Delivering the Right Assurance

Security Target for the Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware: EAL2+

EWA Document No. 1701-001-D002

Fortinet Document No. ST0006

Version 1.2, 18 February 2011

Prepared for:

Fortinet, Incorporated
326 Moodie Drive
Ottawa, Ontario
Canada K2H 8G3

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

EWA
Delivering the Right Assurance

Security Target for the Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware: EAL2+

EWA Document No. 1701-001-D002

Fortinet Document No. ST0004

Version 1.2, 18 February 2011

<Original> Approved by:

Project Engineer: B. Cuthbert 18 February 2011

Project Manager: M. Gauvreau 18 February 2011

Program Director: E. Connor 18 February 2011

(Signature) (Date)

AMENDMENT RECORD SHEET

Rev.	Issue Date	Description	Author	Reviewer
0.9 DRAFT	10 November 2010	Initial Release	Ben Cuthbert	
1.0 DRAFT	12 November 2010	Updated for comments from Alan and spelling and grammar.	Ben Cuthbert	Dave Squires
1.0 DRAFT 2	15 November 2010	Added SFRs for COP dependencies as per CCS Instruction #4 and addressed further comments from Alan.	Ben Cuthbert	
1.0	26 November 2010	Addressed ORs and CRs raised during ST registration quality review.	Ben Cuthbert	
1.1	16 February 2011	Updated build version	Ben Cuthbert	
1.2	18 February 2011	Updated build version	Ben Cuthbert	Greg Lague

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware, and will hereafter be referred to as the TOE throughout this document. The TOE is a hardware security system designed to provide firewall, VPN, antivirus protection, antispam protection and content filtering etc. to provide network protection.

1.1 DOCUMENT ORGANIZATION

This ST is made up of the following sections:

- Section 1, Introduction, provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.

- Section 2, Conformance Claims, provides the identification of any Common Criteria (CC), ST, Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.

- Section 3, Security Problem, 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 and its operational environment must comply, and assumptions on operational environment to uphold the TOE's secure operation.

- Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment.

- Section 5, IT Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE.

- Section 6, TOE Summary Specification, describes the security functions that satisfy TOE's security requirements.

- Section 7, Protection Profile Claims provides reference to the PP to which adherence is claimed by this ST. This section also describes the changes that were made with respect to the PP.

- Section 8, Rationale, provides rationale that the security objectives satisfy the threats, policies, and assumptions; TOE's security requirements satisfy TOE's security objectives; and the TOE summary specification satisfies the security requirements. This section also presents rationale for any dependencies that are not satisfied, and a rationale for any extended requirements.

- Section 9, References, provides background material for further investigation by users of the ST.

- Section 10, Terminology, provides definitions for specific terms used in the ST.

- Section 11, Acronyms, Abbreviations, and Initializations, provides expansions for the acronyms, abbreviations, and initializations that are used in the document. Common CC terminology has been excluded from this list.

1.2 IDENTIFICATION

- ST Title

  Security Target for the Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware: EAL2+, Version 1.2, 18 February 2011, by EWA-Canada, Ltd.

- TOE Reference

  Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware, by Fortinet Inc. TOE detailed information is illustrated in Table 1 below.

Product	**Firmware Version**	**Hardware Version**[1]	**FIPS 140-2 Certificate Number**
FortiGate-1240B	4.0 build 6443, 110212	C4CN43	Crypto Module Certificate: 1431 Algorithm Certificates: See Note 1

Table 1 - TOE Identification Details

Note 1 – The following FIPS 140-2 algorithm certificates are applicable:

Triple-DES:	957 and 962
AES:	1404 and 1409
SHS:	1274 and 1279
HMAC:	825 and 830
RSA:	686
RNG:	770

[1] For the purposes of the ST, only the first 6 characters of the hardware version are relevant. The complete version includes a padding field for compatibility with other Fortinet version naming conventions and a field for non-CC relevant changes such as the amount of memory, CPU clock speed or external labelling.

Documentation for the FortiGate-1240B operated in Common Criteria mode consists of the standard FortiOS version 4.0 documentation set plus a FIPS-CC-specific technical note.

1.3 TOE OVERVIEW

The TOE, i.e. the Fortinet FortiGate™-1240B Unified Threat Management Solution and FortiOS 4.0 CC Compliant Firmware, is a network appliance designed to provide firewall, IPv6, VPN, VLAN, antivirus protection, antispam protection and content filtering etc. to provide protection on TCP/IP networks.

The FortiGate-1240B Unified Threat Management Solution offers a cost-effective system. It is a hardware security system designed to protect computer networks from abuse. It resides between the network it is protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by the Security Administrator. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real-time; without degrading network performance. In addition to providing stateful application-level protection, the FortiGate-1240B delivers a full range of network-level services including; firewall, IPv6, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering etc.; using dedicated, easily managed platforms.

The FortiGate unit consists of a hardware box and the FortiOS™ custom Unified Threat Management Solution firmware. Administration of the system may be performed locally using an administrator console or remotely via a network management station.

The FortiGate Unified Threat Management Solution employs Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ operating system to achieve breakthrough price/performance. Their unique, ASIC-based architecture analyzes content and behaviour in real time, enabling key applications to be deployed right at the network edge, where they are most effective at protecting enterprise networks. They provide a critical layer of real-time, network-based antivirus protection that complements host-based antivirus software and supports "defense-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-1240B supports the 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 provide SSL VPN services.

The FortiGate's firewall, IPv6, VPN, VLAN, antivirus and intrusion prevention functionality are within the scope of this evaluation. Features such as antispam, content filtering and traffic shaping have been placed outside the TOE boundary for this evaluation. Section 2 provides a detailed description of the product functionality which is included in the TOE and a list of the product functionality which is excluded from the TOE.

1.4 TOE DESCRIPTION

This section primarily describes the physical and logical components of the TOE included in the evaluation.

1.4.1 Physical Boundary

1.4.1.1 Physical Configuration

The FortiGate-1240B is a stand-alone appliance that does not require additional supporting hardware to function.

The FortiGate Unified Threat Management Solution, termed a FortiGate unit, consists of custom hardware and firmware. The FortiGate unit consists of the following major components: FortiOS FIPS-CC compliant firmware, processor, memory, FortiASIC™, and I/O interfaces. It uses a proprietary Application-Specific Integrated Circuit (FortiASIC™) to improve performance. The FortiASIC™ is a hardware device which forms part of the FIPS 140-2 validated cryptographic module used by each FortiGate unit. The FortiASIC™ primarily provides crypto acceleration.

1.4.1.2 Network Interfaces

The FortiGate unit has the interfaces defined in Table 2.

Product	Interfaces				Log Storage Type and Maximum Size
	Network (Ethernet) Interfaces		Administrator Interfaces		
	No.	Speed	Local Console	Network	
FortiGate-1240B	24	1 GBit SFP	RS232/RJ-45	Yes	64GB SSD
	16	10/100/1000 Base-T			

Table 2 - FortiGate Unified Threat Management Solution Interfaces

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

- A dedicated console port is available. The port is RS232 with a RJ-45 connector. When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiGate unit via a Command Line Interface (CLI). This Local Console CLI permits a Security Administrator to configure the FortiGate unit, monitor its operation and examine the audit logs that are created;

- Remote administration may be performed via any network port that has been configured by a Security Administrator to allow HTTPS (for the Network Web-Based GUI) and SSH (for the Network CLI) traffic. When connected to a Network Management Station, this port provides remote access to the Network CLI or 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;

The FG-1240B supports removable hard disks for log data storage – 1 AMC (advanced mezzanine card) based or up to 6 FSM (Fortinet storage module) based. If a disk isn't present, the module supports memory logging.

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

1.4.1.3 TOE Boundary - Single-Unit Configuration

In the Single-Unit configuration, which is supported by the FortiGate-1240B, the TOE consists of a single FortiGate. The FortiGate-1240B controls network access by implementing the classic firewall concepts, in which the firewall is linked to two or more networks and controls the transfer of data between the networks. The configuration supports additional networks, each of which is physically connected to one of the Network Interfaces identified in Table 2.

Figure 1 shows an example of a single FortiGate 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.

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

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

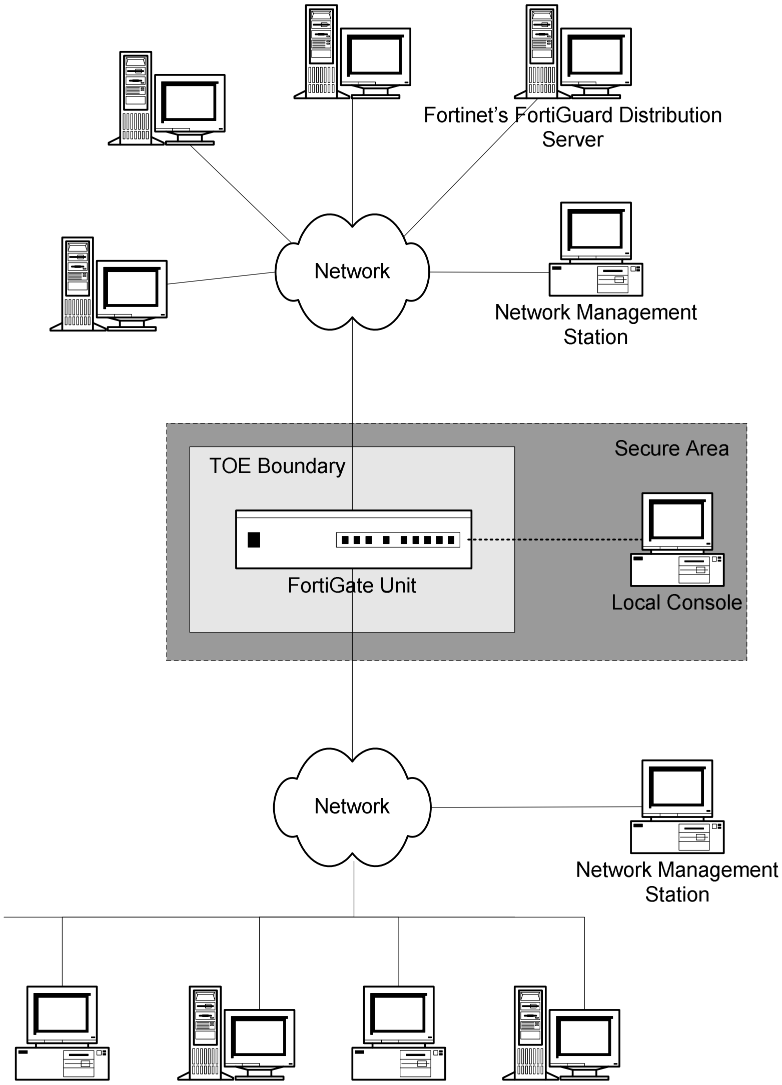
Fortinet's FortiGuard Distribution Server
Network
Network Management Station
TOE Boundary
Secure Area
FortiGate Unit
Local Console
Network
Network Management Station

Figure 1 – Single Unit FortiGate Unified Threat Management Solution Network Configuration

1.4.1.4 User Interfaces

Table 3 describes each of the interfaces that are included in the TOE in terms of the external entity to which it connects, the interface data that is transferred, the purpose of the interface and the protocol used for the transfer.

External Entity	Interface Data	Interface Purpose	Protocol(s)
Network Management Station	Administration Data	Allow remote administration using the CLI command interface	SSH
Network Management Station	Administration Data	Allow administration using the Web-Based GUI.	HTTPS
Certificate Server	Certificates/CRLs	Transfer certificates and certificate revocation lists to the FortiGate.	X.509
VPN Peer/Server	VPN Configuration	Configuration of VPN tunnels between the FortiGate and a remote peer or server.	IPSec/IKE
Local Console	Administration Data	Allow local administration using the CLI command interface	Serial
Local Console	Alarms	Transfer alarms to the local console.	Serial
Network User	User Data	Send and receive user data to/from the Network Users.	TCP/IP and protocols built on it.
Fortinet's FortiGuard Distribution Server	AV/Attack Updates	Transfer anti-virus and attack updates from Fortinet to the FortiGate Unit.	TCP/IP and protocols built on it.
USB Token	Keys	Allow the Cryptographic Administrator to load cryptographic keys.	Serial (USB)

Table 3 - FortiGate Interfaces

1.4.1.5 Features Included in the TOE

The function of the FortiGate-1240B 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 the Security 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 the Security Administrator, provides the capabilities claimed in this ST. FIPS-CC Mode provides initial default values, makes excluded features unavailable by default, and enforces the FIPS configuration requirements.

Table 4 summarizes the FortiGate features that are included in the TOE.

