ROS-ISÄK
Ronny Janse
010-2404426
ronny.janse@msb.se

Firewall Protection Profile

Innehållsförteckning

1. Introduction

1.1 PP reference

Title:	Firewall Protection Profile
Version:	Release Version 3.0, 2015-03-12
TOE Type:	IP Firewall
Evaluation Assurance Level:	EAL2, augmented with ALC_FLR.1
CC Version:	3.1 release 4
PP Author:	Staffan Persson Robert Hoffmann
Keywords:	Firewall, Package Filter, Network Gateway, IP, TCP/IP

1.2 TOE Overview

This Protection Profile (PP) describes the security requirements for a Firewall.

Unlike most other Protection Profiles, the Firewall Protection Profile (FPP) is structured into a “base” part and a set of (optional) “extended packages”. This structure was chosen to maximize adaptability for different operational environments and different operational requirements, since firewalls may provide a wide range of different functionality.

Firewalls often operate as a perimeter protection between an internal (protected network) and an external network, allowing certain traffic to pass through based on specific filtering rules. The filtering rules may be different for each specific environment, but more important is that the nature of the filtering functionality may be different between different firewalls. It is the different nature of these filtering mechanisms that are candidates for the different extended packages.

A firewall is a network device consisting of hardware and software providing perimeter protection of networks operating at network and transport level (layer 3 and 4) and/or application level (layer 7). The firewall described in this PP is limited to the Internet protocols IPv4, IPv6, TCP, UDP and ICMP.

Usually perimeter protection consists of a range of different security functionalities in addition to the address and port filtering, such as application level analysis and filtering, intrusion detection and prevention, use of authentication services, Virtual Private Networks, content analysis (malware analysis). Not all of these security features are considered part of the firewall security functionality and only some of these features are part of this Protection Profile.

The firewall in this context is assumed to provide a packet filter, audit of security relevant events and accountability of administrator actions. It is assumed that the firewall can be administrated remotely over a trusted

channel, allowing configuration changes and software updates to be made. It is also expected that the firewall performs self-tests to verify the correct functionality.

The firewall is intended for use by organizations that need controlled, protected and audited access to services, between the inside and the outside of the organization's network. In order to do this, the firewall must be located between the internal and external network, such as a local area network and the Internet, and shall mediate traffic according to information flow control policies.

1.3 TOE Description

1.3.1 Introduction

The TOE may be all of or a part of a stand-alone firewall appliance that is dedicated to perimeter protection of the internal network. The TOE may provide additional functionality such as VPN and IDS. But any such security functionality is not part of the scope of the firewall security functionality described here.

There are at least two types of network interfaces of the firewall, the network interface to external networks and the network interface to internal networks. They are distinctly separate and there is at least one interface of each type, but there may be multiple interfaces of each type.

There may be additional networks (not shown in the picture below) for remote administration and audit, and additional interfaces for local administration. But this PP makes no requirements neither on availability or nature of any such interfaces.

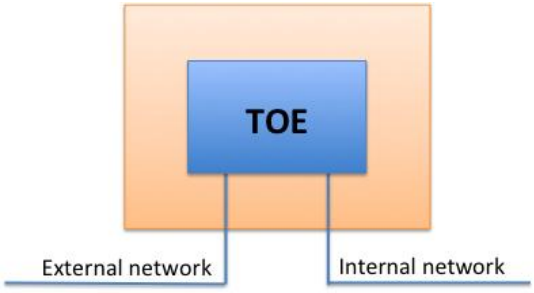

Figure 1: TOE scope and interfaces

1.3.2 Intended usage

The TOE is intended for use by organizations that need controlled, protected and audited access to services, both from inside and outside their organization's network. The TOE is intended to be located between the internal and external network, such as a local area network and the Internet, and shall mediate traffic according to information flow control policies. It is assumed to be the only connection between these two networks.

The administrators of the TOE are assumed to be trained and trusted in managing the TOE, as well as in general network management and network security. The TOE shall operate in a physically protected environment to ensure that the TOE cannot be physically accessed and tampered with.

1.3.3 Security features

The TOE provides the following security functions:

- Information flow control: Information flow control (layer 3 and 4) between the external and the internal networks.
- Management of the TOE: Local and/or remote administration, configuration changes and software updates.
- Administrator identification and authentication: The remote administrators must be identified and authenticated by the TOE.
- Audit: Audit of security relevant events, trusted updates, configuration changes and self-tests.
- Verification of software updates: The TOE may perform software updates when initiated by an administrator. The TOE must verify the authenticity and integrity of the software and also verify that the software is newer that the current version before the TOE is using the new software.
- Self-test and protection of system files: Self-test and integrity verification of system files must be performed during start-up as well as initiated by the administrator.

1.4 Conditional security features

The TOE claiming compliance to this Protection Profile must provide at least one of two security functionalities:

- Stateful Packet Filter (SPF)
- Deep Package Inspection (DPI)

Items in the formal parts of the PP, such as threats, security objectives and SFRs that are unique to a specific conditional part, are clearly identified as such with the unique tag {SPF} for Stateful Packet Filter and {DPI} for Deep Package Inspection.

1.4.1 Stateful packet filter

The Stateful Packet Filter (SPF) describes the security requirements for a packet filtering firewall that is capable of tracking information flow states.

A SPF is defined as a packet filtering firewall that is also able to react on the logical state of an information flow. An information flow is a transaction within a communication protocol, with a defined start and end (the end of a

transaction can be active, i.e., through a command, or passive, e.g., through a time out). The firewall notes the start and end of a supported information flow, and allows for filtering rules that cover all packets that are part of the flow. The typical use case is to either allow or deny a specific information flow by specifying one rule, and have the firewall inherit the decision for all subsequent packets of that specific flow.

Certain protocols allow for multiple actions within one transaction. E.g., within one FTP session, multiple files can be transferred. In such a case the overarching session, e.g., the FTP session, is considered as the information flow within this PP.

If SPF functionality for multiple protocols is to be supported, the ST author must include the SFRs once and then iterate through the protocols.

States of information flows can exist at any layer of the ISO/OSI model. Security Targets that claim compliance with SPF functionality can claim support for those protocols that are listed in the FPP, or higher layer protocols that build upon them.

If keeping state of a supported protocol requires keeping the state of further underlying protocols, only those protocols that can be used as a filter criterion shall be documented herein. E.g., an SPF firewall that only allows filtering the state of HTTP connections, will most probably also need to keep the state of the underlying TCP sessions. But since it does not expose TCP state filtering to the user, it must not make any claim to the TCP protocol.

1.4.2 Deep packet inspection

The Deep Packet Inspection (DPI) describes the security requirements for a protocol aware filtering firewall, typically at layer 7 (e.g., HTTP).

A DPI firewall is defined as a packet filtering firewall that is also able to react on higher layer protocol information, including the protocol header and the payload. The DPI firewall is therefore protocol aware, and allows the administrator to define filter rules based on the protocol information.

Note: In order to manage single units of the claimed protocol (e.g., a HTTP request), the DPI firewall might need to collect and assemble multiple underlying packets. This required vertical integration action should not be mistaken with the horizontal analysis of a stateful firewall, which collects the states or items of an interaction flow.

