 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 [minimum] level of audit; and

c) [*All auditable events listed in Table 18*].

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, 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 ST, [*information specified in Table 18*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAR.1	Reading of information from the audit records (Opening the audit trail)	The identity of the administrator performing the function
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	The identity of the administrator attempting the function

FCS_CKM.1(1)
FCS_CKM.1(2)
	Success or failure of the activity	

FCS_CKM.4	Failure of the key zeroization	
FCS_COP.1	Failure of the cryptographic operation	

FDP_IFF.1(1)
FDP_IFF.1(2)
FDP_IFF.1(3)
FDP_IFF.1(4)
	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

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2	All uses of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	User identity
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)
FMT_MSA.1(3)
FMT_MSA.1(4)
	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 the TSF	
FPT_STM.1	Changes to the time	The identity of the administrator performing the operation
FTP_ITC.1	Failure of the trusted channel functions	Identification of the initiator and target of the failed trusted channel functions
FTP_TRP.1	Failure of the trusted path functions	Identification of the claimed user identity
FAV_ACT_EXT	Actions taken on the information flow when virus is detected	

Requirement	Auditable Events	Additional Audit Record Contents
FIP_DOS_EXT.1	Detection of a potential Denial of Service	
FIP_SIG_EXT.1	Triggering of a match to a known signature	

Table 18 – 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.

6.2.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorized administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.2 Restricted Audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

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_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 (AES)*] and specified cryptographic key sizes [*listed in Table 19*] that meet the following: [*NIST Special Publication 800-90A*].

Key Usage	Key Size
AES	128, 192 or 256

Table 19 – Cryptographic Key Generation

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

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1(2).1 The TSF shall generate **asymmetric** 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 186-3 Appendix B*].

6.2.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: 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 PUB 140-2 Cryptographic Key Management Security Level 1*].

6.2.2.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key generation
FCS_CKM.1 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in Table 20*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 20*] and cryptographic key sizes [*cryptographic key sizes specified in Table 20*] that meet the following: [*standards listed in Table 20*].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Encryption and Decryption of remote administrator sessions, between devices in HA configuration	AES (Advanced Encryption Standard in CBC mode)	128, 192, 256	FIPS PUB 197 (AES) and National Institute of Standards and Technology (NIST) SP 800-38A (CBC mode)	3964, 3965, 3966

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Encryption and Decryption in support of the VPN policy	AES (operating in CBC mode for IPsec and SSL)	128, 192, and 256 for AES	FIPS PUB 197 (AES) and National Institute of Standards and Technology (NIST) SP 800-38A (CBC mode)	3963
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS1 using SHA-256)	2048, 3072	PKCS #1 v. 2.1	2024, 2025, 2026
Hashing	SHA-1	160	FIPS PUB 180-3	3267, 3268, 3269, 3270
	SHA-256	256	FIPS PUB 180-3	3267, 3268, 3269, 3270
Keyed Hash	HMAC-SHA-1	160 key 160 digest	FIPS PUB 198	2581, 2582, 2583, 2584
	HMAC-SHA-256	256 key 256 digest	FIPS PUB 198	2581, 2582, 2583, 2584

Table 20 – Cryptographic Operation

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1(1) Subset information flow control (unauthenticated policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(1).1 The TSF shall enforce the [*Unauthenticated Information Flow SFP*] on:
[*Subjects: unauthenticated users and IT entities*[3]*;*
Information: network traffic[4]*;*
Operations: pass information].

6.2.3.2 FDP_IFC.1(2) Subset information flow control (authenticated policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(2).1 The TSF shall enforce the [*Authenticated Information Flow SFP*] on:
[*Subjects: authenticated users and IT entities;*
Information: FTP and Telnet traffic; and
Operations: initiate service and pass information].

6.2.3.3 FDP_IFC.1(3) Subset information flow control (VPN policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(3).1 The TSF shall enforce the [*VPN SFP*] on:
[*Subjects: TOE interfaces*
Information: network packets
Operation: IPsec operations].