Feature	Description
Access Control	The FortiGate Unified Threat Management Solution provides a role-based access control capability to ensure that only authorized administrators are able to administer the FortiGate unit.
Administration (Network CLI)	The FortiGate provides management capabilities via a text-based Network CLI interface.
Administration (Local Console CLI)	The FortiGate provides management capabilities via a text-based Local Console CLI.
Administration (Network Web-Based GUI)	The FortiGate provides a Network Web-Based GUI, accessed via HTTPS, for system management and configuration.
Authentication	The FortiGate implements a FIPS-Compliant 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.
Authentication (RADIUS)	The FortiGate provides an option of using an external RADIUS Server for administrator authentication.
Certificate Management	The FortiGate provides the ability to obtain certificates and certificate revocation lists from an external certificate management server.
Cryptography	The FortiGate incorporates a FIPS 140-2 validated cryptographic module.
Firewall (Information Flow Control)	The FortiGate Unified Threat Management Solution implements a stateful traffic filtering firewall. Information flow is restricted to that permitted by a policy (set of rules) defined by the Security Administrator. The default policy is restrictive (i.e., no traffic flows without Security Administrator action to configure policy).
ICMP	The FortiGate responds to Internet Control Message Protocol (ICMP) pings without requiring that the user be authenticated. It also passes ICMP through in accordance with policies.
Intrusion Prevention	The FortiGate compares signatures to the data passing through it to detect and prevent attacks. The intrusion prevention system (IPS) attack signatures can be updated manually or the FortiGate unit can 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.
Logging (management)	The FortiGate supports management activities for configuration of logging, retention of logs, archiving of logs, and backing up of logs.
Logging (recording)	Logging is performed and data is stored in memory or written to a removable hard disk if it is present.
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 only supports user authentication for the FTP and Telnet protocols.
Self-test	The FortiGate performs self-tests of both the cryptographic and the non-cryptographic functions.

Feature	Description
Time	The FortiGate maintains internal time on a system clock, settable by the Security Administrator. This clock is used when time stamps are generated.

Table 4 - Features Included in the TOE

1.4.2 Logical Boundary

The TOE's security functionality is implemented to enforce its Security Functional Policies.

1.4.2.1 TOE Security Functional Policies

The following are two information flow control Security Functional Policies (SFPs) which the TOE enforces:

- the UNAUTHENTICATED SFP;
- the AUTHENTICATED SFP;

For the UNAUTHENTICATED SFP, the subjects under control of this policy are the TOE interfaces that connect to unauthenticated users on an internal or external network sending information through the TOE to other destinations on the internal or external network. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(1), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(1). FMT_MSA.3 requires that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the Security Administrator.

For the AUTHENTICATED SFP, the subjects under control of this policy are the TOE interfaces that connect to authenticated users on an internal or external network sending information through the TOE to other destinations on the internal or external network. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1(2), including source and destination addresses. The rules that define the SFP are found in FDP_IFF.1.2(2). FMT_MSA.3 requires that these rules be assigned restrictive initial values. FMT_MSA.1 ensures that the rules are subsequently managed only by the Security Administrator.

1.4.2.2 TOE DATA

The TOE retains TSF Configuration Data, consisting of:

- Cryptographic Data;
- Alarm Configuration;
- Audit Configuration;
- Identification and Authentication Data (User Attributes);
- Role/Permission Data;

- Time Data;
- Self-Test Parameters;
- Information Flow Policy Ruleset, including Protection Profiles;
- TOE Services Configuration;
- TSF Data Limits On Transport-Layer Resources And Actions If Exceeded;
- TSF Data Limits On Connection-Oriented Resources And Actions If Exceeded;
- TOE Access Banners;
- Trusted Channel Definition Parameters; and
- Trusted Path Definition Parameters.

The TOE retains TSF Operational Data, consisting of:

- Audit Records;
- Alarm Data;
- Session Data;
- Trusted Channel Usage;
- Trusted Paths Usage;
- Transport-Layer Resource Usage; and
- Connection-Oriented Resource Usage.

1.4.2.3 User Data

The TOE mediates the following User Data, based on a defined information flow policy:

- Information Flows to/from the TOE.

The TOE responds to the following User Data, based on a defined TOE services policy:

- TOE Service Request.

1.4.2.4 Security Attributes

The following security attributes are defined:

- Unauthenticated Policy Attributes;
- Authenticated Policy Attributes;

1.4.2.5 SUMMARY OF TOE SECURITY FUNCTIONS

1.4.2.5.1 Identification and Authentication

All administration requires authentication by UNIX style user identification (ID) and password mechanism or authentication through a RADIUS server, which can provide single-use authentication. Administration may either be performed locally using the Local Console

CLI or remotely using the Network Web-Based GUI or Network CLI. TOE users (when so configured by the Security Administrator) are required to authenticate via HTTPS in order to use some TOE services. Remote authentication data is protected via encryption (trusted path).

1.4.2.5.2 Administration

The TOE provides remote and local administrative interfaces that permit the administrative roles to configure and manage the TOE. The TOE is connected to two or more networks and remote administration data flows from a Network Management Station to the TOE. There is also a Local Console, located within a Secure Area, with an interface to the TOE.

The TOE provides three separate administrative roles: Cryptographic Administrator, Audit Administrator and Security Administrator. A user assigned to the Cryptographic Administrator role is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. A user assigned to the Audit Administrator role is the only user permitted to delete audit data. A user assigned to the Security Administrator role is responsible for all other administrative tasks (e.g., creating the TOE security policy) not addressed by the other two administrative roles.

In this Security Target the terms Cryptographic Administrator, Audit Administrator and Security Administrator refer to an administrative user assigned to that role. For instance, Audit Administrator is an administrator who has been assigned the audit administrator role. The terms Administrator and Administrators refer to administrative users that have been assigned one of the Administrator roles.

1.4.2.5.3 Information Flow Control

The TOE provides interfaces to a defined set of networks and mediates information flow between these networks. The TOE is connected to two or more networks and network data flows from a connected network, through the TOE, to a connected network.

Section 5.1 ‘TOE Security Functional Requirements’ defines the minimum set of configurable security attributes required to permit or deny information flows to or through the TOE. The set of security attributes includes items such as source and destination identification, service identifiers, and user authentication. The TOE Security Administrator configures the security attributes to construct one or more access control rules as part of a security policy on the TOE. The TOE implementation consists of one or more ‘rulesets’ that are subsequently applied to one or more TOE interfaces. Packets arriving at the TOE interface are compared to the security attributes in the ‘rulesets’. When the packet attributes ‘match’ the rules security attributes, that packet or connection is approved or denied, based on the rule. In addition to restricting access via the rules, the TOE must generate and maintain ‘state’ information for all approved connections mediated by the TOE. The TOE utilizes the ‘state’ information to monitor the status of an approved connection and validate incoming packets purporting to be part of an approved connection. The TOE is required to perform a complete reassembly of all packet fragments prior to making an access control decision on the packet.

1.4.2.5.4 Encryption

Section 5.1.2 ‘Cryptographic Support’ defines the minimum set of cryptographic attributes required by the TOE. The TOE’s cryptographic module is FIPS PUB 140-2 validated and meet Security Level 1 overall. The TOE generates and distributes symmetric and asymmetric keys. The implementation selections for key generation and key distribution are provided in Section 5.1.2. The TOE performs data encryption/decryption using the Advanced Encryption Standard (AES) algorithm with a minimum key size of 128 bits. Additional requirements for key destruction, digital signature generation/verification, random number generation and cryptographic hashing are provided in Section 5.1.2.

1.4.2.5.5 Audit

Section 5.1.1 ‘Security Audit (FAU)’ describes the TOE’s generation of audit records, alarms and audit management. Table 7 in the FAU_GEN.1 requirement lists the set of auditable events. Each auditable event generates an audit record. Table 7 also provides a list of attributes that are included in each audit record.

In addition to generating audit records, the TOE monitors auditable events and provides a Security Administrator configurable threshold for determining a potential security violation. Once the TOE has detected a potential security violation, an alarm message is displayed at the TOE’s local console as well as each active remote administrative session. The alarm message is also displayed at any remote administrative sessions which become active before the alarm is acknowledged. The message contains the potential security violation and a means to view audit records associated with the potential security violation. The message will be displayed at the various consoles until administrator acknowledgement of the message has occurred.

As mentioned in the ‘Administration’ section above, the Audit Administrator’s role is restricted to viewing the contents of the audit records and the deletion of the audit trail. The TOE provides the Administrators with a sorting and searching capability to improve audit analysis. The Security Administrator configures auditable events, backs-up audit data and manages (but cannot delete) audit data storage. The TOE provides the Security Administrator with a configurable audit trail threshold to track the storage capacity of the audit trail. As soon as the threshold is met, the TOE displays a message in the same fashion as for potential security violations, including the option of the audible alarm. If log rolling is not enabled, when the TOE reaches the audit storage capacity threshold, the TOE will enter its CC Error Mode which prevents all auditable events except for those events resulting from actions taken by the Security and Audit Administrators to correct the audit storage problem. If log rolling is enabled and the audit log becomes full, the TOE will overwrite the oldest audit records in the audit trail.

1.4.2.5.6 Self-Protection

The TOE provides self-protection functionality to ensure continued correct operation. Self-test functions are provided to detect problems in operation and respond to problems in a defined, repeatable manner. Failure of any self-test causes the TOE to enter its FIPS Error Mode. Administrator intervention is then required to return the TOE to normal operations. Additionally, the TOE protects itself by rejecting replay of communications, avoiding overload of its interfaces, managing sessions, and restricting information released on banners.

1.4.3 Exclusions

The FortiGate provides more capability than is being claimed in the ST. When FIPS-CC Mode is enabled to place the TOE into the evaluated configuration, the excluded features are not enabled. The excluded features could be enabled by an Administrator though this would contravene the CC-specific guidance that is provided to the Administrator.

Table 5 presents a summary of the features that are excluded from the TOE. These features do not contribute to any of the SFRs claimed in this ST.

Feature Excluded	Description
Administration (FortiManager)	Multiple FortiGate units may be managed by a FortiManager Server.
Alarms and Alerts	The FortiGate provides audible and visible alarms that announce detected security policy violations.
Alert Emails	In addition to alerts, the FortiGate can be configured to provide email notification.
Anti-Virus	The FortiGate Series provides anti-virus protection for network traffic passing through the FortiGate.
Authentication (Active Directory)	Windows Active Directory Server may be used to authenticate users.
Authentication (User Group Firewall Policy Authentication)	The FortiGate Firewall Policy may be configured to require authentication by user groups before the information flow is enabled. A user group is a list of users or Radius Servers, or LDAP servers. These groups may be used in the Firewall Policy to require authentication by group rather than individually.
Authentication (LDAP)	The FortiGate provides an option of using an external LDAP Server for authentication.
Backup Configuration	The FortiGate provides a means by which the Security Administrator can back up the configuration.
DHCP	The FortiGate can operate as a DHCP Server and as a DHCP relay.
Differentiated Services	The FortiGate supports differentiated services, as defined by Request for Comments (RFC) 2474 and RFC 2475.
DNS	The FortiGate can operate as a DNS server and as a DNS relay.
Dynamic Routing	Dynamic routes are configured through dynamic routing protocols that enable the FortiGate unit to automatically share information about routes with neighbouring routers and learn about routes and networks advertised by neighbouring routers.

Feature Excluded	Description
Engine Update	The FortiGate anti-virus and IPS engines may be updated.
Firmware Update	The FortiGate firmware may be updated through a. SSL/TLS link (default method); or b. bootstrap Trivial File Transfer Protocol (TFTP) to install new firmware or replace existing configuration or firmware (disabled in FIPS-CC Mode).
Instant Messaging	The FortiGate unit is able to check Instant Messaging (IM) communications and block, rate limit, pass, and bandwidth limit the IM traffic. This capability of the TOE is excluded from the evaluation. However, a FortiGate unit is also capable of scanning IM/P2P traffic for viruses and this capability is included in the evaluation.
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 supports static routing, periodic router advertisements, and tunnelling of IPv6-addressed traffic over an IPv4-addressed network.
Logging	The FortiGate unit is able to send log information to external servers (e.g., FortiAnalyzer, (formerly known as FortiLog) Server, ftp, Syslog Server, tftp, or WebTrends Server).
NTP Clock Setting	The FortiGate internal clock may be set through NTP.
Online Help and Documentation	The online help and documentation supplements the external administrative and user documents.
Protection Profile[2]	Protection profiles are used to configure anti-virus protection, and IPS.
Proxies	The FortiGate supports FTP, HTTP/HTTPS, IMAP, POP3, SMTP, and Telnet proxies for firewall users. Firewall rules may be defined that are applicable only to users who have authenticated to the firewall to use one of these proxies. The evaluated configuration only supports user authentication for FTP and Telnet.
Replacement Messages	The Security Administrator may configure replacement messages to customize alert email and information that the FortiGate unit adds to content streams such as email messages, web pages and FTP sessions. The FortiGate unit adds replacement messages to a variety of content streams. For example, if a virus is found in an email message attachment, the attached file is removed from the email and replaced with a replacement message. The same process applies to pages blocked by web-filtering and email blocked by spam filtering.
SMTP Server	The Simple Mail Transfer Protocol (SMTP) is used to send alert emails from the FortiGate.
SNMP	The FortiGate unit is able to transfer status information to a Simple Network Management Protocol (SNMP) Manager.
Spam Filter (Email Filtering)	Email filtering can be configured to scan all IMAP and POP3 email content for unwanted senders or for unwanted content.

[2] The term 'Protection Profile' is also used by Fortinet and is not to be confused with the CC terminology.

