SECURITY TARGET

FOR

FORTINET FORTIGATE™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B AND FORTIWIFI-50B, 60C AND 80CM UNIFIED THREAT MANAGEMENT SOLUTIONS AND FORTIOS 4.0 CC COMPLIANT FIRMWARE

Document No. 1660-011-D002

Version: 2.1, 6 December 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

SECURITY TARGET

FOR

FORTINET FORTIGATE™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B AND FORTIWIFI-50B, 60C AND 80CM UNIFIED THREAT MANAGEMENT SOLUTIONS AND FORTIOS 4.0 CC COMPLIANT FIRMWARE

Document No. 1660-011-D002

Version: 2.1, 6 December 2011

<Original> Approved by:

Project Engineer:	T. MacArthur	6 December 2011
Project Manager:	M. Gauvreau	6 December 2011
Program Director:	E. Connor	6 December 2011
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

This document, version 2.1, dated 6 December 2011, is the Security Target for the Fortinet FortiGate™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B and FortiWiFi-50B, 60C and 80CM Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware.

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation for this Security Target is identified in Table 1.

The Fortinet FortiGate™ 50B, 60C, 80C, 110C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, 5001SX, 5001A-DW, 5001A-SW, 5001B and FortiWiFi-50B, 60C and 80CM Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware is a combined hardware and software TOE.

Product	Firmware[1] Version	Hardware Version[2]	FIPS 140-2 Certificate Number
FortiGate-50B	Build 8892,111128	C5GB38	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-60C	Build 8892,111128	C4DM93	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-80C	Build 8892,111128	C4BC61	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-110C	Build 8892,111128	C4HA15	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-200B	Build 8892,111128	C4CD24	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-310B	Build 8892,111128	C4ZF35	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-311B	Build 8892,111128	C4CI39	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-620B	Build 8892,111128	C4AK26	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-1000A	Build 8892,111128	C4WA49	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-1240B	Build 8892,111128	C4CN43	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-3016B	Build 8892,111128	C4XA14	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-3040B	Build 8892,111128	C4CX55 (AC) C4JH55 (DC)	Crypto Module Certificate: tbd Algorithm Certificates: tbd

[1] The firmware is assigned a version number that is identical to the version number of the software that is loaded onto it. The firmware version number is shown here because the operational program for the FortiGate series is stored in firmware.

[2] 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.

Product	Firmware[1] Version	Hardware Version[2]	FIPS 140-2 Certificate Number
FortiGate-3140B	Build 8892,111128	C4CX55	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-3950B	Build 8892,111128	C4DE23	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-3951B	Build 8892,111128	C4EL37	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-5001SX	Build 8892,111128	P4CF76	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-5001A-DW	Build 8892,111128	P4CJ36	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiGate-5001A-SW	Build 8892,111128	P4CJ36	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiWiFi-50B	Build 8892,111128	C5WF27	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiWiFi-60C	Build 8892,111128	C4DM95	Crypto Module Certificate: tbd Algorithm Certificates: tbd
FortiWifi-80CM	Build 8892,111128	C4BD62	Crypto Module Certificate: tbd Algorithm Certificates: tbd

Table 1 - TOE Identification Details

The products listed in Table 1 are collectively termed the FortiGate Series or FortiGate Family of Unified Threat Management (UTM) Solutions.

Documentation for the FortiGate Series operated in Common Criteria mode consists of the standard FortiOS version 4.0 documentation set plus a Federal Information Processing Standards –Common Criteria (FIPS-CC)-specific technical note.

1.4 TOE OVERVIEW

The TOE is a group of network appliances designed to provide firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering to provide network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks.

The FortiGate family of Unified Threat Management Solutions span the full range of network environments, from the remote office and branch office (ROBO) to service provider, offering cost-effective systems for any size of application. They are hardware security systems designed

to protect computer networks from abuse. They reside between the network they are protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by an authorized administrator. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real-time; without degrading network performance. In addition to providing stateful application-level protection, the FortiGate series delivers a full range of network-level services including; VPN, VLAN, Network Address Translation (NAT)[3], intrusion protection, web filtering, antivirus, antispam and traffic shaping; using dedicated, easily managed platforms.

Each 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 can operate either alone or as part of a cluster in order to provide high availability of services. The models offered in the FortiGate Series share common source code but different firmware builds due to different device drivers. The different models in the series provide for increased performance and additional protected ports.

All CC-evaluated FortiGate Unified Threat Management Solutions employ Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ operating system to achieve breakthrough price/performance. Their unique, Application-specific Integrated Circuit (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 "defence-in-depth" strategies without compromising performance or cost. They can be deployed to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, VLAN, and related devices, or to provide complete network protection.

The FortiGate series supports the Internet Protocol Security (IPSec) industry standard for VPN, allowing VPNs to be configured between a FortiGate model and any client or gateway/firewall that supports IPSec VPN. The FortiGate series also provides Secure Sockets Layer (SSL) VPN services.

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

[3] Network Address Translation is only applied after an information flow has been allowed by the rules which implement the FortiGate's security policy enforcement. For this reason the use of NAT by the FortiGate is not a security relevant feature of the TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

1.5.1.1 Physical Configuration

The FortiGate-50B, 60C, 80C, 200B, 310B, 311B, 620B, 1000A, 1240B, 3016B, 3040B, 3140B, 3950B, 3951B, FortiWiFi-50B, 60C and 80CM are stand-alone appliances that do not require supporting hardware. The FortiGate-5001SX, 5001A-DW, 5001A-SW and 5001B are Unified Threat Management Solution modules (blades) that may be installed in the FortiGate-5050 or 5140 chassis, each of which is capable of holding multiple blades. The chassis supports the blades by providing mounting, power and cooling fans only. As network and management interfaces are part of the blade itself, each blade acts as an independent Unified Threat Management Solution.

Each member of the series of FortiGate Unified Threat Management Solutions, 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. The FortiGate-5001SX, 5001A-SW, 5001A-DW and 5001B models offer dual processors in order to increase performance. All models share a common software platform and use a proprietary ASIC (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™ performs security and content processing.

1.5.1.2 Network Interfaces

The FortiGate units have the network interfaces defined in Table 2.

Product	Interfaces				Log Storage Type and Maximum Size
	Network (Ethernet) Interfaces		Administrator Interfaces		
	No.	Speed	Local Console	Network	
FortiGate-50B	5	10/100 Base-T	RS232/RJ-45	Yes	RAM Configurable 612KB – 3.2MB
FortiGate-60C	5	10/100/1000 Base-T	RS232/RJ-45	Yes	25.6 MB RAM
	3	10/100 Base-T			
FortiGate-80C	2	10/100/1000 Base-T	RS232/RJ-45	Yes	25.6 MB RAM
	7	10/100 Base-T			

Product	Interfaces				Log Storage Type and Maximum Size
	Network (Ethernet) Interfaces		Administrator Interfaces		
	No.	Speed	Local Console	Network	
FortiGate-110C	2	10/100/1000 Base-T	RS232/RJ-45	Yes	32 MB RAM
	8	10/100 Base-T			
FortiGate-200B	4	10/100/1000 Base-T	RS232/RJ-45	Yes	64GB SSD 1FSM slot
	8	10/100 Base-T			
FortiGate-310B	10	10/100/1000 Base-T	RS232/RJ-45	Yes	RAM Configurable 648KB – 51.2MB
FortiGate-311B	10	10/100/1000 Base-T	RS232/RJ-45	Yes	64GB SSD 2 FSM Slots
FortiGate-620B	8	10/100 Base-T	RS232/RJ-45	Yes	1x 80GB HDD (AMC module)
	4	10/100/1000 Base-T			
FortiGate-1000A	10	10/100/1000 Base-T	RS232/RJ-45	Yes	RAM Configurable 864KB – 51.2MB
FortiGate-1240B	24	1 GBit SFP	RS232/RJ-45	Yes	6 x 64GB SSD (FSM module)
	16	10/100/1000 Base-T			

Product	Interfaces				Log Storage Type and Maximum Size
	Network (Ethernet) Interfaces		Administrator Interfaces		
	No.	Speed	Local Console	Network	
FortiGate-3016B	16	1 GBit SFP	RS232/RJ-45	Yes	1 x 80GB HDD (AMC module)
FortiGate-3040B	10	1 GBit SFP	RS232/RJ-45	Yes	4x64GB SSD
	8	10 GbE SFP+			
FortiGate-3140B	10	10 GbE SFP+	RS232/RJ-45	Yes	4x64GB SSD
	10	1 GbE SFP			
	2	10/100/1000 Base-T			
FortiGate-3950B	1	10/100 Base T	RS232/DB-9	Yes	RAM only
	4	1000 Base SX			
	2	1000 Base-T			
	2	1 GBit SFP			
	1	AMC Card Slot[9]			
FortiGate-3951B	8	10/100 Base T	RS232/RJ-45	Yes	up to 4 x 64GB SSD (FSM module)
	2	1 GBit SFP			
	1	AMC Card Slot[9]			
FortiGate-5001SX	4	10/100/1000 Base T	RS232/DB-9	Yes	RAM Configurable 1.7MB – 102.4MB
	4	1 GBit SFP			
FortiGate-5001A-DW	2	1000 Base-T	RS232/RJ-45	Yes	RAM Configurable 1.7MB – 102.4MB
FortiGate-5001A-SW	2	1000 Base-T	RS232/RJ-45	Yes	RAM Configurable 1.7MB – 102.4MB

Product	Interfaces				Log Storage Type and Maximum Size
	Network (Ethernet) Interfaces		Administrator Interfaces		
	No.	Speed	Local Console	Network	
FortiGate-5001B	8	10GbE SFP+	RS232/RJ-45	Yes	64GB SSD
	2	10/100/1000 Base-T			
FortiWiFi-50B	5	10/100 Base-T	RS232/RJ-45	Yes	RAM Configurable 612KB – 3.2MB
	2	WiFi 802.11b and 802.11g			
FortiWiFi-60C	5	10/100/1000 Base-T	RS232/RJ-45	Yes	25.6 MB RAM
	3	10/100 Base-T			
	1	802.11 a/b/g/n			
FortiWiFi-80CM	2	10/100/1000 Base-T	RS232/RJ-45	Yes	25.6 MB RAM
	7	10/100 Base-T			

Table 2 - FortiGate Unified Threat Management Solution Interfaces

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

- A dedicated console port is available on all models. The port is RS232 with either a DB-9 or RJ-45 connector. When connected to a terminal which supports VT100 emulation, the console port allows access to the FortiGate unit via a Command Line Interface (CLI). This Local Console CLI permits an authorized administrator to configure the FortiGate unit, monitor its operation and examine the audit logs that are created;
- On all models remote administration may be performed via any network port that has been configured by an authorized administrator to allow Hypertext Transfer Protocol Secure (HTTPS) (for the Network Web-Based Graphical User Interface (GUI)) and Secure Shell (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;

- On models equipped with a Universal Serial Bus (USB) port an authorized administrator may perform key loading using a USB token;
- On all models, an authorized administrator may configure logging information to be sent to a FortiAnalyzer unit;
- On all models, an authorized administrator may configure automatic Anti-Virus and Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) updates, from the FortiGuard Distribution Server; and
- Model FortiGate-1000A is equipped with a Local Control Panel. The input portion of this panel is disabled in FIPS-CC mode, but the Liquid Crystal Display (LCD) portion provides limited status information to an administrator.

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

1.5.1.3 TOE Boundary - Single-Unit Configuration

In the Single-Unit configuration, which is supported by all of the FortiGate series, the TOE consists of a single FortiGate unit. The FortiGate units control network access by implementing classic firewall concepts, in which the firewall is linked to two or more networks and controls the transfer of data between 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 unit mediating information flow between two networks. One of the networks provides access to the FortiGuard Distribution Server, which permits Anti-Virus and IDS/IPS updates to be downloaded and facilitates access to web filtering data, and a FortiAnalyzer Server, which collects and analyzes logging information.

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

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

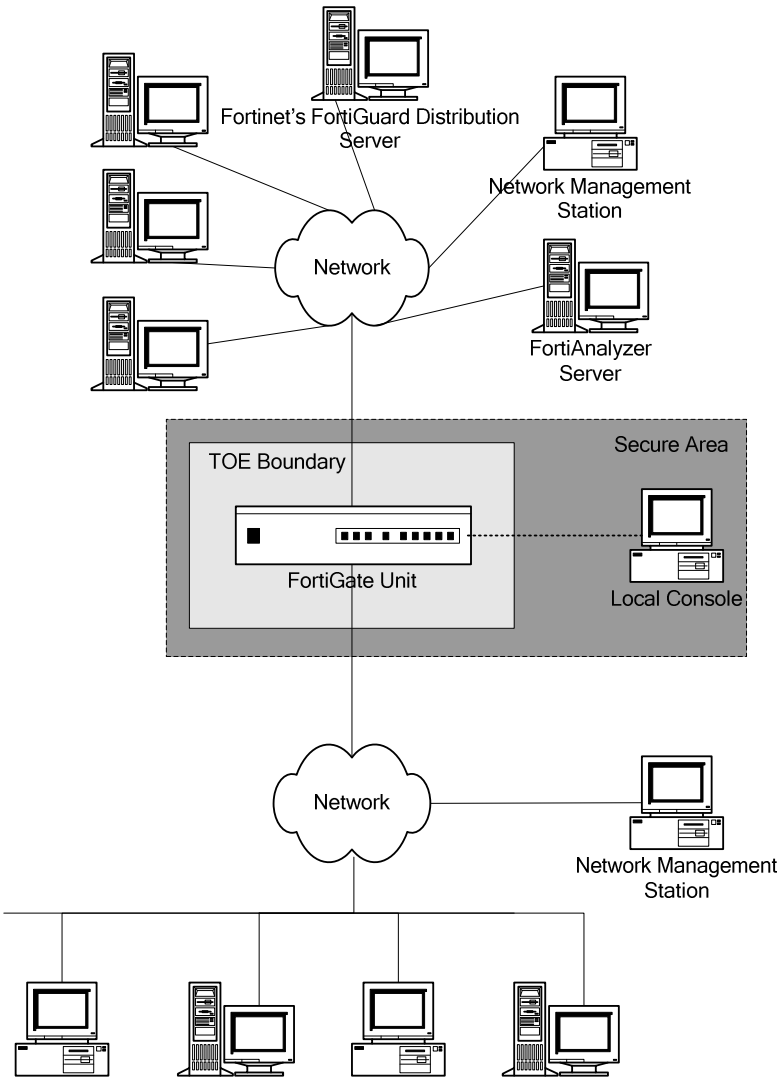

Figure 1 – Single Unit FortiGate Unified Threat Management Solution Network Configuration

1.5.1.4 TOE Boundary - High-Availability Configuration

In the High-Availability (HA) configuration, which is supported by all FortiGate units, the TOE consists of two or more FortiGate units interconnected to form a FortiGate Cluster. The FortiGate Cluster controls network access by implementing classic firewall concepts, in which the firewall is linked to two or more networks and controls the transfer of data between the networks. The configuration supports additional networks, each of which is physically connected to one of the Network Interfaces identified in Table 2.

