McAfee®

Securify^{TM} 6.0

Security Target

Version 3.2

Last Revision: August 7, 2009

Table of Contents

Figures and Tables

Figures

Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title:	Securify^{TM} Version 6.0 Security Target
ST Version:	**v3.2**
ST Authors:	Luis Chirinos and Jose Caldera
ST Date:	**August 7, 2009**
Assurance level:	EAL2+
Protection Profile:	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007
Keywords:	Intrusion Detection System, Network Security, Monitoring, Analysis, Identification, Authentication, Access Control, Audit, and Security Target

1.2 TOE Reference

TOE Identification:
Securify^{TM} Version 6.0 consisting of the following components:

- Securify^{TM} Studio: 6.0 (Build V60_CC_9)
- Securify^{TM} Monitor: 6.0 (Build V60_CC_9)
- Securify^{TM} Monitor (LE): 6.0 (Build V60_CC_9)
- Securify^{TM} Monitor (SE): 6.0 (Build V60_CC_9)
- Securify^{TM} Enterprise Manager: 6.0 (Build V60_CC_9)
- Securify^{TM} Enterprise Reporting Gateway: 6.0 (Build V60_CC_9)

1.3 TOE Overview

Securify™ Version 6.0 (TOE) is a security system that enables customers to generate business-driven security policies, monitor networks for compliance, threats and known attack patterns, and produce relevant network operational information. This software product consists of an environment for policy development and security analysis, a real-time monitoring system to continuously verify conformance to security policies and known attack patterns, and an enterprise management and trend reporting system. The Securify™ Version 6.0 system is driven by a customer-specified policy that formally describes the desired operation of the network.

1.3.1 TOE Type

The TOE is used as an Intrusion Detection System (IDS), meaning the system alerts on deviations from expected network behavior (such as network behavior anomalies) and the system matches to explicit known attack patterns.

It is important to mention that the TOE is an IDS that does not perform active scanning (active probing of individual systems) to collect static configuration or detect security vulnerabilities.

1.3.2 Required Non-TOE hardware/software/firmware

Securify Studio:

The Securify™ Studio software requires a standard PC with 1GHz or higher processor and 512MB or more RAM, running version 2000, XP or Vista of the Microsoft Windows operating system.

Components on the IT Environment:

The IT environment needs to provide the following capabilities:

- SNMP
- SMTP
- NTP
- DNS
- SYSLOG
- The Securify™ Monitor requires the availability of a SPAN port where traffic to be monitored is mirrored.

1.4 TOE Description

1.4.1 Acronyms

CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
IT	Information Technology
NTP	Network Time Protocol
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.4.2 Terminology

Correlated Event	A correlated event occurs when the threshold is crossed for a rate defined for a type of connection and an alert is triggered (or generated). Such a rate driven alert is useful in drawing attention to specific spikes in bandwidth or in connection counts.
DME	It is a proprietary Securify format that compacts connection data into a file. It is an alternative to storing complete packet data.
Negative Model Subscription Service (NMSS)	Provides timely updates of signature and vulnerability definitions to its subscribers.
Protocol Event	Protocol events are independent network protocol units that must happen to produce a complete session between two network entities. Depending on the highest protocol involved (e.g. ICMP, HTTP, etc.); a protocol event can be as complex as a series of exchanges between two hosts, or as simple as an ICMP echo request. For example, a TCP connect is a Protocol event.
Network Event	When the policy engine evaluates network traffic against policy, the output is a network event. A network event is a summary of the set of protocol events that make up a complete application level session on the network. For example, for an FTP Session (Network Event), the following protocol events must occur: IP association, TCP Connect, FT Open, FTP Get and FTP Close.
Outcome	A Policy object that encapsulates all the monitored events associated with a protocol. Outcomes are assigned to relationships to define a complete policy statement made about a specific protocol or service interaction between hosts

	on the network. An outcome contains a set of behaviors that describe the different aspects of a protocol being monitored by Securify, with a criticality assigned to each. An outcome name need only be unique per protocol.
Policy	A technical specification of network security for a specific network. A policy is made up of objects that are defined in Studio and used by the policy engine to characterize network traffic.
Policy Domain	Represents a collection of Monitors running the same policy. It is also called Security Zone.
Policy Engine	A component of the Monitor that evaluates a policy against network data that has come from either a packet-capture file or from packets captured directly from a network in real time. The policy engine classifies the packet data into a connection. The connection is evaluated to determine which policy rule best describes the event, then an outcome is associated with the event.
Policy Evaluation	The dynamic process of interpreting packet data from a file or a live network and comparing the connections against a policy to determine if it violates the security policy. A primary feature of Securify is its ability to compare actual network traffic with a specified policy.
Negative Model	A detection technique used in IDS systems. It compares the network traffic against known malicious patterns in order to detect possible security violations.
Positive Model	A detection technique used in IDS systems. It defines an expected (good) network behavior and any network traffic that is outside of this behavior is considered a security violation.
Scanner	Network system that actively and remotely probes other network systems and components to gather information about operating systems, installed software, open ports, and so on. A scanner generates a list of possible vulnerabilities for correction purposes.
Connection	An output of the policy engine created when network traffic is evaluated against a policy. A connection is a summary of the set of protocol events that make up a complete application level session on the network. For example, viewing a Web page creates a connection that summarizes the underlying IP association, TCP connection and HTTP Get protocol events.
Service	A category of network traffic that is associated with a specific application. A service has a base protocol, which specifies both the transport protocol and application layer protocols supported by Securify. Most services are based on the UDP or TCP protocols and are specified by means of one or more TCP and/or UDP port number. Other services include BOOTP, ICMP, and broadcast services.
Security Zone	Represents a collection of Monitors running the same policy. It is also called Policy Domain.
Signature	A signature describes an exploit for a known vulnerability that may be found when evaluating traffic to a destination network object.
Security Information Event Manager (SIEM) / Security Event Manager (SEM)	Computerized tools used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software running on the network. They aid network administrator and security personnel to perform Log Consolidation, Threat Correlation, Incident Management and Reporting from a centralized location.

SPFM	Securify Packet Filter Module. This is the Securify component in charge of capturing network traffic.
SPM	Securify Policy Manager. This is the internal component responsible for processing DME, populating the internal database, and preparing the batch files to export IDS data to the Securify Enterprise Manager.
Harvester	The Securify component responsible for processing the raw packets captured by SPFM to generate the DME stream.
Identity	An Identity is a representation of a user, computer, or group generated by the Securify Identity feature using Active Directory information.
Behavior	A description of the different aspects of a protocol being monitored by Securify, with a criticality assigned to each. For example, the SSL protocol has a behavior for identifying a connection where low-quality encryption is used. The TCP protocol has a behavior for identifying a connection where data is transferred, and it has another behavior for identifying a connection where no data is transferred.
SPAN port	Switched Port Analyzer. A port on a switch that is configured to mirror traffic transmitted on one or more switch ports or VLANS.
Collection point	A physical place in the network (typically a SPAN port on a switch) where traffic capture is occurring and the policy engine is applying policy. The location of the collection point determines what traffic is visible to the Monitor. A collection point is associated with one or more subnet objects in policy. A Securify policy, which describes a policy security zone, can define multiple collection points.
Network object	A policy asset or group of assets in a policy about which policy statements can be written. A network object represents anything that generates or receives network traffic.
Network topology diagram	Logical and simplified representation of the network for which policy is being developed. It is composed of symbols that represent the Internet, subnets, routers, firewalls, and the connections between them. The network topology diagram provides useful information for policy evaluation. The network topology diagram does not need to represent as much detail as a network diagram
Relationship	A description of expected or anticipated network traffic. It is the basis for the rules used by the policy engine. A relationship comprises a service offered by a destination object (or server application), and used by a source object (or client application). An associated outcome defines how policy applies to the relationship. Relationships can describe both expected, good traffic and traffic that is forbidden by policy.

1.4.3 TOE Description

Securify™ Version 6.0 (Securify™ or TOE) combines positive and negative security models to provide more comprehensive security coverage. In broad terms, the former defines what traffic is deemed acceptable on the network whereas the latter defines what is not acceptable. Any traffic different from the positive behavior OR that perfectly matches one of the negative behaviors is considered suspicious.

The positive model relies on a proprietary policy language that translates business driven security policies into a formal, machine monitored specification (a “Policy”) describing the “correct” behavior of the network.

The negative model is the traditional pattern matching technique that relies in a set of signatures to define known attack patterns (negative behavior). Customers usually rely on Securify Negative Model Subscription Service (NMSS) to provide them with a set of signatures that are relevant to the current state of the network threats. In addition, customers can configure their own set of signatures.

Securify™ then evaluates, in real time, the packets flowing through the network at all levels of the protocol stack and makes decisions on whether the traffic is consistent with the policy specification, and whether the traffic matches any configured signature. This information is presented in a Web-based analysis environment in terms that are specific to the business, and actionable for the team running the network. Securify^{TM} consists of four major components:

- **Securify™ Studio** (Studio) provides management interfaces that allows for the authoring of network security policy at multiple levels.

- **Securify™ Monitor** (Monitor) evaluates monitored network traffic according to the security policy translating business requirements.

- **Securify™ Enterprise Manager** (Enterprise Manager) combines multiple monitoring points (Monitors) into a single, real-time monitoring and management console. Each Monitor belongs to a single Security Zone (groups of Monitors that run the same policy) and the Enterprise Manager can manage multiple Security Zones.

- **Securify™ Enterprise Reporting Gateway** (ERGW or ER Gateway) component of Securify™ Enterprise Reporting solution, is used in providing quantitative network and application trend reporting.

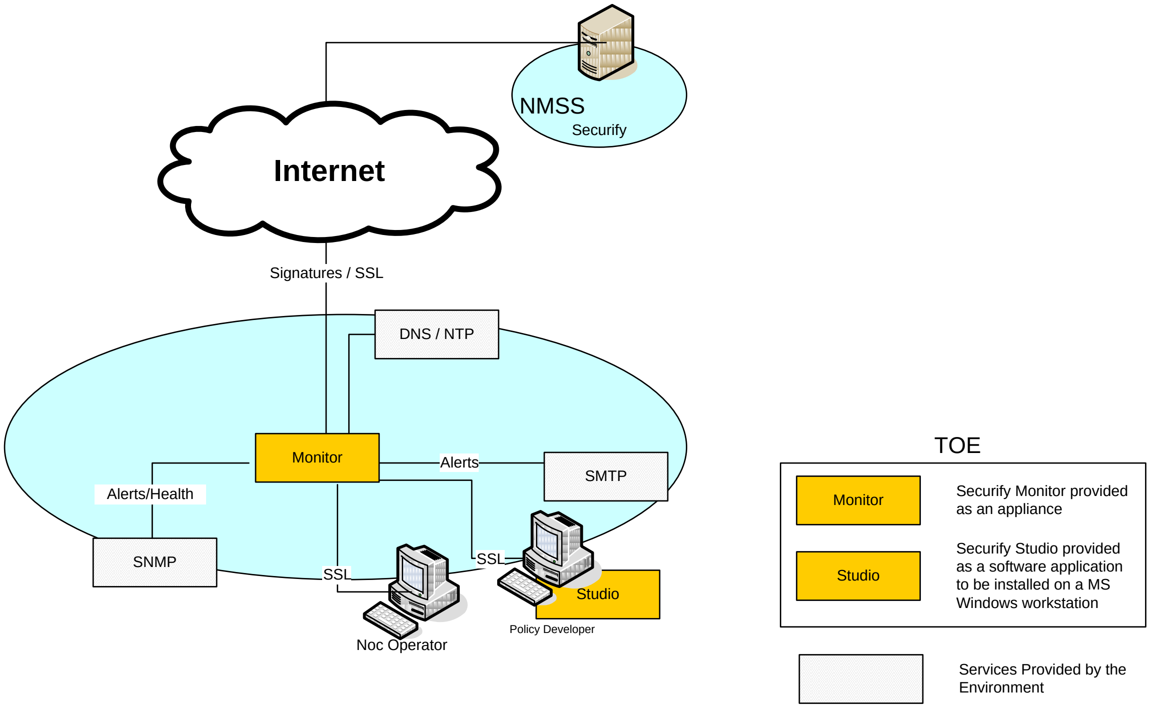

NMSS
Securify
Internet
Signatures / SSL
DNS / NTP
Monitor
Alerts
SMTP
Alerts/Health
SNMP
SSL
SSL
Studio
Noc Operator
Policy Developer
TOE
Monitor
Securify Monitor provided as an appliance
Studio
Securify Studio provided as a software application to be installed on a MS Windows workstation
Services Provided by the Environment

Figure 1-1 Securify Deployment – 1 Monitor Configuration

Figure 1-1 shows a deployment that consists of one Securify™ Monitor and Securify™ Studio. Although Securify™ Monitor can be placed anywhere on the network, typically, Securify™ Monitor is connected to the SPAN port of a switch (see limitations) where there is traffic relevant to the policy. However, there are no assumptions about the source of the traffic. It is recommended that the Monitor be deployed in a trusted environment.

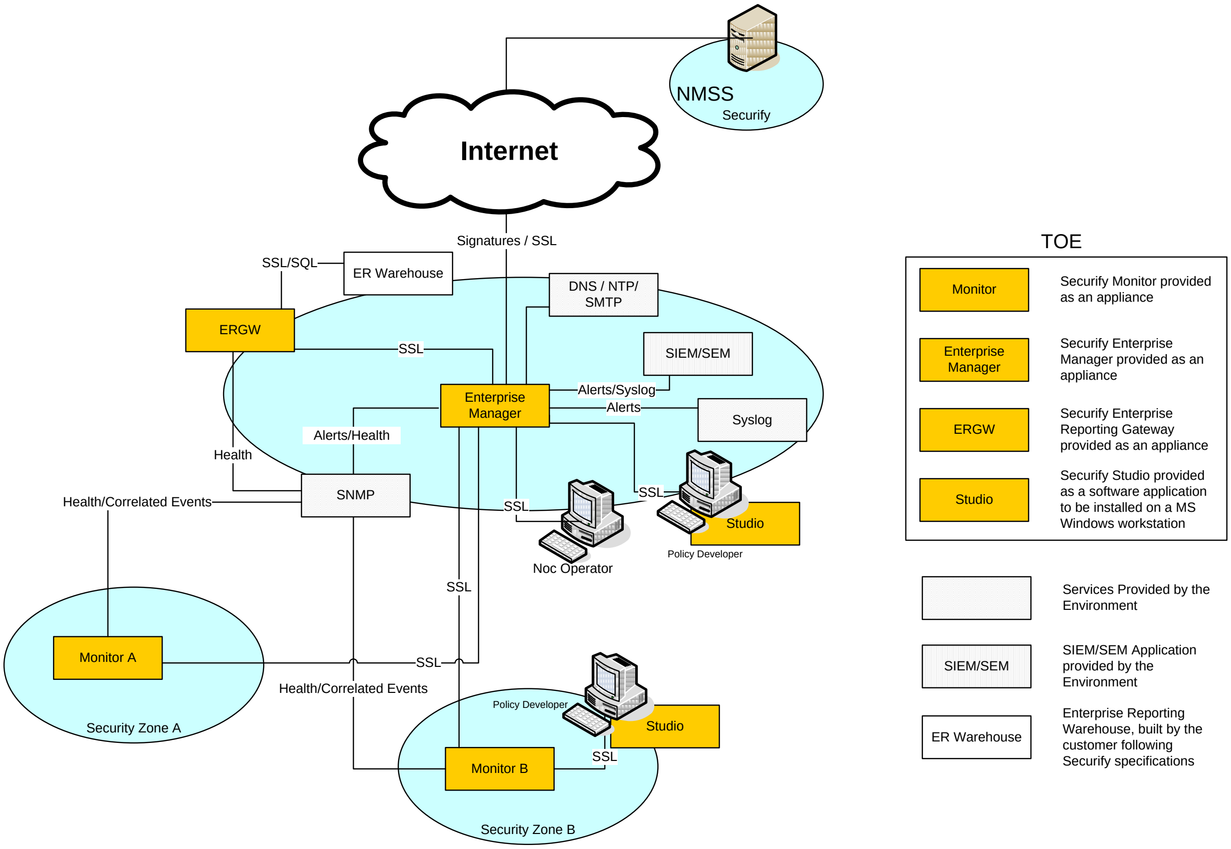

NMSS
Securify
Internet
Signatures / SSL
SSL/SQL
ER Warehouse
DNS / NTP/ SMTP
ERGW
SSL
SIEM/SEM
Enterprise Manager
Alerts/Syslog
Alerts
Syslog
Alerts/Health
Health
SNMP
Health/Correlated Events
SSL
SSL
Studio
Policy Developer
Noc Operator
SSL
Monitor A
Security Zone A
SSL
Health/Correlated Events
Policy Developer
Studio
SSL
Monitor B
Security Zone B
TOE
Monitor
Securify Monitor provided as an appliance
Enterprise Manager
Securify Enterprise Manager provided as an appliance
ERGW
Securify Enterprise Reporting Gateway provided as an appliance
Studio
Securify Studio provided as a software application to be installed on a MS Windows workstation
Services Provided by the Environment
SIEM/SEM
SIEM/SEM Application provided by the Environment
ER Warehouse
Enterprise Reporting Warehouse, built by the customer following Securify specifications

Figure 1-2 Securify Deployment – Full Configuration

Figure 1-2 shows a full configuration deployment of Securify™, although Securify™ Monitor can be placed anywhere on the network, typically, Securify™ Monitor is connected to the SPAN port of a switch (see limitations) where there is traffic relevant to the policy. However, there are no assumptions about the source of the traffic. It is recommended that the Monitor be deployed in a trusted environment.

Limitations

Securify™ Monitor audits IPv4 and IPv6 packets when transported over Ethernet frames, including jumboframes. IPv6 jumbo grams, however, are discarded without logging.

Product Overview

A Securify™ Policy is a set of rules that describes the expected behavior of the systems within a network as well as describing signatures for known attack patterns. Network objects represent systems. A network object can be one or many IP addresses.

