SOPHOS
Security made simple.

Security Target Sophos Firewall OS Version 17.0

Assurance Level EAL4+
Common Criteria v3.1 Revision 5

Document version: 1.00
Document date: 2020-02-04

Contents

List of Tables

List of Figures

1 ST Introduction

1.1 ST Reference and TOE Reference

Title:	Security Target Sophos Firewall OS
Sponsor:	Sophos Ltd.
Editor(s):	Sophos, SRC
Document version:	1.00
Document date:	2020-02-04
CC version:	3.1, Revision 5
Assurance level:	EAL4+ (EAL4 augmented by ALC_FLR.3)
Certification ID:	BSI-DSZ-CC-1016
Keywords:	Firewall OS, network security, information flow control
TOE name:	Sophos Firewall OS
TOE version:	v17.0

1.2 TOE Overview

1.2.1 Usage, Major Security Features and TOE Type

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

The TOE is the Sophos Firewall OS v17.0 that runs on the Sophos XG series hardware and virtual appliances. The TOE is installed on a network whenever firewall services are required, as depicted in Figure 1 and Figure 2 below. The TOE can be deployed in Gateway or Bridge mode in both hardware or virtual configuration. The delivery of the TOE and its parts is outlined in Table 2: Scope of TOE delivery and can be downloaded on a specific portal of the developer.

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) network 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 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 or UDP 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 v17.0 relies on information available at OSI layer 3 and layer 4 for policy enforcement. The Sophos Firewall OS v17.0 supports IPv4 [4] and IPv6 [5]. 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 issues and reduce network abuse. These logs can be viewed through the Web Admin Console.

The TOE also provides the following management functionalities:

- System administration and configuration;
- Firewall rules management;
- Configure user authentication;
- Users management;
- Management of the following Traffic Information Flow Control SFP security attributes:
  - Subject IP address
  - Traffic Source IP address
  - Traffic Destination IP address
  - Traffic TCP or UDP transport protocols
  - Traffic port number

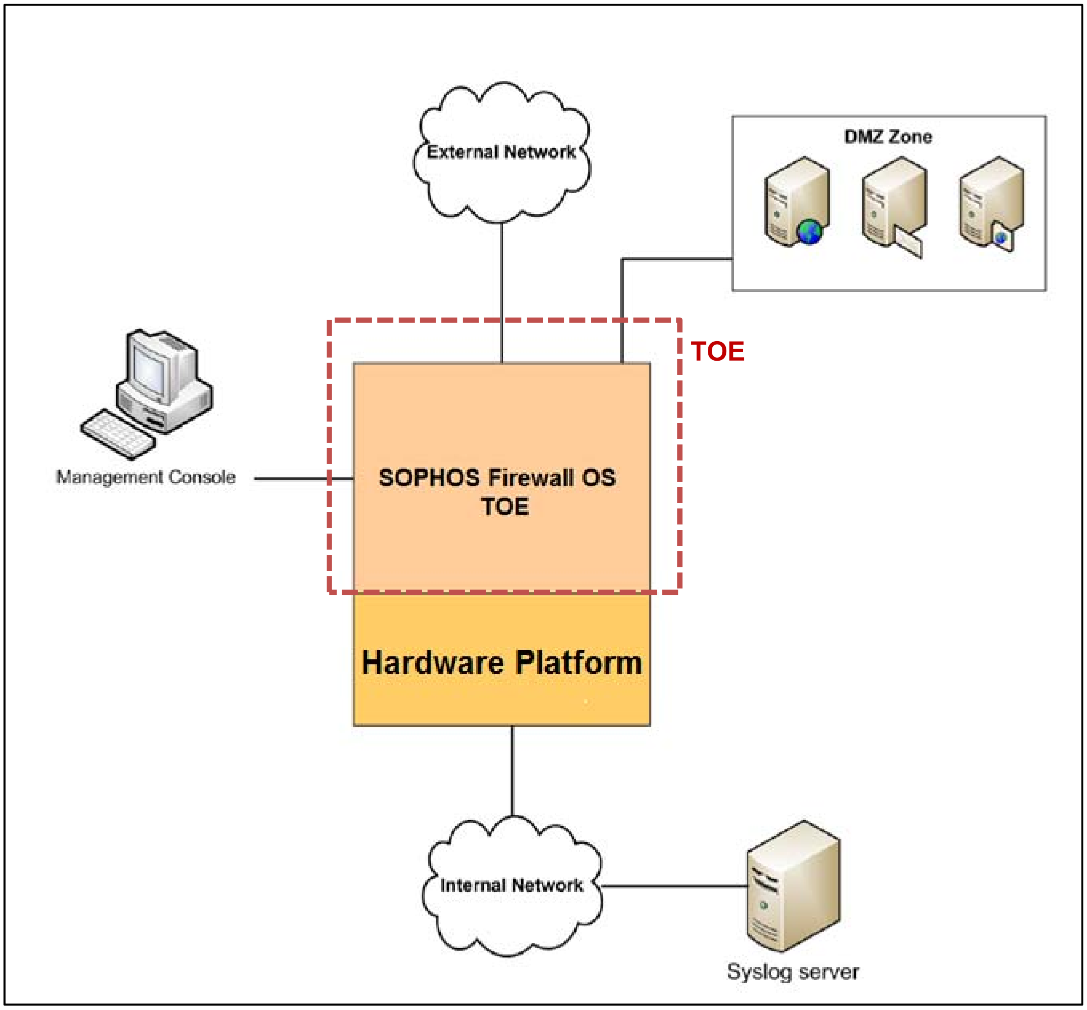

Figure 1: TOE and its Hardware Platform

The TOE major security features are:

- **Web Admin Console**
  - The Web Admin Console is a web-based graphical interfaced used to configure and manage the Sophos appliance.
- **Local Authentication**
  - The TOE provides administrator level authentication that can be performed using the local PostgreSQL database on the TOE.
- **Firewall**
  - 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, and IP/MAC Spoofing attacks.
  - **Packet Filtering**
    - The TOE enforces the Packet Filter information flow policy. This policy ensures that the TOE will only forward data from and to the internal network if the Security Functional Policy 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 networks filter traffic rules and configuration data.

