SOPHOS
Security made simple.

Security Target

Sophos UTM V9 Packet Filter Version 1.000

Assurance Level EAL4+
Common Critera v3.1 Revision 4

Document version: 1.00
Document date: 2015-03-25

Document History

Version	Date	Change(s)	Author(s)
0.90	2014-02-19	Created first version for evaluation body	Martin Becker
0.91	2014-04-25	- Changed TOE name to “Sophos UTM V9 Packet Filter” - Added certification ID - Minor adoptions in text	Martin Becker
0.92	2014-07-14	Deleted statement “The assumption A.SECINIT is covered by OE.SECINIT as directly follows.” in Section 4.3.3	Martin Becker
0.93	2014-09-19	Updated hardware requirements in section 1.2.2	Martin Becker
0.94	2014-09-22	Fixed incongruent OSI layer of ICMP	Martin Becker
0.95	2014-10-27	Added application developer as external entity in section 3.3	Martin Becker
1.00	2015-03-25	Replaced placeholder for guidance document in Section 1.3.1	Martin Becker

Contents

List of Tables

1 ST Introduction

1.1 ST Reference and TOE Reference

Title:	Security Target Sophos UTM V9 Packet Filter
Sponsor:	Sophos Technology GmbH
Editor(s):	Martin Becker
Document version:	1.00
Document date:	2015-03-25
CC version:	3.1, Revision 4
Assurance level:	EAL4+ (EAL4 augmented by ALC_FLR.2)
Certification ID:	BSI-DSZ-CC-0942
Keywords:	Packet filter, network security, information flow control
TOE name:	Sophos UTM V9 Packet Filter
TOE version:	1.000

1.2 TOE Overview

1.2.1 Usage, Major Security Features and TOE Type

This Security Target defines the security objectives and requirements for the Sophos UTM V9 Packet Filter (TOE), a software component of Sophos Technology GmbH. Sophos UTM V9 Packet Filter provides packet filter functionality. Sophos UTM V9 Packet Filter allows the integration of packet filter capability into Sophos UTM. Therefore, the Sophos UTM V9 Packet Filter is delivered to an application developer. The application developer integrates the Sophos UTM V9 Packet Filter into an application in order to build a network component. The administrator of this application is defined as “TOE end-user”.

When IP networks with different levels of security are interconnected, this is usually done by introducing special network components at the border of the networks. These components provide firewall functionality and separate the two or more networks from each other on different levels of the network stack. Data flow from one to another network can be allowed by a rule based policy enforced by these network components.

The Sophos UTM V9 Packet Filter consists of software on machines to implement packet filter functionality for the network components; i.e. the Sophos UTM V9 Packet Filter is part of the network components. The Sophos UTM V9 Packet Filter relies on information available at OSI layer 3 and layer 4 for policy enforcement. The functionality for packet filtering is part of the operating system (Linux). The Sophos UTM V9 Packet Filter supports IPv4 [4] and IPv6 [5].

The TOE major security features are:

- 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 information flow 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 TOE verifies the identification information of an administrator provided by the environment (application) before any management function is performed.

The following security services are not part of the TOE and are thus to be provided by the IT environment (application):

- The environment provides Identification and Authentication of the administrator
- Forwarding of audit data to a management machine (syslog host)

The generation of networks filter traffic rules (policy) and configuration data takes place in the IT environment. The IT environment provides NTP service and Syslog service.

After start-up of a network component that comprise the TOE and a secure initialisation process the initial TOE configuration data is read via I/O-control interface in the TOE system start-up process. The configuration data is the human readable content of the configuration file. The configuration data comprise IP address- and network interface definition, static routes and other system parameters. If no configuration data is available on start-up the TOE will not start-up automatically.

