DCSSI
Direction Centrale de la Sécurité des Systèmes d'Information

Protection Profile - Personal Firewall (PP-PFP)

Publication date	**:**	14 May 2008
Reference	**:**	PP-PFP
Version	**:**	1.7

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/01.

Table of contents

List of tables

List of figures

1 Introduction

1.1 Protection profile reference

Title: Protection Profile – Personal Firewall

Reference: PP-PFP, Version 1.7, 14 May 2008

Author: Fidens

1.2 Context

This PP has been drawn up under the aegis of the *Direction Centrale de la Sécurité des Systèmes d'Information* (DCSSI).

The aim is to provide an administration framework for the certification of personal firewalls to meet the requirements of the public and private sectors with a view to their qualification.

1.3 General overview of the Target of Evaluation (TOE)

Note: a detailed description of the TOE can be found in Appendix A .

1.3.1 TOE type

This protection profile presents the security objectives and the functional and assurance requirements for a personal firewall (the TOE).

This personal firewall is a software component installed on a workstation for the purpose of filtering that workstation's incoming and outgoing network data flows.

1.3.2 Usage and major security features of the TOE

The main purpose of the personal firewall is to analyse and filter data flows entering and leaving a workstation in order to protect it from:

- The transmission of the workstation's local data to the exterior without the basic user's knowledge (via Trojan horses, spyware, etc.)
- The transmission of the workstation's local data to the exterior via services unauthorised by the organisation's security policy
- Attacks emanating from the network: illegal remote use of local resources, remote corruption or destruction of local data and saturation of the station's local resources (denial of service type attacks)

An administration component of the PFP serves to define the filtering policy and the access rights relating to this policy. Administrative tasks may be carried out by an administrator, by a basic user or by both. It can be undertaken locally, at the workstation, or remotely from an

administration centre.

A logging and monitoring component enables the operations relating to the operation and administration of the personal firewall to be logged and alarms to be issued should the security policy be violated. It also makes it possible to log network flows processed by the personal firewall. Monitoring can take place locally, at the workstation, or remotely from a monitoring centre.

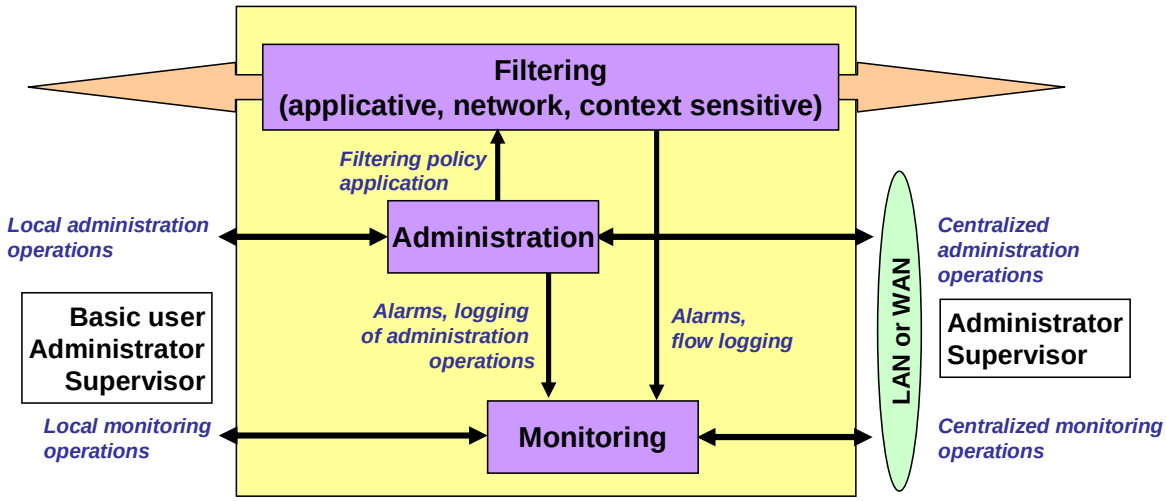

Figure 1: overview of the TOE

1.3.3 Specific conditions and security specificities of the TOE

This communication filtering component can, as a minimum, perform application filtering and network filtering. Application filtering is associated with a control function for the integrity of applications with access to the network. Network filtering takes into account the notion of contextual or behavioural filtering[1].

This personal firewall is intended to be installed and used on a fixed or portable workstation. A portable workstation may be used inside or outside company premises. The security policy implemented takes into account this network environment.

The workstation can be multi-user. The personal firewall makes it possible to adapt the security policy according to the basic user of the workstation. The basic user can be an administrator or a privileged workstation user[2].

In some organisations, the personal firewall shall have the capacity to operate in a transparent manner for the basic user.

[1] Contextual or behavioural filtering is understood to mean the ability of the TOE to filter a packet according to packets already received or issued.

[2] This protection profile distinguishes between “basic user”, a term describing a person whose main role is to use the workstation, and “user”, a term describing a person whose role can be that of a basic user, an administrator or a supervisor with or without privileges (i.e. a “root” account under Unix or equivalent under Windows).

1.3.4 Hardware and software environment

In order to operate, the TOE depends greatly on the operating system used at the workstation in need of protection.

This operating system must make it possible to identify workstation users and contribute to the protection of the TOE and its data in relation to these users.

The workstation must have at least one network interface and associated software.

2 Conformance claims

2.1 Conformance of this protection profile

2.1.1 Conformance with the Common Criteria

This protection profile complies with:

- Part 2 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [CC2])
- Part 3 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [CC3])

No recourse has been made to extension or interpretation.

2.1.2 Conformance with an assurance package

The level of assurance targeted by this protection profile is EAL3, augmented by the following components:

- ALC_FLR.3
- AVA_VAN.3

This level of security assurance complies with the DCSSI reference document “Processus de qualification d’un produit de sécurité – Niveau standard” (see [QUALIF_STD]).

2.1.3 Conformance with a protection profile

This protection profile is not dependent on any other protection profile.

2.2 Conformance of security targets and protection profiles

This PP requires “**demonstrable”** conformance of the PP or ST claiming conformance to this PP.

The “demonstrable” conformity level allows:

- conformity with several protection profiles to be announced
- the specification of a higher assurance package
- the specification of alternative security functional requirements
- a security objective for the operational environment to be transformed into a security objective for the TOE
- PP operations to be modified provided that they are more restrictive

Application notes detail which assumptions can be partially or completely transformed into an OSP by the STs and PPs in conformity with this PP. These application notes are shown for the assumptions concerned.

3 Security problem definition

3.1 Assets

The TOE provides services intended to protect the workstation against the untimely transmission of local data (attacks by Trojan horses, KeyLoggers, backdoor viruses, etc.), against the remote use of local resources (CPU time of the machine, ping attacks, etc.) and against the remote destruction or corruption of local data (Trojan horse type of attack, viral application spoofing, direct remote access to static resources - file systems - of the workstation).

The TOE protects these assets via:

- the analysis and filtering of all incoming and outgoing communications and connections (on local and remote networks) at the workstation
- the control of the integrity of the “communicating” applications at the workstation on which it is installed

3.1.1 Assets in the operational environment

3.1.1.1 Sensitive assets protected by the TOE

The assets protected by the TOE are:

D_data	Data stored on the workstation
D_appli	Applications installed or that can be used on the workstation
D_services	Workstation services and logical resources

D_data

This asset corresponds to data stored on the workstation in files or databases. Such data may be user data, configuration data or parameters for applications. This data may be accessed from the exterior and corrupted or made unavailable. It may be exported illegally by a Trojan horse.

Sensitivity: confidentiality, integrity, availability

D_appli

This asset corresponds to applications, programs and libraries of programs installed on the workstation and used by basic users. These applications may be made unavailable, corrupted (insertion of Trojan horses) or contain spy programs (spyware).

Sensitivity: integrity, availability

D_services

Workstation services or logical resources can be protected by the TOE. This is notably the

case for workstation resources that could become saturated by repeated external access (denial of service type attacks).

Sensitivity: availability

3.1.1.2 Sensitive assets of the TOE

The sensitive assets of the TOE are:

D_software	The TOE itself as a software program
D_flow_filter	Filtering rule for the flow of incoming and outgoing communications
D_appli_filter	Filtering rule for applications wanting to gain network access
D_config	TOE configuration parameters
D_AC_param	Control parameters for local or remote access to the TOE
D_flow_audit	Logged data relative to the communication activity of the workstation (network flows)
D_admin_audit	Logged data relative to the administration, monitoring and operation of the TOE: start-up, shutdown, modification of rules, alert levels or configuration parameters, etc.
D_alarm	Alerts generated upon the detection of attempted attacks

D_software

This sensitive asset corresponds to all TOE programs. These programs are held in memory and used on the workstation.

Sensitivity: integrity, availability

D_flow_filter

A flow filtering rule defines how the workstation's incoming and outgoing flows are to be processed in order to determine whether or not these flows are authorised. These flows are flows transmitted by the TCP/IP protocol stack[3].

These rules are held in memory on the workstation and can be modified by administrators and possibly by basic users.

Sensitivity: confidentiality, integrity

D_appli_filter

An applications filtering rule determines how to process external connection requests made by workstation applications. Its purpose is to avoid communication outside the workstation with Trojan horse type software programs. It includes controlling the integrity of applications to avoid spoofing of an authorised software program by a malicious software program and the control of communications requested by the application.

These rules are held in memory on the workstation and can be modified by administrators and possibly by basic users.

Sensitivity: confidentiality, integrity

[3] STs in conformity with this PP must specify the proprietary or non-IP protocols covered.

D_config

Among others, configuration parameters of the TOE include:

- the general configuration of the TOE
- parameters relating to logging and monitoring: the level of logs produced by the TOE, the frequency at which information is transmitted, the level of alerts to be sent and the frequency and address of the server for updates
- parameters relating to the administration policy

These parameters are stored locally and can be modified locally (through the MMI of the TOE) or remotely (via the remote administration interface).

Sensitivity: integrity

D_AC_param

Control parameters for local and remote access to the TOE include data used for controlling TOE access. This data may notably include:

- user[4] authentication data (basic users, administrators and supervisors) for local access to the TOE interface
- centralised monitoring and administration authentication data
- centralised monitoring and administration connection data (server address, security data exchange protocol)
- the level of TOE visibility (impossible or partial local access to the TOE interface)

These parameters are stored locally and can be modified locally (through the MMI of the TOE) or remotely (via the remote administration interface).

Sensitivity: confidentiality, integrity

D_flow_audit

The TOE supplies monitoring data (connection data, connected addresses, connection information concerning the various flows), which may only be used partially since the transmission of such data can generate considerable traffic.

This data is stored and used locally or transmitted to a monitoring entity.

Sensitivity: confidentiality, integrity

D_admin_audit

The TOE logs its own operational (start-up, shutdown) and administration data (modification of rules or parameters).

These data are stored and used locally or transmitted to a monitoring entity.

Sensitivity: confidentiality, integrity

D_alarm

The TOE generates alerts that are systematically logged locally; their transmission to the monitoring centre can be configured according to severity.

A mechanism exists to guarantee the delayed transmission of these alerts to ensure their

[4] Defined in section 3.2 of this PP.

coherent use; this is also true for portable workstations that are connected to the administration centre in an occasional way.

Sensitivity: integrity, availability

Application note: publishers of personal firewalls who wish to protect the alerts in confidentiality must specify it in the STs in conformity with this PP.

3.1.1.3 Summary table

The following table summarises the security needs of the various identified sensitive assets:

	Confidentiality	Integrity	Availability
D_data	X	X	X
D_appli		X	X
D_services			X
D_software		X	X
D_flow_filter	X	X	
D_appli_filter	X	X	
D_config		X	
D_AC_param	X	X	
D_flow_audit	X	X	
D_admin_audit	X	X	
D_alarm		X	X

Table 1: Sensitivity of the various assets

3.2 Users

The following individuals and software programs have access to the TOE:

U_local_program	Workstation programs interacting with the TOE
U_remote_program	Programs located on remote systems interacting with the TOE across the network
U_administrator	Administrators in charge of the TOE
U_supervisor	Supervisors in charge of the TOE
U_basic_user	Basic users of the workstation

U_local_program

Programs installed on the workstation hosting the TOE that communicate with the exterior via the TOE.

U_remote_program

Programs located on remote systems that interact via the network with either the TOE for monitoring or administrative needs, or with the local workstation via the TOE for application needs.

U_administrator

The administrator in charge of the TOE is responsible for the definition and the administration of TOE filtering rules relative to the policy defined by the security officer[5]. Tasks can be performed via local or remote access.

These users are described as "administrators" in the remainder of this PP.

U_supervisor

The supervisor in charge of the TOE controls and audits the application by the TOE of the filtering policy defined for workstations by means of alerts and TOE data logs. The supervisor manages alerts sent by the TOE, and monitors and analyses security events logged by the TOE. Tasks can be performed via local or remote access.

These users are described as "supervisors" in the remainder of this PP.

U_basic_user

The basic user uses the workstation on which the TOE is installed in a single or multi-user context. According to the policy defined and authorised by the security officer, the basic user may:

- Either be responsible for TOE administration, alone or in collaboration with an administrator, or on the contrary have no administrative responsibilities whatsoever
- Either be responsible for TOE monitoring, alone or in collaboration with a supervisor, or on the contrary have no monitoring responsibilities whatsoever

The basic user may be an administrator or a privileged user (i.e. with a "root" account under Unix or an equivalent account under Windows) of the workstation.

3.3 Threats

Typology and threats origin

Threats may occur as a result of:

1. The malfunction of the TOE or of the TOE environment (workstation, network, etc.).
2. A non-privileged basic user of the workstation hosting the TOE preventing the correct operation of the TOE either with malicious intent (fraudulent use, abuse of consented rights), or by mistake (negligence, oversight, ignorance).
3. A privileged user or administrator of the workstation hosting the TOE preventing the correct operation of the TOE by mistake (negligence, oversight).
4. An administrator or supervisor preventing the correct operation of the TOE by mistake (negligence, oversight).
5. Individuals with access to the network to which the workstation is connected acting in a malicious manner, abusing consented rights or making mistakes. In particular, these individuals might:
    - Try to gain access to the workstation or disrupt its operation
    - Intercept or tamper with (modify, delete, disrupt, reroute) communications (administration, monitoring or alarm data) between this workstation and other equipments

[5] The notion of security officer is defined in section A.4 of this PP.

Attack potential

Individuals performing attacks have a **basic** attack potential. They correspond to malicious persons possessing the computing skills of a well-informed user.

Threats not included

In this PP, the following are not considered as being threats to the TOE in operation:

1. Physical disaster, natural events, the loss of basic services and disturbance caused as a result of radiation.
2. Threats occurring as a result of the intentional acts of administrators or supervisors. These are not considered hostile.
3. Threats occurring as a result of the intentional acts of workstation administrators or privileged users. These are not considered hostile.

3.3.1 Threats relative to the TOE in operation

Note: the figures in brackets correspond to the numbering system used by the [EBIOS] method.

T_eavesdropping (19)

An attacker uses the network on which the workstation hosting the TOE is connected to find out what data is being exchanged between the TOE and an administration or monitoring centre.

Assets concerned: D_flow_filter, D_appli_filter, D_AC_param, D_flow_audit, D_alarm.

This threat is considered high risk. The threat is remembered.

T_disclosure (23)

An attacker gains access to confidential sensitive TOE assets and uses them to violate the security policy implemented by the TOE.

Assets concerned: D_AC_param, D_flow_filter, D_appli_filter, D_flow_audit.

This threat is considered high risk. The threat is remembered.

T_spoofing (24)

An attacker transmits information to the TOE by assuming the identity of an administration or monitoring centre.

An attacker transmits information to an administration or monitoring centre by assuming the identity of the TOE.

Assets concerned: D_data, D_appli, D_services, D_software, D_flow_filter, D_appli_filter, D_config, D_AC_param, D_flow_audit, D_admin_audit, D_alarm.

This threat is considered high risk. The threat is remembered.

T_software_trapping (26)

A malicious individual with access to the workstation modifies the software to disable or modify one of its functions.

Assets concerned: D_software, D_services.

This threat is considered high risk, but a high attack potential is required for it to be feasible. This threat is however selected.

T_flooding (30)

Repeated, logged attacks resulting in log file saturation. These attacks may be deliberate or linked to the malfunctioning of a software program; they may occur locally or emanate from the network.

Assets concerned: D_flow_audit, D_admin_audit.

Repeated attacks resulting in the saturation of a TOE service. These attacks may be deliberate or linked to the malfunctioning of a software program; they may occur locally or emanate from the network.

Assets concerned: D_services.

This threat is considered high risk. The threat is remembered.

T_malfunction (31)

A TOE malfunction prevents necessary security functions being performed in relation to the workstation and users (basic users, administrators and supervisors).

This malfunction can block the TOE, and prevent access to workstation services.

Assets concerned: D_services.

This malfunction can also result in the TOE being unable to control access to administration and monitoring functions, or to control network and application flows. In this case, the confidentiality, integrity and availability of TOE sensitive assets and of the workstation may be violated.

Assets concerned: D_data, D_appli, D_services, D_software, D_flow_filter, D_appli_filter, D_config, D_AC_param, D_flow_audit, D_admin_audit, D_alarm.

This threat is considered high risk. The threat is remembered.

T_data_alteration (36)

An attacker corrupts (modification, deletion or insertion) sensitive TOE assets on the workstation hosting the TOE or assets protected by the TOE.

An attacker corrupts (modification, deletion or insertion) administration or monitoring data during its transmission between the workstation hosting the TOE and a remote site.

This attacker may be a local user of the workstation, for example, or a person with remote access to data held in the workstation's memory or exchanged between the workstation and a remote site.

Assets concerned: D_data, D_appli, D_services, D_software, D_flow_filter, D_appli_filter, D_config, D_AC_param, D_flow_audit, D_admin_audit, D_alarm.

This threat is considered high risk. The threat is remembered.

T_illicit_processing (37)

An attacker retrieves data containing information of a personal nature and uses it in a malicious manner.

This attacker may, for example, be a basic user of a multi-user workstation authorised to

access logs.

This may also occur during the reuse of a workstation on which the firewall is installed.

Assets concerned: D_flow_audit.

This threat is considered high risk. The threat is remembered.

T_error (38)

A basic user or an administrator makes an administrative error (data modification) and causes a TOE malfunction or corrupts the filtering policy.

Assets concerned: D_flow_filter, D_appli_filter, D_config, D_AC_param, D_services.

This threat is considered high risk. The threat is remembered.

T_abuse (39)

A user intentionally disables a TOE function resulting in the violation of the security policy.

Assets concerned: D_config, D_AC_param.

This threat is considered high risk. The threat is remembered.

T_filter_inhibition (39, 40)

A malicious program or user disables, possibly unobtrusively, the filtering functions of the TOE thereby leaving the workstation unprotected and open to illegal connections

Assets concerned: D_flow_filter, D_appli_filter.

This threat is considered high risk. The threat is remembered.

T_usurpation (40)

An unauthorised person gains access to the TOE or to TOE functions to which it does not normally have access and uses them to modify the security policy.