The following are the Product Physical/Logical Features and Functionality that are not included in the TOE and must not be used during runtime of the certified Version of TOE described in the guidance documentation:

- **CLI**
    - The CLI console that provides a collection of tools to manage, monitor, and control certain components of the appliances through a serial connection, mostly for advanced trouble shooting.
- **SNMP**
    - SNMP to allow administrators to monitor the status of the appliances and receive notification of critical events as they occur on the network.
- **External Authentication**
    - Administrator level authentication that can be performed using an external ADS server, LDAP server or RADIUS server.
- **VPN**
    - Secure remote access to organizations with the flexibility to choose from IPSec, L2TP, PPTP, and SSL VPN technologies over its UTM appliances. Identity-based access policies to prevent unauthorized network access over VPN, besides controlling ‘who accesses what’ over VPN is provided with that service.
- **Intrusion Prevention System**
    - Intrusion Prevention System (IPS) that protects against network and application attacks through thousands of automatically updated signatures that enable protection against latest vulnerabilities. It offers security against intrusions, malware, Trojan, DoS and DDoS attacks, malicious code transmission, blended threats and more.
- **Anti-Virus**
    - Gateway Anti-Virus and Anti-Spyware that protects against malware, including viruses, worms, spyware, backdoors, Trojans, and keyloggers over web, email, and Instant Messaging. With a database of millions of signatures updated periodically, it scans malware over incoming/outgoing traffic to reduce the window of vulnerability in organizations.
- **Anti Spam**
    - The Gateway Anti-Spam that offers real-time spam protection over all email protocols - SMTP, POP3, IMAP providing protection against blended threats involving spam, malware, botnets, phishing, and more.
- **Outbound Spam Protection**
    - Outbound Spam Protection that blocks outbound spam in real-time in service provider networks. It enables detection of locally generated outbound spam and spam that is part of a global outbreak, putting an end to IP address blacklisting and loss of corporate reputation, besides identifying the spammer source to eliminate the real source of spam.
- **Web Filtering**
    - Web Filtering that blocks access to harmful, inappropriate, and dangerous websites through its comprehensive uniform resource locator (URL) databases with millions of URLs grouped into 82+ categories.

- **Web Application Firewall**
  - Web Application Firewall on its appliances that secures websites and web applications in organizations against attacks like SQL injection, cross-site scripting, and more, including the Open Web Application Security Project's Top 10 vulnerabilities.
- **Multiple Link Management**
  - Reliable WAN connectivity while supporting WAN redundancy – giving assured access to business applications involved in collaboration, Cloud and software as a service deployments. Automated Load Balancing of multiple ISP links, link failover, and user-identity-based routing delivers higher return on investment and minimizes overload in organizations.
- **IPv6 Ready**
  - IPv6 traffic, which makes Sophos appliances future-ready for the move to IPv6 technology.
- **Wi-Fi Appliances**
  - Identity-based Wi-Fi access that enhances network and data security, and protects remote offices and public hotspots from intrusions, identity theft through MAC, DoS attacks and malware entry. The appliances support 802.11n/b/g wireless standards while combining the features of a router along with offering Sophos's complete set of UTM features.
- **NTP**
  - Synchronizing time with an external NTP server is excluded from the evaluation and not allowed in the evaluated configuration.
- **DoS Protection mode**
  - To preserve the firewall functionality during DoS/DDoS attacks, the firewall reduces logging functionality over the syslog interface and the web admin console log viewer when under heavy load. The threshold of this behavior can be set in the web admin console.

1.2.2 Required Non-TOE Hardware/Software

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

Category	Hardware Requirement	Virtual Requirement
Platform	XG 115	General purpose computer with: • CPU – 1GHz • RAM – 2GB RAM • Number of Network Interfaces – Minimum 3 • HDD – 2 o 1st HDD – 4GB o 2nd HDD – 80GB • Running VMWare ESX.4.1 or later
Management Console	General purpose computer with the functionality to connect to the Web-Admin-Console using	General purpose computer with the functionality to connect to the Web-Admin-Console using

	• Latest version of Firefox (recommended) • latest version of Chrome • latest version of Safari or • Microsoft Internet Explorer 10 onwards • with JavaScript enabled • Recommended minimum screen resolution for utilizing the management console is 1024x768 and 32-bit true color	• Latest version of Firefox (recommended) • latest version of Chrome • latest version of Safari or • Microsoft Internet Explorer 10 onwards • with JavaScript enabled • Recommended minimum screen resolution for utilizing the management console is 1024x768 and 32-bit true color
Environmental Component	External syslog server Uninterruptable power supply (UPS)	External syslog server Uninterruptable power supply (UPS)

Table 1: Hardware platform requirements

For the current evaluation, the hardware appliance XG 115 is in scope of the certification. However, the TOE also runs on all other XG hardware appliances (XG 105, XG 105w, XG 106, XG 106w, XG 115w, XG 125, XG 125w, XG 135, XG 135w, XG 210, XG 230, XG 310, XG 330, XG 430, XG 450, XG 550, XG 650, XG 750) with the same functionality. Running the TOE on these hardware appliances however has not been evaluated.

For the current evaluation, the VMware package is in scope of the certification. However, the TOE also runs on other virtual machines (Xen, HyperV, KVM) with the same functionality. Running the TOE on these virtual machines however has not been evaluated.

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

1.3 TOE Description

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

The TOE can be configured for HTTPS web-based administration from a management console through the Web-Admin Console. To connect to the Web Admin Console, the administrator must input a username and password. The Web Admin Console supports multiple languages, but by default appears in English. The Web Admin Console provides the following management functionalities for an Administrator and Security Admin:

- Add users
- Set time
- Configure syslog server
- Configure firewall rules
- Configure lock-out, logout, and block administrator sessions
- View Logs (Administrator and Audit Admin only)

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, 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 or UDP protocol, and port number and tries to match it with the firewall rule.

The TOE provides extensive logging capabilities for traffic, system, and network protection functions. Detailed log information and reports are available remotely (over https) through the Web Admin Console until a system shutdown for analysis of current network activity. An external syslog server is required 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 1.3.2.

1.3.1 Physical Scope of the TOE

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is Sophos Firewall OS v17.0 which runs on a Sophos XG series hardware or a virtual appliance. The TOE is installed on a network whenever a firewall/UTM services are required as depicted in Figure 2 and Figure 3 below. The essential components for the proper operation of the TOE in the evaluated configuration are:

- Sophos Firewall OS v17.0

The following table shows the delivered Software that is provided to the User

Deliverable	**Description**	**Remarks**
Installer(s)	Installers are used for the fresh installation of SFOS and usually do following, • Detect & Sanitize underlying hardware(s) / hypervisor(s) • Format & Partition Disk(s) • Install the SFOS firmware image	The Installers are not in scope of TOE evaluation

<table>
<tr>
<td></td>
<td><b>Current Installers:</b>
<table>
<tr><th>Installer</th><th>Use</th></tr>
<tr><td>ISO image for Sophos Hardware Appliances</td><td>Used for the fresh installation of SFOS on Sophos provided XG hardware appliances.</td></tr>
<tr><td>VMware Package</td><td>Pre-installed VMware specific package that can be directly imported in VMWare Hypervisor</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

The TOE must be downloaded from the “MySophos” portal to be installed on a hardware or virtual configuration. The file is downloaded to the location specified by the authorized customer. This file includes a firmware with the Sophos Firewall OS v17.0 included. Any configurations specific to the appliance on which it will be installed is done during the first configuration. A SHA-256 hash sum is provided on the portal for each download package to verify the integrity.