If DPI of multiple protocols is to be supported, the ST author must include the SFRs once and then iterate through the protocols.

If a supported protocol requires further underlying protocols to function, only those protocols that can be used as a filter criterion shall be documented herein. E.g., a DPI firewall that can only filter the HTML protocol must not claim HTTP or TLS.

1.5 Optional security features

The firewall may have optional functionality that may describe in extended packages or claimed by the ST author directly in the ST. They are not part of or described as part of this PP. Such examples are:

- Virtual Private Network, VPN (connecting the inside network to with a remote network over an external, untrusted network)
- Network Address Translation (NAT) or Port Address Translation (PAT). This means that the firewall will translate the network addresses or port numbers as part of its firewall functionality.
- User authentication for access (from inside to outside and vice versa). This means that the firewall is aware of individual users and applies access control rules that may be associated to addresses or services accessed, i.e. control at address or port level.
- Fail-over mechanism that will allow for multiple firewalls to operate as a cluster, i.e., having another firewall taking over when the current one goes down.

1.6 Additional TOE software, hardware and firmware

The scope of the TOE as described in this PP requires underlying software and hardware, which may include the operating system and hardware platform and network cards. The environment is able to receive, store and protect the audit records generated by the TOE and provides the means for analysis of the audit records. The TOE environment provides the TOE with a reliable time stamp, which is typically in a network environment an NTP source that is trusted, typically located in the internal network.

The TOE requires functionality to process X.509 certificates. It is up to the ST author to either:

- Claim this functionality as part of the TOE:
  No additional changes are required.
- Require the environment to provide the functionality:
  The source of the functionality must be stated in this chapter as an external resource. OE.RELHARD ensures that this resource is reliable. An application note must be added to FCS_COP.1 {ADMIN}/{UPDATE} to indicate the location of the X.509 functionality.

1.7 Glossary

NAT	Network Address Translation. A mechanism for assigning local networks a set of IP addresses for internal traffic and another for external traffic. NAT was originally described in RFC 1631 as

	a means for solving the rapidly diminishing IP address space. It provides a supplemental security purpose by hiding internal IP addresses.
Packet filter	A method of controlling access to a network, or set of networks, by examining packets for source and destination address information, and permitting those packets to pass, or halting them based on defined rules.
PAT	Port Address Translation. A mechanism for reassigning port numbers used on the local connection to different port number on the external network assignment. It is often used in combination with Network Address Translation (NAT).
Protocol	An agreed-upon format and sequence for transmitting data between two or more devices. Protocols typically define how to check for errors, how the sender will announce they have completed the sending of data, how the receiver will acknowledge receipt of the data, and how they will compress the data.

1.8 References

[NDPP]	U.S. Government Approved Protection Profile - Protection Profile for Network Devices Version 1.1, 08 June 2012.
[OSPP]	Operating System Protection Profile, Common Criteria Protection Profile BSI-CC-PP-0067, Version 2.0, June 2010.

1.9 Firewall Protection Profile framework

The Firewall Protection Profile (FPP) specifies alternative approaches of security functionality as well as the definition of functional extensions that can be optionally claimed by an ST in addition to the FPP base. The functional extensions use a model that was developed for the Operating System Protection Profile [OSPP]. As such, the FPP defines the following components:

- The FPP base specifies the conformance claim, security problem, objectives, and security functional requirements that are to be implemented by every firewall. The FPP base is mandatory and defines the common denominator for all firewalls claiming conformance with the FPP.
- The FPP base contains security functional requirements that are mandatory but conditional, such as alternative filtering functionalities where at least one of the approaches must be implemented. These conditional security functionalities must only be used for parts that are mandatory, but for which there are alternative approaches of which at least one must be implemented.
- An FPP extended package specifies the security problem definition, objectives, and security functional requirements for mechanisms that may be implemented in addition to the FPP base. Usually, an FPP extended package defines an extension that is either desired or implemented by several firewalls. However, the functionality specified in an FPP extended package is not commonly found among general-

purpose operating systems. FPP extended packages can optionally be added to the FPP base functionality when writing an ST. The ST author may choose from the FPP extended packages when deriving an ST.

The FPP is defined as a flexible and extensible framework. The current set of FPP extended packages can be enhanced with new or updated FPP extended packages. Those will then be part of a re-evaluation and re-certification of the FPP base.

1.9.1 Mandatory information given by the ST

The following information must be given as part of the ST derived from the FPP.

When specifying conformance to the PP, the ST must specify to which of the conditional parts and to which extended packages the ST shall conform to. In addition, the ST must claim conformance to any PP extended packages that are dependencies of the PP extended packages claimed by the ST.

When specifying the SFRs as part of the ST, a reference to the PP base or extended package abbreviation must be given in order to facilitate a direct mapping of the SFR, specifically considering iterations.

This requirement shall support ST authors and evaluators to ensure that no SFR from the FPP base or an FPP extended package the ST claims conformance to is left uncovered.

1.9.2 Mandatory information given by the extended packages

The following information must be given for each extended package to allow the extended package to be embedded into the framework of the PP.

The following information must be given to identify an extended package:

- Extended package name in narrative English
- Abbreviation of the extended package name to allow easy and unambiguous reference to the extended package
- Version of the extended package
- Owner of the extended package; that is, who is in charge of performing authoritative changes

To specify how the PP extended package can be used together with other extended packages, the following information must be provided:

- A list of dependent extended packages with their respective minimum versions
- A list of disallowed extended packages with their respective minimum versions

Note that the extended package must not exclude the PP base or any portion of it (with the exception of any conditional parts that are not included). However, the extended package may specify a minimum version of the PP base that is required for the respective extended package.

If an existing extended package must be changed to accommodate another extended package (the “current” extended package), the author of the current extended package is requested to approach the owner of the existing extended package to agree on the required modifications.

The PP extended packages may define many aspects as an addition to the PP base. Specification includes the following information:

- Package introduction
- Dependencies on other extended packages
- Security Problem Definition
- Objectives
- Security Functional Requirements
- Refinements to Security Assurance Requirements.

1.9.3 Specification restricted to the PP base

The FPP base exclusively defines the following properties:

- Conformance claims to other Protection Profiles
- Conformance type (either strict or demonstrable)
- Conformance claim to the EAL including any augmentation

An FPP extended package may define refinements to assurance components. Refinements may provide guidance on how to satisfy the assurance requirements specifically for the SFRs in the extended package. However, one of the core requirements for the FPP is to keep the Protection Profile and all its modules covered under the CCRA mutual recognition agreement. Therefore, no PP extended package shall add an SAR or modify the level of an SAR that would exceed the boundary set by the CCRA mutual recognition agreement. Note that refinements are allowed operations for SFRs and SARs, and such refinements can well be used to guide the evaluator on how to evaluate aspects specific for the functionality defined in a package. Especially for SARs, refinements should be used; extended assurance components should be avoided when possible.

2. Conformance claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012. CC Part 2 extended.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 4 September 2012. CC Part 3 conformant.

The assurance package conformance is Evaluation Assurance level 2 (EAL2) augmented with ALC_FLR.1 Basic flaw remediation.

No Protection Profile conformance is claimed.