Feature Excluded	Description
Static Routing	Static routes are configured by defining the destination IP address and netmask of packets that the FortiGate unit is intended to intercept, and specifying a (gateway) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.
Support to Flaw Remediation	The FortiGate unit provides a means of sending bug reports to Fortinet in aid of flaw remediation.
Traffic Shaping	The FortiGate unit can be configured to restrict traffic based on bandwidth and time. Traffic Shaping controls the bandwidth available to and sets the priority of the traffic. The FortiGate can provide a guaranteed bandwidth, maximum bandwidth, and traffic priorities.
Troubleshooting Support	The FortiGate unit provides a capability of sending troubleshooting data directly to Fortinet.
USB Disk Support	The FortiGate-500A provides support for a Universal Serial Bus (USB) disk on which firmware and configuration data may be stored.
USB Token	The FortiGate provides for key loading via the USB port.
Virtual domain	FortiGate virtual domains provide multiple logical firewalls in a single FortiGate unit, so that one FortiGate unit can provide exclusive firewall and services to multiple networks. Traffic from each network is effectively separated from every other network.
VLAN	The FortiGate supports Virtual Local Area Network (VLAN) as a sub interface attached to a physical interface port.
VPN	The FortiGate supports Virtual Private Networking (VPN) using IPSec to provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.
Web Content Filtering	Web content filtering can be configured to scan and block all HTTP content protocol streams for Uniform Resource Locators (URLs) or for web page content. If a match is found between a URL on the URL block list, or if a web page is found to contain a word or phrase in the content block list, the FortiGate blocks the web page. The blocked web page is replaced with a message that an administrator can edit using the web-based manager.
Zone	The FortiGate supports the use of a zone as a shorthand notation to form a group of related interfaces and VLAN sub interfaces.

Table 5 - Features Excluded from the TOE

1.5 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations 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, however in cases where such a selection has been omitted, the omission is noted in Section 7.2.

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown, however in cases where such an assignment has been omitted, the omission is noted in Section 7.2.

- Refinement: Refined components are identified in three ways; (1) they are listed in Table 6 - Security Functional Requirements by using bold text, (2) the word **Refinement:** (in bold text) is added to the requirement statement in Section 5, and a description of the refinement is included in Section 7.2 PP TAILORING. It should be noted that the PP includes numerous refinements to functional requirements taken from the CC. However these refinements are NOT indicated in this document. The only refinements marked in this document are those which have been made to the text of the requirements listed in the PP or to the text of a requirement drawn from the CC which is not included in the PP.

- 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_IFC.1(1), Subset information flow control (unauthenticated policy)' and 'FDP_IFC.1(2) Subset information flow control (authenticated policy)'.

This ST is based on the Application-level Firewall PP (ALFWPP). As noted previously, the ST also includes some requirements taken from CC Part 2 and Part 3 that are not in the protection profile. Deviations in phrasing from the PP text are noted as refinements. For non-PP requirements deviations from the CC text are noted as refinements.

1.6 TERMINOLOGY

The following terminology is used in this ST:

Administrator	An Administrator is responsible for administering the TOE. The TOE has three administrative roles; Audit Administrator, Security Administrator, and Cryptographic Administrator. Administration is performed using the Administrator Interfaces which consist of the Local Console, Network Web-Based GUI, and Network CLI. Wherever possible, the ST uses the specific administrator role. However in some instances a function may be available to any member of one of the three administrative roles. In these cases the ST uses the generic term 'Administrator' to denote that the function may be performed by any member of an administrative role.

Attack Potential
The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Controlled Subject
Entity under control of the TOE Security Policy (TSP).

Presumed Address
The TOE can make no claim as to the real address of any source or destination subject, therefore 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. The appropriate definitions for both usages of the term may be found in Section 10. Within the document, 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 denoted by spelling out the complete term.

User
A User is an entity that uses the TOE's services to pass information through the TOE over the Network Interfaces. Authentication is required for some services. An 'authenticated proxy user' denotes a user who has been identified and authenticated by the TOE.

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.

Firewall Rules
Firewall rules are configuration parameters set by the Security Administrator that allow or deny data flow through the TOE. These rules may optionally include the use of a firewall protection profile that enforces Anti-Virus (AV) and Intrusion Prevention System (IPS) configuration parameters.

2 CONFORMANCE CLAIMS

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1R3, July 2009, CCIMB-2009-07-001 -002 and -003, with all current interpretations.

This ST contains functional requirements based upon functional components in CC Part 2. Therefore, the TOE is CC Part 2 conformant.

The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 2, augmented with ALC_FLR.2 –Flaw Reporting Procedures.

The TOE for this ST is demonstrably conformant with the U.S. Government Protection Profile for Application-level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007. This ST also includes additional security functional requirements drawn from Part 2 of the CC.

3 SECURITY PROBLEM

3.1 ASSUMPTIONS

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

A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

3.2 THREATS

3.2.1 Threats Addressed by the TOE

The threats discussed below are addressed by the TOE. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself. The threat agents are assumed to have a low 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 unit will be protected to the extent necessary to ensure that they remain connected to the network it protects. The following threats are addressed by the TOE and should be read in conjunction with Section 8.1.2 TOE Security Objectives Rationale.

T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.LOWEXP	An unauthorized person may attempt to compromise the TOE using obvious penetration attacks requiring minimal attack potential.
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.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

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.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

3.2.2 Threats Addressed by the Operating Environment

The threat possibility discussed below must be counted by procedural measures and/or administrative methods.

T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.3 ORGANIZATIONAL SECURITY POLICIES

The TOE must address the organizational security policies described below.

P.CRYPTO	AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).

4 SECURITY OBJECTIVES

This chapter 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 Operating 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 8.

4.1 TOE SECURITY OBJECTIVES

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

O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
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.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

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, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

4.2 SECURITY OBJECTIVES FOR THE OPERATING ENVIRONMENT

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

OE.PHYSEC	The TOE is physically secure.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	The TOE does not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.

5 IT SECURITY REQUIREMENTS

This section provides security functional and assurance requirements that must be satisfied by the TOE. These requirements consist of components from the CC Part 2 and Part 3.

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for the TOE are summarized in Table 6. These requirements consist of components derived solely from the Application-level FW PP. Requirements which have been refined in this document are shown in Table 6 using bold text.

Component	Description
FAU_GEN.1	**Audit data generation**
FAU_SAR.1	**Audit review**
FAU_SAR.3	Selectable audit review
FAU_STG.1	**Protected audit trail storage**
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
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)
FDP_IFF.1(1)	**Simple security attributes (unauthenticated policy)**
FDP_IFF.1(2)	**Simple security attributes (authenticated policy)**
FDP_RIP.1	Subset residual information protection

Component	**Description**
FIA_AFL.1	**Authentication failure handling**
FIA_ATD.1	**User attribute definition**
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MOF.1(1)	**Management of security functions behaviour (on/off)**
FMT_MOF.1(2)	**Management of security functions behaviour (modify)**
FMT_MSA.1(1)	**Management of security attributes (unauthenticated attributes)**
FMT_MSA.1(2)	**Management of security attributes (authenticated attributes)**
FMT_MSA.1(3)	**Management of security attributes (unauthenticated rules)**
FMT_MSA.1(4)	**Management of security attributes (authenticated rules)**
FMT_MSA.3	**Static attribute initialization**
FMT_MTD.1(1)	**Management of TSF data (user attributes)**
FMT_MTD.1(2)	**Management of TSF data (time TSF data)**
FMT_MTD.2	**Management of limits on TSF data**

Component	**Description**
FMT_SMR.1	**Security roles**
FPT_STM.1	**Reliable time stamps**

Table 6 - Security Functional Requirements

5.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

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

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

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

c) [*the events listed in Table 7*].

FAU_GEN.1.2 - **Refinement:** 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 column three of Table 7*].

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FCS_COP.1	Success and failure, and the type of cryptographic operation.	The identity of the external IT entity attempting to perform the cryptographic operation
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent	The identity of the offending user and the authorized administrator.

Requirement	Auditable Events	Additional Audit Record Contents
	restoration by the authorized administrator of the user's capability to authenticate.	
FIA_UAU.5	Any use of the authentication mechanism.	The user identities provided to the TOE.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.
FMT_SMR.2	Modification to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.

Table 7 - Auditable Events

FAU_SAR.1 Audit review

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

FAU_SAR.1.2 - **Refinement:** The TSF shall provide the audit records in a manner suitable for the administrator to interpret the information.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 - The TSF shall provide the ability to perform [searches and sorting] of audit data based on:

a) [*user identity;*

b) *presumed subject address;*

c) *ranges of dates;*

d) *ranges of times;*

e) *ranges of addresses*].

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 – The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 – **Refinement:** The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 - The TSF shall [prevent auditable events, except those taken by the authorized administrator] and [*shall limit the number of audit records lost*] if the audit trail is full.

5.1.2 Cryptographic Support (FCS)

This section specifies the cryptographic support required in the TOE. As previously stated the cryptographic support is required for authentication mechanisms, for trusted path, trusted channel and for integrity mechanisms. The cryptographic requirements are structured to accommodate use of the FIPS 140-2 standard and the CSE and NIST Cryptographic Module Validation Program (CMVP) in meeting the requirements, and to accommodate use of multiple cryptographic modules in meeting the required cryptographic functionality.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 – The TSF shall generate cryptographic keys in accordance with a specified cryptgraphic key generation algorithm [*SSH*, *SSL*] and specified cryptographic key sizes [at least *128 binary digits in length*] that meet the following: [*FIPS PUB 140-2 (Level 1)*].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 – The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*key zeroization*] that meets the following: [*FIPS PUB 140-2 (Level 1)*].

FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 – The TSF shall perform [*encryption of remote authorized administrator sessions*] in accordance with a specified cryptographic algorithm: [*AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in*

SP 800-67)] and cryptographic key sizes [*that are at least 128 binary digits in length*] that meet the following: [*FIPS PUB 140-2 (Level 1)*].

Application Note: FCS_COP.1 is taken exactly from the ALFWPP and includes any erroneous references exactly as found in that validated PP. FIPS SP 800-67 refers to a Triple-DES related specification and not AES.

5.1.3 User data protection (FDP)

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

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

a) [*subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;*

b) *information: traffic sent through the TOE from one subject to another;*

c) *operation: pass information*].

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

FDP_IFC.1.1(2) – The TSF shall enforce the [*AUTHENTICATED SFP*] on

a) [*subjects: a human user or external IT entity that sends and received FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5;*

b) *information: FTP and Telnet traffic sent through the TOE from one subject to another;*

c) *operation: initiate service and pass information*].

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

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

a) [*subject security attributes:*

- *presumed address*

b) *information security attributes:*

- *presumed address of source subject;*

- *presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs; and*
- *service*].

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

- [*Subjects on an internal network 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, created by the authorized administrator;*
  - *The presumed address of the source subject, in the information, translates to an internal network address;*
  - *And the presumed address of the destination subject, in the information, translates to an address on the other connected network.*
- *Subjects on the external network 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, created by the authorized administrator;*
  - *The presumed address of the source subject, in the information, translates to an external network address;*
  - *And the presumed address of the destination subject, in the information, translates to an address on the other connected network*].

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

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

FDP_IFF.1.5(1) – **Refinement:** 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 information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;*

c) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;*

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;*

e) *The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and*

f) *For application protocols supported by the TOE (e.g., DNS, HTTP, SMTP and POP3), the TOE shall deny any access or service requests that match known intrusion signatures. This shall be accomplished through protocol filtering proxies that are designed for that purpose.*]

Application Note: Rule f) applies when an application-level proxy is provided for the following protocols: DNS, HTTP, SMTP, and POP3.

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

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

a) [*subject security attributes:*

- *Presumed address*

b) *Information security attributes:*

- *User identity;*

- *Presumed address of source subject;*
- *Presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs;*
- *Service (i.e., FTP and Telnet); and*
- *Security-relevant service command.*]

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

- [*Subject on an internal network can cause information to flow through the TOE to another connected network if:*
  - *The human user initiating the information flow authenticates according to FIA_UAU.5;*
  - *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, created by the authorized administrator;*
  - *The presumed address of the source subject, in the information, translates to an internal network address;*
  - *And the presumed address of the destination subject, in the information, translates to an address on the other connected network.*
- *Subjects on the external network can cause information to flow through the TOE to another connected network if:*
  - *The human user initiating the information flow authenticates according to FIA_UAU.5;*
  - *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, created by the authorized administrator;*

- *The presumed address of the source subject, in the information, translates to an external network address; and*
- *The presumed address of the destination subject, in the information, translates to an address on the other connected network*].

FDP_IFF.1.3(2) – The TSF shall enforce the [*none*].

FDP_IFF.1.4(2) - The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5(2) – **Refinement:** 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 information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;*

c) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;*

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;*

e) *The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and*

f) *The TOE shall reject Telnet or FTP command requests that match known intrusion signatures. This must be accomplished through protocol filtering proxies designed for that purpose.*]

Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses. A "service", listed in FDP_IFF.1.1(b) could be identified, for example, by a source port number and/or destination port *number. A "service command", also mentioned in FDP_IFF.1.1(b) could be identified, for example, in the case of the File Transfer Protocol (FTP) service as an FTP STOR or FTP RETR.*

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] [*all objects*].

5.1.4 Identification and authentication (FIA)

FIA_AFL.1 - Authentication failure handling

FIA_AFL.1.1 - **Refinement:** The TSF shall detect when [[*a non-zero number determined by the Security Administrator*]] of unsuccessful authentication attempts occur related to [*authorized TOE administrator access or authorized TOE IT entity access*].

FIA_AFL.1.2 – **Refinement:** When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [*prevent the offending user from successfully authenticating until the Security Administrator takes some action to make authentication possible for the user in question or until a Security Administrator defined time period has elapsed*].

FIA_ATD.1 User attribute definition

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

a) [*identity; and*

b) *association of a human user with the authorized administrator role*].

FIA_UAU.1 – Timing of authentication

FIA_UAU.1.1 – The TSF shall allow [*UNAUTHENTICATED SFP information flows*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 – The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 – Multiple authentication mechanisms

FIA_UAU.5.1 – The TSF shall provide [*password and single-use authentication mechanisms*] to support user authentication.