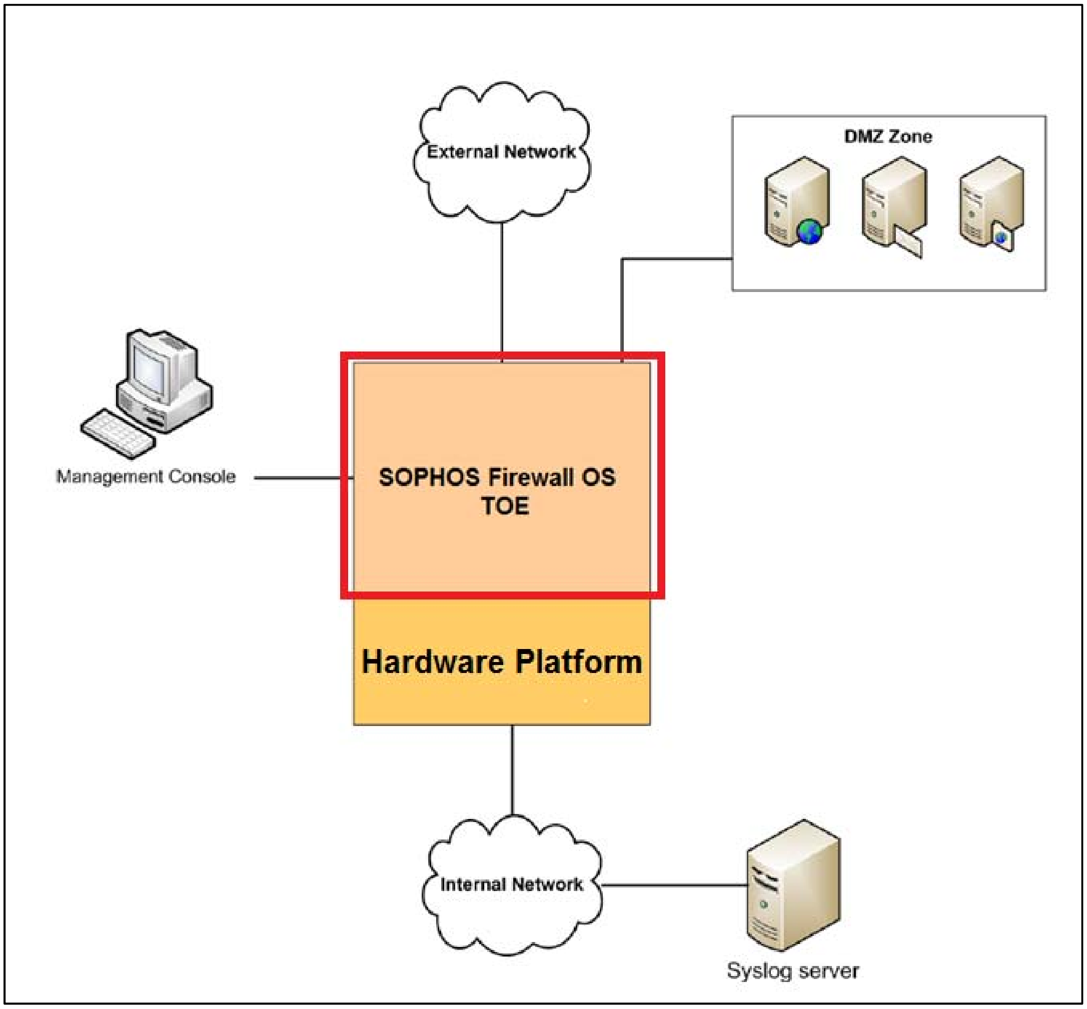

Figure 2: TOE Physical scope and boundary

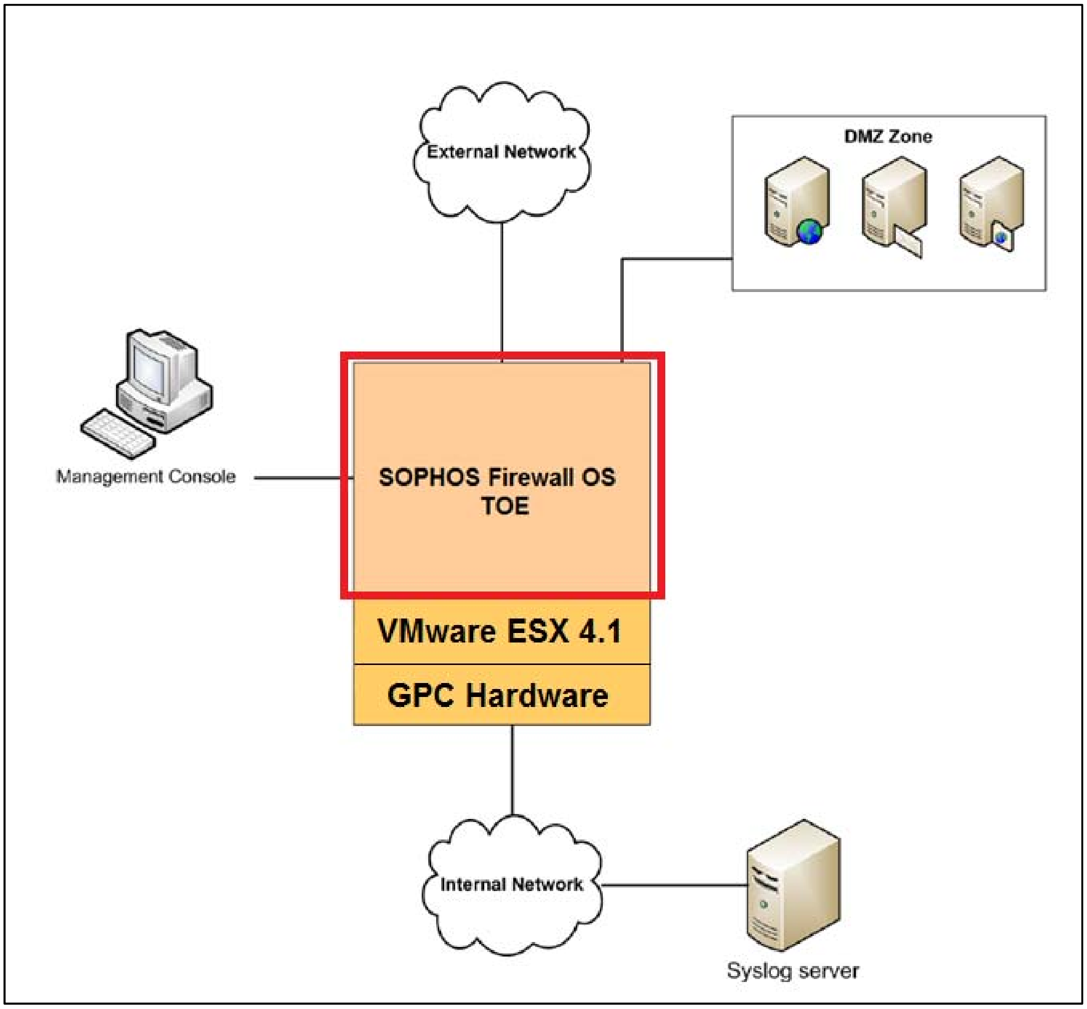

Figure 3: TOE Physical scope and boundary on a virtual platform

To install a downloaded version of the TOE the customer has to check the SHA-256 checksum with the one provided in the guidance documentation.

The TOE delivery includes the Sophos Firewall OS v17.0 and guidance documentation (see Table 2).