1.2.2 Required Non-TOE Hardware/Software/Firmware

The TOE has the following minimal requirements concerning the physical machine they run on:

- Intel i686 compatible CPU
- PCI bus system
- Two or more PCI Ethernet network interface cards (100Mbit or 1000Mbit)
- 1024 MB RAM
- Storage entity (20 GB IDE or SCSI hard disk drive)
- Bootable IDE or SCSI CD-ROM drive

The hardware must be compatible with the Linux operating system used for the application.

The physical connections are:

- power supply
- network interfaces
- PS/2- or USB-attached keyboard
- VGA graphics adapter

1.3 TOE Description

1.3.1 Physical Scope of the TOE

The TOE consists of several components that are all running in kernel-space on the Linux operating system. These components are the following kernel parts: packet filter, management, and audit mechanism. All other parts of the system are considered to be environment of the TOE.

The TOE is delivered to an application developer. The TOE delivery includes the software Sophos UTM V9 Packet Filter and the guidance document (see [6]). The software component is electronically signed.

Delivered TOE Parts	Version	Remarks
Software component Sophos UTM V9 Packet Filter	Version 1.000	Sophos UTM V9 Packet Filter Software on CD-ROM
Guidance Document	Version 0.92	Delivered as PDF on Sophos UTM V9 Packet Filter CD-ROM

Table 1: Scope of TOE delivery

1.3.2 Logical Scope of the TOE

1.3.2.1 Audit Data

The TOE collects audit data 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. Furthermore, the shutdown of the underlying system always generates an audit record. 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

1.3.2.2 Information Flow Protection

The TOE 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 based on the information flow policy. Therefore the TOE implements the information flow control (as routers) on the network layer (IP/ICMP) and transport layer (TCP/UDP). In order to apply the packet filter rules the network components take the information from the IP/ICMP and TCP/UDP-Header (where applicable).

1.3.2.3 Management

The TSF is capable of performing the following management functions:

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

The TOE verifies the identification information of an administrator provided by the environment (application) before any management function can be performed. The TOE is initialized with a strict packet filter rule set, that is, everything is dropped.

1.3.2.4 Components

The Sophos UTM V9 Packet Filter consists of several components. Table 2 shows which components are parts of the TOE and which ones are parts of the IT environment:

	IT environment	TOE
Kernel	-	Packet filter Audit mechanism Management
User space	Secure transport mechanism for configuration data and audit data. Management (configuration tool)	-

Table 2: Sophos UTM V9 Packet Filter components

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.2**.

ALC_FLR.2 adds flaw reporting 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 machine. Configuration data transmitted from the management machine to the network components.
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.

Table 3: Assets

3.2 Subjects

No active entity in the TOE that performs operations on objects is defined.

3.3 External Entities

The following external entities may interact with the TOE:

External entity	Description
Administrator	The administrator of a network component is an entity that has complete trust with respect to all policies implemented by the TSF. He is in charge of installing and configuring the TOE as well as performing the management functions of the TOE.
User	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE. A goal of a user may be to access or modify sensitive information by sending IP packets to or receiving from the components of the TOE. This includes attacks from the protected networks behind the network components as well as attacks from outside those networks. Attackers with an Enhanced-Basic attack potential are assumed.
Application developer	The application developer is an entity that integrates the TOE into other firewall and UTM products. Prior to integrating the TOE into such applications, the application developer is obliged to verify the integrity and authenticity of the TOE deliverables.

Table 4: External entities

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 (see A.I&A) with care, specifically that he will keep them secret and can use it in a way that nobody else can read it.

Assumption	Description
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.
A.INFLOW	The administrator assures that the packet filter components provide the only connection for the different networks.
A.CONFW	The configuration interface of the network components (TOE and application) refuses all connections, except the SSH protocol from the management machine.
A.TSP	The IT environment provides reliable timestamps (NTP server).
A.PROT	The connection between the management machine 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.I&A	The environment facilitates Identification and Authentication of an administrator.

Table 5: Assumptions

3.5 Threats

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.

Threat	Description
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.