Figure 2 shows three FortiGate units of the same type configured in HA mode to form a FortiGate Cluster. A FortiGate Cluster may be configured to work in active-passive mode for failover protection, or in active-active mode for failover protection and load balancing. Both active-passive mode and active-active mode are part of the evaluated configuration of the TOE.

The cluster units share state and configuration information over a dedicated High Availability Link. The TOE accesses the FortiGuard Distribution Server, which permits Anti-Virus and IDS/IPS updates to be downloaded, and a FortiAnalyzer Server, which collects and analyzes logging information.

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

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

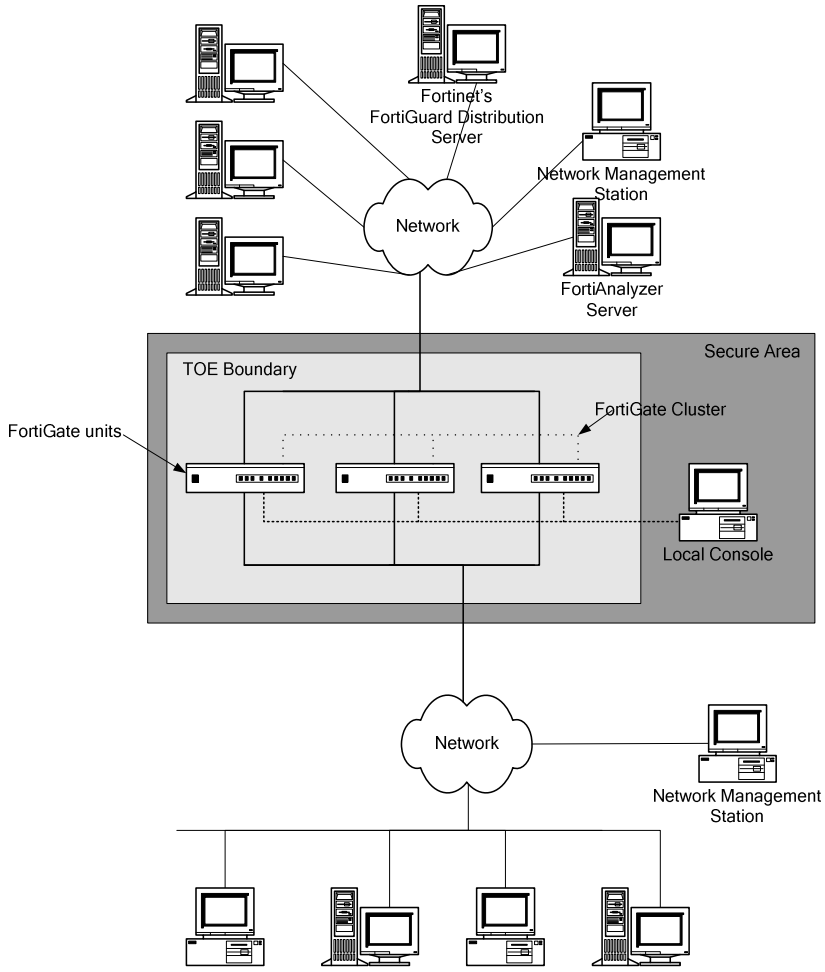

Figure 2 – High Availability FortiGate Unified Threat Management Solution Configuration

1.5.1.5 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/ Certificate Revocation Lists (CRLs)	Transfer certificates and CRLs to the FortiGate.	X.509 Certificate Management Protocol (CMP)
VPN Peer/Server	VPN Configuration	Configuration of VPN tunnels between the FortiGate and a remote peer or server.	IPSec/Internet Key Exchange (IKE) or SSL
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.	Transmission Control Protocol/ Internet Protocol (TCP/IP) and protocols built on it.
FortiGate Cluster	High Availability Data	Exchange data to configure and synchronize the FortiGate units that form a High Availability cluster.	FortiGate Clustering Protocol (FGCP)

External Entity	Interface Data	Interface Purpose	Protocol(s)
Fortinet's FortiGuard Distribution Server	Anti-Virus (AV)/Attack Updates Web filtering data	Transfer AV and attack updates from Fortinet to the FortiGate Unit. Allow access to categorization data for any URL.	TCP/IP and protocols built on it.
USB Token	Keys	Allow an authorized administrator to load cryptographic keys.	Media transfer protocol

Table 3 - FortiGate Interfaces

1.5.1.6 TOE Features

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

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

Table 4 summarizes the most security-relevant FortiGate features.

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.
Alarms and Alerts	The FortiGate provides audible and visible alarms that announce detected security policy violations.

Feature	Description
Anti-Virus	The FortiGate Series provides anti-virus protection for web HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and email (Simple Mail Transfer Protocol (SMTP), Post-Office Protocol Version 3 (POP3), and Internet Message Access Protocol (IMAP)) content as it passes through the FortiGate unit.
Authentication	The FortiGate implements a username and password mechanism for identification and authentication.
Authentication (Firewall Policy Authentication)	The FortiGate Firewall Policy may be configured to require authentication by the user before the information flow is enabled for that user.
Authentication (FortiToken)	The FortiGate provides an option of using a FortiToken one-time password for remote administrator and user authentication.
Certificate Management	The FortiGate provides the ability to obtain certificates and CRLs from an external certificate management server in support of SSL functionality.
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 an authorized administrator. The default policy is restrictive (i.e., no traffic flows without administrator action to configure policy).
FortiGuard Web Filtering	When a request for a web page appears in traffic controlled by the FortiGate unit, the URL is sent to a FortiGuard server, and the URL category is returned. The FortiGate unit determines if the URL should be allowed or blocked, based on the category and the implemented policy.
USB Token	The FortiGate provides for key loading via the USB port.

Feature	Description
High Availability (FortiGate Cluster)	The FortiGate Series provides a high availability capability between two or more identical units communicating via the FortiGate clustering protocol. Two modes of operation are supported: active-passive for failover protection and active-active for failover protection and load balancing.
Intrusion Detection and Prevention	FortiGate units use signatures to detect and prevent attacks to the data passing through them. The IPS attack signatures may be updated manually or the FortiGate unit may be configured to automatically download updates. The TOE also includes local anomaly detection to protect itself from direct attacks such as denial of service (DOS) attacks.
IPv6	Both an IPv4 and an IPv6 address may be assigned to any interface on a FortiGate unit. The interface functions as two interfaces, one for IPv4-addressed packets and another for IPv6-addressed packets. The FortiGate series supports static routing, periodic router advertisements, and tunnelling of IPv6-addressed traffic over an IPv4-addressed network. All relevant security claims apply to IPv4 and IPv6.
Logging	The FortiGate unit is able to send log information to external FortiAnalyzer servers. Other servers (e.g. FTP, Syslog Server, Trivial File Transfer Protocol (TFTP), or WebTrends Server) are not included.
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, written to hard disk, or written to a FLASH memory card, depending on the FortiGate model.
Protection Profile[4]	Protection profiles are used to configure anti-virus protection, and IDS/IPS.

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

Feature	Description
Proxies	Firewall rules may be defined that are applicable only to users who have authenticated to the firewall in order to use a proxy service. The evaluated configuration supports user authentication for the FTP, HTTP and Telnet protocols.
Residual Data	All residual information in any resource is over-written or otherwise destroyed such that it cannot be reused or otherwise accessed either inadvertently or deliberately.
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.
Self-test	The FortiGate performs self-tests of both the cryptographic and the non-cryptographic functions.
Time	The FortiGate maintains internal time on a system clock, settable by an authorized administrator. This clock is used when time stamps are generated.
VLAN	The FortiGate supports VLAN as a sub interface attached to a physical interface port. The firewall rules detailed herein may be applied to VLANs.
VPN	The FortiGate supports VPN using SSL or IPSec to provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.

Table 4 - Features Included in the TOE

1.5.1.7 Excluded Features

The FortiGate provides more capability than is being claimed in the ST. When using the TOE in the evaluated configuration, the excluded features are not enabled. The excluded features could be enabled by an administrator; however, this would contravene the CC-specific guidance that is provided to the administrator. Any feature not detailed herein, which allows an external entity to connect to the TOE, is an excluded feature.

The local console hardware is not included in the TOE.

1.5.1.8 TOE Environment

The FortiGate units are 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.

1.5.1.9 TOE Guidance Documentation

The following guidance documentation is an integral part of the TOE:

QuickStart Guides	FortiGate-50B QuickStart Guide 01-30003-0361-20070419
	FortiGate-60C QuickStart Guide 01-420-002122-20110128
	FortiGate-80C QuickStart Guide 01-412-89805-20090615
	FortiGate-110C QuickStart Guide 01-412-0468-20101119
	FortiGate-200B QuickStart Guide 01-420-110056-20090910
	FortiGate-310B QuickStart Guide 01-412-112401-20091020
	FortiGate-311B QuickStart Guide 01-30007-97512-20090525
	FortiGate-620B QuickStart Guide 01-420-112406-20110126
	FortiGate-1000A/FA2 QuickStart Guide 01-30007-114859-20091203
	FortiGate-1240B QuickStart Guide 01-30007-106971-20091117
	FortiGate-3016B QuickStart Guide 01-30006-0402-20080328
	FortiGate-3040B QuickStart Guide 01-413-125361-20101210
	FortiGate-3140B QuickStart Guide 01-420-129377-20101210
	FortiGate-3950B QuickStart Guide 01-413-124384-20100404
	FortiGate-3951B QuickStart Guide 01-413-119330-20100210
	FortiGate-5001SX Security System Guide 01-30000-0380-20070201
	FortiGate-5001A Security System Guide 01-30000-83456-20081023 (applies to both 5001A-DW and 5001A-SW)
	FortiGate-5001B Security System Guide 01-400-134818-20110118
	FortiGate-WIFI-50B QuickStart Guide 01-30005-0399-20070830
	FortiGate- WIFI-60C QuickStart Guide 19-420-002122-20110128
	FortiGate- WIFI-80CM QuickStart Guide 01-412-89807-20090615

Installation Guides	FortiGate Desktop Install Guide 01-400-95522-20090501
	FortiGate 1U Install Guide 01-400-95523-20090501
	FortiGate 2U Install Guide 01-400-95524-20090501
FortiOS	The FortiOS Handbook – The Complete Guide for FortiOS 4.0 MR3 01-430-99686-20110311

1.5.2 Logical Scope

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

1.5.2.1 Audit

In addition to generating audit records, the TOE monitors auditable events and provides a 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 at 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 all audit records associated with the potential security violation. The message will be displayed at the various consoles until acknowledged by an administrator. Additionally, an authorized administrator may configure the TOE to generate an audible alarm to indicate a potential security violation.

An authorized administrator may view the contents of the audit records and delete the audit trail. The TOE provides an authorized administrator with a sorting and searching capability to improve audit analysis. An authorized administrator may configure auditable events, back-up audit data and manage audit data storage. The TOE provides an authorized administrator with a configurable audit trail threshold to track the audit storage capacity. Once the threshold is met, the TOE displays a message in the same fashion as for potential security violations, including the optional 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 an authorized administrator 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.

The auditing function is supported by reliable timestamps.

1.5.2.2 Encryption

The TOE's cryptographic module(s) are FIPS PUB 140-2 validated and meet Security Level 1 overall and Security Level 3 for cryptographic module ports and interfaces, roles, services and authentication, and design assurance.

1.5.2.3 Information Flow Control

The TOE provides interfaces to a defined set of networks and mediates information flow among these networks. The two evaluated configurations are the Single-Unit Configuration, as shown in Figure 1 and a High-Availability Configuration, as shown in Figure 2. In both of these configurations the TOE is connected to two or more networks and user data flows from a connected network, through the TOE, to a connected network.

The TOE supports the information flow control policies required for the Application level Firewall PP and the Traffic Filter Firewall PP. Additionally, the TOE supports a VPN information flow control policy and a web filtering information flow control policy.

1.5.2.4 Identification and Authentication

All administration requires authentication by user identification and password mechanism. In addition, remote administration requires the use of the FortiToken one-time password, which provides 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 are required to authenticate using a password and FortiToken one-time password in order to use FTP and Telnet protocols. Remote authentication data is protected via encryption (trusted path). The TOE blocks users after a configurable number of authentication failures, after which an administrator must intervene to allow access.

1.5.2.5 Security Management

The TOE provides remote and local administrative interfaces that permit the administrative roles to configure and manage the TOE. In each of the two evaluated configurations (i.e., the Single-Unit Configuration, as shown in Figure 1 and a High-Availability Configuration, as shown in Figure 2), the TOE is connected to two or more networks and remote administration data flows from a Network Management Station to the TOE. In each configuration there is also a Local Console, located within a Secure Area, with an interface to the TOE.

An administrator account is associated with an access profile, which determines the permissions of the individual administrator. Additionally, each FortiGate unit comes with a default administrator account with all permissions, which may not be deleted. The term ‘authorized administrator’ is used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required.

1.5.2.6 Trusted Channel/Path

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

The TOE requires an encrypted trusted channel for communication with Fortinet's FortiGuard Distribution Server and FortiAnalyzer Server.