Delivered TOE Parts	Version	Remarks	256-Checksum
Sophos Firewall OS	Version 17.0.10	Image to be installed on a virtual machine or on an XG hardware appliance	65875f5d8c1dcda770d613bc9b100273a00b0de02e96e4c062c10ea6ee9fd589

Delivered TOE Parts	Version	Remarks	256-Checksum
	VMware package		7aa46e24063a13d5abe832a860cc61117f63521dc149cbbe696a351ee6db2224
Sophos Firewall OS Sophos XG Firewall Web Interface Reference and Admin Guide v17	June 2019	Delivered as download link on the “MySophos” portal	0863d5e153da76961f45191eeffecaa15d71a6928bb819fd6652665e70d7103c
Guidance Documentation Supplement Sophos Firewall OS Version 17.0	1.00	Delivered as download link on the “MySophos” portal	35fa0b4fec074117d2b3bfcdac2cddf65c58a1fa0f286948c4dc93d60624d7e3

Table 2: Scope of TOE delivery

1.3.2 Logical Scope of the TOE

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 security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Information Flow Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access

1.3.2.1 Security Audit

The TOE generates local audit records further named audit records. In addition, the TOE can be configured to send audit data to a syslog server to be saved as historical audit records. Audit records are generated for the startup and shutdown of the audit functions, rejected and blocked traffic, administrator account activity, firewall rule modification, firewall activity, and login attempts. An Administrator or Audit Admin can view and search in the audit records based on different factors that vary between administrator logs and invalid traffic log files. Audit records are available in the local audit log only until a reboot or system shutdown occurs. The TOE protects audit records in the audit trail from unauthorized deletion and modification. All historical audit records are maintained and stored in the external syslog server.

The packet filter collects audit data also into a memory buffer to facilitate identification of policy violations. This allows the administrator to inspect the received audit data from the packet filter. The TOE generates audit records for

- start-up and shutdown of the audit functions. It must be noted that the shutdown of the audit functions mentioned in FAU_GEN.1.1 is not directly visible as a separate audit record. However, a shutdown of the audit functions of the TOE always correlates with a shutdown of the underlying system supporting the TOE. This means, the shutdown of the underlying system always generates an audit record and the TOE functionality is shut down also. For that reason, the shutdown of the TOE audit functions is indicated by the audit record of the shutdown of the system.
- datagrams received or sent through a network components network interfaces if they match configured patterns
- the functionality is provided for the hardware and virtual configuration

1.3.2.2 Information Flow Protection

The TOE controls network traffic via the Traffic Information Flow Control Security Functional Policy (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 Lists to determine how to treat the network traffic. The rules determine whether traffic should be accepted through the TOE to its destination, passage rejected through the network, or dropped.

The Packet Filter component is the main Package of SFP enforces a Packet Filter information flow policy, whose filtering rules are set during operation. This policy ensures that the TOE will only forward data from and to the internal network if the information flow policy allows it. Therefore, the TOE implements the information flow control (as routers) on the network layer (IP) and transport layer (TCP/UDP/ICMP). In order to apply the packet filter rules the network components take the information from the IP and TCP/UDP/ICMP-Header (where applicable).

1.3.2.3 Identification and Authentication

Administrators are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. Username, password, and role are stored locally in the TOE and are compared against the username and password entered by an entity before assigning a role and allowing access. The TOE provides a way of preventing unauthorized entities from gaining access to the TOE by configuring a settable number of unsuccessful login attempts from an IP address, before the address is locked out by the TOE.

1.3.2.4 Security Management

The TOE offers a Web Admin Console that administrators can use to configure and manage specific TOE settings and the Traffic Information Flow Control SFP. The TOE supports different Administrator roles represented by specific profiles. Administrator, Audit Admin, Crypto-admin, HA-Profile and Security Admin profiles are provided. 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 HA-Profile is an administrator Role for monitoring with no modification abilities (not in the scope) and the crypto Admin is only able to change certification aspects. The Audit Admin has the ability to modify and monitor the logs and reports of the TOE.

The Packet filter that is implemented in the SFP is capable of performing the following management functions:

- Modification of network traffic filter rules
- Modification of configuration data

The Filter is initialized with a strict packet filter rule set, that is, everything is dropped.

1.3.2.5 Protection of the TOE Security Functionality

The TOE environment provides a reliable timestamp for operations in the TOE.

1.3.2.6 TOE Access

An Administrator and Security Admin can configure the TOE to terminate management sessions after one to 99 minutes of inactivity. The default time for termination is 10 minutes. Additionally, an Administrator can terminate the interactive session by himself. An Administrator and Security Admin can configure the TOE to display a warning message regarding unauthorized use of the TOE before an authentication session occurs.

2 Conformance Claim

2.1 CC Conformance Claim

This Security Target and the TOE claim conformance to Part 2 [1] and Part 3 [2] of the Common Criteria for Information Technology Security Evaluation.

2.2 PP and Security Requirement Package Claim

This Security Target does neither claim conformance to a Protection Profile nor to a security requirement package.

2.3 CC Conformance Claim Rationale

As this Security Target does neither claim conformance to a Protection Profile nor to a security requirement package, a conformance claim rationale is not necessary.

2.4 Package Claim

This Security Target claims conformance to the assurance package **EAL4 augmented by ALC_FLR.3**.

ALC_FLR.3 adds systematic flaw remediation procedures to the assurance package EAL4.

3 Security Problem Definition

This chapter introduces the security problem definition of the TOE. This comprises:

- The **assets** which have to be protected by the TOE.
- The **subjects** which are interacting with the TOE.
- The **assumptions** which have to be made about the environment of the TOE.
- The **threats** which exist against the assets of the TOE
- The **organizational security policies** the TOE has to comply to.

3.1 Assets

The following assets need to be protected by the TOE and its environment:

Asset	Description
TSF Data (Information Flow)	Audit data transmitted from the network components to the management console. Configuration data transmitted from the management console to the network components. Audit Data transported to the Syslog Server.
TSF Data (On the TOE)	TSF data stored on the TOE which are necessary for its own operation. This includes packet filter rules and configuration data.
Resources	The resources in the connected networks that the TOE components are supposed to protect. The resources are outside the TOE components.
User Data	Data saved on or transitioning through the TOE and the hosts on the protected network

Table 3: Assets

3.2 Subjects

The different Roles of a user that can be configured for the TOE are administration roles with 5 different profiles that are outlined in the next Table 4.

Name	Role
Default user 'admin'	Super administrator with full privileges.
Administrator with Security Admin Profile	Read-write privileges for all features except

	Profiles and Log & Reports.
Administrator with Administrator Profile	Super administrator with full privileges.
Administrator with Audit Admin Profile	Read-write privileges for Logs & Reports only.
Administrator with Crypto Admin Profile	Read-write privileges for Certificate configuration only.
Administrator with HA Profile	Read-only privileges. This role is assigned to Administrators accessing the Web Admin Console when HA is configured. HA is not configured in the evaluated configuration, so this role will not be assigned.

Table 4: Subjects

3.3 External Entities

There are no external entities that may interact directly with the TOE management. Administrators with specific Profiles are Subjects and mentioned in Chapter 3.2.

3.4 Assumptions

The following assumptions need to be made about the IT environment of the TOE to allow the secure operation of the TOE.

Assumption	Description
A.ENV	The TOE is used in a controlled environment. It is assumed: ■ That only the administrator gains physical access to the TOE, ■ That the administrator handles the authentication secrets with care, specifically that he will keep them secret and can use it in a way that nobody else can read it.
A.NOEVIL	The administrator of the TOE is non hostile, well trained and knows the documentation of the TOE. The administrator is responsible for the secure operation of the host running the TOE.