6.2.3.4 FDP_IFC.1(4) Subset information flow control (web filtering policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(4).1 The TSF shall enforce the [*Web Filtering SFP*] on:

[*Subjects: users*
Information: web pages
Operation: HTTP and HTTPS].

6.2.3.5 FDP_IFF.1(1) Simple security attributes (unauthenticated policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

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

[3] unauthenticated users and IT entities that send and receive information through the TOE to one another

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

[*Subjects: unauthenticated users and external entities*

Subject security attributes: presumed address

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(1).2 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(1).3 The TSF shall ~~enforce the~~ **ensure that** [*an authorized administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied*].

FDP_IFF.1(1).4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1(1).5 The TSF shall explicitly deny an information flow based on the following rules:

[*none*].

6.2.3.6 FDP_IFF.1(2) Simple security attributes (authenticated policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1(2).1 The TSF shall enforce the [*Authenticated Information Flow SFP*] based on the following types of subject and information security attributes:

[*Subjects: authenticated users and IT entities*
Subject security attributes:

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

Information: FTP and Telnet traffic
Information security attributes:

- *presumed address of source subject;*
- *presumed address of destination subject;*
- *TOE interface on which traffic arrives and departs;*
- *service (i.e. FTP and Telnet);*

- *schedule*].

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:

[*Subjects can cause information to flow through the TOE to another connected network if:*

- *the subject is authenticated;*
- *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(2).3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1(2).4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1(2).5 The TSF shall explicitly deny an information flow based on the following rules:

[*the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., Request for Comments (RFC)). This shall be accomplished through protocol filtering proxies that are designed for that purpose*].

6.2.3.7 FDP_IFF.1(3) Simple security attributes (VPN policy)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1(3).1 The TSF shall enforce the [*VPN SFP*] based on the following types of subject and information security attributes:

[*Subjects: TOE Interfaces*

Security attributes:

- *set of source subject identifiers.*
- *set of destination subject identifiers.*

Information: network packets

Security attributes:

- *presumed identity of source subject; and*
- *identity of destination subject.*]

FDP_IFF.1(3).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 presumed identity of the source subject is in the set of source subject identifiers*;

b. the identity of the destination subject is in the set of source destination identifiers;

c. the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy *ruleset defined by an authorized administrator) according to the first match algorithm; and*

d. the selected information flow policy rule specifies that the information flow is to be permitted, and which SSL or IPsec operation is to be applied to that information flow].

FDP_IFF.1(3).3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1(3).4 The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1(3).5 The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;*

b) *The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;*

c) *The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier*].

6.2.3.8 FDP_IFF.1(4) Simple security attributes (web filtering policy)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1(4).1 The TSF shall enforce the [*Web Filtering SFP*] based on the following types of subject and information security attributes: [

Subjects: human users

Security attributes:

- *optional user ID*
- *optional user group*

Information: web pages

Security attributes:

- *URL;*
- *category assigned by FortiGuard web filtering service based on the website content; and*
- *category group assigned by FortiGuard web filtering service; and*
- *classification assigned by FortiGuard web filtering service based on the characteristics of the site, if applicable;*
- *local category, if applicable;*
- *override, if applicable.*]

FDP_IFF.1(4).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, category group and classification to which the URL has been assigned by the FortiGuard web filtering service is set to 'allow'; or*
b) *The local category, if used, is set to 'allow'*].

FDP_IFF.1(4).3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1(4).4 The TSF shall explicitly authorise an information flow based on the following rules:

[*An override has been set for the URL*].

FDP_IFF.1(4).5 The TSF shall explicitly deny an information flow based on the following rules:

[*The authenticated user has reached the daily quota for this category, category group or classification*].

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. Category groups are similar categories grouped together for ease of administration. A classification is assigned based on the characteristics of the site rather than the site content. For example, the cached content classification indicates that the site caches content, but provides no indication of the content type. Not every URL has an assigned classification. A quota is a time limit placed on viewing URLs assigned to a particular category, category group or classification.