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

a) *single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;*

b) *single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;*

c) *single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user;*

d) *reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator*].

FIA_UID.2 User identification before any action

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

5.1.5 Security management (FMT)

FMT_MOF.1(1) Management of security functions behavior (on/off)

FMT_MOF.1.1(1) – **Refinement:** The TSF shall restrict the ability to [enable, disable] the functions: [*operation of the TOE; multiple use authentication functions described in FIA_UAU.5*] to [*the Security Administrator*].

FMT_MOF.1(2) Management of security functions behavior (modify)

FMT_MOF.1.1(2) – **Refinement:** The TSF shall restrict the ability to [enable, disable, determine and modify the behaviour of] the functions: [*audit trail management; backup and restore for TSF data, information flow rules, and audit trail data; and communication of authorized external IT entities with the TOE*] to [*the Security Administrator*].

FMT_MSA.1(1) Management of security attributes (unauthenticated attributes)

FMT_MSA.1.1(1) – **Refinement:** 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 [*listed in section FDP_IFF.1.1(1)*] to [*the Security Administrator*].

FMT_MSA.1(2) Management of security attributes (authenticated attributes)

FMT_MSA.1.1(2) – **Refinement:** 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 [*listed in section FDP_IFF.1.1(2)*] to [*the Security Administrator*].

FMT_MSA.1(3) Management of security attributes (unauthenticated rules)

FMT_MSA.1.1(3) – **Refinement:** The TSF shall enforce the [*UNAUTHENTICATED SFP*] to restrict the ability to [delete and [*create*]] the security attributes [*information flow rules described in FDP_IFF.1(1)*] to [*the Security Administrator*].

FMT_MSA.1(4) Management of security attributes (authenticated rules)

FMT_MSA.1.1(4) – **Refinement:** The TSF shall enforce the [*AUTHENTICATED SFP*] to restrict the ability to [delete and [*create*]] the security attributes [*information flow rules described in FDP_IFF.1(2)*] to [*the Security Administrator*].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 – The TSF shall enforce the [*UNAUTHENTICATED SFP and AUTHENTICATED SFP*] to provide [restrictive] default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 – **Refinement:** The TSF shall allow [*the Security 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 the Security Administrator

FMT_MTD.1(1) Management of TSF data (user attributes)

FMT_MTD.1.1(1) – **Refinement:** The TSF shall restrict the ability to [query, modify, delete, [*and assign*]] the [*user attributes defined in FIA_ATD.1.1*] to [*the Security Administrator*]

FMT_MTD.1(2) Management of TSF data (time TSF data)

FMT_MTD.1.1(2) – **Refinement:** The TSF shall restrict the ability to [[*set*]] the [*time and date used to form the timestamps in FPT_STM.1.1*] to [*the Security Administrator*].

FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 – **Refinement:** The TSF shall restrict the specification of the limits for [*the number of authentication failures*] to [*the Security Administrator*].

FMT_MTD.2.2 -The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [*actions specified in FIA_AFL.1.2*].

FMT_SMR.1 Security roles

FMT_SMR.1.1 - **Refinement:** The TSF shall maintain the roles: [

a) *Security Administrator;*

b) *Cryptographic Administrator; and*

c) *Audit Administrator*].

FMT_SMR.1.2 – **Refinement:** The TSF shall be able to associate users with roles.

5.1.6 Protection of the TOE Security Functions (FPT)

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 – **Refinement:** The TSF shall be able to provide reliable time stamps.

Application Note: The word “reliable” in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2).

The assurance requirements are summarized in the Table 8 below.

Assurance Class	**Assurance Components**	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage

Assurance Class	Assurance Components	
	Identifier	**Name**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 8 - Assurance Requirements

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions of the TOE. The demonstration that TOE's security functions meet the TOE SFRs specified in Section 5 is presented in Section 8.

6.1 TOE SECURITY FUNCTIONS

6.1.1 Overview

The TOE security functions that were introduced in Section 1.4.2.5 are further elaborated in this section.

6.1.2 Identification and Authentication

F.I&A

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. 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 and specific services. The identification and authentication mechanism is a username and password combination or authentication via RADIUS (which can provide single-use mechanisms). The accounts are created by the Security Administrator over the serial or network interfaces.

The TOE generates an alarm indicating a possible security violation when the number of consecutive unsuccessful attempts to establish a remote session, by a given administrative or network account, exceeds a maximum limit. The maximum limit is set by the Security Administrator.

In addition to the generation of an alarm, the Security Administrator can specify whether or not exceeding the maximum number of login attempts results in the account becoming locked. If the Security Administrator specifies that the account does become locked, the Security Administrator also specifies the period of time for which the account is locked.

Once a user account has been locked, that user may not establish a remote session with the TOE until the lockout time period has expired or the Security Administrator has taken action to unlock the account.

Note: The TOE does not enforce an authentication limit for the Local Console.

6.1.3 Administration

F.ADMIN	Administrative access to the TOE is restricted to authorised administrators and is controlled through a set of pre-defined roles (Security Administrator, Audit Administrator and Crypto Administrator). The roles permit specific types of administrative activities to be performed.

All Administrators can read audit log data, acknowledge alarms and execute self-tests. In addition the Audit Administrator can delete audit records and the Crypto Administrator can modify the cryptographic security data. The Security Administrator can not delete audit records or modify cryptographic security data but can perform all other TOE administration functions.

The TOE also supports a non-administrative role, 'Authenticated User'. The 'Authenticated User' role is used by network users that are authenticating to the TOE while attempting to use the FTP or Telnet transport-layer protocols.

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 or Network CLI interfaces.

Only the Audit Administrator may delete stored audit data. The TOE prevents all modifications (except deletion) to the audit data.

The Cryptographic Administrator can control whether the cryptographic self-tests are executed automatically every time a key is generated.

Only the Security Administrator may perform the following operations:

- modify, disable or delete authenticated user accounts;
- modify, disable or delete the account of another administrator;
- specify the attributes which are used to define the firewall rules;
- specify the frequency for the automatic execution of cryptographic self-tests (in the range of 1 to 480 minutes);

- define or modify the rules that determine whether a potential security violation has taken place;
- specify whether auditable events are included or excluded from the audit trail;
- determine if an alarm includes an audible signal;
- action to be taken by the TOE in the event of audit storage exhaustion;
- configure the use of an NTP server;
- specify the limits for the number of authentication failures;
- ability to enable, disable operation of the TOE;
- ability to enable, disable the multiple-use authentication functions described in FIA_UAU.5;
    - this refers to setting the configuration values that either establish or terminate a trusted channel with an external IT entity; and
    - this refers to adding or deleting setting which define the valid locations from which an administrator can SSH into the TOE.
- specify the period of inactivity which causes an administrative or authenticated user session to be terminated by the TOE; and
- modify the time and date setting of the TOE’s hardware clock;

Security Administrator modification to the list of TOE services which require authentication are applied immediately after the Security Administrator completes the modification. Security Administrator modifications to the firewall rules are applied immediately after the Security Administrator completes the modification.

When the account of an administrator or an authenticated user is disabled or deleted, any sessions belonging to that account are immediately terminated by the TOE. The TOE also immediately enforces the revocation of an administrative role.

6.1.4 Information Flow Control

F.IFC

The TOE operates in accordance with two information flow security functional policies.

The UNAUTHENTICATED SFP allows unauthenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by the Security Administrator.

The AUTHENTICATED SFP allows authenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by the Security Administrator.

The security functional policies are implemented as firewall rules. The rules that implement the SFPs have restrictive default values and by default no information is allowed to flow, and TOE services are not available to unauthenticated users. Regardless of firewall rules, packets which include specific 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 the Security Administrator and the Security Administrator can also specify alternative initial values to override the default values. The TOE allows the Security 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 the Security Administrator specified firewall rules which permit the information flow.

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

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

The TOE ensures that no information from previously processed information flows is transferred to subsequent information flows.

This applies both to information that is input to the TOE from an external source and to information (e.g., padding bits) that might be added by the TOE during processing of the information from the external source.

The TOE follows a sequence of ordered steps in order to decide whether or not a requested information flow is allowed to proceed.

Incoming information is 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.

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.

For information which flows via an application proxy, the TOE ensures that the connection from the source terminates at the TOE and that the connection between the TOE and the destination does not include any of the stateful protocol attributes associated with the subject.

The Security Administrators may define firewall rules which permit (or deny) the flow of information based upon (but not limited to) the following criteria:

- The TOE interface which originates the information flow (the source subject);
- The TOE interface which is the destination of the information flow (the destination subject);
- The information contained within the information flow (packet contents); and
- The type of application proxy request (protocol).

The TOE completely reassembles fragmented packets before applying the firewall policy rules to the packets. The TOE implements stateful packet inspection rules in that each, non-fragmented, packet that is received by the TOE is either associated with an existing allowed connection, or is considered as an attempt to establish a new connection and therefore subject to the firewall rules. The stateful packet inspection considers the following attributes for IP-based network stacks:

1) Connection-oriented protocols;

   a) sequence number;

   b) acknowledgement number;

   c) Flags (SYN, ACK, RST, and FIN)

2) Connectionless protocols;

   a) source and destination network identifiers;

   b) source and destination service identifiers

For connectionless protocols, a TOE optimization creates a 'conceptual session' for the connectionless protocol that is based upon the addresses and port numbers. Then, as occurs for connection oriented protocols, packets associated with an established session need not go through the entire firewall rule processing.

The Security Administrator has the ability to specify the order in which the firewall rules are applied to requested information flows. The first rule which explicitly applies to the application proxy request is used to determine whether or not the request is accepted or rejected. If there are no rules which explicitly apply to the requested information flow or to the requested application proxy, then the request is rejected. The TOE also provides tools which allow the Security Administrator to view information flows allowed by the set of defined firewall rules before applying the ruleset.

Requests for unauthenticated TOE services are controlled by configuration of each interface. Regardless of other firewall rules, the TOE will deny any information flow request if:

- The presumed source is not included in the set of source identifiers for the TOE.

- The presumed source is a broadcast identity;

- The presumed source is a loopback identifier; and

The request specifies the route of information flow from the source subject to the destination subject.

6.1.5 Encryption

F.CRYPTO

The TOE uses FIPS-approved cryptography that has been implemented in FIPS 140-2 validated cryptographic modules. The FIPS-validated cryptographic modules implemented in the TSF meet Security Level 1 overall and meet Security Level 3 for the following: cryptographic module ports and interfaces; roles, services and authentication; and design assurance. The proprietary FortiASIC™ chip is a hardware component which forms part of the validated cryptographic modules used in the TOE. Cryptographic key destruction by the TOE 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 RAM or Flash memory. Keys in RAM are destroyed by overwriting the key storage area with an alternating pattern at least once. Keys in Flash memory are destroyed by lifting the voltage from the bits that comprise the key, which produces the same effect as overwriting those bits with zeros.

The TSF provides a cryptographic function that an Administrator may use to verify the integrity of all TSF data except the audit data and to verify the integrity of the TSF executable code. These self-tests are executed on initial start-up or at the request of an Administrator.

The TOE destroys cryptographic keys in accordance with a cryptographic key zeroization method which meets the Key Zeroization Requirements of FIPS PUB 140-2 Key Management Security Level 1.

The zeroization of all private cryptographic keys, plaintext cryptographic keys and all other critical cryptographic security parameters is immediate and complete.

Zeroization of intermediate storage areas for private cryptographic keys, plaintext cryptographic keys and all other critical cryptographic security parameters is accomplished by overwriting the storage area three times with an alternating pattern.

The storage area for private cryptographic keys, plaintext cryptographic keys and all other critical cryptographic security parameters is a flash RAM device. Zeroization of these storage areas occurs when the Security Administrator executes a factory reset or enables FIPS-CC mode. At these times, all non-hard-coded keys and critical security parameters are zeroized by lifting the voltage from the bits comprising the key, which has the same effect as overwriting the storage area with zeroes. The hard-coded keys are ANSI X9.31 RNG AES Key, Firmware update key, configuration integrity key, configuration backup key.

For AES key establishment, the cryptomodule provides the capability to act as the initiator or responder (that is, act as Party U or Party V as defined in the standard) to agree on cryptographic keys of all sizes using the dhEphem key agreement scheme where domain parameter p is a prime of 3072 bits and domain parameter q is a prime of 1024 bits and that conforms with ANSI X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography.

6.1.6 Audit

F.AUDIT

The TOE creates audit records for administrative events, potential TSP 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.

Upon detecting a potential TSP violation, the TOE immediately displays an alarm message identifying the potential TSP violation and, at the option of the Security Administrator, generates an audible alarm and makes accessible the audit record contents associated with the auditable event(s) that generated the alarm. The TOE displays alarm messages and sounds the audible alarm until the alarm has been acknowledged.

The administrator can review, search and sort the audit records. The audit records are stored locally; using memory, a hard disk or a FLASH memory card depending on the model. The storage devices used for audit record storage are identified in Table 2.

The Security Administrator specifies whether the TOE prevents the loss of audit records or provides log rolling capabilities. If log rolling is not enabled, reaching 95% of the audit storage capacity results in the TOE entering an error mode which shuts down the network interfaces and therefore prevents the occurrence of auditable events (except those taken by an authorized administrator to clear the error mode). When the TOE is in the error mode, only administrative access is allowed and this access is restricted to the Security Administrator and Audit Administrator. The 95% audit log threshold limit allows the TOE to record the actions taken by Security Administrator or Audit Administrator to clear the error mode. When log rolling is enabled the oldest audit records are overwritten.