Each rule in the Policy describes how the system will log a network transaction between two network objects. All network transactions are logged and represented as a network event (see definition in 1.4.2 Terminology). Each network event represents the information contained in the headers of the actual packets within the network transaction.

A network event is identified by the packet, which initiates an application session between devices. The policy engine assigns the following information to the network event, based on the protocol events and the most relevant policy rule that fires during policy evaluation:

- Source and destination IP addresses, the derived policy network objects, network object names, and services that those IP addresses resolve to.
- Outcome components assigned, including: protocol, outcome, protocol component and criticality.
- Owner: either the outcome, service, or reporting element owner in that order of precedence.
- Source and destination routing objects to provide IP routing information.
- Event time and other relevant protocol details.

The policy by default assigns a severity to every event, such that all events are logged by default. These default values can be changed by the user of the system to accommodate specific security policies. A severity has one of the following options: Critical, High, Medium, Warning, Monitor, or OK. All events other than Monitor and OK are fully logged in the system down to the protocol details level (source and target network object name, IP addresses, protocols, SRC port, DST port, TCP flags, UDP association, etc.). Events that have a severity value of OK are logged at a summary level (source and target network object name and service name).

Network events can be exported to other management systems (Security Information Event Managers) via Syslog, SNMP traps or through a proprietary XML API. Exporting events by way of the XML API is not included in the scope of the TOE evaluation.

Securify™ systems are also able to provide information and alerts regarding their operational status to network management systems via SNMP traps.

Time synchronization is paramount when it comes to network monitoring tools. Securify™ Monitor, Enterprise Manager and ER Gateway should synchronize their times with a trusted NTP server within the monitored infrastructure. If the time in the Securify systems is not correctly synchronized it will be very difficult for the user to correlate information from different sources.

Each Securify™ system provides a Web interface that allows the user to interact with the system and configure Enterprise Managers and Monitors. The deployment may consist of an Enterprise Manager and its Monitors or a stand-alone Monitor. In both cases, the same configuration options are used.

A Monitor managed by an Enterprise Manager must be configured through the Enterprise Manager; if you use the Web interface when logged into the Monitor, the changes are over-written by its managing Enterprise Manager.

Flow of Information

A Monitor captures network traffic and converts it into network events. Every event has an associated severity. The Monitor compares the event with a local copy of the Security Policy (previously uploaded by the user – Policy files are identified by a "pdx" suffix) and logs the events according to their assigned severity as specified in the Security Policy. Logged traffic is stored in the Monitor database and can be accessed with the Monitor's Web interface or through Studio. Data is stored in the Monitor for a window of time; for normal deployment scenarios, this is around three weeks. This data is accessible by the Web interface for the last 48 hours and through Studio for as long as the data stays in the database.

Enterprise Manager copies information from the Monitors connected to it and aggregates this into a local database. This database is accessible through the Monitor and Enterprise Manager Web interface for a period of 48 hours. The Enterprise Manager also serves as a conduit to the Monitors' databases when detailed information is requested by the Studio application.

Data moves from the Enterprise Manager system to the ER Gateway. The ER Gateway enables the user to implement a third-party data warehouse (not part of the TOE) to extract data for report generation or any other purpose.

Securify™ consists of the policy development and analysis environment (Studio) coupled with a monitoring system (Monitor) and optionally, the Enterprise Manager system. The figures below show the Monitor and Enterprise Manager system architectures.

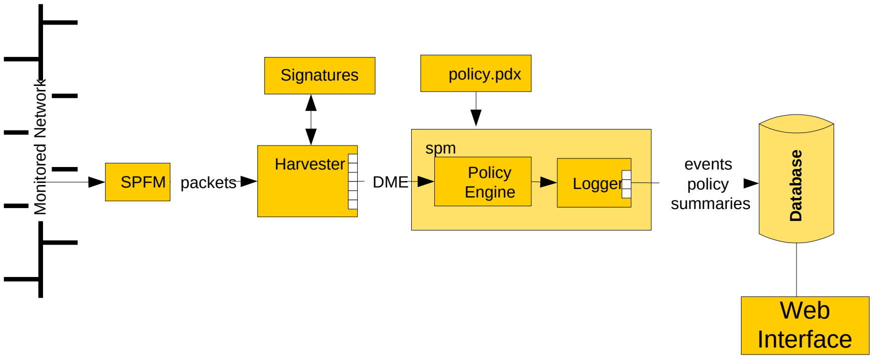


Figure 1-3 Securify^{TM} Monitor System Architecture

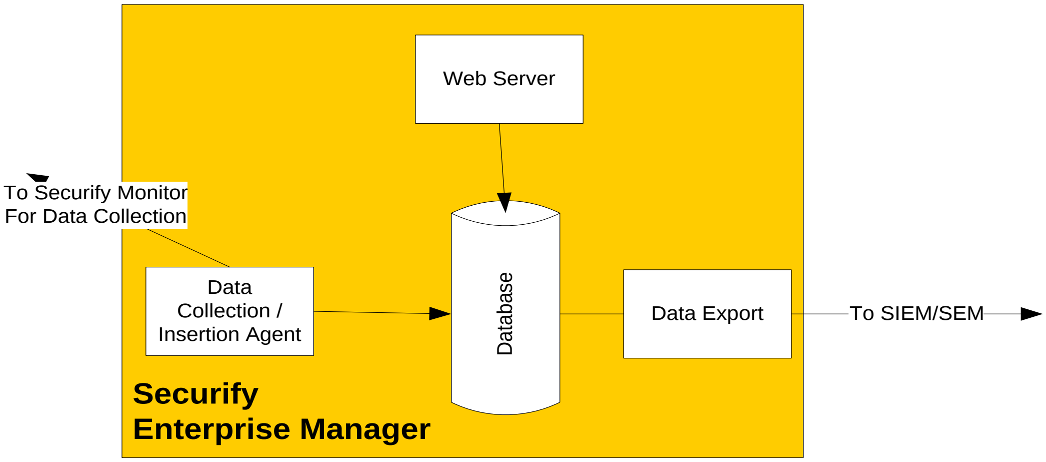

Web Server
To Securify Monitor For Data Collection
Data Collection / Insertion Agent
Database
Data Export
To SIEM/SEM
Securify Enterprise Manager

Figure 1-4 Securify™ Enterprise Manager System Architecture

1.4.3.1 Securify™ Studio

Securify™ Studio (Studio) provides an interface for authoring network security policy at multiple levels.

A typical policy requires a simple depiction of the topology of the network to be monitored. The network topology is constructed with "network objects" such as routers, firewalls, and subnets that can be created within the drag and drop environment, depicted in the figure below:

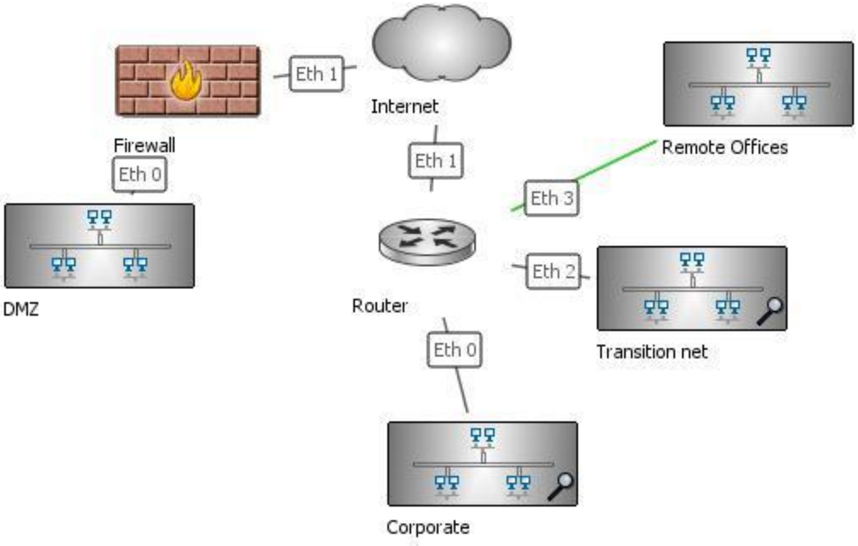


Figure 1-5 Sample Network Topology

Using Rules to Tie Together Network Objects: The Security Policy is a set of rules used to create a set of relationships between network objects and describe how these network objects should interact. Rules can be general and applied throughout the OSI protocol stack, applied to multiple IP addresses, or applied to one specific network address. A rule can be general and consist of only routing tables and allowed IP level traffic, or it can be very specific and include the exact HTTP requests allowed into a Web server or the authentication mechanism that the SSH protocol should exhibit on a network.

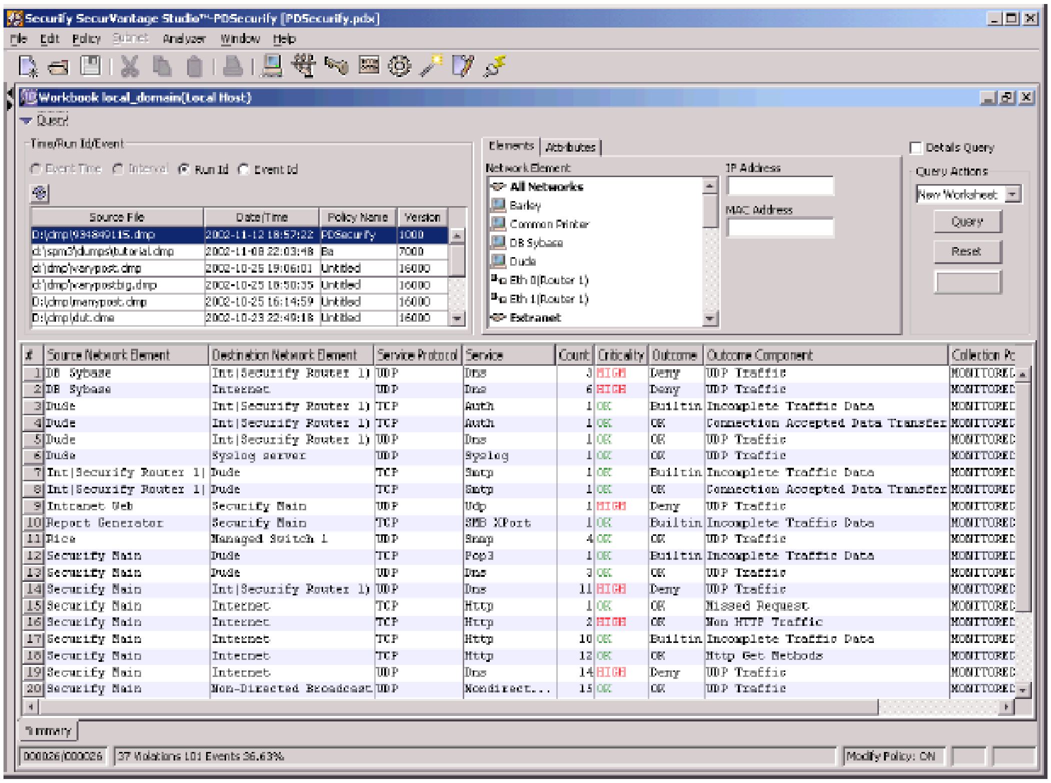
Analysis Interface: Studio provides an interface that enables users to perform detailed analysis on network traffic being evaluated by the security policy. This analysis can be performed either locally in the Studio or remotely on a Monitor/Enterprise Manager through the Web interface.

- **Offline analysis of Network Traffic**

  The Monitor can be configured to capture network traffic (in files) before policy evaluation occurs on the Monitor. These files are called DME files (a Securify proprietary format) and are downloadable through the Web interface. Studio is able to read DME files from disk and then evaluate the traffic contained in them using a policy running locally in Studio. Information about network security events is written to a local database and queried using a Java-based user interface within the Studio application. This analysis interface, depicted in Figure 1-5 below, enables easy querying using various constraints on specific scenarios of interest by way of a spreadsheet metaphor. Studio enables you to drill down through the network security events to the protocol layers.

- **Online analysis of Network Traffic**

  Studio can be also be configured to query the database running remotely on a Monitor or Enterprise Manager. When the user wants to access these databases to access information about network security events, Studio makes an authenticated SSL connection to the Enterprise Manager or Monitor. The same interface depicted in Figure 1-5 is used for such purposes.



Source File	Date/Time	Policy Name	Version
D:\dmp\934849115.dmp	2002-11-12 18:57:22	PDSecurify	1000
d:\spm3\dumps\tutorial.dmp	2002-11-08 22:03:48	Ba	7000
d:\dmp\verypost.dmp	2002-10-25 19:06:01	Untitled	16000
d:\dmp\verypostbig.dmp	2002-10-25 18:50:35	Untitled	16000
D:\dmp\manypost.dmp	2002-10-25 16:14:59	Untitled	16000
D:\dmp\dut.dme	2002-10-23 22:49:18	Untitled	16000

#	Source Network Element	Destination Network Element	Service Protocol	Service	Count	Criticality	Outcome	Outcome Component	Collection Pc
1	DB Sybase	Int|Securify Router 1)	UDP	Dns	3	HIGH	Deny	UDP Traffic	MONITORED
2	DB Sybase	Internet	UDP	Dns	6	HIGH	Deny	UDP Traffic	MONITORED
3	Dude	Int|Securify Router 1)	TCP	Auth	1	OK	Builtin	Incomplete Traffic Data	MONITORED
4	Dude	Int|Securify Router 1)	TCP	Auth	1	OK	OK	Connection Accepted Data Transfer	MONITORED
5	Dude	Int|Securify Router 1)	UDP	Dns	1	OK	OK	UDP Traffic	MONITORED
6	Dude	Syslog server	UDP	Syslog	1	OK	OK	UDP Traffic	MONITORED
7	Int|Securify Router 1|	Dude	TCP	Smtp	1	OK	Builtin	Incomplete Traffic Data	MONITORED
8	Int|Securify Router 1|	Dude	TCP	Smtp	1	OK	OK	Connection Accepted Data Transfer	MONITORED
9	Intranet Web	Securify Main	UDP	Udp	1	HIGH	Deny	UDP Traffic	MONITORED
10	Report Generator	Securify Main	TCP	SMB XPort	1	OK	Builtin	Incomplete Traffic Data	MONITORED
11	Rice	Managed Switch 1	UDP	Snmp	4	OK	OK	UDP Traffic	MONITORED
12	Securify Main	Dude	TCP	Pop3	1	OK	Builtin	Incomplete Traffic Data	MONITORED
13	Securify Main	Dude	UDP	Dns	3	OK	OK	UDP Traffic	MONITORED
14	Securify Main	Int|Securify Router 1)	UDP	Dns	11	HIGH	Deny	UDP Traffic	MONITORED
15	Securify Main	Internet	TCP	Http	1	OK	OK	Missed Request	MONITORED
16	Securify Main	Internet	TCP	Http	2	HIGH	OK	Non HTTP Traffic	MONITORED
17	Securify Main	Internet	TCP	Http	10	OK	Builtin	Incomplete Traffic Data	MONITORED
18	Securify Main	Internet	TCP	Http	12	OK	OK	Http Get Methods	MONITORED
19	Securify Main	Internet	UDP	Dns	14	HIGH	Deny	UDP Traffic	MONITORED
20	Securify Main	Non-Directed Broadcast	UDP	Nondirect...	15	OK	OK	UDP Traffic	MONITORED

000026|000026 37 Violations 101 Events 36.63% Modify Policy: ON

Figure 1-6 Studio Analysis Interface

It is important to mention that Securify™ Studio is an application installed on a computer running the Windows operating system. Securify™ Studio does not enforce any user role locally and therefore, any Windows user with the appropriate privileges can invoke Studio. Securify™ Studio does not protect the integrity and confidentiality of the security policy file while this file is stored on the local hard drive. To upload a new security policy on a Securify™ system using Studio, the user must be a Developer and be authenticated correctly by the Enterprise Manager.

The Securify™ Studio software runs on a standard PC with 1GHz or higher processor and 512MB or more RAM, running Windows 2000, Windows XP or Windows Vista.

The TOE does not include the underlying Windows operating system software, embedded databases or hardware to run Studio.

1.4.3.2 Securify^{TM} Monitor

Securify™ Monitor (Monitor) is a network monitoring system. Monitor evaluates real-time traffic on a continuous basis against the security policy. Monitor is available in the following forms:

- 1Gbps bandwidth version (Securify™ Monitor SE)
- 500 Mbps bandwidth version (Securify™ Monitor)
- 100Mbps bandwidth version (Securify™ Monitor LE)
- Flow Monitor which supports Cisco Netflow as an input (Securify™ Flow Monitor)

  NOTE: Flow Monitor is **not** included in the scope of the evaluation.

The software remains the same across all Monitor systems, but the ability to support higher traffic differs between the systems. From this point forward in this document, unless otherwise noted, the generic term Monitor will be used to refer to various forms: Monitor, Monitor SE, and Monitor LE.

Real-Time Monitoring: Monitor resides within a customer's network and evaluates, in real time, IPv4 and IPv6 packets flowing through the network at all levels of the protocol stack. Network transactions are automatically and continuously evaluated for conformance to a customer specific policy.

Analysis and Actions: Data related to network traffic is captured, evaluated, and stored as network and protocol events in a database for analysis and generating alerts. Monitor uses this data to make decisions on whether the traffic is consistent with the policy specification. This information is then presented in a Web-based analysis environment in terms specific to the business and actionable by the team running the network.

Controlled Access: To meet security and operational requirements, Monitor provides independent role-based access to views and system functionality. User-roles include: the Operator role, for viewing operations conformance data; the Analyst role, for analyzing the network security events generated by specific policies; the Developer role for creating, modifying and uploading policy; the SV Manager role for managing the operations of Securify™ Monitor; and the Account Manager role, for defining and managing user access to the application.