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*] of 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 account for a configurable period of time*].

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.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [*authentication attempts from either an internal or external network by*

a) authorized administrators;

b) authorized users].

Application Note: The single use authentication functionality is provided by the FortiToken device.

6.2.4.5 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 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 [*following rules:*

a) administrators authenticate to the console via username and password;

b) a one time passcode generator may be used to authenticate administrators to the CLI or web management interface;

c) a one time passcode generator may be used to authenticate users in support of the authenticated information flow SFP; and

d) X.509 certificates are used to authenticate VPN peers in support of the VPN SFP].

6.2.4.6 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 (IPS Functions)

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 (Unauthenticated SFP)

Hierarchical to: No other components.

Dependencies: 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 [*Unauthenticated SFP*] to restrict the ability to [*delete attributes from a rule, modify attributes in a rule, add attributes to a rule*] the security attributes [*source address, destination address, service, schedule*] to [*the authorized administrator*].

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

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(2).1 The TSF shall enforce the [*Authenticated 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*].

6.2.5.4 FMT_MSA.1(3) Management of security attributes (VPN)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(3).1 The TSF shall enforce the [*VPN SFP*] to restrict the ability to [query, modify, delete] the security attributes [*source and destination subject identifiers*] to [*the authorized administrator*].

6.2.5.5 FMT_MSA.1(4) Management of security attributes (Web Filtering)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(4).1 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, category group, classification and override setting*] to [*the authorized administrator*].

6.2.5.6 FMT_MSA.3(1) Static attribute initialisation (Authenticated SFP, Unauthenticated SFP, VPN)

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 [*Unauthenticated SFP, Authenticated SFP and VPN 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) and FDP_IFF.1 (2) 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.

6.2.5.7 FMT_MSA.3(2) Static attribute initialisation (Web Filtering)

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.

6.2.5.8 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 unauthenticated and authenticated information flow rules;

b) *administer web filtering functionality;*

c) *administer VPN rules, including those related to cryptographic functionality;*

d) *administer security audit functionality;*

d) *administer user account information;*

e) *administer authentication mechanisms and authentication failure handling policy;*

f) *review and delete audit logs; and*

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

6.2.5.9 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 role~~s~~.

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*].

6.2.7.2 FTP_TRP 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].

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 REQUIREMENTS RATIONALE

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

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.PROTCT	O.REUSE	O.TIME	O.VIRUS
FAU_GEN.1			X							
FAU_GEN.2			X							
FAU_SAR.1	X	X	X							
FAU_SAR.2	X		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_IFC.1(3)						X				
FDP_IFC.1(4)						X				
FDP_IFF.1(1)						X				
FDP_IFF.1(2)						X				
FDP_IFF.1(3)						X				
FDP_IFF.1(4)						X				
FIA_AFL.1							X			
FIA_ATD.1					X					
FIA_UAU.2	X				X			X		
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			

	O.ACCESS	O.ADMIN	O.AUDIT	O.ENCRYP	O.IDAUTH	O.MEDIAT	O.PROTCT	O.REUSE	O.TIME	O.VIRUS
FMT_MSA.1(3)	X	X					X			
FMT_MSA.1(4)	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	X			
FIP_SIG_EXT.1	X					X	X			
FAV_ACT_EXT.1						X				X

Table 21 – Mapping of SFRs to Security Objectives

6.3.1 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:	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MOF.1	Management of functions in TSF
	FMT_MSA.1(1)	Management of security attributes (unauthenticated policy)
	FMT_MSA.1(2)	Management of security attributes (authenticated policy)
	FMT_MSA.1(3)	Management of security attributes (VPN

		policy)
	FMT_MSA.1(4)	Management of security attributes (web filtering policy)
	FIP_DOS_EXT.1	Denial of service
	FIP_SIG_EXT.2	Signature protection
Rationale:	FAU_SAR.1 and FAU_SAR.2 meet this objective by ensuring that only authorized administrators are able to access and read audit records. 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, 2, 3 and 4) ensure that only authorized administrators have access to the security attributes associated with the information flow security function policies. FIP_DOS_EXT.1 restricts the modification and configuration of DoS policies to authorized administrators. FIP_SIG_EXT.1 restricts the modification and configuration of IPS policies and IPS signature updates to authorized administrators.	