1.5.2.7 Protection of the TOE Security Functionality (TSF)

The TOE provides failover in support of the high availability features. Inter-TSF communications are protected to ensure availability, confidentiality and detection of modification.

1.5.2.8 IDS Functionality

The TOE provides IDS functionality including reliable collection and storage of sensor data, and restricted viewing of this data by an authorized administrator.

1.5.2.9 Anti Virus Functionality

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

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, CCMB-2006-09-001 July 2009 Revision 3, CCMB-2009-07-002 July 2009 Revision 3 and CCMB-2007-09-003 July 2009 Revision 3.

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

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

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST is demonstrably conformant with the U.S. Government Protection Profile Intrusion Detection System Sensor For Basic Robustness Environments, Version 1.3, July 25, 2007; U.S. Government Protection Profile for Application level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007; and U.S. Government Protection Profile for Traffic Filter 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 DEFINITION

3.1 THREATS, POLICIES AND ASSUMPTIONS

3.1.1 Threats

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

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.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
T.IMPCON	The TOE may be susceptible to improper configuration by any user, causing potential intrusions to go undetected.
T.INADVE	Inadvertent activity and access may occur on an IT System.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.LOSSOF	An unauthorized user may attempt to remove or

	destroy data collected by the TOE.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.MISACT	Malicious activity, such as introduction of Trojan horses and viruses, may occur on an IT System.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the Sensor's collection functionality by halting execution of 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.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.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	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).
T.SELPRO	An unauthorized person may read, modify, or

	destroy security critical TOE configuration data.
T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.

3.1.2 Threats Addressed by the Environment

The threat discussed below is addressed by the TOE Environment. It must be countered 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.

3.1.3 Organizational Security Policies

The TOE must address the organizational security policies described below.

P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.ACCESS	All data collected by the TOE shall only be used for authorized purposes.
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).
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.INTGTY	Data collected by the TOE shall be protected from modification.
P.INTEGRITY	Data transmitted to a peer TOE will be protected by encryption, where deemed appropriate.

P.MANAGE	The TOE shall be manageable only by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of collection activities.

3.1.4 Assumptions

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

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.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.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PHYSEC	The TOE is physically secure.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from

	unauthorized physical modification.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the 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 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

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

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
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.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
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.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
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.EXPORT	When the TOE makes its Sensor data available to other IDS components, the TOE will ensure the confidentiality of the Sensor data.
O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.

O.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.
O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer TOE via encryption and provide authentication for such data.
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.OFLOWS	The TOE must appropriately handle potential audit and Sensor data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
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.
O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
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.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.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Sensor.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.PHYSEC	The TOE is physically secure.
OE.PUBLIC	The TOE does not host public data.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.ASPOOF	T.AUDACC	T.AUDFUL	T.COMDIS	T.COMINT	T.IIMPCON	T.INADVE	T.INFLUX	T.LOSSOF	T.MEDIAT	T.MISACT	T.MISUSE	T.NOAUTH	T.NOHALT	T.OLDINF	T.PRIVIL	T.PROCOM	T.REPEAT	T.REPLAY	T.SELPRO	T.VIRUS	T.TUSAGE	P.ACCACT	P.ACCESS	P.CRYPTO	P.DETECT	P.INTGTY	P.INTEGRITY	P.MANAGE	P.PROTCT	A.DIRECT	A.GENPUR	A.LOCATE	A.LOWEXP	A.MANAGE	A.NOEVIL	A.NOREMO	A.NOTRST	A.PHYSEC	A.PROTCT	A.PUBLIC	A.REMACC	A.SINGEN
O.ACCESS				X	X	X			X					X		X									X				X															
O.ACCOUN		X																																										
O.AUDITS							X				X	X											X			X																		
O.AUDREC		X																					X																					
O.EADMIN						X																							X															
O.ENCRYP													X				X								X																				
O.EXPORT				X																																								
O.IDACTS							X				X	X		X												X																			
O.IDAUTH				X	X	X			X				X	X		X							X	X					X															
O.INTEGR					X				X				X														X																		
O.INTEGRITY																												X																	
O.LIMEXT													X																																
O.MEDIAT	X									X					X																														
O.OFLOWS								X																						X															
O.PROTCT				X	X				X						X									X				X																
O.SECFUN			X										X						X																										

	T.ASPOOF	T.AUDACC	T.AUDFUL	T.COMDIS	T.COMINT	T.IIMPCON	T.INADVE	T.INFLUX	T.LOSSOF	T.MEDIAT	T.MISACT	T.MISUSE	T.NOAUTH	T.NOHALT	T.OLDINF	T.PRIVIL	T.PROCOM	T.REPEAT	T.REPLAY	T.SELPRO	T.VIRUS	T.TUSAGE	P.ACCACT	P.ACCESS	P.CRYPTO	P.DETECT	P.INTGTY	P.INTEGRITY	P.MANAGE	P.PROTCT	A.DIRECT	A.GENPUR	A.LOCATE	A.LOWEXP	A.MANAGE	A.NOEVIL	A.NOREMO	A.NOTRST	A.PHYSEC	A.PROTCT	A.PUBLIC	A.REMACC	A.SINGEN
O.SECSTA													X							X																							
O.SELPRO			X																	X																							
O.SINUSE																		X	X																								
O.TIME																							X			X																	
O.VIRUS																					X																						
OE.ADMTRA																						X																					
OE.CREDEN																													X						X		X					
OE.DIRECT																															X											
OE.GENPUR																																X										
OE.GUIDAN																						X																					
OE.INSTAL						X																							X						X							
OE.LOWEXP																																	X										
OE.NOEVIL																																				X							
OE.NOREMO																																					X						
OE.PERSON																													X						X							
OE.PHYCAL																														X			X			X		X		X		
OE.PHYSEC																																							X				
OE.PUBLIC																																									X		

	T.ASPOOF	T.AUDACC	T.AUDFUL	T.COMDIS	T.COMINT	T.IIMPCON	T.INADVE	T.INFLUX	T.LOSSOF	T.MEDIAT	T.MISACT	T.MISUSE	T.NOAUTH	T.NOHALT	T.OLDINF	T.PRIVIL	T.PROCOM	T.REPEAT	T.REPLAY	T.SELPRO	T.VIRUS	T.TUSAGE	P.ACCACT	P.ACCESS	P.CRYPTO	P.DETECT	P.INTGTY	P.INTEGRITY	P.MANAGE	P.PROTCT	A.DIRECT	A.GENPUR	A.LOCATE	A.LOWEXP	A.MANAGE	A.NOEVIL	A.NOREMO	A.NOTRST	A.PHYSEC	A.PROTCT	A.PUBLIC	A.REMACC	A.SINGEN
OE.REMACC																																										X	
OE.SINGEN																																											X

Table 5 - Mapping Between Objectives and Threats, Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

Threat: 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.	
Objectives:	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
Rationale:	O.MEDIAT mitigates this threat by ensuring that all information between clients and servers located on internal and external networks is mediated by the TOE.	
Threat: T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.	
Objectives:	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.
Rationale:	O.AUDREC provides for a readable, searchable audit trail. 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.	
Threat: 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.	
Objectives:	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.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
Rationale:	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 requires that the TOE provide functionality that ensures that only the authorized administrators have access to the TOE security functions.	
Threat: T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EXPORT	When the TOE makes its Sensor data available to other IDS components, the TOE will ensure the confidentiality of the Sensor data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.	
Threat: T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.	

Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.	
Threat: T.IMPCON	The TOE may be susceptible to improper configuration by any user, causing potential intrusions to go undetected.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
Rationale:	The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. These objects are	

	supported by the OE.INSTAL, which ensures that the TOE is delivered, installed, managed, and operated in a manner consistent with IT security.	
Threat: T.INADVE	Inadvertent activity and access may occur on an IT System.	
Objectives:	O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
	O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
Rationale:	The O.AUDITS and O.IDACTS objectives address this threat by requiring collection of audit and Sensor data.	
Threat: T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.	
Objectives:	O.OFLOWS	The TOE must appropriately handle potential audit and Sensor data storage overflows.
Rationale:	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.	
Threat: T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.

Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.	
Threat: T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.	
Objectives:	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
Rationale:	O.MEDIAT requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.	
Threat: T.MISACT	Malicious activity, such as introduction of Trojan horses and viruses, may occur on an IT System.	
Objectives:	O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
	O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
Rationale:	The O.AUDITS and O.IDACTS objectives require collection of audit and Sensor data.	
Threat: T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System.	
Objectives:	O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
	O.IDACTS	The Sensor must collect and store information

		about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
Rationale:	The O.AUDITS and O.IDACTS objective address this threat by requiring collection audit and Sensor data.	
Threat: T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality 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 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.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.
	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.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.
Rationale:	O.IDAUTH requires that users be uniquely identified 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.SECFUN requires that the TOE provide	

	functionality that ensures that only the authorized administrator has access to the TOE security functions. O.INTEGR ensures the integrity of the data associated with those security functions. O.LIMEXT requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.	
Threat: T.NOHALT	An unauthorized user may attempt to compromise the continuity of the Sensor's collection functionality by halting execution of the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
	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.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.	
Threat: 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.	
Objectives:	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
Rationale:	O.MEDIAT requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.	

Threat: T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.	
Threat: T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
Rationale:	O.ENCRYP requires that an authorized administrator uses encryption when performing administrative functions on the TOE remotely.	
Threat: T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.	
Objectives:	O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
Rationale:	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.	
Threat: 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).	
Objectives:	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	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
Rationale:	O.SINUSE mitigates this threat by preventing the reuse of authentication data. This is supported by O.SECFUN, which ensures that only authorized administrators have access to security functions.	
Threat: T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.	
Objectives:	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.
Rationale:	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.	
Threat: T.VIRUS	A malicious agent may attempt to pass a virus through or to the TOE.	
Objectives:	O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any

		of the TOE network interfaces.
Rationale:	The O.VIRUS objective ensures that the TOE detects and blocks viruses which are contained in any information flow which reaches one of the TOE network interfaces.	
Threat Addressed by the Environment: T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.	
Objectives:	OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
	OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
Rationale:	OE.ADMTRA and OE.GUIDAN provide the procedural and administrative measures necessary to mitigate this threat.	

4.3.2 Security Objectives Rationale Related to Policies

Policy: P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.	
Objectives:	O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
	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.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.

Rationale:	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The O.AUDREC requires a readable audit trail and a means to search and sort the information contained in the audit trail. O.TIME supports the audit trail with reliable time stamps.	
Policy: P.ACCESS	All data collected by the TOE shall only be used for authorized purposes.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
Rationale:	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection.	
Policy: 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).	
Objectives:	O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
Rationale:	O.ENCRYP requires that an authorized administrator use encryption when performing administrative functions on the TOE remotely.	
Policy:	All events that are indicative of inappropriate activity that may have	

P.DETECT	resulted from misuse, access, or malicious activity of IT System assets must be collected.	
Objectives:	O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.
	O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
	O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
Rationale:	The O.AUDITS and O.IDACTS objectives require collection of audit and Sensor data. O.TIME supports the audit functionality with reliable timestamps.	
Policy: P.INTGTY	Data collected by the TOE shall be protected from modification.	
Objectives:	O.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.
Rationale:	The O.INTEGR objective ensures the protection of data from modification.	
Policy: P.INTEGRITY	Data transmitted to a peer TOE will be protected by encryption, where deemed appropriate.	
Objectives:	O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer TOE via encryption and provide authentication for such data.
Rationale:	The O.INTEGRITY objective ensures that data transmitted between peers can be encrypted.	
Policy: P.MANAGE	The TOE shall be manageable only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.

	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions, data or, for certain specified services, to a connected network.
	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Sensor.
Rationale:	The O.EADMIN objective ensures there is a set of functions for administrators to use, and is supported by the OE.PERSON objective, which ensures competent administrators will manage the TOE, and the OE.CREDEN objective which ensures that those administrators will protect their access credentials. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection.	
Policy: P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of collection activities.	
Objectives:	O.OFLOWS	The TOE must appropriately handle potential audit and Sensor data storage overflows.
	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Rationale:	The O.OFLOWS objective requires the TOE handle disruptions. It is supported by the OE.PHYCAL objective, which protects the TOE from unauthorized physical attack.

4.3.3 Security Objectives Rationale Related to Assumptions

Assumption: 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)	
Objectives:	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.
Rationale:	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.	
Assumption: 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.	
Objectives:	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.
Rationale:	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.	
Assumption: A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.	

Assumption: A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	
Objectives:	OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
Rationale:	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	
Assumption: A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Sensor.
Rationale:	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.	
Assumption: A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	
Objectives:	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
	OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	Administrators are non-hostile (OE.NOEVIL), have access credentials (OE.CREDEN), operate in a manner consistent with IT security (OE.INSTAL), and ensure that the TOE is protected from physical attack	

	(OE.PHYCAL).	
Assumption: A.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.	
Objectives:	OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
Rationale:	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.	
Assumption: A.NOTRST	The TOE can only be accessed by authorized users.	
Objectives:	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.	
Assumption: A.PHYSEC	The TOE is physically secure.	
Objectives:	OE.PHYSEC	The TOE is physically secure.
Rationale:	The TOE is physically secure.	
Assumption: A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	
Objectives:	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYCAL objective provides for the physical protection of the	

	TOE hardware and software.	
Assumption: A.PUBLIC	The TOE does not host public data.	
Objectives:	OE.PUBLIC	The TOE does not host public data.
Rationale:	The TOE does not host public data.	
Assumption: A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.	
Objectives:	OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
Rationale:	Authorized administrators may access the TOE remotely from the internal and external networks.	
Assumption: A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	
Objectives:	OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
Rationale:	Information cannot flow among the internal and external networks unless it passes through the TOE.	

5 EXTENDED COMPONENTS DEFINITION

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

5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 6 identifies all extended SFRs implemented by the TOE.