Table 6: Threats

3.6 Organisational Security Policies

The TOE does not enforce organisational 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 4.2) 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.AUDIT	The TOE must provide an audit trail of security-related events.

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 (see A.I&A) 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.
OE.INFLOW	The administrator must assure that the packet filter components provide the only connection for the different networks.
OE.CONFW	The configuration interface of the network components (TOE and application) refuses all connections, except the SSH protocol from the management machine.
OE.TSP	The IT environment provides reliable timestamps (NTP server).
OE.PROT	The connection between the management machine 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.
OE.I&A	The environment must facilitate Identification and Authentication of an administrator.

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.CONFW	OE.TSP	OE.PROT	OE.AUDIT	OE.I&A	O.FILTER	O.AUDIT	O.MANAGEMENT
A.ENV	X										
A.NOEVIL		X									
A.INFLOW			X								
A.CONFW				X							
A.TSP					X						
A.PROT						X					
A.AUDIT							X				
A.I&A								X			
T.BYPASS	X		X			X			X		
T.WEAKNESS				X			X	X		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,* 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 machine or network components nor routes around the management machine or network components. 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 machine 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.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.I&A*, *O.AUDIT*, *OE.AUDIT*, *OE.CONFW* and *O.MANAGEMENT*. *O.AUDIT* and *OE.AUDIT* ensure detection of attempts to compromise the fenced network including the network component that includes the TOE. *O.MANAGEMENT* and *OE.I&A* 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. Other users will be rejected at the configuration interface. The environmental objective *OE.CONFW* ensures that no service beside SSH run on the network components.

4.3.2 Covering the OSPs

The TOE does not enforce organisational 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.CONFW** is covered by *OE.CONFW* 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.I&A** is covered by *OE.I&A* 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 5.2).

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
User Data Protection (FDP)	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
User identification (FIA)	
FIA_UID.1	Timing of identification
Security management (FMT)	

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

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:

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

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

c) [*starting of network components*; IP datagrams matching log filters in packet filter rules]

FAU_GEN.1.2 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, [*no other audit relevant information*]

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: 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. Furthermore, the shutdown of the underlying system always generates an audit record. For that reason, whenever an audit record of the shutdown of the system is generated, one can be assured that the audit functions of the TOE are shut down as well.

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 [*Packet Filter SFP*] on [

Subjects: users (external entities) that send and/or receive information through the

TOE to one another;

Information: data sent from one subject through the TOE to one another;

Operation: pass the data].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

Application Note: The Packet Filter SFP 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: users (external entities) that send and/or receive information through the TOE to one another;

Subject security attributes: none;

Information: data sent 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, time].

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*].

FDP_IFF.1.3 The TSF shall enforce the [*reassembly of fragmented IP datagrams before inspection*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- The TOE shall reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject does not belong to the network associated with the interface (spoofed packets);
- The TSF shall drop IP datagrams with the source routing option;
- The TOE shall reject fragmented IP datagrams that cannot be

reassembled completely within a bounded interval].

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

Application Note: The subject definition in FDP_IFF.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.

5.1.3 User Identification (UID)

5.1.3.1 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [*the following TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

- all actions except for administrative actions as specified by FMT_SMF.1

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Refinement: The TOE verifies the identification information of an administrator provided by the environment (see OE.I&A) before any management function can be performed.

Application Note: The “user” in FIA_UID.1.2 is identical to the Administrator defined in the external entities definition in Chapter 3.3.

5.1.4 Security Management (FMT)

5.1.4.1 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*, [*no other operations*]] the security attributes [*network traffic filter rules and configuration data*] to [*the role 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

5.1.4.2 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 [*no roles*] 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

5.1.4.3 FMT_SMF.1 Specification of management functions

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

- Modification of network traffic filter rules,
- Modification of configuration data].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.4.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role [*administrator*].