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:	FAU_SAR.1	Audit review
	FMT_MOF.1	Management of security functions behaviour (IPS Functions)
	FMT_MSA.1(1)	Management of security attributes (Unauthenticated SFP)
	FMT_MSA.1(2)	Management of security attributes (Authenticated SFP)
	FMT_MSA.1(3)	Management of security attributes (VPN)
	FMT_MSA.1(4)	Management of security attributes (Web Filtering)
	FMT_MSA.3(1)	Static attribute initialisation
	FMT_MSA.3(2)	Static attribute initialisation (web filtering)

	FMT_SMF.1	Specification of Management Functions
Rationale:	FAU_SAR.1 meets this objective by providing authorized administrators with the ability to read audit logs. 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(1,2,3 and 4) meets the objective by providing the functionality to manage the parameters associated with the information flow control security functional policies. FMT_MSA.3(1,2) meets the objective by providing the initial values required to manage the information flow control 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 and view a readable 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
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
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. FAU_SAR.1 provides the means to read the audit information, while FAU_SAR.2 ensures that only those specifically granted access may read the logs.	

Objective: **O.ENCRYP**	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, 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 that cryptography between the TOE devices, and between the TOE and the remote administrator.	

Objective: O.IDAUTH	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.MEDIAT	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 (unauthenticated policy)
	FDP_IFC.1(2)	Subset information flow control (authenticated policy)
	FDP_IFC.1(3)	Subset information flow control (VPN Policy)

	FDP_IFC.1(4)	Subset information flow control (Web Filtering)
	FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)
	FDP_IFF.1(2)	Simple security attributes (authenticated policy)
	FDP_IFF.1(3)	Simple security attributes (VPN policy)
	FDP_IFF.1(4)	Simple security attributes (web filtering policy)
	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 unauthenticated information flow 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 authenticated information flow policy. FDP_IFC.1(3) and FDP_IFF.1(3) support the objective by detailing how the TOE mediates the flow of information for the VPN policy. FDP_IFC.1(4) and FDP_IFF.1(4) 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.PROTCT	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 (IPS Functions)
	FMT_MSA.1(1)	Management of security attributes (Unauthenticated SFP)
	FMT_MSA.1(2)	Management of security attributes

		(Authenticated SFP)
	FMT_MSA.1(3)	Management of security attributes (VPN)
	FMT_MSA.1(4)	Management of security attributes (Web Filtering)
	FMT_MSA.3(1)	Static attribute initialisation
	FMT_MSA.3(2)	Static attribute initialisation (web filtering)
	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.1(3), FMT_MSA.1(4), 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 a 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.	
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
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 access.	

Objective:	The TOE shall provide reliable time stamps.

O.TIME		
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 DEPENDENCY RATIONALE

Table 22 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	Dependencies	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	Yes	
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.2	FAU_SAR.1	Yes	
FCS_CKM.1(1)	FCS_COP.1 FCS_CKM.4	Yes	
FCS_CKM.1(2)	FCS_COP.1 FCS_CKM.4	Yes	
FCS_CKM.4	FCS_CKM.1	Yes	
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Yes	
FDP_IFC.1(1)	FDP_IFF.1	Yes	
FDP_IFC.1(2)	FDP_IFF.1	Yes	