Real-Time Event Viewing and Reporting: Traffic conformance data can be accessed by way of a defined user role in real-time through a Web browser over SSL. The Monitor uses the network objects as defined in the policy, to provide the context to view network security events. Users can query details of recent network security events within a window of 48 hours. The Securify™ Monitor Web interface provides numerous views for traffic data. This enables the user to see live data by events or bandwidth, analyze specific events or signatures, analyze events by bandwidth, and so on. Users can also access data in a window of 4 weeks or more with Studio, depending upon the density of the network events.

Auditing: Monitor stores the results of monitored and evaluated network traffic in a local database. These records cannot be deleted or modified. In addition, Monitors keep an auditing trail of every transaction that occurs in the system. These audit trails are referred to as Application Logs and User Logs. Application Logs store audit trails of the application's internal subsystems, internal operations, Web- and application-related logs and system syslogs. User Logs store audit trails of every user transaction, including actions and configuration. A user must have a valid role to be able to download log files from the Web interface: the SV Manager role is required to download Application Logs and the Account Manager role is required to download User Logs. Furthermore, each Monitor allows the Enterprise Manager that manages it to pull both Application and User Logs.
Securify v6.0 Monitor also provides basic read, sort and search capabilities on its most important Application and User Log files by way of a character-based interface viewer. In order to use the viewer it is required both root and console access to the Monitor system.

Alerting: Monitor is able to send SNMP traps to network management systems to inform of any operational status change. Monitor is also able to send operational status changes and CORRELATED events via SMTP servers. The email addresses of the recipients of the SMTP alerts are configurable by a user with the SV Manager role. The Monitor is not able to verify their identities or their privileges.

1.4.3.3 Securify^{TM} Enterprise Manager

Securify™ Enterprise Manager aggregates and manages multiple Monitors into a single, real-time Web-based management console. Enterprise Manager provides a common operational environment for user access, Monitor configuration and policy management across multiple Monitors and policy domains.

With Enterprise Manager, real-time network security events and conformance information is viewable through a Web browser and can be presented in a variety of screens, ranging from general network health to detailed network event information about a given IP, host, service, or port in the network.

Management of Multiple Policy Domains: Policy management can be centralized by connecting multiple Monitors to an Enterprise Manager. Promoting (uploading a new security policy) and reverting (reactivating an old security policy) policy is performed on the Enterprise Manager by mapping a policy to one or more Monitors. Such mapping across Monitors is called a "Security Zone". A Monitor can run only one policy, but one policy can be run on multiple Monitors. The resulting network events can be viewed on the Enterprise Manager by individual Security Zones as well as across multiple ones. Administration of policy on stand-alone Monitors also utilizes the same policy-to-monitor mapping mechanism.

Controlled Access: Enterprise Manager enforces role-based access to views and system functionality to meet security and operational requirements. User-roles include: the Operator role, for viewing operations conformance data; the Analyst role, for analyzing the network security events generated by specific policies; the Developer role for creating, modifying, and promoting policy; the SV Manager role for managing the operations of Securify™ in the operations environment; and the Account Manager role, for defining and managing user access to the application

Real-Time Event Viewing and Reporting: Traffic conformance data can be accessed by way of a defined user role in real-time through a Web browser over SSL. The Enterprise Manager uses the network objects as defined in the policies (running in each connected Monitor) to provide the context to view aggregated network security events across multiple Monitors. Users can query details of recent network security events within a window of 48 hours. The Securify™ Enterprise Manager Web interface provides numerous views for traffic data. This enables the user to see live data by events or bandwidth, analyze specific events or signatures, analyze events by bandwidth, and so on.

Auditing: Enterprise Manager pulls network event data from the associated Monitors and stores this data in a local database for user consumption. This data is a reduced copy of the data stored in the Monitor's database. These records cannot be deleted or modified. Securify™ Enterprise Manager keeps an audit trail of all Application related transactions and User related transactions (these audit trails are described under the Auditing section of the Monitor component). A user must have a valid role to be able to download log files: the SV Manager role to download Application Logs and the Account Manager role to download User Logs from the Web interface. Besides roles, the user must also have permission to see the Security Zone where the Monitor resides to download any log file from a Monitor. The Enterprise Manager also has its own User Logs and Application Logs and a user must have the appropriate role (SV Manager for Application Logs and Account Manager for User Logs) on the Enterprise Manager to download them.

Securify v6.0 Enterprise Manager also provides basic read, sort and search capabilities on its most important Application and User Log files by way of a character-based interface viewer. In order to use the viewer it is required both root and console access to the Enterprise Manager system.

Alerting: Enterprise Manager has a data export capability by way of SNMP, Syslog and a proprietary XML API. The XML API is not included in the evaluation. Enterprise Manager can send SNMP traps to network management systems to inform of any operational status change or policy compliance violation (for example, when the policy compliance falls below a given threshold). Enterprise Manager is also able to send alerts regarding its operational status and policy compliance violations to an SMTP server.

Signature Update: Enterprise Manager can automatically connect to the Securify Negative Model Subscription Service (NMSS) and download the most current set of signatures (if the feature is enabled on the Enterprise Manager). The interval of time (in hours) for checking the Security NMSS updates is a configurable parameter.

1.4.3.4 Securify^{TM} Enterprise Reporting Gateway

The Securify™ Enterprise Reporting (ER) solution is composed of an ER Gateway (ERGW) and an ER Warehouse. Each of these is installed on a separate system.

NOTE: The ER Warehouse is **not** included in the TOE.

The ERGW includes a Web interface for administering the ERGW components. Users and roles are defined at the ERGW and are independent from users defined in the Enterprise Manager and Monitors.

The ERGW is a mechanism that enables you to deploy a more permanent repository of data (such as the ER Warehouse or a third-party data warehouse) from which you can generate quantitative network and application trend reporting from one or multiple Enterprise Managers.

Controlled Access: ERGW uses role-based access to views and system functionality to meet security and operational requirements. User-roles include: the ER SV Manager role for managing the operations of Securify v6.0 ERGW; and the ER Account Manager role, for defining and managing user access to the application.

Auditing: ERGW pulls network event data from the associated Enterprise Managers and stores this data temporarily in a local database before it is stored in the final data warehouse. These records cannot be seen, deleted or modified because ERGW is just a staging system to connect third-party warehouse implementation to the TOE. In addition, ERGW keeps an auditing trail of every transaction that occurs in the system. These audit trails are referred to as Application Logs and User Logs. Application Logs store audit trails of the application's internal subsystems, internal operations, Web- and application-related logs and system syslogs. User Logs store audit trails of every user transaction, including actions and configuration. A user must have a valid role to be able to download log files from the Web interface: the ER SV Manager role is required to download Application Logs and the ER Account Manager role is required to download User Logs.
Securify v6.0 ERGW also provides basic read, sort and search capabilities on its most important Application and User Log files by way of a character-based interface viewer. In order to use the viewer it is required both root and console access to the ERGW system.

Alerting: ERGW can send SNMP traps to network management systems to inform of any operational status change. ERGW is also able to send alerts regarding its operational status to an SMTP server.

1.4.3.5 Securify System Configurations and Inter-connections

Securify™ Version 6.0 (TOE) is a scalable security solution that enables customers to generate business-driven security policies, monitor networks for compliance, threats and known attack patterns, and produce relevant network operational information.

The Securify deployment could encompass just a single Monitor or a more complex monitoring infrastructure like the one shown in the full configuration (Figure 1-2). Although the functionality and capacity of a single Monitor is substantially lower than the full configuration, both deployments provide the same levels of confidentiality, integrity, availability and accountability.

Both configurations discussed in this section require Studio to create security policies and optionally, to perform advanced network analysis.

The following sections depict the security properties and configuration for the mentioned deployments: Stand-alone Monitor and the Full Configuration.

1.4.3.5.1 Stand-alone Monitor

This configuration consists of the following Securify components:

- Securify Studio
- One Securify Monitor

Studio

Securify Studio is a client application that is installed from a CD on a Windows computer. The OS enforces all discretionary controls for all local resources. This means that any authenticated user might be able to use Studio and open any security policy stored locally on that computer. Securify Studio does not enforce any user role nor does it provide confidentiality to or protect integrity of the security policy while stored locally. Securify recommends deploying dedicated computers for using Studio where only trusted users can log on.

In this configuration, a user with the Developer role can use Studio to create and modify policies locally, and manage them (upload or download) on the Monitor. All users can use Studio to evaluate security policies offline by way of DME files. Only users with the Analyst or Developer role can also perform online security analysis on the current Monitor data.

Studio does not maintain any security log on the local drive. It is assumed the computer where Studio runs has the appropriate security countermeasures to avoid unauthorized use.

Monitor

The Securify Monitor is a network-monitoring appliance that must have access to the network traffic under observation.

Regardless of the deployment configuration, the Securify Monitor is always the component in charge of capturing the network traffic. The Monitor analyzes the traffic against its current security policy to detect violations. The Monitor can show up to 48 hours of network data through the Web interface and up to 8 weeks with Studio.

Monitor – External Servers Interactions

A stand-alone Monitor may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify Monitor requires a valid time source for timestamp purposes. Ideally, the Monitor should synchronize its time with a valid NTP server. In cases where it is not possible to use an external NTP server, the Monitor can use the system local hardware clock.
SNMP	If configured, the Securify Monitor can send operational status changes, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Securify Monitor can alert operational status changes and policy compliance violations by way of SMTP. **Note**: the Securify Monitor does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Securify Monitor is able to export policy correlated events to any external SYSLOG server.
DNS	If configured, the Securify Monitor can use machine names instead of IP addresses and look up important DNS information.
SPAN Port	The Securify Monitor captures the network traffic directly from a port in the main switch where all the traffic is mirrored.

Securify Monitor Web interface

The Monitor provides a Web interface through which you can perform tasks such as analyze the network behavior, upload or download policies, maintain users and configure the system. The Monitor has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. For each user role, the Monitor ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Monitor’s Web interface using a regular Web browser and HTTPS. The Monitor presents a server certificate that the client uses to verify the Monitor during the SSL handshake. Optionally, the Monitor can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Monitor’s certificate can be either self-signed (default) or signed by any CA the user deems valid. It’s not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. A user with the SV Manager role is responsible for configuring this aspect of the system.

Log Files

With a stand-alone Monitor, neither the network event information nor the log files leave the Monitor unless a user with the appropriate role explicitly downloads them using the Web interface. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

The following table shows the files available for each role:

Role	Downloadable Information
Operator	none
Analyst	Captured DME
Developer	Captured DME
Account Manager	User logs
SV Manager	Application logs
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

The Monitor has different disk partitions exclusively used to store log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

For a stand-alone Monitor, log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Monitor does not generate an alert for these ordinary tasks.

DME files

These files are not considered log files and the Monitor stores them in a special partition. By default, the Monitor does not store DME files on disk. A user with the SV Manager role must explicitly enable their capture through the Monitor Web interface. It is important to mention that DME is a proprietary Securify format that compresses connection data. After capturing the network traffic, the Monitor transforms raw packets into this compact format before evaluating the security policy. If the user wants to use Studio to evaluate a policy offline, they have to download DME files to the local hard drive after authenticating to the Monitor with either the Analyst or Developer role.

Studio-Monitor Interaction
Securify Studio is a client application that enables the user to create and modify security policy, evaluate security policies offline using a DME file, analyze network events stored on a Monitor and download or upload security policies.

Some of these tasks require Studio to connect to the Monitor on behalf of the user. This connection is an SSL connection initiated by Studio where the Monitor presents its certificate and the user is authenticated by either a userid and password, or a certificate (depending on the user account configuration). It is important to mention that Monitor does not allow the SV Manager or Account Manager roles to connect remotely using Studio; only the Operator, Analyst and Developer roles can authenticate to the Monitor.

1.4.3.5.2 Full Configuration

The number of Securify v6.0 systems present in a full configuration varies. However, any full configuration of Securify v6.0 systems must have three hierarchical levels containing Monitors at the bottom, Enterprise Manager in the middle and ERGW at the top. Therefore, a full configuration may have multiple Monitors reporting to one Enterprise Manager and several Enterprise Managers reporting to one ERGW.
The full configuration used for testing purposes of the Securify v6.0 was representative of more complex full Securify v6.0 deployments without adding too many systems that would have complicated unnecessarily the tests. The chosen test configuration contained the following Securify v6.0 systems:

- Securify Studio
- Two Securify Monitors in two different Security Zones
  A security zone is one or more Securify Monitors that run the same security policy. Therefore, this configuration has two different Securify Monitors each one with a different security policy.
- One Securify Enterprise Manager to combine policy conformance and manage both Monitors
- One Securify Enterprise Reporting Gateway (ERGW)

Studio

Securify Studio is a client application that is installed from a CD on a Windows computer. The OS enforces all discretionary controls for all local resources. This means that any authenticated user might be able to use Studio and open any security policy stored locally on that computer. Securify Studio does not enforce any user role nor does it provide confidentiality to or protect integrity of the security policy while stored locally. Securify recommends deploying dedicated computers for using Studio where only trusted users can log on.

In this configuration, a user with the Developer role can use Studio to create and modify policies locally, and manage them (upload or download) on an Enterprise Manager. All users can use Studio to evaluate security policies from a Monitor or Enterprise Manager offline by way of DME files. Only users with the Analyst or Developer role can also perform online security analysis on the current Monitor or Enterprise Manager data.

Although it is possible to use Studio to upload security policies directly to a Monitor, the Enterprise Manager overwrites such changes to ensure that the Security Zone is consistent across the managed Monitors. This is also true for any configuration changes performed directly on the Monitors.

Monitors

The Securify Monitor is a network-monitoring appliance that must have access to the network traffic under observation.

Regardless of the deployment configuration, the Securify Monitor is always the component in charge of capturing the network traffic. The Monitor analyzes the traffic against its current security policy to detect violations. The Monitor can show up to 48 hours of network data through the Web interface and up to 8 weeks with Studio.

Monitors – External Servers Interactions

The Monitors may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify Monitors require a valid time source for timestamp purposes. Ideally, a Monitor should synchronize its time with a valid NTP server. Even though each Monitor could have its own time (as in locations with different time), it is possible to synchronize time among all the Monitors using the Enterprise Manager's time. In cases where it is not possible to use an external NTP server, the Monitors can use the system local hardware clock.
SNMP	If configured, the Monitors can send operational status changes, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Monitors can alert operational status changes and policy compliance violations by way of SMTP. **Note**: The Monitors do not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Monitors can export policy correlated events to any external SYSLOG server.
DNS	If configured, the Monitors can use machine names instead of IP addresses and look up important DNS information.
SPAN Port	The Monitors capture the network traffic directly from a port in the main switch where all the traffic is mirrored.

Securify Monitor Web interface

Each Monitor provides a Web interface through which you can perform tasks such as analyze the network behavior on that specific network segment, download security policies and maintain users local to that Monitor. In the full configuration, changes to a Monitor should be made through the Enterprise Manager Web interface. This includes uploading new policies. To ensure the integrity and consistency of the Security Zone, the Enterprise Manager overwrites changes made directly on its registered Monitors.

A Monitor has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. For each user role, the Monitor ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Monitor's Web interface using a regular Web browser and HTTPS. The Monitor presents a server certificate that the client uses to verify the Monitor during the SSL handshake. Optionally, the Monitor can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Monitor's certificate can be either self-signed (default) or signed by any CA the user deems valid. It's not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. An Enterpise Manager user with the SV Manager role and access to the Security Zone is responsible for configuring this aspect of the system.

Log Files

In the full configuration, each Monitor maintains its own set of log files locally. The type, number, and location of these log files are the same as in the stand-alone Monitor configuration. The log files do not leave the Monitor unless a user with the appropriate role explicitly downloads them using either the Monitor's Web interface or the Enterprise Manager Web interface.

An Enterprise Manager user can download any Monitor's log file using the Enterprise Manager Web interface. This is only possible if the user has the correct role and permission to access the Security Zone where the Monitor resides. This log transfer is twofold: one transfer from the Monitor to the Enterprise Manage and another transfer from the Enterprise Manager to the Web browser. The former connection is a normal intra-system connection protected by SSL (transparent to the user), while the latter is the already established SSL connection between the user's Web browser and the Enterprise Manager Web interface. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

Each Securify Monitor has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Securify Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

DME files

These files are not considered log files and the Monitor stores them in a special partition. By default, the Monitor does not store DME files on disk. A user with the SV Manager role must explicitly enable their capture through the Monitor Web interface. It is important to mention that DME is a proprietary Securify format that compresses connection data. After capturing the network traffic, the Monitor transforms raw packets into this compact format before evaluating the security policy. If the user wants to use Studio to evaluate a policy offline, they must download the DME files to the local hard drive by way of the Monitor's Web interface, after authenticating to the Monitor with either the Analyst or Developer role.

The following table shows the files available for each role on the Monitors:

Role	Downloadable Information
Operator	None
Analyst (defined on Monitor)	DME via Monitor Web interface.
Analyst (defined on Enterprise Manager)	DME via Enterprise Manager Web interface (security zone permission needed)
Developer (defined on Monitor)	DME via Monitor Web interface.
Developer (defined on Enterprise Manager)	DME via Enterprise Manager Web interface (security zone permission needed)
Account Manager (defined on Monitor or Enterprise Manager)	User logs via Monitor or Enterprise Manager Web interface
SV Manager (defined on Monitor)	Application logs via Monitor Web interface
SV Manager (defined on Enterprise Manager)	Application logs via Enterprise Manager Web interface (security zone permission needed)
root (defined at the OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, log files do not leave a system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Monitor does not generate an alert for these ordinary tasks.

Securify Enterprise Manager

The Enterprise Manager supervises the functional and configuration aspects of all Monitors registered to it. Enterprise Manager security is based on zones, where a security zone consists of one or more Monitors that run the same security policy.

The main tasks of the Enterprise Manager are:

- Aggregate network events generated by up to ten Monitors. The Enterprise Manager pulls network events from all registered Monitors on a regular basis and stores the data in the Enterprise Manager's internal database.
- Control the configuration of Security Zones and individual registered Monitors. The Enterprise Manager constantly ensures that each Monitor uses the correct security policy and configuration by overwriting anything that is changed directly on the Monitor.