Examples: a basic user gaining access to functions reserved for the administrator or supervisor, or a person gaining access to an administration interface of the TOE left unsupervised.

An attacker may become aware of the TOE filtering rules and therefore be able to violate the security policy implemented by the TOE.

Attacker: a workstation user or a person with remote access to data held in the workstation memory.

Assets concerned: D_flow_filter, D_appli_filter, D_config, D_AC_param.

This threat is considered high risk. The threat is remembered.

T_denial (41)

A user uses his administration rights to modify the TOE security policy or to prevent the correct operation of the TEO and then denies having made these modifications.

Assets concerned: D_flow_filter, D_appli_filter.

This threat is considered high risk. The threat is remembered.

3.4 Organisational security policies (OSP)

3.4.1 Policies relative to the services provided

OSP_filtering

The TOE shall implement a mechanism, based on the filtering rules, to control network access. It shall make it possible to define several filtering levels. These filtering rules shall take into account the workstation network environment, and connections, users and applications criteria. The TOE shall also provide for contextual filtering.

OSP_application_integrity

The TOE shall make it possible to control the integrity of applications seeking access to the network, and to detect and specify applications that have been modified.

OSP_roles

The TOE shall distinguish at the very least between administrator, supervisor and basic user roles. It shall make it possible to track actions performed by the holders of these roles.

OSP_admin

The TOE shall allow to administer its configuration, locally or by remote, and the filtering rules. All filtering rules shall be visible. Access to the administration module and use of administration functions shall be monitored.

OSP_monitoring

The TOE shall provide local or remote monitoring of TOE operations. Access to the monitoring module and use of monitoring functions shall be controlled. Only the supervisor shall be authorised to consult and clear logs; no user shall have the right to modify logs.

OSP_admin_audit

The TOE shall log administrative actions that modify the configuration of the TOE. It shall make it possible to select, sort and view this data according to various criteria (date, user, etc.).

OSP_flow_audit

The TOE shall be able to log the flows it processes within the scope of the security policy. It shall make it possible to select, sort and view this data according to various criteria (time stamping, user, network address, application, protocol, flow acceptance or rejection, etc.).

OSP_sec_pol_violation_detection

The TOE shall make it possible, as far as this is possible, to detect attempts made to violate the security policy and signal any such attempts by issuing an alarm.

OSP_trusted_configuration

It shall be possible to reinstall and reconfigure the TOE to ensure the availability of a trusted TOE on the workstation.

3.4.2 Policies taken from applicable regulations

OSP_crypto

The TOE's cryptographic mechanisms shall conform to the requirements of the cryptographic specifications of the DCSSI for the standard level of robustness [CRYPT-STD].

3.5 Assumptions

3.5.1 Assumptions concerning personnel

A_admin_no_evil

The personnel responsible for the administration or monitoring of the TOE and of the workstation hosting the TOE shall be trustworthy. They shall receive the necessary training and elements to carry out their duties correctly.

A_no_priv_user

Basic users of the workstation hosting the TOE shall not have "system" privileges or their equivalent for this workstation, or they shall be trusted basic users.

3.5.2 IT environment assumptions

A_configuration_control

TOE administrators shall have the necessary resources to save, check (against a reference state) and restore a TOE configuration.

Application note: TOE contributions to this assumption, if they exist, must be highlighted in the STs and PPs in conformity with this PP in the form of an OSP covering all or part of this assumption.

A_enough_resource

The workstation hosting the TOE shall provide it with the necessary resources for its operation.

Resources concerned: disk space, CPU time, memory, bandwidth, network interface and associated software, MMI, time stamping.

A_TOE_protection

The workstation hosting the TOE shall ensure the adequate protection of TOE elements (programs, data files, logs) and of the elements required for its operation (time stamping, elements relative to applications, users and connection, etc.).

A_known_localization

The TOE environment shall place trusted elements at the disposal of the TOE to allow it to determine whether the workstation hosting the TOE is connected inside or outside the company premises.

Application note: TOE contributions to this assumption, if they exist, must be highlighted in the STs and PPs in conformity with this PP in the form of an OSP. The TOE could for

example determine that it is inside the company by mutual authentication with a company authentication server.

A_no_bypass

The workstation hosting the TOE shall not allow incoming or outgoing network connections to be made that short circuit the TOE and the filtering policy implemented by the TOE.

Application note: TOE contributions to this assumption, if they exist, must be highlighted in the STs and PPs in conformity with this PP in the form of an OSP covering all or part of this assumption.

A_known_user

The TOE environment shall ensure the identification and authentication of users (basic users, administrators, supervisors) who connect, either locally or remotely, to the workstation hosting the TOE and shall be able to supply the TOE with trusted elements relating to these users (identity, role) and required for its operation.

3.5.3 Non-IT environment assumptions

A_physical_protection

The TOE environment shall ensure sufficient physical protection to limit the risk of TOE integrity coming under attack (equipment and data media).

4 Security objectives

4.1 Security objectives for the TOE

Note: the way these objectives are set out is only intended to make their reading easier.

4.1.1 Functional objectives

OT_filtering_level

The TOE shall make it possible to define at least the following filtering levels:

- Global filtering performed as soon as the TOE is started independently of any user connection; this filtering is controlled by the administrator.
- User filtering specific to a basic user (or a group of basic users) performed as soon as that basic user is connected. This filtering is controlled by the administrator, who may delegate the control of all or part of this filtering process to basic user in question.
- Adaptive filtering, specific to a basic user (or a group of basic users) generated by a learning mechanism and controlled by the basic user in question. This filtering mechanism may be activated or not by the administrator.

User filtering and adaptive filtering must not conflict with global filtering.

OT_filtering_criteria

The TOE shall make it possible to define filtering rules based on a logical combination of criteria. Such criteria may include:

- the application: identification, link between the application and protocols
- the communication flow: communication protocols[6], source or destination network addresses, direction (incoming or outgoing), source or destination ports, MAC address etc.
- the basic user: identity, role
- the workstation's network environment: the physical interface used, trusted zone (connection inside or outside the company)
- the connection context (notion of contextual filtering)

OT_application_integrity

The TOE shall make it possible to control the integrity of communicating applications and to detect and signal to authorised users all modifications made to these applications.

[6] This PP only takes into account the TCP/IP protocol stack (see glossary in appendix). Proprietary protocols other than IP shall be defined by the STs in conformity with this PP.

4.1.2 Administration and monitoring

OT_administration

The TOE shall allow to administer its configuration, locally or by remote, and the filtering rules. All filtering rules applied by the TOE shall be visible. Access to the administration function shall be limited to the administrator (U_administrator).

OT_monitoring

The TOE shall provide for the local or remote monitoring of TOE operations and of the various security-related events. Access to the monitoring function shall be limited to the supervisor (U_supervisor).

4.1.3 Identification, authentication, access control

OT_roles

The TOE shall distinguish at the very least between basic user, administrator and supervisor roles.

OT_identification

The TOE shall have at its disposal a mechanism enabling it to identify in a unique manner all users of administration or monitoring functions.

OT_authentication

The TOE shall authenticate users of administration and monitoring functions before any use of these functions is made.

OT_access_control

The TOE shall limit access to administration or monitoring functions to authorised users only. Access control shall cover: access (consultation, modification, deletion) to parameters, filtering rules and logs, and the shutdown or disabling of the TOE. It shall be configurable by the administrator, and based on defined TOE roles.

4.1.4 TOE data security

OT_TOE_reuse

The TOE shall be able to block access to its parameters (configuration, access control) and filtering rules if necessary (maintenance, deinstallation of software, workstation reassignment, etc.).

OT_log_protection

The TOE shall have at its disposal a mechanism to protect the confidentiality and integrity of logs. This mechanism shall make it possible to detect the corruption or deletion of an audit record and then inform authorised users (supervisor). This mechanism shall also be able to detect the reaching of a critical log saturation threshold and then inform authorised users.

4.1.5 Security of administration or monitoring data transmission

OT_remote_admin_authentication

The TOE shall guarantee the mutual identification and authentication of remote sites with which it communicates within the context of remote administrative or monitoring operations.

OT_remote_admin_integrity

The TOE shall guarantee and control the integrity of data shared with remote sites within the context of remote administrative or monitoring operations.

OT_remote_admin_confidentiality

The TOE shall guarantee the confidentiality of data shared with remote sites within the context of remote administrative or monitoring operations.

OT_remote_admin_no_replay

The TOE shall ensure that data shared with remote sites within the context of remote administrative or monitoring operations is protected from replay.

4.1.6 Audit and logging

OT_flow_audit

The TOE shall be able to track and record elements relative to the flows it processes within the scope of the security policy. The administrator shall be able to configure the granularity of these logs.

The TOE shall enable authorised users to view these logs according to various selection and sorting criteria (date, basic user, application, protocol, address, status, etc).

OT_admin_audit

The TOE shall be able to track and record the use of the administration and monitoring functions as well as events relating to its operation (TOE start-up and shutdown, login and logoff of administrators and supervisors, etc). The administrator shall be able to configure the granularity of these logs.

The TOE shall enable authorised users to view these logs according to various selection and sorting criteria (date, user, event, result, site, etc.). The TOE shall also enable authorised users to clear these logs.

OT_violation_detection

The TOE shall, as far as this is possible, detect attempts made to intrude on or violate the security policy and the risk of saturation, and issue an alarm to authorised users when necessary. The administrator shall be able to configure this alert mechanism.

OT_violation_reaction

The TOE shall react alone, or allow authorised users to react, in order to rapidly block all network access in the event of an alarm and then return to the former nominal state. The administrator shall be able to configure this alert mechanism. It shall be possible to log its use.

4.1.7 TOE reliability and availability

OT_TOE_integrity

The TOE shall be able to control the integrity of its configuration data and filtering, administration and logging functions and, if corruption is detected, indicate this by issuing an alarm.

Application note: the STs and PPs in conformity with this PP must state which elements (functions, data, etc.) are to be controlled and the integrity control mechanisms used.

OT_operational_state

The TOE shall allow the holders of authorised roles to know its operational state.

OT_crypto

The TOE's cryptographic mechanisms shall conform to the requirements of the cryptographic specifications of the DCSSI for the standard level of robustness [CRYPT-STD].

4.2 Security objectives for the operational environment

4.2.1 Objectives concerning the personnel

OE_admin_no_evil

The personnel responsible for the administration or monitoring of the TOE and workstation shall be trustworthy. They shall receive the necessary training and elements to carry out their duties correctly.

OE_non_priv_user

Basic users of the workstation hosting the TOE shall not have "system" privileges or their equivalent for this workstation, or they shall be trusted users.

4.2.2 Objectives relative to the IT environment

OE_configuration_control

TOE administrators shall have the necessary resources to save, check (against a reference state) and restore a TOE configuration.

OE_enough_resource

The workstation hosting the TOE shall provide it with the necessary resources for its operation: disk space, CPU time, memory, bandwidth, network interfaces, MMI, time stamping.

Application note: the STs and PPs in conformity with this PP and the manuals of the products concerned must provide recommendations regarding the amount of resources necessary for the TOE to function correctly, in particular regarding the disk space in order to reduce the risk of a TOE audit log saturation.

OE_TOE_protection

The workstation hosting the TOE shall ensure the adequate protection of TOE elements

(programs, data files, logs) and of the elements required for its operation (time, application and user identification, connection-related elements, etc.).

OE_trusted_known_context

The TOE environment shall supply the TOE with the elements required for its operation, and ensure such elements are sufficiently trustworthy: information relative to the connection, to users connected locally and to local programs requesting access to the network.

Application note: the STs and PPs in conformity with this PP can supplement this security objective for the IT environment with a TOE security objective. In particular, the TOE user manuals must clearly state these elements.

OE_known_localization

The TOE environment shall place trusted elements at the disposal of the TOE to allow it to determine whether the workstation hosting the TOE is connected inside or outside the company premises.

Application note: the STs and PPs in conformity with this PP can replace this security objective for the IT environment with a TOE security objective and revise the associated assumption. In particular, the TOE user manuals must clearly state the elements that will allow this context to be identified.

OE_no_bypass

The workstation hosting the TOE shall not allow incoming or outgoing network connections to be made that short circuit the TOE and the filtering policy implemented by the TOE.

Application note: the STs and PPs in conformity with this PP can replace this security objective for the IT environment with a TOE security objective and revise the associated assumption.

OE_known_user

The TOE environment shall ensure the identification and authentication of users (basic users, administrators, supervisors) who connect, either locally or remotely, to the workstation hosting the TOE and shall be able to supply the TOE with trusted elements relating to these users (identity, role) and required for its operation.

4.2.3 Objectives relative to the non-IT environment

OE_physical_protection

The TOE environment shall ensure sufficient physical protection to limit the risk of TOE integrity coming under attack (equipment and data media).

4.3 Rationale

4.3.1 Coverage of threats in the operational environment

T_eavesdropping (19)

Protection:

OT_remote_admin_confidentiality protects the confidentiality of data exchanged between the TOE and an administration or monitoring centre.

Detection:

Response:

T_disclosure (23)

Protection:

Regarding the network, **OT_remote_admin_authentication** ensures that all access to data takes place from an authorised remote site.

Regarding the workstation, data (filters, logs, authentication data, etc.) is protected from all unauthorised access via the workstation (**OE_TOE_protection**) or the TOE (**OT_log_protection**).

Regarding the TOE, **OT_monitoring, OT_identification, OT_authentication, OT_access_control** protect access to the monitoring functions that allow this data to be accessed.

Detection:

OT_admin_audit makes it possible to log all access to this data through the TOE via administrative or monitoring functions, and to make use of these logs.

Response:

T_spoofing (24)

Protection:

OT_remote_admin_authentication ensures that all network exchanges take place between the TOE and an authorised site.

OT_authentication ensures the authentication of administrators and supervisors and limits the risk of spoofing.

OT_remote_admin_integrity and **OT_remote_admin_no_replay** guarantee that data received by the TOE is not modified, or counterfeit, or replayed and that data transmitted by the TOE is only sent to an authorised system or user.

Detection:

OT_admin_audit enables the actions of administrators or supervisors to be logged and these logs to be used. This objective therefore makes it possible to detect attempts made to penetrate by brute force (access code attempts), and attempts made to send counterfeit or modified data.

Response:

OT_administration enables the administrator to modify access codes or TOE configuration to increase protection from this threat.

OE_configuration_control makes it possible to restore a trusted TOE configuration if necessary.

T_software_trapping (26)

Protection:

OE_known_user guarantees controlled access to the workstation, which limits the

risk of threats. **OE_TOE_protection** guarantees the protection of TOE elements (files) stored on the workstation.

Detection:

OT_TOE_integrity makes it possible to detect TOE corruption or the loss of TOE data coherency (filters, parameters, etc.), and to issue and alert (**OT_violation_detection** + **OT_monitoring**). When in operation, **OT_TOE_integrity** does not offer protection against the trapping of the integrity control function itself (no software self-check option).

OT_operational_state reveals the operational state of the TOE.

OT_admin_audit, OT_flow_audit and OT_violation_detection allow possible TOE malfunction to be detected.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_flooding (30)

Attack on the workstation's resources:

Protection:

OT_filtering_level and **OT_filtering_criteria** make it possible to block multiple attempts to access a workstation resource.

Detection:

OT_admin_audit, OT_flow_audit and **OT_violation_detection** make it possible to detect saturation of the workstation countered by the TOE.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected.

Attack on the TOE:

Protection:

OE_enough_resource states which resources are required for the nominal correct operation of the TOE.

Detection:

OT_violation_detection makes it possible to inform supervisors of the occurrence of saturations.

OT_admin_audit, OT_flow_audit and OT_violation_detection also allow a possible attack of the TOE to be detected.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

T_malfunction (31)

Protection:

Detection:

OT_operational_state ensures the detection of TOE malfunctions (such as the disabling of filtering processes or the non-operation of security functions) and informs supervisors (**OT_monitoring**).

OT_violation_detection makes it possible to detect violations of the security policy resulting from a malfunction.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_data_alteration (36)

Protection:

Controlling access to the workstation (**OE_known_user**), to the TOE (**OT_authentication**) and to administration and monitoring functions (**OT_access_control**) limits the possibility of this threat occurring.

OE_TOE_protection ensures that TOE elements are protected by the workstation.

Detection:

OT_TOE_integrity makes it possible to detect the loss of TOE parameters coherence or of defined filters.

OT_admin_audit, OT_flow_audit and **OT_violation_detection** make it possible to log administrative actions and to detect parameters or filtering rules corruption.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_illicit_processing (37)

Protection:

Regarding the network, **OT_remote_admin_confidentiality** protects the confidentiality of flow audit trails exchanged between the TOE and a monitoring centre. **OT_remote_admin_authentication** ensures that logged elements are transmitted to an authorised remote site.

Regarding the workstation, logs are protected from all access via the workstation (**OE_TOE_protection**) or the TOE (**OT_log_protection**).

Regarding the TOE, **OT_monitoring, OT_identification, OT_authentication, OT_access_control** protect access to the monitoring functions that allow this data

to be accessed.

In the event of the reuse of a workstation, **OT_TOE_reuse** makes it possible to destroy all sensitive data.

Detection:

OT_admin_audit makes it possible to log all access to this data through the TOE via the audit mechanism.

Response:

T_error (38)

Protection:

OE_Admin_no_evil limits the risk of this threat occurring as a result of use by authorised personnel (training and awareness of personnel).

Detection:

OT_admin_audit, OT_flow_audit and OT_violation_detection make it possible to log administrative actions and to detect parameters or filtering rules corruption.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_abuse (39)

Prevention / protection:

OE_Admin_no_evil limits the risk of this threat occurring as a result of use by authorised personnel (training and awareness of personnel).

OT_access_control makes it possible to limit user access to only useful elements (data, functions, etc.) required for their duties.

Detection:

OT_admin_audit makes it possible to log administrative actions and to detect parameters or filtering rules corruption.

OT_violation_detection makes it possible to detect the consequences of abused rights resulting in an obvious TOE malfunction or a major violation of the security policy.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_filter_inhibition (39, 40)

Protection (spoofing):

OT_identification and **OT_authentication** limit the risks of spoofing.

Protection (abuse):

The administration and monitoring personnel shall be trustworthy (**OE_Admin_no_evil**).

Detection:

OT_admin_audit makes it possible to log administrative actions and to detect parameters or filtering rules corruption.

OT_violation_detection makes it possible to detect the consequences of a disabled function resulting in an obvious TOE malfunction or a major violation of the security policy.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_usurpation (40)

Protection:

OT_identification and **OT_authentication** limit the risks of spoofing.

Detection:

OT_admin_audit makes it possible to log administrative actions and to detect parameters or filtering rules corruption.

OT_violation_detection makes it possible to detect the consequences of spoofing resulting in an obvious TOE malfunction or a major violation of the security policy.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

T_denial (41)

Protection:

OE_Admin_no_evil limits the risk of this threat occurring as a result of actions performed by the personnel.

Detection:

OT_admin_audit makes it possible to log administrative actions and to detect

parameters or filtering rules corruption.

OT_violation_detection makes it possible to detect the consequences of an action resulting in a violation of the security policy.

Response:

OT_violation_reaction makes it possible, where necessary, to block network access when an alarm is detected on the workstation.