SFR	Dependencies	Dependency Satisfied	Rationale
FDP_IFC.1(3)	FDP_IFF.1	Yes	
FDP_IFC.1(4)	FDP_IFF.1	Yes	
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Yes	
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Yes	
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	Yes	
FDP_IFF.1(4)	FDP_IFC.1 FMT_MSA.3	Yes	
FIA_AFL.1	FIA_UAU.1	Yes	FIA_UAU.2 is hierarchical to FIA_UAU.1; therefore this dependency has been satisfied.
FIA_ATD.1	None	Yes	
FIA_UAU.2	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency has been satisfied.
FIA_UAU.4	None	Yes	
FIA_UAU.5	None	Yes	
FIA_UID.2	None	Yes	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes	
FMT_MSA.1(1)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	
FMT_MSA.1(2)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	
FMT_MSA.1(3)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	
FMT_MSA.1(4)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	Yes	

SFR	Dependencies	Dependency Satisfied	Rationale
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	Yes	
FMT_SMF.1	None	Yes	
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency has been satisfied.
FPT_FLS.1	None	Yes	
FPT_STM.1	None	Yes	
FTP_ITC.1	None	Yes	
FTP_TRP.1	None	Yes	
FAV_ACT_EXT.1	None	Yes	
FIP_DOS_EXT.1	None	Yes	
FIP_SIG_EXT.1	None	Yes	

Table 22 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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 current Fortinet flaw remediation practices and procedures meet or exceed this level of assurance.

The assurance requirements are summarized in Table 23.

Assurance Class	Assurance Components	
	Identifier	Name
Development	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_OPE.1	Operational user guidance

Assurance Class	Assurance Components	
	Identifier	Name
	AGD_PRE.1	Preparative procedures
Life-cycle support	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
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objective
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	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_VAN.3	Focused vulnerability analysis

Table 23 – Security Assurance Requirements

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 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 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.

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

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

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

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

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

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

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

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

7.1.2 Cryptographic Support

The cryptographic libraries used by the TOE are listed in Table 24.

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

Table 24 – Cryptographic Libraries

Fortinet has verified the correctness of the implementation of the cryptographic support to fulfil the requirements stated in Section 6.2.2.

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

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

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

Cryptographic operations are performed in accordance with the detail provided in Table 20. Note that the Fortinet FortiASIC CP7 Cryptographic Library and the Fortinet FortiASIC CP8 Cryptographic Library are considered to be in the operational environment.

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

7.1.3 User Data Protection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

If the request is an HTTP or HTTPS, the URL may be checked against the FortiGuard Web Filtering Policy. FortiGuard Web Filtering is made up of an external service which provides category, category group and classification information for any requested website, and an internal policy that applies that information. When FortiGuard Web Filter is enabled in a web filter profile, the setting is applied to all

[5] Modular Exponential

firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the TOE provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

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

1. Local IPS Anomaly protection (kernel level);
2. Firewall flow control policy enforcement: First matched policy must explicitly allow traffic to flow;
3. Authenticated flow control policies: If configured for flow-control policy, successful authentication is required for traffic to flow; and
4. Protection Profile services (if explicitly enabled):
    a. Scheduling: If scheduling is enabled, time period must be explicitly allowed,
    b. SMTP Commands: All SMTP commands permitted unless explicitly denied,
    c. MIME Types: All MIME types permitted unless explicitly denied,
    d. FTP Sub-Commands: All FTP sub-commands permitted unless explicitly denied,
    e. HTTP Request Methods: All HTTP request methods permitted unless explicitly denied,
    f. FortiGuard Web Filter: All URL requests are checked against the web filter policy to determine if they are allowed or blocked.
    g. Virus protection: If content is matched against an Anti-Virus (AV) signature, the configured action is performed, and
    h. IPS Signature matching: If the nature of the connection or content is matched against an IPS signature, the configured action is performed.

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

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

TOE Security Functional Requirements addressed: FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFC.1(4), FDP_IFF.1(1), FDP_IFF.1(2), FDP_IFF.1(3), FDP_IFF.1(4), FMT_MSA.3(1), FMT_MSA.3(2).

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

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

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UID.2.

7.1.5 Security Management

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

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

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

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

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_SMF.1, FMT_SMR.1.

