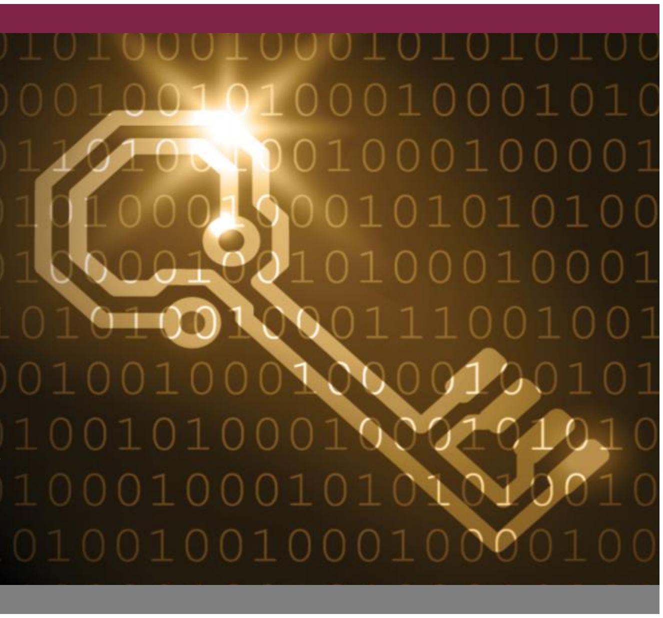
Sophos Ltd.

Sophos Firewall OS

v19.0.2

Security Target



Evaluation Assurance Level (EAL): EAL4+
Document Version: 0.9

Prepared for:

Sophos Ltd.
The Pentagon
Abingdon Science Park
Abingdon OX14 3YP
United Kingdom

Phone: +1 866 866 2802
www.sophos.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

1. Introduction 4
1.1 Purpose 4
1.2 Security Target and TOE References 5
1.3 TOE Overview 5
1.3.1 TOE Environment 7
1.4 TOE Description 8
1.4.1 Physical Scope 8
1.4.2 Logical Scope 10
1.4.3 Product Physical/Logical Features and Functionality not included in the TOE 11
2. Conformance Claims 12
3. Security Problem 13
3.1 Threats to Security 13
3.2 Organizational Security Policies 14
3.3 Assumptions 14
4. Security Objectives 15
4.1 Security Objectives for the TOE 15
4.2 Security Objectives for the Operational Environment 15
4.2.1 IT Security Objectives 15
4.2.2 Non-IT Security Objectives 16
5. Extended Components 17
5.1 Extended TOE Security Functional Components 17
5.2 Extended TOE Security Assurance Components 17
6. Security Requirements 18
6.1 Conventions 18
6.2 Security Functional Requirements 18
6.2.1 Class FAU: Security Audit 19
6.2.2 Class FDP: User Data Protection 22
6.2.3 Class FIA: Identification and Authentication 23
6.2.4 Class FMT: Security Management 24
6.2.5 Class FTA: TOE Access 25
6.3 Security Assurance Requirements 25
7. TOE Summary Specification 27
7.1 TOE Security Functionality 27
7.1.1 Security Audit 27
7.1.2 User Data Protection 28
7.1.3 Identification and Authentication 28
7.1.4 Security Management 29
7.1.5 TOE Access 29
8. Rationale 30
8.1 Conformance Claims Rationale 30
8.2 Security Objectives Rationale 30
8.2.1 Security Objectives Rationale Relating to Threats 30
8.2.2 Security Objectives Rationale Relating to Policies 32
8.2.3 Security Objectives Rationale Relating to Assumptions 32
8.3 Rationale for Extended Security Functional Requirements 32

8.4 Rationale for Extended TOE Security Assurance Requirements 32
8.5 Security Requirements Rationale 33
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 33
8.5.2 Security Assurance Requirements Rationale 35
8.5.3 Dependency Rationale 35
9. Acronyms 37
10. Appendix A 38
10.1 Sophos XGS Firewall Hardware Models 38
10.2 Sophos Firewall Virtual Appliance Supported Platforms 39

List of Figures

Figure 1 – Hardware Configuration TOE Boundary 9
Figure 2 – Virtual Configuration TOE Boundary 9

List of Tables

Table 1 – ST and TOE References 5
Table 2 – TOE Minimum Requirements 7
Table 3 – Guidance Documentation 10
Table 4 – CC and PP Conformance 12
Table 5 – Threats 13
Table 6 – Assumptions 14
Table 7 – Security Objectives for the TOE 15
Table 8 – IT Security Objectives 15
Table 9 – TOE Security Functional Requirements 18
Table 10 – Auditable Events 19
Table 11 – Firewall Audit Record Contents 19
Table 12 – Admin Audit Record Contents 21
Table 13 – Security Functions 24
Table 14 – Assurance Requirements 25
Table 15 – Mapping of TOE Security Functionality to Security Functional Requirements 27
Table 16 – Threats: Objectives Mapping 30
Table 17 – Assumptions: Objectives Mapping 32
Table 18 – Objectives: SFRs Mapping 33
Table 19 – Functional Requirements Dependencies 35
Table 20 – Acronyms 37
Table 21 – Sophos XGS Firewall Hardware Models 38
Table 22 – Sophos Firewall VM Supported Platforms 39

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Sophos Ltd. (Sophos) Sophos Firewall OS[1] v19.0.2 and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only network firewall that runs on the Sophos XGS series hardware appliances or in a Sophos virtual appliance. The TOE offers traffic management capabilities and identity-based comprehensive security to organizations against multiple security services, applications, and over secure protocols.

1.1 Purpose

This ST is divided into ten sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.
- Appendix A (Section 10) – Identifies the supported TOE hardware models and virtual machine hypervisors.

[1] OS – Operating System

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Sophos Ltd. Sophos Firewall OS v19.0.2 Security Target*
ST Version	Version 0.9
ST Author	Corsec Security, Inc.
ST Publication Date	2023-11-16
TOE Reference	Sophos Firewall OS v19.0.2-MR-2-Build472

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. This section provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is a software-only network firewall that runs on the Sophos XGS series hardware and virtual appliances. The TOE is installed on a network whenever firewall services are required.