Name	Description
FAV_ACT_EXT.1	Anti Virus Actions
IDS_COL_EXT.1	Sensor data collection
IDS_RDR_EXT.1	Restricted data review
IDS_STG_EXT.1	Guarantee of sensor data availability
IDS_STG_EXT.2	Prevention of sensor data loss

Table 6 – Extended TOE Security Functional Requirements

5.1.1 Anti-Virus Action Requirements (FAV)

5.1.1.1 FAV_ACT_EXT.1

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

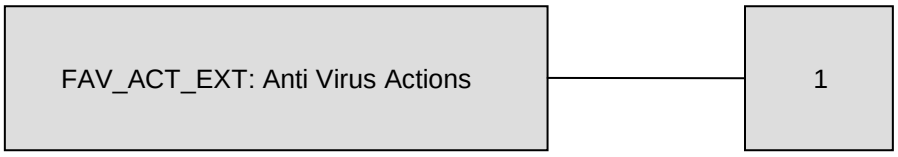

Figure 3 - FAV_ACT_EXT Component Levelling

Management: FAV_ACT_EXT.1

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

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

Audit: FAV_ACT_EXT.1

The following actions should be auditable:

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- quarantine the content of the information flow
- remove the content of the information flow

to be taken on detection of a virus in an information flow.

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

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

5.1.2 IDS Class

A class of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. This class of requirements has three families of IDS_COL_EXT, IDS_RDR_EXT, and IDS_STG_EXT, and these requirements have no dependencies since the stated requirements embody all the necessary security functions. Component levelling is shown in Figure 4.

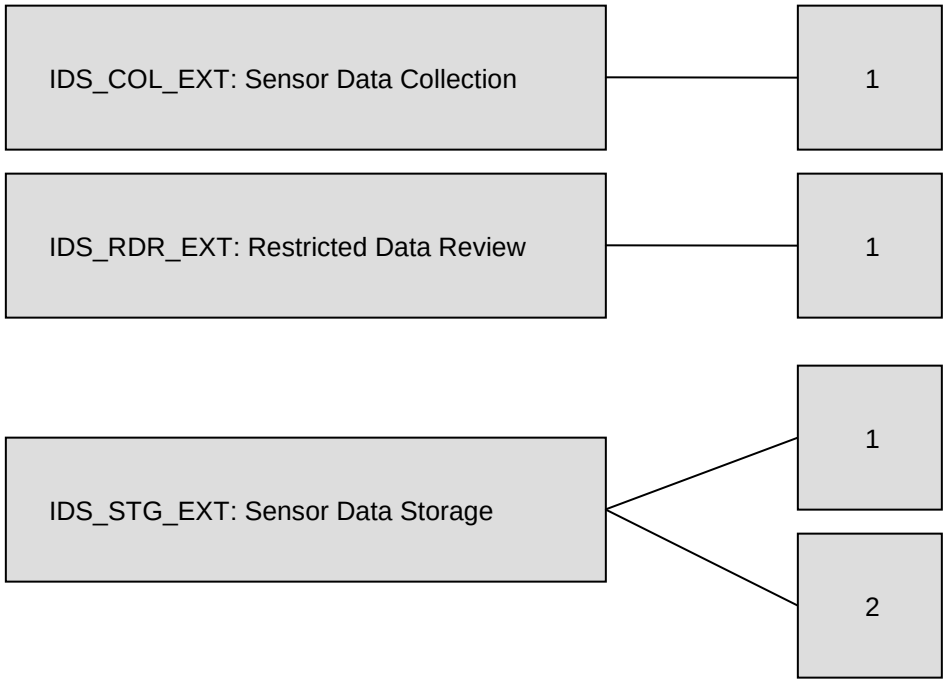

Figure 4 - IDS Component Levelling

5.1.2.1 IDS_COL_EXT.1 Sensor Data Collection (EXT)

Management: IDS_COL_EXT.1

There are no management activities foreseen.

Audit: IDS_COL_EXT.1

There are no auditable events foreseen.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_COL_EXT.1.1 The Sensor shall be able to collect the following events from the targeted IT System resource(s):

a) [selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction]; and

b) [*assignment: other specifically defined events*].

IDS_COL_EXT.1.2 At a minimum, the Sensor shall collect 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) The additional information specified in the Details column of Table 3 Sensor Events.

Component	Event	Details
IDS_COL_EXT.1	Start-up and shutdown	none
IDS_COL_EXT.1	Identification and authentication events	User identity, location, source address, destination address
IDS_COL_EXT.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_COL_EXT.1	Service Requests	Specific service, source address, destination address
IDS_COL_EXT.1	Network traffic	Protocol, source address, destination address
IDS_COL_EXT.1	Security configuration changes	Source address, destination address
IDS_COL_EXT.1	Data introduction	Object IDS, location of object, source address, destination address

Table 7 - Sensor Events

Application Note: In the case where the Sensor is collecting host-based events, for the identification and authentication event, the source address could be a subject IDS on a local machine and the destination is defined by default. For the data access and data introduction events, the source address could be filename and the destination address may be target location for the file.

5.1.2.2 IDS_RDR_EXT.1 Restricted Data Review (EXT)

Management: IDS_RDR_EXT.1

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

- The management (review) of actions on Sensor data.

Audit: IDS_RDR_EXT.1

There are no auditable events foreseen.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_RDR_EXT.1.1 The Sensor shall provide [*assignment: authorised users*] with the capability to read [*assignment: list of Sensor data*] from the Sensor data.

Application Note: This requirement applies to authorized users of the Sensor. The requirement is left open for the writers of the ST to define which authorized users may access what Sensor data.

IDS_RDR_EXT.1.2 The Sensor shall provide the Sensor data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The Sensor shall prohibit all users read access to the Sensor data, except those users that have been granted explicit read-access.

5.1.2.3 IDS_STG_EXT.1 Guarantee of Sensor Data Availability (EXT)

Management: IDS_STG _EXT.1

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

- The management (selection) of metric for Sensor Data; and
- The management (selection) of conditions of stored Sensor Data.

Audit: IDS_STG _EXT.1

The following actions should be auditable:

- Minimal: occurrence of conditions of stored Sensor Data.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_STG_EXT.1.1 The Sensor shall protect the stored Sensor data from unauthorised deletion.

IDS_STG_EXT.1.2 The Sensor shall protect the stored Sensor data from modification.

Application Note: Authorized deletion of data is not considered a modification of Sensor data in this context. This requirement applies to the actual content of the Sensor Data, which should be protected from any modifications.

IDS_STG_EXT.1.3 The Sensor shall ensure that [*assignment: metric for saving Sensor data*] Sensor data will be maintained when the following conditions occur: [selection: Sensor data storage exhaustion, failure, attack].

5.1.2.4 IDS_STG_EXT.2 Prevention of Sensor Data Loss (EXT)

Management: IDS_STG _EXT.2

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

- The management (selection) of actions on Sensor Data.

Audit: IDS_STG _EXT.2

There are no auditable events foreseen.

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_STG_EXT.2.1 The Sensor shall [*selection: 'ignore Sensor data', 'prevent Sensor data, except those taken by the authorised user with special rights', 'overwrite the oldest stored Sensor data '*] and send an alarm if the storage capacity has been reached.

Application Note: The ST must define what actions the Sensor takes if the storage capacity has been reached. Anything that causes the Sensor to stop collecting events may not be the best solution, as this will only affect the Sensor and not the system on which it is collecting data (e.g., shutting down the Sensor).

5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS

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

6 SECURITY REQUIREMENTS

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

6.1 CONVENTIONS

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

- Selection: Indicated by surrounding brackets, e.g., [selected item]. To improve readability selections of [none] are generally not shown.
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown.
- Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, the referenced Application level Firewall PP, the Traffic Filter Firewall PP, the IDS Sensor PP, and extended components defined in Section 5. These are summarized in Table 8.

Component	Description	Source
FAU_ARP.1	Security alarms	CC Part 2
FAU_GEN.1	Audit data generation	Application level Firewall (FW), Traffic Filter FW, and IDS Sensor PPs
FAU_GEN.2	User identity association	CC Part 2
FAU_SAA.1	Potential violation analysis	CC Part 2
FAU_SAR.1	Audit review	Application level FW, Traffic Filter FW, and IDS Sensor PPs
FAU_SAR.2	Restricted audit review	IDS Sensor PP

Component	Description	Source
FAU_SAR.3	Selectable audit review	Application level FW, Traffic Filter FW, and IDS Sensor PPs
FAU_SEL.1	Selective audit	IDS Sensor PP
FAU_STG.2	Guarantees of audit data availability	Application level FW, Traffic Filter FW, and IDS Sensor PPs
FAU_STG.4	Prevention of audit data loss	Application level FW, Traffic Filter FW, and IDS Sensor PPs
FCS_CKM.1	Cryptographic Key Generation	CC Part 2
FCS_CKM.4	Cryptographic key destruction	CC Part 2
FCS_COP.1	Cryptographic operation	Application level FW and Traffic Filter FW PPs
FDP_IFC.1(1)	Subset information flow control (unauthenticated policy)	Application level FW and Traffic Filter FW PPs
FDP_IFC.1(2)	Subset information flow control (authenticated policy)	Application level FW PP
FDP_IFC.1(3)	Subset information flow control (VPN policy)	CC Part 2
FDP_IFC.1(4)	Subset information flow control (web filtering policy)	CC Part 2
FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)	Application level FW and Traffic Filter FW PPs
FDP_IFF.1(2)	Simple security attributes (authenticated policy)	Application level FW PP
FDP_IFF.1(3)	Simple security attributes (VPN policy)	CC Part 2
FDP_IFF.1(4)	Simple security attributes (web filtering policy)	CC Part 2
FDP_RIP.2	Full residual information protection	Application level FW and Traffic Filter FW PPs

Component	Description	Source
FIA_AFL.1(1)	Authentication failure handling (Application Level Firewall)	Application level FW PP
FIA_AFL.1(2)	Authentication failure handling (Traffic Filter Firewall)	Traffic Filter FW PP
FIA_ATD.1	User attribute definition	Application level FW, Traffic Filter FW, and IDS Sensor PPs
FIA_UAU.1	Timing of authentication	Traffic Filter FW and IDS Sensor PPs
FIA_UAU.4	Single-use authentication mechanisms	Traffic Filter FW PP
FIA_UAU.5	Multiple authentication mechanisms	Application level FW and Traffic Filter FW PPs
FIA_UID.2	User identification before any action	Application level FW, Traffic Filter FW and IDS Sensor PPs
FMT_MOF.1(1)	Management of security functions behaviour (Traffic Filter FW)	Traffic Filter FW PP
FMT_MOF.1(2)	Management of security functions behaviour (IDS Sensor)	IDS Sensor PP
FMT_MOF.1(3)	Management of security functions behaviour (Application Level FW 1)	Application level FW PP
FMT_MOF.1(4)	Management of security functions behaviour (Application Level FW 2)	Application level FW PP
FMT_MSA.1(1)	Management of security attributes (Application Level FW 1)	Application level FW PP
FMT_MSA.1(2)	Management of security attributes (Application Level FW 2)	Application level FW PP
FMT_MSA.1(3)	Management of security attributes (Application Level FW 3)	Application level FW PP
FMT_MSA.1(4)	Management of security attributes (Application Level FW 4)	Application level FW PP

Component	Description	Source
FMT_MSA.1(5)	Management of security attributes (VPN)	CC Part 2
FMT_MSA.3	Static attribute initialization	Application level FW and Traffic Filter FW PPs
FMT_MTD.1(1)	Management of TSF data (audit data)	IDS Sensor PP
FMT_MTD.1(2)	Management of TSF data (cryptographic TSF data)	Application level FW PP
FMT_MTD.1(3)	Management of TSF data (time TSF data)	Application level FW PP
FMT_MTD.2	Management of limits on TSF data	Application level FW PP
FMT_SMF.1	Specification of Management Functions	Application level FW, Traffic Filter FW and IDS Sensor PPs
FMT_SMR.1	Security Roles	CC Part 2
FPT_FLS.1	Failure with preservation of secure state	CC Part 2
FPT_ITA.1	Inter-TSF availability within a defined availability metric	IDS Sensor PP
FPT_ITC.1	Inter-TSF confidentiality during transmission	IDS Sensor PP
FPT_ITI.1	Inter-TSF detection of modification	IDS Sensor PP
FPT_STM.1	Reliable time stamps	Application level FW, Traffic Filter FW and IDS Sensor PPs
FTP_ITC.1	Inter-TSF trusted channel	CC Part 2
FTP_TRP.1	Trusted path	CC Part 2
IDS_COL_EXT.1	Sensor data collection	IDS Sensor PP
IDS_RDR_EXT.1	Restricted data review	IDS Sensor PP
IDS_STG_EXT.1	Guarantee of sensor data availability	IDS Sensor PP
IDS_STG_EXT.2	Prevention of sensor data loss	IDS Sensor PP

Component	Description	Source
FAV_ACT_EXT.1	Anti Virus Actions	Extended requirement added to specify Anti Virus capabilities of the TOE

Table 8 - Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall ~~take~~ [*display an alarm message (with or without an audible alarm) send a notification to an email address, SNMP trap or Syslog server*] upon detection of a potential security violation.

6.2.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

b) All auditable events for the [basic] level of audit; and

c) [*All auditable events listed in Table 9, which is a complete list, encompassing events required by the basic level of audit, the IDS-specific events required by the IDS Sensor PP, and the FW-specific events required by the Application level FW PP and Traffic Filter FW PP*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*information specified in Table 9 Auditable Events*.]