The Protection Profile specifies two conditional parts Stateful Packet Filter (SPF) and Deep Package Inspection (DPI). At least one of the two has to be fully included in any ST claiming conformance to this PP.

2.1 Conformance statement

This PP requires demonstrable conformance by any ST or PP claiming conformance to this PP.

3. Security problem definition

3.1 Assets

The assets to be protected are the following assets:

ID	Description
User Data	Access to IT assets, i.e., information and IT resources, within the network perimeter of the TOE. Assets that may be compromised by unauthorized access from the external network or by misuse from users or services on the internal network through access to the external network.
TSF Data	The firewall software, including configuration files and other system files. Assets that may be compromised by external or internal access to the firewall or malfunction of the TOE hardware.

Although the firewall is part of the connection and the perimeter protection it will not ensure the availability of the connection between the internal and external network, but only mediate the information flow between the internal and external network. This will not protect the availability of the IT resources on the internal network, but as a side effect it may limit the access to internal resources and thereby protect them from attackers on the external network.

3.2 Threat agents

Attackers are either unauthorized persons or IT entities on the external network, or users on the internal network trying to undetected transmitting

information or access services on the external network. The attackers are assumed to have no physical access, but unlimited network access (inside and outside) and time available.

3.3 Threats

ID	Description
T.UNDETECTED	Security Events Go Undetected An attacker may attempt to compromise the User Data and/or TSF Data without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.FLOW	Information Flow Control An attacker may send information through the TOE, which results in the exploitation and/or compromise of User Data.
T.TAMPER	Tampering with the TSF or TSF Data An attacker may access TOE management functions and read, modify or destroy security critical system data or tamper with the security functions.
T.UPDATE	TOE update An attacker may provide malicious TOE updates or old versions of the TOE software to introduce back-doors or known exploitable weaknesses into the TSF Data.

3.4 Organizational security policies

ID	Description
P.MANAGE	The TOE shall support the means to administrators to manage the security functions. The management may be performed locally at the TOE, remotely from a separate management network or from the internal network.
P.ADMACC	Administrators shall be held accountable for their actions through audit records.

3.5 Assumptions

ID	Description
A.LOCATE	The TOE is located between an external network, and an internal network containing the User Data that is to be protected. It is the only point at which traffic can flow between the two networks.
A.PHYSICAL	The TOE is operated in a physically secure environment, i.e., no unauthorized person has physical access to the TOE or its underlying software and hardware.
A.RELHARD	The underlying hardware, software, firmware (BIOS and device drivers) and the operating system functions needed by the TOE to guarantee secure operation are working correctly, and have no undocumented security critical side effect on the security objectives of the TOE.
A.AUDIT	The environment is able to receive, store and protect the

	audit records generated by the TOE and provides the means for analysis of the audit records.
A.ADMIN	Authorized administrators given privileges to administrate the TOE are competent, non-hostile and follow all their guidance; however, they are capable of error.
A.TIME	The TOE environment provides the TOE with a reliable time stamp.

4. Security objectives

4.1 Security objectives for the TOE

ID	Description
O.MEDIATE	The TOE must mediate the flow of all information flowing between the internal and external network interfaces of the TOE.
O.AUDIT	The TOE must be able to provide an audit trail of security relevant events and of authorized use of security functions, and allow an authorized administrator to configure additional security relevant events that are to be audited.
O.MANAGE	The TOE must provide the means for an authorized administrator to configure and manage the TOE security functions.
O.RESTRICT	The TOE must restrict the means for configuration and control of the TOE to authorized administrators.
O.REMOTE	The TOE must uniquely identify and authenticate the identity of all remote administrators and provide them with a secure communication channel before allowing remote administrators any access to the TOE.
O.INITIAL	Upon initial start-up of the TOE or during configuration, the TOE shall provide well-defined initial settings for security relevant functions.
O.PROTECT	The TOE must protect itself against attempts by attackers to bypass, deactivate or tamper with TOE security functions.
O.UPDATE	The TOE must only accept updates that are newer than the currently running version and where the origin and integrity of the update can be trusted.

4.2 Security objectives for the environment

ID	Description
OE.LOCATE	The TOE must be located between an external network, and an internal network containing the User Data that is to be protected. It must be the only point at which traffic can flow between the two networks.
OE.PHYSICAL	The TOE must be operated in a physically secure environment, i.e., no unauthorized person may have physical access to the TOE or its underlying software and hardware.
OE.RELHARD	The underlying hardware, software, firmware (BIOS and device drivers) and the operating system functions needed by the TOE to guarantee secure operation must be working

	correctly and must have no undocumented security critical side effect on the security objectives of the TOE.
OE.AUDIT	The environment must be able to receive, store and protect the audit records generated by the TOE and provide the means for analysis of the audit records.
OE.ADMIN	Authorized administrators given privileges to administrate the TOE must be competent, non-hostile and follow all their guidance; however, they may be capable of error.
OE.TIME	The TOE environment must provide the TOE with a reliable time stamp.
OE.LOCAL_ADMIN	The environment must provide a mechanism to identify who had access at which time to the local administrative interface of the TOE.

4.3 Rationales

4.3.1 Security objectives coverage

The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective for the TOE covers at least one threat or policy and that each security objective for the TOE environment covers at least one threat, organizational security policy or assumption.

	O.MEDIATE	O.AUDIT	O.MANAGE	O.RESTRICT	O.REMOTE	O.INITIAL	O.PROTECT	O.UPDATE	OE.LOCATE	OE.PHYSICAL	OE.RELHARD	OE.AUDIT	OE.ADMIN	OE.TIME	OE.LOCAL_ADMIN
T.UNDETECTED		X										X		X	
T.FLOW	X					X			X						
T.TAMPER				X	X		X			X			X		
T.UPDATE								X		X					
P.MANAGE			X	X	X					X					
P.ADMACC		X			X					X				X	X
A.LOCATE									X						
A.PHYSICAL										X					
A.RELHARD											X				
A.AUDIT												X			
A.ADMIN													X		
A.TIME														X	

4.3.2 Security objectives sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

Threat	Rational for the security objectives
T.UNDETECTED	*An attacker may attempt to compromise the user Data and/or TSF Data without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.* This threat is addressed by: • Audit trail of security relevant events (O.AUDIT), • To received, store and protect the audit trail in the environment, and also provide the means for analysis of the audit records (OE.AUDIT), • Reliable timestamps being available for the audit trail (OE.TIME).
T.FLOW	*An attacker may send information through the TOE, which results in the exploitation and/or compromise of User Data.* This threat is addressed by: • Applying the TOE security policy to all information that passes through the networks between users and external IT entities (O.MEDIAT), • Upon initial start-up of the TOE or during configuration, the TOE provides well-defined initial settings for the security functions ensuring that the information flow control has well-defined settings (O.INITIAL) • Ensuring that the TOE is placed so that it can mediate the information flow (OE.LOCATE).
T.TAMPER	*An attacker may access TOE management functions and read, modify, or destroy security critical system data or tamper with the security functions.* This threat is addressed by: • The restricting the means to configuration and control of the TOE to authorized administrators (O.RESTRICT), who are competent, non-hostile and follow all their guidance (OE.ADMIN); • The uniquely identification and authentication of administrators and providing them with a secure communication channel before allowing administrators access to the TOE (O.REMOTE); • The protection of the TOE against attempts by attackers to bypass, deactivate or tamper with TOE security functions (O.PROTECT); • The TOE is operated in a physically secure environment, where an attacker has no physical access to the TOE (OE.PHYSICAL).
T.UPDATE	*An attacker may provide malicious TOE updates or old versions of the TOE software to introduce back-doors or known exploitable weaknesses into the TOE.* This threat is addressed by: • The TOE only accepting updates that are newer than the current running version and where the origin and integrity of the update can be trusted (O.UPDATE), • The TOE is operated in a physically secure environment, where an attacker has no physical

	access to the TOE (OE.PHYSICAL).