This allows the TOE to be used as a firewall as well as a gateway for routing traffic. To control Internet access entirely through the TOE, the entire Internet bound traffic from the Local Area Network (LAN) must first pass through the TOE. The TOE is software-only with the Sophos hardware or virtual appliance as part of the TOE environment.

The firewall rules functionality protects the network from unauthorized access and typically guards the LAN and Demilitarized Zone (DMZ) networks against malicious access. Firewall rules may also be configured to limit the access to harmful sites for LAN users.

Firewall rules provide centralized management of security policies. From a single firewall rule, you can define and manage an entire set of TOE security policies. Firewall rules control traffic passing through the TOE. Depending on the instruction in the rule, the TOE decides on how to process the access request. When the TOE receives the request, it checks for the source address, destination address, TCP[2] or UDP[3] protocol, and port number and tries to match it with the firewall rule. It also keeps track of the state of connection and denies any traffic that is not part of the connection state.

The packet filter that is part of the Sophos Firewall OS relies on information available at OSI[4] layer 3 and layer 4 for policy enforcement. The Sophos Firewall OS supports IP[5]v4 and IPv6. In scope of the TOE are the IPv4 security functionalities not the IPv6.

The TOE provides extensive logging capabilities for traffic, system, and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security

[2] TCP – Transmission Control Protocol
[3] UDP – User Datagram Protocol
[4] OSI – Open System Interconnect
[5] IP – Internet Protocol

issues and reduce network abuse. These logs can be viewed through the Web Admin Console. The TOE relies on its environment for reliable timestamps.

The TOE also provides the following management functionalities:

- Managing firewall rules including the associated security attributes for the Traffic Information Flow Control Security Functional Policy (SFP)
- Configure user authentication protection
- User management
- Search or filter the Log Viewer

The TOE's major security features are:

- Web Admin Console
    - The Web Admin Console is a web-based graphical interface used to configure and manage the TOE's security functionality.
    - The Web Admin Console can also be configured to display a custom advisory warning when accessing the login page.
- Audit Logging
    - The TOE is capable of generating audit logs for security-related activity, providing methods of reviewing the audit logs, controlling access to the audit logs, and protecting the stored audit logs.
- Local Authentication
    - The TOE provides TOE users with authentication that can be performed using the locally saved account information in the PostgreSQL database on the TOE.
    - The TOE also provides configurable options on how to handle failed authentication.
- Firewall
    - The TOE's stateful and deep packet inspection firewall allows identity-based policy creation for its multiple security features through a single interface, giving ease of management and high security with flexibility. The TOE protects organizations from DoS[6] and IP/MAC[7] spoofing attacks.
    - Packet Filtering
        - The TOE enforces the Traffic Information Flow Control SFP. This SFP ensures that the TOE will only forward data from and to the destination network if the SFP allows it.
        - The TOE collects audit data into a memory buffer to facilitate identification of policy violations.
        - The TOE is capable of performing management functions such as modification of network filter traffic rules and configuration data.

[6] DoS – Denial of Service

[7] MAC – Media Access Control

1.3.1 TOE Environment

The TOE has the following minimal requirements concerning the physical machine in the second column and the virtual machine they run on in the third column.

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – TOE Minimum Requirements

Category	Hardware Requirement	Virtual Requirement
Platform	Sophos XGS appliance (see models listed in Appendix A)	General purpose computer (GPC) with the following minimum specifications: • Processor – 1 GHz[8] • Memory – 2 GB[9] • Number of Network Interfaces – Minimum 3 • Hard drives – 2 ○ 1st drive – 4 GB ○ 2nd drive – 80 GB • Compatible hypervisor (See platforms listed in Appendix A)
Workstation	General purpose computer with the functionality to connect to the Web Admin Console using the following browsers (with JavaScript enabled): • Mozilla Firefox v101 or higher (recommended) • Google Chrome v102 or higher • Apple Safari v15 or higher • Microsoft Edge v102 or higher • Opera v93 or higher Recommended minimum screen resolution for utilizing the Web Admin Console is 1024 x 768 and 32-bit true color.	
Environmental Component	External syslog server Uninterruptable power supply (UPS)	

The TOE software is capable of running on all Sophos XGS hardware appliances listed in Appendix A with the same functionality available to all models. The different models in the series provide for increased performance and additional connectivity and port availability. Models with a "w" variant, such as the XGS 87w variant of the XGS 87, offer built-in Wi-Fi connectivity.

The TOE may also be deployed as a virtual machine on any of the supported hypervisor platforms listed in Appendix A, with the same functionality available to all platforms.

The TOE supports the same functionality in both hardware and virtual appliance applications.

In addition, the TOE needs cables and connectors that allow all of the TOE and environmental components to communicate with each other.

All of the above resources are outside the boundary of the TOE and therefore a part of the TOE environment.

[8] GHz – Gigahertz

[9] GB – Gigabyte

1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

The TOE is configured for HTTPS[10] web-based administration from a workstation through the Web Admin Console. To connect to the Web Admin Console, the TOE user can access it using the system's IP address and port 4444. Once the login page is displayed, the TOE user can input a username and password to authentication with the TOE. The Web Admin Console supports multiple languages, which the default is English. The Web Admin Console provides the following management functionalities for the TOE users:

- Managing firewall rules including the associated security attributes
- Configure user authentication protection
- User management
- Search or filter the Log Viewer

The firewall rules' functionality protects the network from unauthorized access and typically guards the LAN and DMZ networks against malicious access. Firewall rules may also be configured to limit the access to harmful sites for LAN users.

The responsibility of the firewall is to grant access from Internet to DMZ or Service Network according to the rules and policies configured. It also keeps track of the state of connection and denies any traffic that is not part of the connection state.

Firewall rules provide centralized management of security policies. From a single firewall rule, TOE users can define and manage an entire set of TOE security policies.

Firewall rules control traffic passing through the TOE. Depending on the instruction in the rule, the TOE decides on how to process the access request. When the TOE receives the request, it checks for the source address, destination address, TCP or UDP protocol, and port number and tries to match it with the firewall rule.