Assumption	Description
A.INFLOW	The administrator assures that the packet filter components provide the only connection for the different networks.
A.TSP	The IT environment provides reliable timestamps.
A.PROT	The connection between the management console and the network components is protected by cryptographic transforms (e. g. SSH authorization and SSH transport protection as defined in [3]).
A.AUDIT	The IT environment provides a Syslog server and a means to present a readable view of the audit data.
A.REMACC	TOE users may only access the TOE remotely via https connection.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.PHYSEC	The TOE is physically secure.
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended function.

Table 5: Assumptions

3.5 Threats

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 and moderate time to perform an attack.

The following threats have to be countered by the TOE. Hereby attackers with an enhanced-basic attack potential are assumed.

Threat	Description
T.BYPASS	A user might attempt to bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected networks. E. g., a user might send non-permissible data through the TOE in order to gain access to resources in protected networks by sending IP packets to circumvent filters. This attack may happen from outside the protected network.
T.WEAKNESS	A user 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 user might also try to access sensitive data of the TOE via its management interface.
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.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.MEDIAT	An attacker may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.AUDACC	TOE users or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.

Table 6: Threats

3.6 Organizational Security Policies

The TOE does not enforce organizational security policies.

4 Statement of Security Objectives

This chapter describes the security objectives for the TOE (in Chapter 4.1), the security objectives for the operational environment of the TOE (in Chapter 0) and contains the security objectives rationale.

4.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE:

Objective	Description
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 administrator is required. Other users are rejected. Note: the user identification is provided by the environment (application).
O.FILTER	The TOE must filter the incoming and the outgoing data traffic of all data between all connected networks according to the rule sets.
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, sort, and order the audit trail based on relevant attributes.
O.ACCOUNT	The TOE must provide accountability for information flows through the TOE and for TOE users' use of security functions related to audit.
O.AUTHENTICATE	The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials. The operational environment provides mechanisms to support the authentication.
O.LIMEXT	The TOE must provide the means for TOE users to control and limit access to TOE security functions by an authorized external IT entity.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.

Objective	Description
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.

Table 7: Security objectives for the TOE

4.2 Security Objectives for the Operational Environment

The following security objectives have to be met by the operational environment of the TOE:

Objective	Description
OE.ENV	The TOE is used in a controlled environment. The environment ensures: ■ That only the administrator gains physical access to the TOE, ■ That the administrator handles the authentication secrets with care, specifically that he will keep them secret and can use it in a way that nobody else can read it.
OE.NOEVIL	The administrator of the TOE shall be non-hostile, well trained and has to know the documentation of the TOE. The administrator is responsible for the secure operation of the host running the TOE. TOE users are non-hostile and follow all administrator guidance.
OE.INFLOW	The administrator must assure that the packet filter components provide the only connection for the different networks.
OE.TSP	The hardware provides reliable timestamps.
OE.PROT	The connection between the management console and the network components is protected by cryptographic transforms (e. g. SSH authorization and SSH transport protection as defined in [3]).
OE.AUDIT	The IT environment provides a Syslog server and a means to present a readable view of the audit data.

Objective	Description
OE.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
OE.PHYSEC	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.REMACC	TOE users may only access the TOE through a local network remotely via https. The connection between the Web-Admin Console and the Management Console is protected by https with the following configuration: Certificate Encryption: RSA (Default) • Key Size: 2048 bits (Default) • Signing / Hashing: Certificates used are SHA-256 signed (Default)
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

Table 8: Security objectives for the environment of the TOE

4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage. The following chapters provide a more detailed explanation of this mapping.

	OE.ENV	OE.NOEVIL	OE.INFLOW	OE.TSP	OE.PROT	OE.AUDIT	OE.GENPUR	OE.PHYSEC	OE.REMACC	OE.SINGEN	OE.TRAFFIC	O.AUDREC	O.FILTER	O.MANAGEMENT	O.ACCOUNT	O.AUTHENTICATE	O.LIMEXT	O.MEDIATE	O.SECFUN
A.ENV	X																		
A.NOEVIL		X																	
A.INFLOW			X																
A.TSP				X															
A.PROT					X														
A.AUDIT						X													
A.REMACC									X										
A.SINGEN										X									
A.PHYSEC								X											
A.GENPUR							X												
A.NETCON											X								
T.BYPASS	X		X		X							X	X						
T.WEAKNESS						X						X	X	X					
T.REPEAT																X			
T.NOAUTH																X	X		X
T.MEDIAT																		X	
T.AUDACC												X			X				

Table 9: Security Objectives Rationale

4.3.1 Countering the Threats

The threat **T.BYPASS** which describes that an attacker may bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected networks is countered by a combination of the objectives *OE.PROT, OE.ENV, OE.INFLOW, O.AUDRECC,* and *O.FILTER*. The environmental objectives *OE.ENV and OE.INFLOW* ensure that a user can neither interfere with the initial setup or the physical setup of the management console or network components nor routes around the management console or network components. O.AUDREC provides a readable audit trail of security-related events, thereby allowing an Administrator or Audit Admin to discover attacker actions. Thus, all data pass through the TOE. *O.FILTER* ensures that this data is always checked and filtered according to the policy. Since the internal network is trusted (*OE.ENV*), the checked data is not modified after leaving the packet filter. The environmental objective *OE.PROT* ensures that data flow between the management console and the network components is protected by cryptographic transforms, i.e. that sessions always provide proof of identification and illegitimate users cannot be taken over established sessions.

The threat **T.REPEAT** which describes that 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 is countered by the objective *O.AUTHENTICATE* which ensures that the TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The *O.AUTHENTICATE* objective addresses the T.REPEAT threat by requiring the TOE to provide functionality that enables TOE users to block a login session after a configurable number of failed login attempts from the same IP.

The threat **T.WEAKNESS** which describes that an attacker may try to exploit a weakness of the protocol used in order to read, modify or destroy security sensitive data on the TOE is countered by a combination of the objectives *OE:AUDIT, O.AUDREC*, and *O.MANAGEMENT*. *O.AUDREC* ensures detection of attempts to compromise the fenced network including the network component that includes the TOE. *O.MANAGEMENT* ensure that only the administrator is able to manage the TSF data and counters threats against sensitive data of the TOE via its management interface. *O.AUDREC* provides a readable audit trail of security-related events, thereby allowing an Administrator or Audit Admin to discover attacker actions. Other users will be rejected at the configuration interface.

The threat **T.AUDACC** which describes that TOE users or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection is countered by a combination of the objectives *O.ACCOUNT, and O.AUDREC. O.ACCOUNT* ensures accountability for information flows through the TOE and for TOE users' use of security functions related to audit. *O.AUDREC* provides a readable audit trail of security-related events, thereby allowing an Administrator or Audit Admin to discover attacker actions. An Administrator or Audit Admin may use the audit records to identify attacker actions.

The threat **T.MEDIAT** which describes that an attacker may send impermissible information through the TOE which results in the exploitation of resources on the internal network. is countered by *O.MEDIATE*, which ensures that the TOE mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.