The following rationale provides justification that the security objectives of the TOE and the TOE environment are suitable to address each individual OSP and that each security objective tracing back to an OSP actually contributes in addressing the OSP.

OSP	Rational for the security objectives
P.MANAGE	*The TOE shall support the means to administrators to manage the security functions. The management may be performed locally at the TOE, remotely from a separate management network or from the internal network.* This policy is addressed by: • The TOE providing the means for an authorized administrator to configure and manage the TOE security functions (O.MANAGE); • Uniquely identifying and authenticating all administrators and providing them with a secure communication channel before any remote administrators is allowed any access (O.REMOTE); • The TOE must restrict the means for configuration and control of the TOE to authorized administrators (O.RESTRICT); • The TOE is operated in a physically secure environment, where an attacker has no physical access to the TOE (OE.PHYSICAL). While O.MANAGE applies to both local and remote access, O.REMOTE and O.RESTRICT apply to remote access only since OE.PHYSICAL is addressing this in the TOE environment.
P.ADMACC	*Administrators shall be held accountable for their actions through audit records.* This policy is addressed by: • Audit records which record security relevant events as well as allowing the authorized administrator to configure additional security relevant events to be audited (O.AUDIT); • Reliable time stamps for the audit records (OE.TIME); • Uniquely identifying and authenticating all remote administrators and providing them with a secure communication channel before any remote administrators is allowed any access (O.REMOTE); • Requiring the environment to identify who had access at a specific time to the local administration interface (OE.LOCAL_ADMIN); • Having the TOE operate in a physically secure environment, where attackers have no physical access to the TOE (OE.PHYSICAL) and its audit functionality.

The following rationale provides justification that the security objectives of the TOE environment are suitable to address each individual assumption and that each security objective tracing back to an assumption actually contributes in addressing the assumption.

Assumption	Rational for the security objectives
A.LOCATE	Addressed by OE.LOCATE, which is a rephrasing of the assumption.
A.PHYSICAL	Addressed by OE.PHYSICAL, which is a rephrasing of the assumption.
A.RELHARD	Addressed by OE.RELHARD, which is a rephrasing of the assumption.
A.AUDIT	Addressed by OE.AUDIT, which is a rephrasing of the assumption.
A.ADMIN	Addressed by OE.ADMIN, which is a rephrasing of the assumption.
A.TIME	Addressed by OE.TIME, which is a rephrasing of the assumption.

5. Extended components definition

The extended requirement FPT_TUD_EXT.1 is used to specify the SFR for trusted updates. It has been based on the extended component defined by the [NDPP] Protection Profile for Network Devices, published by NIAP in June 2012.

5.1 FPT_TUD_EXT – Trusted updates

5.1.1 Family Behaviour

The family defines the requirements for the trusted updates of the software of the TSF that may be part of or the entire TOE, and may also include parts that are outside of the scope of the TOE. These updates may be carried out at the request of the authorised administrator. Before the update is being installed, the updates must be verified to ensure the authenticity of the update and also that the updates is newer than the current running version. This is to prevent that manipulated or older updates, with known weaknesses, are being used.

5.1.2 Component levelling

FPT_TUD_EXT.1 Trusted updates allows an administrator to query the TOE software version and updated it with a newer one.

5.1.3 Management

While management functions have been specified as part of this component already, the following actions could be considered for the management functions in FMT:

a) Administrator initiation of updates or specification of certificates used for signature verification.

5.1.4 Audit

The following actions should be auditable if "FAU_GEN - Security audit data generation" is included in the PP/ST:

1. Minimum: Software update initiated.
2. Minimum: Failure of verification (digital signature, published hash or version number).

5.1.5 FPT_TUD_EXT.1 Trusted updates

Hierarchical to:	none
Dependencies:	FCS_COP.1 Cryptographic operation
FPT_TUD_EXT.1.1	The TSF shall provide administrators the ability to query the current version of the TOE software.
FPT_TUD_EXT.1.2	The TSF shall provide administrators the ability to update the TOE software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify software updates to the TOE using a [selection: *digital signature mechanism, published hash*] prior to installing those updates.
FPT_TUD_EXT.1.4	The TSF shall provide a means to verify software updates to the TOE to ensure that the software update version is newer than the current version of the TOE prior to installing those updates.

Application note: The term "current version of the TOE" shall be interpreted as the currently executing (i.e., active) TOE code.

ST author note: The digital signature mechanism and hash mechanisms referenced in the third element must be specified in FCS_COP.1. The ST author should choose the mechanism implemented by the TOE; it is acceptable to implement both mechanisms.

6. IT Security Requirements

6.1 Security Function Policies

6.1.1 FIREWALL Information Flow Control SFP {SPF}

The TOE will implement an information flow control Security Function Policy (SFP) called "FIREWALL Information Flow Control SFP {SPF}" that is used for the Stateful Packet Filter. The TSF shall enforce the SFP on the unauthenticated external IT entities that send and/or receive data through the TOE for all traffic sent through the TOE from one entity to another. The policy is named FIREWALL Information Flow Control SFP {SPF} to indicate that the information flow control SFP is implementing the Stateful Packet Filter.

The TSF shall enforce the FIREWALL Information Flow Control SFP {SPF} based on at least the following types of objects and security attributes:

- Objects:
    - network packet of protocol IPv4, IPv6, TCP, UDP or ICMP

- Security attributes:
    - presumed source IP address;
    - presumed destination IP address;
    - protocol [protocol name]: flow ID;
    - TOE interface on which the packet arrived;
    - TOE interface on which the packet is intended to leave, after a routing decision (if applicable);
    - service (protocol and port, if applicable).

The TSF shall permit an information flow if all of the following rules hold:

- the packet does belong to a protocol that is supported by the TOE
- the protocol is one of those allowed to pass through the TOE from the receiving to the sending interface
- the IP source and destination address are defined as being allowed to use the protocol
- the protocol specific filter rules allow the information to flow and this is the flow establishing packet
- the packet is part of an information flow that is allowed by an SPF rule, and the state has been previously established and this is not the flow establishing packet

The TSF shall explicitly deny an information flow if any of following rules applies:

- packets that are invalid fragments
- packets which cannot be reassembled completely
- packets where the source address of the packet is equal to the address of the network interface where the packet was received
- packets where the source address of the packet does not belong to the networks associated with the network interface where the packet was received
- packets where the source address of the packet is defined as being a broadcast address as specified in RFC 919 and RFC 922 for IPv4
- packets where the source address of the packet is defined as being a multicast address as specified in RFC 5771 for IPv4, and RFC 4291 for IPv6

- packets where the source address of the packet is defined as being a loopback address as specified in RFC 5735 for IPv4, and RFC 4291 for IPv6
- packets where the source or destination address of the packet is a link-local address as specified in RFC 3927 for IPv4, or link-/site-local address as specified in RFC 4291 for IPv6
- packets where the source or destination address of the packet is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4
- packets where the source or destination address of the packet is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6
- packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified
- packets in a wrong context, e.g., when an IP packet is not part of a valid TCP session
- the packet is part of an information flow that is denied by an SPF rule,
- the packet is part of an information flow but not the state establishing packet, and the state is currently not or no longer active

Application note: The security attribute “protocol (…): flow ID” is to be repeated for each additional (2nd etc.) protocol that is supported by the Stateful Packet Filter.