- Enforce restricted access to both configuration and network event data based on user roles and security zones. Each user who has an account on the Enterprise Manager has associated user roles and security zones to restrict and control what she can do.

Enterprise Manager – External Servers Interactions

The Enterprise Manager may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify deployment requires a valid time source for timestamp purposes. Even though each Monitor could have its own time (as in locations with different time), it is possible to synchronize time among all the Monitors using the Enterprise Manager's time. The Enterprise Manager can be configured to use an external NTP server. In cases where it is not possible to use any external NTP server, Enterprise Manager can use the system local hardware clock.
SNMP	If configured, the Enterprise Manager can send operational status changes for itself or registered Monitors, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Enterprise Manager can alert operational status changes for itself or registered Monitors, and policy compliance violations by way of SMTP. **Note**: The Enterprise Manager does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Enterprise Manager can export policy correlated events to any external SYSLOG server.
DNS	If configured, the Monitors can use machine names instead of IP addresses and look up important DNS information.

Securify Enterprise Manager Web interface

The Securify Enterprise Manager provides a Web interface through which you can perform tasks such as view network behavior and policy compliance for all security zones at once or for any individual security zone. You can also configure the Enterprise Manager itself, a security zone and individual Monitors. The Enterprise Manager has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. Furthermore, all roles except Account Manager and SV Manager (for tasks related to the Enterprise Manager system only) also have a security zone scope. For each user role, the Enterprise Manager ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Enterprise Manager's Web interface using a regular Web browser and HTTPS. The Enterprise Manager presents a server certificate that the client uses to verify the Enterprise Manager during the SSL handshake. Optionally, the Enterprise Manager can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Enterprise Manager's certificate can be either self-signed (default) or signed by any CA the user deems valid. It's not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. The certificate used by the Enterprise Manager is used by the system to identify itself when communicating with users and other Securify v6.0 systems. Therefore, this is an internal configuration parameter of the Enterprise Manager that is not related to any Security Zone that can be configured by a user with SV Manager role.

Log Files

In a full configuration, the Enterprise Manager maintains its own set of local log files. These files are available for download by way of the Enterprise Manager Web interface if a user has the correct role. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

NOTE: Although it is possible to download a Monitor's log files by way of the Enterprise Manager Web interface, only downloading the Enterprise Manager log files is covered in this section.

The Enterprise Manager has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

The following table shows the files available for each role on the Enterprise Manager:

Role	Downloadable Information
Operator	none
Analyst	none
Developer	none
Account Manager	User logs
SV Manager	Enterprise Manager Application logs Monitor Application logs (from authorized security zones)
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, the Enterprise Manager log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Securify Enterprise Manager does not generate an alert for these ordinary tasks.

Securify Enterprise Reporting Gateway (ERGW)

The ERGW is a staging system whose main function is to aggregate network data from one or more Enterprise Managers. The ERGW prepares this information for more permanent data repositories. The ERGW is the interface from where external data warehouses obtain network information from the Securify infrastructure.

NOTE: No data warehouse, including the Securify Enterprise Reporting Warehouse (ERWH), is part of the TOE.

ERGW – External Servers Interactions

The ERGW may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify deployment requires a valid time source for timestamp purposes. The ERGW can be configured to synchronize its time with an external NTP server. In cases where it is not possible to use an external NTP server, the ERGW can use the system local hardware clock.
SNMP	If configured, the ERGW can send operational status changes to any SNMP server.
SMTP	If configured, the ERGW can alert operational status changes by way of SMTP. **Note**: The ERGW does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.

ERGW Web interface

The ERGW provides a Web interface through which you can configure and manage the system.

The ERGW Web interface only has two roles: SV Manager and Account Manager. Since the ERGW is an aggregation point, its Web interface does not provide any network data analysis tools. Instead, this interface is primarily used to configure the system to retrieve network data from one or more Enterprise Managers and to authorize external data warehouses to retrieve network data from the ERGW.

The SV Manager role is responsible for configuring the system, while the Account Manager role is responsible for maintaining users.

The users connect to the ERGW's Web interface using a regular Web browser and HTTPS. The ERGW presents a server certificate the client uses to verify the ERGW during the SSL handshake. Optionally, the ERGW can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The ERGW's certificate can be either self-signed (default) or signed by any CA the user deem valid. It's not possible to mix self-signed and signed certificates in the same deployment with interconnected

Securify v60_CC_9 systems. A user with SV Manager role is in charge of configuring this feature on the ERGW.

Log Files

The ERGW maintains its own set of local log files. These files are available for download by way of the ERGW Web interface if a user has the correct role. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

The ERGW has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application’s internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

The following table shows the files available for each role on the ERGW:

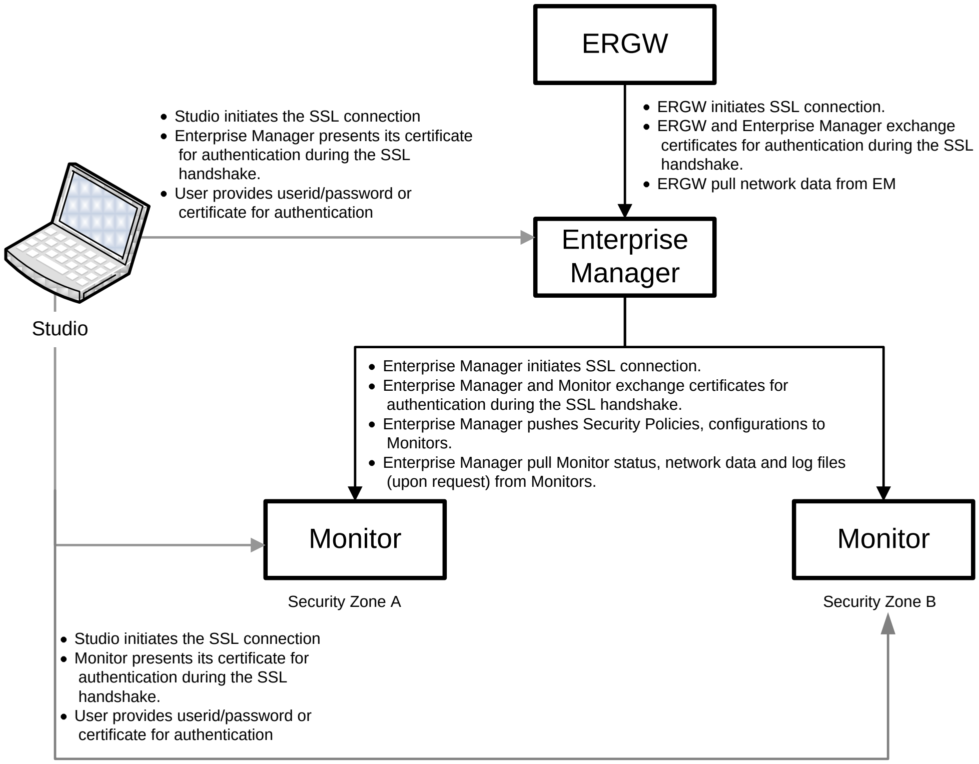
Role	Downloadable Information
Account Manager	User logs
SV Manager	Application logs
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, the ERGW log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The ERGW does not generate an alert for these ordinary tasks.

Interactions and Trusted Relationships between Securify Systems

In the full configuration, the individual Securify components must interact with one another so that network event data can move from the Monitor to the ERGW. Each interaction requires establishing mutually trusted relationships between the involved systems before the actual data moves.

The following picture depicts the Securify systems interacting in the full configuration:


ERGW
- ERGW initiates SSL connection.
- ERGW and Enterprise Manager exchange certificates for authentication during the SSL handshake.
- ERGW pull network data from EM
- Studio initiates the SSL connection
- Enterprise Manager presents its certificate for authentication during the SSL handshake.
- User provides userid/password or certificate for authentication
Enterprise Manager
Studio
- Enterprise Manager initiates SSL connection.
- Enterprise Manager and Monitor exchange certificates for authentication during the SSL handshake.
- Enterprise Manager pushes Security Policies, configurations to Monitors.
- Enterprise Manager pull Monitor status, network data and log files (upon request) from Monitors.
Monitor
Monitor
Security Zone A
Security Zone B
- Studio initiates the SSL connection
- Monitor presents its certificate for authentication during the SSL handshake.
- User provides userid/password or certificate for authentication

This section covers how the different trusted relationships are configured and how they are established through the network during normal operations.

Studio – Monitor/Enterprise Manager Interactions

During the interaction between Studio and a Monitor or Enterprise Manager, the trusted relationship is based on user credentials and Studio acts as the front-end to establish this relationship.

Studio enables users to connect to either an Enterprise Manager or a Monitor. Studio initiates the SSL connection and the Monitor or Enterprise Manager presents its certificate for server authentication during the SSL handshake. Optionally, if the user's account uses certificates instead of usernames and passwords, the server requests client certificates to complete a mutual authentication during the SSL handshake. If the user does not present either a client certificate or valid credentials, the Monitor or Enterprise Manager immediately resets the connection.

With the connection established, the user can upload/download security policies or analyze traffic data.

NOTE: You cannot upload security policies directly to a Monitor that is registered with an Enterprise Manager.

Enterprise Manager – Monitor Interactions

The Enterprise Manager must establish a secure SSL connection to each of the Monitors registered to it to retrieve network data and to enforce security zone configurations. This involves mutual authentication for each system, so the Enterprise Manager and Monitors must be properly configured beforehand.

Establishing a relationship between the Enterprise Manager and Monitors requires two separate SV Manager accounts: one for the Enterprise Manager and the other for the Monitor. It is important to understand that during this initial configuration, the SV Manager account for the Monitor is still a local Monitor account. Once the Enterprise Manager takes over the configuration of the Monitor, this SV Manager account is no longer useful. All subsequent configuration changes for the Monitor must be done by way of the Enterprise Manager Web interface using an Enterprise Manager account with the SV Manager role and access to the Security Zone where the Monitor resides.

Monitor Configuration:

- Identify the Enterprise Manager on the Monitor
  The SV Manager user on the Monitor must create a machine account for the Enterprise Manager to identify it on the Monitor. The SV Manager user does this by typing the Enterprise Manager's Common Name and certificate hash in the relevant locations.

Enterprise Manager Configuration:

- Synchronizing Clocks
  The SV Manager user on the Enterprise Manager must ensure that the Enterprise Manager and Monitor clocks are synchronized within a 5 minute interval.
- Security Zone
  If the Security Zone where the Monitor will reside does not exist, the SV Manager user on the Enterprise Manager must create it.
- Adding a Monitor
  The SV Manager user on the Enterprise Manager must add the new Monitor and provide the Monitor's Machine ID (unique identifier assigned to each Securify system) and the Monitor's IP address. When the SV Manager user on the Enterprise Manager submits this information, the Monitor's certificate is presented on the screen and the SV Manager user on the Enterprise Manager must accept it.

Establishing Connections

From this point on, the Monitor is under the administrative control of the Enterprise Manager and the Enterprise Manager gathers network event data every five minutes from all its registered Monitors.

Each time the Enterprise Manager contacts a Monitor, both the Enterprise Manager and the Monitor must present their certificates to authenticate each other and establish a trusted channel. If either the Enterprise Manager or the Monitor is not able to correctly authenticate the other system, the SSL connection is not established and the Enterprise Manager displays a warning status message on its Web interface. The Enterprise Manager may also send an SMTP and/or SNMP alert (depending on configuration).

ERGW – Enterprise Manager Interactions

The ERGW is responsible for collecting network event data from a set of Enterprise Managers to then provide this information to authorized data warehouse systems. It is important to remember that no warehouse implementations, including the Securify ERWH, are part of the TOE.

Configuration

The Securify ERGW must establish a secure SSL connection to each of the Enterprise Managers to collect network event data. This involves mutual authentication for each system, so the ERGW and Enterprise Managers must be properly configured beforehand.

Establishing a relationship between the ERGW and an Enterprise Manager requires two separate SV Manager accounts: one for the ERGW and the other for the Enterprise Manager.

Enterprise Manager Configuration

- Identify the ERGW on the Enterprise Manager
  The SV Manager user on the Enterprise Manager must create a machine account for the ERGW to identify it on the Enterprise Manager. The SV Manager user does this by typing the ERGW's Common Name and certificate hash in the relevant locations.

ERGW Configuration

- Synchronizing Clocks
  The SV Manager user on the ERGW must ensure that the ERGW and Enterprise Manager clocks are synchronized within a 5 minute interval.
- Adding an Enterprise Manager
  The SV Manager user on the ERGW must add the new Enterprise Manager and provide the Enterprise Manager's Machine ID (unique identifier assigned to each Securify system) and the Enterprise Manager's IP address. When the SV Manager user on the ERGW submits this information, the Enterprise Manager's certificate is presented on the screen and the SV Manager user on the ERGW must accept it.

Establishing Connections

From this point on, the ERGW can collect network event data from the Enterprise Manager every ten minutes.

Each time the ERGW contacts an Enterprise Manager, both the ERGW and the Enterprise Manager must present their certificates to authenticate each other and establish a trusted channel. If either the ERGW or the Enterprise Manager is not able to correctly authenticate the other system, the SSL connection is not established and the ERGW displays a warning status message on its Web interface. The ERGW may also send an SMTP and/or SNMP alert (depending on configuration).

1.4.4 Positive Model and Negative Models

Securify v6.0 combines in one security policy two different security models: positive and negative models:

Positive Model: this is the essential model Securify v6.0 employs to provide security. This non-optional model explicitly defines a positive behavior of the traffic in terms of what traffic is deemed acceptable on the monitored network. Despite of its name the positive model can also describe non-acceptable traffic.

The positive model relies on a on a proprietary policy language that translates business driven security policies into a formal, machine monitored specification (a “Policy”) describing the “correct” behavior of the network. This policy language enables users to define what service can be offered by one server, or what services a given set of hosts can access or what traffic is allow to conduct normal business operations.

A user with developer role defines this policy on Securify v6.0 Studio by creating network objects (e.g. networks, group of hosts or individual hosts) and relationships between them (e.g. host A can use HTTP on host B). When the policy is ready, she uploads the security policy with the positive model directly to the Monitor (i.e. non-managed Monitor) or Enterprise (i.e. managed Monitor).

Negative Model: This is an optional model (not required to operate a Securify v6.0 deployment) that requires a subscription to the Securify Negative Model Subscription Service (NMSS). The negative model relies on patterns of well-known network attacks (negative behavior) that are defined in a set of signatures. An internal component called signature engine loads the set of signatures at start-up time and inspects every network packet in search of any defined pattern. If found, the Securify v6.0 system generates a special violation called signature event.

The idea behind the negative model in Securify v6.0 systems is to complement the security coverage already provided by the positive model.

The negative model has two types of signatures:

- NMSS Signatures: these are the rules that Securify includes in the NMSS packets. Since the negative model complements the security of the positive model it is not expected that the negative model defines rules for any possible malicious pattern. In fact, a regular NMSS packet may have about four hundred signatures but only the most important rules are enabled by default. It is trivial to enable any existing rule in the NMSS using Studio however, for possible performance issues Securify does not recommend enabling all of the rules.
- Custom Signatures: besides the NMSS signatures users are able to adapt the negative model to their specific needs by creating their own rules. This is done in Studio and it is extensively documented in the Studio User Guide.

Note: More information regarding the positive and negative models and well as NMSS and custom signatures is available in the Studio User Guide.

1.4.5 Protocol Behaviors and Outcomes.

In order to create sound security policies Securify v6.0 users must understand the following concepts:

Protocol Behaviors: Securify V60 Monitor has a more complete model of certain network protocols. For these protocols Securify v6.0 is able to identify their common behaviors in terms of phases or states and even potential problems. For instance, Securify is able to identify WebDAV Methods or a URL decode errors on HTTP over TCP traffic.

Security v6.0 understands behaviors of the following network protocols:

Protocol	Transport	Application?
UDP	Yes	No
TCP	Yes	No
IP	Yes	No
ICMP	Yes	No
DNS (over TCP/UDP)	No	Yes
FTP (over TCP)	No	Yes
HTTP (over TCP)	No	Yes
SSH (over TCP)	No	Yes
SSL (over TCP)	No	Yes

Securify v6.0 also identifies some other protocols even if they do not use their well-known ports. However, for this set of protocols Securify cannot model their internal behaviors and therefore, it is not able to break them down into their pieces. Some of these protocols are:

Protocols Where Transport is IP Only
- GRE (non-application)

Protocols Where Transport is UDP Only
- DHCP
- GNUTELLA-GND
- SNMP
- TEAMSPEAK
- WINS

Protocols Where Transport is TCP Only
- BITTORRENT
- GNUTELLA-TCP
- IMAP
- IRC
- Kerberos
- LPD
- PGSQL
- POP
- RDP
- SKYPE-LOGON
- SMB
- SMTP

WOW

Protocols Where Transport is Combination

SIP (TCP/UDP)
RTP (TCP/UDP)
AIM (TCP/HTTP)
YIM (TCP/HTTP)

Outcomes: Securify v6.0 classifies traffic based on categories of behaviors named outcomes. These outcomes simply group protocol behaviors that are deemed to be at same level of importance. They are used in security policies to call out anticipated behavior on a given network in terms of “good” or “bad” behaviors.

Behaviors are protocol-specific actions that are observed when a network event occurs. A criticality specifies the level of attention a behavior requires.

For instance, the Netbios service (for Windows file sharing) is generally considered acceptable within corporate Intranets. Therefore, for this example it may be appropriate to assign the outcome “Expected” to Netbios. On the other hand, Netbios packets coming from the Intranet to the Internet or packets sent to a production server can be assigned the outcome Unexpected.

Note: the concepts of protocol behavior and outcomes are extensively explained in the Studio User Guide.