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1	Action taken due to detection	Condition that was matched and message details
FAU_GEN.1	Start-up and shutdown of audit Access to Sensor	 Object IDS, requested access
FAU_GEN.2	None	
FAU_SAA.1	Changes to the monitoring rules	
	Detection of violation	Condition that was matched and action performed
FAU_SAR.1	Reading of information from the audit records (Opening the audit trail)	The identity of the administrator performing the function
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	The identity of the administrator attempting the function
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the administrator performing the function
FAU_STG.2	None	
FAU_STG.4	Actions taken due to the audit storage failure.	The identity of the administrator performing the function
FCS_CKM.1	Generation and loading of a key Failure of the activity	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.4	Failure of the key zeroization	Type of cryptographic operation Any applicable cryptographic mode(s) of operation excluding any sensitive information
FCS_COP.1	Failure of the cryptographic operation	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information Identity of the external IT entity attempting to perform the cryptographic operation
FDP_IFC.1(1)	None	
FDP_IFC.1(2)	None	
FDP_IFC.1(3)	None	
FDP_IFC.1(4)	None	
FDP_IFF.1(1)	Decisions to permit/deny information flows Failure to reassemble fragmented packets	Presumed identity of source subject Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface on which the

Requirement	Auditable Events	Additional Audit Record Contents
		TOE received the packet Identity of the rule that allowed or disallowed the packet flow Reason why fragmented packets could not be reassembled (i.e., invalid fragment identifier, invalid offset, invalid fragment data length)
FDP_IFF.1(2)	Decisions to permit/deny information flows Failure to reassemble fragmented packets	Presumed identity of source subject Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow Reason why fragmented packets could not be reassembled (i.e., invalid fragment identifier, invalid offset, invalid fragment data length)
FDP_IFF.1(3)	Decisions to permit/deny information flows	Presumed identity of source subject

Requirement	Auditable Events	Additional Audit Record Contents
	Operation applied to each information flow permitted	Identity of destination subject Transport layer protocol, if applicable Source subject service identifier, if applicable Destination subject service identifier, if applicable Identity of the firewall interface on which the TOE received the packet For denied information flows, the reason for denial.
FDP_IFF.1(4)	Decisions to permit/deny information flows	Identification of the user creating the traffic Identification of the policy that applies Applicable URL Status (e.g. blocked, allowed)
FDP_RIP.2	None	
FIA_AFL.1 (1) and (2)	The reaching of the threshold for the unsuccessful authentication attempts The actions (e.g. disabling of an account) taken The subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of an	Identity of the unsuccessfully authenticated user Claimed identity of the unsuccessfully authenticated user and the identity of an authorized administrator

Requirement	Auditable Events	Additional Audit Record Contents
	account)	performing the function.
FIA_ATD.1	None	
FIA_UAU.1	All uses of the authentication mechanism	User identity, location
FIA_UAU.4	Use of the authentication mechanism	User identity, location
FIA_UAU.5	All use of the authentication mechanism	Claimed identity of the user attempting to authenticate
FIA_UID.2	All use of the user identification mechanism used for authorized users (that is, those that authenticate to the TOE)	Claimed identity of the user using the identification mechanism, location
FMT_MOF.1(1)	All modifications in the behaviour of the functions in the TSF	The identity of the administrator performing the function
FMT_MOF.1(2)	All modifications in the behaviour of the functions in the TSF	The identity of the administrator performing the function
FMT_MOF.1(3)	Use of the functions listed in this requirement pertaining to audit	The identity of the administrator performing the function
FMT_MOF.1(4)	Use of the functions listed in this requirement pertaining to audit	The identity of the administrator performing the function
FMT_MSA.1(1)	All manipulation of the security attributes	The identity of the administrator performing the function
FMT_MSA.1(2)	All manipulation of the security attributes	The identity of an authorized administrator performing the function
FMT_MSA.1(3)	All manipulation of the	The identity of the administrator performing

Requirement	Auditable Events	Additional Audit Record Contents
	security attributes	the function
FMT_MSA.1(4)	All manipulation of the security attributes	The identity of the administrator performing the function
FMT_MSA.3	None	
FMT_MTD.1(1)	All modifications to the values of TSF data	
FMT_MTD.1(2,3,4,5)	None	
FMT_MTD.2	All modifications of the limits Actions taken when the quota is exceeded (include the fact that the quota was exceeded)	The identity of the administrator performing the function
FMT_SMF.1	Use of management functions	The identity of the administrator performing the function
FMT_SMR.1	Modifications to the group of users that are part of a role Unsuccessful attempts to use a role due to the given conditions on the roles	User identification of the administrator performing modification, and the user whose role is modified. The identity of the administrator performing the function
FPT_FLS.1	Failure of the TSF	
FPT_ITA.1	The absence of TSF data when required by a TOE.	
FPT_ITC.1	None	
FPT_ITI.1	The detection of modification of transmitted TSF data. The action taken upon	

Requirement	Auditable Events	Additional Audit Record Contents
	detection of modification of transmitted TSF data.	
FPT_STM.1	Changes to the time	The identity of the administrator performing the operation
FTP_ITC.1	All attempted uses of the trusted channel functions	Identification of the initiator and target of all trusted channels
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of the claimed user identity
IDS_COL_EXT.1	See IDS_COL_EXT.1.2	
IDS_RDR_EXT.1	None	
IDS_STG_EXT.1	Occurrence of conditions of stored Sensor Data.	
IDS_STG_EXT.2	None	
FAV_ACT_EXT	Actions taken on the information flow when virus is detected	

Table 9 - Auditable Events

6.2.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.2.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring ~~the audited~~ events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [

(1)Administrator-specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address), destination network identifier or individual destination subject service identifier (e.g., TCP port) within an administrator-specified time period;

(2)Any failure of the self-tests; and

(3)Administrator-specified number of encryption or decryption failures.]

known to indicate a potential security violation;

b) [*the following additional rules:*

Administrator-specified percentage of available audit storage usage known to indicate a potential security violation].

6.2.1.5 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

6.2.1.6 FAU_SAR.2 Restricted Audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.2.1.7 FAU_SAR.3 Selectable Audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to ~~apply~~ 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].

6.2.1.8 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [event type];

b) [*traffic flow and event severity level*].

6.2.1.9 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [*an authorized administrator's selection of all or the most recent*] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion].

Application Note: Both the Traffic Filter Firewall and Application Level Firewall PPs require FAU_STG.1. The IDS PP requires FAU_STG.2. As FAU_STG.2 is hierarchical to FAU_STG.1, the requirement is sufficiently covered. Therefore, FAU_STG.1 is not included herein.

6.2.1.10 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [prevent audited events, except those taken by the authorised user with special rights] and [*shall limit the number of audit records lost]* if the audit trail is full.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*FIPS-approved Random Number Generator American National Standards Institute (ANSI) X9.31 Appendix A*] and specified cryptographic key sizes [*listed in Table 10*] that meet the following: [*standards listed in Table 10*].

Key Usage	Key Size	Standard	Cryptographic Algorithm Validation Program (CAVP) Certificate Number
For symmetric cryptography (AES)	128, 192 or 256	a minimum overall rating of FIPS PUB 140-2, Level 1	tbd
For symmetric cryptography (3DES)	192 (including parity)	National Institute of Standards and Technology (NIST) SP 800-67 (TDEA)	tbd
For asymmetric cryptography	2048	ANSI X9.31	tbd

Table 10 - Cryptographic Key Generation

6.2.2.2 FCS_CKM.4 Cryptographic key Destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*keys are zeroized when a factory reset is performed via the web-based manager, CLI, or console*] that meets the following: [*FIPS PUB 140-2 Key Management Security Level 1*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in Table 11*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 11*] and cryptographic key sizes [*cryptographic key sizes specified in Table 11*] that meet the following: [*standards listed in Table 11*].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard	CAVP Certificate Number
Encryption and Decryption of remote administrator sessions	AES (Advanced Encryption Standard)	at least 128	FIPS PUB 140-2 (Level 1)	tbd
Encryption and Decryption in support of the VPN policy	AES (operating in CBC mode for IPSec and SSL) Triple Data Encryption Algorithm (TDEA) (operating in CBC mode for SSL)	128, 192, and 256 for AES and 192 (including parity) for TDEA	FIPS PUB 197 (AES) and National Institute of Standards and Technology (NIST) SP 800-67 (TDEA)	tbd
Cryptographic Signature Services	RSA Digital Signature Algorithm (rDSA)	2048	ANSI X9.31-1998	tbd
Hashing	SHA-1 and HMAC	n/a	FIPS 140-2 PUB 180-2, and FIPS 140-2 PUB 198	tbd
Random Number Generation	ANSI X9.31 Appendix A	n/a	ANSI X9.31	tbd

Table 11- Cryptographic Operation

6.2.3 User Data Protection (FDP)

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

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

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].

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

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(2).1 The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW SFP*] on:

a) [*subjects: a human user or external IT entity that sends and receives 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; and

c) operation: initiate service and pass information].

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

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(3).1 The TSF shall enforce the [*VPN SFP*] on:

S*ubjects*

TOE interfaces

Information

network packets

Operation

SSL and IPSec operations].

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

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

S*ubjects*

Human users

Information

Web pages

Operation

HTTP and HTTPS].

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

Hierarchical to: No other components.

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

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

a) [*subject security attributes:*
- *presumed address;*
- *schedule*.

b) information security attributes:
- *presumed address of source subject;*
- *presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which the traffic arrives and departs; service;*
- *Schedule: One-time schedule (Start Time, End Time), Recurring schedule (Days of week on which schedule is active, Start Time, End Time)*

- *Stateful packet attributes: Connection-oriented protocols (sequence number, acknowledgement number, Flags (SYN, ACK, RST, FIN)); Connectionless protocols (source and destination network identifiers, source and destination service identifiers)*].

FDP_IFF.1(1).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:

a) [*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.*

b) 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(1).3 The TSF shall enforce the [*none*].

FDP_IFF.1(1).4 The TSF shall provide the following [*an authorized administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied*].

FDP_IFF.1(1).5 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1(1).6 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 do not conform to its associated published protocol specification (e.g., Request for Comments (RFC)). This shall be accomplished through protocol filtering proxies that are designed for that purpose].

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

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

Hierarchical to: No other components.

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

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

a) [*Subject security attributes:*

- *presumed address;*
- *source network identifier.*
- *Set of destination subject identifiers.*

b) Information security attributes:

- *identity of source subject (combination of user identity and presumed address of source subject);*

- *identity of destination subject (combination of user identity and presumed address of destination subject);*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs;*
- *service (i.e. FTP and Telnet);*
- *destination subject service identifier (e.g. TCP destination port number):*
- *security relevant service command;*
- *FTP sub-commands specified in RFC 959, and the optional commands introduced by RFC 2228;*
- *HTTP request methods specified in RFC 2616.*
- *Stateful packet attributes: for Connection-oriented protocols (sequence number, acknowledgement number, Flags (SYN, ACK, RST, and FIN)) and Connectionless protocols (source and destination network identifiers, source and destination service identifiers)*].

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:

a) [*Subjects 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.*

b) 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(2).6 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);

f) The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose].

Application Note: FDP_IFF.1(2).3, FDP_IFF.1(2).4, and FDP_IFF.1(2).5 are omitted as indicated in the Application level FW PP.

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

Hierarchical to: No other components

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

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

Subjects: TOE Interfaces

Security attributes:

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

Information: network packets

Security attributes:

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

FDP_IFF.1(3).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [*the presumed identity of the source subject is in the set of source subject identifiers*;
b) the identity of the destination subject is in the set of source destination identifiers;
c) the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by an authorized administrator) according to the first match algorithm; and
d) the selected information flow policy rule specifies that the information flow is to be permitted, and which SSL or IPSec operation is to be applied to that information flow].

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

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

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

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

d) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.)].

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

Hierarchical to: No other components

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

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

Subjects: Human users

Security attributes:

- *Optional User ID*
- *Optional User Group*

Information: Web pages

Security attributes:

- *URL;*
- *Category assigned by FortiGuard web filtering service based on the website content; and*
- *Category group assigned by FortiGuard web filtering service; and*
- *Classification assigned by FortiGuard web filtering service based on the characteristics of the site, if applicable;*
- *Local category, if applicable;*
- *Override, if applicable.*]

FDP_IFF.1(4).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [*The policy for the category, category group and classification to which the URL has been assigned by the FortiGuard web filtering service is set to 'allow'; or*

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

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

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

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

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

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

Application Note: The FortiGuard web filtering service assigns all websites to a category based on content. Those not assigned to other categories are assigned to the 'Unrated' category. Category groups are similar categories grouped together for ease of administration. A classification is assigned based on the characteristics of the site rather than the site content. For example, the cached content classification indicates that the site caches content, but provides no indication of the content type. Not every URL has an assigned classification. A quota is a time limit placed on viewing URLs assigned to a particular category, category group or classification.

6.2.3.9 FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all objects.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1(1) Authentication failure handling (Application Level Firewall)

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1(1).1 The TSF shall detect when [a non-zero number determined by the authorized administrator] of unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1(1).2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question.]

6.2.4.2 FIA_AFL.1(2) Authentication failure handling (Traffic Filter Firewall)

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1(2).1 The TSF shall detect when [a settable, non-zero number determined by the authorized administrator] of unsuccessful authentication attempts occur related to [external IT entities attempting to authenticate from an internal or external network].

FIA_AFL.1(2).2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT entity from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT entity in question.]

6.2.4.3 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) [*identity;*

b) association of a human user with the authorized administrator role;

c) authentication data; and

d) authorizations.]

6.2.4.4 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*identification as stated in FIA_UID.2*] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA_UAU.1.2 The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized external IT entity.

6.2.4.5 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) authorized administrators;

b) authorized external IT entities].

6.2.4.6 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*password; single use* ***and device level X.509 certificate based*** *authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authentication 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].

6.2.4.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is identified.

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

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1(1) Management of security functions behaviour (Traffic Filter FW)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(1).1 The TSF shall restrict the ability to [perform] the functions

a) [*start up and shutdown;*

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);

g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);

h) modify and set the time and date;

i) archive, create, delete, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup; and

l) additionally, if the TSF supports remote administration from either an internal or external network:

- *enable and disable remote administration from internal and external networks;*
- *restrict addresses from which remote administration can be performed*]

to [*an authorized administrator*].

6.2.5.2 FMT_MOF.1(2) Management of security functions behaviour (IDS Sensor)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(2).1 The TSF shall restrict the ability to [modify the behaviour of] the functions [*Sensor data collection and review*] to [*authorized Sensor administrators*] .

Application Note: For this requirement, the phrase 'modify the behaviour of' refers to the ability of all Administrators to manage the IDS functions of the TOE.

Application Note: The term "Sensor administrator" originates from the IDS Sensor PP. It is essentially an administrator whose profile allows sensor data collection and review activities.

6.2.5.3 FMT_MOF.1(3) Management of security functions behaviour (Application Level FW 1)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(3).1 The TSF shall restrict the ability to [enable, disable] the functions

a) [*operation of the TOE;*

b) multiple use authentication functions described in FIA_UAU.5] to[*an authorized administrator*].