The TOE provides extensive logging capabilities for firewall and administration functions. Detailed log information and reports are available over HTTPS through the Web Admin Console. An external syslog server is used in the TOE environment to provide historical analysis of network activity to help identify security issues and reduce network abuse.

For further information about the TOE security functionality, please refer to section 1.4.2.

1.4.1 Physical Scope

Figure 1 and Figure 2 illustrate the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a firewall application which runs on the Sophos XGS series hardware (see models listed in Appendix A) and virtual appliances (See platforms listed in Appendix A) compliant to the minimum requirements as listed in Table 2. The TOE is installed on a network whenever firewall services are required as depicted in Figure 1 and Figure 2. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

[10] HTTPS – Hypertext Transport Protocol Secure

- A workstation
- A syslog server
- The hardware for the TOE
- The network components for the separate networks

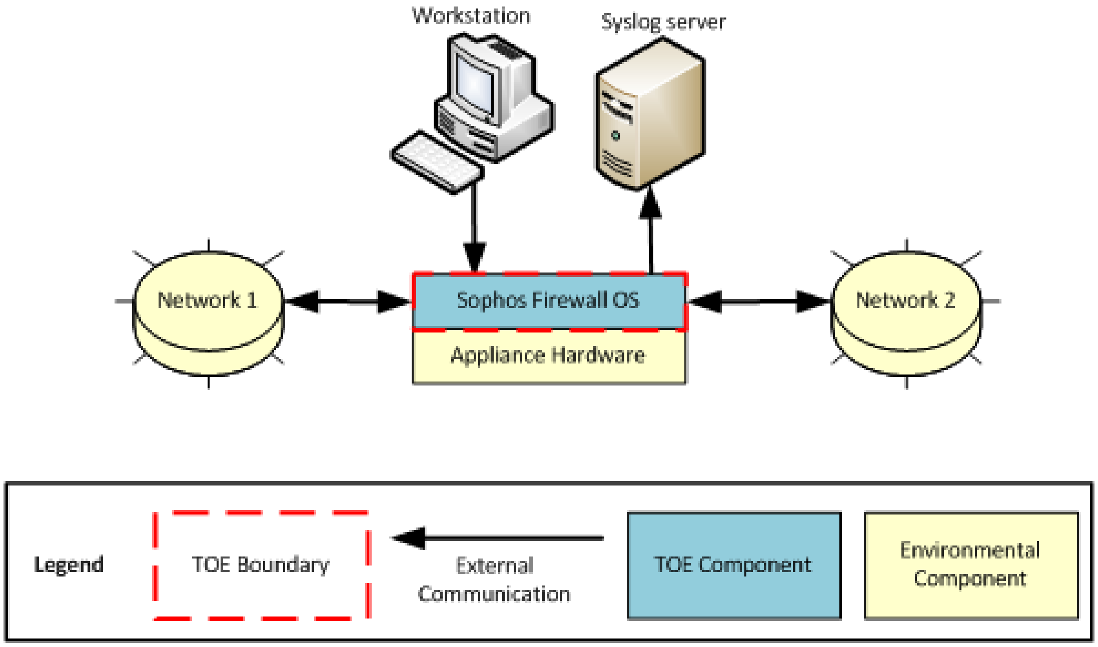


Figure 1 – Hardware Configuration TOE Boundary

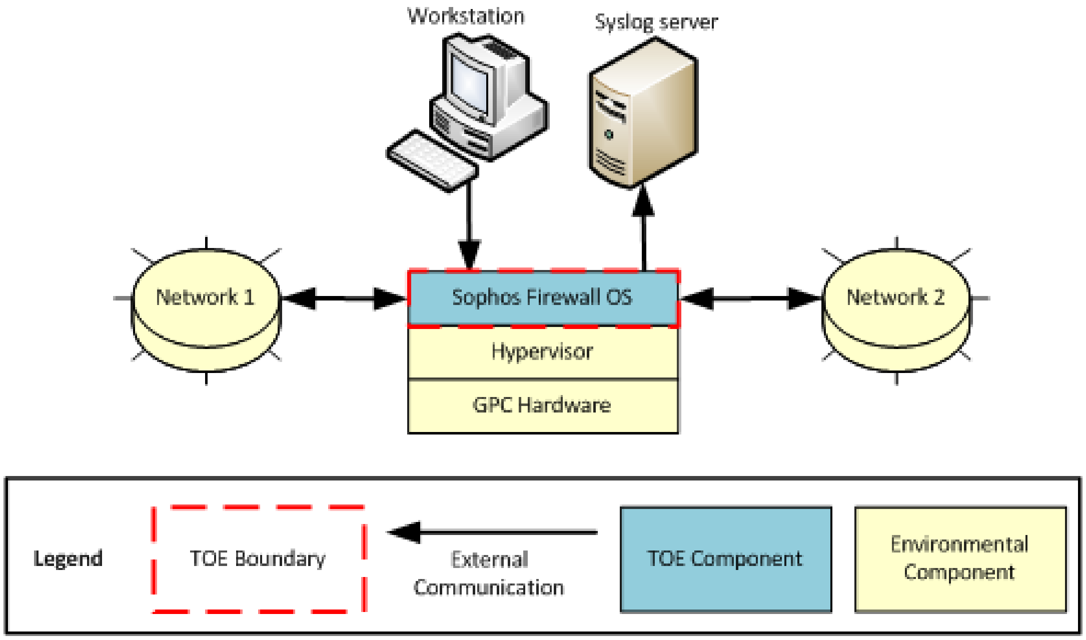


Figure 2 – Virtual Configuration TOE Boundary

1.4.1.1 TOE Software

The TOE is a software-only TOE and is comprised of Sophos Firewall OS v19.0.2. The installers for deploying on hardware appliances are packaged in the *.iso file format while installers for virtual deployments are packaged in the *.zip format. The TOE installer for XGS hardware is HW-19.0.2_MR-2-472.iso and the TOE installer for VMware is VI-19.0.2_MR-2.VMW-472.zip. TOE users can download the hardware or virtual installers from the Downloads tab of the Sophos Support page located at https://www.sophos.com/en-us/support/downloads/firewall-installers.

1.4.1.2 Guidance Documentation

Table 3 lists the PDF[11] formatted guides that are required reading and part of the TOE.