The TOE generates audit records for the startup and shutdown of the audit function and all of the events.

The TOE generates timestamps for all audit events and records the timestamp with each audit record. Also recorded are the type of event, identity of the user or subject which caused the event (if applicable), and outcome of the event.

Standard audit records are 512 bytes in length. If an audit record exceeds 512 bytes, it is wrapped into a second 512 byte audit record to ensure no audit detail is lost.

The TOE has eight (8) different classes of audit records:

- Event log – includes all system level events such as identification, authentication, configuration changes, audit record deletion, etc.
- Traffic log – includes all data flow decisions, source/destination information, etc.
- Attack log – includes any IDS or local protection events such as DoS events, etc. (not part of evaluated configuration)
- Web filter log (not part of evaluated configuration).
- Antispam log (not part of evaluated configuration).
- IM/P2P log (not part of evaluated configuration).
- Antivirus log, (not part of evaluated configuration).
- VoIP log (not part of evaluated configuration).

It is not possible to startup and shutdown the auditing function independently of the TOE. However since the TOE writes audit records for the startup and termination of each TOE subprocess (daemon), the audit trail will contain records which show the startup and shutdown of the auditing function coincident with the startup and shutdown of the TOE itself.

Upon detecting a potential violation, the TOE immediately displays an alarm message identifying the potential security violation, generates an audible alarm (at the option of the Security Administrator), and makes accessible the audit record contents associated with the auditable event(s) that generated the alarm.

The TOE displays alarm messages and sounds the audible alarm until the alarm has been acknowledged. The alarm message will be displayed and the audible alarm will sound at the Local Console regardless of whether or not an administrator is currently logged into the Local Console. At the Local Console, the TOE will repeat the display of the alarm message to ensure that the message is not scrolled off the display by other activity at the Local Console.

The alarm message will display and the audible alarm will sound at any Network Management Stations which have administrative sessions at the time the potential security violation was detected.

The alarm message will display and the audible alarm will sound at any Network Managements Stations which establish administrative sessions with the TOE before the alarm is acknowledged.

Alarms can only be acknowledged by an Administrator who has successfully authenticated to the TOE through the Local Console, Network CLI or Network Web-based GUI. The TOE creates an audit record which includes the identity of the Administrator that acknowledged the alarm and the time the alarm was acknowledged. When an alarm is acknowledged, the TOE displays a message at the Local Console and at any Network Management Stations with administrative sessions identifying:

1) the potential security violation which caused the alarm,

2) the identity of the administrator who acknowledged the alarm and

3) the time the alarm was acknowledged.

This acknowledgement message will be displayed at the Local Console regardless of whether or not an administrator is currently logged into the Local Console.

When using the Network Web-based GUI, acknowledgement is done by selecting the 'OK' button on the alarm notification. When using the Local Console or Network CLI, the administrator must execute an 'ackalarm' command in order to acknowledge the alarm.

The Security Administrator can specify thresholds for the following events:

1. Administrator authentication failures;
2. Authenticated user[3] authentication failures;
3. Replay attempts of TSF data or security attributes;
4. Self-test failures; and
5. Firewall rule violations, based on source/destination address and port and rule.

An alarm is triggered if the number of events exceeds the defined threshold.

Administrative guidance is provided which instructs the Security Administrator to set the thresholds for replay attempts and self-test failures to a value of one (1). This ensures that an alarm is triggered for all detected replay attempts and all failures of the cryptographic and non-cryptographic self-tests.

All administrative roles have read access to the audits records (Security Administrator, Audit Administrator and Crypto Administrator). The audit records can be accessed through the Local Console, Network CLI, and the Network Web-based GUI.

When using the Network Web-Based GUI, administrators can view all audit records either as raw data (all columns) or as a filtered subset of columns. Filtered audit records (columns and rows) can be viewed through the Local Console or Network CLI. Administrators can modify the filters to change the view of the audit records. The number of records to display at one time can also be specified.

The TOE restricts access to all TOE administrative functions to authenticated administrators by assigned role. All administrative roles have read access to the audit records (Security Administrator, Audit

[3] Authenticated user in FortiGate refers to non-administrative users that must authenticate in order to pass information through the TOE. This equates to ‘proxy user’ as the term is used in the requirements of section 5.

Administrator and Crypto Administrator). Non-administrative users have no access to the audit log files and the data that they contain.

The TOE supports selectable review (display) of audit data through the Local Console or the Network CLI. Log data can be filtered for display. Specific audit information can be specified as part of the filter. For example, the administrator could execute a CLI command to filter (list) all audit records with a specific source IP and/or all records between 2 dates. Filter criteria include (but are not limited to):

- user identification (including a range of users);
- source subject identity;
- destination subject identity;
- dates and times (from/to, included/excluded);
- a range of one or more subject service identifiers;
- a range of one of more transport layer protocols;
- firewall rule identity;
- TOE network interface;
- log severity level (information, alert, emergency, critical, error, warning, notification, debug); and
- action (accept, deny).

The TOE allows the Security Administrator to modify the set of auditable events using the Local Console or the Network CLI. Events can be excluded from the audit record as they are written to the log storage device based on a filter. Filter parameters include (but are not limited to); administrator identity, authenticated user identity, event type, network identifier, source/destination IP address, subject service identifier, success or failure of the auditable event and firewall rule identity.

Deletion of individual audit records, sets of audit records, and the audit logs themselves is restricted to administrators with the Audit Administrator role. No user (administrative or otherwise) has the ability to modify the records in the audit logs.

6.1.7 Self-Protection

F.PROTECT

The TOE ensures that no information flows from one network interface to another without passing through the TOE and being subject to the firewall rules.

The TOE maintains an isolated security domain for its own execution. FortiOS is the only application that is on the TOE and no other applications can be loaded onto the TOE. Administrators and users do not have access to the operating system or the file system (there are no root/system level users). The TOE stores all security and configuration data in segregated configuration files. The TOE only provides identification, authentication and information flow services to non-administrative users.

The TOE ensures that no residual data from previous packets passing through the TOE is reused in any way. Any residual information in any resource is over-written or otherwise destroyed so that it cannot be reused or otherwise accessed either inadvertently or deliberately.

The TOE runs a suite of self-tests during initial start-up, periodically during normal operation as specified by the Security Administrator, and at the request of an administrator to demonstrate the correct operation of the hardware portions of the TSF. The TOE also runs the suite of self-tests provided by the FIPS 140-2 cryptographic module during initial start-up, at the request of an administrator, and periodically at a Security Administrator-specified interval not less than once a day, to demonstrate the correct operation of the cryptographic components of the TSF.

TOE Self-tests

The TOE provides self-tests for hardware portions of the TSF, cryptographic functionality, and integrity verification. These tests are run during initial start-up, periodically during normal operation as specified by the Security Administrator, and at the request of an administrator. The cryptographic self-tests will also be executed periodically by the TOE at a Security Administrator specified interval which may not be less than once per day. The Security Administrator may also configure the TOE such that the cryptographic self-tests are executed immediately after the generation of a key.

The success or failure of each cryptographic self-test and integrity verification self-tests is displayed on local console as the execution of the test is completed. If one of the cryptographic self-tests or integrity validation self-tests fails, the TOE enters its FIPS Error Mode. This mode provides the ability to return the TOE to a secure state. The operation which caused the FIPS error mode is considered incomplete and no further action in that regard takes place. Note that for non-log storage errors, cycling the power is necessary which doubly ensures that keys stored in volatile memory are cleared. No temporary keys are written to non-volatile memory

Hardware self-tests demonstrate the correct operation of the hardware portions of the TSF.

Cryptographic self-tests

The cryptographic self-tests demonstrate the integrity of the following cryptographic functions: AES, 3DES, SHA-1, HMAC-SHA1, RNG and HW-Accelerated Crypto Libraries.

The TOE also runs the suite of self-tests provided by the FIPS 140-2 cryptographic module during initial start-up, at the request of an administrator, and periodically at a Security Administrator-specified interval not less than once a day.

Included in the cryptographic self-tests are tests to demonstrate the correct operation of the cryptographic components of the TSF. The TOE enters its FIPS Error Mode when any of the following are detected:

- Failure of an integrity verification self-test; and
- Failure of a cryptographic self-test.

The TOE enters its CC Error Mode when any of the following are detected:

- Audit log size reaches 95% of the allocated audit log storage capacity and the ‘shutdown network interfaces’ option is in effect.

Integrity verification self-tests

The TOE maintains, in its flash memory, a RSA signature value for its firmware and an HMAC SHA-1 digest for the TSF data (configuration data). The stored values are updated whenever the TOE firmware is updated and whenever a change is made to the configuration data.

The TOE performs a series of integrity verification self-tests at startup to ensure the integrity of the TOE firmware and TSF data (excluding audit data). The tests verify the RSA signature for the TOE firmware and the HMAC SHA-1 digest value for the TSF data.

Failure of the self-tests cause the TOE to enter a mode where the ability to return the TOE to a secure state is provided.

Time is provided by the TSF and can only be changed by the Security Administrator. Changes to the time are audited.

Before establishing a user session that requires authentication or before establishing an administrative session, the TOE displays a Security Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

The TOE protects itself by rejecting replay of communications, avoiding overload of its interfaces, managing sessions, and restricting information released on banners.

The TOE terminates Authenticated User and administrative sessions after a Security Administrator-configurable time interval of inactivity.

7 PROTECTION PROFILE CLAIMS

This section provides the Application-level FW conformance claim statement.

7.1 PP REFERENCES

The TOE demonstrably conforms to the following Application-level FW PP:

- U.S. Government Protection Profile for Application-level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007.

7.2 PP TAILORING

The following tailoring was applied to the Application-level FW PP to produce this ST:

- The names of the security objectives for the environment were changed from the “O.XXX” notation in the Application-level FW PP to “OE.XXX” notation to provide a clearer distinction from the TOE security objectives, which are labeled “O.XXX”;
- T.LOWEXP was reworded as the wording in the PP is consistent with an assumption (and in fact is identical to A.LOWEXP). The rewording reflects the objective that the PP ties the threat to (O.EAL).
- FIA_AFL.1 – Modified to more accurately reflect what the TOE supports, and specifically mention the Security Administrator.
- FIA_ATD.1 - No other security attributes are required to be assigned to administrators;
- FDP_IFF.1.4(1) – removed 1.4 in the PP as it is not in the CC Part 2 v3.1r3. It does not affect the intent of the SFR as the PP assigned “none” to what the TSF shall provide, therefore not having the requirement at all, is equivalent to assigning “none”. Also renumbered 1.5 in the PP to 1.4 in the ST.
- FDP_IFF.1.5(1) – Changed .”do not conform to generally accepted published protocol definitions (e.g. RFCs)” to “match known intrusion signatures”. By matching traffic to known intrusion signatures, the TOE can detect malicious traffic even if it conforms to the generally accepted published protocol definitions. Also renumbered 1.5 in the PP to 1.4 in the ST.
- FDP_IFF.1.3(2) – Added the text as it is not present in the PP and assigned “none” to keep the requirement consistent with the PP.
- FDP_IFF.1.4(2) - Added the text as it is not present in the PP and assigned “none” to keep the requirement consistent with the PP.
- FDP_IFF.1.5(2) – Changed .”do not conform to generally accepted published protocol definitions (e.g. RFCs)” to “match known intrusion signatures”. By

matching traffic to known intrusion signatures, the TOE can detect malicious traffic even if it conforms to the generally accepted published protocol definitions. Also renumbered 1.6 in the PP to 1.5 in the ST.

- FAU_GEN.1 – Changed the table reference to match the number in the ST, instead of that in the PP.
- FAU_SAR.1.2 – The word 'user' was changed to 'administrator' since audit review is restricted to administrators.
- FAU_STG.1 – Updated with the wording in CC Part 2 v3.1r3.
- FMT_MOF.1 – The PP requirement was modified to better specify the specific administrator able to perform the particular type of management.
- FMT_MSA.1 – Explicitly stated that it is the Security Administrator that performs management of security attributes.
- FMT_MSA.3 – Explicitly stated that it is the Security Administrator that can specify alternative initial values.
- FMT_MTD.1 – Explicitly stated that it is the Security Administrator that can set the time.
- FMT_MTD.2 – Explicitly stated that it is the Security Administrator that can specify the number of authentication failures.
- FMT_SMR.1.1 – Expanded the generic "administrator" to the three administrators supported by the TOE: the Security, Cryptographic and Audit Administrators.
- FMT_SMR.1.2 – Reworded to the CC Part 2 v3.1r3 wording to better support FMT_SMR.1.1.
- FPT_STM.1 – removed "for its own use" to match CC Part 2 v3.1r3. The meaning of the SFR is not changed significantly as it is assumed that if the TOE should provide reliable timestamps, that it should be able to use them.

8 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Section 4 and Section 6, respectively. Additionally, this section describes the rationale for satisfying all of the dependencies and the rationale for the TOE security functions.

8.1 RATIONALE FOR SECURITY OBJECTIVES

8.1.1 Overview

Table 9, presents a bi-directional mapping of Assumptions, Threats, and Organizational Policies to Security Objectives for the TOE and for the Environment. In order to allow the reader to ensure that the mapping is complete, each table includes all assumptions, threats and policies. Consequently all rows in a given table do not map to an objective. The tables show that each of the assumptions, threats and organizational policies is addressed by at least one security objective, and that each security objective addresses at least one of the assumptions, threats, or organizational policies. This overview is followed by detailed descriptions and rationale for the mapping to TOE Security Objectives and to the Security Objectives for the Environment.