OT_administration allows an administrator to correct a corrupted rule or parameter.

OE_configuration_control makes it possible to restore a trusted TOE configuration.

4.3.2 Coverage of organisational security policies

OSP_filtering

This organisational security policy is implemented by:

OT_filtering_criteria, which defines the criteria used by filtering rules.

OT_filtering_level, which defines the various types of filtering (global, user or specific).

OSP_application_integrity

This organisational security policy is implemented by:

OT_application_integrity, which is dedicated to the coverage of this policy.

OSP_roles

This organisational security policy is implemented by:

OT_roles, which is dedicated to the coverage of this policy.

This is supplemented by **OT_admin_audit** for the control of users' actions.

OSP_admin

This organisational security policy is implemented by:

OT_administration, which is dedicated to the coverage of this policy.

This is supplemented by **OT_admin_audit** for the control of administrative actions.

OSP_monitoring

This organisational security policy is implemented by:

OT_monitoring, which is dedicated to the coverage of this policy.

This is supplemented by **OT_admin_audit** for the control of monitoring actions.

OSP_admin_audit

This organisational security policy is implemented by:

OT_admin_audit, which covers the audit of administrative or monitoring actions performed.

OSP_flow_audit

This organisational security policy is implemented by:

OT_flow_audit, which is dedicated to the coverage of this policy.

OSP_sec_pol_violation_detection

This organisational security policy is implemented by:

OT_violation_detection, which is dedicated to the coverage of this policy.

OT_admin_audit and **OT_monitoring** for information regarding an alert.

OT_violation_reaction for the processing of alerts at the level of the workstation.

OSP_trusted_configuration

This organisational security policy is implemented by:

OE_configuration_control guarantees that administrators have the resources to back up a trusted configuration and restore it.

OSP_crypto

This organisational security policy is implemented by:

OT_crypto, which is dedicated to the coverage of this policy.

4.3.3 Coverage of assumptions

A_admin_no_evil

The **OE_Admin_no_evil** security objective is dedicated to the coverage of this assumption.

A_no_priv_user

The **OE_non_priv_user** security objective is dedicated to the coverage of this assumption.

A_configuration_control

The **OE_configuration_control** security objective is dedicated to the coverage of this assumption.

A_enough_resource

The **OE_enough_resource** security objective is dedicated to the coverage of this assumption.

A_TOE_protection

The **OE_TOE_protection** security objective is dedicated to the coverage of this assumption.

Moreover, **OE_trusted_known_context** guarantees that data used by the TOE corresponds to data made available by its environment.

A_known_localization

The **OE_known_localization** security objective is dedicated to the coverage of this assumption.

Moreover, **OE_trusted_known_context** guarantees that data used by the TOE corresponds to data made available by its environment.

A_no_bypass

The **OE_no_bypass** security objective is dedicated to the coverage of this assumption.

A_known_user

The **OE_known_user** security objective is dedicated to the coverage of this assumption.

A_physical_protection

The **OE_physical_protection** security objective is dedicated to the coverage of this assumption.

4.3.4 Coverage matrix

	T_eavesdropping	T_disclosure	T_spoofing	T_software_trapping	T_flooding	T_malfunction	T_data_alteration	T_illicit_processing	T_error	T_abuse	T_filter_inhibition	T_usurpation	T_denial	OSP_filtering	OSP_application_integrity	OSP_roles	OSP_admin	OSP_monitoring	OSP_admin_audit	OSP_flow_audit	OSP_sec_pol_violation_detection	OSP_trusted_configuration	OSP_crypto	A_admin_no_evil	A_no_priv_user	A_configuration_control	A_enough_resource	A_TOE_protection	A_known_localization	A_no_bypass	A_known_user	A_physical_protection
OT_filtering_level					X									X																		
OT_filtering_criteria					X									X																		
OT_application_integrity															X																	
OT_roles																X																
OT_administration			X				X		X	X	X	X	X				X															
OT_monitoring		X		X		X		X										X			X											
OT_identification		X						X			X	X																				
OT_authentication		X	X				X	X			X	X																				
OT_access_control		X					X	X		X																						
OT_TOE_reuse								X																								
OT_log_protection		X						X																								
OT_remote_admin_authenitcation		X	X					X																								
OT_remote_admin_integrity			X																													
OT_remote_admin_confidentiality	X							X																								
OT_remote_admin_no_replay			X																													
OT_flow_audit				X	X		X		X											X												
OT_admin_audit		X	X	X	X		X	X	X	X	X	X	X			X	X	X	X		X											
OT_violation_detection				X	X	X	X		X	X	X	X	X								X											
OT_violation_reaction				X	X	X	X		X	X	X	X	X								X											
OT_TOE_integrity				X			X																									
OT_operational_state				X		X																										
OT_crypto																							X									
OE_admin_no_evil									X	X	X		X											X								
OE_non_priv_user																									X							

	T_eavesdropping	T_disclosure	T_spoofing	T_software_trapping	T_flooding	T_malfunction	T_data_alteration	T_illicit_processing	T_error	T_abuse	T_filter_inhibition	T_usurpation	T_denial	OSP_filtering	OSP_application_integrity	OSP_roles	OSP_admin	OSP_monitoring	OSP_admin_audit	OSP_flow_audit	OSP_sec_pol_violation_detection	OSP_trusted_configuration	OSP_crypto	A_admin_no_evil	A_no_priv_user	A_configuration_control	A_enough_resource	A_TOE_protection	A_known_localization	A_no_bypass	A_known_user	A_physical_protection
OE_configuration_control			X	X		X	X		X	X	X	X	X									X				X						
OE_enough_ressource					X																						X					
OE_TOE_protection		X		X			X	X																				X				
OE_trusted_known_context																												X	X			
OE_know_localization																													X			
OE_no_bypass																														X		
OE_known_user				X			X																								X	
OE_physical_protection																																X

Table 2: Security objectives / Security problem definition

5 Extended components definition

Not applicable.

6 IT security requirements

6.1 Introduction

The TOE and its environment can be represented by the following diagram. The TSF is an additional module that is not shown in this diagram.

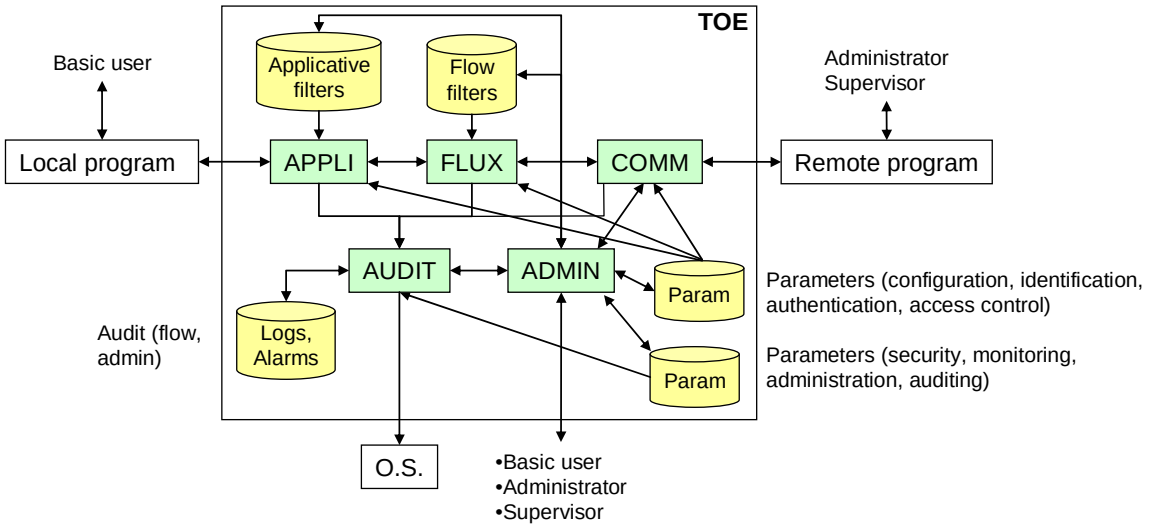

Figure 2: Modelling of the TOE and its environment

Application note: The only purpose of this modelling is to detail TOE behaviour at the security level. It does not impose any restrictions in terms of product software architecture and its implementation (the number of modules and functions, the structure of the data, etc.). The STs and PPs in conformity with this PP can adapt this model according to the products concerned. They must in this case indicate the collection between the elements of the adapted model and those of the model described here.

6.1.1 Subjects

The various subjects of the TOE are:

S_APPLI: This subject implements the application filtering policy and the application integrity control. It takes “ADAPTIVE” filtering into account (see A.5.1.1). It can generate tracking messages and alerts.

S_FLOW: This subject implements the network filtering policy. It can generate tracking messages and alerts.

S_AUDIT: This subject implements management functions relative to audit logs, the issuing of alerts and tracking messages.

S_ADMIN: This subject implements the TOE administration and monitoring functions. It can generate tracking messages and alerts.

S_COMM: This subject implements communication functions across the network with remote sites. It can generate tracking messages and alerts.

6.1.2 Objects

The following objects refer to the sensitive assets of the TOE described in the section 3.1.1.2, with the exception of **D_software,** which corresponds to the TOE itself:

D_FLOW_FILTER: network filtering rules.

D_APPLI_FILTER: application filtering rules and application integrity check values.

D_FLOW_AUDIT: tracking messages relative to the application and network filtering policy.

D_ADMIN_AUDIT: tracking messages relative to administrative operations, monitoring operations and the operation of the TOE.

D_ALARM: alert messages.

D_AC_PARAM: TOE access control parameters.

D_CONFIG: TOE configuration parameters (parameters relative to the TOE environment, to the configuration, to the network context, etc.).

The following objects do not appear in section 3.1.1.2. They correspond to TOE assets.

D_MON_PAR: configuration parameters of audit and alert monitoring functions (audit level of detail, alert thresholds, etc.).

D_SEC_PAR: configuration parameters of the security administration function.

6.1.3 Information

D_FLOW_IN: incoming communication flows for a local program (excluding the TOE).

D_FLOW_OUT: outgoing communication flows transmitted by a local program (excluding the TOE).

6.1.4 Operations

Operations performed by subjects on objects can be grouped into the following categories:

C: this operation corresponds to the creation or generation of data (filtering rule, alarm, audit message, basic user access parameter, etc.).

W: this operation corresponds to the storing, writing, modification, updating, transmission, display or printing of data

R: this operation corresponds to the reading or receipt of data

D: this operation corresponds to the removal, the clearing or the resetting of data

B: this operation corresponds to the saving of parameters or filtering rules

6.1.5 Security attributes

Attributes relative to basic user identification and rights:

SA_IDENT: corresponds to the identity of a subject or an object.
Possible values for a subject: S_APPLI, S_FLOW, S_COMM, S_ADMIN, S_AUDIT.
Possible values for an object: D_FLOW_IN, D_FLOW_OUT, D_ALARM, D_FLOW_FILTER, D_APPLI_FILTER, D_FLOW_AUDIT, D_ADMIN_AUDIT, D_CONFIG, D_AC_PARAM, D_MON_PAR, D_SEC_PAR, S_APPLI, S_FLOW, S_COMM, S_ADMIN, S_AUDIT.

SA_ROLE: corresponds to a role. Possible values: ADMINISTRATOR, SUPERVISOR, BASIC USER.

SA_USER: associated with a subject, it corresponds to the identity of the user linked with this subject; associated with an object (e.g. an application filter), it corresponds to the identity of a user with access right to this object.

SA_RIGHT: corresponds to a right owned by a basic user. Possible values: AUDIT (that basic user's right to consult audit and alert messages).

SA_CONNECTION: corresponds to the source of the connection for an administrator or supervisor. Possible values: "LOCAL" (connection on the workstation) or "REMOTE" (connection from a remote site).

Attributes relative to the filtering process or used for the filtering process:

SA_NETWORK: groups together security attributes relative to the network parameters used for filtering: source address, destination address, source port (or equivalent), destination port (or equivalent), protocol, direction (incoming or outgoing), status (of the connection, used in the event of contextual filtering), MAC address.

Application note: the STs and PPs in conformity with this PP must provide the exact list of network parameters used.

SA_ADAPTIVITY: makes it possible to define whether a filter (for which the SA_LEVEL attribute has the value "SPECIFIC") is "PERMANENT" or "ADAPTIVE", i.e. modifiable by the basic user.

SA_ENVIRONMENT: corresponds to the network environment of the workstation. Possible values: "IN" for connections made inside the company, "OUT" for connections made from premises outside the company.

SA_DIGEST: corresponds to the integrity check value calculated for a program, alarm or audit message.

SA_LEVEL: makes it possible to define if a filter is "GLOBAL" (i.e. valid for everyone) or "SPECIFIC" to one basic user.

SA_PROG_ID: corresponds to the identity of a program.

6.1.6 External entities

These entities, external to the TOE, referred to as users in this PP, can be either software programs or individuals. They are defined in section 3.2 of this document.

Security properties:

These users have security properties inherited by subjects with which/whom they establish links:

Users	Associated security properties
U_LOCAL_PROGRAM	Program identity, integrity check value
U_REMOTE_PROGRAM	Program identity, role
U_ADMINISTRATOR	User identity, role, connection
U_SUPERVISOR	User identity, role, connection
U_BASIC_USER	User identity, role

Table 3: User security properties

Binding:

Links (*binding*) that can be established between users and subjects are as follows:

	S_ADMIN	S_COMM	S_APPLI	S_FLOW	S_AUDIT
U_LOCAL_PROGRAM			X		
U_REMOTE_PROGRAM		X			
U_ADMINISTRATOR	X	X			
U_SUPERVISOR	X	X			
U_BASIC_USER	X				

Table 4: User - subject links

6.1.7 Access control rules

Access control rules for subjects to objects (or to other subjects considered as objects) and the flow control rules are shown in the following table.

Application note: the STs and PPs in conformity with this PP must state the manner in which these access control rules are implemented according to the connection between the model described in this PP and its adaptation.

Functions permitted by the access or flow control rule	Subjects with access	Information or objects accessed	Operations	Access authorised if:
Loading of user data and configuration parameters by the TOE	S_ADMIN	D_AC_PARAM D_CONFIG D_SEC_PAR D_MON_PAR D_APPLI_FILTER D_FLOW_FILTER	R	SA_IDENT (subject) = S_ADMIN & SA_IDENT (object) = (D_AC_PARAM or D_SEC_PAR or D_APPLI_FILTER or D_FLOW_FILTER or D_MON_PAR or D_CONFIG)
Loading of audit parameters by the TOE	S_AUDIT	D_MON_PAR	R	SA_IDENT (subject) = S_AUDIT & SA_IDENT (object) = D_MON_PAR
Loading of user data and configuration parameters by the TOE	S_COMM	D_CONFIG D_AC_PARAM	R	SA_IDENT (subject) = S_COMM & SA_IDENT (object) = (D_CONFIG or D_AC_PARAM)
Loading of network filtering rules and parameters by the TOE	S_FLOW	D_CONFIG D_FLOW_FILTER	R	SA_IDENT (subject) = S_FLOW & SA_IDENT (object) = (D_CONFIG or D_FLOW_FILTER)
Loading of application filtering rules and parameters by the TOE	S_APPLI	D_CONFIG D_APPLI_FILTER	R	SA_IDENT (subject) = S_APPLI & SA_IDENT (object) = (D_CONFIG or D_APPLI_FILTER)
Management by the administrator of security parameters and filtering rules	S_ADMIN	D_AC_PARAM D_SEC_PAR D_APPLI_FILTER D_FLOW_FILTER	C / W / R / D	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = ADMINISTRATOR & SA_IDENT (object) = (D_AC_PARAM or D_SEC_PAR or D_APPLI_FILTER or D_FLOW_FILTER)
Management by authorised basic users of their specific adaptive or permanent filters	S_ADMIN	D_APPLI_FILTER	C / W / R / D	SA_IDENT (subject) = S_ADMIN & SA_USER (subject) = SA_USER (object) & SA_ROLE (subject) = BASIC USER & SA_LEVEL (object)= (SPECIFIC) & SA_ADAPTIVITY (object) = (ADAPTIVE or PERMANENT) & SA_IDENT (object) = D_APPLI_FILTER
Management by supervisors of audit and monitoring parameters	S_ADMIN	D_MON_PAR	C / W / R / D	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = SUPERVISOR & SA_IDENT (object) = D_MON_PAR
Issuing of alarms and audit messages	S_ADMIN S_COMM S_FLOW S_APPLI	S_AUDIT	W	SA_IDENT (subject) = (S_ADMIN or S_COMM or S_APPLI or S_FLOW) & SA_IDENT (object) = S_AUDIT
Recording of alerts and audit messages in the logs concerned	S_AUDIT	D_ALARM D_ADMIN_AUDIT D_FLOW_AUDIT	C	SA_IDENT (subject) = S_AUDIT & SA_IDENT (object) = (D_ALARM or D_ADMIN_AUDIT or D_FLOW_AUDIT)
Relaying of commands issued by remote administrators and supervisors	S_COMM	S_ADMIN	W	SA_IDENT (subject) = S_COMM & SA_ROLE (subject) = (ADMINISTRATOR or SUPERVISOR) & SA_IDENT (object) = S_ADMIN

Functions permitted by the access or flow control rule	Subjects with access	Information or objects accessed	Operations	Access authorised if:
Relaying of responses to commands made by remote administrators and supervisors	S_ADMIN	S_COMM	W	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = (ADMINISTRATOR or SUPERVISOR) & SA_IDENT (object) = S_COMM
Relaying of supervisors' commands	S_ADMIN	S_AUDIT	W	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = SUPERVISOR & SA_IDENT (object) = S_AUDIT
Relaying of requests for reading audit messages and alerts by authorised basic users	S_ADMIN	S_AUDIT	W	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = BASIC USER & SA_RIGHT (subject) = AUDIT & SA_IDENT (object) = S_AUDIT
Reading or deletion of alerts and audit messages by supervisors	S_AUDIT	D_ALARM D_ADMIN_AUDIT D_FLOW_AUDIT	R / D	SA_IDENT (subject) = S_AUDIT & SA_ROLE (subject) = SUPERVISOR & SA_IDENT (object) = (D_ALARM or D_ADMIN_AUDIT or D_FLOW_AUDIT)
Reading of alerts and audit messages for authorised basic users	S_AUDIT	D_ALARM D_FLOW_AUDIT	R	SA_IDENT (subject) = S_AUDIT & SA_ROLE (subject) = BASIC USER & SA_RIGHT (subject) = AUDIT & SA_IDENT (object) = (D_ALARM or D_FLOW_AUDIT)
Relaying of responses to supervisors' commands and requests for reading audit messages and alerts by authorised basic users	S_AUDIT	S_ADMIN	W	SA_IDENT (subject) = S_AUDIT & SA_IDENT (object) = S_ADMIN
Saving of TOE parameters	S_ADMIN	D_AC_PARAM D_CONFIG D_SEC_PAR D_MON_PAR D_APPLI_FILTER D_FLOW_FILTER	B	SA_IDENT (subject) = S_ADMIN & SA_ROLE (subject) = ADMINISTRATOR & SA_IDENT (object) = (D_AC_PARAM or D_CONFIG or D_SEC_PAR or D_MON_PAR or D_APPLI_FILTER or D_FLOW_FILTER)
Relaying by the TOE of incoming packets	S_COMM	S_FLOW	W	SA_IDENT (subject) = S_COMM & SA_IDENT (object) = S_FLOW
Implementation by the TOE of network filtering rules for incoming or outgoing packets	S_FLOW	S_COMM S_APPLI	W	SA_IDENT (subject) = S_FLOW & SA_IDENT (object) = (S_COMM or S_APPLI) & SA_NETWORK (object), SA_ENVIRONMENT (object), SA_LEVEL (object), SA_ADAPTIVITY (object) coherent with the rules defined in D_FLOW_FILTER
Implementation by the TOE of application filtering rules for outgoing packets	S_APPLI	S_FLOW	W	SA_IDENT (subject) = S_APPLI & SA_IDENT (object) = S_FLOW & SA_NETWORK (subject), SA_ENVIRONMENT (object), SA_LEVEL (object), SA_ADAPTIVITY(object), SA_PROG_ID (object), SA_DIGEST (object) coherent with the rules defined in D_APPLI_FILTER

Table 5: Access control rules

6.2 TOE security functional requirements

These requirements are set out in the same manner as the TOE security objectives, as follows:

- *Services carried out by the TOE (i.e. application filtering and network filtering)*
- *Identification, authentication, access to the TOE*
- *Security of TOE parameters and filtering rules*
- *Security of administration and monitoring exchange from a remote site*
- *Audit and security of logs*

- *Reliability of the TOE*
- *Other requirements*

6.2.1 Services carried out by the TOE (application and network filtering)

The following requirements contribute to the TOE's implementation of the application or network filtering policy.