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

5.2 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.2**, ALC_LCD.1, ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

Table 11: Chosen Evaluation Assurance Requirements

These assurance components represent EAL4 augmented by the component ALC_FLR.2 (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

	O.FILTER	O.AUDIT	O.MANAGEMENT
FAU_GEN.1		X	
FIA_UID.1			X
FDP_IFC.1	X		
FDP_IFF.1	X		
FMT_MSA.1			X
FMT_MSA.3	X		
FMT_SMF.1			X
FMT_SMR.1			X

Table 12: 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.AUDIT** is met by *FAU_GEN.1*. *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.

The security objective **O.MANAGEMENT** is met by *FMT_SMF.1, FMT_MSA.1, FIA_UID.1 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.1* 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.

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).
FIA_UID.1	No dependencies	-
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_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

Table 13: Fulfilling the SFR dependencies

5.4.3 Security Assurance Requirements Rationale

The TOE claims compliance to EAL4 level of assurance augmented by ALC_FLR.2. 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.2 (flaw reporting procedures) 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

The following table illustrates the mapping of the TOE security functionality and SFRs.

	FAU_GEN.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1
SF1.1		X	X					
SF1.2			X					
SF1.3			X					
SF2.1	X							
SF2.2	X							
SF3.1							X	
SF3.2				X	X			X
SF3.3						X		

Table 14: TOE security functionality and SFR mapping

The following sections provide a more detailed explanation of the TOE security functionality.

6.1.1 SF1 Information Flow Protection

SF1.1 meets FDP_IFC.1. SF1.1, SF1.2, and SF1.3 meet FDP_IFF.1:

SF1.1: The TSF implements the information flow control (as routers) on the network layer (IP/ICMP) and transport layer (TCP/UDP). In order to define packet filter rules, the TSF provides packet filter criteria and packet filter actions. The packet filter criteria are:

- source address
- destination address
- transport layer protocol
- interface on which traffic arrives and departs
- port
- time

The packet filter actions are:

- accept (= permit)
- reject[1] (= deny)
- drop

In order to apply the packet filter rules the network components take the information from the IP/ICMP and TCP/UDP-Header (where applicable).

SF1.2: The TSF reassembles IP datagrams before further processing is performed. IP datagrams which cannot be reassembled are dropped in a predefined span of time.

SF1.3: The TSF drops packets with spoofed source- or destination-IP addresses. Packets with source routing options are also dropped.

6.1.2 SF2 Security Audit

SF2.1 and SF2.2 meet FAU_GEN.1:

SF2.1: The TSF 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. Furthermore, the shutdown of the underlying system always generates an audit record. For that reason, whenever an audit record of the shutdown of the system is generated, one can be assured that the audit functions of the TOE are shut down as well.
- datagrams received or sent through a network components network interfaces if they match configured patterns

SF2.2: Each record includes:

- Time and Date
- Affected network component

[1] reject = drop and signal an error

- Subject identity (source IP)
- Type of event
- Affected interface
- Direction
- Action (accept, drop or reject)
- Optional depending on the protocol: IP addresses and ports

6.1.3 SF3 Management

SF3.1 meets FMT_SMF.1. SF3.2 meets FIA_UID.1, FMT_MSA.1 and FMT_SMR.1. SF3.3 meets FMT_MSA.3.

SF3.1: The TSF is capable of performing the following management functions:

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

SF3.2: In order to modify the security attributes network traffic filter rules and configuration data, the TOE maintains the role administrator. The TOE verifies the identification information of an administrator provided by the environment (see OE.I&A) before any management function can be performed. Therefore, the TOE verifies whether the user id is equal to zero.

SF3.3: The TOE is initialised with a strict packet filter rule set, i.e., everything is dropped.

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

Term	Definition
TSF	TOE Security Function

8 References

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4, CCMB-2012-09-002

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4, CCMB-2012-09-003

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

Documentation

[6] Sophos UTM V9 Packet Filter, documentation