	O.ACCOUN	O.AUDREC	O.EAL	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.SECFUN	O.SELPRO	O.SINUSE	O.SECSTA	OE.PHYSEC	OE.LOWEXP	OE.GENPUR	OE.PUBLIC	OE.NOEVIL	OE.SINGEN	OE.DIRECT	OE.NOREMO	OE.REMACC	OE.GUIDAN	OE.ADMTRA
A.DIRECT																		X				
A.GENPUR														X								
A.LOWEXP													X									
A.NOEVIL																X						
A.NOREMO																			X			
A.PHYSEC												X										
A.PUBLIC															X							
A.REMACC																				X		
A.SINGEN																	X					
T.ASPOOF							X															
T.AUDACC	X	X																			X	X
T.AUDFUL								X	X													
T.LOWEXP			X																			
T.MEDIAT							X															
T.NOAUTH				X	X	X		X	X		X											
T.OLDINF							X															
T.PROCOM				X																		
T.REPEAT										X												
T.REPLAY								X		X												
T.SELPRO									X		X											
T.TUSAGE																					X	X
P.CRYPTO				X																		

Table 9- Mapping of Security Assumptions, Threats, and Policies to Objectives

8.1.2 TOE Security Objectives Rationale

Table 10 provides detailed descriptions and rationale for the mapping from Security Objectives to Threats and Policies.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.ASPOOF An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal 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, and must ensure that residual information from a previous information flow is not transmitted in any way.	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.
T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	O.AUDREC requires a readable audit trail and a means to search and sort the information contained in the audit trail to increase the probability of audit records being reviewed.
	O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.	O.ACCOUN 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.
T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	O.SELPRO requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions, including, but not limited to audit functionality.
	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	O.SECFUN requires that the TOE provide functionality that ensures that only the authorized administration has access to the TOE security functions.
T.LOWEXP An unauthorized person may attempt to compromise the TOE using obvious penetration attacks requiring minimal attack potential.	O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.	O.EAL requires that the TOE is resistant to penetration attacks performed by an attacker possessing minimal attack potential.
T.MEDIAT An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal 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, and must ensure that residual information from a previous information flow is not transmitted in any way.	O.MEDIAT requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
T.NOAUTH	O.IDAUTH	O.IDAUTH requires that users be uniquely identified

Threat/Policy	Objectives Addressing the Threat	Rationale
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.	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.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. 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. O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality. O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.	before accessing the TOE. O.SECSTA ensures no information is compromised by the TOE upon start-up or recovery. O.ENCRYP requires that an authorized administrator use encryption when performing administrative functions on the TOE remotely. O.SELPRO requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. O.SECFUN requires that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions. O.LIMEXT requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.
T.OLDINF Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.	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, and must ensure that residual information from a previous information flow is not transmitted in any way.	O.MEDIAT requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
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	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.	O.ENCRYP requires that an authorized administrator uses encryption when performing administrative functions on the TOE remotely.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.	O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	O.SINUSE requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
T.REPLAY A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).	O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network. O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	O.SINUSE requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack. O.SECFUN requires that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.
T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.	O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	O.SECSTA ensures that no information is compromised by the TOE upon start-up or recovery. O.SELPRO requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
P.CRYPTO AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).	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.	O.ENCRYP requires that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

Table 10 - Security Objectives to Threats and Policies Mappings

8.1.3 Operational Environment Security Objectives Rationale

Table 11 provides detailed descriptions and rationale for the mapping from Security Objectives to Threats and Policies. Where relevant, the objectives are also mapped to the Security Functional Requirements for the Environment.

Assumption	Objectives Addressing the Assumption	Rationale
A.PHYSEC The TOE is physically secure.	OE.PHYSEC The TOE is physically secure.	
A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	OE.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	
A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.	OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.	
A.PUBLIC The TOE does not host public data.	OE.PUBLIC The TOE does not host public data.	
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	
A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	
A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.	OE.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.	
A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.	OE.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.	
A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.	OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.	
T.AUDACC	OE.GUIDAN	OE.GUIDAN requires that those responsible for the

Assumption	Objectives Addressing the Assumption	Rationale
Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.	The TOE must be delivered, installed, administered, and operated in a manner that maintains security. OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.	TOE ensure that it is delivered, installed, administered, and operated in a secure manner. O.ADMTRA ensures that authorized administrators receive the proper training.
T.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.	OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security. OE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.	OE.GUIDAN requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner. O.ADMTRA ensures that authorized administrators receive the proper training.

Table 11 – Rationale for Operational Environment Security Objectives

8.2 RATIONALE FOR TOE SECURITY REQUIREMENTS

Table 12 provides a bi-directional mapping of Security Functional Requirements and Security Assurance Requirements to Security Objectives. It shows that each of the objectives for the TOE is addressed by at least one of the functional or assurance requirements, and that each of the functional and assurance requirements addresses at least one of the objectives for the TOE.

	O.ACCOUN	O.AUDREC	O.EAL	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE
FAU_GEN.1	X	X									
FAU_SAR.1		X									
FAU_SAR.3		X									
FAU_STG.1.								X	X	X	
FAU_STG.4								X	X	X	
FCS_CKM.1			X	X							
FCS_CKM.4			X	X							
FCS_COP.1			X	X							
FDP_IFC.1(1)							X				
FDP_IFC.1(2)							X				
FDP_IFF.1(1)							X				
FDP_IFF.1(2)							X				
FDP_RIP.1							X				
FIA_AFL.1										X	
FIA_ATD.1					X			X			
FIA_UAU.1										X	
FIA_UAU.5					X						X
FIA_UID.2	X				X						
FMT_MOF.1(1)						X		X	X		

	O.ACCOUN	O.AUDREC	O.EAL	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE
FMT_MOF.1(2)						X		X	X		
FMT_MSA.1(1)							X	X	X		
FMT_MSA.1(2)							X	X	X		
FMT_MSA.1(3)							X	X	X		
FMT_MSA.1(4)							X	X	X		
FMT_MSA.3							X		X		
FMT_MTD.1(1)								X			
FMT_MTD.1(2)								X			
FMT_MTD.2								X			
FMT_SMR.1								X			
FPT_STM.1		X									
ADV_ARC.1									X	X	

Table 12 - Security Requirements Rationale Summary

Table 13 provides detailed descriptions and rationale for the mapping from Security Objectives to TOE Security Functional Requirements.

Objective	Requirements Addressing the Objective	Rationale
O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.	FAU_GEN.1 FIA_UID.2	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FIA_UID.2 ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE.
O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.	FAU_SAR.3 FAU_SAR.1 FPT_STM.1 FAU_GEN.1	FAU_SAR.1 provides the administrators with the capability to read all the audit data contained in the audit trail. This requirement also mandates the audit information be presented in a manner that is suitable for the administrators to interpret the audit trail, which is subject to interpretation. It is expected that the audit information be presented in such a way that the administrators can examine an audit record and have the appropriate information presented together to facilitate the analysis of the audit review. FAU_SAR.3 complements FAU_SAR.1 by providing the administrators the flexibility to specify criteria that can be used to search or sort the audit records residing in the audit trail. FAU_SAR.3 requires the administrators be able to establish the audit review criteria based on a userid and source subject identity, so that the actions of a user can be readily identified and analyzed. The criteria also includes a destination subject identity so the administrators can determine what network traffic is destined for an individual machine. Allowing the administrators to perform searches or sort the audit records based on dates, times, subject identities, destination service identifier, or transport layer protocol provides the capability to extract the network activity to what is pertinent at that time in order facilitate the administrator's review. Being able to search on the destination service identifier affords the administrators the opportunity to see what traffic is destined for a service (e.g., TCP port) or set of services regardless of where the traffic originated. It is important to note that the intent of sorting

Objective	Requirements Addressing the Objective	Rationale
		in this requirement is to allow the administrators the capability to organize or group the records associated with a given criteria. For example, if the administrators wanted to see what network traffic was destined for the set of TCP ports 1-1024, they would be able to have the audit data presented in such a way that all the traffic for TCP port 1 was grouped together, all the traffic for port 2 was grouped together and so on. The criteria includes the rule identity that determines whether a packet was allowed or denied to flow. This provides the administrators to determine what network traffic a given rule is governing. FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FPT_STM.1 is a dependency of FAU_GEN.1 to ensure that the date and time on the TOE is dependable, which is important for the audit trail.
O.EAL The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.	FCS_COP.1 FCS_CKM.1 FCS_CKM.4	FCS_COP.1 ensures that the TOE supports cryptographic operations that are necessary in order for the TOE to be resistant to obvious vulnerabilities. It also ensures that the TOE has been evaluated to FIPS 140-2 level 1 or greater. FCS_CKM.1 and FCS_CKM.4 support FCS_COP.1 as they are dependencies to ensure proper generation and destruction of keys used by FCS_COP.1.
O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption.	FCS_COP.1 FCS_CKM.1 FCS_CKM.4	FCS_COP.1 ensures that the TOE supports cryptographic operations that are necessary to protect the confidentiality of its dialogue with an authorized administrator through encryption. It also ensures that the TOE has been evaluated to FIPS 140-2 level 1 or greater. FCS_CKM.1 and FCS_CKM.4 support FCS_COP.1 as they are dependencies to ensure proper generation and destruction of keys used by FCS_COP.1.
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.	FIA_UAU.5 FIA_ATD.1 FIA_UID.2	Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process before anything occurs on behalf of that user [FIA_UID.2, FIA_UAU.5].
O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.	FMT_MOF.1(1), FMT_MOF.1(2)	FMT_MOF.1 ensures that the TSF restricts the ability to modify the behaviour of functions such as audit trail management, back and restore for TSF data, communication of authorized external IT entities with the TOE, start-up and shutdown operation and multiple authentication function to an authorized administrator.

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, and must ensure that residual information from a previous information flow is not transmitted in any way.
	FDP_IFF.1(1) , FDP_IFF.1(2)
	FDP_IFC.1(1), FDP_IFC.1(2)
	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3),
		The FDP_IFF and FDP_IFC requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place.
		FDP_IFC.1(1) and FDP_IFC.1(2) define the subjects, information (e.g., objects) and the operations that are performed with respect to the two information flow policies.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1(4) FMT_MSA.3	FMT_MSA.1(1) and FMT_MSA.1(2) ensures the TSF enforces the UNAUTHENTICATED and AUTHENTICATED SFPs to restrict the ability to delete, modify, and add within a rule those specified security attributes that are listed in section FDP_IFF1.1. FMT_MSA.1(3) and FMT_MSA.1(4) ensures the TSF enforces the UNAUTHENTICATED and AUTHENTICATED SFPs to restrict the ability to create or delete rules for security attributes that are listed in FDP_IFF.1. FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules.
O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	FAU_STG.1 FAU_STG.4 FIA_ATD.1 FMT_MOF.1(1), FMT_MOF.1(2) FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4) FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.2 FMT_SMR.1	FAU_STG.1 ensures that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full. It also ensures that no other auditable events as defied in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions through these events will not be recorded until the audit trail is restored to a non-full status. FIA_ATD.1 provides users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. FMT_MOF.1 ensures the TSF restricts the ability of the TOE start-up and shutdown operation, multiple authentication function, audit trail management, back and restore for TSF data and communication of authorized external IT entities with the TOE to an authorized administrator. FMT_MSA.1 ensures the TSF enforces the UNAUTHENTICATED and AUTHENTICATED SFPs to restrict the ability to modify security attributes that are listed in FDP_IFF.1(1) for UNAUTHENTICATED and FDP_IFF.1(2) for AUTHENTICATED. FMT_MTD.1 ensures that the TSF restrict abilities to manipulate certain user attributes as defined in FIA_ATD.1.1 and time and date to only the authorized administrator. FMT_MTD.2 ensures that the TSF restrict the specification of limits on the number of unauthenticated failures to the authorized administrator and specifies the action to be taken if limits on the TSF data are reached or exceeded. FMT_SMR.1 supports each of the FMT components that depend on it. It requires roles to be chosen.
O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected	FAU_STG.1 FAU_STG.4 FMT_MOF.1(1),	FAU_STG.1 ensures that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. FAU_STG.4 ensures that the authorized administrator will be able

Objective	Requirements Addressing the Objective	Rationale

network.	FMT_MOF.1(2)
	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4)
	FMT_MSA.3
	ADV_ARC.1
		to take care of the audit trail if it should become full. It also ensures that no other auditable events as defied in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions through these events will not be recorded until the audit trail is restored to a non-full status.
		FMT_MOF.1 ensures the TSF restricts the ability of the TOE start-up and shutdown operation, multiple authentication function, audit trail management, back and restore for TSF data and communication of authorized external IT entities with the TOE to an authorized administrator.
		FMT_MSA.1 ensures the TSF enforces the UNAUTHENTICATED and AUTHENTICATED SFPs to restrict the ability to modify security attributes that are listed in FDP_IFF.1(1) for UNAUTHENTICATED and FDP_IFF.1(2) for AUTHENTICATED.
		FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules.
		ADV_ARC.1 must describe how the architecture ensures that the TSF are always invoked.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	FAU_STG.1 FAU_STG.4 FIA_AFL.1 FIA_UAU.1 ADV_ARC.1	FAU_STG.1 ensures that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full. It also ensures that no other auditable events as defied in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions through these events will not be recorded until the audit trail is restored to a non-full status. FIA_AFL.1 ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. FIA_UAU.1 is a dependency if FIA_AFL.1 and therefore supports FIA_AFL.1 ADV_ARC.1 must describe how the architecture ensures that the TSF are always invoked.
O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	FIA_UAU.5	FIA_UAU.5 ensures that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network.