Application Note: By "Operation of the TOE" in a) above, the PP means having the TOE start up (enable operation) and shut down (disable operation). By "multiple use authentication" in b) above, the PP means the management of password and single use authentication mechanisms.

6.2.5.4 FMT_MOF.1(4) Management of security functions behaviour (Application Level FW 2)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(4).1 The TSF shall restrict the ability to [enable, disable, determine and modify the behaviour of] the functions

a) [*audit trail management;*

b) backup and restore for TSF data, information flow rules, and audit trail data; and

c) communication of authorized external IT entities with the TOE] to [*an authorized administrator*].

Application Note: Determine and modify the behaviour of element c (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

6.2.5.5 FMT_MSA.1(1) Management of security attributes (Application Level FW 1)

Hierarchical to: No other components.

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

FMT_MSA.1(1).1 The TSF shall enforce the [*UNAUTHENTICATED SFP*] to restrict the ability to [*delete attributes from a rule, modify attributes in a rule, add attributes to a rule*] the security attributes [*listed in section FDP_IFF.1(1).1*] to [*the authorized administrator*].

6.2.5.6 FMT_MSA.1(2) Management of security attributes (Application Level FW 2)

Hierarchical to: No other components.

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

FMT_MSA.1(2).1 The TSF shall enforce the [*AUTHENTICATED SFP*] to restrict the ability to [*delete attributes from a rule, modify attributes in a rule, add attributes to a rule*] the security attributes [*listed in section FDP_IFF.1(2).1*] to [*the authorized administrator*].

6.2.5.7 FMT_MSA.1(3) Management of security attributes (Application Level FW 3)

Hierarchical to: No other components.

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

FMT_MSA.1(3).1 The TSF shall enforce the [*UNAUTHENTICATED SFP*] to restrict the ability to delete and [*create*] the security attributes [*information flow rules described in FDP_IFF.1(1)*] to [*the authorized administrator*].

6.2.5.8 FMT_MSA.1(4) Management of security attributes (Application Level FW 4)

Hierarchical to: No other components.

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

FMT_MSA.1(4).1 The TSF shall enforce the [*AUTHENTICATED SFP*] to restrict the ability to delete and [*create*] the security attributes [*information flow rules described in FDP_IFF.1(2)*] to [*the authorized administrator*].

6.2.5.9 FMT_MSA.1(5) Management of security attributes (VPN)

Hierarchical to: No other components.

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

FMT_MSA.1(5).1 The TSF shall enforce the [*VPN SFP*] to restrict the ability to [query, modify, delete] the security attributes [*source and destination subject identifiers*] to [*the authorized administrator*].

6.2.5.10 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

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

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

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 (1) and FDP_IFF.1 (2) are intended to be restrictive in the sense that

both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

6.2.5.11 FMT_MTD.1(1) Management of TSF data (IDS Sensor)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1(1).1 The TSF shall restrict the ability to [query *and add Sensor and audit data, and shall restrict the ability to query and modify all other TOE data*] to [*the authorized administrators*].

6.2.5.12 FMT_MTD.1(2) Management of TSF data (Application Level Firewall 1)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1(2).1 The TSF shall restrict the ability to [query, modify, delete] the [*user attributes defined in FIA_ATD.1.1*] to [*the authorized administrator*].

6.2.5.13 FMT_MTD.1(3) Management of TSF data (Application Level Firewall 2)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1(3).1 The TSF shall restrict the ability to [*set*] the [*time and date used to form the timestamps in FPT_STM.1.1*] to [*the authorized administrator*].

6.2.5.14 FMT_MTD.2 Management of limits on TSF data (Application Level Firewall)

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security Roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [*the number of authentication failures*] to [*the authorized 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)1.2*]

6.2.5.15 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) administer cryptographic functionality;

b) administer web filtering functionality;

c) administer VPN functionality; and

d) administer security audit and alarm functionality].

Application Note: Many of the management functions are covered in FMT_MOF.1, iterations 1 through 4, as detailed in the referenced PPs. This SFR is used to cover any management functions not explicitly expressed therein.

6.2.5.16 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the following roles [*authorised administrator, and authorised Sensor administrators*].

Application Note: The TOE does not specifically maintain a role called "Sensor administrator". However, an access profile may be created to limit any administrator to manage only the sensor functionality.

FMT_SMR.1.2 The TSF shall be able to associate human users with the authorized administrator role~~s~~.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.2.6.2 FPT_ITA.1 Inter-TSF availability within a defined availability metric (IDS Sensor)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITA.1.1 The TSF shall ensure the availability of [audit and sensor data] provided to a remote trusted IT product within [*one minute of creating the audit record*] given the following conditions [*audit or Sensor data is available for transmission*].

6.2.6.3 FPT_ITC.1 Inter-TSF confidentiality during transmission (IDS Sensor)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

6.2.6.4 FPT_ITI.1 Inter-TSF detection of modification (IDS Sensor)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*by comparing SHA-1 hash results*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*drop and log the packet*] if modifications are detected.

6.2.6.5 FPT_STM.1 Reliable time stamps (IDS Sensor, Application Level FW, Traffic Filter FW)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*authentication and High Availability Cluster communication*].

6.2.7.2 FTP_TRP Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*proxy user, VPN User and remote administration*].

6.2.8 IDS Component Requirements (IDS)

6.2.8.1 IDS_COL_EXT.1 Sensor Data Collection (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_COL_EXT.1.1 The Sensor shall be able to collect the following events from the targeted IT System resource(s):

a) [network traffic]; and

b) [*no other specifically defined events*].

IDS_COL_EXT.1.2 At a minimum, the Sensor shall collect 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) The additional information specified in the Details column of Table 3 Sensor Events.

Component	Event	Details
IDS_COL_EXT.1	Start-up and shutdown	none
IDS_COL_EXT.1	Identification and authentication events	User identity, location, source address, destination address

Component	Event	Details
IDS_COL_EXT.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_COL_EXT.1	Service Requests	Specific service, source address, destination address
IDS_COL_EXT.1	Network traffic	Protocol, source address, destination address
IDS_COL_EXT.1	Security configuration changes	Source address, destination address
IDS_COL_EXT.1	Data introduction	Object IDS, location of object, source address, destination address

6.2.8.2 IDS_RDR_EXT.1 Restricted Data Review (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_RDR_EXT.1.1 The Sensor shall provide [*Administrators*] with the capability to read [*all entries*] from the Sensor data.

IDS_RDR_EXT.1.2 The Sensor shall provide the Sensor data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The Sensor shall prohibit all users read access to the Sensor data, except those users that have been granted explicit read-access.

6.2.8.3 IDS_STG_EXT.1 Guarantee of Sensor Data Availability (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_STG_EXT.1.1 The Sensor shall protect the stored Sensor data from unauthorised deletion.

IDS_STG_EXT.1.2 The Sensor shall protect the stored Sensor data from modification.

Application Note: Authorized deletion of data is not considered a modification of Sensor data in this context. This requirement applies to the actual content of the Sensor Data, which should be protected from any modifications.

IDS_STG_EXT.1.3 The Sensor shall ensure that [*the authorized administrator's selection of all or the most recent*] Sensor data will be maintained when the following conditions occur: [Sensor data storage exhaustion].

6.2.8.4 IDS_STG_EXT.2 Prevention of Sensor Data Loss (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

IDS_STG_EXT.2.1 The Sensor shall provide an authorized administrator the capability to select one of the following actions [

a) prevent Sensor data, except those taken by the authorised user with special rights; or

b) overwrite the oldest stored Sensor data.]

and send an alarm if the storage capacity has been reached.

6.2.9 Anti-Virus Action Requirements (FAV)

6.2.9.1 FAV_ACT_EXT.1 Anti-Virus Actions (EXT)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- quarantine the content of the information flow
- remove the content of the information flow

to be taken on detection of a virus in an information flow.

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

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

6.3 SECURITY REQUIREMENTS RATIONALE

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

	O.ACCESS	O.ACCOUN	O.AUDITS	O.AUDREC	O.EADMIN	O.ENCRYP	O.EXPORT	O.IDACTS	O.IDAUTH	O.INTEGR	O.INTEGRITY	O.LIMEXT	O.MEDIAT	O.OFLOWS	O.PROTCT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE	O.TIME	O.VIRUS
FAU_ARP.1				X																	
FAU_GEN.1		X	X	X																	
FAU_GEN.2			X																		
FAU_SAA.1				X																	
FAU_SAR.1				X	X																
FAU_SAR.2	X								X												
FAU_SAR.3				X	X																
FAU_SEL.1			X		X																
FAU_STG.2	X								X	X				X	X	X	X	X			
FAU_STG.4			X											X		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_IFC.1(3)											X										
FDP_IFC.1(4)													X								
FDP_IFF.1(1)													X								
FDP_IFF.1(2)													X								
FDP_IFF.1(3)											X										
FDP_IFF.1(4)													X								
FDP_RIP.2													X								
FIA_AFL.1(1)																		X			
FIA_AFL.1(2)																		X			
FIA_ATD.1									X							X			X		
FIA_UAU.1	X								X										X		
FIA_UAU.4									X										X		

	O.ACCESS	O.ACCOUN	O.AUDITS	O.AUDREC	O.EADMIN	O.ENCRYP	O.EXPORT	O.IDACTS	O.IDAUTH	O.INTEGR	O.INTEGRITY	O.LIMEXT	O.MEDIAT	O.OFLOWS	O.PROTCT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE	O.TIME	O.VIRUS
FIA_UAU.5									X										X		
FIA_UID.2	X	X							X												
FMT_MOF.1(1)	X											X					X				
FMT_MOF.1(2)	X				X				X							X					
FMT_MOF.1(3)												X				X	X				
FMT_MOF.1(4)												X				X	X				
FMT_MSA.1(1)	X												X			X	X				
FMT_MSA.1(2)	X												X			X	X				
FMT_MSA.1(3)	X												X			X	X				
FMT_MSA.1(4)	X												X			X	X				
FMT_MSA.1(5)													X			X	X				
FMT_MSA.3													X			X	X				
FMT_MTD.1(1)	X								X	X					X						
FMT_MTD.1(2)																X					
FMT_MTD.1(3)																X					
FMT_MTD.2																X					
FMT_SMF.1																X					
FMT_SMR.1									X							X					
FPT_FLS.1																	X	X			
FPT_ITA.1							X														
FPT_ITC.1							X			X											
FPT_ITT.1							X			X											
FPT_STM.1				X																X	
FTP_ITC.1							X														
FTP_TRP.1						X															
IDS_COL_EXT.1								X													
IDS_RDR_EXT.1	X				X				X												
IDS_STG_EXT.1															X						
IDS_STG_EXT.2	X								X	X				X							

	O.ACCESS	O.ACCOUN	O.AUDITS	O.AUDREC	O.EADMIN	O.ENCRYP	O.EXPORT	O.IDACTS	O.IDAUTH	O.INTEGR	O.INTEGRITY	O.LIMEXT	O.MEDIAT	O.OFLOWS	O.PROTCT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE	O.TIME	O.VIRUS
FAV_ACT_EXT.1																					X

Table 12 - Mapping of SFRs to Security Objectives

6.3.1 Security Functional Requirements Rationale Related to Security Objectives

Table 13 shows the Security Functional Requirements Rationale related to Security Objectives.

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FAU_SAR.2	Restricted audit review
	FAU_STG.2	Guarantees of audit data availability
	FIA_UAU.1	Timing of authentication
	FIA_UID.2	User identification before any action
	FMT_MTD.1(1)	Management of TSF data (audit data)
	IDS_RDR_EXT.1	Restricted data review
	IDS_STG_EXT.2	Prevention of sensor data loss
Rationale:	The TOE restricts the review of audit data to those granted explicit access in accordance with FAU_SAR.2, and protects the audit data from deletion as well as guarantee the availability of the audit data in accordance with FAU_STG.2. Users authorized to access the TOE are defined using an identification and authentication process as directed by FIA_UID.2 and FIA_UAU.1. Only authorized administrators of the Sensor may query and add Sensor and audit data, as indicated in FMT_MTD.1. The Sensor is required to restrict the review of collected Sensor data to those granted with explicit read access in accordance with IDS_RDR_EXT.1, and the sensor protects the Sensor data collected from an IT System from any modification and unauthorized deletion as detailed in IDS_STG_EXT.1.	
Objective: 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.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FIA_UID.2	User identification before any action
Rationale:	FAU_GEN.1 outlines the data that must be included in audit records and which events must be audited. FIA_UID.2 ensures that a user is identified to the TOE prior to the execution of any action on behalf of that user.	

Objective: O.AUDITS	The TOE must record audit records for data accesses and use of the Sensor functions.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
	FAU_STG.4	Prevention of audit data loss
Rationale:	FAU_GEN.1 details the set of events that the TOE must be capable of recording, ensuring that any security relevant event that takes place in the TOE is audited. This requirement also details the information that must be contained in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. FAU_SEL.1 allows an authorized administrator to configure which auditable events will be recorded in the audit trail. FAU_STG.4 mitigates audit data loss by taking specific action when the audit trail is full.	
Objective: 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.	
Security Functional Requirements:	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_ARP.1 requires that the alarm be displayed at the local administrative console and at the remote administrative console(s) when an administrative session exists. FAU_GEN.1 ensures that audit data is recorded, while FAU_SAA.1 defines the events that indicate a potential security violation and will generate an alarm. FAU_SAR.1 provides the administrators with the capability to read the entire audit data contained in the audit trail. 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. FPT_STM.1 supports the	

	audit functionality by ensuring the availability of reliable timestamp information.	
Objective: O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.	
Security Functional Requirements:	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FMT_MOF.1(2)	Management of security functions behaviour (IDS Sensor)
	IDS_RDR_EXT.1	Restricted data review
Rationale:	The TOE must provide the ability to review and manage the audit trail in accordance with FAU_SAR.1, FAU_SAR.3, and FAU_SEL.1. The TOE provides the capability to collect and review sensor data in accordance with FMT_MOF.1(2) and IDS_RDR_EXT.1.	
Objective: 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.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FTP_TRP.1	Trusted path
Rationale:	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 ensure that the TOE supports cryptographic operations that are necessary to protect the confidentiality of its dialogue with an authorized administrator through encryption. FTP_TRP.1 further details that protected communication.	
Objective: O.EXPORT	When the TOE makes its Sensor data available to other IDS components, the TOE will ensure the confidentiality of the Sensor data.	