The threat **T.NOAUTH** which describes that 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 is countered by a combination of the objectives *O.AUTHENTICATE, O.LIMEXT* and *O.SECFUN. O.AUTHENTICATE* requires that the TOE uniquely identify and authenticate the claimed identity of all TOE users before granting access to TOE functions and data, or to a connected network. *O.LIMEXT* requires the TOE to provide a means for TOE users to control and limit access to TOE security functions by an authorized external IT entity. *O.SECFUN* requires the TOE to provide functionality that enables TOE users to use the TOE security functions, and ensure that only authenticated TOE users are able to access such functionality.

4.3.2 Covering the OSPs

The TOE does not enforce organizational security policies.

4.3.3 Covering the Assumptions

The assumption **A.ENV** is covered by *OE.ENV* as directly follows.

The assumption **A.NOEVIL** is covered by *OE.NOEVIL* as directly follows.

The assumption **A.INFLOW** is covered by *OE.INFLOW* as directly follows.

The assumption **A.TSP** is covered by *OE.TSP* as directly follows.

The assumption **A.PROT** is covered by *OE.PROT* as directly follows.

The assumption **A.AUDIT** is covered by *OE.AUDIT* as directly follows.

The assumption **A.REMACC** is covered by *OE.REMACC* as directly follows.

The assumption **A.SINGEN** is covered by *OE.SINGEN* as directly follows.

The assumption **A.PHYSEC** is covered by *OE.PHYSEC* as directly follows.

The assumption **A.GENPUR** is covered by *OE.GENPUR* as directly follows.

The assumption **A.NETCON** is covered by *OE.TRAFFIC* as directly follows.

5 Statement of Security Requirements

This chapter defines the security functional requirements (see Chapter 5.1) and the security assurance requirements for the TOE (see Chapter 5.3). No extended components are defined in this Security Target (see Chapter 5.1.5).

5.1 Security Functional Requirements for the TOE

The TOE satisfies the SFRs delineated in the following table. The rest of this chapter contains a description of each component and any related dependencies.

Security Audit (FAU)	
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)	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	
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)	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
TOE Access (FTA)	
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
FTA_TAB.1	Default TOE access banners

Table 10: Security Functional Requirements for the TOE

5.1.1 Security Audit

5.1.1.1 FAU_GEN.1 Audit data generation

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

<table>
<tr>
<td></td>
<td>
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [<i>not specified</i>] level of audit; and
c) [<i>Other specifically defined auditable events – see</i> Table 11 <i>below</i>]
<table>
<tr><th>Type of Log</th><th>Auditable Events</th></tr>
<tr><td>Firewall Rules Logs</td><td>Firewall traffic allowed</td></tr>
<tr><td></td><td>Firewall traffic denied</td></tr>
<tr><td>Invalid Traffic Logs</td><td>Invalid traffic denied</td></tr>
<tr><td></td><td>Invalid Fragmented Traffic Denied</td></tr>
<tr><td>Administration Logs</td><td>Add operation</td></tr>
<tr><td></td><td>Update operation</td></tr>
<tr><td></td><td>Delete operation</td></tr>
<tr><td></td><td>Admin login logout</td></tr>
</table>
<b>Table 11: Auditable Events</b>
</td>
</tr>
<tr>
<td><b>FAU_GEN.1.2</b></td>
<td>The TSF shall record within each audit record at least the following information:
a) Date and time of 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, [<i>no other audit relevant information</i>]</td>
</tr>
<tr>
<td>Hierarchical to:</td>
<td>No other components.</td>
</tr>
<tr>
<td>Dependencies:</td>
<td>FPT_STM.1 Reliable time stamps</td>
</tr>
<tr>
<td>Application Note:</td>
<td>An auditable event is any event that occurs, when the TOE is not in DoS protection mode. When the TOE is in DoS protection mode, to preserve the firewall functionality, only the number of dropped packets is logged, but no log events are created for dropped packets. Other events, such as configuration changes are also logged in DoS protection mode (see Section 1.2.1).</td>
</tr>
</table>

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*Administrator or Audit Admin*] with the capability to read [

audit data collected since the last reboot, including the audit shutdown event] 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.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: Audit records are recordable log entries that are stored in the local persistent memory. The Administrator or Audit Admin can also run a syslog server where the audit records are saved as historical audit records.

5.1.1.3 FAU_SAR.3 Selectable Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*searches, filtering*] of audit data based on [*Table 15*].

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

5.1.1.4 FAU_STG.1 Protected audit trail storage

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.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [*Traffic information flow Control*] on [

Subjects: External IT entities that send and/or receive information through the TOE to *one another;*

Information: data sent (IP Datagrams) from one subject through the TOE to one another;

Operation: pass or drop the data].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

Application Note: The Traffic Information flow is given in FDP_IFF. The subject definition in FDP_IFC.1.1 belongs to a former CC version. Thus, the subjects are identical to the users defined in the external entities definition in Chapter 3.3.

5.1.2.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [*Packet Filter SFP*] based on the following types of subject and information security attributes: [

Subjects: External IT entities that send and/or receive information through the TOE to one another;

Subject security attributes: none;

Information: data sent (IP Datagrams) from one subject through the TOE to one another;

Information security attributes: source address of subject, destination address of subject, 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*].

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 administrator-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 administrator-defined Traffic Information*

Flow Control List]

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

Application Note: The subject definition in FDP_IFF.1.1 belongs to a former CC version. Thus, the subjects are identical to the subjects defined in the definition in Chapter 3.2.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [an administrator-configurable positive integer within [*1 and 5*]] of unsuccessful authentication attempts occur related to [*authorized TOE administrator access from the same IP in an administrator-configurable 1-120 seconds*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block any administrator account from that IP address for an administrator-configurable timeframe of 1-60 minutes].*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.3.2 FIA_UAU.2 User authentication before any action

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.

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

5.1.3.3 FIA_UID.2 User identification before any action

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.

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of security functions behavior

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

- *System administration and configuration;*
- *Firewall rules management;*
- *Configure entity authentication; and*
- *Entity management*]

to [*authorized administrators with sufficient permission level*].

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management functions

Application Note: The Entity definitions are identical to the subjects defined in Chapter 3.2 and 3.3.

5.1.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*Packet Filter SFP*] to restrict the ability to [*modify, create and delete*, [*no other operations*]] the security attributes [*Packet Filter rules and configuration data*] to [*the role security administrator and administrator*].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management

5.1.4.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [*Packet Filter 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 [*Administrator and Security Administrator*] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.1.4.4 FMT_SMF.1 Specification of management functions

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

- *System administration and configuration;*
- *Firewall rules management;*
- *Configure user authentication; and*
- *Users management*
- *Management of the following Traffic Information Flow Control security attributes*
- *Subject IP address*
- *Traffic Source IP address*
- *Traffic Destination IP address*
- *Traffic transport protocol type*
- *Traffic port number*].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator with the Profile: Administrator, Audit Admin, HA-Profile, Crypto Admin and Security Admin*].

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 TOE Access (FTA)

5.1.5.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*configurable time interval of administrator inactivity at the Web Admin Console from 1 to 99 minutes, defaulting to 10 minutes*].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.5.2 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.5.3 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an authorized administrator-specified advisory warning message regarding unauthorized use of the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2 Extended Components Definition

No extended components are defined in this Security Target.