Table 3 – Guidance Documentation

Document Name	Description
Sophos Firewall 19.0 Help	Contains information regarding the setup, installation, and maintenance of the TOE. Generated on June 15, 2022.
Sophos Ltd. Sophos Firewall OS v19.0.2 Guidance Documentation Supplement Evaluation Assurance Level (EAL): EAL4+ Document Version: v0.5	Contains information regarding specific configuration for the TOE evaluated configuration.

1.4.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

1.4.2.1 Security Audit

The TOE generates audit records for the startup and shutdown of the audit functions along with audit records for firewall functionality and administration activity. An Administrator or Audit Admin can view, search, and filter the audit records based on different factors that vary between Admin and Firewall log files. The TOE protects audit records in the audit trail from unauthorized deletion and modification by limited which profiles have access to the audit records and by uploading logs to the external syslog server for redundancy. All historical audit records are maintained and stored in the external syslog server.

1.4.2.2 User Data Protection

The TOE controls data sent through the TOE from one external entity to another via the Traffic Information Flow Control SFP. The Traffic Information Flow SFP relies on source and destination IP addresses, TCP or UDP protocol, port numbers, and rules defined in the Traffic Information Flow Control List to determine how to treat the network traffic. The rules determine whether traffic should be accepted through the TOE to its destination, or if the traffic should be dropped/rejected.

[11] PDF – Portable Document Format

1.4.2.3 Identification and Authentication

TOE users are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. The TOE limits unsuccessful login attempts from an IP address to prevents unauthorized entities from gaining access to the TOE. This feature is configurable and allows a settable number of unsuccessful logins and settable lockout timer.

1.4.2.4 Security Management

The TOE offers a Web Admin Console that TOE users can use to configure and manage specific TOE settings, manage the firewall runs and the Traffic Information Flow Control SFP, configure authentication protection, manage users, and use the Log Viewer. The TOE supports different profiles: Administrator, Audit Admin, and Security Admin. The Administrator and Security Admin profiles have the ability to modify and delete the restrictive default security attributes for the Traffic Information Flow Control SFP. The Audit Admin profile has the ability to monitor the logs and modify reports of the TOE.

1.4.2.5 TOE Access

A TOE user can terminate their own interactive session. An Administrator or Security Admin can configure the TOE to display a warning message regarding unauthorized use of the TOE before an authentication session occurs.

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and/or Functionality that are not part of the evaluated configuration of the TOE are:

- Use of the Command Line Interface (CLI)
- Use of the User Portal
- Use of the HAProfile and Crypto Admin profiles
- Creation of new Administrator-type profiles
- Use of the SNMP[12] functionality
- Use of the external authentication functionality
- Use of the VPN[13] functionality
- Use of the intrusion prevention system functionality
- Use of the gateway antivirus/antispyware functionality
- Use of the gateway antispam functionality
- Use of the outbound spam protection functionality
- Use of the web filtering functionality
- Upgrading from previous TOE firmware versions

[12] SNMP – Simple Network Management Protocol

[13] VPN – Virtual Private Network

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 conformant; CC Part 3 conformant.
PP Identification	None
Evaluation Assurance Level	EAL4 augmented with Flaw Remediation (ALC_FLR.3).

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[14] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess an enhanced basic skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[15] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.AUDACC	A TOE user or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.
T.FILTER	An attacker might attempt to bypass network policies in order to gain unauthorized access to resources in a destination network.
T.MEDIATE	An attacker may send impermissible information through the TOE which results in the exploitation of resources on the destination network.
T.NOAUTH	An attacker 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.REPEAT	An attacker may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.
T.WEAKNESS	An attacker might gain access to the TOE in order to read, modify or destroy TSF data by sending IP packets to the TOE and exploiting a weakness of the protocol used. This attack may happen from outside and inside the protected network. A TOE user might also try to access sensitive data of the TOE via its management interface.

[14] IT – Information Technology

[15] TSF – TOE Security Functionality

3.2 Organizational Security Policies

There are no Organizational Security Policies (OSPs) defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.AUDIT	It is assumed that the IT environment will provide a syslog server and a means to present a readable view of the audit data.
A.GENPUR	It is assumed that the TOE will only store and execute security-relevant applications and only store data required for its secure operation.
A.NETCON	It is assumed that the TOE environment will provide the network connectivity required to allow the TOE to perform its intended function.
A.NOEVIL	It is assumed that the TOE users are non-hostile, well trained, and follow all documentation related to the TOE.
A.PHYSEC	It is assumed that the TOE is physically secure in a controlled environment and only TOE users gain physical access to the TOE.
A.SINGEN	It is assumed that information will not flow between the two networks unless it passes through the TOE.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, and allow TOE users to terminate their own sessions after logging in.
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 for TOE users to search and filter the audit trail based on relevant criteria. The records must be protected from unauthorized deletion.
O.AUTHENTICATE	The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administration access to TOE functions and data. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.
O.FILTER	The TOE must filter the incoming and outgoing data traffic of all data between all connected networks according to the rule sets.
O.MANAGEMENT	The TOE must provide management functions in order to modify the configuration data and the traffic filter rules. For any command received via the configuration interface, authentication of the TOE user must be required. Other users must be rejected.
O.MEDIATE	The TOE must mediate the flow of all information between the two networks governed by the TOE, disallowing passage of non-conformant protocols.
O.SECFUN	The TOE must provide functionality that enables TOE users to use the TOE security functions and must ensure that only TOE users are able to access such functionality.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 – IT Security Objectives

Name	Description
OE.AUDIT	The IT environment will provide a syslog server for the TOE to upload audit records and provide a means to present the records in a human-readable view.
OE.GENPUR	The TOE will only be used to store and execute security-relevant applications and to only store data required for its secure operation.

Name	Description
OE.NETCON	The TOE environment will be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.NOEVIL	The TOE users will be non-hostile, well trained, and follow all TOE documentation.
OE.PHYSEC	The TOE's physical environment will be access controlled and limited to only TOE users.
OE.SINGEN	All information that flows between the two networks will pass through the TOE.