6.2.1.1 Network filtering of outgoing flows

FDP_IFC.1 (ONF) Subset information flow control (network filtering of outgoing flows)

Audit - No audit messages for this component
Dependencies FDP_IFF.1 (ONF)

FDP_IFC.1.1 The TSF shall enforce the **[assignment: network filtering policy for outgoing flows]** on: **[assignment:**
- subjects: S_FLOW, S_COMM
- information: D_FLOW_OUT, D_FLOW_FILTER
- operation: W].

FDP_IFF.1 (ONF) Simple security attributes (network filtering of outgoing flows)

Audit - Refusal of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)
- Acceptance of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)
Dependencies FDP_IFC.1 (ONF)
FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the **[assignment: network filtering policy for outgoing flows]** based on the following types of subject and information security attributes: **[assignment:**
- subjects: S_FLOW, S_COMM
- subject security attributes: SA_IDENT
- information: D_FLOW_OUT, D_FLOW_FILTER
- information security attributes: SA_IDENT, SA_NETWORK, SA_ENVIRONMENT, SA_PROG_ID, SA_USER].

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: **[assignment: there exists at least one filtering rule selected in D_FLOW_FILTER authorising this flow].**

FDP_IFF.1.3 The TSF shall enforce the **[assignment: no additional information flow control SFP rules]**.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: no rules that explicitly authorise information flows].**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **[assignment: there exists at least one filtering rule selected in D_FLOW_FILTER prohibiting this flow].**

FDP_ETC.2 (ONF) Export of user data with security attributes (network filtering of outgoing flows)

Audit - Detail of the export request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))
Dependencies FDP_IFC.1 (ONF)

FDP_ETC.2.1 The TSF shall enforce the **[assignment: network filtering policy for outgoing flows]** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: **[assignment: no additional exportation control rules]**.

FDP_IFF.5 (ONF) No illicit information flows (network filtering of outgoing flows)

Audit - Result of the identification of an illicit information bypass flow
Dependencies FDP_IFC.1 (ONF)

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [**assignment: network filtering policy for outgoing flows**].

6.2.1.2 Network filtering of incoming flows

FDP_IFC.1 (INF) Subset information flow control (network filtering of incoming flows)

Audit - No audit messages for this component
Dependencies FDP_IFF.1 (INF)

FDP_IFC.1.1 The TSF shall enforce the [**assignment: network filtering policy for incoming flows] on: [assignment:**
- subjects: S_FLOW, S_COMM
- information: D_FLOW_IN, D_FLOW_FILTER
- operation: R].

FDP_IFF.1 (INF) Simple security attributes (network filtering of incoming flows)

Audit *- Refusal of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)*
- Acceptance of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)

Dependencies *FDP_IFC.1 (INF)*
FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the [**assignment: network filtering policy for incoming flows**] based on the following types of subject and information security attributes: **[assignment:**
- subjects: S_FLOW, S_COMM
- subject security attributes: SA_IDENT
- information: D_FLOW_IN, D_FLOW_FILTER
- information security attributes: SA_IDENT, SA_NETWORK, SA_ENVIRONMENT].

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: [**assignment: there exists at least one filtering rule selected in D_FLOW_FILTER authorising this flow**].

FDP_IFF.1.3 The TSF shall enforce the [**assignment: no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**assignment: no rules that explicitly authorise information flows**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**assignment: there exists at least one filtering rule selected in D_FLOW_FILTER prohibiting this flow**].

FDP_ITC.1 (INF) Import of user data without security attributes (network filtering of incoming flows)

Audit *- Detail of the import request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))*

Dependencies *FDP_IFC.1 (INF)*
FMT_MSA.3

FDP_ITC.1.1 The TSF shall enforce the [**assignment: network filtering policy for incoming flows**] when importing user data, controlled under the SFP(s), from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**assignment: no additional importation control rules**].

FDP_IFF.5 (INF) No illicit information flows (network filtering of incoming flows)

Audit *- Result of the identification of an illicit information bypass flow*
Dependencies *FDP_IFC.1 (INF)*

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [**assignment: network filtering policy for incoming flows**].

6.2.1.3 Application filtering of outgoing flows

FDP_IFC.1 (OAF) Subset information flow control (application filtering of outgoing flows)

Audit *- No audit messages for this component*
Dependencies *FDP_IFF.1 (OAF)*

FDP_IFC.1.1 The TSF shall enforce the [**assignment: application filtering policy for outgoing flows**] on: [**assignment:**
- subject: S_APPLI
- information: D_FLOW_OUT, D_APPLI_FILTER
- operation: R].

FDP_IFF.1 (OAF) Simple security attributes (application filtering of outgoing flows)

Audit *- Refusal of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)*
- Acceptance of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)
Dependencies *FDP_IFC.1 (OAF)*
FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the [**assignment: application filtering policy for outgoing flows**] based on the following types of subject and information security attributes: **[assignment:**
- subjects: S_APPLI
- subject security attributes: SA_IDENT
- information: D_FLOW_OUT, D_APPLI_FILTER
- information security attributes: SA_PROG_ID, SA_USER, SA_DIGEST, SA_NETWORK (destination port), SA_ENVIRONMENT, SA_IDENT].

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: [**assignment: there exists at least one filtering rule selected in D_APPLI_FILTER authorising this flow**].

FDP_IFF.1.3 The TSF shall enforce the [**assignment: no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**assignment: no rules that explicitly authorise information flows**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**assignment: there exists at least one filtering rule selected in D_APPLI_FILTER prohibiting this flow**].

FDP_ITC.1 (OAF) Import of user data without security attributes (application filtering of outgoing flows)

Audit *- Detail of the import request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))*
Dependencies *FDP_IFC.1 (OAF)*
FMT_MSA.3

FDP_ITC.1.1 The TSF shall enforce the [**assignment: application filtering policy for outgoing flows**] when importing user data, controlled under the SFP from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**assignment: no additional importation control rules**].

FDP_IFF.5 (OAF) No illicit information flows (application filtering of outgoing flows)

Audit *- Result of the identification of an illicit information bypass flow*
Dependencies *FDP_IFC.1 (OAF)*

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [**assignment: application filtering policy for outgoing flows**].

6.2.1.4 Local program integrity control

FTA_TSE.1 (OAF) TOE session establishment (Application filtering of outgoing flows)

Audit *- Refusal to establish a link for a local program (associated data: reason for the refusal, security parameters used and the security rule on which refusal to establish a link is based)*
Dependencies *none*

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment: attributes**].

Refinement *The TSF shall be able to prohibit all local programs (U_LOCAL_PROGRAM) from establishing a session with the application filtering module (S_APPLI) if at least one of the following conditions is met:*

1. *The integrity check value for this program, calculated when the connection request is made, is different from the integrity check value memorised by the TOE in D_APPLI_FILTER.*
2. *Other conditions.*

Application note:
The STs in conformity with this PP must state the manner in which the integrity check value is calculated and other conditions selected.

6.2.1.5 Application filtering of incoming flows

FDP_IFC.1 (IAF) Subset information flow control (application filtering of incoming flows)

Audit *- No audit messages for this component*
Dependencies *FDP_IFF.1 (IAF)*

FDP_IFC.1.1 The TSF shall enforce the [**assignment: application filtering policy for incoming flows**] on: [**assignment:**
- subject: S_APPLI
- information: D_FLOW_IN, D_APPLI_FILTER
- operation: W].

FDP_IFF.1 (IAF) Simple security attributes (application filtering of incoming flows)

Audit *- Refusal of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)*
- Acceptance of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)
Dependencies *FDP_IFC.1 (IAF)*
FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the [**assignment: application filtering policy for incoming flows**] based on the following types of subject and information security attributes: **[assignment:**
- subject: S_APPLI
- subject security attributes: SA_IDENT
- information: D_FLOW_IN, D_APPLI_FILTER
- information security attributes: SA_DIGEST, SA_NETWORK (source port), SA_ENVIRONMENT, SA_IDENT].

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: [**assignment: there exists at least one filtering rule selected in D_APPLI_FILTER authorising this flow**].

FDP_IFF.1.3 The TSF shall enforce the [**assignment: no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**assignment: no rules that explicitly authorise information flows**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**assignment: there exists at least one filtering rule selected in D_APPLI_FILTER prohibiting this flow**].

FDP_ETC.2 (IAF) Export of user data with security attributes (application filtering of incoming flows)

Audit - Detail of the request (associated data: filtering rule and attributes upon which acceptance or refusal of the packet is based, status (acceptance or refusal))
Dependencies FDP_IFC.1 (IAF)

FDP_ETC.2.1 The TSF shall enforce the [**assignment: application filtering policy for outgoing flows**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [**assignment: no additional exportation control rules**].

FDP_IFF.5 (IAF) No illicit information flows (application filtering of incoming flows)

Audit - Result of the identification of an illicit information bypass flow
Dependencies FDP_IFC.1 (IAF) Subset information flow control

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [**assignment: application filtering policy for incoming flows**].

6.2.1.6 Local program connection

FIA_UID.2 (LP) User identification (local program)

Audit - Connection of a local program (associated data: identification of the program, connection context)
Dependencies none

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.

Refinement *The TSF shall require that all local programs (U_LOCAL_PROGRAM) be identified successfully before establishing a link with the application filtering module (S_APPLI).*

FIA_USB.1 (LP) User-subject binding (local program)

Audit *- Establishment of a link between a local program and a subject (associated data: identification of the program, identification of the subject, values of the security attributes defined when establishing the link)*

Dependencies *FIA_ATD.1 (LP)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**assignment: security attributes: SA_PROG_ID, SA_DIGEST, SA_ENVIRONMENT, SA_USER, SA_NETWORK**].

Refinement *The TSF shall associate the following security attributes with the application filtering module (S_APPLI) following the establishment of a link between a local program (U_LOCAL_PROGRAM) and the application filtering module (S_APPLI): SA_PROG_ID, SA_DIGEST, SA_ENVIRONMENT, SA_USER, SA_NETWORK*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment: the security attributes of S_APPLI are updated according to the security properties of U_LOCAL_PROGRAM in the following manner:**
- 1. SA_PROG_ID = program identity
- 2. SA_DIGEST = value calculated by the TOE for this program
- 3. SA_ENVIRONMENT = value corresponding to the network environment of the workstation (“IN” or “OUT”); this value is supplied by the workstation
- 4. SA_USER = identity of the user connected to the workstation; this value is supplied by the workstation
- 5. SA_NETWORK is assigned the values relative to the network connection; these values are calculated by the TOE according to information taken from the requested network connection].

Application note:
The STs in conformity with this PP must state the matter in which the integrity check value is calculated.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**assignment: no additional rules for the changing of attributes**].

FIA_ATD.1 (LP) User attribute definition (local program)

Audit *- No audit messages for this component*

Dependencies none

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: security attributes: SA_PROG_ID, SA_DIGEST, SA_ENVIRONMENT, SA_USER, SA_NETWORK**].

FTA_SSL.4 (LP) User-initiated termination (local program)

Audit - Closing of an interactive session by a local program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)
Dependencies none

FTA_SSL.4.1 The TSF shall allow [**refinement: local program]-initiated termination of the [refinement: local program**]'s own interactive session.

6.2.1.7 Remote program connection

FIA_UID.1 (RP) Timing of identification (remote program)

Audit - Anonymous connection of a remote program (associated data: connection context)
Dependencies none

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

Refinement The TSF shall enable remote programs (U_REMOTE_PROGRAM) to establish a link with the communication module (S_COMM) without identifying themselves when these programs are not seeking to communicate with the administration and monitoring module (S_ADMIN).

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.

FIA_USB.1 (RP) User-subject binding (remote program)

Audit - Establishment of a link between a remote program and a subject (associated data: identification of the subject, values of the security attributes defined when establishing the link)
Dependencies FIA_ATD.1 (RP)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**assignment: security attributes: SA_ENVIRONMENT, SA_NETWORK**].

Refinement The TSF shall associate the following security attributes with the communication module (S_COMM) following the establishment of a link between a remote program (U_REMOTE_PROGRAM) and the communication module (S_COMM): SA_ENVIRONMENT, SA_NETWORK

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment: S_COMM's security attributes are updated in the following manner:**
- 1. SA_ENVIRONMENT = value corresponding to the network environment of the workstation ("IN" or "OUT"); this value is supplied by the workstation
- 2. SA_NETWORK is assigned the values relative to the network connection; these values are calculated by the TOE according to information taken from the requested network connection].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**assignment: no additional rules for the changing of attributes**].

FIA_ATD.1 (RP) User attribute definition (remote program)

Audit *- No audit messages for this component*
Dependencies *none*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: security attributes: SA_NETWORK, SA_ENVIRONMENT**].

FTA_SSL.4 (RP) User-initiated termination (remote program)

Audit *- Closing of an interactive session by a remote program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)*
Dependencies *none*

FTA_SSL.4.1 The TSF shall allow [**refinement: remote program**]-initiated termination of the [**refinement: remote program**]'s own interactive session.

6.2.2 User identification, authentication & TOE access

The following requirements help to define users, to generate authentication data and rules relative to the establishment or the ending of sessions by local or remote users.

FMT_MTD.1 Management of TSF data

Audit *- Recording of a new user*
- Access (successful or not for reading, writing or modification) to a user's properties
Dependencies *FMT_SMR.1*
FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection: change_default, query, modify, delete, clear, record**] the: [**assignment:**
1. Identity of a new user.
2. Role or roles (ADMINISTRATOR, SUPERVISOR, BASIC USER)

owned by the user]
to [**assignment: ADMINISTRATOR**].

FMT_MTD.3 Secure TSF data

Audit *- Refusal of authentication data or security properties relative to user management*
Dependencies *FMT_MTD.1*

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [**assignment: D_AC_PARAM, which contains the authentication data and all security properties relative to user management**].

FIA_SOS.1 Verification of secrets

Audit *- Acceptance or refusal of the authentication data supplied*
Dependencies *none*

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment: the authentication data chosen by the administrator include a minimum number of characters mixing upper and lower case letters, figures and non-alphanumeric characters**].

Application note:
It is for the authors of the STs to choose between the entry of authentication data by the administrator (FI1_SOS.1) and the generation of authentication data by the TOE (FIA_SOS.2).
The STs in conformity with this PP must state the minimum number of characters and the conditions relative to the choice of these characters.
The STs in conformity with this PP must also indicate, where necessary, the cryptographic mechanisms used to protect this authentication data.

FIA_SOS.2 TSF generation of secrets

Audit *- Generation of authentication data*
Dependencies *none*

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [**assignment: random generation with a minimum number of characters mixing upper and lower case letters, figures and non-alphanumeric characters**].

Application note:
It is for the authors of the STs to choose between the entry of authentication data by the administrator (FI1_SOS.1) and the generation of authentication data by the TOE (FIA_SOS.2).
The STs in conformity with this PP must state the minimum number of characters and the method used for the generation of random numbers.
The STs in conformity with this PP must also indicate, where necessary, the cryptographic mechanisms used to protect this authentication data.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [**assignment: the use of this authentication data for establishing the link with the administration and monitoring module (S_ADMIN) or the communication module (S_COMM)**].

FIA_UID.2 (LU) User identification (local user)

Audit *- Connection of a local user (associated data: user identity, connection context)*
Dependencies *none*

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.

Refinement *The TSF shall require that each local user (U_ADMINISTRATOR, U_SUPERVISOR, U_BASIC_USER) be successfully identified before authorising the establishment of a link with the administration and monitoring module (S_ADMIN) on behalf of this user.*

FIA_UID.2 (RU) User identification (remote user)

Audit *- Connection of a remote user (associated data: user identity, connection context)*
Dependencies *none*

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.

Refinement *The TSF shall require that each remote user (U_ADMINISTRATOR, U_SUPERVISOR) be successfully identified before authorising the establishment of a link with the administration and monitoring module (S_ADMIN) on behalf of this user.*

FIA_UAU.2 (LU) User authentication before any action (local user)

Audit *- Authentication attempt (successful or not) of a local user*
Dependencies *FIA_UID.1 (covered by FIA_UID.2 (LU))*

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.

Refinement *The TSF shall require that each local user (U_ADMINISTRATOR, U_SUPERVISOR, U_BASIC_USER) be successfully authenticated before authorising the establishment of a link with the administration and monitoring module (S_ADMIN) on behalf of this user.*

FIA_UAU.2 (RU) User authentication before any action (remote user)

Audit *- Authentication attempt (successful or not) of a remote user*
Dependencies *FIA_UID.1 (covered by FIA_UID.2 (RU))*

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.

Refinement *The TSF shall require that each remote user (U_ADMINISTRATOR, U_SUPERVISOR) be successfully authenticated before authorising the establishment of a link with the administration and monitoring module (S_ADMIN) on behalf of this user.*

FIA_UAU.7 Protected authentication feedback

Audit *- No audit messages for this component*
Dependencies *FIA_UAU.1 (covered by FIA_UAU.2 (LU) and FIA_UAU.2 (RU))*

FIA_UAU.7.1 The TSF shall provide only [**assignment: information indicating keystrokes**] to the user while the authentication is in progress.

Application note:
The STs in conformity with this PP must state if a piece of information (e.g. "asterisks") is transmitted back to the user or not, and whether or not this enables the number of characters entered by the user to be counted.