5.3 Security Assurance Requirements for the TOE

The following table lists the chosen evaluation assurance components for the TOE:

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, **ALC_FLR.3**, ALC_LCD.1, ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

Assurance Class	Assurance Components
AVA	AVA_VAN.3

Table 12: Chosen Evaluation Assurance Requirements

These assurance components represent EAL4 augmented by the component ALC_FLR.3 (text marked in bold). The complete text for these requirements can be found in [2].

5.4 Security Requirements Rationale

5.4.1 TOE Functional Requirements Rationale

TOE Security Functionality	SFR ID	O.FILTER	O.AUDREC	O.MANAGEMENT	O.ACCOUNT	O.AUTHENTICATE	O.LIMEXT	O.MEDIATE	O.SECFUN
Security Audit	FAU_GEN.1		X		X				
	FAU_SAR.1		X						
	FAU_SAR.3		X						
	FAU_STG.1		X						
User Data Protection	FDP_IFC.1	X						X	
	FDP_IFF.1	X						X	
Identification and Authentication	FIA_AFL.1					X			
	FIA_UAU.2					X			X
	FIA_UID.2			X		X			
Security Management	FMT_MOF.1						X		X
	FMT_MSA.1			X				X	X
	FMT_MSA.3	X						X	X
	FMT_SMF.1			X			X		X
	FMT_SMR.1			X					X

TOE Security Functionality	SFR ID	O.FILTER	O.AUDREC	O.MANAGEMENT	O.ACCOUNT	O.AUTHENTICATE	O.LIMEXT	O.MEDIATE	O.SECFUN
TOE Access	FTA_SSL.3								X
	FTA_SSL.4								X
	FTA_TAB.1								X

Table 13: Coverage of Security Objective for the TOE by SFR

The security objective **O.FILTER** is met by a combination of *FDP_IFC.1*, *FDP_IFF.1* and *FMT_MSA.3*. *FDP_IFC.1* and *FDP_IFF.1* describe the information flow controls and information flow control policy. Together, the SFRs describe how the packet filter information flow policies and the administrator specified rule sets apply. *FMT_MSA.3* defines that the TOE has to provide restrictive default values for the *Packet Filter SFP* (information flow policy) attributes. The SFRs are therefore sufficient to satisfy the objective **O.FILTER**.

The security objective **O.AUDREC** is met by *FAU_GEN.1, FAU_STG.1, FAU_SAR.1, FAU_SAR.3*. *FAU_GEN.1* describes when and what kind of audit data is generated. The SFR ensures that audit log reports report the state of the TOE. *FAU_STG.1* meets this objective by ensuring the TOE restricts the ability to modify or delete the audit trail to an Administrator or Audit Admin and to detect any such behavior by auditing all management operations. *FAU_SAR.3* meets this objective by ensuring that an Administrator or Audit Admin can search, sort, and order the audit data based on time, log comp, action, username, Firewall rule, in interface, out interface, source IP, and destination IP. *FAU_SAR.1* meets this objective by ensuring that an Administrator or Audit Admin are able to read and interpret all audit information from the audit records.

The security objective **O.ACCOUNT** is met by *FAU_GEN.1. FAU_GEN.1* describes when and what kind of audit data is generated and that accountability is ensured by preventing unauthorized modifications to the stored audit records in the audit trail and traceability of the recorded data.

The security objective **O.MANAGEMENT** is met by *FMT_SMF.1, FMT_MSA.1, FIA_UID.2 and FMT_SMR.1*. *FMT_SMF.1* describes the set of management functionality provided by the TOE. FMT_MSA.1 defines, which roles are allowed to administer the security attributes of the TOE. *FIA_UID.2* requires each user to be identified before allowing any relevant actions on behalf of that user. Further the objective requires that the TOE will at least maintain the role administrator. This is defined in *FMT_SMR.1*, which defines the role.

The security objective **O.AUTHENTICATE** is met by *FIA_AFL.1, FIA_UAU.2 and FIA_UID.2*. *FIA_AFL.1* meets this objective by ensuring that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials. After some configurable number of failed login attempts from the same IP, the IP address is blocked from authenticating again. *FIA_UAU.2* meets this objective by requiring that all TOE users be successfully authenticated before allowing any other TSF-mediated actions on behalf of those TOE users. *FIA_UID.2* meets this objective by requiring that all TOE users be successfully identified before allowing any other TSF-mediated actions on behalf of those TOE users.

The security objective **O.LIMEXT** is met by *FMT_MOF.1 and FMT_SMF.1*. *FMT_MOF.1* meets this objective by restricting the ability to access and perform security functions to TOE users with sufficient permission level. *FMT_SMF.1* meets this objective by requiring that the TOE provides specification of Management Functions for TOE users.

The security objective **O.MEDIATE** is met by *FDP_IFC.1, FDP_IFF.1*, *FMT_MSA.1 and FMT_MSA.3*. *FDP_IFC.1* meets this objective by specifying the rules by which subjects will accept, reject, or drop information to flow to and from other subjects. *FDP_IFF.1* meets this objective by specifying the rules by which subjects will accept, reject, or drop information to flow to and from other subjects. *FMT_MSA.1* meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy, which restricts the ability create or delete security attributes in the Traffic Information Flow Control List to an Administrator or Security Admin. *FMT_MSA.3* meets this objective by ensuring that the Traffic Information Flow Control Security Functional Policy has a permissive default policy that can be changed only by an Administrator or Security Admin.

The security objective **O.SECFUN** is met by *FIA_UAU.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3, FTA_SSL.4 and FTA_TAB.1*. *FIA_UAU.2* meets this objective by requiring that all TOE users be successfully authenticated before allowing any other TSF-mediated actions on behalf of those TOE users. *FMT_MOF.1* meets this objective by restricting access and performance of TOE security functions to TOE users with sufficient permission level. *FMT_MSA.1* meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy, which restricts the ability to create or delete security attributes in the Traffic Information Flow Control List to Administrator or Security Admin. *FMT_MSA.3* meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy to provide restrictive default values for security attributes. *FMT_SMF.1* meets this objective by requiring that the TOE provides specification of Management Functions for TOE users. *FMT_SMR.1* meets this objective by defining the permission levels available to TOE users. *FTA_SSL.3* meets this objective by terminating an interactive session after a configurable time interval of TOE user inactivity at the Management Console. The TOE users must then login again to access the TOE. FTA_SSL.4 meets this objective by allowing the user to terminate an interactive session by himself. *FTA_TAB.1* meets this objective by allowing the Administrator or Security Admin to configure the TOE by displaying an access banner warning against unauthorized access.

5.4.2 Fulfilling the SFR Dependencies

The following table shows that all dependencies are met:

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1 is satisfied in the IT environment (see OE.TSP).
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FIA_UID.3	No dependencies	-

SFR	Dependencies	Fulfilled by
FIA_UAU.2	FIA_UID.1	FIA_UID.3
FIA_AFL.1	FIA_UID.1	FIA_UID.3
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_SSL.3	No dependencies	-
FTA_SSL.4	No dependencies	-
FTA_TAB.1	No dependencies	-

Table 14: Fulfilling the SFR dependencies

5.4.3 Security Assurance Requirements Rationale

The TOE claims compliance to EAL4 level of assurance augmented by ALC_FLR.3. As described in [2], the level EAL4 indicates that the product is methodically designed, tested, and reviewed.