4.2.2 Non-IT Security Objectives

There are no Non-IT Security Objectives defined for this ST.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection, and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FTA_SSL.4	User-initiated termination				
FTA_TAB.1	Default TOE access banners				

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

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

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

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

c. [*The TSF-related auditable events listed in Table 10 below*].

Table 10 – Auditable Events

Log Viewer Selection	Auditable Events
Firewall	Firewall traffic allowed
	Firewall traffic denied
	Invalid traffic denied
	Invalid fragmented traffic denied
Admin	Add operation
	Update operation
	Delete operation
	TOE user login/logout to the Web Admin Console

FAU_GEN.1.2

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

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

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the fields listed in Table 11 for the Firewall log and Table 12 for the Admin log*].

Table 11 – Firewall Audit Record Contents

Field	Description
timestamp	Date/Time (yyyy-mm-dd (hh:mm:ss) when the event occurred
messageid	Message identifier for event
log_type	Type of event occurred in the TOE
log_component	Component responsible for logging
log_subtype	Sub type of event occurred in the TOE
status	Status of log
con_duration	Duration of connection
fw_rule_id	Rule ID[16] used for particular firewall rule
fw_rule_name	Firewall rule name corresponding to fw_rule_id
fw_rule_section	Section in which firewall rule belongs to

[16] ID – Identification

Field	Description
nat_rule_id	Rule ID used for particular NAT[17] rule
nat_rule_name	NAT rule name corresponding to nat_rule_id
policy_type	Firewall template (network / user / business policy)
sdwan_profile_id_request	ID of the SDWAN profile applied on request direction of flow
sdwan_profile_name_request	SDWAN profile name corresponding to sdwan_profile_id_request
sdwan_profile_id_reply	ID of the SDWAN profile applied on reply direction of flow
sdwan_profile_name_reply	SDWAN profile name corresponding to sdwan_profile_id_reply
gw_id_request	ID of the Gateway applied on request direction of flow
gw_name_request	Gateway name corresponding to gw_id_request
gw_id_reply	ID of the Gateway applied on reply direction of flow
gw_name_reply	Gateway name corresponding to gw_id_reply
sdwan_route_id_request	ID of the SDWAN route applied on request direction of flow
sdwan_route_name_request	SDWAN route name corresponding to sdwan_route_id_request
sdwan_route_id_reply	ID of the SDWAN route applied on reply direction of flow
sdwan_route_name_reply	SDWAN route name corresponding to sdwan_route_id_reply
user	Client login username
user_group	User group detail
web_policy_id	ID of the web policy applied
ips_policy_id	ID of the IPS[18] policy applied
appfilter_policy_id	ID of the application filter policy applied
app_name	Application name at client machine
app_risk	Defined risk level (1-5)
app_technology	Technology of application
app_category	Category in which application belong
vlan_id	VLAN ID associated with the flow
ether_type	Ethernet Type associated with the flow
bridge_name	Bridge Interface associated with the flow
bridge_display_name	Display name of the Bridge interface
in_interface	In interface name of traffic of firewall
in_display_interface	Display name of the In interface
out_interface	Out interface name of traffic of firewall
out_display_interface	Display name of the Out interface
src_mac	Client source MAC address
dst_mac	Destination MAC address
src_ip	Client source IP address
src_country	Client source country code
dst_ip	Destination IP address
dst_country	Destination country code

[17] NAT – Network Address Translation

[18] IPS – Intrusion Prevention System

Field	Description
protocol	Port protocol (UDP or TCP)
src_port	Source port number
dst_port	Destination port number
icmp_type	ICMP type
icmp_code	ICMP code
packets_sent	Number of packets sent
packets_received	Number of packets received
bytes_sent	Number of bytes sent
bytes_received	Number of bytes received
src_trans_ip	Translated source IP (NAT source IP)
src_trans_port	Translated source port (NAT source port)
dst_trans_ip	Translated destination IP (NAT source IP)
dst_trans_port	Translated destination port (NAT source port)
src_zone_type	Type of custom zone (LAN or DMZ)
src_zone	The TOE's source zone
dst_zone_type	Type of custom zone (LAN or DMZ)
dst_zone	The TOE's destination zone
con_direction	Direction of connection
con_event	Connection event
con_id	Connection ID
virt_con_id	Master connection ID (in case of related connections)
hb_status	Endpoint Heartbeat status
message	Message about particular packet
appresolvedby	Module via which client application name is resolved
app_is_cloud	Set if application is web/cloud based
log_occurrence	Occurrence count of the audit record
web_policy	Web policy name corresponding to web_policy_id

Table 12 – Admin Audit Record Contents

Field	Description
timestamp	Date/Time (yyyy-mm-dd (hh:mm:ss) when the event occurred
messageid	Message identifier for event (local logs only)
log_type	Type of event occurred in the TOE
log_component	Component responsible for logging
log_subtype	Sub type of event occurred in the TOE
status	Status of log
user	Client login username
src_ip	Client source IP address
additional_information	Additional information about the log
message	Message about particular packet

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 [*Administrator or Audit Admin*] with the capability to read [*all recorded audit data*] 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.

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 [*searches, filtering*] of audit data based on [*general character strings for searching and filtered by the values of fields listed in Table 11 and Table 12*].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

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

6.2.2 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] on [

- *Subjects: External IT entities that send and/or receive information through the TOE to another external IT entity*
- *Information: Data sent (IP Datagrams) from one subject through the TOE to another subject*
- *Operation: Pass or drop/reject the data*].

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] based on the following types of subject and information security attributes: [

- *Subject security attributes: source address of subject, destination address of subject*
- *Information security attributes: transport layer protocol, interface on which the traffic arrives and departs, port*].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*Subjects on a network connected to the TOE can cause* *information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information policy rules:*

All rules are based on the IP Datagrams, including:

- *Source address of subject;*
- *Destination address of subject;*
- *Transport layer protocol*

Rules are kept in an ordered list and applied to the connection once the criteria of a rule matches the connection.].

FDP_IFF.1.3

The TSF shall enforce the [*reassembly of fragmented IP datagrams before inspection*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*ACCEPT rules contained in the authorized TOE user-defined Traffic Information Flow Control List*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*DROP/REJECT rules contained in the authorized TOE user-defined Traffic Information Flow Control List*].