FIA_AFL.1 Authentication failure handling

Audit *- Reaching or exceeding one of the alert thresholds during connection (associated data: threshold, number of attempts)*
- Actions taken (issuing of an alert, blocking of the connection, etc.)
Dependencies *FIA_UAU.1 (covered by FIA_UAU.2 (LU) and FIA_UAU.2 (RU))*

FIA_AFL.1.1 The TSF shall detect when [**selection: N1 (or more)**] unsuccessful authentication attempts occur related to: [**assignment:**
- 1. Erroneous connection attempts to the administration and monitoring module (S_ADMIN) using the same identity or different identities in less than N2 minutes.
- 2. Other rules].

Application note:
The STs in conformity with this PP must state the chosen or possible values for N1 and N2 as well as the other selected rules.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**selection: met**], the TSF shall: [**assignment:**
- 1. Issue an alert.
- 2. Take the actions defined by the administrator].

Application note:
The STS in conformity with this PP must state the actions the administrator can define in response to exceeding the authentication threshold.

FTA_TSE.1 (LU) TOE session establishment (local user)

Audit *- Refusal to establish a link between a local user and a subject (associated data: reason for the refusal, security parameters upon which acceptance or refusal of the establishment of the link are based)*
Dependencies *none*

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on: [**assignment:**
- 1. Another local user is already connected using the same identity.
- 2. Other conditions].

Application note:
The STs in conformity with this PP must state the other conditions selected.

FTA_TSE.1 (RU) TOE session establishment (remote user)

Audit *- Refusal to establish a link between a remote user and a subject (associated data: reason for the refusal, security parameters upon which acceptance or refusal of the establishment of the link are based)*
Dependencies *none*

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on: [**assignment:**
- 1. Another remote user is already connected using the same identity.
- 2. Other conditions].

Application note:
The STs in conformity with this PP must state the other conditions selected.

FIA_USB.1 (LU) User-subject binding (local user)

Audit *- Establishment of a link between a user and a subject (associated data: identification of the user, identification of the subject, values of the security attributes defined when establishing the link)*
Dependencies *FIA_ATD.1 (LU)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**assignment: security attributes: SA_USER, SA_ROLE, SA_CONNECTION**].

Refinement *The TSF shall associate the following security attributes with the administration and monitoring module (S_ADMIN) following the establishment of a link between a user connected locally (Users concerned: U_BASIC_USER, U_SUPERVISOR, U_ADMINISTRATOR) and the administration and monitoring module (S_ADMIN): SA_USER, SA_ROLE, SA_CONNECTION*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment: the security attributes of S_ADMIN are updated according to user security properties in the following manner:**
- 1. SA_USER = user identity (value taken from D_AC_PARAM).
- 2. SA_ROLE = role owned by the user (value from D_AC_PARAM).
- 3. SA_CONNECTION = "LOCAL"].

Application note:
The STs in conformity with this PP must state the conditions selected.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**assignment: no additional rules for the changing of attributes**].

FIA_ATD.1 (LU) User attribute definition (local user)

Audit *- No audit messages for this component*
Dependencies *none*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: security attributes: SA_USER, SA_ROLE, SA_CONNECTION**].

FIA_USB.1 (LU) User-subject binding (local user)

Audit *- Establishment of a link between a remote user and a subject (associated data: identification of the user, identification of the subject, values of the security attributes defined when establishing the link)*
Dependencies *FIA_ATD.1 (RU)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**assignment: security attributes: SA_USER, SA_ROLE, SA_CONNECTION**].

Refinement *The TSF shall associate the following security attributes with the communication module (S_COMM) following the establishment of a link between a remote user and the communication module (S_COMM): SA_USER, SA_ROLE, SA_CONNECTION*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment: S_COMM's security attributes are updated in the following manner:**
- 1. SA_USER = user identity (value from D_AC_PARAM).
- 2. SA_ROLE = role held by the user (value from D_AC_PARAM).
- 3. SA_CONNECTION = "REMOTE"].

Application note:
The STs in conformity with this PP must state the conditions selected.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**assignment: no additional rules for the changing of attributes**].

FIA_ATD.1 (RU) User attribute definition (remote user)

Audit *- No audit messages for this component*
Dependencies *none*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: security attributes: SA_USER, SA_ROLE, SA_CONNECTION**].

FTA_SSL.3 (RU) TSF-initiated termination (remote user)

Audit *- Closing of an interactive session by the TSF (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the interactive session)*

Dependencies *none*

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [**assignment: time interval of user inactivity**].

Refinement *The TSF shall put an end to the link between the user and the communication module (S_COMM) under the following conditions:*

1. *A break in the network connection between the remote site and the TOE.*
2. *Shutdown of the TOE.*
3. *Removal of the user in D_AC_PARAM.*
4. *A break in the trusted channel (following the detection of an anomaly on this channel for example) established between the TOE and the remote program and used by this link.*
5. *Other conditions.*

Users concerned: U_ADMINISTRATOR, U_SUPERVISOR

Application note:

The STs in conformity with this PP must state the conditions that can lead to a break in the link by the TSF.

FTA_SSL.4 (LU) User-initiated termination (local user)

Audit *- Closing of an interactive session by a local user (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the session)*

Dependencies *none*

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the [**refinement: local**] user's own interactive session.

FTA_SSL.4 (RU) User-initiated termination (remote user)

Audit *- Closing of an interactive session by a remote user (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the session)*

Dependencies *none*

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the [**refinement: remote**] user’s own interactive session.

6.2.3 TOE data security

The following requirements contribute to the protection of TOE data.

6.2.3.1 Access control to TOE configuration parameters

FDP_ACC.1 (PAR) Subset access control (access to configuration parameters)

Audit *- No audit messages for this component*
Dependencies *FDP_ACF.1 (PAR)*

FDP_ACC.1.1 The TSF shall enforce the [**assignment: access control policy for configuration parameters**] on: [**assignment:**
- subjects: S_APPLI, S_FLOW, S_AUDIT, S_ADMIN
- objects: D_AC_PARAM, D_CONFIG, D_SEC_PAR, D_MON_PAR, D_APPLI_FILTER, D_FLOW_FILTER
- operations: C, W, R, D, B].

FDP_ACF.1 (PAR) Security attribute-based access control (access to configuration parameters)

Audit *- Refusal or acceptance of the access request (associated data: identity inherited by the user, object concerned and security attributes used)*
- Saving (associated data: result of the operation, type of data saved)
Dependencies *FDP_ACC.1 (PAR)*
FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [**assignment: access control policy for configuration parameters**] to objects based on the following: [**assignment:**
- subjects: S_APPLI, S_FLOW, S_AUDIT, S_ADMIN
- objects: D_AC_PARAM, D_CONFIG, D_SEC_PAR, D_MON_PAR, D_APPLI_FILTER, D_FLOW_FILTER
- security attributes: SA_IDENT, SA_ROLE, SA_USER, SA_DIGEST, SA_PROG_ID, SA_NETWORK, SA_ADAPTIVITY, SA_LEVEL].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment: there exists at least one access control rule selected in Table 5: Access control rules**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment: no rules that explicitly authorise access of subjects to objects**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**assignment: there exists at least one control access rule selected in Table 5: Access control rules prohibiting this access**].

6.2.3.2 Filtering rule access control

FDP_ACC.1 (FI) Subset access control (access to filtering rules)

Audit *- No audit messages for this component*
Dependencies *FDP_ACF.1 (FI)*

FDP_ACC.1.1 The TSF shall enforce the [**assignment: access control policy for filtering rules**] on: [**assignment:**
- subjects: S_APPLI, S_FLOW, S_COMM, S_ADMIN
- objects: D_AC_PARAM, D_FLOW_IN, D_FLOW_OUT, D_APPLI_FILTER, D_FLOW_FILTER
- operations: C, W, R, D].

FDP_ACF.1 (FI) Security attribute-based access control (access to filtering rules)

Audit *- Refusal or acceptance of the access request (associated data: identity inherited by the user, object concerned and security attributes used)*
- Saving (associated data: result of the operation, type of data saved)
Dependencies *FDP_ACC.1 (FI)*
FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [**assignment: access control policy for filtering rules**] to objects based on the following: [**assignment:**
- subjects: S_APPLI, S_FLOW, S_COMM, S_ADMIN
- objects: D_AC_PARAM, D_FLOW_IN, D_FLOW_OUT, D_APPLI_FILTER, D_FLOW_FILTER
- security attributes: SA_IDENT, SA_ROLE, SA_USER, SA_DIGEST, SA_PROG_ID, SA_NETWORK, SA_ADAPTIVITY, SA_LEVEL].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment: there exists at least one control access rule selected in Table 5: Access control rules**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment: no rules that explicitly authorise access of subjects to objects**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment**: there exists at least one control access rule selected in Table 5: Access control rules prohibiting this access**].

6.2.3.3 Other TOE data protection

FDP_RIP.1 Subset residual information protection

Audit *- No audit messages for this component*
Dependencies *none*

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**selection: deallocation of the resource from**] the following objects: [**assignment: D_APPLI_FILTER, D_FLOW_FILTER, D_AC_PARAM, D_FLOW_AUDIT**].

6.2.4 TOE administration

FMT_MSA.1 Management of security attributes

Audit *- Any request (accepted or refused) for access to a security attribute (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*

Dependencies *FDP_IFC.1 (OAF) + FDP_IFC.1 (ONF) + FDP_IFC.1 (INF) + FDP_IFC (IAF) FMT_SMR.1 and FMT_SMF.1*

FMT_MSA.1.1 The TSF shall enforce the [**assignment: access control policy for filtering rules and access control policy for configuration parameters**] to restrict the ability to [**selection: change_default, query, modify, delete**] the security attributes: [**assignment:**
- 1. D_APPLI_FILTER, D_FLOW_FILTER: In order to read or modify the security attributes of these objects, the attribute SA_LEVEL of the object shall have the "SPECIFIC" value, the SA_USER attribute of the subject and of the object shall be equal and the SA-ADAPTIVITY attribute shall have the value "ADAPTIVE"
- 2. D_AC_PARAM, D_CONFIG: The security attributes of these objects are not modifiable
- 3. D_SEC_PAR, D_MON_PAR: The security attributes of these objects are not modifiable
- 4. D_FLOW_AUDIT, D_ADMIN_AUDIT, D_ALARM: The security attributes of these objects are not modifiable
- 5. D_FLOW_IN, D_FLOW_OUT: In order to read or modify the security attributes of these objects, the security attribute SA_IDENT of the subject shall have the value "S_APPLI" or "S_FLOW"]
to [**assignment: ADMINISTRATOR, SUPERVISOR, BASIC USER**].

Application note:
The STs in conformity with this PP shall detail or supplement these rules.

FMT_SMR.1 Security roles

Audit *- Any modification to the role held by a user (Associated data: user identity, role, status or result of the request)*

Dependencies *FIA_UID.1 (covered by FIA_UID.2 (LU) and FIA_UID.2 (RU))*

FMT_SMR.1.1 The TSF shall maintain the roles [**assignment: ADMINISTRATOR, SUPERVISOR, BASIC USER**].

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

FMT_SMF.1 Specification of Management Functions

Audit: *- Any request (accepted or refused) for access to a management function (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*

Dependencies *none*

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**assignment:**
- 1. Monitoring of the TOE and display of the filtering policy.
- 2. Management of the audit and display parameters for audit messages.
- 3. Management of TOE users (basic users, administrators, supervisors).
- 4. Management of the filtering policy.
- 5. Management of TOE configuration parameters].

FMT_MSA.3 Static attribute initialisation

Audit *- Any request (accepted or refused) for modification to the initial value of a security attribute (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*

Dependencies *FMT_MSA.1 and FMT_SMR.1*

FMT_MSA.3.1 The TSF shall enforce the [**assignment: filtering policies**] to provide [**selection: restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment: ADMINISTRATOR, BASIC USER**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 Security attribute value inheritance

Audit *- Creation of an object or of a subject (associated data: identity of the subject or of the object + list of security attributes)*

Dependencies *FDP_IFC.1 (OAF) + FDP_IFC.1 (ONF) + FDP_IFC.1 (INF) + FDP_IFC (IAF)*

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes: [**assignment:**
- 1. Creation of a D_APPLI_FILTER or D_FLOW_FILTER object:
- where the SA_ROLE attribute of the subject (S_ADMIN) is different from "ADMINISTRATOR", the attribute SA_LEVEL takes as its value the identity of the user and the attribute SA_ADAPTIVITY takes as its value "ADAPTIVE"
- where the SA_ROLE of the subject (S_ADMIN) is "ADMINISTRATOR", the attribute SA_LEVEL takes as its value " GLOBAL"
- for D_APPLI_FILTER, the attribute SA_DIGEST takes the value calculated by the TOE for this program

- 2. Creation of a D_FLOW_AUDIT or D_ADMIN_AUDIT object: the SA_DIGEST attribute takes the value calculated by the TOE. This attribute makes it possible to control of the integrity of the object and the linking of this message with previous objects of the same type (i.e. D_FLOW_AUDIT or D_ADMIN_AUDIT)].

Application note:

The STs in conformity with this PP must provide a list of the other rules implemented for initialising security attributes when subjects or objects are created.
The STs in conformity with this PP must state the calculation method of the integrity check value of the program and the scope of this integrity check value.
The STs in conformity with this PP must state the calculation method of the integrity check value corresponding to a D_FLOW_AUDIT or D_ADMIN_AUDIT object and the scope of this integrity check value.

6.2.5 Security of administration or monitoring data transmission

The following requirements contribute to establishing a trusted channel between the TOE and a remote administration or monitoring site.

FIA_UID.2 (TC) User identification before any action (trusted channel)

Audit *- Connection of a remote program (associated data: identification of the program, connection context)*
Dependencies *none*

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.

Refinement *The TSF shall require that any remote program (U_REMOTE_PROGRAM) wishing to communicate with the administration and monitoring module (S_ADMIN) be successfully identified before the latter can establish a link with the communication module (S_COMM).*

FIA_UAU.2 (TC) User authentication before any action (mutual authentication)

Audit *- Authentication attempt (successful or not) of a remote program.*
Dependencies *FIA_UID.1 (RP)*

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.

Refinement *The TSF shall authenticate all remote programs (U_REMOTE_PROGRAM) making a connection for administration or monitoring purposes before the latter can establish a link with the communication module (S_COMM).*

FIA_USB.1 (TC) User-subject binding (trusted channel)

Audit *- Establishment of a link between a remote program and a subject (associated data: identification of the program, identification of the subject, values of the security attributes defined when establishing the link).*
Dependencies *FIA_ATD.1 (TC)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**assignment: security attributes: SA_ENVIRONMENT, SA_NETWORK**].

Refinement *The TSF shall associate the following security attributes to the communication module (S_COMM) following the establishment of a link between a remote program (U_REMOTE_PROGRAM) and the communication module (S_COMM): SA_ENVIRONMENT, SA_NETWORK*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**assignment: the security attributes of S_COMM are updated according to the security properties of U_REMOTE_PROGRAM in the following manner:**
1. SA_ENVIRONMENT = value corresponding to the network environment of the workstation ("IN" or "OUT"); this value is supplied by the workstation
2. SA_NETWORK is assigned the values relative to the network connection. These values are calculated by the TOE according to information taken from the requested network connection].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**assignment: no additional rules for the changing of attributes**].

FIA_ATD.1 (TC) User attribute definition (trusted channel)

Audit *- No audit messages for this component*
Dependencies *none*

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment: security attributes: SA_ENVIRONMENT, SA_NETWORK**].

FTA_SSL.3 (TC) TSF-initiated termination (trusted channel)

Audit *- Closing of an interactive session by the TSF (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the interactive session)*
Dependencies *none*

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [**assignment: time interval of user inactivity**].

Refinement *The TSF shall put an end to the link between a remote program and the communication module (S_COMM) under the following conditions:*
1. A break in the network connection between the remote site and the TOE.
2. Shutdown of the TOE.

3. A break in the trusted channel (following the detection of an anomaly on this channel for example) established between the TOE and the remote program and used by this link.
4. Other conditions.

Application note:
The STs in conformity with this PP must specify the conditions that can lead to a break in the link by the TSF.

FTA_SSL.4 (TC) User-initiated termination (trusted channel)

Audit *- Closing of an interactive session by a remote program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)*
Dependencies *none*

FTA_SSL.4.1 The TSF shall allow [**refinement: remote program**]-initiated termination of the [**refinement: remote program**]'s own interactive session.

FPT_ITI.1 Inter-TSF detection of modification

Audit *- Result of the detection of a modification, deletion or insertion of data (associated data: result of detecting an anomaly, corrupted data)*
- Action taken (issuing of an alert)
Dependencies *none*

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [**assignment: detection of any anomaly, such as the modification, deletion or insertion of data in messages relative to D_FLOW_FILTER, D_APPLI_FILTER, D_CONFIG, D_AC_PARAM, D_ALARM, D_FLOW_AUDIT, D_ADMIN_AUDIT, D_FLOW_IN, D_FLOW_OUT, D_MON_PAR, D_SEC_PAR**].

Application note:
The STs in conformity with this PP must specify the anomalies taken into account and the mechanisms used.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [**assignment: Issuing an alert**] if modifications are detected.

FPT_RPL.1 Replay detection

Audit *- Result of the detection of a replay attack (associated data: result of the detection of an attack, the element replayed, the network address of the source of replay)*
- Action taken (issuing of an alert)
Dependencies *none*

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [**assignment: administration or monitoring commands received from a remote program**].

FPT_RPL.1.2 The TSF shall perform [**assignment: ignore the message and issue an alarm**] when replay is detected.

FPT_ITC.1 Inter-TSF confidentiality during transmission

Audit *- No audit messages for this component*

Dependencies *none*

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

Refinement *The TSF shall protect the confidentially of data transmitted across the network by the communication module (S_COMM) to a remote program (U_REMOTE_PROGRAM) linked to this subject when this data emanates from the administration and monitoring module (S_ADMIN).*
Data concerned: D_ALARM, D_FLOW_AUDIT, D_ADMIN_AUDIT, D_AC_PARAM, D_CONFIG, D_SEC_PAR, D_MON_PAR

Application note:
STs in conformity with this PP must detail the methods used.

FTP_ITC.1 Inter-TSF trusted channel

Audit *- Authentication by the TOE of a remote program (associated data: success or failure of the operation, identity of the remote program)*
- Any anomaly detected during communication between the TOE and a remote user (associated data: determination of a user's identity, corrupted data)

Dependencies *None*

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 [**selection: a remote program (U_REMOTE_PROGRAM)**] to initiate communication via the trusted channel.

Application note:
The STs in conformity with this PP must state the authentication method used.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**assignment: ensuring the confidentiality and controlling the integrity of data (data concerned: D_AC_PARAM, D_CONFIG, D_SEC_PAR, D_MON_PAR, D_FLOW_FILTER, D_APPLI_FILTER) shared between the communication module (S_COMM) and a remote program (U_REMOTE_PROGRAM) to which it is linked**

through the network when this data is intended for the administration and monitoring module (S_ADMIN)].

Application note:
The STs in conformity with this PP must state the methods used (for ensuring confidentiality and controlling integrity) and the anomalies taken into account.