6.1.2 FIREWALL Information Flow Control SFP {DPI}

The TOE will implement an information flow control Security Function Policy (SFP) called “FIREWALL Information Flow Control SFP {DPI}” that is used for the Deep Packet Inspection. The TSF shall enforce the SFP on the unauthenticated external IT entities that send and/or receive data through the TOE for all traffic sent through the TOE from one subject to another. The policy is named FIREWALL Information Flow Control SFP {DPI} to indicate that the information flow control SFP is implementing the Deep Packet Inspection.

The TSF shall enforce the FIREWALL Information Flow Control SFP {DPI} based on at least the following types of objects and security attributes:

- Objects:
    - network packet of protocol IPv4, IPv6, TCP, UDP or ICMP
- Security attributes
    - presumed source IP address;
    - presumed destination IP address;

- TOE interface on which the packet arrived;
- TOE interface on which the packet is intended to leave, after a routing decision (if applicable);
- service (protocol and port, if applicable);
- protocol [protocol name]: header information;
- protocol [protocol name]: payload content.

The TSF shall permit an information flow if all of the following rules hold:

- The packet does belong to a protocol that is supported by the TOE, and
- the protocol is one of those allowed to pass through the TOE from the receiving to the sending interface, and
- the IP source and destination address are defined as being allowed to use the protocol, and
- the protocol specific filter rules do not deny the information to flow.

The TSF shall explicitly deny an information flow if any of the following rules applies:

- packets that are invalid fragments
- packets which cannot be reassembled completely
- packets where the source address of the packet is equal to the address of the network interface where the packet was received
- packets where the source address of the packet does not belong to the networks associated with the network interface where the packet was received
- packets where the source address of the packet is defined as being a broadcast address as specified in RFC 919 and RFC 922 for IPv4
- packets where the source address of the packet is defined as being a multicast address as specified in RFC 5771 for IPv4, and RFC 4291 for IPv6
- packets where the source address of the packet is defined as being a loopback address as specified in RFC 5735 for IPv4, and RFC 4291 for IPv6
- packets where the source or destination address of the packet is a link-local address as specified in RFC 3927 for IPv4, or link-/site-local address as specified in RFC 4291 for IPv6

- packets where the source or destination address of the packet is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4
- packets where the source or destination address of the packet is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6
- packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified
- the packet is part of an information flow that is denied by an SPF rule

Application note: The security attributes “protocol (…): header information” and “protocol (…): payload content” are to be repeated for each additional (2nd etc.) protocol that is supported with deep packet inspection.

6.1.3 ADMINISTRATOR ACCESS SFP

The TOE will implement the access control policy ADMINISTRATOR ACCESS SFP. The TSF shall enforce identification and authentication of remote administrators and operators before giving any administrative access to the TOE (i.e., giving any access to TSF management functions and TSF data).

6.2 Security Functional Requirements

This chapter specifies the security functional requirements for the TOE. If the FPP mandates a specific option that cannot be specified as part of the SFR or SAR, the PP marks it as “ST author note”. The ST author must apply this note when writing an ST and claiming conformance with this PP.

Notes marked as “Application note” are informative to support the understanding of the SFR or SAR.

The following styles of marking operations are applied with this Protection Profile:

- Any assignment, selection and refinements performed are marked as bold.
- Any requirements on assignments and selections operations are shown where the assignment and selection element is marked as italics, following the convention used by CC Part 2.

6.2.1 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) All administrative actions
d) Self test (automatic or administrator initiated)

e) **Trusted update**

f) **[assignment: *other specifically defined auditable events*].**

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST: **none**

Application note: If the TOE provides security functionality specified in the ST in addition to the ones specified in this PP, additional events have to be added. E.g., this would be the case if local authentication is added as a security function.

6.2.2 FAU_SEL.1 – Selective audit

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

a) [selection: *object identity, user identity, subject identity, host identity, event type*]

b) [assignment: *list of additional attributes that audit selectivity is based upon*]

Application note: This is to allow the administrator to adjust the events to be audited to the information flow control policy, the risk level and to the capacity of the audit review and analysis.

6.2.3 FCS_COP.1 {ADMIN} – Cryptographic Operation

FCS_COP.1.1 {ADMIN} The TSF shall perform **signature verification** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes **of at least 2048 bit** that meet the following: **RSA [PKCS1v2.1] and [selection: *SHA-224, SHA-256, SHA-384, SHA-512*] [FIPS180-4].**

Application note: This SFR specifies the cryptographic operation that is used to verify the X.509 certificate of the remote administrator.

6.2.4 FCS_COP.1 {UPDATE} – Cryptographic Operation

FCS_COP.1.1 {UPDATE} The TSF shall perform **signature verification** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes **of at least 2048 bit** that meet the following: **RSA [PKCS1v2.1] and [selection: *SHA-224, SHA-256, SHA-384, SHA-512*] [FIPS180-4].**

Application note: This SFR specifies the cryptographic operation that is used to verify the X.509 certificate of a TOE update.

6.2.5 FDP_ACC.2 – Complete access control

FDP_ACC.2.1 The TSF shall enforce the **ADMINISTRATOR ACCESS SFP** on **the subjects:**

- **remote administrators**

and objects:

- **management functions of the TSF**
- **configuration data of the TSF**
- **[assignment: *list of additional TSF data*]**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.6 FDP_ACF.1 – Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **ADMINISTRATOR ACCESS SFP** to objects based on the following:

subject remote administrator:

- **X.509 certificate**
- **Common Name (CN) of the certificate**

objects management function and TSF data:

- **none.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **If the CN of the subject's certificate is part of a list managed by the TOE that allows it to connect as a client to the TOE, then the subject is allowed access to resources on the TOE.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **If the client certificate is not signed with a public key of a certification authority trusted by the TOE, access is denied.**

6.2.7 FDP_IFC.2 {FPP} – Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the **[selection: *FIREWALL Information Flow Control SFP {SPF}, FIREWALL Information Flow Control SFP {DPI}*]** on

a) **subjects: packet filter;**
b) **information: packet of a supported protocol sent through the TOE from one external IT entity to another**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

ST author note: The information flow control SFP referred to above ({SPF}, {DPI}) must be the one that has been selected for this ST. It is permissible to select both, in which case this SFR must be iterated as "FDP_IFC.2 {SPF}" and "FDP_IFC.2 {DPI}".