Security Functional Requirements:	FPT_ITA.1	Inter-TSF availability within a defined availability metric
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FTP_ITC.1	Inter-TSF trusted channel
Rationale:	The TOE makes the collected data available to other IT products in accordance with FPT_ITA.1. The TOE protects the collected data from modification, and ensures its integrity when the data is transmitted to another IT product, as detailed in FPT_ITC.1, FPT_ITI.1, and FTP_ITC.1.	
Objective: O.IDACTS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	
Security Functional Requirements:	IDS_COL_EXT.1	Sensor data collection
Rationale:	The Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System, as detailed IDS_COL_EXT.1.	
Objective: 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.	
Security Functional Requirements:	FAU_SAR.2	Restricted audit review
	FAU_STG.2	Guarantees of audit data availability
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action

	FMT_MOF.1(2)	Management of security functions behaviour (IDS Sensor)
	FMT_MTD.1(1)	Management of TSF data (audit data)
	FMT_SMR.1	Security Roles
	IDS_RDR_EXT.1	Restricted data review
	IDS_STG_EXT.2	Prevention of sensor data loss
Rationale:	FAU_SAR.2 requires that the TOE restrict the review of audit data to those granted with explicit read-access permission, and FAU_STG.2 requires that the TOE protect the stored audit records from unauthorized deletion. Subject security attributes are uses to enforce the authentication policy of the TOE, as detailed in FIA_ATD.1. Users authorized to access the TOE must be identified and authenticated in accordance with FIA_UID.2, FIA_UAU.1, FIA_UAU.4, and FIA_UAU.5. The TOE provides the ability to restrict the management of the behaviour of functions of the TOE to authorized users as detailed in FMT_MOF.1(2) and FMT_MTD.1. The Sensor restricts the review of collected Sensor data to those granted explicit read access, as noted in IDS_RDR_EXT.1, and protects the collected Sensor data and guarantees the availability of the data in the event of storage exhaustion, failure or attack in accordance with IDS_STG_EXT.1. The TOE roles supporting this functionality are detailed FMT_SMR.1.	
Objective: O.INTEGR	The TOE must ensure the integrity of all audit and Sensor data.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FMT_MTD.1(1)	Management of TSF data (audit data)
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	IDS_STG_EXT.2	Prevention of sensor data loss
Rationale:	FAU_STG.2 ensures that the TOE protects the audit data from deletion, and guarantees the availability of the audit data in the event of storage exhaustion, failure or attack. Only authorized administrators may query or add audit and Sensor data, in accordance with FMT_MTD.1(1). The Sensor protects the collected data from modification and ensures its integrity when the data is transmitted to	

	another IT product, as detailed in FPT_ITC.1 and FPT_ITI.1. The TOE prevents the loss of Sensor data, as detailed in IDS_STG_EXT.2.	
Objective: O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer TOE via encryption and provide authentication for such data.	
Security Functional Requirements:	FDP_IFC.1(3)	Subset information flow control (VPN policy)
	FDP_IFF.1(3)	Simple security attributes (VPN Policy)
Rationale:	FDP_IFC.1(3) and FDP_IFF.1(3)) satisfies this objective by defining the VPN Information Flow Security Functional Policy that ensures that all IPSec and SSL encrypted data is authenticated and integrity is ensured through encryption.	
Objective: 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.	
Security Functional Requirements:	FMT_MOF.1(1)	Management of security functions behaviour (Traffic Filter FW)
	FMT_MOF.1(3)	Management of security functions behaviour (Application Level FW 1)
	FMT_MOF.1(4)	Management of security functions behaviour (Application Level FW 2)
Rationale:	FMT_MOF.1(1), FMT_MOF.1(3) and FMT_MOF.1(4) ensure that the TSF restricts the ability to modify the behaviour of management functions relevant to the firewall functionality to an authorized administrator.	
Objective: O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.	
Security Functional Requirements:	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_IFC.1(4)	Subset information flow control (web filtering policy)
	FDP_IFF.1(4)	Simple security attributes (web filtering policy)
	FDP_RIP.2	Full residual information protection
	FMT_MSA.1(1)	Management of security attributes (Application Level FW 1)
	FMT_MSA.1(2)	Management of security attributes (Application Level FW 2)
	FMT_MSA.1(3)	Management of security attributes (Application Level FW 3)
	FMT_MSA.1(4)	Management of security attributes (Application Level FW 4)
	FMT_MSA.1(5)	Management of security attributes (VPN)
	FMT_MSA.3	Static attribute initialization
Rationale:	FDP_IFC.1(1) and FDP_IFF.1(1) detail how the TOE mediates the flow of information for the unauthenticated policy required for the Traffic Filter Firewall and Application Level Firewall functionality. FDP_IFC.1(2) and FDP_IFF.1(2) detail how the TOE mediates the flow of information for the authenticated policy required for the Traffic Filter Firewall and Application Level Firewall functionality. FDP_IFC.1(4) and FDP_IFF.1(4) detail how the TOE mediates the flow of information for the web filtering policy. FDP_RIP.2 ensures that residual information from a previous information flow becomes unavailable on reallocation of the resource. FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.1(5) and FMT_MSA.3 provide for the management of that functionality.	
Objective:	The TOE must appropriately handle potential audit and Sensor data	

O.OFLOWS	storage overflows.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
	IDS_STG_EXT.1	Guarantee of sensor data availability
	IDS_STG_EXT.2	Prevention of sensor data loss
Rationale:	The TOE protects the audit data from deletion as well as guarantees the availability of the audit data in the event of storage exhaustion, failure or attack, in accordance with FAU_STG.2. The TOE prevents the loss of audit data in the event its audit trail is full, as detailed in FAU_STG.4. The Sensor protects the collected Sensor data from modification and unauthorized deletion, as well as guarantees the availability of the data in the event of storage exhaustion, failure or attack, as noted in IDS_STG_EXT.1, and the Sensor prevents the loss of audit data in the event its audit trail is full as detailed in IDS_STG_EXT.2.	
Objective: O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FMT_MTD.1(1)	Management of TSF data (audit data)
	IDS_STG_EXT.1	Guarantee of sensor data availability
Rationale:	The TOE protects audit data from unauthorized modification in accordance with FAU_STG.2. FMT_MTD.1 restricts the ability to add Sensor and audit data, and to query and modify TOE data to authorized administrators. The Sensor protects the Sensor data from any modification and unauthorized deletion, in accordance with IDS_STG_EXT.1.	
Objective: 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.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
	FIA_ATD.1	User attribute definition

	FMT_MOF.1(2)	Management of security functions behaviour (IDS Sensor)
	FMT_MOF.1(3)	Management of security functions behaviour (Application Level FW 1)
	FMT_MOF.1(4)	Management of security functions behaviour (Application Level FW 2)
	FMT_MSA.1(1)	Management of security attributes (Application Level FW 1)
	FMT_MSA.1(2)	Management of security attributes (Application Level FW 2)
	FMT_MSA.1(3)	Management of security attributes (Application Level FW 3)
	FMT_MSA.1(4)	Management of security attributes (Application Level FW 4)
	FMT_MSA.1(5)	Management of security attributes (VPN)
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(2)	Management of TSF data (cryptographic TSF data)
	FMT_MTD.1(3)	Management of TSF data (time TSF data)
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMR.1	Security Roles
	FMT_SMF.1	Specification of Management Functions
Rationale:	FAU_STG.2 ensures that the audit trail is protected from tampering, and access to the security functionality is limited to the authorized administrator. FAU_STG.4 ensures that the authorized administrator will be able to manage the audit trail if it should become full. FIA_ATD.1 allows for the provision of attributes to distinguish user permissions and support accountability. The FMT_MOF iterations detail a list of security functions supported by the TOE. The FMT_MSA.1 iterations further detail the functionality required to manage the TOE, and to restrict that functionality to authorized users. The FMT_MTD iterations describe the types of TSF data, and detail how access to this data must be restricted. FMT_MTD.2 ensures that the TSF restricts 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_SMF.1 also specifies management functions, and FMT_SMR.1 details the security roles supporting all this functionality.	
Objective: 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.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
	FMT_MOF.1(1)	Management of security functions behaviour (Traffic Filter FW)
	FMT_MOF.1(3)	Management of security functions behaviour (Application Level FW 1)
	FMT_MOF.1(4)	Management of security functions behaviour (Application Level FW 2)
	FMT_MSA.1(1)	Management of security attributes (Application Level FW 1)
	FMT_MSA.1(2)	Management of security attributes (Application Level FW 2)
	FMT_MSA.1(3)	Management of security attributes (Application Level FW 3)
	FMT_MSA.1(4)	Management of security attributes (Application Level FW 4)
	FMT_MSA.1(5)	Management of security attributes (VPN)
	FMT_MSA.3	Static attribute initialization
	FPT_FLS.1	Failure with preservation of secure state
Rationale:	FAU_STG.2 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 administer the audit trail, should it become full. The FMT_MOF.1 iterations restrict the ability to perform various security management functions to authorized administrators, mitigating the risk of compromise to TOE or other connected resources. The FMT_MSA.1	

	iterations ensure that the TSF enforces the various SFPs to restrict the ability to modify TOE security attributes. FMT_MSA.3 provide for restrictive default values to ensure that the flow of information is denied, unless specifically authorized. FPT_FLS.1 allows for further protection, maintaining a secure state in the case of failover.	
Objective: O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	
Security Functional Requirements:	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
	FIA_AFL.1(1)	Authentication failure handling
	FIA_AFL.1(2)	Authentication failure handling
	FPT_FLS.1	Failure with preservation of secure state
Rationale:	FAU_STG.2 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 administer the audit trail if it should become full. FIA_AFL.1(1) and FIA_AFL(2) ensure that unauthorized users cannot perform a brute force attack in an attempt to authenticate. After a configurable number of failures, authentication becomes unavailable to the user until restored by an authorized administrator. FPT_FLS.1 allows for further protection, maintaining a secure state in the case of failover.	
Objective: O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms

Rationale:	FIA_ATD.1 supports this objective by detailing the user attributed used in identification and authentication. FIA_UAU.1, FIA_UAU.4 and FIA_UAU.5 describe the multiple authentication mechanisms, and require their appropriate use in all attempts to authenticate at the TOE from an internal or external network.	
Objective: O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
	FMT_MTD.1(3)	Management of TSF data (AppFW2)
Rationale:	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use. FMT_MTD.1(3) provides the capability to set the time used for generating time stamps to an authorized administrator.	
Objective: O.VIRUS	The TOE will detect and block viruses contained within an information flow which arrives at any of the TOE network interfaces.	
Security Functional Requirements:	FAV_ACT_EXT.1	Anti Virus Actions
Rationale:	FAV_ACT_EXT.1 ensures that the TOE can detect and block information that may contain a virus.	

Table 13 - Security Functional Requirements Rationale

6.4 DEPENDENCY RATIONALE

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.

SFR	Dependencies	Dependency Satisfied
FAU_ARP.1	FAU_SAA.1	Yes
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes
FAU_SAA.1	FAU_GEN.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes

SFR	Dependencies	Dependency Satisfied
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Although FAU_STG.1 is not included, FAU_STG.2, which is hierarchical to FAU_STG.1 is included, thereby satisfying the dependency.
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Yes
FCS_CKM.4	FCS_CKM.1	Yes
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Yes
FDP_IFC.1(1)	FDP_IFF.1	Yes
FDP_IFC.1(2)	FDP_IFF.1	Yes
FDP_IFC.1(3)	FDP_IFF.1	Yes
FDP_IFC.1(4)	FDP_IFF.1	Yes
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFF.1(4)	FDP_IFC.1 FMT_MSA.3	FMT_MSA.3 is not included for this SFR. None of the security attributes used by the web filtering SFP have default values. User ID and User Group have no values until assigned. Only the local category and override attributes are set within the TOE, and these have no values until assigned. Therefore, the dependency is satisfied.

SFR	Dependencies	Dependency Satisfied
FDP_RIP.2	None	Yes
FIA_AFL.1(1)	FIA_UAU.1	Yes
FIA_AFL.1(2)	FIA_UAU.1	Yes
FIA_ATD.1	None	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.4	None	Yes
FIA_UAU.5	None	Yes
FIA_UID.2	None	Yes
FMT_MOF.1(1)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MOF.1(2)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MOF.1(3)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MOF.1(4)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1(1)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1(2)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1(3)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1(4)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.1(4)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes

SFR	Dependencies	Dependency Satisfied
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes
FMT_MTD.1(1)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MTD.1(2)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MTD.1(3)	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_FLS.1	None	Yes
FPT_ITA.1	None	Yes
FPT_ITC.1	None	Yes
FPT_ITI.1	None	Yes
FPT_STM.1	None	Yes
FTP_ITC.1	None	Yes
FTP_TRP.1	None	Yes
IDS_COL_EXT.1	None	Yes
IDS_RDR_EXT.1	None	Yes
IDS_STG_EXT.1	None	Yes
IDS_STG_EXT.2	None	Yes
FAV_ACT_EXT.1	None	Yes

Table 14 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.3). EAL 4 was chosen for competitive reasons. The developer is

claiming the ALC_FLR.3 augmentation since there are a number of areas where current Fortinet practices and procedures exceed the minimum requirements for EAL 4.

The assurance requirements are summarized in Table 15.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objective
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition

Assurance Class	Assurance Components	
	Identifier	**Name**
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Table 15 - EAL 4 Assurance Requirements

6.6 PROTECTION PROFILE TAILORING

The following tailoring was applied to the Application Level FW PP, the Traffic Filter FW PP and the IDS Sensor PP to produce this ST. All changes are compliant with demonstrable PP conformance in accordance with Section D3 of the CC.