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [an administrator configurable positive integer within [*1 and 5*]] unsuccessful authentication attempts occur related to [*access from the same IP in a configurable 1-120 second timeframe*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block any account from that IP address for a configurable timeframe of 1-60 minutes*].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1

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

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies

FIA_UID.2.1

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

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1

The TSF shall restrict the ability to [disable, enable, modify the behavior of] the functions [*listed in the Functionality column of Table 13 below*] to [*the Profile column of Table 13 below*].

Table 13 – Security Functions

Functionality	Actions	Profile
Managing firewall rules including the associated security attributes	disable, enable, modify the behavior of	Administrator, Security Admin
Configure user authentication protection	disable, enable, modify the behavior of	Administrator, Security Admin
User management	disable, enable, modify the behavior of	Administrator, Security Admin
Search or filter the Log Viewer	modify the behavior of	Administrator, Audit Admin
Device access	modify the behavior of	Administrator

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] to restrict the ability to [create, modify, delete] the security attributes [*source address of subject, destination address of subject, transport layer protocol, interface on which the traffic arrives and departs, port*] to [*Security Admin or Administrator*].

FMT_MSA.3 Static attribute initialization

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 [*Traffic Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Security Admin or Administrator*] to specify alternative initial values to override the default values when an object or information is created.

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: [

- *Managing firewall rules including the associated security attributes*
- *Configure user authentication protection*

- *User management*
- *Search or filter the Log Viewer*
- *Device access*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the ~~roles~~ **profiles** [*Administrator, Audit Admin, and Security Admin*].

FMT_SMR.1.2

The TSF shall be able to associate users with ~~roles~~ **profiles** .

6.2.5 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.3. Table 14 summarizes these requirements.

Table 14 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: 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_LCD.1 Developer Defined Life-Cycle Model

Assurance Requirements	
	ALC_TAT.1 Well-Defined Development Tools
	ALC_FLR.3 Systematic Flaw Remediation
Class ADV: 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
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

7. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the security functionality and their associated SFRs.

Table 15 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The TOE contains functionality for generating, storing, and viewing of audit records. As TOE users manage and configure the TOE, their activities are tracked by recording audit records into the logs. All TSF-related configuration changes are recorded in the Admin log to ensure accountability of the TOE user’s actions. As traffic flows through the TOE, related audit records are also recorded in the Firewall log. The TOE audit records contain the fields listed in Table 11 for the Firewall log and Table 12 for the Admin log.

The generated logs are used by TOE users to identify security risks and monitor network security and activity. These logs are also uploaded to a syslog server for historical review. The Administrator and Audit Admin have the ability to view, search, and filter in all audit events generated and saved to the local audit logs. The Log Viewer can be searched for basic text strings or filtered by the values in different fields. The TSF-related audit events are viewable in the following views in the Log Viewer:

- Firewall – Log records for all of the traffic that passes through the firewall. This includes the dropped traffic that does not follow the protocol standards, invalid fragmented traffic, and traffic whose packets the TOE is not able to relate to any connection.
- Admin – Log records for all TSF-related management activity and the logs for TOE users logging in and out.

The TOE protects the stored audit records from unauthorized deletion and modification by limiting access to only the Administrator and Audit Admin profiles.

If the connection between the TOE and the external syslog server is lost, any audit logs output during that outage are lost.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1.

7.1.2 User Data Protection

The TOE implements functionality that allows it to protecting user data by controlling the flow of information. The user data that the TOE is protecting is the data sent from one network, passing through the TOE, to another network. The Traffic Information Flow Control SFP enforces rules on the external IT entities (subjects) that send traffic through the TOE or receive traffic from the TOE. The rules in the security policy determine whether traffic should be accepted from the sender to the receiver, passage rejected, or dropped. The rules are controlled by security attributes related to the subjects (source IP address and destination IP address) and the information (port number, protocol, and interface).

By default, the TOE denies all packets that are not specifically allowed based on the security attributes. The TOE enables TOE users to add/modify/delete policies inside the TOE. Through the use of policies, TOE users configure a set of firewall rules that tell the TOE to allow, reject, or drop traffic based upon factors such as source and destination of the packet, port number, as well as the transport protocol type.

TOE Security Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1.

7.1.3 Identification and Authentication

The TOE establishes and verifies a claimed TOE user's identity and requires successful identification and authentication before allowing access to any TSF-mediating functionality within the Web Admin Console. When a TOE user enters a username and password at the Web Admin Console, the information is passed to the TOE, where it is verified against the username and password stored in the TOE. If the provided credentials match, the TOE user is assigned the profiles associated with that username. If the provided credentials do not match, the TOE counts the failed authentication attempts for that IP address. If the count meets the configured threshold, the TOE will lock out all user accounts from an IP address for a configurable timeframe of 1-60 minutes.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

The TOE provides several aspects of management related to the TSF. The management functionality is access controlled by the profiles within the TOE. A profile separates the TOE's features into access control categories for which a TOE user can enable none, read only, or read-write access. The default profiles that the TOE maintains are the following:

- Administrator – Super user with full privileges.
- Audit Admin – Read-write privileges for Logs & Reports only.
- Security Admin – Read-write privileges for all features except Device Access Profiles (read-only), Device Access (no privileges), and Logs & Reports (no privileges).

With the above profiles, the TOE allows TOE users to administrate the TOE as outlined in Table 13 above. This includes managing the following:

- Managing firewall rules including the associated security attributes
    - This includes TSF-related functionality about managing the Traffic Information Flow Control SFP, its security attributes, and the accept/drop/reject rules.
    - The TOE sets restrictive default values for the firewall and must be configured by a TOE user with the Security Admin or Administrator to overwrite the default values.
- Configure user authentication protection
    - This includes TSF-related functionality about managing the authentication failure handling, session timeouts, and access banner.
- User management
    - This includes TSF-related functionality about managing the profiles associated to user accounts.
- Search or filter the Log Viewer
    - This includes TSF-related functionality about managing the views in the Log Viewer.
- Device Access
    - This includes TSF-related functionality about managing admin and network service access permissions, as well as defining and managing administrator user profile permissions.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.5 TOE Access

The TOE contains functionality for controlling the establishment of a TOE user's session. The TOE user can directly terminate their own session by using the logout link in the Web Admin Console. If a TOE user's session is terminated, the TOE user must log back in to perform any further functions. The TOE also allows an Administrator or Security Admin to configure an advisory warning message regarding unauthorized use of the TOE before an authentication session occurs.