The assurance requirements for life cycle support have been augmented by ALC_FLR.3 (Systematic flaw remediation) to account for regular bug fixes for the TOE.

This is considered appropriate for attackers with Enhanced-Basic attack potential. The Security assurance requirements are chosen because of the evaluation level EAL4 according to [2].

6 TOE Summary Specification

6.1 TOE Security Functionality

6.1.1 Security Audit functionality

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security-relevant configuration changes are recorded to ensure accountability of the administrator's actions. All logs contain the time, device, type of event, log ID, and priority. Firewall log files additionally contain component, action, username, firewall rule, incoming interface, outgoing interface, source IP, and destination IP.

The TOE generates log files with information about security related events for administrator review to monitor network security and activity, identify security risks, and address these risks. These events are maintained in the local logs until the system is shutdown or rebooted. Records are also sent to an external syslog server, which maintains and stores historical audit records.

A log file is a list of events, along with information about those events. An event is an activity that occurs on the TOE. For example, TOE's denying of a packet based on a policy set is an event. The TOE also captures information about allowed events to give a more complete picture of the activities on the network.

The TOE audit events are generated in the form of logs which are generated and saved in several types of log messages. The log message types are:

- Firewall rules – Log records of the entire traffic for firewall
- Invalid traffic log – Log records of the dropped traffic that do not follow the protocol standards, invalid fragmented traffic, and traffic whose packets the TOE is not able to relate to any connection
- Administration log – Administrator logins and changes to configuration parameters and access rules

To preserve the firewall functionality during DoS/DDoS attacks, the firewall reduces logging functionality over the syslog interface and the web admin console log viewer when under heavy load. When the firewall is in this mode, no packet information is logged. The other log events are still logged (e.g. user login, configuration change).

The TOE administrator has the ability to view and search in all audit events generated since the last system reboot on the local audit logs. Audit events that precede a system power loss can only be viewed on the external syslog server. This includes the audit record of the shutdown of the audit function. The local logs can be searched based on common fields for all events, as well as access firewall rule fields. They can be sorted and ordered based on any of the fields listed in Table 15 below. The TOE protects the stored audit records from unauthorized deletion and modification.

The TOE audit records contain the following information:

Field	Content

Date	Date (yyyy-mm-dd) when the event occurred
Time	Time (hh:mm:ss) when the event occurred
Timezone	Time zone of Sophos Appliance
Device_name	Model Number of the Sophos Appliance (syslog only)
Device_id	Unique Identifier of the Sophos Appliance (syslog only)
Log_id	Unique 12 characters code (syslog only)
Log_type	Type of event occurred in Sophos
Log_component	Component responsible for logging
Log_subytpe	Sub type of event occurred in Sophos
Priority	Severity level of the event
Message_id	Message identifier for event (local logs only)

Table 15: Common Fields

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

6.1.2 User Data Protection

The security policy of an organization in the context of computer networking is a set of rules to protect the computer networks of an organization and the information that goes through it. By default, the TOE denies all packets that are not specifically allowed. The TOE enables the administrator of the TOE to add a policy. Through the use of policies, the administrator configures a set of firewall rules that tell the TOE to allow or deny traffic based upon factors such as source and destination of the packet, port number, as well as the transport protocol type. Transport protocol that can be filtered are TCP and UDP.

The User Data Protection function implements functionality for TOE security functions and TOE security functional policies related to protecting user data. The user data that the TOE is protecting is the information passing through the TOE. This functionality is provided by the application of firewall access rules. The Traffic Information Flow Control Security Functional Policy enforces rules on subjects that send traffic through the TOE, or receive traffic flowing through the TOE. The rules in the security policy determine whether traffic should be accepted from the sender to the receiver, passage rejected, or dropped based on the following security attributes: source IP address, destination IP address, port number, and TCP and UDP protocols.

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

6.1.3 Identification and Authentications

The Identification and Authentication functionality establishes and verifies a claimed administrator identity. The TOE requires successful identification and authentication of all users (administrator) before allowing access to any management functionality of the Web Admin Console. The TOE provides the identification and authentication mechanism by means of a PostgreSQL database for storing the credentials. This ensures that the user has the appropriate privileges associated with the assigned profile. Only authenticated users are allowed access to the TOE and TOE security functions. Users must be identified and authenticated prior to performing any TSF-mediated actions on the TOE. For each user, the TOE stores the following security attributes locally: username, password, and profile. 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 username and password match, the TOE administrator is assigned the roles associated with that username.

The TOE will lock out all user accounts from an IP address if a user fails to enter the proper credentials after an administrator-configurable number of failed login attempts.

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

6.1.4 Security Management

The Security Management function specifies the management of several aspects of the TSF, including security function behavior and security attributes. The TOE provides two built-in administrative accounts: admin and Sophos. Both these accounts have default passphrases pre-supplied for them, which must be changed during the initial configuration and both fall into the Administrator profile. The TOE allows administrators to create profiles for various administrator users. Profiles are a function of an organization’s security needs and can be set up for special-purpose administrators in areas such as firewall administration, network administration, and logs administration. A profile separates the TOE’s features into access control categories for which an administrator can enable none, read only, or read-write access. Profiles created by an administrator can represent the following five different roles by default:

- Administrator – super administrator with full privileges
- Audit Admin – read-write privileges for Logs & Reports only
- Security Admin – read-write privileges for all features except Profiles and Log & Reports
- Crypto Admin – read-write privileges for Certificate configuration only
- HAProfile – read-only privileges. This role is assigned to Administrators accessing the Web Admin Console when HA is configured. HA is not configured in the evaluated configuration, so this role will not be assigned.

Adding or deleting rules in the Traffic Information Flow Control SFP (i.e. accept, reject, or discard) is limited only to the Administrator or Security Admin roles.

The TOE provides restrictive default values for the Traffic Information Flow Control SFP security attributes and allows only the Administrator or Security Admin to set different values. Also, specifying alternative initial values for security attributes to override the default values is limited to Administrator and Security Admin profiles.

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

6.1.5 TOE Access

The TOE Access function specifies requirements for controlling the establishment of an administrator's session, which is configured by Administrator roles with sufficient permission level. The TSF terminates an administrator's interactive session after a configurable time interval of administrator inactivity at the Web Admin Console, the default time interval is 10 minutes. Additionally, the Administrator can terminate the interactive session by himself. If an administrator's session is timed out, the administrator must log back in to the TOE to perform any further functions.

An Administrator or Security Admin can configure the TOE to display an advisory warning message regarding unauthorized use of the TOE before an authentication session occurs.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

7 Glossary and Acronyms

Term	Definition
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
LAN	Local Area Network
NTP	Network Time Protocol
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8 References

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

Cryptography

[3] RFC4253, SSH Transport Layer Protocol, http://www.ietf.org/rfc/rfc4253.txt

[4] RFC 791, Internet Protocol, http://www.ietf.org/rfc/rfc791.txt

[5] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, http://www.ietf.org/rfc/rfc2460.txt