Table 13 - Rationale for TOE Security Requirements

8.3 RATIONALE FOR ASSURANCE REQUIREMENTS

The selection of the EAL2+ level of assurance was made by Fortinet, Incorporated, in response to the needs of prospective clients.

8.4 RATIONALE FOR DEPENDENCIES

8.4.1 Rationale for Satisfying Functional Requirement Dependencies

Table 14 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. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FAU_GEN.1	FPT_STM.1	Yes	FPT_STM.1 is in the ST
FAU_SAR.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_SAR.3	FAU_SAR.1	Yes	FAU_SAR.1 is in the ST
FAU_STG.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_STG.4	FAU_STG.1	Yes	FAU_STG.2 is hierarchical and is in the ST
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[No Yes] Yes	FCS_COP.1 and FCS_CKM.4 are in the ST
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[No No Yes]	FCS_CKM.1 is in the ST
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[No No Yes] Yes	FCS_CKM.1 and FCS_CKM.4 are in the ST
FDP_IFC.1	FDP_IFF.1	Yes	FDP_IFF.1(1), FDP_IFF.1(2) are in the ST

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes	FDP_IFC.1(1), FDP_IFC.1(2) are in the ST FMT_MSA.3 is in the ST
FDP_RIP.1	None	N/A	
FIA_AFL.1	FIA_UAU.1	Yes	While this dependency was not met by the PP, it has been added to this ST.
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical and is in the ST
FIA_UAU.5	None	N/A	
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	No Yes	See note below FMT_SMR.2 is hierarchical and is in the ST
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	[No Yes] No Yes	 FDP_IFC.1 is in the ST See note below FMT_SMR.2 is hierarchical and is in the ST
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes	FMT_MSA.1 is in the ST FMT_SMR.2 is hierarchical and is in the ST
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	No Yes	See note below FMT_SMR.2 is hierarchical and is in the ST
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	Yes Yes	FMT_MTD.1 is in the ST FMT_SMR.2 is hierarchical and is in the ST
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical and is in the ST
FPT_STM.1	None	N/A	

Table 14 - Security Functional Requirement Dependencies

Note: Although the FMT_SMF.1 requirement is a dependency of FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1, it has not been included in this ST. The requirements FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 express the functionality required by the TSF to provide the specified functions to manage TSF data, security attributes and management functions. These requirements make it clear that the TSF has to provide the functions to manage the identified data, attributes and functions. Therefore FMT_SMF.1 is not necessary.

8.5 TOE SUMMARY SPECIFICATION RATIONALE

Table 15 provides a bi-directional mapping of Security Functions to Security Functional Requirements from the CC Part 2. Table 16 demonstrates how the TOE meets each SFR.

	F.ADMIN	F.AUDIT	F.CRYPTO	F.I&A	F.IFC	F.PROTECT
FAU_GEN.1		X				
FAU_SAR.1	X	X				
FAU_SAR.3		X				
FAU_STG.1	X	X				X
FAU_STG.4	X	X				X
FCS_CKM.1			X			
FCS_CKM.4			X			
FCS_COP.1			X			
FDP_IFC.1(1)					X	
FDP_IFC.1(2)					X	
FDP_IFF.1(1)	X				X	
FDP_IFF.1(2)	X				X	
FDP_RIP.1						X
FIA_AFL.1	X			X		
FIA_ATD.1	X			X		
FIA_UAU.1	X			X		
FIA_UAU.5				X		
FIA_UID.2				X		
FMT_MOF.1(1)	X					
FMT_MOF.1(2)	X					
FMT_MSA.1(1)	X					
FMT_MSA.1(2)	X					
FMT_MSA.1(3)	X					
FMT_MSA.1(4)	X					

	F.ADMIN	F.AUDIT	F.CRYPTO	F.I&A	F.IFC	F.PROTECT
FMT_MSA.3	X				X	
FMT_MTD.1(1)	X					
FMT_MTD.1(2)	X					
FMT_MTD.2	X					
FMT_SMR.1	X					
FPT_STM.1						X

Table 15 - Mapping of Security Functions to SFRs from CC Part 2

Security Functional Requirement	TOE Security Function	Rationale
FAU_GEN.1 - Audit data generation	F.AUDIT	The TOE generates audit records for the start-up and shutdown of the audit function and all of the events defined in Table 7. The TOE generates timestamps for all audit events and records the timestamp with each audit record. Also recorded are the type of event, identity of the user or subject which caused the event (if applicable), outcome of the event and any additional information listed in the third column of Table 7. Standard audit records are 512 bytes in length. If an audit record exceeds 512 bytes, it is wrapped into a second 512 byte audit record to ensure no audit detail is lost. The TOE has 8 different classes of audit records: • Event log – includes all system level events such as identification, authentication, configuration changes, audit record deletion, etc; • Traffic log – includes all data flow decisions, source/destination information, etc;

Security Functional Requirement	TOE Security Function	Rationale
		• Attack log – includes any IPS or local protection events such as DoS events, etc; (not part of evaluated configuration) • Web filter log (not part of evaluated configuration); • Antispam log (not part of evaluated configuration); • Antivirus log – includes any AV related events such as the detection of an infected file and the action taken; (not part of evaluated configuration); • IM/P2P log (not part of evaluated configuration); and • VoIP log (not part of evaluated configuration). Application Note: It is not possible to start-up and shutdown the auditing function independently of the TOE. However since the TOE writes audit records for the start-up and termination of each TOE subprocess (daemon), the audit trail will contain records which show the start-up and shutdown of the auditing function coincident with the start-up and shutdown of the TOE itself.
FAU_SAR.1 - Audit review	F.AUDIT F.ADMIN	All administrative roles have read access to the audits records (Security Administrator, Audit Administrator and Crypto Administrator). The audit records can be accessed through the Local Console, Network CLI, and the Network Web-based GUI. When using the Network Web-Based GUI, administrators can view all audit records either as raw data (all columns) or as a filtered subset of columns. Filtered audit records (columns and rows) can be viewed through the Local Console or Network CLI. Administrators can modify the filters to change the view of the audit records. The number of records to display at one time can also be specified.
FAU_SAR.3 - Selectable audit review	F.AUDIT	The TOE supports selectable review (display) of audit data through the Local Console or the Network CLI. Log data can be filtered for display. Specific audit information can be specified as part of the filter. For example, the administrator could execute a CLI command to filter (list) all audit records with a specific source IP or all records between 2 dates. Filter criteria include (but are not limited

Security Functional Requirement	TOE Security Function	Rationale
		to): • user identification (including a range of users); • source subject identity; • destination subject identity; • dates and times (from/to, included/excluded); • a range of one or more subject service identifiers; • a range of one of more transport layer protocols; • firewall rule identity; • TOE network interface; • log severity level (information, alert, emergency, critical, error, warning, notification, debug); and • action (accept, deny).
FAU_STG.1 - Protected audit trail storage	F.AUDIT F.ADMIN F.PROTECT	Deletion of individual audit records, sets of audit records, and the audit logs themselves is restricted to administrators with the Audit Administrator role. No user (administrative or otherwise) has the ability to modify the records in the audit logs.
FAU_STG.4 - Site-Configurable Prevention of Audit Loss	F.ADMIN F.AUDIT F.PROTECT	The TOE supports three different Security Administrator settable actions to prevent loss of audit data: • Shut down network interfaces (default action); • Overwrite audit records (FIFO); and • Stop logging The enabled action is taken once the log storage device reaches 95% capacity. If the “shut down network interfaces” option is enabled, the TOE enters an error mode in addition to shutting down the network interfaces. The Security Administrator must clear the error mode by freeing space on the log storage device using the Local Console connection. By taking action when the log size reaches 95% of log storage capacity, the TOE ensures that the Security Administrator actions taken in order to resolve the log storage problem are themselves logged and that no

Security Functional Requirement	TOE Security Function	Rationale
		audit records are lost. Application Note: Administrative guidance is provided which informs the Security Administrator that only the first option is permitted in the evaluated configuration of the TOE.
FCS_CKM.1	F.CRYPTO	The TOE generates AES keys of at least 128 binary digits in length to support the encryption of remote authorized administrator sessions using HTTPS for web interface based administration and SSH for commandline interface based administration.
FCS_CKM.4	F.CRYPTO	The TOE destroys AES keys by zeroizing them when they are no longer needed for the encryption of remote authorized administrator sessions using HTTPS for web interface based administration and SSH for commandline interface based administration.
FCS_COP.1 – Cryptographic operation	F.CRYPTO	The TOE performs encryption of remote authorized administrator sessions using HTTPS for web interface based administration and SSH for commandline interface based administration. The AES algorithm is used for these two protocols with a key of at least 128 binary digits in length. The algorithm meets FIPS PUB 140-2.
FDP_IFC.1(1) - Subset information flow control (unauthenticated policy)	F.IFC	The TOE permits the Security Administrator to define firewall rules which determine whether or not the TOE permits information (packets) to flow through the TOE without authentication of the user sending the information. The TOE may permit two general types of unauthenticated information flow: • Information flow through the TOE from a source to a destination; and • SMTP information flow via an application proxy. For information which flows via an application proxy, the TOE ensures that the connection from the source terminates at the TOE and that the connection between the TOE and the destination does not include any of the stateful protocol attributes associated with the subject. The Security Administrators may define firewall rules which permit (or deny) the flow of information based upon (but not limited to) the following criteria:

Security Functional Requirement	TOE Security Function	Rationale
		• The TOE interface, VLAN or VDOM which originates the information flow (the source subject); • The TOE interface, VLAN or VDOM which is the destination of the information flow (the destination subject); and • The information contained within the information flow (packet contents).
FDP_IFC.1(2) - Subset information flow control (authenticated policy)	F.IFC	The TOE permits the Security Administrator to define firewall rules which determine whether or not the TOE permits information (packets) to flow through the TOE without authentication of the user sending the information. The TOE may permit two general types of unauthenticated information flow: • Information flow through the TOE from a source to a destination; and • SMTP information flow via an application proxy. For information which flows via an application proxy, the TOE ensures that the connection from the source terminates at the TOE and that the connection between the TOE and the destination does not include any of the stateful protocol attributes associated with the subject. The Security Administrators may define firewall rules which permit (or deny) the flow of information based upon (but not limited to) the following criteria: • The TOE interface, VLAN or VDOM which originates the information flow (the source subject); • The TOE interface, VLAN or VDOM which is the destination of the information flow (the destination subject); and • The information contained within the information flow (packet contents).
FDP_IFF.1(1) - Simple security attributes (unauthenticated policy)	F.ADMIN F.IFC	The TOE provides the Security Administrator with the ability to define a set of firewall rules which determine whether or not the TOE permits an information flow. The Security Administrator has the ability to specify the order

Security Functional Requirement	TOE Security Function	Rationale
		in which the firewall rules are applied to requested information flows. The first rule which explicitly applies to the requested information flow is used to determine whether or not the information flow is accepted or rejected. If there are no rules which explicitly apply to the requested information flow, the information flow is rejected. The TOE also provides tools which allow the Security Administrator to view information flows allowed by the set of defined firewall rules before applying the ruleset. The criteria that the Security Administrator may use in order to define a firewall rule are listed in Section 5 of this document under FDP_IFF.1.1(1). The TOE completely reassembles fragmented packets before applying the firewall policy rules to the packets. The TOE implements stateful packet inspection rules in that each, non-fragmented, packet that is received by the TOE is either associated with an existing allowed connection, or is considered as an attempt to establish a new connection and therefore subject to the firewall rules. Regardless of other firewall rules, the TOE will deny an information flow if: • The source of the information flow is a broadcast identity; • The source if the information flow is a loopback identifier; • The information flow specifies the route of information flow from the source subject to the destination subject; and The information flow is SMTP traffic that includes source routing symbols.
FDP_IFF.1(2) - Simple security attributes (authenticated policy)	F.ADMIN F.IFC	The TOE provides the Security Administrator with the ability to define a set of firewall rules which determine whether or not the TOE requires authentication in order to access an application proxy for a specific transport-layer protocol. The Security Administrator has the ability to specify the order in which the firewall rules are applied to requested information flows. The first rule which explicitly applies to the application proxy request is used to determine whether or not the request is accepted or rejected. If there are no rules which explicitly apply to the requested application proxy, the request is rejected. The TOE also provides tools which allow the Security