ST author note: The subject "packet filter" refers to the active entity inside

the TOE that performs the SPF or DPI functionality. The ST author may want to refine this into the actual subsystem/module name of the specific TOE.

ST author note: The SFR is marked as {FPP} to avoid naming issues with Extended Packages for this PP, which also contain such an SFR. If no such package is claimed, the ST author may remove this postfix.

6.2.8 FDP_IFF.1 {SPF} – Simple security attributes

FDP_IFF.1.1 {SPF} The TSF shall enforce the **FIREWALL Information Flow Control SFP {SPF}** based on the following types of subject and information security attributes:

a) subject packet filter, with security attributes:
- **[selection: [assignment*: additional subject security attributes*], *none*]**

b) object network packet of a supported protocol, with security attributes:
- **presumed source IP address;**
- **presumed destination IP address;**
- **protocol [assignment: *protocol name*]: flow ID;**
- **TOE interface on which traffic arrives;**
- **TOE interface on which the packet is intended to leave, after a routing decision (if applicable);**
- **service (protocol and port, if applicable);**
- **[assignment: *additional information security attributes*].**

FDP_IFF.1.2 {SPF} The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
- **the packet is part of the protocol IPv4, IPv6, TCP, UDP or ICMP; and**
- **the protocol is one of those allowed to pass through the TOE from the receiving to the sending interface; and**
- **the IP source and destination address are defined as being allowed to use the protocol; and**
- **the packet is the flow establishing packet, and all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from [select: *some; all*] possible combinations of the values of the information flow security attributes, created by the authorized administrator; and**
- **the packet is part of an information flow that is allowed by an SPF rule, and the state has been previously established and this is not the flow establishing packet; and**
- **[selection: [assignment: *other default rules enforced by the TOE*], no other rules].**

FDP_IFF.1.3 {SPF} The TSF shall enforce the **following additional information flow control rules:**
- **The TSF shall reject and be capable of logging**

packets that are not affected by the rules stated in FDP_IFF.1.2 {SPF} and FDP_IFF.1.5 {SPF}; and

- **[selection: [assignment: *additional information flow control rules*], *no other rules*].**

FDP_IFF.1.4 {SPF} The TSF shall explicitly authorise an information flow based on the following rules: **no explicit authorisation rules**.

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

- **The TSF shall reject and be capable of logging packets which are invalid fragments.**
- **The TSF shall reject and be capable of logging fragmented packets which cannot be re-assembled completely.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is equal to the address of the network interface where the packet was received.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet does not belong to the networks associated with the network interface where the packet was received.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is defined as being a broadcast address as specified in RFC 919 and RFC 922 for IPv4.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is defined as being a multicast address as specified in RFC 5771 for IPv4, and RFC 4291 for IPv6.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is defined as being a loopback address as specified in RFC 5735 for IPv4, and RFC 4291 for IPv6.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the network packet is a link-local address as specified in RFC 3927 for IPv4, or link-/site-local address as specified in RFC 4291 for IPv6.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the packet is defined as an "unspecified address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6.**
- **The TSF shall reject and be capable of logging packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route**

specified.

- **The TSF shall reject and be capable of logging packets that are received in a wrong context, e.g., when an IP packet is not part of a valid TCP session.**
- **The TSF shall reject and be capable of logging packets that are part of an information flow that is denied by an SPF rule.**
- **The TSF shall reject and be capable of logging packets that are part of an information flow but not the state establishing packet, and the state is currently not or no longer active.**
- **[assignment: *additional information flow control rules*]**

ST author note: The item "protocol (...): flow ID" should be repeated for each additional protocol that is supported by the SPF. The unique identification of an information flow is required for stateful inspection of the flow, i.e., to logically group otherwise separate packets. It is dependent on the protocol used. The term "flow ID" is used as a placeholder for such state information. The ST author is not required, but may want to specify in the ST (using a refinement) how the flow handle is identified for a specific protocol and TOE.

Application note: The term "presumed IP address" refers to the IP address information provided in network packets. Due to the design of the IPv4/v6 protocol there is no guarantee that they indeed represent the claimed source/destination subject. I.e., it is trivial for an attacker outside of the TOE to replace them with different addresses. The TOE, as any other network device, has therefore to presume that they represent the correct subject.

Application note: Not all protocols include a "port" attribute (e.g., IPv4). The information security attribute "port" of a service is therefore only available where applicable to the specific protocol.

Application note: FDP_IFF.1.3 {SPF} requires a "default deny" policy. It is not required to log why no other rule was activated, but only that this default was applied.

6.2.9 FDP_IFF.1 {DPI} – Simple security attributes

FDP_IFF.1.1 {DPI} The TSF shall enforce **the FIREWALL Information Flow Control SFP {DPI}** based on the following types of subject and information security attributes:

a) subject packet filter, with security attributes:
- **[selection: [assignment: *additional subject security attributes*], none]**

b) object network packet of a supported protocol, with security attributes:
- **presumed source IP address;**
- **presumed destination IP address;**
- **TOE interface on which the packet arrived;**
- **TOE interface on which the packet is intended to leave, after a routing decision (if applicable);**
- **service (protocol and port, if applicable);**
- **protocol [assignment: *protocol name*]: header information;**
- **protocol [assignment: *protocol name*]:**

payload content;

- **[assignment: *additional information security attributes*].**

FDP_IFF.1.2 {DPI} The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **the packet is part of the protocol IPv4, IPv6, TCP, UDP or ICMP; and**
- **the protocol is one of those allowed to pass through the TOE from the receiving to the sending interface; and**
- **the IP source and destination address are defined as being allowed to use the protocol; and**
- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from [select: *some; all*] possible combinations of the values of the information flow security attributes, created by the authorized administrator; and**
- **the protocol specific filter rules do not deny the information to flow; and**
- **[selection: [assignment: *additional information flow control rules*], *no other rules*].**

FDP_IFF.1.3 {DPI} The TSF shall enforce the **following additional information flow control rules:**

- **[selection: [assignment: *additional information flow control rules*], *no other rules*].**

FDP_IFF.1.4 {DPI} The TSF shall explicitly authorise an information flow based on the following rules:

- **The packet is not denied by any rule stated in any of the claimed SFRs.**

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

- **The TSF shall reject and be capable of logging packets which are invalid fragments.**
- **The TSF shall reject and be capable of logging fragmented packets which cannot be re-assembled completely.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is equal to the address of the network interface where the network packet was received.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet does not belong to the networks associated with the network interface where the packet was received.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet is defined as being a broadcast address as specified in RFC 919 and RFC 922 for IPv4.**
- **The TSF shall reject and be capable of logging packets where the source address of the packet**

is defined as being a multicast address as specified in RFC 5771 for IPv4, and RFC 4291 for IPv6.

- **The TSF shall reject and be capable of logging packets where the source address of the packet is defined as being a loopback address as specified in RFC 5735 for IPv4, and RFC 4291 for IPv6.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the packet is a link-local address as specified in RFC 3927 for IPv4, or link-/site-local address as specified in RFC 4291 for IPv6.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4.**
- **The TSF shall reject and be capable of logging packets where the source or destination address of the packet is defined as an "unspecified address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6.**
- **The TSF shall reject and be capable of logging packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.**
- **The TSF shall reject and be capable of logging packets where the combination of information security attribute values in at least one information flow security policy rule denies the packet flow, and where such rules may be composed from [select: *some; all*] possible combinations of the values of the information flow security attributes, created by the authorized administrator.**
- **[assignment: *additional information flow control rules*].**

ST author note: The item "protocol (...): flow ID" should be repeated for each additional protocol that is supported by the SPF.