TOE Security Functional Requirements Satisfied: FTA_SSL.4, FTA_TAB.1.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 below provides a mapping of the objectives to the threats they counter.

Table 16 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDACC A TOE user or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means for TOE users to search and filter the audit trail based on relevant criteria. The records must be protected from unauthorized deletion.	The objective O.AUDREC provides a readable audit trail of security-related events, thereby allowing an Administrator or Audit Admin to discover attacker actions.
T.FILTER An attacker might attempt to bypass network policies in order to gain unauthorized access to resources in a destination network.	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 for TOE users to search and filter the audit trail based on relevant criteria. The records must be protected from unauthorized deletion.	The objective O.AUDREC ensures that unauthorized attempts to bypass traffic policies are recorded.
	O.FILTER The TOE must filter the incoming and outgoing data traffic of all data between all connected networks according to the rule sets.	The objective O.FILTER ensures that data passed through the TOE is always checked and filtered and checked according to policy.
T.MEDIATE An attacker may send impermissible information through the TOE which results in the exploitation of resources on the destination network.	O.MEDIATE The TOE must mediate the flow of all information between the two networks governed by the TOE, disallowing passage of non-conformant protocols.	The objective O.MEDIATE ensures that the TOE mediates the flow of all information between clients and servers located on the two networks governed by the TOE.

Threats	Objectives	Rationale
T.NOAUTH An attacker 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.	O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administration access to TOE functions and data. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.	The objective O.AUTHENTICATE ensures that the TOE uniquely identifies and authenticates the claimed identity of all TOE users before granting access to TOE functions and data, or to a controlled network.
	O.SECFUN The TOE must provide functionality that enables TOE users to use the TOE security functions and must ensure that only TOE users are able to access such functionality.	The objective O.SECFUN ensures that the TOE provides functionality that enables TOE users to use the TOE security functions and ensures that only authenticated TOE users are able to access such functionality.
T.REPEAT An attacker may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.	O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administration access to TOE functions and data. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.	The objective O.AUTHENTICATE ensures that the TOE uniquely identifies and authenticates the claimed identity of all TOE users before granting access to TOE functions and data, or to a controlled network. The objective ensures that the TOE provides functionality enabling TOE users to block a login session after a configurable number of failed login attempts from the same IP.
T.WEAKNESS An attacker might gain access to the TOE in order to read, modify or destroy TSF data by sending IP packets to the TOE and exploiting a weakness of the protocol used. This attack may happen from outside and inside the protected network. A TOE user might also try to access sensitive data of the TOE via its management interface.	O.ACCESS The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, allow TOE users to terminate their own sessions after logging in, and terminate inactive sessions.	The objective O.ACCESS ensures that sessions accessing the TOE will be terminated either by the TOE user or by inactivity before an attacker can gain access to their session.
	OE.AUDIT The IT environment will provide a syslog server for the TOE to upload audit records and provide a means to present the records in a human-readable view.	OE.AUDIT supports the mitigation of this threat by ensuring that a redundant copy of audit logs are stored on a syslog server for review of attacks.
	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 for TOE users to search and filter the audit trail based on relevant criteria. The records must be protected from unauthorized deletion.	The objective O.AUDREC ensures the detection of attempts to compromise the destination network including the network component that includes the TOE.
	O.MANAGEMENT The TOE must provide management functions in order to modify the configuration data and the traffic filter rules. For any command received via the configuration interface, authentication of the TOE user must be required. Other users must be rejected.	The objective O.MANAGEMENT ensures that only TOE users are able to manage the TSF data and counters threats against sensitive data of the TOE via its management interface.

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.AUDIT It is assumed that the IT environment will provide a syslog server and a means to present a readable view of the audit data.	OE.AUDIT The IT environment will provide a syslog server for the TOE to upload audit records and provide a means to present the records in a human-readable view.	OE.AUDIT satisfies this assumption by providing a syslog server in the TOE environment.
A.GENPUR It is assumed that the TOE will only store and execute security-relevant applications and only store data required for its secure operation.	OE.GENPUR The TOE will only be used to store and execute security-relevant applications and to only store data required for its secure operation.	OE.GENPUR satisfies this assumption by ensuring that the TOE is only used to store and execute security-relevant applications and data.
A.NETCON It is assumed that the TOE environment will provide the network connectivity required to allow the TOE to perform its intended function.	OE.NETCON The TOE environment will be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETCON ensures that the TOE is appropriately located within the network to perform its intended function.
A.NOEVIL It is assumed that the TOE users are non-hostile, well trained, and follow all documentation related to the TOE.	OE.NOEVIL The TOE users will be non-hostile, well trained, and follow all TOE documentation.	OE.NOEVIL ensures that the TOE users are non-hostile, well-trained, and follow all guidance related to the TOE.
A.PHYSEC It is assumed that the TOE is physically secure in a controlled environment and only TOE users gain physical access to the TOE.	OE.PHYSEC The TOE's physical environment will be access controlled and limited to only TOE users.	OE.PHYSEC satisfies the assumption that the TOE is physically secured and only physically accessed by TOE users.
A.SINGEN It is assumed that information will not flow between the two networks unless it passes through the TOE.	OE.SINGEN All information that flows between the two networks will pass through the TOE.	OE.SINGEN ensures that information cannot flow between the two networks without first passing through the TOE.