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

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

7.1.7 Trusted Path/Channel

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

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

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

TLS_RSA_WITH_AES_128_CBC_SHA (RFC 4346)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC 5246)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (RFC 5246)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (RFC 4346, RFC 5246)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (RFC 4346, RFC 5246)

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

- The server sends the 2048-bit RSA public certificate

- The server generates, signs (RSA PKCS#1) and sends DH parameters and the DH public value
- The client generates and sends the DH public value. The keying material is then used to encrypt/decrypt (using AES128 or AES256) and authenticate (using HMAC-SHA1 or HMAC-SHA256) the data exchange.

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

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

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

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

7.1.8 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 is allowed to pass based on the information flow policy (based on the Fortinet Protection Profile), it is examined against IPS signatures known to indicate potential attacks. If evidence of an attack is found, the TOE records the event in the IPS or packet logs. These logs are made available only to authorized administrators, and is provided in a manner suitable for the administrators to interpret the information.

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

7.1.9 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. Although the Local Console falls outside the TOE Boundary 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 25 - 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
BOM	Bill of Materials
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
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
HWID	Hardware Identification
IDS	Intrusion Detection System
IFC	Integer Factorization Cryptography
IKE	Internet Key Exchange

Acronym	Definition
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
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	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
SSL	Secure Sockets Layer
ST	Security Target

Acronym	Definition
TDEA	Triple Data Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
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 26 – Acronyms

ANNEX A MODELS SUPPORTED BUT NOT INCLUDED IN THE EVALUATED CONFIGURATION

The following features were not included in the evaluated configuration of the TOE:

- The FortiGate unit is able to send log information to external log servers including FortiAnalyzer server, File Transfer Protocol (FTP), Syslog Server or Trivial File Transfer Protocol (TFTP).
- Fortinet FortiManager may be used to provide centralized management of multiple FortiGate devices.

The following models are supported, but were not tested as part of this evaluation.

DESKTOP MODELS

Model	QuickStart Guide
FG-20C	FortiGate 20C QuickStart Guide
	July 29, 2013 01-430-155969-20130729
FWF-20C	FortiWiFi 20C QuickStart Guide
	August 20, 2013 01-430-155970-20130820
FG-30D	FortiGate/FortiWiFi 30D QuickStart Guide
	July 5, 2013 01-502-202497-20130705
FWF-30D	FortiGate/FortiWiFi 30D QuickStart Guide
	July 5, 2013 01-502-202497-20130705
FWF-30D- PoE	FortiGate/FortiWiFi 30D QuickStart Guide
	July 5, 2013 01-502-202497-20130705
FG-40C	FortiGate-40C QuickStart Guide
	July 29, 2013 01-430-155912-20130729
FWF-40C	FortiWifi-40C QuickStart Guide
	July 31, 2013 19-430-155933-20130731
FG-60C	FortiGate 60C QuickStart Guide
	July 29, 2013 01-430-128372-20130729
FWF-60C	FortiWiFi 60C QuickStart Guide
	August 20, 2013 01-430-128372-20130820

Model	QuickStart Guide
FG-60D-PoE	FortiGate/FortiWiFi 60D Series QuickStart
	December 10, 2013 01-502-202499-20131
FG-80C	FortiGate-80C QuickStart Guide
	4 July 2010 01-412-89805-20090615
FWF-80CM	FortiWiFi-80CM QuickStart Guide
	12 March 2010 01-412-89807-20090615
FG-90D	FortiGate/FortiWiFi 70D/90D QuickStart Guide
	February 19, 2014 01-500-199105-20140
FG-90D-PoE	FortiGate/FortiWiFi 70D/90D QuickStart Guide
	February 19, 2014 01-500-199105-20140
FGR-100C	FortiGate Rugged 100C QuickStart Guide
	September 24, 2012 01-430-182317-20120924
FG-110C	FortiGate-110C QuickStart Guide
	19 November 2010 01-412-0468-20101119
FG-111C	FortiGate-111C QuickStart Guide
	15 April 2009 01-30007-0469-20090415