Application note: The term "presumed IP address" refers to the IP address information provided in network packets. Due to the design of the IPv4/v6 protocol there is no guarantee that they indeed represent the claimed source/destination subject. I.e., it is trivial for an attacker outside of the TOE to replace them with different addresses. The TOE, as any other network device, has therefore to presume that they represent the correct subject.

Application note: Not all protocols include a "port" attribute (e.g., IPv4). The information security attribute "port" of a service is therefore only available where applicable to the specific protocol.

Application note: FDP_IFF.1.4 {DPI} requires a "default allow" policy for packets, if no other SFR applies. Please note that e.g., FDP_IFF.1.3 {SPF}, if included in an ST, will override this {DPI} item, since it is an applicable SFR.

6.2.10 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes

belonging to individual users:

- **identity of the remote administrator in form of the Common Name (CN) of the client's certificate**
- **association of the remote administrator with a X.509 certificate.**

Application note: The administrator's certificate has to be signed by a trusted root CA. This root certificate is internal and provided in a trusted way to the TOE.

Application note: Only remote administrators have to be known to the TOE and identified and authenticated by the TOE. The TOE must not identify and authenticate local administrators. Local access is limited to the administrators by A.PHYSICAL, and the environment must provide measures to achieve accountability between these administrators (OE.LOCAL_ADMIN).

6.2.11 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.

Application note: The only users known to the TOE are administrators. Only remote administrators are required to authenticate since local access is limited to authorized persons (OE.PHYSICAL). In case of multiple local administrators, the environment must provide measures to achieve accountability between these administrators (OE.LOCAL_ADMIN).

6.2.12 FIA_UID.2 – User identification before any actions

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.

Application note: The only users known to the TOE are administrators. Only remote administrators are required to identify since local access is limited to authorized persons (OE.PHYSICAL). In case of multiple local administrators, the environment must provide measures to achieve accountability between these administrators (OE.LOCAL_ADMIN).

6.2.13 FMT_MOF.1 – Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour of** the functions **listed below** to **an administrator:**

- **change the configuration of the TOE**.

6.2.14 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **ADMINISTRATOR ACCESS SFP** to restrict the ability to **modify** the security attributes **consisting of possible configuration options** to **administrators**.

Application note: The TOE must also provide management functions both to administrators with remote access as well as to administrators with local access to the TOE. The restriction to locally modify security attributes must be enforced by the TOE environment (OE.PHYSICAL).

6.2.15 FMT_MSA.3 {ADMIN}– Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **ADMINISTRATOR ACCESS 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** to specify alternative initial values to override the default values when an object or information is created.

Application note: An administrator can restrict unauthenticated access and specify security relevant initial values by changing the rules in the configuration file.

6.2.16 FMT_MSA.3 {FILTER} – Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **[selection*: FIREWALL Information Flow Control SFP {SPF}, FIREWALL Information Flow Control SFP {DPI}, FIREWALL Information Flow Control SFP {SPF} and {DPI}*]** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

ST author note: The information flow control SFP selected to above ({SPF}, {DPI}, or both) must be the ones that have been selected for this ST.

6.2.17 FMT_MTD.1 – Management of TSF data (administrator)

FMT_MTD.1.1 The TSF shall restrict the ability to **query or modify** the **TSF data listed below** to **the administrator**:

- **version of the TOE (query)**
- **configuration files (query, modify)**
- **[assignment: *list of additional TSF data*]**

6.2.18 FMT_SMF.1 – Specification of management functions

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

- **query the software version**
- **apply changes to the configuration file**
- **restart the TOE**
- **initiate update of the TOE software**
- **[assignment: *additional actions to be taken*].**

Application note: The security management functions related to changes of the configuration of the TOE are described in more detail in FMT_MOF.1.

Application note: The TOE software update must only be possible after the authenticity of the software has been verified (using the services and the trust anchor of the TOE) and if the version number of the new software is higher or equal to the version of the installed software. It is only the software update function that will be covered by this PP, not the software update itself.

6.2.19 FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles**:**

- **administrator**

- **[assignment: *any other authorised identified roles*].**

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

Application note: Remote administrators are known to the TOE by remote authentication. For local administrators the TOE environment must ensure that only administrators have local access to the TOE (OE.PHYSICAL). For this reason local administrators may not be known to the TOE.

6.2.20 FPT_FLS.1 – Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **invalid configuration file**
- **failed integrity and version verification of software update**
- **[assignment: *list of additional types of failures in the TSF*].**

Application note: If the new configuration file is unreadable or does not conform to the syntax expected by the TOE then the previous configuration file will be kept and used.

Application note: In case the syntax of the configuration file may allow for certain insecure configurations which may result in insecure states, this may be addressed by this SFR. Such insecure states are considered an invalid configuration file.

Application note: A secure state may include shutting down the TOE.

6.2.21 FPT_TST.1 – TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up [selection: *and periodically during normal operation, and at the request of the authorised user, and at the conditions [assignment: conditions under which self test should occur]*]** to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].

ST author note: During start-up the self-test has to be performed. Additional conditions for performing self-tests may be considered, for example after an update has been performed, and at the request of the administrator. In such a case the rationale below must be updated accordingly.

6.2.22 FPT_TUD_EXT.1 – Trusted updates

FPT_TUD_EXT.1.1 The TSF shall provide administrators the ability to query the current version of the TOE software.

FPT_TUD_EXT.1.2 The TSF shall provide administrators the ability to update the TOE software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify software updates to the TOE using a **digital signature mechanism** prior to

installing those updates.

FPT_TUD_EXT.1.4	The TSF shall provide a means to verify software updates to the TOE to ensure that the software update version is newer than the current version of the TOE prior to installing those updates.

Application note: The term "current version of the TOE" shall be interpreted as the currently executing (i.e., active) TOE code.

Application note: Trusted update is an administrator controlled mechanism. The TOE may also be updated outside of the control of the TSF by authorized persons with physical access to the TOE (relying on OE.PHYSICAL).

ST author note: It is permissible to add "automated updates" as an additional TOE functionality. All ST chapters must be updated consistently in this case.

6.2.23 FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall **never** initiate communication via the trusted channel.

Application note: The "other trusted IT product" referred to above is to be interpreted as the administration client.

ST author note: The administration client may be a user client such as a web browser or a management server from which the firewall administration is performed. For this reason the SFR does not prescribe whether the trusted channel is a TLS connection, IPsec connection or is relying on any other protocol for the trusted channel.

ST author note: The ST author must add an application note to this SFR, describing how the TOE provides this trusted channel (e.g., IPsec). The ST author also must perform the necessary additions to the ST in order to specify this functionality. I.e., if it is implemented in the TSF then FCS_COP/FCS_CKM or other SFRs may be required. If functionality in the environment is used, additional requirements in chapter 1 and 3 might be required.