1.4.6 Rate Limiting

Securify v6.0 like any other IDS system can process up to certain amount of traffic. Beyond that limit, IDS systems are saturated and they usually drop network packets reducing their security coverage. Although this is a limitation of the IDS technology, it is not deemed too critical because any successful attack would be immediately noticed because of the amount of traffic required to perform a Denial of Service (DoS) attack on a well-designed IDS system.

Securify v6.0 Monitor does not dropping networks packets randomly, instead Securify v6.0 systems employ a proprietary rate-limiting algorithm to intelligently drop packets that belong to certain connections only. When Securify v6.0 Monitor reaches its saturation point it tags some connections and only drops packages that belong to those connections. This approach keeps intact the rest of the connections reducing the overall impact of any successful DoS attack.

1.4.7 Data

Application Log Data	Audit trail of all system functions with the exception of user related functions
User Log Data	Audit trail of user related functions
Event Data	Same as Analyzer Data
Analyzer Data	Data collected by the Analyzer functions
Scanner Data	Data collected by the Scanner functions
Sensor Data	Data collected by the Sensor functions
TSF Data	Data created by and for the TOE, that might affect the operation of the TOE.

1.4.8 Users

Securify v6.0 Monitor, Enterprise Manager and ERGW maintain its own definition of users and roles. These are not shared among these components. When properly configure Enterprise Manager and Monitor(s) can establish a full trust relationship that allows users of Enterprise Manager to access data and manage its security functions through the Enterprise Manager Web UI.

Additionally, Securify v6.0 Monitor, Enterprise Manger and ERGW have two local users at the operating system level: root and svs.

- **root**: this is the super user for any regular Linux OS and therefore, this account must be assigned to a very trusted administrator. Although this account is not honored at the application level it can perform ANY action in the system including manipulating the database and log files.
  Securify highly recommends following security best practices to use this account only to perform directly on the console those tasks that cannot be executed from the systems' Web interfaces such as network parameter changes, read/sort of audit logs, etc.
  Since root is able to manipulate and remove log files, the system might not log the commands performed by root. However, I&A events are logged in /var/log/messages.
- **svs**: this is an internal account used to run certain internal processes without root privileges. This account is not honored at the application level. Securify recommends to make sure the svs account is assigned to the same administrator in charge of the root account.

Both OS local accounts, svs and root, require physical access to the system's console. These accounts are authenticated by way of regular usernames and passwords like any other Linux account. Therefore, Securify assumes final users took the required countermeasures to limit and secure the physical access to the system. Securify strongly recommends following security best practices to assign these accounts only to trusted administrators and choose strong passwords to protect these accounts at the installation time.

Securify Studio does not have a local user role definition for accessing Studio functions. Users that are able to log in to the Windows OS in which Studio reside would have access to the Securify Studio application and all the local data stored in the Windows file system. In order to access Monitor or Enterprise Manager from Studio, the user must provide credentials of a valid user defined in either Monitor or Enterprise Manager respectively.

The following table summarizes user roles and functionality per component

User Access Policy: Roles / Subjects								
Objects	Operator	Analyst	Developer	SV Manager	Account Manager	ER SV Manager	ER Account Manager	root (OS level)
Network Event Data	View	View	View					
Machines	View Status	View Status	View Status Start/Restart/ Stop	View Status Start/Restart/ Stop	View Status	View Status Start/Restart/ Stop	View Status	
DMEs		Download	Download/Read					
User Access/Definition					Manage		Manage	
Policy History	View	View	View					
Policies		Extract	Upload Revert Extract					
Application Logs				Download		Download		Read/Sort/Search local application log. (console access required)
User Logs					Download		Download	Read/Sort/Search local user log. (console access required)

1.4.9 Product Guidance

The following are the user documents provided to cover all functionality of the product:

- Securify^{TM} Studio User Guide version 6.0
- Securify^{TM} Web Application Operations Guide version 6.0
- Securify^{TM} Installation Guide version 6.0
- Securify^{TM} Deployment Guide version 6.0
- Securify^{TM} Enterprise Reporting Operations Guide version 6.0
- Securify^{TM} Release Notes version 6.0
- Securify^{TM} v6.0 Admin Supplemental Guide for Common Criteria
- Securify^{TM} v6.0 Administrator Addendum

1.4.10 Physical Scope of the TOE

The evaluated configuration includes the following:

- Securify^{TM} Studio: 6.0 (Build V60_CC_9)
  The Securify™ Studio software running on a standard PC with 1GHz or higher processor and 512MB or more RAM, running version 2000, XP or Vista of the Microsoft Windows operating system.

The TOE does not include the underlying windows operating system software, embedded databases or hardware.

- Securify^{TM} Monitor: 6.0 (Build V60_CC_9)
  The Securify Monitor comprises Patriot SB5000 Platform Woodcrest Dual Core CPU systems with Monitor software running on proprietary OS and Hardware.

  Other configuration information:
  CPU: 1x2 GHz – 5130
  Memory: 4 GBytes
  Drives: 2 x 74G @ 10K revolutions
  OS: CentOS 4.1
  Network interface: Ethernet 1 (Eth 1)
  Network Interface: Ethernet 2 (Eth2)
  All Software, Operating System and Hardware mentioned above are included in the TOE.

- Securify^{TM} Monitor (LE): 6.0 (Build V60_CC_9)
  The Securify Monitor (LE) comprises Patriot SB5000 Platform Woodcrest Dual Core CPU systems with Monitor software running on proprietary OS and Hardware.

  Other configuration information:
  CPU: 1x2 GHz – 5130
  Memory: 4 GBytes
  Drives: 2 x 74G @ 10K revolutions
  OS: CentOS 4.1
  Network interface: Ethernet 1 (Eth 1)
  Network Interface: Ethernet 2 (Eth2)

  All Software, Operating System and Hardware mentioned above are included in the TOE.

- Securify^{TM} Monitor (SE): 6.0 (Build V60_CC_9)
  The Securify Monitor (LE) comprises Patriot SB5000 Platform Woodcrest Dual Core CPU systems with Monitor software running on proprietary OS and Hardware.

  Other configuration information:
  CPU: 1x2.66 GHz - 5150
  Memory: 4 GBytes
  Drives: 2 x 74G @ 10K revolutions
  OS: CentOS 4.1
  Network interface: Ethernet 1 (Eth 1)
  Network Interface: Ethernet 2 (Eth2)

  All Software, Operating System and Hardware mentioned above are included in the TOE.

- Securify^{TM} Enterprise Manager: 6.0 (Build V60_CC_9)
  The Securify^{TM} Enterprise Manager comprises Patriot SB5000 Platform Woodcrest Dual Core CPU systems with Enterprise Manager version 6.0 software running on proprietary OS and Hardware.

  Other configuration information:
  CPU: 1x2.66 GHz – 5150
  Memory: 4 GBytes

Drives: 2 x 74G @ 10K revolutions
OS: CentOS 4.1
Network interface: Ethernet 1 (Eth 1)
Network Interface: Ethernet 2 (Eth2)

All Software, Operating System and Hardware mentioned above are included in the TOE.

- Securify^{TM} Enterprise Reporting Gateway: 6.0 (Build V60_CC_9)
  The Securify^{TM} Enterprise Reporting Gateway comprises Patriot SB5000 Platform Woodcrest Dual Core CPU systems with Enterprise Reporting Gateway version 6.0 software running on proprietary OS and Hardware.

  Other configuration information:
  CPU: 1x2.00 GHz - 5130
  Memory: 4 GBytes
  Drives: 3 x 74G @ 10K revolutions
  OS: CentOS 4.1
  Network interface: Ethernet 1 (Eth 1)
  Network Interface: Ethernet 2 (Eth2)

  All Software, Operating System and Hardware mentioned above are included in the TOE.

The following are not included in the Evaluation Scope:

- Securify^{TM} Flow Monitor
- Securify^{TM} Enterprise Reporting v6.0 Warehouse is not included in the scope of this evaluation.
- Securify^{TM} Enterprise Global v6.0 is not included in the scope of this evaluation
- Distributed Login Collector (DLC), which connects in to a number of directory controllers for one or more Microsoft Windows Active Directory domains is not included in the scope of this evaluation. Hence, Identity based monitoring and its components (i.e. DLC) and the ability of Securify Studio to develop identities based policy is outside the scope of this evaluation.
- Active vulnerability Scanner management (known as Vulnerability Assessment feature) and Packet Capture though shipped with the Monitor and Enterprise Manager products are not part of the evaluation. These features are turned off by default and must be remain off in the evaluated configuration.
- Management of the Monitor, Enterprise Manager and ERGW using SSH is disabled in the evaluated configuration.
- The Securify proprietary XML API for exporting network events to external Security Information Event Management (SIEM) systems.

Component Interfaces:

TOE Component	Internal Interfaces	External Interfaces
Securify Studio	SSL to Monitor/Enterprise Manager (Data Analysis)	DNS (optional)
Securify Monitor	SSL from Studio (Data Analysis) SSL from Enterprise Manager (Data and Management)	DNS (optional) SNMP (Network Management) SMTP (Network Management) NTP SSL from users (Configuration and Data Analysis)
Securify Enterprise Manager	SSL from Studio (Data Analysis, Policy and Signature configuration) SSL to Monitor (Data Analysis and Management) SSL from ERGW (Data Migration)	DNS (optional) SNMP (Network Management and SIEM) SMTP (Network Management) Syslog (SIEM) NTP SSL (Configuration and Data Analysis) SSL to NMSS service (Signature configuration)
Securify Enterprise Reporting Gateway (ERGW)	SSL to Enterprise Manager (Data Migration)	SNMP (Network Management) SMTP (Network Management) NTP SSL from users (Configuration) SSL to ER Warehouse (Data migration and management)

Components on the IT Environment:

The IT environment needs to provide the following capabilities:

- SNMP servers are required for alerting system status changes, policy compliance violations and exporting critical policy violations.
- SMTP servers are required for alerting system status changes and policy compliance violations.
- SYSLOG servers are required for export of critical policy violations.
- NTP server is required for SecurifyTM relies upon to obtain reliable time stamps
- DNS server
- The Securify™ Monitor requires the availability of a SPAN port where traffic to be monitored is mirrored to.
- SecurifyTM Enterprise Reporting Warehouse is a third party product and therefore is not considered part of the TOE environment
- Computer System(s) with SSL/TLS enabled Web browser to logon to the Monitor(s), Enterprise Manager(s) and ERGW.
- Computer System with 1GHz or higher processor and 512MB or more RAM, running version 2000, XP or Vista of the Microsoft Windows operating system to host the Studio software.

1.4.11 Logical Scope of the TOE

The TOE provides the following security features:

- Manage User Functions
  Securify^{TM} provides its own access control (authorization) separate from the Operating System between subjects and objects within the TOE's Scope of Control. This is covered by the Securify^{TM} User Access Policy.
- User Login Functions
  Securify^{TM} provides user identification and authentication through the use of user accounts.
- Audit Functions
  Securify^{TM} provides its own auditing capabilities separate from those of the Operating System.
- Self Protection Functions
  Securify^{TM} protects its programs and data from unauthorized access through its own interfaces.
- IDS Functions
  Securify^{TM} provides the ability of detecting potential intrusions to the network by evaluating network traffic against the Securify Policy and alerting on deviation from expected prescribed behavior and alerting on the matching to explicit behavioral malicious patterns.

Please see Section 7 for additional details.

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 from the Common Criteria Version 3.1 R2.

2.2 Protection Profile Claim

This Security Target claims conformance to U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007. (IDS System Protection Profile).

- This Security Target includes all of the threats described in the Protection Profile, verbatim, except:

  - T.SCNCFG, T.SCNMLC and T.SCNVUL: these are threats that apply to IDS systems with active scanning functionality and do not apply to the TOE as it does not provide any active scanning functionality.

- This Security Target includes all of the assumptions in the Protection Profile. verbatim, except:

  - A.SECWH: This assumption is not present in the Protection Profile. It was added to the Security Target to emphasize that users must take all countermeasures required to protect the IDS data when stored in the Securify v6.0 ERWH (not part of the TOE) or any other third-party data warehouse implementation.
  - SECSTD: This assumption is not present in the Protection Profile. It was added to the Security Target to ensure that the Windows operation system where Securify Studio v6.0_CC_9 and the Web browser to interact with the Securify v6.0_CC_9 Web interface are installed is protected from tampering by using best IT practices. This Windows host must be used to interact with Securify v6.0_CC_9 systems only.

- This Security Target includes all of the Security Objectives from the Protection Profile, verbatim, except:

  - O.IDSCAN: This objective does not apply to the TOE as it is an objective that mitigates the threats related to scanning functionality.
  - O.EXPORT: This objective is removed from the Security Target based on PD-0097. O.EXPORT objective was erroneously replicated into the system Protection Profile.
  - O.SECTRANS: This objective is not present in the Protection Profile. It was added to the Security Target to ensure the TOE guarantees the confidentiality and integrity of the IDS data while in transit.

- This Security Target includes all of the Security Functional and Security Assurance Requirements from the Protection Profile, except:
  - Those SFRs exclusively related to authenticating or communicating TSF data with external IT products, specifically: FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.2, have been replaced by FPT_ITT.1 through the precedence of PD-0097.
  - FMT_SMF.1 has been added to satisfy the dependencies of FMT_MOF.1 and FMT_MTD.1
  - The Security requirements IDS_SDC_EXT.1, IDS_ANL_EXT.1, IDS_RCT_EXT.1, IDS_RDR_EXT.1, IDS_STG_EXT.1 and IDS_STG_EXT.2 are added instead of the IDS requirements in the Protection Profile. All of the components defined below have been modeled on components from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. They had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality.
  - FCS_COP.1: This security functional requirement is not present in the Protection Profile. This SRF was added to the Security Target to protect the IDS data against unauthorized disclosure and modification when it is transmitted over a network. FCS_CKM.1 Cryptographic key generation and FCS_CKM.4

Cryptographic key destruction are not further expanded because there are not functional requirements for key management. In particular, no user intervention is involved with the processes of creation, distribution, access and destruction of any cryptographic key for the operation of the TOE.

2.3 Package Claim

This ST claims conformance to the EAL2 assurance requirements package augmented with ALC_FLR.2.

3 Security Problem Definition

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

Table 3-1 TOE Threats

Threats		
1	T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
2	T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
3	T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
4	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
5	T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
6	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
7	T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
8	T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

Table 3-2 TOE IT System Threats

Threats		
9	T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
10	T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

Threats		
11	T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
12	T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
13	T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
14	T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
15	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
16	T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
17	T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

Application Note: the active scanner functionality is not included in the TOE. Therefore, T.SCNCFG, T.SCNMLC and T.SCNVUL does not apply to Securify v6.0.

3.2 Organisational Security Policies (OSPs)

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

Table 3-3 Organisational Security Policies

Organizational Security Policies		
1	P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
3	P.MANAGE	The TOE shall only be managed by authorized users.
4	P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
5	P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
6	P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
7	P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-4 OE Usage Assumptions

TOE Intended Usage Assumptions		
1	A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
2	A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
3	A.ASCOPE	The TOE is appropriately scalable to the IT system the TOE Monitors

Table 3-5 TOE Physical Assumptions

TOE Physical Assumptions		
4	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
5	A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Table 3-6 TOE Personnel Assumptions

TOE Personnel Assumptions		
7	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
8	A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
9	A.NOTRST	The TOE can only be accessed by authorized users
10	A.SECWH	The administrator implements all security countermeasures to protect the confidentiality, integrity and availability of the IDS data when stored in the ERWH (not part of the TOE) or any other third-party data warehouse solution.
11	A.SECSTD	The operating system that hosts Securify v6.0 Studio and the Web browser to access the Securify v6.0 Web interface is protected from tampering by best IT practices. This system is only used to access Securify v6.0 systems.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives

4.1.1 Security Objectives for the TOE

The following are the TOE security objectives:

Table 4-1 TOE Security Objectives

TOE Security Objectives		
1	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
2	O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion of the occurrence of a past intrusion of an IT System
3	O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
4	O.IDSANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
5	O.RESPON	The TOE must respond appropriately to analytical conclusions
6	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data
7	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data
8	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data
9	O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows
10	O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
11	O.INTEGR	The TOE must ensure the integrity of all audit and System data.
~~12~~	~~O.EXPORT~~	~~When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.~~
12	O.SECTRANS	The TOE must ensure the confidentiality and integrity of the IDS data while in transit.

Application Note: the active scanner functionality is not included in the TOE. Therefore, O.IDSCAN does not apply to Securify v6.0.

4.1.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are as follows:

Table 4-2 Security Objectives for the Operational Environment

Security Objectives for the Operational Environment		
13	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
14	OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information
15	OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
16	OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
17	OE. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
18	OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
19	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
20	OE.INTROP	The TOE is interoperable with the IT System it monitors.

4.2 Relation between security objectives and the security problem definition

4.2.1 Tracing between security objectives and the security problem definition

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Intrusion Detection System System Protection Profile. Table below Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 4-3 Security Objectives and Security Environment Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECTRANS	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
A.ACCESS																	X			
A.DYNMIC																X	X			
A.ASCOPE																	X			
A.PROTCT														X						
A.LOCATE														X						
A.MANAGE																X				
A.NOEVIL													X	X	X					
A.NOTRUST														X	X					
T.COMINT	X						X	X			X	X								
T.COMDIS	X						X	X				X								
T.LOSSOF	X						X	X			X									
T.NOHALT		X	X	X			X	X												
T.PRIVIL	X						X	X												
T.IMPCON						X	X	X												
T.INFLUX									X											
T.FACCNT										X										
T.SCNCFG		X																		
T.SCNMLC		X																		
T.SCNVUL		X																		
T.FALACT					X															
T.FALREC				X																
T.FALASC				X																
T.MISUSE			X																	
T.INADVE			X																	
T.MISACT			X																	
P.DETECT		X	X							X								X		
P.ANALYZ				X																
P.MANAGE	X					X	X	X					X		X	X				
P.ACCESS	X						X	X												X
P.ACCACT								X		X								X	X	
P.INTGTY											X									
P.PROTCT									X					X						

4.2.2 Providing a justification for the tracing

A.ACCESS: The TOE has access to all the IT System data it needs to perform its functions*.*

> The OE.INTROP objective ensures the TOE has the needed access.