FPT_TDC.1 Inter-TSF basic TSF data consistency

Audit *- Result of using the mechanisms ensuring the coherency TSF data*
Dependencies none

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**assignment: list of TSF data types**] when shared between the TSF and another trusted IT product.

Application note:
The STs in conformity with this PP must detail the data requiring interpretation.

FPT_TDC.1.2 The TSF shall use [**assignment: list of interpretation rules to be applied by the TSF**] when interpreting the TSF data from another trusted IT product.

Application note:
The STs in conformity with this PP must detail the interpreting rules.

6.2.6 Audit and logging

The following components contribute to the implementation of the audit function, logging, the detection of attacks and responses to attacks.

FAU_GEN.1 Audit data generation

Audit *- No audit messages for this component*
Dependencies FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions
b) All auditable events for the [**selection: operations (defined each component) giving rise to the creation of an audit message (see Table 6: List of audited events by component)**] level of audit; and
c) [**assignment: other specifically defined auditable events**].

Application note:
The STs in conformity with this PP must provide an accurate list of audited events and operations giving rise to the recording of an audit message.

Component	Associated audit messages
FDP_IFC.1 (ONF)	*- No audit messages for this component*
FDP_IFF.1 (ONF)	*- Refusal of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)*

Component	Associated audit messages
	- Acceptance of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)
FDP_ETC.2 (ONF)	*- Detail of the export request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))*
FDP_IFF.5 (ONF)	*- Result of the identification of an illicit information bypass flow*
FDP_IFC.1 (INF)	*- No audit messages for this component*
FDP_IFF.1 (INF)	*- Refusal of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)*
	- Acceptance of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)
FDP_ITC.1 (INF)	*- Detail of the import request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))*
FDP_IFF.5 (INF)	*- Result of the identification of an illicit information bypass flow*
FDP_IFC.1 (OAF)	*- No audit messages for this component*
FDP_IFF.1 (OAF)	*- Refusal of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)*
	- Acceptance of an outgoing access request (associated data: identity inherited by the user, object concerned and security attributes used)
FDP_ITC.1 (OAF)	*- Detail of the import request (associated data: identity of requestor, remote site concerned and result of the request (acceptance or refusal))*
FDP_IFF.5 (OAF)	*- Result of the identification of an illicit information bypass flow*
FTA_TSE.1 (OAF)	*- Refusal to establish a link for a local program (associated data: reason for the refusal, security parameters used and the security rule on which refusal to establish a link is based)*
FDP_IFC.1 (IAF)	*- No audit messages for this component*
FDP_IFF.1 (IAF)	*- Refusal of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)*
	- Acceptance of an incoming access request (associated data: identity inherited by the user, object concerned and security attributes used)
FDP_ETC.2 (IAF)	*- Detail of the request (associated data: filtering rule and attributes upon which acceptance or refusal of the packet is based, status (acceptance or refusal))*
FDP_IFF.5 (IAF)	*- Result of the identification of an illicit information bypass flow*
FIA_UID.2 (LP)	*- Connection of a local program (associated data: identification of the program, connection context)*
FIA_USB.1 (LP)	*- Establishment of a link between a local program and a subject (associated data: identification of the program, identification of the subject, values of the security attributes defined when establishing the link)*
FIA_ATD.1 (LP)	*- No audit messages for this component*
FTA_SSL.4 (LP)	*- Closing of an interactive session by a local program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)*
FIA_UID.1 (RP)	*- Anonymous connection of a remote program (associated data: connection context)*
FIA_USB.1 (RP)	*- Establishment of a link between a remote program and a subject (associated data: identification of the subject, values of the security attributes defined when establishing the link)*
FIA_ATD.1 (RP)	*- No audit messages for this component*
FTA_SSL.4 (RP)	*- Closing of an interactive session by a remote program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)*
FMT_MTD.1	*- Recording of a new user*
	- Access (successful or not for reading, writing or modification) to a user's properties
FMT_MTD.3	*- Refusal of authentication data or security properties relative to user management*
FIA_SOS.1	*- Acceptance or refusal of the authentication data supplied*
FIA_SOS.2	*- Generation of authentication data*
FIA_UID.2 (LU)	*- Connection of a local user (associated data: user identity, connection context)*
FIA_UID.2 (RU)	*- Connection of a remote user (associated data: user identity, connection context)*
FIA_UAU.2 (LU)	*- Authentication attempt (successful or not) of a local user*
FIA_UAU.2 (RU)	*- Authentication attempt (successful or not) of a remote user*
FIA_UAU.7	*- No audit messages for this component*
FIA_AFL.1	*- Reaching or exceeding one of the alert thresholds during connection (associated data: threshold, number of attempts)*
	- Actions taken (issuing of an alert, blocking of the connection, etc.)
FTA_TSE.1 (LU)	*- Refusal to establish a link between a local user and a subject (associated data: reason for the refusal, security parameters upon which acceptance or refusal of the establishment of the link are based)*
FTA_TSE.1 (RU)	*- Refusal to establish a link between a remote user and a subject (associated data: reason*

Component	Associated audit messages
	for the refusal, security parameters upon which acceptance or refusal of the establishment of the link are based)
FIA_USB.1 (LU)	*- Establishment of a link between a user and a subject (associated data: identification of the user, identification of the subject, values of the security attributes defined when establishing the link)*
FIA_ATD.1 (LU)	*- No audit messages for this component*
FIA_USB.1 (RU)	*- Establishment of a link between a remote user and a subject (associated data: identification of the user, identification of the subject, values of the security attributes defined when establishing the link)*
FIA_ATD.1 (RU)	*- No audit messages for this component*
FTA_SSL.3 (RU)	*- Closing of an interactive session by the TSF (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the interactive session)*
FTA_SSL.4 (LU)	*- Closing of an interactive session by a local user (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the session)*
FTA_SSL.4 (RU)	*- Closing of an interactive session by a remote user (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the session)*
FDP_ACC.1 (PAR)	*- No audit messages for this component*
FDP_ACF.1 (PAR)	*- Refusal or acceptance of the access request (associated data: identity inherited by the user, object concerned and security attributes used)* *- Saving (associated data: result of the operation, type of data saved)*
FDP_ACC.1 (FI)	*- No audit messages for this component*
FDP_ACF.1 (FI)	*- Refusal or acceptance of the access request (associated data: identity inherited by the user, object concerned and security attributes used)* *- Saving (associated data: result of the operation, type of data saved)*
FDP_RIP.1	*- No audit messages for this component*
FMT_MSA.1	*- Any request (accepted or refused) for access to a security attribute (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*
FMT_SMR.1	*- Any modification to the role held by a user (Associated data: user identity, role, status or result of the request)*
FMT_SMF.1	*- Any request (accepted or refused) for access to a management function (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*
FMT_MSA.3	*- Any request (accepted or refused) for modification to the initial value of a security attribute (associated data: identity of the subject, identity of the user, object, attribute, value, type of access requested, status or result of the request)*
FMT_MSA.4	*- Creation of an object or of a subject (associated data: identity of the subject or of the object + list of security attributes)*
FIA_UID.2 (TC)	*- Connection of a remote program (associated data: identification of the program, connection context)*
FIA_UAU.2 (TC)	*- Authentication attempt (successful or not) of a remote program*
FIA_USB.1 (TC)	*- Establishment of a link between a remote program and a subject (associated data: identification of the program, identification of the subject, values of the security attributes defined when establishing the link).*
FIA_ATD.1 (TC)	*- No audit messages for this component*
FTA_SSL.3 (TC)	*- Closing of an interactive session by the TSF (associated data: identification of the user, identification of the subject, values of the security attributes defined when closing the interactive session)*
FTA_SSL.4 (TC)	*- Closing of an interactive session by a remote program (associated data: identification of the subject, values of the security attributes defined during the closing of the session)*
FPT_ITI.1	*- Result of the detection of a modification, deletion or insertion of data (associated data: result of detecting an anomaly, corrupted data)* *- Action taken (issuing of an alert)*
FPT_RPL.1	*- Result of the detection of a replay attack (associated data: result of the detection of an attack, the element replayed, the network address of the source of replay)* *- Action taken (issuing of an alert)*
FPT_ITC.1	*- No audit messages for this component*
FTP_ITC.1	*- Authentication by the TOE of a remote program (associated data: success or failure of the operation, identity of the remote program)* *- Any anomaly detected during communication between the TOE and a remote user*

Component	Associated audit messages
	(associated data: determination of a user's identity, corrupted data)
FPT_TDC.1	*- Result of using the mechanisms ensuring the coherency TSF data*
FAU_SAA.1	*- Rejection of an incoming connection (associated data: reason for refusal, connection context)*
FAU_SAA.3	*- Rejection of an incoming connection (associated data: reason for refusal, connection context)*
FAU_SAR.1 (SUP)	*- No audit messages for this component*
FAU_SAR.1 (USR)	*- No audit messages for this component*
FAU_SAR.2	*- An unsuccessful attempt to read audit data (associated data: identification of the user*
FAU_SAR.3	*- No audit messages for this component*
FAU_ARP.1	*- Actions taken by the TSF following the detection of a potential violation of the security policy (associated data: type of violation, action taken)*
FAU_STG.1	*- No audit messages for this component*
FAU_STG.4	*- Reaching the maximum size for an audit file (associated data: size reached)* *- Action(s) taken by the TSF in the event of reaching the maximum size for an audit file (associated data: audit file)*
FPT_TST.1	*- Results and details of tests undertaken*
FRU_RSA.1 (RES)	*- Reaching of a quota for the number of simultaneous network connections (associated data: quota reached)*

Table 6: List of audited events by component

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment: any other relevant information connected to this operation or event (see Table 6: List of audited events by component)**].

Application note:
The STs in conformity with this PP must provide a detailed and exhaustive list of recorded information.

FAU_GEN.2 User identity association

Audit *- No audit messages for this component*
Dependencies *FAU_GEN.1 and FIA_UID.1 (RP)*

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

Application note:
The STs in conformity with this PP must provide an accurate list of audited events and operations giving rise to the recording of the user's identity in an audit message.

FAU_SAA.1 Potential violation analysis

Audit: *- Rejection of an incoming connection (associated data: reason for refusal, connection context)*
Dependencies *FAU_GEN.1 Audit data generation*

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

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [**assignment: more than N3 "Refusal of an incoming access request (associated data: inherited identity of the user, object concerned, security attributes used)" in the last N4 minutes**] known to indicate a potential security violation
b) [**assignment: any other rules**].

Application note:
The STs in conformity with this PP must specify the selected or possible values for N3 and N4 as well as the other rules used.

FAU_SAA.3 Simple attack heuristics

Audit *- Rejection of an incoming connection (associated data: reason for refusal, connection context)*
Dependencies *none*

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events: [**assignment:**
- 1. Number of simultaneous connections from the network greater than N5.
- 2. Number of refusals for an incoming access request from a same remote system greater than N3 in the last N4 minutes.
- 3. Other events
that may indicate a violation of the enforcement of the SFRs.

Application note:
The STs in conformity with this PP must provide the list of events chosen and specify the selected or possible values for N3, N4 and N5.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [**assignment:**
- 1. Number of active connections.
- 2. Number of connection attempts having taken place in fewer than N4 minutes.
- 3. Other information.]

Application note:
The STs in conformity with this PP must specify what this other information is.

FAU_SAA.3.3 The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

FAU_SAR.1 (SUP) Audit review

Audit *- No audit messages for this component*

Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**assignment: users holding a SUPERVISOR role**] with the capability to read [**assignment: audit messages and alarm messages**] from the audit records.

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

FAU_SAR.1 (USR) Audit review (user access)

Audit - No audit messages for this component
Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**assignment: users with an "audit" right**] with the capability to read [**assignment: audit messages and alerts**] from the audit records.

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

FAU_SAR.2 Restricted audit review

Audit - An unsuccessful attempt to read audit data (associated data: identification of the user
Dependencies FAU_SAR.1 Audit review

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

FAU_SAR.3 Selectable audit review

Audit - No audit messages for this component
Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**assignment: methods of selection and/or ordering**] of audit data based on [**assignment: criteria with logical relations**].

Application note:
The STs in conformity with this PP must specify the available selection and viewing methods and which selection criteria can be used.

FAU_ARP.1 Security alarms

Audit - Actions taken by the TSF following the detection of a potential violation of the security policy (associated data: type of violation, action taken)
Dependencies FAU_SAA.1

FAU_ARP.1.1 The TSF shall take [**assignment: actions defined by the administrator**] upon detection of a potential security violation.

Application note:
The STs in conformity with this PP must specify the action that an administrator can select in response to a potential violation of the security policy.

FAU_STG.1 Prevention of audit data loss

Audit *- No audit messages for this component*
Dependencies *FAU_GEN.1*

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.1 The TSF shall be able to [selection: prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Audit *- Reaching the maximum size for an audit file (associated data: size reached)*
- Action(s) taken by the TSF in the event of reaching the maximum size for an audit file (associated data: audit file)
Dependencies *FAU_STG.1*

FAU_STG.4.1 The TSF shall [**selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"**] and [**assignment: other actions to be taken in case of audit storage failure**] if the audit trail is full.

Refinement *The files concerned are audit files (D_FLOW_AUDIT, D_ADMIN_AUDIT) and the alert file (D_ALARM).*
Application note:
- The STs in conformity with this PP must detail which actions are taken when one of the audit files is full
- The STs in conformity with this PP must specify the maximum sizes for audit and alert files or how they are managed

6.2.7 TOE reliability and availability

FPT_TST.1 TSF testing

Audit *- Results and details of tests undertaken*
Dependencies *none*

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

Application note:
The STs in conformity with this PP must detail the tests undertaken and give a list of the TSF components tested.

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

Application note:
The STs in conformity with this PP must detail the mechanisms used for carrying out this integrity inspection and give a list of TOE components that have undergone an integrity check.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

FRU_RSA.1 (RES) Maximum quotas (incoming access)

Audit - Reaching of a quota for the number of simultaneous network connections (associated data: quota reached)
Dependencies none

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [**assignment: network access from remote sites**] that [**selection: remote programs (U_REMOTE_PROGRAM)] can use [selection: simultaneously**].
Application note:
The STs in conformity with this PP must specify the possible values for these quotas.

6.3 Security assurance requirements for the TOE

The TOE shall be evaluated according to EAL3 augmented by components ALC_FLR.3 and AVA_VAN.3.

This corresponds to the assurance package provided for the standard level qualification of a security target (see [QUALIF_STD]) defined by the "QS" column of the following table:

Assurance classes	Assurance families	Assurance components for each evaluation level							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
Development	ADV_ARC		1	**1**	1	1	1	1	**1**
	ADV_FSP	1	2	**3**	4	5	5	6	**3**
	ADV_IMP				1	1	2	2	
	ADV_INT					2	3	3	
	ADV_SPM						1	1	
	ADV_TDS		1	**2**	3	4	5	6	**2**
Guidance documents	AGD_OPE	1	1	**1**	1	1	1	1	**1**
	AGD_PRE	1	1	**1**	1	1	1	1	**1**
Life-cycle support	ALC_CMC	1	2	**3**	4	4	5	5	**3**
	ALC_CMS	1	2	**3**	4	5	5	5	**3**
	ALC_DEL		1	**1**	1	1	1	1	**1**
	ALC_DVS			**1**	1	1	2	2	**1**

Assurance classes	Assurance families	Assurance components for each evaluation level							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
	ALC_FLR								**3**
	ALC_LCD			**1**	1	1	1	2	**1**
	ALC_TAT				1	2	3	3	
Security Target evaluation	ASE_CCL	1	1	**1**	1	1	1	1	**1**
	ASE_ECD	1	1	**1**	1	1	1	1	**1**
	ASE_INT	1	1	**1**	1	1	1	1	**1**
	ASE_OBJ	1	2	**2**	2	2	2	2	**2**
	ASE_REQ	1	2	**2**	2	2	2	2	**2**
	ASE_SPD		1	**1**	1	1	1	1	**1**
	ASE_TSS	1	1	**1**	1	1	1	1	**1**
Tests	ATE_COV		1	**2**	2	2	3	3	**2**
	ATE_DPT			**1**	2	3	3	4	**1**
	ATE_FUN		1	**1**	1	1	2	2	**1**
	ATE_IND	1	2	**2**	2	2	2	3	**2**
Vulnerability assessment	AVA_VAN	1	2	2	**3**	4	5	5	**3**

Table 7: Requirements for the standard level qualification of a ST

Application note: STs in conformity with this PP must respect the assurance package required for the standard level qualification.