Table 27 – Supported Desktop Models

1U MODELS

Model	QuickStart Guide
FG-200B	FortiGate 200B QuickStart Guide
	July 06, 2012 01-430-175181-20120706
FG-200B-PoE	FortiGate 200B-PoE QuickStart Guide
	May 25, 2012 01-420-117374-201001
FG-240D	FortiGate 240D QuickStart Guide
	April 01, 2014 01-501-190858-20140
FG-300C	FortiGate 300C QuickStart Guide
	August 20, 2012 01-430-149396-20120820

Model	QuickStart Guide
FG-310B	FortiGate 310B QuickStart Guide
	July 05, 2012 01-430-175078-20120705
FG-311B	FortiGate 311B QuickStart Guide
	25 May 2009 01-30007-97512-20090525
FG-400D	FortiGate 400D Information Supplement
	24 July 2015 01-523-277788-20150824
FG-600C	FortiGate 600C QuickStart Guide
	May 29, 2012 01-430-154621-20120529
FG-620B	FortiGate 620B QuickStart Guide
	September 19, 2012 01-420-112406-20120919
FG-621B	FortiGate 621B QuickStart Guide
	13 July 2010 01-420-127994-201007
FG-800C	FortiGate 800C QuickStart Guide
	October 04, 2013 01-430-169975-20131004
FG-800D	FortiGate 800D Information Supplement
	November 1, 2015 01-540-273916-2015111

Table 28 – Supported 1U Models

2U MODELS

Model	QuickStart Guides
FG-280D-PoE	FortiGate 280D-PoE QuickStart Guide
	April 01, 2014 01-501-190855-20140
FG-1000C	FortiGate 1000C QuickStart Guide
	October 04, 2013 01-430-154711-20131004
FG-1240B	FortiGate 1240B QuickStart Guide
	17 November 2009 01-30007-106971-20091117
FG-3000D	FortiGate 3000D Information Supplement
	10 November 2015 01-522-266144-20150

Model	QuickStart Guides
FG-3016B	FortiGate 3016B QuickStart Guide
	4 July 2010 01-30006-0402-20080328
FG-3040B	FortiGate 3040B QuickStart Guide
	December 05, 2012 01-420-125361-20121005
FG-3100D	FortiGate 3100D Information Supplement
	10 November 2015 01-5011-275737-20150806
FG-3240C	FortiGate 3240C QuickStart Guide
	March 18, 2013 01-436-162400-20130318
FG-3810A	FortiGate 3810A QuickStart Guide
	31 August 2007 01-30005-0401-20070831

Table 29 – Supported 2U Models

3U MODELS

Model	QuickStart Guides
FG-3600C	FortiGate 3600C QuickStart Guide
	September 18, 2013 01-500-191999-20130918
FG-3950B	FortiGate 3950B QuickStart Guide
	February 23, 2012 01-430-153621-20120223
FG-3951B	FortiGate 3951B QuickStart Guide
	3 May 2010 01-413-119330-2010021

Table 30 – Supported 3U Models

BLADE MODELS

The FortiGate 5000 series chassis are modular enclosures for blade systems. The following blade systems are capable of running in the evaluated configuration:

- FortiGate-5020 (2 Blade Slots)
- FortiGate-5060 (6 Blade Slots)
- FortiGate-5140B (14 Blade Slots)

The FortiGate series chassis requires one or more of the hardware blades shown in Table 5.

Model	Security System Guides
FG-5001A	FortiGate 5001A Security System Guide
	01-30000-83456-20081023
FG-5001B/ FG-5001BX	FortiGate 5001B Security System Guide
	01-400-134818-20120216
FG-5001C	FortiGate 5001C Security System Guide
	01-500-181221-20140923
FSW-5203B	FortiSwitch 5203B Security System Guide
	01-520-145204-20140730

Table 31 – Supported Blade Models