The following tailoring was performed with respect to the three referenced PPs:

a) Additional threats were added, but these threats are not contradictory and only add to the required functionality of the TOE;

b) Additional organizational security policies were added, but these are not contradictory and only add to the required functionality of the TOE;

c) Additional security objectives were added, but these are not contradictory and only add to the required functionality of the TOE;

d) In response to consumer demand, the assurance package was upgraded from EAL2 to EAL4, augmented by ALC_FLR.3; and

e) The names of the security objectives for the environment were changed from the "O.XXX" notation in the FW PPs to "OE.XXX" notation to provide a clearer distinction from the TOE security objectives, which are labelled "O.XXX".

f) A.ACCESS was removed as an assumption, as the assumption was not appropriate for the Application Level FW PP and the Traffic Filter FW PP. OE.INTROP was removed as there is a 1-to-1 mapping between A.ACCESS and OE.INTROP. This assumption and objective for the environment are not necessary as the IDS function is performed on data passing through the TOE (not collected from systems external to the TOE) and is processed based on rules internal to the TOE. Therefore it is unnecessary to restrict the environment in such a way. A.SINGEN was added to ensure that the TOE has access to all information (e.g. traffic) it needs.

g) FDP_RIP.1 (from the FW PPs) was replaced with FDP_RIP.2. Since FDP_RIP.2 is hierarchical to FDP_RIP.1, the PP requirement is met.

h) FAU_GEN.1.1 – Subparagraph c) from the PP was reworded to include the requirements from all three PPs.

i) The PP-specific requirements for audit data generation (FAU_GEN.1) were merged with other audit requirements into one comprehensive table;

j) FAU_STG.1 was replaced with FAU_STG.2. Since FAU_STG.2 is hierarchical to FAU_STG.1, the requirement from the FW PPs has been met.

k) From the Application Level Firewall PP, FIA_UAU.5.1 – Added device level X.509 certificate based authentication mechanism in support of VPN peers;

l) Several assumptions not included in the IDS Sensor PP were included in the Firewall PPs, and are therefore included in the ST;

m) FAU_SAA.1.1 from the IDS Sensor PP - 'the audited events' was changed to 'events';

n) FAU_STG.2.2 – The IDS Sensor PP requires that a compliant TOE ‘detect’ audit trail modifications. The requirement has been refined to be more restrictive by replacing the word ‘detect’ with ‘prevent’;

o) FIA_UID.1 was replaced by FIA_UID.2. Since FIA_UID.2 is hierarchical to FIA_UID.1, the IDS Sensor PP requirement is met; and

p) IDG_STG_EXP.2 – This requirement from the IDS Sensor PP has been refined to show that the TOE is capable of two, rather than just one of the selections provided by that PP.

7 TOE SUMMARY SPECIFICATION

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

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

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

The administrator can review, search and sort the audit records. Filtering which audit records are to be displayed may be done using the FortiOS reports feature, which allows reports to be configured and run from logs stored on the FortiGate unit's hard drive. Report configurations essentially provide a means of filtering and sorting logs. This is only supported in the Network Web-Based GUI. The audit records are stored locally; using memory, a hard disk or a FLASH memory card depending on the model. The storage devices used by each model for audit record storage are identified in Table 2.

An authorized 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 an authorized administrator. The 95% audit log threshold limit allows the TOE to record the actions taken by an authorized administrator to clear the error mode. When log rolling is enabled the oldest audit records are overwritten.

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

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

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

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

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

Upon detecting a potential policy violation, the TOE immediately displays an alarm message identifying the potential policy violation and, at the option of an authorized 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.

TOE Security Functional Requirements addressed: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2 FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.2 and FAU_STG.4.

7.1.2 Identification and Authentication

In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access and network user access to specific services. The TOE maintains identity, role/authorization and authentication data to support this functionality. Identification and authentication is always enforced on the serial interface (local console). On the network interfaces identification and authentication is enforced for all administrator access, specific services, and VPN users. For local administrators, the identification and authentication mechanism is a username and password combination; for remote administration and user access to Telnet and FTP protocols, a FortiToken one-time password is required for authentication. Proxy users and administrators are presented with a system screen (configurable by an authorized administrator) prior to authentication, and must access this screen and authenticate prior to access. VPN users authenticate using preshared keys or certificates for IPSec VPNs and certificates for SSL VPNs. The accounts are created by an authorized administrator over the serial or network interfaces. All proxy user sessions, VPN user sessions, and administrator sessions are subject to a time out value. When a session is inactive for a period of time which exceeds this value, the session is terminated by the TOE. An authorized administrator may set the timeout value in the range from 1 to 480 minutes. The timeout values for proxy user sessions and administrator sessions are independent and may be set to different values by an authorized administrator. The user is required to re-authenticate to gain access following timeout.

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

The TOE also requires identification and authentication for high availability units in a cluster. Each unit has a unique identifier (username) and a shared password.

The USB interface does not directly require identification and authentication since the authorized administrator must be authenticated to load keys from the USB token.

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

7.1.3 Protection (Cryptographic Support and Trusted Path/Channel)

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

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

The Network CLI uses SSH version 2 and only supports the use of the following FIPS PUB 140-2 approved algorithms to encrypt all authentication and communications data:

- 3DES
- AES
- HMAC-SHA1

Only administrator accounts stored in the local authentication database are permitted to be authenticated (i.e. root authentication and proxy user accounts cannot be used).

By default, SSH connections to the TOE are disabled and must be explicitly enabled before an administrator can use the Network CLI interface.

The TOE supports the use of fingerprints as defined in RFC 4251, in that it provides "[a method] for verifying the correctness of host keys, e.g., a hexadecimal fingerprint derived from the SHA-1 hash [FIPS-180-2] of the public key." When a Network CLI connection is first established, the TOE transmits a 2048-bit RSA public key to the connecting client which can be used to validate the identity of the TOE. Each FortiGate unit is delivered with a factory installed 2048-bit RSA public/private key pair. However an authorized administrator may use a USB token to replace this key pair with another key pair which he has generated or obtained from an alternate source. An administrator attempting to establish a Network CLI connection with the TOE can choose to allow or disconnect the connection based on the aforementioned fingerprint. If the administrator chooses to continue, the identity of the TOE is considered to be valid and the TOE prompts the connecting client for user and password credentials.

The Network Web-Based GUI uses the HTTPS protocol for secure administrator communications. With respect to the TOE implementation of HTTPS, TLS version 1.0 (RFC 2246) is used to encrypt and authenticate administration sessions between the remote browser and TOE. The TOE supports ciphersuites; TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (RFC 2246) and TLS_DHE_RSA_WITH_AES_128_CBC_SHA (RFC 3268).

These ciphersuites mean that the keying material is determined when the session is established through a Diffie-Hellman (DH) exchange which consists of:

- Server sends 2048-bit RSA public certificate

- Server generates, signs (RSA PKCS#1) and sends DH parameters and DH public value
- Client generates and sends DH public value. The keying material is then used to encrypt/decrypt (AES128 and 3DES) and authenticate (HMAC-SHA1) the data exchange.

By default, HTTPS connections to the TOE are disabled and must be explicitly enabled before an administrator may use the Network Web-Based GUI.

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

The trusted channels provide communication between the TOE and the FortiGuard Distribution Server and FortiAnalyzer units. These channels are logically distinct from other communication channels and provide assured identification of the end points and protection of the channel data from disclosure. A FortiGuard Distribution Server may be used to obtain updates to the IDS/IPS (attack) signatures and virus definitions, and a FortiAnalyzer unit may be used to collect and analyze logging information.

The TOE must be explicitly configured to obtain AV and IDS/IPS signature updates from the FortiGuard Distribution Server. A User Datagram Protocol (UDP) port must be specified for this purpose. This UDP port is used by the FortiGuard Distribution Network to advise the TOE that signature updates are available for download. When the TOE becomes aware that an update is available it will, if so configured, initiate a trusted channel connection to the FortiGuard Distribution Server using the factory-loaded 2048-bit RSA certificate which is issued by the Fortinet CA. This certificate cannot be modified by any TOE administrator. Alternatively, the AV and IDS/IPS signature updates can be downloaded manually by the TOE administrator or on a schedule (hourly/daily/weekly). A trusted channel is also used for these manual/schedules updates.

AV and IDS/IPS signature updates consist of updates to both the signatures data files and the AV and IDS/IPS processing engines. The TOE provides specific guidance to administrators which notes that in the evaluated configuration of the TOE, only updates to the signatures data files may be applied.

The TOE must be explicitly configured to send logging information to the FortiAnalyzer Server. The IP address of the FortiAnalyzer must be specified, and this address is used by the TOE to send logging information to the FortiAnalyzer. When the TOE sends logging information it will, if so configured, initiate a trusted channel connection to the FortiAnalyzer Server using IPSec.

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 are destroyed by overwriting the key storage area with an alternating pattern at least once.

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. The TOE 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 an administrator-specified interval not less than once a day, to demonstrate the correct operation of the cryptographic components of the TSF. The TOE will enter into a FIPS Error Mode when failure of a self test (integrity verification self-test, or cryptographic self-test) is detected. This mode allows the TOE to enter into a secure state. These self-tests are executed on initial start-up or at the request of an administrator.

The TOE provides a USB interface which may be used by an authorized administrator to load private keys for the DSA asymmetric algorithm from a USB token.

The 2048-bit RSA certificate used by the Network Web-Based GUI can be replaced by certificates trusted by an authorized administrator. These keys/certificates are to be placed on the USB token and the load operation can be executed via a Network CLI or Network Web-Based GUI administrator session.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITC.1, and FTP_TRP.1

7.1.4 User Data Protection

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

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

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

c. The VPN SFP allows authenticated users to send and receive information protected by trusted paths and channels to and from the TOE; and

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

The security functional policies are implemented as firewall rules. The rules that implement the 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 an authorized administrator, and an authorized administrator may also

specify alternative initial values to override the default values. The TOE allows an authorized administrator to view all information flows allowed by the information flow policy rules before the rules are applied.

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

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

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

The 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 also ensures that TSF data may not be replayed.

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

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

- Scheduling
- SMTP commands
- SMTP MIME types
- FTP subcommands
- HTTP request methods
- Virus signatures
- IPS signature matching

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

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

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

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

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

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

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

7.1.5 Security Management

Appropriately authorized administrators may read audit log data, acknowledge alarms and manage cryptographic functionality, including the execution of self-tests, delete audit records and modify the cryptographic security data, and perform all other TOE administration functions. The TOE immediately enforces the revocation of a user from an administrative access profile.

The TOE provides a web-based GUI and a CLI to manage all of the security functions behaviour and security attributes required by the Application level FW PP, the Traffic Filter FW PP, the IDS Sensor PP, as well as the VPN, cryptographic and security audit and alarm functionality detailed in Section 6. 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.

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

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

TOE Security Functional Requirements addressed: FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.1(5), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.2, FMT_SMF.1 and FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE maintains an isolated security domain for its own execution. FortiOS is the only application running on the TOE hardware, and no other applications may be loaded onto the TOE. Administrators and users do not have access to the operating system or the file system (i.e. 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. Before establishing a user session that requires authentication or before establishing an administrative session, the TOE displays an administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE. Additionally, the TOE protects itself by rejecting replay of communications, avoiding overload of its interfaces, and managing sessions. The TOE terminates Authenticated User, administrative sessions, and VPN sessions after an administrator-configurable time interval of inactivity.

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 Sensor data is made available to remote trusted IT products within one minute of receipt of request for the data, provided the data is available for transmission. The TOE uses encryption to

ensure that data transmitted from the TSF to a remote trusted IT product is protected from unauthorized disclosure during transmission. The TOE detects modification of TSF data transmitted between the TSF and a remote trusted IT product. The TOE will retransmit the data if the remote trusted IT product detects modifications and requests a re-transmission.

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

Time is provided by the TSF and can only be changed by an authorized administrator. Changes to the time are audited. 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 an authorized administrator and all such modifications are recorded in the audit log. The integrity of the hardware clock is verified during the TOE self-tests.

TOE Security Functional Requirements addressed: FDP_RIP.2, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_STM.1.

7.1.7 Intrusion Detection/Intrusion Prevention

The TOE provides an Intrusion Detection/Intrusion Prevention System that examines network traffic arriving on its interfaces for evidence of intrusion attempts. If such evidence is found, the TOE records the event in a sensor log. The sensor log is made available only to authorized administrators, and is provided in a manner suitable for the administrators to interpret the information.

The TOE protects the stored sensor data from modification and from unauthorized deletion. The TOE allows an authorized administrator to specify the action to be taken if the storage allocated for sensor data is full, either stop generating sensor data, or overwrite the oldest sensor data. An alarm is sent if the storage capacity has been reached.

TOE Security Functional Requirements addressed: IDS_COL_EXT.1, IDS_RDR_EXT.1, IDS_STG_EXT.1, and IDS_STG_EXT.2.

7.1.8 Anti Virus Actions

The TOE detects and prevents virus attacks contained within information flows which arrive at any of its network interfaces. An authorized administrator may configure the TOE to block and or quarantine a virus which is detected in an information flow. The TOE provides a secure mechanism via a trusted channel for the update of virus signatures used by the TSF.

TOE Security Functional Requirements addressed: FAV_ACT_EXT.1,

TERMINOLOGY AND ACRONYMS

7.2 TERMINOLOGY

The following terminology is used in this ST:

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

7.3 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASIC	Application-specific Integrated Circuit

Acronym	Definition
AV	Anti-Virus
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMP	Certificate Management Protocol
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name Service
DOS	Denial of Service
EAL	Evaluation Assurance Level
FGCP	FortiGate Clustering Protocol
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
FW	Firewall
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security

Acronym	Definition
IPv4, IPv6	Internet Protocol version 4, Internet Protocol version 6
IT	Information Technology
LCD	Liquid Crystal Display
n/a	Not Applicable
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PKCS	Public-Key Cryptography Standards
POP3	Post-Office Protocol Version 3
PP	Protection Profile
rDSA	RSA Digital Signature Algorithm
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
SFP	Security Functional Policy
SFP	Small form factor pluggable (in hardware table)
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Secure Network Mail Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TFTP	Trivial File Transfer Protocol

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network