Security Functional Requirement	TOE Security Function	Rationale
		Administrator to view information flows allowed by the set of defined firewall rules before applying the ruleset. The criteria that the Security Administrator may use in order to define a firewall rule for access to an application proxy which requires authentication are listed in Section 5 of this document under FDP_IFF.1.1(2). The TOE completely reassembles fragmented packets before applying the firewall policy rules to the packets. The TOE implements stateful packet inspection rules in that each, non-fragmented, packet that is received by the TOE is either associated with an existing allowed connection, or is considered as an attempt to establish a new connection and therefore subject to the firewall rules.
FDP_RIP.1 - Subset residual information protection	F.PROTECT	Users of the TOE do not have access to any of the TOE's resources. Users do not have access to the file system maintained by the TOE and there are no operating system commands which provide access to either memory or the file system. The only resource provided by the TOE to users, is the information content of packets transmitted by the TOE. Packets transmitted by the TOE are assembled in memory which has been overwritten by the TOE before allocation to the packet. This ensures that any previous information content of the memory is not revealed.
FIA_AFL.1- Authentication failure handling	F.ADMIN F.I&A	The TOE generates an alarm indicating a possible security violation when the number of consecutive unsuccessful attempts to establish a remote session, by a given user account, exceeds a maximum limit. The maximum limit is set by the Security Administrator. In addition to the generation of an alarm, the Security Administrator can specify whether or not exceeding the maximum number of login attempts results in the account becoming locked. If the Security Administrator specifies that the account does become locked, the Security Administrator also specifies the period of time for which the account is locked. Once a user account has been locked, that user may not establish a remote session with the TOE until the lockout time period has expired or the Security Administrator has taken action to unlock the account. Application Note: The authentication failure limits apply to remote administrator authentication attempts and proxy

Security Functional Requirement	TOE Security Function	Rationale
		user authentication attempts. The TOE does not enforce an authentication limit for the Local Console.
FIA_ATD.1 - User attribute definition	F.ADMIN F.I&A	For each Administrator account maintained by the TOE, the following information is recorded: • The user identifier (user name); and • The administrative role associated with the user identifier (Security Administrator, Audit Administrator, Cryptographic Administrator)..
FIA_UAU.1- Timing of authentication	F.ADMIN F.I&A	The TOE allows information to flow according to the UNAUTHENTICATED SFP before requiring authentication to be performed. The TOE requires user authentication before taking any AUTHENTICATED SFP information flows or management functions.
FIA_UAU.5 - Authentication mechanism	F.I&A	The TOE provides a local password mechanism as well as integration with RADIUS to perform a single-use authentication..
FIA_UID.2 - User identification before any action	F.I&A	The TOE requires user identification before taking any action on behalf of a user (information flow or TOE services). For authenticated users (administrators and proxy users) a user name is provided during the authentication process. For unauthenticated users, the Network Interface on which information is received by the TOE is considered to be the user identification.
FMT_MOF.1(1) – Management of security functions behavior (on/off)	F.ADMIN	The Security Administrator can perform start-up and shutdown and enable and disable multiple use authentication functions described in FIA_UAU.5.
FMT_MOF.1(2) – Management of security functions behavior (modify)	F.ADMIN	The Security Administrator can enable and disable external IT entities from communicating to the TOE and perform audit trail management. Backup and restore of TSF data, information flow rules, and audit trail data is excluded from the evaluated configuration of the TOE.
FMT_MSA.1(1) - Management of security attributes (unauthenticated attributes)	F.ADMIN	Only the Security Administrator can specify the attributes which are used to define the firewall rules which implement the security functional policies described in this document. For details of the attributes which may be specified by the Security Administrator for each of the security functional policies refer to the iterations of the FDP_IFF.1 requirement in Section 5.

Security Functional Requirement	TOE Security Function	Rationale
FMT_MSA.1(2) - Management of security attributes (authenticated attributes)	F.ADMIN	Only the Security Administrator can specify the attributes which are used to define the firewall rules which implement the security functional policies described in this document. For details of the attributes which may be specified by the Security Administrator for each of the security functional policies refer to the iterations of the FDP_IFF.1 requirement in Section 5.
FMT_MSA.1(3) - Management of security attributes (unauthenticated rules)	F.ADMIN	Only the Security Administrator can specify the attributes which are used to define the firewall rules which implement the security functional policies described in this document. For details of the attributes which may be specified by the Security Administrator for each of the security functional policies refer to the iterations of the FDP_IFF.1 requirement in Section 5.
FMT_MSA.1(4) - Management of security attributes (authenticated rules)	F.ADMIN	Only the Security Administrator can specify the attributes which are used to define the firewall rules which implement the security functional policies described in this document. For details of the attributes which may be specified by the Security Administrator for each of the security functional policies refer to the iterations of the FDP_IFF.1 requirement in Section 5.
FMT_MSA.3 - Static attribute initialization	F.IFC F.ADMIN	The TOE implements two security functional policies for information flow control; the UNAUTHENTICATED SFP security functional policy and the AUTHENTICATED SFP security functional policy. These policies are implemented in the TOE via a set of firewall rules which determine which information flows are permitted by the TOE. By default, in the evaluated configuration, no firewall rules are defined and therefore no traffic can flow through the TOE. The absence of any firewall rules in the default configuration is considered to be 'restrictive default values'. The Security Administrator can modify the default configuration of the TOE by creating firewall rules which determine what traffic is allowed to flow through the TOE. The specification of firewall rules by the Security Administrator is considered to be the specification of 'alternative initial values to override the default values'.
FMT_MTD.1(1) - Management of TSF data (user attributes)	F.ADMIN	Only the Security Administrator has the ability to create and subsequently modify user accounts. User accounts include all administrative accounts (Security Administrator, Audit Administrator and Cryptographic Administrator) as well as proxy user accounts.

Security Functional Requirement	TOE Security Function	Rationale
FMT_MTD.1(2) - Management of TSF data (time data)	F.ADMIN	Only the Security Administrator has the ability to modify the time and date setting of the TOE's hardware clock.
FMT_MTD.2 - Management of limits on TSF data	F.ADMIN	The Security Administrator is responsible for the specification of the limits for the number of authentication failures. The lockout is set for a period of time, as set by the Security Administrator.
FMT_SMR.1 - Security roles	F.ADMIN	The TOE maintains the following three roles: • Security Administrator; • Cryptographic Administrator; and • Audit Administrator. All user identities that are associated with one of the administrative roles are able to establish an administrative session via the Local Console, the Network Web-Based GUI and the Network CLI. All administrative roles are distinct in that there is no overlap of operations performed by each role, except: • all administrators are able to review the audit trail; and • all administrators are able to invoke self-tests (cryptographic and non-cryptographic).
FPT_STM.1 - Reliable time stamps	F.AUDIT F.PROTECT	The TOE includes 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 the System Administrator and all such modifications are recorded in the audit log. The integrity of the hardware clock is verified during the TOE self-tests.

Table 16 - TOE Security Functions Rationale

9 REFERENCES

1) Common Criteria for Information Technology Security Evaluation Part 1*:* Introduction and general model, *Version 3.1 Revision 3, July 2009*

2) Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, *Version 3.1 Release 3, July 2009*

3) Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, *Version 3.1 Release 3, July 2009*

4) Common Methodology for Information Technology Security Evaluation, Evaluation methodology*, Version 3.1 Revision 3, July 2009*

5) *Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510,* Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG), *June 2000*.

6) U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, *Version 1.4, May 1, 2000.*

7) U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments, *Version 1.1, December 2001*.

8) Information Assurance Technical Framework, *Version 3.0, September 2000.*

9) *Federal Information Processing Standard Publication (FIPS-PUB) 46-3,* Data Encryption Standard (DES), *October 1999.*

10) *Federal Information Processing Standard Publication (FIPS-PUB) 140-2,* Security Requirements for Cryptographic Modules, *May 25, 2001*.

11) *Internet Engineering Task Force*, IP Encapsulating Security Payload (ESP), *RFC 2406, November 1998.*

12) *Internet Engineering Task Force,* Internet Key Exchange (IKE), *RFC 2409, November 1998.*

13) *Internet Engineering Task Force,* ESP CBC-Mode Cipher Algorithms, *RFC 2451, November 1998.*

14) *Internet Engineering Task Force,* Use of HMAC-SHA-1-96 within ESP and AH, *RFC 2404, November 1998.*

15) *Department of Defense Directive, Information Assurance,* 8500.1, October 24, 2002.

16) *Department of Defense Instruction, Information Assurance Implementation,* 8500.2, February 6, 2003.

17) *The AES Cipher Algorithm and Its Use with IPSec* <draft-ietf-ipsec-ciph-aes-cbc.03.txt>, Internet draft, November 2001.

18) *Federal Information Processing Standard Publication (FIPS-PUB) 197,* Specification for the Advanced Encryption Standard (AES), *November 26, 2001*

19) *NSA Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

10 TERMINOLOGY

In the Common Criteria, many terms are defined in Section 4 of Part 1. The following are a definitions of terms used in this ST and common to the U.S. Government Application-level Firewall Protection Profile for Basic Robustness Environments, as well as other DoD PPs.

Access -- Interaction between an entity and an object that results in the flow or modification of data.

Access Control -- Security service that controls the use of resources[4] and the disclosure and modification of data[5].

Accountability --Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator -- A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance -- A measure of confidence that the security features of an IT system are sufficient to enforce it's' security policy.

Asymmetric Cryptographic System -- A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key -- The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system.

Attack -- An intentional act attempting to violate the security policy of an IT system.

Authentication -- Security measure that verifies a claimed identity.

Authentication data -- Information used to verify a claimed identity.

Authorization -- Permission, granted by an entity authorized to do so, to perform functions and access data.

[4] Hardware and software

[5] Stored or communicated

Authorized user -- An authenticated user who may, in accordance with the TSP, perform an operation.

Availability -- Timely[6], reliable access to IT resources.

Compromise -- Violation of a security policy.

Confidentiality -- A security policy pertaining to disclosure of data.

Critical Security Parameters (CSP) -- Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic Administrator -- An authorized user who has been granted the authority to perform cryptographic initialization and management functions. These users are expected to use this authority only in the manner prescribed by the guidance given to them.

Cryptographic boundary -- An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.

Cryptographic key (key) -- A parameter used in conjunction with a cryptographic algorithm that determines [7]:

- the transformation of plaintext data into ciphertext data,
- the transformation of cipher text data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a data authentication code computed from data.

Cryptographic Module -- The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptographic Module Security Policy -- A precise specification of the security rules under which a cryptographic module must operate, including the rules derived from the requirements of this ST and additional rules imposed by the vendor.

[6] According to a defined metric

Defense-in-Depth (DID) --A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Discretionary Access Control (DAC) -- A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. These controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

DMZ --A Demilitarized Zone (DMZ) is a network that is mediated by the TOE but, as a result of less stringent access controls, provides access to publicly available services, such as web servers.

Embedded Cryptographic Module -- One that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).

Enclave -- A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity -- A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

External IT entity -- Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Identity -- A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity -- A security policy pertaining to the corruption of data and TSF mechanisms.

Integrity label --A security attribute that represents the integrity level of a subject or an object. Integrity labels are used by the TOE as the basis for mandatory integrity control decisions.

Integrity level -- The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of data.

Mandatory Access Control (MAC) -- A means of restricting access to objects based on subject and object sensitivity labels[7].

Mandatory Integrity Control (MIC) -- A means of restricting access to objects based on subject and object integrity labels.

[7] The Bell LaPadula model is an example of Mandatory Access Control

Multilevel -- The ability to simultaneously handle (e.g., share, process) multiple levels of data, while allowing users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access.

Named Object[8] -- An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to request a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

Non-Repudiation -- A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

Object -- An entity within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment --The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Operating System (OS) -- An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

Operational key -- Key intended for protection of operational information or for the production or secure electrical transmissions of key streams.

Peer TOEs -- Mutually authenticated TOEs that interact to enforce a common security policy.

Public Object -- An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

[8] The only named objects in this ST are operating system controlled files.

Robustness -- A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

- **Basic:** Security services and mechanisms that equate to good commercial practices.
- **Medium:** Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.
- **High:** Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State -- Condition in which all TOE security policies are enforced.

Security attributes -- TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.

Security level -- The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity on the information [10].

Sensitivity label -- A security attribute that represents the security level of an object and that describes the sensitivity (e.g. Classification) of the data in the object. Sensitivity labels are used by the TOE as the basis for mandatory access control decisions [10].

Split key -- A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables.

Subject -- An entity within the TSC that causes operations to be performed.

Symmetric key -- A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.

Threat -- Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent - Any human user or Information Technology (IT) product or system which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

User --Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Vulnerability -- A weakness that can be exploited to violate the TOE security policy.

11 ACRONYMS, ABBREVIATIONS, AND INITIALIZATIONS

The following acronyms, abbreviations, and initializations are used in this Security Target:

AES	Advanced Encryption Standard
AH	Authenticating Header
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
AV	Anti-Virus
BGP	Border Gateway Protocol
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DAC	Discretionary Access Control
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DID	Defense In Depth
DMZ	Demilitarized zone
DNS	Domain Name System
DoD	Department of Defense

DoS	Denial of Service
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FGCP	FortiGate Clustering Protocol
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
FW	Firewall
GIG	Global Information Grid
GUI	Graphical user interface
HMI	Human-Machine Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol (Secure)
I&A	Identification and Authentication
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IDSS	Intrusion Detection System Sensor
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IP	Internet Protocol

IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IT	Information Technology
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MIC	Mandatory Integrity Control
MIME	Multipurpose Internet Mail Extensions
N/A	Not Applicable
NAT	Network Address Translation
NBIAT&S	Network Boundary Information Assurance Technologies and Solutions Support
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OS	Operating System
P2P	Peer to Peer
OSPF	Open Shortest Path First
PIN	Private Identification Number
POP3	Post Office Protocol Version 3
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service

PP	Protection Profile
RFC	Request for Comments
RIP	Routing Information Protocol
RNG	Random Number Generator
ROBO	Remote Office or Branch Office
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TBD	To Be Determined
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TFFW	Traffic Filter Firewall
TFS	Terminal Final State
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TP	Transparent (Mode)
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSFI	TSF Interface

TSP	TOE Security Policy
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDOM	Virtual Domain
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

--- End of Document ---