A.DYNMIC: The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors*.*

> The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE: The TOE is appropriately scalable to the IT System the TOE monitors*.*

> The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT: The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

> The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

> The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

> The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL: The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

> The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST: The TOE can only be accessed by authorized users.

> The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.SECWH: The administrator implements all security countermeasures to protect the confidentiality, integrity and availability of the IDS data when stored in the ERWH (not part of the TOE) or any other third-party data warehouse solution.

> The OE.AUDIT_PROTECTION objective provides the capability to protect audit information including IDS data when stored out of the control of the TOE.

A.SECSTD: The Operating System of the host where Studio is installed only accepts login from users that also have Securify roles of analyst or developer only.

> The OE.INSTALL objective ensures that the OS where Studio is installed, managed and operated in a manner that is consistent with IT security.

T.COMINT: An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

> The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. The O.SECTRANS objective ensures no TOE data will be modified while in transit between TOE components.

T.COMDIS: An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

> The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The O.SECTRANS objective ensures no TOE data will be disclosed while in transit between TOE components.

T.LOSSOF: An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

> The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT: An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

> The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

> The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON: An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

> The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX: An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

> The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

T.FACCNT: Unauthorized attempts to access TOE data or security functions may go undetected.

> The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.SCNCFG: Improper security configuration settings may exist in the IT System the TOE monitors.

> The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

T.SCNMLC: Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

> The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.

T.SCNVUL: Vulnerabilities may exist in the IT System the TOE monitors.

> The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of vulnerability. The ST will state whether this threat must be addressed by a Scanner.

T.FALACT: The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

> The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC: The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

> The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC: The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

> The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

> The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INADVE: Inadvertent activity and access may occur on an IT System the TOE monitors.

> The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.MISACT: Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

> The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

P.DETECT: Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

> The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

P.ANALYZ: Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

> The O.IDANLZ objective requires analytical processes are applied to data collected from Sensors and Scanners.

P.MANAGE: The TOE shall only be managed by authorized users.

> The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS: All data collected and produced by the TOE shall only be used for authorized purposes.

> The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT: Users of the TOE shall be accountable for their actions within the IDS.

> The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

P.INTGTY: Data collected and produced by the TOE shall be protected from modification.

> The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT: The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

> The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

4.3 Security Objectives: Conclusion

Based on the security objectives and the security objectives rationale, the following conclusion can be drawn: the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

5 Extended Components Definition

All of the components defined below have been modeled on components from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. The extended components are denoted by adding "_EXT" in the component name.

Table 5-1 Extended Components

Item	SFR ID	SFR Title
1	IDS_SDC_EXT.1	System Data Collection
2	IDS_ANL_EXT.1	Analyser analysis
3	IDS_RCT_EXT.1	Analyser react
4	IDS_RDR_EXT.1	Restricted Data Review
5	IDS_STG_EXT.1	Guarantee of System Data Availability
6	IDS_STG_EXT.2	Prevention of System data loss

5.1 IDS_SDC_EXT.1 System Data Collection

5.1.1 Extended Component Definition

5.1.1.1 Class IDS: Intrusion Detection System

5.1.1.2 Family: System Data Collection (IDS_SDC)

5.1.1.2.1 Family Behavior

This family defines the requirements for the TSF to be able to collect information from targeted IT System resources.

5.1.1.3 Management

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s);

b) the management (addition, removal, or modification) of specific targeted IT System resources.

5.1.1.4 Audit

There are no auditable events foreseen.

5.1.1.5 Definition

IDS_SDC_EXT.1 System Data Collection

Hierarchical to: No other components.

IDS_SDC_EXT. 1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) **[*selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities***]; and

b) [**assignment:** ***other specifically defined events***].

IDS_SDC_EXT. 1.2 At a minimum, the System shall collect and record the following information

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

b) The additional information specified in the *Details* column of Table 3-2 System Events.

Table 5-2 System Events

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	1 Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Start-up and shutdown of audit functions	none
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked, passwords, account policy, parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known, vulnerability

Dependencies: No dependencies

5.1.1.6 Rationale

IDS_SDC_EXT.1 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_SDC_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically system data collection.

5.2 IDS_ANL_EXT.1 Analyser analysis

5.2.1 Extended Component Definition

5.2.1.1 Class IDS: Intrusion Detection System

5.2.1.2 Family: Analyser analysis (IDS_ANL)

5.2.1.3 Family Behavior

This family defines the requirements for the TSF to be able to analyze the IDS data that has been gathered from targeted IT System resources.

5.2.1.4 Management

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s).

5.2.1.5 Audit

There are no auditable events foreseen.

5.2.1.6 Definition

IDS_ANL_EXT.1 Analyser analysis

Hierarchical to: No other components.

IDS_ANL_EXT.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [**selection:** ***statistical, signature, integrity***]; and

b) [assignment: ***other analytical functions***].

IDS_ANL_EXT.1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: ***other security relevant information***]

Dependencies: IDS_SDC_EXP.1

5.2.1.7 Rationale

IDS_ANL_EXT.1 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_ANL_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the analysis function.

5.3 IDS_RCT_EXT.1 Analyser react

5.3.1 Extended Component Definition

5.3.1.1 Class IDS: Intrusion Detection System

5.3.1.2 Family: Analyser react (IDS_RCT)

5.3.1.3 Family Behavior

This family defines the requirements for the TSF to be able to send an alarm and react when an intrusion is detected.

5.3.1.4 Management

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

5.3.1.5 Audit

There are no auditable events foreseen.

5.3.1.6 Definition

IDS_RCT_EXT.1 Analyser react

Hierarchical to: No other components.

IDS_RCT_EXT.1.1 The System shall send an alarm to [**assignment: *alarm destination*]** and take [**assignment: *appropriate actions***] when an intrusion is detected.

Dependencies: IDS_SDC_EXP.1

5.3.1.7 Rationale

IDS_RCT_EXT.1 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_RCT_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the alarm and reaction function.

5.4 IDS_RDR_EXT.1 Restricted Data Review

5.4.1 Extended Component Definition

5.4.1.1 Class IDS: Intrusion Detection System

5.4.1.2 Family: Security data review (IDS_RDR)

5.4.1.3 Family Behavior

This family defines the requirements for data tools that should be available to authorized users to assist in the review of system data.

5.4.1.4 Management

There are no management activities foreseen.

5.4.1.5 Audit

There are no auditable events foreseen.

5.4.1.6 Definition

IDS_RDR_EXT.1 Restricted Data Review

Hierarchical to: No other components.

IDS_RDR_EXT.1.1 The System shall provide [assignment: ***authorised users***] with the capability to read [assignment: ***list of System data***] from the System data.

IDS_RDR_EXT.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3. The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

Dependencies: IDS_SDC_EXP.1

5.4.1.7 Rationale

IDS_RDR_EXT.1 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_RDR_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the restricted data review function.

5.5 IDS_STG_EXT.1 Guarantee of System Data Availability

5.5.1 Extended Component Definition

5.5.1.1 Class IDS: Intrusion Detection System

5.5.1.2 Family: System data storage (IDS_STG)

5.5.1.3 Family Behavior

This family defines the requirements for the TSF to be able to secure system data.

5.5.1.4 Management

a) There are no management activities foreseen.

5.5.1.5 Audit

There are no auditable events foreseen.

5.5.1.6 Definition

IDS_STG_EXT.1 Guarantee of System Data Availability

Hierarchical to: No other components.

IDS_STG_EXT.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_STG_EXT.1.2 The System shall protect the stored System data from modification.

IDS_STG_EXT.1.3. The System shall ensure that [assignment: ***metric for saving System data***] System data will be maintained when the following condition occurs: [**selection: *System data storage exhaustion, failure, attack***].

Dependencies: IDS_SDC_EXT.1

5.5.1.7 Rationale

IDS_STG_EXT.1 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_STG_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the guarantee of system data availability.

5.6 IDS_STG_EXT.2 Prevention of System data loss

5.6.1 Extended Component Definition

5.6.1.1 Class IDS: Intrusion Detection System

5.6.1.2 Family: System data storage (IDS_STG)

5.6.1.3 Family Behavior

This family defines the requirements for the TSF to be able to secure system data.

5.6.1.4 Management

The following actions could be considered for the management functions in FMT:
a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

5.6.1.5 Audit

There are no auditable events foreseen.

5.6.1.6 Definition

IDS_STG_EXT.2 Prevention of System data loss (EXT)

Hierarchical to: No other components.

IDS_STG_EXT.2.1	The System shall [**selection:** ***'ignore System data', 'prevent System data, except those taken by the authorised user with special rights', 'overwrite the oldest stored System data*** '] and send an alarm if the storage capacity has been reached.

Dependencies: IDS_SDC_EXT.1

5.6.1.7 Rationale

IDS_STG_EXT.2 is from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 July 25, 2007. IDS_STG_EXT.2 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the prevention of system data loss.

6 Security Requirements

6.1 Security Functional Requirements

The TOE security functional requirements are listed in Table 6-1. They are all taken from Part 2 of the Common Criteria.

Table 6-1 Functional Components

("*" refers to all iterations of a component)

TOE Security Functional Components		
No.	**Component**	**Component Name**
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit review
3	FAU_SAR.2	Restricted audit review
4	FAU_SAR.3	Selectable audit review
5	FAU_SEL.1	Selective audit
6	FAU_STG.2	Guarantees of data availabitlity
7	FAU_STG.4	Prevention of audit data loss
8	FIA_UAU.1	Timing of authentication
9	FIA_AFL.1	Authentication failure handling
10	FIA_ATD.1	User attribute definition
11	FIA_UID.1	Timing of identification
12	FMT_MOF.1	Management of security functions behavior
13	FMT_MTD.1	Management of TSF data
14	FMT_SMF.1	Specification of Management Functions
15	FMT_SMR.1	Security roles
16	FPT_ITT.1	Basic internal TSF data transfer protection
17	FPT_STM.1	Reliable time stamps
18	IDS_SDC_EXT.1	System Data Collection (EXT)
19	IDS_ANL_EXT.1	Analyzer analysis (EXT)
20	IDS_RCT_EXT.1	Analyzer react (EXT)
21	IDS_RDR_EXT.1	Restricted Data Review (EXT)
22	IDS_STG_EXT.1	Guarantee of System Data Availability (EXT)
23	IDS_STG_EXT.2	Prevention of System data loss (EXT)
24	FCS_COP.1	Cryptographic operation

Operations on IT security requirements are identified as follows:

- **Iteration – component number is distinguished by appending a number, preceded by a hyphen**
- **Assignment – text is bolded italics and enclosed in brackets**
- **Selection – text is bolded italics and enclosed in brackets**
- **Refinement – text is underlined, bolded italics**
- **Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by Application Note:** ***italicized***

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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

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

b) All auditable events for the **[*basic*]** level of audit; and

c) Access to the System and access to the TOE and System data

Table 6-2 Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL,1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of the TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Application Note: The auditable events for the basic level of auditing are included in Table 6-2 Auditable Events.

Application Note: The IDS_SDC and IDS_ANL requirements in this ST address the recording of results from IDS sensing, and analyzing tasks (i.e. System data)

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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the additional information specified in the Details column of Table 6-2 Auditable Events.

Dependencies: FPT_STM.1 Reliable time stamps

6.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [***Authorized System Administrator (root)***] with the capability to read [***User Log data, Application Log data***] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

6.1.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [***sorting***] of audit data based on [***date and time, subject identity, type of event, and success or failure of related event***].

Dependencies: FAU_SAR.1 Audit review

6.1.1.5 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

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

a) [***event type***]

b) [***no additional attributes***].

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

6.1.1.6 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [***detect***] unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [1 GB] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

Dependencies: FAU_GEN.1 Audit data generation

6.1.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [***send an alarm*** if the audit trail storage is full.

Dependencies: FAU_STG.1 Protected audit trail storage

6.1.2 Class FIA: Identification and Authentication

6.1.2.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [***no actions***] on behalf of the user to be performed before the user is authenticated.

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

6.1.2.2 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [***an SVManager configurable positive integer within 0-100***] unsuccessful authentication attempts occur related to [***unauthorized users attempting to authenticate***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

- [***prevent the unauthorized users from successfully authenticating for period of time configurable by the SV Manager or until an authorized administrator takes some action to make authentication possible for the unauthorized user in question ;and leave an audit trail in the user application log***]

Dependencies: FIA_UAU.1 Timing of authentication

6.1.2.3 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity

b) Authentication data

c) Authorizations and

d) roles

Dependencies: No dependencies

6.1.2.4 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[*no actions*]** on behalf of the user to be performed before the user is identified.

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.

Dependencies: No dependencies

6.1.3 Class FMT: Security Management

6.1.3.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to [***modify the behavior of***] the functions [***as specified in table 6-3***] to [***authorized identified roles specified in table 6-3***]

Table 6-3 Security Functions Behavior

Selection	List of functions	Role
Modify the behavior of	Account lockout	SV Manager ER SV Manager
Modify the behavior of	System data collection, analysis and reaction	Developer

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

6.1.3.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 [1] The TSF shall restrict the ability to [***query, modify, delete, and [other operations as specified in Table 6-4***] the [***TSF Data as specified in Table 6-4***] to [***the role as specified in Table 6-4***].

Table 6-4 Management of TSF Data

Operation	TSF Data	Role
query	Network Event data	Operator Analyst Developer
query	Machines Status	Operator Analyst Developer SV Manager ER SV Manager
modify	Machines Status	SV Manager ER SV Manager
query	DMEs	Analyst Developer
query, modify, delete, or create	User Access	Account Manager ER Account Manager
query	Policy History	Operator Analyst Developer
query	Policies	Analyst Developer
modify, delete, or create	Policies	Developer
query	Application Logs	Authorized System Administrator (root)
query	User Logs	Authorized System Administrator (root)

Dependencies: FMT_SMF.1 Specification of Management Functions

6.1.3.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

- ***operations on the security attributes as specified in Table 6-3 (see FMT_MOF.1)***
- ***operations as specified in Table 6-4 on the TSF Data as specified in Table 6-4 (See FMT_MTD.1)*].**

Dependencies:No dependencies.

6.1.3.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***Authorized Administrator (svs), Authorized System Administrators (root), Operator, Analyst, Developer, SV Manager, Account Manager, ER SV Manager, and ER Account Manager***].

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

Application Note: The roles of ER SV Manager and ER Account Manager apply only to the ER Gateway.

Application Note: The roles of SV Manager, Account Manager, Developer, Analyst and Operator apply to Monitor, EM and Studio.

Application Note: The roles of Authorized Administrator and Authorized System Administrator are one-account roles. They are implemented directly at the operation system by way of the accounts svs and root respectively. These accounts require physical access to the console of the systems and they are not honored by the Securify v6.0 Web interface. The root account has ***unlimited*** *privileges on the systems and therefore, it should be used only to perform special maintenance tasks that are not available at the Web interface as describe in the official documentation. These accounts are created automatically at installation time on all Securify v6.0 systems except Studio (Monitor, Enterprise Manager and ERGW). McAfee recommends using the security best practices to assign these accounts to fully trusted administrators and to ensure they are protected by strong passwords.*

Dependencies: FIA_UID.1 Timing of identification

6.1.4 Class FPT: Protection of the TSF

6.1.4.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

6.1.4.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_SMT.1.1 The TSF shall be able to provide reliable time stamps for its own use

Dependencies: No dependencies

6.1.5 Class IDS: IDS Component Requirements

6.1.5.1 IDS_SDC_EXT.1 System Data Collection (EXT)

Hierarchical to: No other components.

IDS_SDC_EXT. 1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) **[*identification and authentication events, data accesses, service requests, network traffic, detected known vulnerabilities*]**

b) **[*changes from prescribed network behavior*]**

IDS_SDC_EXT. 1.2 At a minimum, the System shall collect and record the following information

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

b) The additional information specified in the *Details* column of Table 6-5 System Events. (EXT)

Table 6-5 System Events

Component	**Event**	**Details**
IDS_SDC_EXT.1	Identification and authentication events	**User identity, location, source address, destination address**
IDS_SDC_EXT.1	Data Accesses	**Object IDS, requested access, sources address, destination address**
IDS_SDC_EXT.1	Service Requests	**Specific service, source address, destination address**
IDS_SDC_EXT.1	Network Traffic	**Protocol, source address, destination address**
IDS_SDC_EXT.1	Detected known vulnerability	**Identification of the known vulnerability**
IDS_SDC_EXT.1	Changes from prescribed network behavior	**Specific service, destination address**

Dependencies: No dependencies

6.1.5.2 IDS_ANL_EXT.1 Analyser analysis (EXT)

Hierarchical to: No other components.

IDS_ANL_EXT.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) **[*signature*]; and**

b) **[*Policy evaluation*].** (EXT)

IDS_ANL_EXT.1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) **[*source, destination, and outcome*]**

Dependencies: IDS_SDC_EXP.1

6.1.5.3 IDS_RCT_EXT.1 Analyser react (EXT)

Hierarchical to: No other components.

IDS_RCT_EXT.1.1 The System shall send an alarm to **[*audit log*]** and take **[*an optionally sending an email*]** when an intrusion is detected (EXT):

Dependencies: IDS_SDC_EXP.1

6.1.5.4 IDS_RDR_EXT.1 Restricted Data Review (EXT)

Hierarchical to: No other components.

IDS_RDR_EXT.1.1 The System shall provide [***Operator, Analyst, and Developer***] with the capability to read **[*Event Data*]** from the System data. (EXT)

IDS_RDR_EXT.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3. The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXT)

Dependencies: IDS_SDC_EXP.1

6.1.5.5 IDS_STG_EXT.1 Guarantee of System Data Availability (EXT)

Hierarchical to: No other components.