6.4 Rationale

6.4.1 Security requirements / Security objectives

6.4.1.1 Coverage of security objectives for the TOE

	OT_filtering_level	OT_filtering_criteria	OT_application_integrity	OT_administration	OT_monitoring	OT_roles	OT_identification	OT_authentication	OT_access_control	OT_TOE_reuse	OT_log_protection	OT_remote_admin_authentication	OT_remote_admin_integrity	OT_remote_admin_confidentiality	OT_remote_admin_no_replay	OT_flow_audit	OT_admin_audit	OT_violation_detection	OT_violation_reaction	OT_TOE_integrity	OT_operational_state	OT_crypto
FDP_IFC.1 (ONF)	X	X																				
FDP_IFF.1 (ONF)	X	X																				
FDP_ETC.2 (ONF)	X	X																				
FDP_IFF.5 (ONF)	X	X																				
FDP_IFC.1 (INF)	X	X																				
FDP_IFF.1 (INF)	X	X																				
FDP_ITC.1 (INF)	X	X		X	X																	
FDP_IFF.5 (INF)	X	X																				
FDP_IFC.1 (OAF)	X	X																				
FDP_IFF.1 (OAF)	X	X																				
FDP_ITC.1 (OAF)	X	X																				
FDP_IFF.5 (OAF)	X	X																				
FTA_TSE.1 (OAF)			X																			
FDP_IFC.1 (IAF)	X	X																				
FDP_IFF.1 (IAF)	X	X																				
FDP_ETC.2 (IAF)	X	X																				

	OT_filtering_level	OT_filtering_criteria	OT_application_integrity	OT_administration	OT_monitoring	OT_roles	OT_identification	OT_authentication	OT_access_control	OT_TOE_reuse	OT_log_protection	OT_remote_admin_authentication	OT_remote_admin_integrity	OT_remote_admin_confidentiality	OT_remote_admin_no_replay	OT_flow_audit	OT_admin_audit	OT_violation_detection	OT_violation_reaction	OT_TOE_integrity	OT_operational_state	OT_crypto
FDP_IFF.5 (IAF)	X	X																				
FIA_UID.2 (LP)	X	X	X																			
FIA_USB.1 (LP)	X	X																				
FIA_ATD.1 (LP)	X	X	X																			
FTA_SSL.4 (LP)	X	X							X													
FIA_UID.1 (RP)	X	X																				
FIA_USB.1 (RP)	X	X																				
FTA_SSL.4 (RP)	X	X																				
FIA_ATD.1 (RP)	X	X																				
FMT_MTD.1				X	X	X	X	X														
FMT_MTD.3				X	X	X	X	X														
FIA_SOS.1				X	X			X														X
FIA_SOS.2				X	X			X														X
FIA_UID.2 (LU)				X	X		X															
FIA_UID.2 (RU)				X	X		X															
FIA_UAU.2 (LU)				X	X			X														
FIA_UAU.2 (RU)				X	X			X														
FIA_UAU.7				X	X			X	X			X										
FIA_AFL.1				X	X			X										X	X			
FTA_TSE.1 (RU)				X	X		X															
FTA_TSE.1 (LU)				X	X		X															
FIA_USB.1 (LU)				X	X	X	X															
FIA_ATD.1 (LU)				X	X	X	X															
FIA_USB.1 (RU)				X	X	X	X															
FIA_ATD.1 (RU)				X	X	X	X															
FTA_SSL.3 (RU)				X	X		X		X													
FTA_SSL.4 (LU)				X	X		X		X													
FTA_SSL.4 (RU)				X	X		X		X													
FDP_ACC.1 (FI)				X	X				X													
FDP_ACF.1 (FI)				X	X				X													
FDP_ACC.1 (PAR)				X	X				X		X					X	X					
FDP_ACF.1 (PAR)				X	X				X		X					X	X					
FMT_MSA.1	X	X		X	X				X													
FMT_SMR.1						X																
FMT_SMF.1				X	X		X	X	X								X					
FMT_MSA.3	X	X		X	X				X													
FMT_MSA.4	X	X		X	X				X													
FDP_RIP.1										X												
FIA_UID.2 (TC)												X										
FIA_UAU.2 (TC)												X										X
FTP_ITC.1												X	X	X	X							X
FIA_USB.1 (TC)												X	X	X	X							
FIA_ATD.1 (TC)												X	X	X	X							
FTA_SSL.3 (TC)									X			X	X	X	X							
FTA_SSL.4 (TC)									X			X	X	X	X							
FPT_ITI.1											X		X									
FPT_RPL.1															X							
FPT_ITC.1														X								X
FPT_TDC.1	X	X		X	X																	

	OT_filtering_level	OT_filtering_criteria	OT_application_integrity	OT_administration	OT_monitoring	OT_roles	OT_identification	OT_authentication	OT_access_control	OT_TOE_reuse	OT_log_protection	OT_remote_admin_authentication	OT_remote_admin_integrity	OT_remote_admin_confidentiality	OT_remote_admin_no_replay	OT_flow_audit	OT_admin_audit	OT_violation_detection	OT_violation_reaction	OT_TOE_integrity	OT_operational_state	OT_crypto
FAU_GEN.1																X	X					
FAU_GEN.2																X	X					
FAU_SAA.1																		X				
FAU_SAA.3																		X				
FAU_SAR.1 (SUP)																X	X					
FAU_SAR.1 (USR)																X	X					
FAU_SAR.2																X	X					
FAU_SAR.3																X	X					
FAU_ARP.1																			X			
FAU_STG.1											X											
FAU_STG.4											X											
FPT_TST.1																				X	X	
FRU_RSA.1 (RES)																		X	X			

Table 8: security functional requirements / security objectives for the TOE

OT_filtering_level, OT_filtering_criteria

FDP_IFF.1 (OAF, IAF, ONF, INF) define the filtering policies to be applied.

FDP_ICF.1 (OAF, IAF, ONF, INF) specify that the TOE implements these filtering policies.

FDP_ETC.2 (ONF, IAF) specify which filtering rules must be implemented for flows leaving the TOE (i.e. network filtering of outgoing flows and application filtering of incoming flows).

FDP_ITC.1 (INF) and **FDP_ITC.1 (OAF)** specify which filtering rules are to be implemented for flows emanating from outside the TOE (i.e. application filtering of outgoing flows and network filtering of incoming flows).

FDP_IFF.5 (OAF, IAF, ONF, INF) ensure that the TOE controls all incoming and outgoing flows without exception (i.e. no by-pass)

FPT_TDC.1 details the data needing to be interpreted and the interpreting rules for mechanisms ensuring the coherency of TSF data.

FIA_UID.1 (RP) specifies that remote programs (other than those used for remote administration or remote monitoring) do not need to identify themselves before establishing a link with the TOE.

FIA_UID.2 (LP) specifies that local programs need to identify themselves before establishing a link with the TOE.

FIA_USB.1 (LP, RP) and FIA_ATD.1 (LP, RP) define the inheritance rules of security attributes for the application filtering module and the network filtering module.

FTA_SSL.4 (LP) and **FTA_SSL.4 (RP)** specify that local or remote programs can end their interactive session.

FMT_MSA.1, **FMT_MSA.3** and **FMT_MSA.4** specify the rules relative to the

definition or modification of security attributes.

OT_application_integrity

FIA_UID.2 (LP) specifies that local programs need identify themselves before establishing a link with the TOE, thereby enabling the TOE to search for the associated integrity check value for comparison.

FIA_ATD.1 (LP) specifies that the TOE manages the integrity check values associated with local programs.

FTA_TSE.1 (OAF) implements the integrity check for local programs seeking to make outgoing connections. **FTA_TSE.1 (OAF)** issues an audit message in the event of the corruption of a local program.

OT_administration, OT_monitoring

FMT_MTD.1 and **FMT_MTD.3** specify the recording conditions of users; **FIA_SOS.1** and **FIA_SOS.2** define criteria relative to user authentication data.

FMT_MSA.1, **FMT_MSA.3** and **FMT_MSA.4** specify the rules relative to the definition of security attributes.

FPT_TDC.1 details the data needing to be interpreted and the interpreting rules for mechanisms ensuring the coherency of data exchanged within the context of remote monitoring and remote administration.

FIA_UID.2 (LU, RU) specify that the TOE begins by identifying users before taking any other action; **FIA_UAU.2 (LU, RU)** specify that the TOE authenticates users before establishing a link. **FIA_UAU.7** specifies that the TOE shall not provide any information to the user as long as this user is not authenticated. **FIA_AFL.1** specifies the conditions required for the TOE to signal user connection errors.

FDP_ITC.1 (INF) specifies the rules authorising the transmission of data to the communication module.

FTA_TSE.1 (LU, RU) specify the rules for establishing a link between a user and the TOE.

FIA_USB.1 (LU, RU) and **FIA_ATD.1 (LU, RU)** specify the rules for the allocation of security attributes enabling authorised users to access the functions they are allowed to use.

FDP_ACC.1 (PAR, FI) and **FDP_ACF.1 (PAR, FI)** present the rules enabling authorised users to gain access to data they are responsible for managing.

FMT_SMF.1 specifies that the TOE logs and records the use of administration and monitoring functions.

FTA_SSL.3 (RU) and **FTA_SSL.4 (LU, RU)** define the conditions relative to a break in the connection between a user and the TOE that results in the blocking of access authorisation for this user via the administration and monitoring module.

OT_roles

FMT_MTD.1, **FMT_MTD.3** and **FMT_SMR.1** specify user recording conditions and also stipulate which roles can be allocated to the user.

FIA_USB.1 (LU, RU) and **FIA_ATD.1 (LU, RU)** specify the rules governing the allocation of security attributes (including the role) according authorised users access to the functions they are allowed to use.

OT_identification

FMT_MTD.1 and **FMT_MTD.3** specify the recording conditions for users.

FIA_UID.2 (LU, RU) specify that the TOE begins by identifying users before any other action.

FTA_TSE.1 (LU, RU) define the conditions under which the establishment of a session can be refused to a local or remote user.

FIA_USB.1 (LU, RU) specify that the TOE associates security attributes to sessions in order to control what local and remote users can do.

FIA_ATD.1 (LU, RU) specify which security attributes are to be maintained for local or remote users.

FTA_SSL.3 (RU) specifies that the TOE can terminate the administration or monitoring sessions of remote users.

FTA_SSL.4 (LU, RU) specify that local or remote users can terminate TOE administration or monitoring sessions.

FMT_SMF.1 specifies that the TOE logs and records the identity of users requesting access to administration and monitoring functions.

OT_authentication

FMT_MTD.1 and **FMT_MTD.3** specify the recording conditions of users, including the recording of authentication data.

FIA_SOS.1 specifies that the TOE controls authentication data quality.

FIA_SOS.2 specifies the conditions required for the TOE to generate authentication data.

FIA_UAU.2 (LU, RU) specify that the TOE authenticates users before establishing a link.

FIA_UAU.7 specifies that the TOE provides no information to the user as long as this user is not authenticated.

FMT_SMF.1 specifies that the TOE logs and records the result of authenticating users requesting access to administration and monitoring functions.

FIA_AFL.1 specifies the rules for managing multiple connection attempts and enables them to be countered.

OT_access_control

FIA_UAU.7 specifies that the TOE provides no information to the user as long as this user is not authenticated.

FDP_ACF.1 (PAR, FI) define the conditions required to access data and TOE functions.

FDP_ACC.1 (PAR, FI) specify that the TOE applies the filtering policies defined by **FDP_ACF.1 (PAR, FI)**.

FMT_MSA.1, **FMT_MSA.3** and **FMT_MSA.4** specify the rules relative to the definition or modification of security attributes.

FMT_SMF.1 specifies that the TOE logs and records the result of requests made by users to access to administration and monitoring functions.

FTA_SSL.4 (LP) defines the conditions restricting access by a local program to the TOE.

FTA_SSL.3 (TC) and **FTA_SSL.4 (TC)** define the conditions restricting access by a remote program to the TOE for establishing a communication channel with the administration and monitoring module.

FTA_SSL.3 (RU) and **FTA_SSL.4 (LU, RU)** define the conditions relative to a break in the connection between a user and the TOE that results in the blocking of access authorisation for this user via the administration and monitoring module.

OT_TOE_reuse

FDP_RIP.1 specifies that it is possible to render unavailable or delete sensitive TOE data.

OT_log_protection

FAU_SAR.1 (SUP), **FAU_SAR.1 (USR)** and **FAU_SAR.2** specify which users are authorised to read audit data.

FAU_STG.1 and **FAU_STG.4** specify that the audit logs are protected from all risk of saturation, and that an alarm is issued and actions taken in the event of reaching a critical threshold.

FPT_ITI.1 specifies that the TOE is able to perform an integrity check on audit data transmitted to an authorised user.

OT_remote_admin_authentication

FIA_UID.2 (TC) and **FIA_UAU.2 (TC)** specify the conditions required for identifying and authenticating a remote site by the TOE (i.e. a remote program).

FTP_ITC.1 specifies that the TOE authenticates itself to remote programs to establish a trusted channel.

FIA_USB.1 (TC) and **FIA_ATD.1 (TC)** define the establishment of a link between the TOE and the remote site.

FTA_SSL.3 (TC) and **FTA_SSL.4 (TC)** specify the conditions required for breaking a link established between the TOE and a remote site within the context of a trusted channel.

FIA_UAU.7 specifies that the TOE provides no data to a user (administrator or supervisor) as long as this user is not authenticated.

OT_remote_admin_integrity

FTP_ITC.1 and **FPT_ITI.1** specify that the TOE is capable of establishing a trusted channel enabling the control of the integrity of administration or monitoring data shared with a remote site.

FIA_USB.1 (TC) and **FIA_ATD.1 (TC)** define the establishment of a link between the TOE and the remote site.

FTA_SSL.3 (TC) and **FTA_SSL.4 (TC)** specify the conditions required for breaking a link established between the TOE and a remote site within the context of a trusted channel.

OT_remote_admin_confidentiality

FTP_ITC.1 specifies that the TOE establishes a trusted channel guaranteeing the confidentiality of administration or monitoring data imported from a remote site.

FPT_ITC.1 specifies that the TOE ensures the confidentiality of administration or monitoring data exported to a remote site.

FIA_USB.1 (TC) and **FIA_ATD.1 (TC)** define the establishment of a link between the TOE and the remote site.

FTA_SSL.3 (TC) and **FTA_SSL.4 (TC)** specify the conditions required for breaking a link established between the TOE and a remote site within the context of a trusted channel.

OT_remote_admin_no_replay

FPT_RPL.1 specifies that the TOE ensures protection against the replay of data shared with remote sites within the context of remote administration or monitoring operations.

FTP_ITC.1 specifies that the TOE establishes a trusted channel enabling the control of the integrity of administration or monitoring data shared with a remote site.

FIA_USB.1 (TC) and **FIA_ATD.1 (TC)** define the establishment of a link between the TOE and the remote site.

FTA_SSL.3 (TC) and **FTA_SSL.4 (TC)** specify the conditions required for breaking a link established between the TOE and a remote site within the context of a trusted channel.

OT_flow_audit

FAU_GEN.1 specifies which events are audited and the contents of audit messages.

FAU_GEN.2 specifies the identity of the user at the source of the audited event.

FAU_SAR.1 (SUP), **FAU_SAR.1 (USR)** and **FAU_SAR.2** specify which users are authorised to read audit data and alerts.

FAU_SAR.3 specifies how these authorised users can select them, sort them and display them.

FDP_ACC.1 (PAR) and **FDP_ACF.1 (PAR)** specify the rules enabling authorised users to modify audit and monitoring parameters including the granularity of the audit.

OT_admin_audit

FAU_GEN.1 specifies which events are audited and the contents of audit messages.

FAU_GEN.2 specifies the identity of the user at the source of the audited event.

FAU_SAR.1 (SUP), **FAU_SAR.1 (USR)** and **FAU_SAR.2** specify which users are authorised to read audit data and alerts.

FAU_SAR.3 specifies how these authorised users can select them, sort them and display them.

FDP_ACC.1 (PAR) and **FDP_ACF.1 (PAR)** specify the rules enabling authorised users to modify audit and monitoring parameters including the granularity of the audit.

FMT_SMF.1 specifies that the TOE logs and records the use of administration and monitoring functions.

OT_violation_detection

FAU_SAA.1 and **FAU_SAA.3** specify which events are considered by the TOE as being potential security violations and which shall lead to the issuing of an alert.

FIA_AFL.1 specifies the conditions required for the TOE to signal user connection errors.

FRU_RSA.1 (RES) specifies that the TOE generates an alert in the event of an attempt made to saturate the TOE by remote access.

OT_violation_reaction

FAU_ARP.1 specifies that the TOE automatically implements actions defined by the administrator in case of a security violation being detected.

FIA_AFL.1 specifies the conditions required for the TOE to process user connection errors.

FRU_RSA.1 (RES) specifies that the TOE ensures protection against attempts made to saturate the TOE by remote access.

OT_TOE_integrity

FPT_TST.1 specifies that TOE integrity is checked on start-up.

OT_operational_state

FPT_TST.1 specifies that the TOE tests its operation on start-up, periodically or at the request of an authorised user.

OT_crypto

FIA_SOS.1, **FIA_SOS.2**, **FIA_UAU.2 (TC)** and **FTP_ITC.1** implement the rules defined in this document.

6.4.2 Dependencies

Functional component dependencies are as follows:

Components	Dependencies	
FDP_IFC.1 (ONF)	FDP_IFF.1 (ONF)	This component is a selected component
FDP_IFF.1 (ONF)	FDP_IFC.1 (ONF) FMT_MSA.3	These components are selected components
FDP_ETC.2 (ONF)	FDP_IFC.1 (ONF)	This component is a selected component
FDP_IFF.5 (ONF)	FDP_IFC.1 (ONF)	This component is a selected component
FDP_IFC.1 (INF)	FDP_IFF.1 (INF)	This component is a selected component
FDP_IFF.1 (INF)	FDP_IFC.1 (INF) FMT_MSA.3	These components are selected components
FDP_ITC.1 (INF)	FDP_IFC.1 (INF) FMT_MSA.3	These components are selected components
FDP_IFF.5 (INF)	FDP_IFC.1 (INF)	This component is a selected component
FDP_IFC.1 (OAF)	FDP_IFF.1 (OAF)	This component is a selected component
FDP_IFF.1 (OAF)	FDP_IFC.1 (OAF) FMT_MSA.3	These components are selected components

Components	Dependencies	
FDP_ITC.1 (OAF)	FDP_IFC.1 (OAF) FMT_MSA.3	These components are selected components
FDP_IFF.5 (OAF)	FDP_IFC.1 (OAF)	This component is a selected component
FTA_TSE.1 (OAF)	None	
FDP_IFC.1 (IAF)	FDP_IFF.1 (IAF)	This component is a selected component
FDP_IFF.1 (IAF)	FDP_IFC.1 (IAF) FMT_MSA.3	These components are selected components
FDP_ETC.2 (IAF)	FDP_IFC.1 (IAF)	This component is a selected component
FDP_IFF.5 (IAF)	FDP_IFC.1 (IAF)	This component is a selected component
FIA_UID.2 (LP)	None	
FIA_USB.1 (LP)	FIA_ATD.1 (LP)	This component is a selected component
FIA_ATD.1 (LP)	None	
FTA_SSL.4 (LP)	None	
FIA_UID.1 (RP)	None	
FIA_USB.1 (RP)	FIA_ATD.1 (RP)	This component is a selected component
FIA_ATD.1 (RP)	None	
FTA_SSL.4 (RP)	None	
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	These components are selected components
FMT_MTD.3	FMT_MTD.1	This component is a selected component
FIA_SOS.1	None	
FIA_SOS.2	None	
FIA_UID.2 (LU)	None	
FIA_UID.2 (RU)	None	
FIA_UAU.2 (LU)	FIA_UID.1	The component FIA_UID.2 (LU), hierarchical to FIA_UID.1, is a selected component
FIA_UAU.2 (RU)	FIA_UID.1	The component FIA_UID.2 (RU), hierarchical to FIA_UID.1, is a selected component
FIA_UAU.7	FIA_UAU.1	The components FIA_UID.2 (LU) and FIA_UAU.2 (RU), hierarchical to FIA_UID.1, are selected components
FIA_AFL.1	FIA_UAU.1	The components FIA_UID.2 (LU) and FIA_UAU.2 (RU), hierarchical to FIA_UID.1, are selected components
FTA_TSE.1 (LU)	None	
FTA_TSE.1 (RU)	None	
FIA_USB.1 (LU)	FIA_ATD.1 (LU)	This component is a selected component
FIA_ATD.1 (LU)	None	
FIA_USB.1 (RU)	FIA_ATD.1 (RU)	This component is a selected component
FIA_ATD.1 (RU)	None	
FTA_SSL.3 (RU)	None	
FTA_SSL.4 (LU)	None	
FTA_SSL.4 (RU)	None	
FDP_ACC.1 (PAR)	FDP_ACF.1 (PAR)	This component is a selected component
FDP_ACF.1 (PAR)	FDP_ACC.1 (PAR) FMT_MSA.3	These components are selected components
FDP_ACC.1 (FI)	FDP_ACF.1 (FI)	This component is a selected component
FDP_ACF.1 (FI)	FDP_ACC.1 (FI) FMT_MSA.3	These components are selected components
FDP_RIP.1	None	
FMT_MSA.1	FDP_IFC.1 (IAF) FDP_IFC.1 (OAF) FDP_IFC.1 (INF) FDP_IFC.1 (ONF) FMT_SMR.1 FMT_SMF.1	These components are selected components
FMT_SMR.1	FIA_UID.1	This component is not selected, but this requirement is

Components	Dependencies	
		covered by components FIA_UID.2 (LU) and FIA_UID.2 (RU)
FMT_SMF.1	None	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	These components are selected components
FMT_MSA.4	FDP_IFC.1 (OAF) FDP_IFC.1 (ONF) FDP_IFC.1 (INF) FDP_IFC (IAF)	These components are selected components
FIA_UID.2 (TC)	None	
FIA_UAU.2 (TC)	FIA_UID.1 (RP)	This component is a selected component
FIA_USB.1 (TC)	FIA_ATD.1 (TC)	This component is a selected component
FIA_ATD.1 (TC)	None	
FTA_SSL.3 (TC)	None	
FTA_SSL.4 (TC)	None	
FPT_ITI.1	None	
FPT_RPL.1	None	
FPT_ITC.1	None	
FTP_ITC.1	None	
FPT_TDC.1	None	
FAU_GEN.1	FTP_STM.1	This component is not retained but the TOE obtains these data from the Operating System which implements this function.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1 (RP)	This component is a selected component This component is a selected component
FAU_SAA.1	FAU_GEN.1	This component is a selected component
FAU_SAA.3	None	
FAU_SAR.1 (SUP)	FAU_GEN.1	This component is a selected component
FAU_SAR.1 (USR)	FAU_GEN.1	This component is a selected component
FAU_SAR.2	FAU_SAR.1	This component is a selected component (see FAU_SAR.1 (SUP) & FAU_SAR.1 (USR))
FAU_SAR.3	FAU_SAR.1	This component is a selected component (see FAU_SAR.1 (SUP) & FAU_SAR.1 (USR))
FAU_ARP.1	FAU_SAA.1	This component is a selected component
FAU_STG.1	FAU_GEN.1	This component is a selected component
FAU_STG.4	FAU_STG.1	This component is a selected component
FPT_TST.1	None	
FRU_RSA.1 (RES)	None	

Table 9: Functional component dependencies

6.4.3 Conformity with a PP

Not applicable.