Every assumption is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, and allow TOE users to terminate their own sessions after logging in.	FTA_SSL.4 User-initiated termination	The requirement meets the objective by allowing TOE users to terminate their own session.
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by allowing the Administrator or Security Admin to configure an access banner warning against unauthorized access.
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 for TOE users to search and filter the audit trail based on relevant criteria. The records must be protected from unauthorized deletion.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE records security-related events that include related information from the event.
	FAU_SAR.1 Audit review	The requirement meets this objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets this objective by ensuring that an Administrator or Audit Admin can search and filter the audit data.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administration access to TOE functions and data. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that the TOE enforces a lockout after a configurable number of unsuccessful authentication attempts to mitigate the risk of a brute force attack on a username and password.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that users are identified before access to TOE administrative functions is allowed.
O.FILTER The TOE must filter the incoming and outgoing data traffic of all data between all connected networks according to the rule sets.	FDP_IFC.1 Subset information flow control	The requirement meets the objective by controlling the flow of information through TOE and filtering traffic based on the security attributes.
	FDP_IFF.1 Simple security attributes	The requirement meets the objective by controlling the flow of information through TOE and filtering traffic based on the security attributes.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by enforcing the Traffic Information Flow Control SFP to restrict the ability to create, modify, or delete security attributes to an Administrator or Security Admin.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring the TOE provides restrictive default values for the Traffic Information Flow Control SFP attributes.
O.MANAGEMENT The TOE must provide management functions in order to modify the configuration data and the traffic filter rules. For any command received via the configuration interface, authentication of the TOE user must be required. Other users must be rejected.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by providing security-related functionality to TOE users with the appropriate permissions.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by defining which profiles are allowed to administer the security attributes of the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring the TOE provides restrictive default values for the Traffic Information Flow Control SFP attributes.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE provides management functionality.
	FMT_SMR.1 Security roles	The requirement meets the objective by defining the profiles that are used to manage the TOE.
O.MEDIATE The TOE must mediate the flow of all information between the two networks governed by the TOE, disallowing passage of non-conformant protocols.	FDP_IFC.1 Subset information flow control	The requirement meets the objective by ensuring that access control is applied to all packets before they are passed to the destination network.
	FDP_IFF.1 Simple security attributes	The requirement meets the objective by ensuring that access control is applied to all packets before they are passed to the destination network.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by enforcing the Traffic Information Flow Control SFP to restrict the ability to create, modify, or delete security attributes to an Administrator or Security Admin.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the Traffic Information Flow Control SFP has a permissive default policy that can only be changed by an Administrator or Security Admin.

Objective	Requirements Addressing the Objective	Rationale
O.SECFUN The TOE must provide functionality that enables TOE users to use the TOE security functions and must ensure that only TOE users are able to access such functionality.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by providing security-related functionality to TOE users with the appropriate permissions.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by enforcing the Traffic Information Flow Control SFP to restrict the ability to create, modify, or delete security attributes to an Administrator or Security Admin.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by enforcing the Traffic Information Flow Control SFP to provide restrictive default values for security attributes.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE provides management functionality.
	FMT_SMR.1 Security roles	The requirement meets the objective by defining the profiles that are used to manage the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was chosen because it is best suited to address the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. EAL4+ allows the vendor to evaluate their product at a detailed level while benefitting from the Common Criteria Recognition Agreement, which would recognize the TOE as an EAL2+ evaluation. The chosen assurance level is appropriate for the threats defined in the environment. At EAL4+, penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

The augmentation of ALC_FLR.3 was chosen to give greater assurance of the developer’s on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 19 – Functional Requirements Dependencies

SFR	Dependency	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although it is not included, FPT_STM.1 is provided by the TOE environment.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	

SFR	Dependency	Dependency Met	Rationale
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FTA_SSL.4	No dependencies		
FTA_TAB.1	No dependencies		

9. Acronyms

Table 20 defines the acronyms used throughout this document.

Table 20 – Acronyms

Acronym	Definition
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DMZ	Demilitarized Zone
DoS	Denial of Service
EAL	Evaluation Assurance Level
GB	Gigabyte
GHz	Gigahertz
GPC	General Purpose Computer
HTTPS	Hypertext Transport Protocol Secure
ID	Identification
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
OS	Operating System
OSI	Open System Interconnect
OSP	Organizational Security Policy
PDF	Portable Document Format
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
UPS	Uninterruptible power supply
VPN	Virtual Private Network

10. Appendix A

10.1 Sophos XGS Firewall Hardware Models

Table 21 lists the Sophos XGS Firewall Hardware Models documentation. The documents listed are accessible only for registered users.

Table 21 – Sophos XGS Firewall Hardware Models

Model	Quick Start Guide
XGS 87	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-87-87w-107-107w.pdf **SHA256:** bb336943d44fda553205962a05337c9fdba057d0d566bcb5a5a14186aa4be8e5
XGS 87w	
XGS 107	
XGS 107w	
XGS 116	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-116-116w-126-126w-136-136w.pdf **SHA256:** 5c0517a75ef31e068a5566006451d0ecf4dd71b3da980bea492b68c0a3d23c0b
XGS 116w	
XGS 126	
XGS 126w	
XGS 136	
XGS 136w	
XGS 2100	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-2100-2300-3100-3300.pdf **SHA256:** a34d3f7bad4fd638b3fb6a6e7317d5e78d7f99dc1cdbfb46a11e7d5db9900246
XGS 2300	
XGS 3100	
XGS 3300	
XGS 4300	**URL**: https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-4300-4500.pdf **SHA256**: 05f18dd78b78d0249b7e696c0a0c87a52fefa09cb9d78de640068c3d59e3b83a
XGS 4500	
XGS 5500	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-5500-6500.pdf **SHA256:** 55d434c39c47b02be1dab8f75f3466e34d5e2143236ce93a58b16a6413a5bc15
XGS 6500	
XGS 7500	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-7500-8500.pdf **SHA256:** 0a7523c2b61140baf42e507e51e4b9f0d0acde7221bf2a7c54cda6e5bd27f75f
XGS 8500	

10.2 Sophos Firewall Virtual Appliance Supported Platforms

Table 22 – Sophos Firewall VM Supported Platforms

Platform	Supported Version
VMware	vSphere Client version 6.7.0.30000 vSphere Client version 6.7.0.20000 vSphere Client version 6.7.0.40000 VMware Workstation 12 VMware Workstation 14 VMware Workstation 15
Citrix XenApp	Citrix XEN Center 6.2.0 Citrix XEN Center 7.2 XCP-ng-Center 8.0
KVM	Proxmox Virtual Environment 6.0-4 On Microsoft Server platform 2016
Microsoft Hyper-V	Windows Server 2012 R2 Windows Server 2016

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com