IDS_STG_EXT.1.1 The System shall protect the stored System data from unauthorized deletion (EXT).

IDS_STG_EXT.1.2 The System shall protect the stored System data from modification. (EXT)

IDS_STG_EXT.1.3. The System shall ensure that **[*10GBytes*]** System data will be maintained when the following condition occurs: **[*System data storage exhaustion*]**. (EXT)

Dependencies: No dependencies

6.1.5.6 IDS_STG_EXT.2 Prevention of System data loss (EXT)

Hierarchical to: No other components.

IDS_STG_EXT.2.1 The System shall **[*overwrite the oldest stored System data*]** and send an alarm if the storage capacity has been reached (EXT).

Dependencies: IDS_SDC_EXP.1

6.1.6 Class FCS: Cryptographic Support

6.1.6.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1 The TSF shall perform [**key exchange, authentication, encryption, decryption, and integrity checks**] in accordance with a specified cryptographic algorithm [**DHE-RSA-AES256-SHA, DHE-DSS-AES256-SHA, AES256-SHA, KRB5-DES-CBC3-MD5, KRB5-DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, AES128-SHA, DHE-DSS-RC4-SHA, KRB5-RC4-MD5, KRB5-RC4-SHA, RC4-SHA, RC4-MD5 and RC4-MD5**] and cryptographic key sizes [**256, 168 and 128 bits**].

Dependencies FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

Application Note: FCS_CKM.1 Cryptographic key generation and FCS_CKM.4 Cryptographic key destruction are not further expanded because there are not functional requirements for key management. In particular, no user intervention is involved with the processes of creation, distribution, access and destruction of any cryptographic key for the operation of the TOE.

According to Common Criteria Part 2 "Security Functional Components" version 3.1 revision 2 paragraph 143 on FCS_CKM:

"This family should be included whenever there are functional requirements for the management of cryptographic keys."

6.2 Relation between SFRs and security objectives

Table 6-6 Requirements vs Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECTRANS
FAU_GEN.1										X		
FAU_SAR.1						X						
FAU_SAR.2							X	X				
FAU_SAR.3						X						
FAU_SEL.1						X				X		
FAU_STG.2	X						X	X	X		X	
FAU_STG.4									X	X		
FIA_UAU.1							X	X				
FIA_ATD.1								X				
FIA_UID.1							X	X				
FMT_MOF.1	X						X	X				
FMT_MTD.1	X						X	X			X	
FMT_SMF.1	X						X	X			X	
FMT_SMR.1								X				
FPT_ITT.1											X	
ADV_ARC.1	X					X		X		X	X	
FPT_STM.1										X		
IDS_SDC_EXT.1		X	X									
IDS_ANL_EXT.1				X								
IDS_RCT.1					X							
IDS_RDR_EXT.1						X	X	X				
IDS_STG_EXT.1	X						X	X	X		X	
IDS_STG_EXT.2									X			
FCS_COP.1												X

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

O.PROTCT: The TOE must protect itself from unauthorized modifications and access to its functions and data.

> The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE is capable of performing the management functions that are defined in FMT_MOF.1 and FMT_MTD.1 [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDSCAN: The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

> A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected is defined in the SFR [IDS_SDC_EXT.1].

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

> A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events are defined in the SFR [IDS_SDC_EXT.1].

O.IDANLZ: The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

> The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL_EXT.1].

O.RESPON: The TOE must respond appropriately to analytical conclusions.

> The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data.

> The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR_EXT.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE is capable of performing the management functions that are defined in FMT_MOF.1 and FMT_MTD.1 [FMT_SMF.1].

O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TSF is able to detect when a user surpasses a set number of unsuccessful authentication attempts [FIA_AFL.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE is capable of performing the management functions that are defined in FMT_MOF.1 and FMT_MTD.1 [FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.OFLOWS: The TOE must appropriately handle potential audit and System data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The System must prevent the loss of audit data in the event the its audit trail is full [IDS_STG_EXT.1].

O.AUDITS: The TOE must record audit records for data accesses and use of the System functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.INTEGR: The TOE must ensure the integrity of all audit and System data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The TOE is capable of performing the management functions that are defined in FMT_MOF.1 and FMT_MTD.1 [FMT_SMF.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between separate parts of the TOE [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1].

O.SECTRANS: The TOE must ensure the confidentiality and integrity of the IDS data while in transit.

The TOE is required to perform cryptographic operations in order to protect the IDS data against unauthorized disclosure and modification when it is transmitted over a network [FCS_COP.1].

6.3 Security Assurance Requirements (SARs)

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 6-7 summarizes the components.

Table 6-7 EAL2+ Assurance Components

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Architectural Design with Domain Separation and non-bypassability
	ADV_FSP.2	Security enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability Analysis

6.4 SARs and the security requirements rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the system will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

7 TOE Summary Specification (ASE_TSS)

Securify™ Version 6.0 (TOE) is a scalable security solution that enables customers to generate business-driven security policies, monitor networks for compliance, threats and known attack patterns, and produce relevant network operational information.

The Securify deployment could encompass just a single Monitor or a more complex monitoring infrastructure like the one shown in the full configuration (Figure 1-2). Although the functionality and capacity of a single Monitor is substantially lower than the full configuration, both deployments provide the same levels of confidentiality, integrity, availability and accountability.

Both configurations discussed in this section require Studio to create security policies and optionally, to perform advanced network analysis.

The following two sections depict the security properties and configuration for the mentioned deployments: Stand-alone Monitor and the Full Configuration.

7.1 Stand-alone Monitor

This configuration consists of the following Securify components:

- Securify Studio
- One Securify Monitor

Studio

Securify Studio is a client application that is installed from a CD on a Windows computer. The OS enforces all discretionary controls for all local resources. This means that any authenticated user might be able to use Studio and open any security policy stored locally on that computer. Securify Studio does not enforce any user role nor does it provide confidentiality to or protect integrity of the security policy while stored locally. Securify recommends deploying dedicated computers for using Studio where only trusted users can log on.

In this configuration, a user with the Developer role can use Studio to create and modify policies locally, and manage them (upload or download) on the Monitor. All users can use Studio to evaluate security policies offline by way of DME files. Only users with the Analyst or Developer role can also perform online security analysis on the current Monitor data.

Studio does not maintain any security log on the local drive. It is assumed the computer where Studio runs has the appropriate security countermeasures to avoid unauthorized use.

Monitor

The Securify Monitor is a network monitoring appliance that must have access to the network traffic under observation.

Regardless of the deployment configuration, the Securify Monitor is always the component in charge of capturing the network traffic. The Monitor analyzes the traffic against its current security policy to detect violations. The Monitor can show up to 48 hours of network data through the Web interface and up to 8 weeks with Studio.

Monitor – External Servers Interactions

A stand-alone Monitor may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify Monitor requires a valid time source for timestamp purposes. Ideally, the Monitor should synchronize its time with a valid NTP server. In cases where it is not possible to use an external NTP server, the Monitor can use the system local hardware clock.
SNMP	If configured, the Securify Monitor can send operational status changes, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Securify Monitor can alert operational status changes and policy compliance violations by way of SMTP. **Note**: the Securify Monitor does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Securify Monitor is able to export policy correlated events to any external SYSLOG server.
DNS	If configured, the Securify Monitor can use machine names instead of IP addresses and look up important DNS information.
SPAN Port	The Securify Monitor captures the network traffic directly from a port in the main switch where all the traffic is mirrored.

Securify Monitor Web interface

The Monitor provides a Web interface through which you can perform tasks such as analyze the network behavior, upload or download policies, maintain users and configure the system. The Monitor has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. For each user role, the Monitor ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Monitor’s Web interface using a regular Web browser and HTTPS. The Monitor presents a server certificate that the client uses to verify the Monitor during the SSL handshake. Optionally, the Monitor can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Monitor’s certificate can be either self-signed (default) or signed by any CA the user deems valid. It is not possible to mix self-signed and signed certificates in the same deployment with interconnected

Securify v60_CC_9 systems. A user with the SV Manager role is responsible for configuring this aspect of the system.

Log Files

With a stand-alone Monitor, neither the network event information nor the log files leave the Monitor unless a user with the appropriate role explicitly downloads them using the Web interface. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

The following table shows the files available for each role:

Role	Downloadable Information
Operator	none
Analyst	Captured DME
Developer	Captured DME
Account Manager	User logs
SV Manager	Application logs
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

The Monitor has different disk partitions exclusively used to store log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

For a stand-alone Monitor, log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Monitor does not generate an alert for these ordinary tasks.

DME files

These files are not considered log files and the Monitor stores them in a special partition. By default, the Monitor does not store DME files on disk. A user with the SV Manager role must explicitly enable their capture through the Monitor Web interface. It is important to mention that DME is a proprietary Securify format that compresses connection data. After capturing the network traffic, the Monitor transforms raw packets into this compact format before evaluating the security policy. If the user wants to use Studio to evaluate a policy offline, they have to download DME files to the local hard drive after authenticating to the Monitor with either the Analyst or Developer role.

Studio-Monitor Interaction

Securify Studio is a client application that enables the user to create and modify security policy, evaluate security policies offline using a DME file, analyze network events stored on a Monitor and download or upload security policies.

Some of these tasks require Studio to connect to the Monitor on behalf of the user. This connection is an SSL connection initiated by Studio where the Monitor presents its certificate and the user is authenticated by either a userid and password, or a certificate (depending on the user account configuration). It is important to mention that Monitor does not allow the SV Manager or Account Manager roles to connect remotely using Studio; only the Operator, Analyst and Developer roles can authenticate to the Monitor.

7.2 Full Configuration

The number of Securify v6.0 systems present in a full configuration varies. However, any full configuration of Securify v6.0 systems must have three hierarchical levels containing Monitors at the bottom, Enterprise Manager in the middle and ERGW at the top. Therefore, a full configuration may have multiple Monitors reporting to one Enterprise Manager and several Enterprise Managers reporting to one ERGW.

The full configuration used for testing purposes of the Securify v6.0 was representative of more complex full Securify v6.0 deployments without adding too many systems that would have complicated unnecessarily the tests. The chosen test configuration contained the following Securify v6.0 systems:
:

- Securify Studio
- Two Securify Monitors in two different Security Zones
  A security zone is one or more Securify Monitors that run the same security policy. Therefore, this configuration has two different Securify Monitors each one with a different security policy.
- One Securify Enterprise Manager to combine policy conformance and manage both Monitors
- One Securify Enterprise Reporting Gateway (ERGW)

Studio

Securify Studio is a client application that is installed from a CD on a Windows computer. The OS enforces all discretionary controls for all local resources. This means that any authenticated user might be able to use Studio and open any security policy stored locally on that computer. Securify Studio does not enforce any user role nor does it provide confidentiality to or protect integrity of the security policy while stored locally. Securify recommends deploying dedicated computers for using Studio where only trusted users can log on.

In this configuration, a user with the Developer role can use Studio to create and modify policies locally, and manage them (upload or download) on an Enterprise Manager. All users can use Studio to evaluate security policies from a Monitor or Enterprise Manager offline by way of DME files. Only users with the Analyst or Developer role can also perform online security analysis on the current Monitor or Enterprise Manager data.

Although it is possible to use Studio to upload security policies directly to a Monitor, the Enterprise Manager overwrites such changes to ensure that the Security Zone is consistent across the managed Monitors. This is also true for any configuration changes performed directly on the Monitors.

Monitors

The Securify Monitor is a network monitoring appliance that must have access to the network traffic under observation.

Regardless of the deployment configuration, the Securify Monitor is always the component in charge of capturing the network traffic. The Monitor analyzes the traffic against its current security policy to detect violations. The Monitor can show up to 48 hours of network data through the Web interface and up to 8 weeks with Studio.

Monitors – External Servers Interactions

The Monitors may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify Monitors require a valid time source for timestamp purposes. Ideally, a Monitor should synchronize its time with a valid NTP server. Even though each Monitor could have its own time (as in locations with different time), it is possible to synchronize time among all the Monitors using the Enterprise Manager's time. In cases where it is not possible to use an external NTP server, the Monitors can use the system local hardware clock.
SNMP	If configured, the Monitors can send operational status changes, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Monitors can alert operational status changes and policy compliance violations by way of SMTP. **Note**: The Monitors do not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Monitors can export policy correlated events to any external SYSLOG server.
DNS	If configured, the Monitors can use machine names instead of IP addresses and look up important DNS information.
SPAN Port	The Monitors capture the network traffic directly from a port in the main switch where all the traffic is mirrored.

Securify Monitor Web interface

Each Monitor provides a Web interface through which you can perform tasks such as analyze the network behavior on that specific network segment, download security policies and maintain users local to that Monitor. In the full configuration, changes to a Monitor should be made through the Enterprise Manager Web interface. This includes uploading new policies. To ensure the integrity and consistency of the Security Zone, the Enterprise Manager overwrites changes made directly on its registered Monitors.

A Monitor has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. For each user role, the Monitor ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Monitor's Web interface using a regular Web browser and HTTPS. The Monitor presents a server certificate that the client uses to verify the Monitor during the SSL handshake. Optionally, the Monitor can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Monitor's certificate can be either self-signed (default) or signed by any CA the user deems valid. It is not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. An Enterprise Manager user with the SV Manager role and access to the Security Zone is responsible for configuring this aspect of the system.

Log Files

In the full configuration, each Monitor maintains its own set of log files locally. The type, number, and location of these log files are the same as in the stand-alone Monitor configuration. The log files do not leave the Monitor unless a user with the appropriate role explicitly downloads them using either the Monitor's Web interface or the Enterprise Manager Web interface.

An Enterprise Manager user can download any Monitor's log file using the Enterprise Manager Web interface. This is only possible if the user has the correct role and permission to access the Security Zone where the Monitor resides. This log transfer is twofold: one transfer from the Monitor to the Enterprise Manager and another transfer from the Enterprise Manager to the Web browser. The former connection is a normal intra-system connection protected by SSL (transparent to the user), while the latter is the already established SSL connection between the user's Web browser and the Enterprise Manager Web interface. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

Each Securify Monitor has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Securify Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to

release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

DME files

These files are not considered log files and the Monitor stores them in a special partition. By default, the Monitor does not store DME files on disk. A user with the SV Manager role must explicitly enable their capture through the Monitor Web interface. It is important to mention that DME is a proprietary Securify format that compresses connection data. After capturing the network traffic, the Monitor transforms raw packets into this compact format before evaluating the security policy. If the user wants to use Studio to evaluate a policy offline, they must download the DME files to the local hard drive by way of the Monitor's Web interface, after authenticating to the Monitor with either the Analyst or Developer role.

The following table shows the files available for each role on the Monitors:

Role	Downloadable Information
Operator	None
Analyst (defined on Monitor)	DME via Monitor Web interface.
Analyst (defined on Enterprise Manager)	DME via Enterprise Manager Web interface (security zone permission needed)
Developer (defined on Monitor)	DME via Monitor Web interface.
Developer (defined on Enterprise Manager)	DME via Enterprise Manager Web interface (security zone permission needed)
Account Manager (defined on Monitor or Enterprise Manager)	User logs via Monitor or Enterprise Manager Web interface
SV Manager (defined on Monitor)	Application logs via Monitor Web interface
SV Manager (defined on Enterprise Manager)	Application logs via Enterprise Manager Web interface (security zone permission needed)
root (defined at the OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, log files do not leave a system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Monitor does not generate an alert for these ordinary tasks.

Securify Enterprise Manager

The Enterprise Manager supervises the functional and configuration aspects of all Monitors registered to it. Enterprise Manager security is based on zones, where a security zone consists of one or more Monitors that run the same security policy.

The main tasks of the Enterprise Manager are:

- Aggregate network events generated by up to ten Monitors. The Enterprise Manager pulls network events from all registered Monitors on a regular basis and stores the data in the Enterprise Manager's internal database.
- Control the configuration of Security Zones and individual registered Monitors. The Enterprise Manager constantly ensures that each Monitor uses the correct security policy and configuration by overwriting anything that is changed directly on the Monitor.
- Enforce restricted access to both configuration and network event data based on user roles and security zones. Each user who has an account on the Enterprise Manager has associated user roles and security zones to restrict and control what she can do.

Enterprise Manager – External Servers Interactions

The Enterprise Manager may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify deployment requires a valid time source for timestamp purposes. Even though each Monitor could have its own time (as in locations with different time), it is possible to synchronize time among all the Monitors using the Enterprise Manager's time. The Enterprise Manager can be configured to use an external NTP server. In cases where it is not possible to use any external NTP server, Enterprise Manager can use the system local hardware clock.
SNMP	If configured, the Enterprise Manager can send operational status changes for itself or registered Monitors, policy compliance violations and correlated events to any SNMP server.
SMTP	If configured, the Enterprise Manager can alert operational status changes for itself or registered Monitors, and policy compliance violations by way of SMTP. **Note**: The Enterprise Manager does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.
SYSLOG	If configured, the Enterprise Manager can export policy correlated events to any external SYSLOG server.
DNS	If configured, the Monitors can use machine names instead of IP addresses and look up important DNS information.

Securify Enterprise Manager Web interface

The Securify Enterprise Manager provides a Web interface through which you can perform tasks such as view network behavior and policy compliance for all security zones at once or for any individual security zone. You can also configure the Enterprise Manager itself, a security zone and individual Monitors. The Enterprise Manager has 5 different roles; Operator, Analyst, Developer, SV Manager and Account Manager. Furthermore, all roles except Account Manager also have a security zone scope. For each user role, the Enterprise Manager ensures that only the appropriate functionality is available in the Web interface.

The users connect to the Enterprise Manager's Web interface using a regular Web browser and HTTPS. The Enterprise Manager presents a server certificate that the client uses to verify the Enterprise Manager during the SSL handshake. Optionally, the Enterprise Manager can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The Enterprise Manager's certificate can be either self-signed (default) or signed by any CA the user deems valid. It is not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. The certificate used by the Enterprise Manager is used by the system to identify itself when communicating with users and other Securify v6.0 systems. Therefore, this is an internal configuration parameter of the Enterprise Manager that is not related to any Security Zone that can be configured by a user with SV Manager role.