6.4.4 Extended components

Not applicable.

Appendix A Additional descriptions of the TOE and its environment

A.1 Architecture of the TOE

The following diagram presents an example of a PFP architecture:

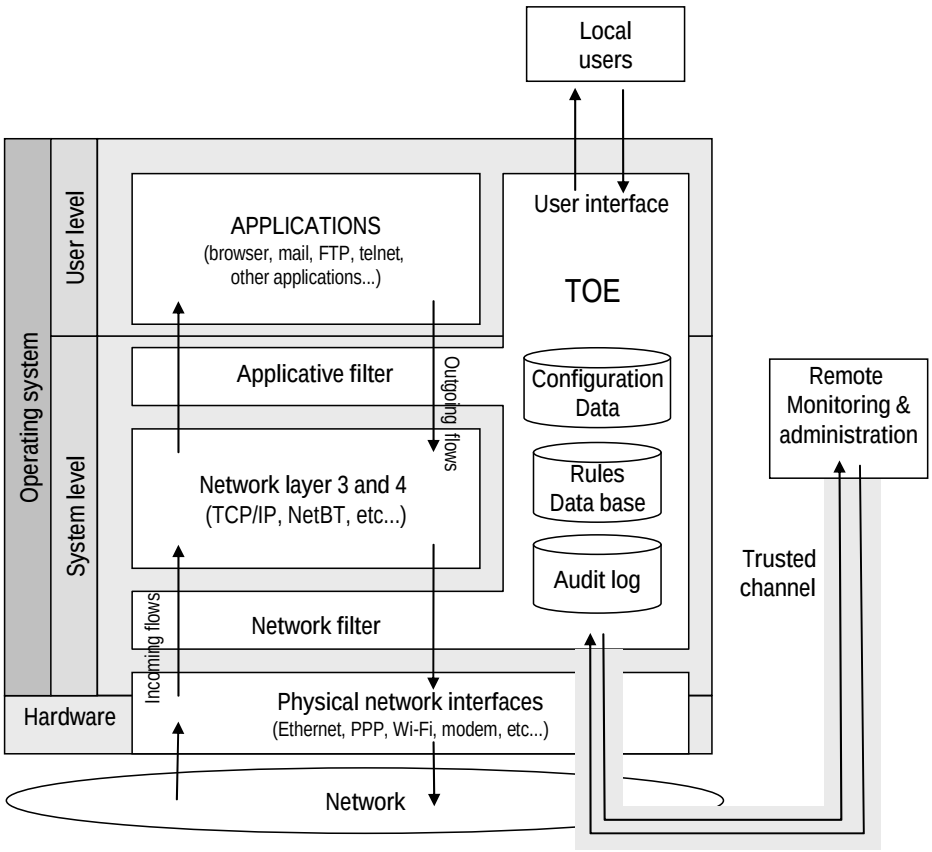

Figure 3: Architectural diagram of the TOE

The TOE exchanges flows with its environment via the following interfaces:

- A “system” interface enabling interactions between the TOE and workstation programs (operating system, other programs)
- A “network” interface used by administrators and supervisors connected remotely
- A “local MMI” used by administrators, supervisors or basic users connected locally to the workstation

Interfaces used for “functional” purposes are not shown in this list.

The STs in conformity with this PP must specify if the TOE provides specific drivers to be used in place of those available on the workstation.

A.2 Physical scope of the TOE

The physical scope of the TOE comprises:

- The TOE installation kit
- Associated documentation

A.3 Logical scope of the TOE

The logical scope of the TOE comprises the following components:

- TOE software
- TOE administration parameters
- The filtering rules adopted by the TOE
- Monitoring data, alarms and logs

A.4 Functional roles

The various functional roles linked to the operation of the workstation and the TOE are as follows:

- The security officer
- The system, network and office application administrator in charge of the workstation
- The system supervisor in charge of the workstation
- The administrator in charge of the TOE [7]
- The supervisor in charge of the TOE[8]
- The basic user of the workstation

Note: the holders of administration or monitoring roles recognised by the TOE and of those recognised by the host machine may be independent. In particular, an administrator in charge of the TOE is not necessarily a system administrator.

A.4.1 Roles recognised by the TOE

The holders of these roles have access (local or remote according to circumstances) to the TOE to fulfil their duties or to make use of the rights at their disposal. Roles can be allocated to different persons or not, according to the security policy chosen by the organisation.

These roles are defined in section 3.2 of this document.

A.4.2 Other roles

The holders of these roles do not require access to the TOE to fulfil their duties.

[7] Designated as “administrator” in the body of the protection profile.
[8] Designated as “supervisor” in the body of the protection profile.

Security officer

Security officers define the filtering policy to be implemented by administrators. In a centralised context, they may be in charge of teams responsible for the monitoring or administration of security.

System administrator

System administrators are in charge of installing the TOE as an application on the workstation, and of the configuration and administration of the workstation at the system and network level. Tasks can be performed via local or remote access.

System supervisor

System supervisors control and audit system and network administration for workstations.

A.5 Functionalities of the TOE

A.5.1 Services provided by the TOE

A.5.1.1 Filtering of communications

The main objective of communications filtering is to ensure a filtering of flows at the level of the TCP/IP protocol stack. This filtering takes into account the standard protocols of the network layer (IP, ICMP) and of the transport layer (TCP, UDP), and the standard protocols of application layers (5, 6 and 7).

The PP does not cover the taking into account of proprietary non-IP protocols (NetBT for example). The STs in conformity with this PP must indicate, if applicable, the non-IP protocols taken into account.

Communications filtering comprises the following filtering methods:

- Filtering based on the protocol analysis of flows (conformity to filtering rules defined according to criteria such as protocol, source or destination address, source or destination port, incoming or outgoing direction, MAC address, interface used, etc.); this filtering takes into account contextual or behavioural filtering[9]
- Filtering based on the analysis of communicating applications (identification, link between the program and the protocol)

Filtering must also take into account the network environment (connection inside or outside the company).

Filtering levels:

The TOE offers three levels of filtering: global, user, adaptive.

Global filtering is applied as soon as the workstation is started up whether or not a user is connected to the workstation.

[9] Contextual or behavioural filtering is understood to mean the TOE's capacity to filter a packet according to packets already received or sent.

Global filtering can be configured during the installation of the PFP and modified, and is controlled by the TOE administrator.

User filtering is specific to a basic user (or to a group of basic users). It is applied as soon as this basic user (or any basic user of the group) connects to the workstation.

This filtering is controlled by the TOE administrator, who may delegate the control of all or part of this filtering process to the basic user in question.

Adaptive filtering is specific to a basic user (or to a group of basic users). Filtering is generated by a learning mechanism that enables basic users to build a filtering policy adapted to their needs by validating connections over time as the workstation is used

This mechanism contributes to an intuitive configuration of the PFP, avoiding presenting the basic user with complex security or network notions. It limits configuration errors. This filtering must remain coherent with the filtering policies created by the TOE administrator.

The learning mechanism can be enabled or disabled by a TOE administrator.

These three notions can be represented graphically as follows:

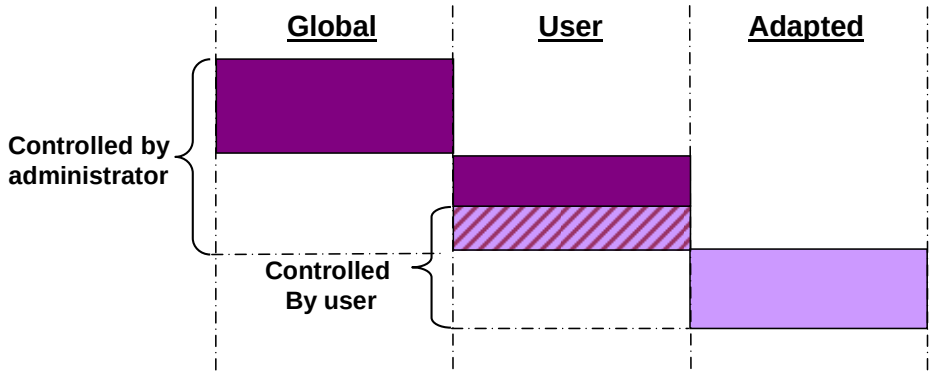

Figure 4: Filtering levels

A.5.1.2 Application integrity control

As a complement to filtering functions, the PFP offers the capability to control the integrity of applications that established network connections.

This integrity check is based on integrity check values enabling the detection of application corruption.

The mechanisms used for this application integrity check do not fall within the scope of the PP. They must be described in the STs in conformity with this PP.

A.5.1.3 Protection against attacks

The TOE can react to counter certain attacks, of a denial of service or saturation type, targeting workstation resources.

The TOE administrator can configure the actions to be taken by the TOE in response to these attacks (e.g. the issuing of an alert or the blocking of flows).

A.5.2 Services required for the TOE to function correctly

Administration and monitoring services are required for the TOE to function correctly. These services can be shared among various functional roles (see § 3.2 and A.4).

A.5.2.1 Administration

PFP administration may be centralised (e.g. the workstation is connected to the local company network) or local (e.g. the workstation is used outside the company or during installations).

It mainly covers the management of parameters and filtering rules. It also concerns the disabling / reactivation of TOE services.

Only the holders of a specific role may access administration services; these roles must be assigned to the persons in charge of these services.

In order to cover the various organisational and operational modes, PFP administration must be possible:

- By a TOE administrator applying company policy, operating locally or in a centralised manner, without basic user control
- By a basic user alone defining their own filtering rules
- In a collaborative manner between the TOE administrator, responsible for defining basic rules, and a basic user, who then refines them (e.g. over time according to a learning model according to the connection requirements of applications)

The TOE administrator can configure a basic user's ability to modify the security policy; this may range from granting total freedom to fully blocking access to security policy modification.

Visibility of configuration parameters and filtering rules

The TOE administrator has access to all TOE configuration parameters, in particular to all the filtering rules and parameters relative to analysed flows, including the rules and technical parameters that might be hidden from a basic user.

A basic user may have access to the filtering rules (user or adaptive level) specified for this basic user. The TOE administrator must be able to configure this access.

A.5.2.2 Monitoring and logging

Monitoring involves the ability to view information (audit logs and audit messages, alerts, monitoring parameters) at a remote site or on the workstation. It must be interoperable with administration functions in order to react to an alert for example.

Logging involves the recording of critical or non-critical events in a log that may be consulted at a later time.

Only the holders of a specific role may access monitoring services; these roles must be assigned to the persons in charge of these services.

Recorded or transmitted information can be used locally by a basic user or processed by a

person in charge of monitoring. An intermediate situation exists, whereby the basic user and the supervisor in charge of the TOE can work together to use monitoring information, alarms and logs.

The TOE can track:

- analysed and filtered flows
- local or remote administration operations
- alerts generated upon the detection of attempted attacks

The use of logged information is configured in such a way as to limit flows transmitted to the monitoring entity or presented to an authorised user.

The level of alerts transmitted by the TOE can be configured in such a way as to limit the amount of information to that strictly required.

The transmission of alarms can be configured according to connection contexts (inside or outside the company) in such a way as to inform the basic user or the supervisor in charge of the TOE.

A mechanism can be used to transfer monitoring information when the workstation is connected to the monitoring centre (deferred transmission for portable workstations).

A.5.3 Services for securing the TOE

A.5.3.1 Protection of administration and monitoring functions

The TOE has an access control mechanism for administration and monitoring functions: management of parameters, filters, logs, TOE shutdown, etc..

This access control mechanism is based notably on the use of roles allocated to authorised users.

Protection of remote administration and monitoring:

The TOE identifies and authenticates users who connect to the administration or monitoring interface, and attributes a role according to their identity.

The TOE ensures the authenticity and integrity of the flows it transmits. It can also ensure the confidentiality of these flows. It controls the integrity and the authenticity of the flows it receives.

It has at its disposal a protection mechanism offering protection from saturation attacks targeting administration or monitoring functions.

Protection of local administration and monitoring:

The TOE identifies and authenticates users who connect to the administration or monitoring interface, and attributes them a role according to their identity.

A.5.3.2 Protection of logs

The TOE controls access to logs according to the roles held by the user.

A.5.3.3 Protection of the TOE

The TOE must:

- Control the integrity of some of its components and indicate any detected loss of integrity
- Inform the user (basic user or supervisor in charge of the TOE) of its status (active or inactive)

A.6 TOE operating environment

The personal firewall application is designed to be installed on a workstation equipped with an operating system and possessing one or more network interfaces (Ethernet, WIFI, STN, IRDA, USB, etc.).

This workstation may be shared among several users, each of whom has personal access (a user account + associated password). It may be connected directly to the company network or used as a portable workstation.

Being portable multiplies use contexts and network environments:

- Periods: may be used any day or at any time
- Access conditions: ADSL or STN (ISP, Internet café, Hotel), public WIFI access (station, train, airport, etc.)

The STs in conformity with this PP must accurately describe the operating environment. In particular, they must indicate the workstation constraints to be respected: operating system version, drivers to be used, the order in which software is installed, etc.

A.7 TOE evaluation platform

The TOE evaluation platform must be representative of normal contexts of TOE use, administration and monitoring.

It must include at least:

- The workstation hosting the TOE. This workstation must possess at least one network interface. The drivers used to drive network interfaces must be those supplied with the TOE or recommended in the TOE documentation.
- A second workstation interconnected with the workstation hosting the TOE. This workstation makes it possible to exchange data with the TOE and to evaluate the TOE filtering function.
- A third workstation interconnected with the workstation hosting the TOE. This workstation makes it possible to evaluate remote administration and monitoring functions.
- A network to which these workstations are connected enabling the simulation of TOE operating environment network configurations.

The STs in conformity with this PP must accurately describe the platform to be used.

A.8 Possible additional functionalities of the personal firewall (PFP)

This section presents additional functionalities that can be offered by manufacturers in response to specific basic user requirements. These functionalities do not fall within the scope of this PP, but can be included in the STs in conformity with this PP by developing the associated security analysis.

Filtering:

The following filtering possibilities have not been included:

- Time-based filtering, URL filtering, content filtering
- Control of file transfer

Furthermore, filtering is limited to connections with host systems: a connection between the workstation and an external disk via a USB port will not be taken into account (although a connection between this workstation and another workstation via the same USB port and a modem will be taken into account).

Temporary disabling of filtering by the basic user:

The temporary disabling of the filtering function by the basic user involves offering the basic user the possibility to temporarily disable filtering rules in order to enable him to perform communications that are normally blocked.

This function must be controlled by the TOE administrator, who must be able to authorise its implementation. The temporary disabling of the filtering function by the basic user must require the use of a code and must be audited, as must the communications carried out in this operational mode. It must be possible to automatically re-enable the rules disabled by this mechanism when no longer used.

This function can also be implemented by adopting organisational measures.

Global learning mode:

This learning mode provides for the dynamic generation of a workstation filtering policy according to the connection habits of the various basic users that can be refined at a later date by TOE administrators.

Confidentiality of TOE processes:

Confidentiality of TOE processes involves hiding the existence of the TOE on a given workstation with regard to basic users or attackers.

Respect for regulations:

As a result of its data protection potential, the TOE contributes to the respect of laws and regulations relative to the protection of sensitive data of a personal or private nature (see [L78]).

Appendix B Definitions and acronyms

B.1 Acronyms

PFP Personal Firewall

PP Protection Profile

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functions

TSP TOE Security Policy

B.2 Conventions used

The following list shows the roots used for the various elements.

Root	Elements described by this root
T_	Threats relative to the TOE and the TOE operational environment
TD_	Threats concerning the TOE development environment
OSP_	Organisational security policy
A_	Assumption
OT_	Security objectives for the TOE
OE_	Security objectives for the operational environment
S_	TOE subjects
SA_	Security attributes
D_	Sensitive TOE assets and objects
U_	Users (programs or individuals) interacting with the TOE

B.3 Definitions

Security Target (ST)

Reference document for the TOE evaluation: the certificate awarded by the DCSSI will attest conformity of the product and its documentation with the (functional and assurance) requirements formulated in the security target.

Target of Evaluation (TOE)

The product to be evaluated and its associated documentation.

TOE Security Functionality (TSF)

A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TCP/IP protocol stack

"TCP/IP protocol stack" is understood to mean the standard protocols of the network layer (IP, ICMP) and of the transport layer (TCP, UDP), and the standard protocols of application layers (5, 6 and 7).

TOE Security Policy (TSP)

Set of rules stipulating how to manage, protect and distribute assets within a TOE.

Interpretation

An addition (clarification, correction or addition) to the Common Criteria; the list of interpretations is available at the following site: www.commoncriteriaportal.org

Appendix C References

C.1 Normative references

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2006, Version 3.1, Revision 1, CCMB-2006-09-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2007, Version 3.1, Revision 2, CCMB-2007-09-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2007, Version 3.1, Revision 2, CCMB-2007-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2007, Version 3.1, Revision 2, CCMB-2007-09-004

[QUALIF_STD] Processus de qualification d'un produit de sécurité – Niveau *standard*. DCSSI, Version 1.1, 18 March 2008, N°549/SGDN/DCSSI/SDR

[CRYPT-STD] Cryptographic mechanisms – Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level (regularly updated version)

C.2 Laws and policies

[L78] Amended law of 6 January 1978 relative to data processing, computer files and individual liberties

C.3 Other documents

[EBIOS] EBIOS method (Expression of needs and identification of security objectives), Version 2, 5 February 2004