6.3 Security functional requirements rationale

This section provides the rationale for the internal consistency and completeness of the security functional requirements.

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective and that each security objective is addressed by at least one SFR.

	FAU_GEN.1	FAU_SEL.1	FCS_COP.1 {ADMIN}	FCS_COP.1 {UPDATE}	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2 {FPP}	FDP_IFF.1 {SPF}/{DPI}	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3 {ADMIN}	FMT_MSA.3 {FILTER}	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TUD_EXT.1	FTP_ITC.1
O.MEDIATE							X	X														
O.AUDIT	X	X																				
O.MANAGE													X				X	X				
O.RESTRICT					X	X						X				X						
O.REMOTE			X						X	X	X							X				X
O.INITIAL														X	X							
O.PROTECT																			X	X		
O.UPDATE				X													X				X	

6.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Objective	Security functions
O.MEDIATE	*The TOE must mediate the flow of all information flowing between the internal and external network interfaces of the TOE.* This objective is satisfied by requiring a firewall security policy to control the information flow (FDP_IFC.2 {FPP} and FDP_IFF.1 {SPF} or {DPI}) requiring that the policy is applied to all traffic between the internal and external interfaces.
O.AUDIT	*The TOE must be able to provide an audit trail of security relevant events and of authorized use of security functions, and allow an authorized administrator to configure additional security relevant events that are to be audited.* This objective is satisfied by requiring that audit records can be generated for security-relevant events (FAU_GEN.1) and that these records have an accurate time stamp (OE.TIME). The administrator shall also be able to select the events to be audited (FAU_SEL.1).
O.MANAGE	*The TOE must provide the means for an authorized administrator to configure and manage the TOE security functions.* This objective is satisfied by requiring there to be security management functions for the administrators (FMT_SMF.1 and FMT_SMR.1) Only authorized administrators are allowed to modify the configuration options (FMT_MSA.1).

O.RESTRICT	*The TOE must restrict the means for configuration and control of the TOE to authorized administrators.* This objective is achieved by requiring that the ability to restart the TOE and to change the configuration is restricted to administrators (FMT_MOF.1) and the management of TSF data is restricted to administrators (FMT_MTD.1). The access is restricted by the ADMINISTRATOR access control SFRs (FDP_ACC.2 and FDP_ACF.1).
O.REMOTE	*The TOE must uniquely identify and authenticate the identity of all remote administrators and provide them with a secure communication channel before allowing remote administrators any access to the TOE.* This objective is achieved by requiring administrators (FMT_SMR.1) to identify (FIA_UID.2) and authenticate (FIA_UAU.2) before any action. Identification and authentication is certificate based using a X.509 certificate (FIA_ATD.1, FCS_COP.1 {ADMIN}), thus providing the administrator with a trusted channel (FTP_ITC.1) for administration.
O.INITIAL	*Upon initial start-up of the TOE or during configuration, the TOE shall provide well-defined initial settings for security relevant functions.* This objective is achieved by requiring that static attributes provides restrictive default values, although the administrator may override certain default values. Authorized administrators are allowed to modify the default configuration options (FMT_MSA.3 {ADMIN}) for the administrative access. The filter functionality uses restrictive default settings which cannot be modified (FMT_MSA.3 {FILTER}).
O.PROTECT	*The TOE must protect itself against attempts by attackers to bypass, deactivate or tamper with TOE security functions.* This objective is achieved by requiring that the TSF shall preserve a secure state (FPT_FLS.1) in case of an invalid configuration file or in case of failure of the integrity and version verification of software update tests (FPT_TST.1).
O.UPDATE	*The TOE must only accept updates that are newer than the currently running version and where the origin and integrity of the update can be trusted.* This objective is achieved by requiring that trusted updates must be initiated by administrators (FPT_TUD_EXT.1 and FMT_SMF.1). The integrity of the updates must be verified and the version of the update must be newer (FPT_TUD_EXT.1). The verification of the integrity and authenticity must be signature based (FCS_COP.1 {UPDATE}) relying on the time stamp for the certificate validation (OE.TIME).

6.4 Dependencies between security functional requirements

SFR	Dependencies	Note
FAU_GEN.1	FPT_STM.1	Not resolved, addressed by OE.TIME.
FAU_SEL.1	FAU_GEN.1	Resolved

	FMT_MTD.1	Resolved
FCS_COP.1 {ADMIN}	FDP_ITC.1 or FDP_ITC.2	Not resolved. It is assumed that verifying the certificate key is part of the initial installation.
	FCS_CKM.1	
	FCS_CKM.4	Not resolved. There is no need to destroy a public key.
FCS_COP.1 {UPDATE}	FDP_ITC.1 or FDP_ITC.2	Not resolved. It is assumed that verifying the certificate key is part of the initial installation.
	FCS_CKM.1	
	FCS_CKM.4	Not resolved. There is no need to destroy a public key.
FDP_ACC.2	FDP_ACF.1	Resolved
FDP_AFC.1	FDP_ACC.1	Resolved by FDP_ACC.2
	FMT_MSA.3	Resolved by FMT_MSA.3 {ADMIN}.
FDP_IFC.2 {FPP}	FDP_IFF.1	Resolved
FDP_IFF.1 {SPF}/{DPI}	FDP_IFC.1	Resolved by FDP_IFC.2 {FPP}
	FMT_MSA.3	Resolved by FMT_MSA.3 {FILTER}.
FIA_ATD.1	None	-
FIA_UAU.2	FIA_UID.1	Resolved by FIA_UID.2
FIA_UID.2	None	-
FMT_MOF.1	FMT_SMR.1	Resolved
	FMT_SMF.1	Resolved
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Resolved by FDP_ACC.2
	FMT_SMR.1	Resolved
	FMT_SMF.1	Resolved
FMT_MSA.3 {ADMIN}	FMT_MSA.1	Resolved
	FMT_SMR.1	Resolved
FMT_MSA.3 {FILTER}	FMT_MSA.1	Not resolved. The default values cannot be modified.
	FMT_SMR.1	Not resolved. The default values cannot be modified.
FMT_MTD.1	FMT_SMR.1	Resolved
	FMT_SMF.1	Resolved
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Resolved by FIA_UID.2
FPT_FLS.1	None	-
FPT_TST.1	None	-
FPT_TUD_EXT.1	FCS_COP.1	Resolved by FCS_COP.1 {UPDATE}

6.5 Security Assurance Requirements

The assurance requirements are the EAL2 package augmented with ALC_FLR.1.

6.5.1 Security assurance requirements rationale

The assurance package EAL2 has been augmented with ALC_FLR.1. EAL2 is applicable in those circumstances where users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

The assurance level EAL2 augmented with ALC_FLR.1 has been chosen as the minimum requirement for a network device separating an internal network from an external (public) network. It provides a basic vulnerability analysis (in addition to the search of the public domain). The augmentation ALC_FLR.1 (basic flaw remediation) has been made to ensure that basic flaw remediation is in place. It is a natural extension considering the extended SFR for trusted updates (FPT_TUD_EXT.1).

All dependencies within the assurance package EAL2 have been resolved. The augmentation ALC_FLR.1 does not introduce any dependencies to components not already present in EAL2.