Log Files

In a full configuration, the Enterprise Manager maintains its own set of local log files. These files are available for download by way of the Enterprise Manager Web interface if a user has the correct role. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

NOTE: Although it is possible to download a Monitor's log files by way of the Enterprise Manager Web interface, only downloading the Enterprise Manager log files is covered in this section.

The Enterprise Manager has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If

the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

The following table shows the files available for each role on the Enterprise Manager:

Role	Downloadable Information
Operator	none
Analyst	none
Developer	none
Account Manager	User logs
SV Manager	Enterprise Manager Application logs Monitor Application logs (from authorized security zones)
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, the Enterprise Manager log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The Securify Enterprise Manager does not generate an alert for these ordinary tasks.

Securify Enterprise Reporting Gateway (ERGW)

The ERGW is a staging system whose main function is to aggregate network data from one or more Enterprise Managers. The ERGW prepares this information for more permanent data repositories. The ERGW is the interface from where external data warehouses obtain network information from the Securify infrastructure.

NOTE: No data warehouse, including the Securify Enterprise Reporting Warehouse (ERWH), is part of the TOE.

ERGW – External Servers Interactions

The ERGW may interact with the following external services:

Service	Purpose
NTP	As with any IDS, the Securify deployment requires a valid time source for timestamp purposes. The ERGW can be configured to synchronize its time with an external NTP server. In cases where it is not possible to use an external NTP server, the ERGW can use the system local hardware clock.
SNMP	If configured, the ERGW can send operational status changes to any SNMP server.
SMTP	If configured, the ERGW can alert operational status changes by way of SMTP. **Note**: The ERGW does not have the means to validate that the recipients are authorized to receive this information. The administrator must exercise special precautions when assigning recipients for this information.

ERGW Web interface

The ERGW provides a Web interface through which you can configure and manage the system.

The ERGW Web interface only has two roles: SV Manager and Account Manager. Since the ERGW is an aggregation point, its Web interface does not provide any network data analysis tools. Instead, this interface is primarily used to configure the system to retrieve network data from one or more Enterprise Managers and to authorize external data warehouses to retrieve network data from the ERGW.

The SV Manager role is responsible for configuring the system, while the Account Manager role is responsible for maintaining users.

The users connect to the ERGW's Web interface using a regular Web browser and HTTPS. The ERGW presents a server certificate the client uses to verify the ERGW during the SSL handshake. Optionally, the ERGW can be configured to request a client certificate and the client must present a valid signed certificate to establish the SSL connection. In any case, the user has to present valid credentials to finally login to the Web interface.

The ERGW's certificate can be either self-signed (default) or signed by any CA the user deem valid. It is not possible to mix self-signed and signed certificates in the same deployment with interconnected Securify v60_CC_9 systems. A user with SV Manager role is in charge of configuring this feature on the ERGW.

Log Files

The ERGW maintains its own set of local log files. These files are available for download by way of the ERGW Web interface if a user has the correct role. It is important to be aware the TOE does not protect the local copies of the log files once they have been downloaded.

The ERGW has different disk partitions exclusively used to store its log files. The system maintains these categories of log files:

- **User Logs**
  These logs keep track of any transaction (including configuration changes) performed with the Web interface or Studio. The system checks the current user log every hour and rotates it daily or when its size is bigger than 300 KB, whichever occurs first. Normally the Monitor keeps the last 5 user logs, but if the partition free space is too small it removes the oldest logs to release space. If the disk partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).
- **Application Logs**
  These logs store audit trails of the application's internal subsystems and system syslogs. The system checks all the current logs every hour and rotates them daily or when any current file is bigger than a configured size. Normally the system keeps the last 5 or 8 log files (depending on the log), but if the partition space is too small it removes the oldest log files to release space. If the partition is full, the system generates an alert through the Web interface and may generate an SNMP and/or SMTP alert (depending on configuration).

The following table shows the files available for each role on the ERGW:

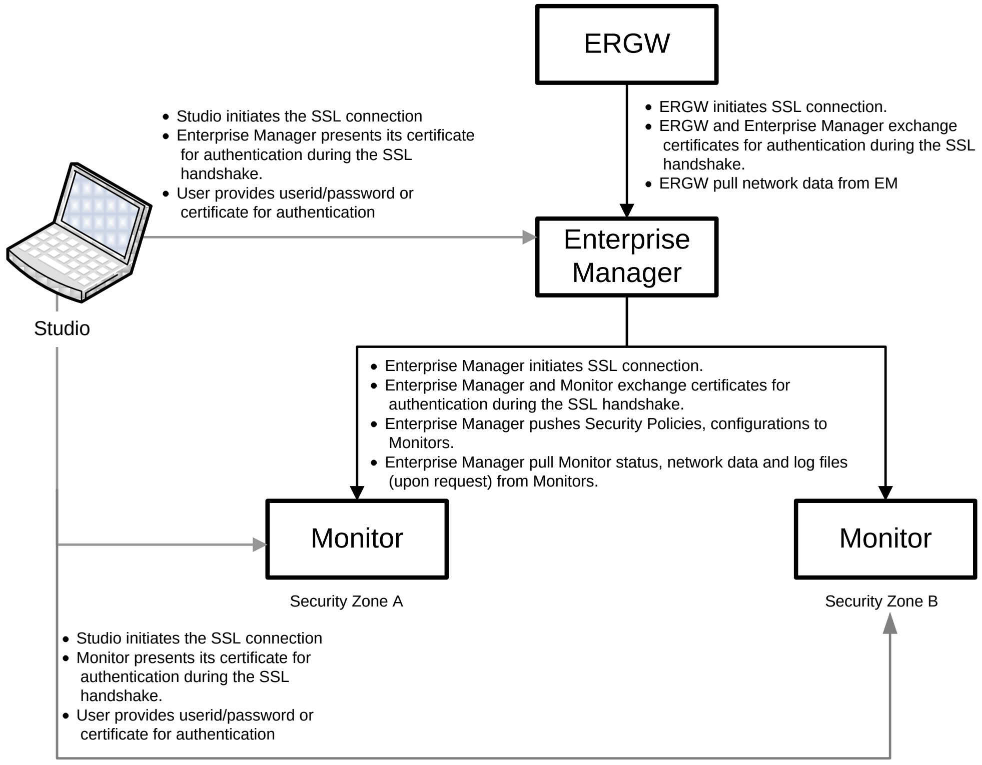
Role	Downloadable Information
Account Manager	User logs
SV Manager	Application logs
root (OS level)	Read/sort/search Application and User Logs (local console access is required).

In a full configuration, the ERGW log files do not leave the system unless a user with the appropriate role explicitly downloads them. The log rotations previously mentioned are considered ordinary system tasks. The ERGW does not generate an alert for these ordinary tasks.

Interactions and Trusted Relationships between Securify Systems

In the full configuration, the individual Securify components must interact with one another so that network event data can move from the Monitor to the ERGW. Each interaction requires establishing mutually trusted relationships between the involved systems before the actual data moves.

The following picture depicts the Securify systems interacting in the full configuration:


ERGW
• ERGW initiates SSL connection.
• ERGW and Enterprise Manager exchange certificates for authentication during the SSL handshake.
• ERGW pull network data from EM
• Studio initiates the SSL connection
• Enterprise Manager presents its certificate for authentication during the SSL handshake.
• User provides userid/password or certificate for authentication
Enterprise Manager
Studio
• Enterprise Manager initiates SSL connection.
• Enterprise Manager and Monitor exchange certificates for authentication during the SSL handshake.
• Enterprise Manager pushes Security Policies, configurations to Monitors.
• Enterprise Manager pull Monitor status, network data and log files (upon request) from Monitors.
Monitor
Security Zone A
Monitor
Security Zone B
• Studio initiates the SSL connection
• Monitor presents its certificate for authentication during the SSL handshake.
• User provides userid/password or certificate for authentication

This section covers how the different trusted relationships are configured and how they are established through the network during normal operations.

Studio – Monitor/Enterprise Manager Interactions

During the interaction between Studio and a Monitor or Enterprise Manager, the trusted relationship is based on user credentials and Studio acts as the front-end to establish this relationship.

Studio enables users to connect to either an Enterprise Manager or a Monitor. Studio initiates the SSL connection and the Monitor or Enterprise Manager presents its certificate for server authentication during the SSL handshake. Optionally, if the user's account uses certificates instead of usernames and passwords, the server requests client certificates to complete a mutual authentication during the SSL handshake. If the user does not present either a client certificate or valid credentials, the Monitor or Enterprise Manager immediately resets the connection.

With the connection established, the user can upload/download security policies or analyze traffic data.

NOTE: You cannot upload security policies directly to a Monitor that is registered with an Enterprise Manager.

Enterprise Manager – Monitor Interactions

The Enterprise Manager must establish a secure SSL connection to each of the Monitors registered to it to retrieve network data and to enforce security zone configurations. This involves mutual authentication for each system, so the Enterprise Manager and Monitors must be properly configured beforehand.

Establishing a relationship between the Enterprise Manager and Monitors requires two separate SV Manager accounts: one for the Enterprise Manager and the other for the Monitor. It is important to understand that during this initial configuration, the SV Manager account for the Monitor is still a local Monitor account. Once the Enterprise Manager takes over the configuration of the Monitor, this SV Manager account is no longer useful. All subsequent configuration changes for the Monitor must be done by way of the Enterprise Manager Web interface using an Enterprise Manager account with the SV Manager role and access to the Security Zone where the Monitor resides.

Monitor Configuration:

- Identify the Enterprise Manager on the Monitor
  The SV Manager user on the Monitor must create a machine account for the Enterprise Manager to identify it on the Monitor. The SV Manager user does this by typing the Enterprise Manager's Common Name and certificate hash in the relevant locations.

Enterprise Manager Configuration:

- Synchronizing Clocks
  The SV Manager user on the Enterprise Manager must ensure that the Enterprise Manager and Monitor clocks are synchronized within a 5 minute interval.
- Security Zone
  If the Security Zone where the Monitor will reside does not exist, the SV Manager user on the Enterprise Manager must create it.
- Adding a Monitor
  The SV Manager user on the Enterprise Manager must add the new Monitor and provide the Monitor's Machine ID (unique identifier assigned to each Securify system) and the Monitor's

IP address. When the SV Manager user on the Enterprise Manager submits this information, the Monitor's certificate is presented on the screen and the SV Manager user on the Enterprise Manager must accept it.

Establishing Connections

From this point on, the Monitor is under the administrative control of the Enterprise Manager and the Enterprise Manager gathers network event data every five minutes from all its registered Monitors.

Each time the Enterprise Manager contacts a Monitor, both the Enterprise Manager and the Monitor must present their certificates to authenticate each other and establish a trusted channel. If either the Enterprise Manager or the Monitor is not able to correctly authenticate the other system, the SSL connection is not established and the Enterprise Manager displays a warning status message on its Web interface. The Enterprise Manager may also send an SMTP and/or SNMP alert (depending on configuration).

ERGW – Enterprise Manager Interactions

The ERGW is responsible for collecting network event data from a set of Enterprise Managers to then provide this information to authorized data warehouse systems. It is important to remember that no warehouse implementations, including the Securify ERWH, are part of the TOE.

Configuration

The Securify ERGW must establish a secure SSL connection to each of the Enterprise Managers to collect network event data. This involves mutual authentication for each system, so the ERGW and Enterprise Managers must be properly configured beforehand.

Establishing a relationship between the ERGW and an Enterprise Manager requires two separate SV Manager accounts: one for the ERGW and the other for the Enterprise Manager.

Enterprise Manager Configuration

- Identify the ERGW on the Enterprise Manager
  The SV Manager user on the Enterprise Manager must create a machine account for the ERGW to identify it on the Enterprise Manager. The SV Manager user does this by typing the ERGW's Common Name and certificate hash in the relevant locations.

ERGW Configuration

- Synchronizing Clocks
  The SV Manager user on the ERGW must ensure that the ERGW and Enterprise Manager clocks are synchronized within a 5 minute interval.
- Adding an Enterprise Manager
  The SV Manager user on the ERGW must add the new Enterprise Manager and provide the Enterprise Manager's Machine ID (unique identifier assigned to each Securify system) and the Enterprise Manager's IP address. When the SV Manager user on the ERGW submits this information, the Enterprise Manager's certificate is presented on the screen and the SV Manager user on the ERGW must accept it.

Establishing Connections

From this point on, the ERGW can collect network event data from the Enterprise Manager every ten minutes.

Each time the ERGW contacts an Enterprise Manager, both the ERGW and the Enterprise Manager must present their certificates to authenticate each other and establish a trusted channel. If either the ERGW or the Enterprise Manager is not able to correctly authenticate the other system, the SSL connection is not established and the ERGW displays a warning status message on its Web interface. The ERGW may also send an SMTP and/or SNMP alert (depending on configuration).

7.3 IT Security Functions

The following sections describe the IT Security Functions in each of the Securify™ components.

7.3.1 Securify™ Studio

Studio IDS Function	
S-IDS-1	Studio enables users to read information from the IDS data records. Users with the role of Operator, Analyst or Developer connect through Studio to either Enterprise Manager or Monitor. This connection is server-side SSL protected. Through Studio, users can perform queries constrained by different Policy attributes and by signatures. Results are presented in the Studio Analyzer interface.The Analyzer interface allows users to sort the data by different policy attributes. (IDS_RDR_EXT.1.1, IDS_RDR_EXT.1.2)
S-IDS-2	Studio provides a full-featured workspace in which users can describe what Policy to evaluate network traffic against. In this workspace, users can define the objects which they would like the system to evaluate and report results. In addition, Studio enables users to write custom signatures for describing explicit malicious behaviors. As part of the configuration of both Policy and signatures, Studio enables users to select what type of events to audit and what severity to assign when such events occur in the network. Assuming Studio users have the appropriate role when connected to an Enterprise Manager, Studio enables users to upload both the Policy and signature configurations so they are applied in the network. Policies as well as signature configuration can be saved in the local file system for backup purposes.(IDS_SDC_EXT.1.1, FCS_COP.1.1)
S-IDS-3	Studio provides a full-featured Analyzer workspace. Using this functionality, users can perform off-line evaluations of previously captured network traffic against the current open security policy (including signatures). After a successful evaluation, Studio displays the results that contain every violation to the security policy. This output includes all required information such as date, time, type of result, and source. (IDS_ANL_EXT.1.1, IDS_ANL_EXT.1.2)

Studio Self Protection Function	
S-SPF-1	Studio only establishes communication with Enterprise Manager and/or Monitor when users are properly authenticated. This communication is server-side SSL/TLS protected and is enforced by the Monitor/Enterprise Manager. When first establishing a connection, Studio users are presented with the certificate of the Monitor/Enterprise Manager. Studio users can verify the certificate and allow or deny the connection. They can also save the certificate for future connections. If a certificate is not saved, the user must accept or deny it every time a connection is attempted. (FPT_ITT.1, FCS_COP.1.1)

7.3.2 Securify^{TM} Monitor

Monitor Manage User Access Function	
M-MUA-1	Monitor maintains the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. Monitor also maintains an authorized identifier for the Enterprise Manager system to which it is registered. The trust relationship with the Enterprise Manager is established by accepting the self-signed certificates manually. (FIA_ATD.1.1)
M-MUA-2	Monitor restricts the ability to access data as specified in Table 6-4. (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)
M-MUA-3	Monitor maintains the roles of Operator, Analyst, Developer, SV Manager, and Account Manager. These roles are applicable when users directly access the Monitor, and not when the Monitor data or configuration is accessed through the Enterprise Manager that is managing it. (FMT_SMR.1.1, FMT_SMR.1.2) For more information about user roles in Monitor see section 1.4.8 Users.
M-MUA-4	Monitor allows SV Manager to set and configure the parameters of the account lockout feature (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)

Monitor User Login Function	
M-UL-1	Monitor requires each user to identify themselves before they are allowed to perform any other actions. Monitor compares the credentials (username/password or hash of the certificate) to a locally maintained database. Monitor does not maintain passwords in clear text. It maintains a salted hash of the password or the certificate. (FIA_UID.1.1, FIA_UID.1.2)
M-UL-2	Monitor requires each user to successfully authenticate with either a password or certificate before they are allowed to perform any other actions. Authentication/authorization is granted after the server-side SSL connection has been established between the user's browser or Studio and the Monitor itself. (FIA_UAU.1.1, FIA_UAU.1.2, FCS_COP.1.1)
M-UL3	Monitor locks user accounts when consecutive failed login attempts are performed on a given account By default accounts are lockout for a 30 min period after 3 failed attempts. (FIA_AFL.1.1, FIA_AFL.1.2)

Monitor Audit Function	
M-AUD-1	Monitor is able to generate audit records. (FAU_GEN.1.1) Application logs: Start-up and shutdown of audit functions Access to System Modifications to the audit function Modifications Use of authentication mechanism User logs: Access to System Access to the TOE and System data Download audit records (whomever can download can view) Unsuccessful attempts to read audit records Use of the user authentication mechanism
M-AUD-2	Monitor records the following information for all auditable events: date and time, type of event, subject identity (where applicable), success or failure, system from which a given request was made (where applicable). (FAU_GEN.1.2).
M-AUD-3	Monitor allows users with Authorized System Administrator role (root) access to read svstrace and svsuser by means of a console text-based application. (FAU_SAR.1.1)
M-AUD-4	Monitor provides audit records in text format. (FAU_SAR.1.2)
M-AUD-5	Monitor denies all users read access to the audit records, except those who have been granted explicit read access. (FAU_SAR.2.1)
M-AUD-6	Monitor provides administrators with root access with the ability to perform searches, sorting, and ordering of the audit data, based on date and time and event type. This is done by means of a console text-based application. (FAU_SAR.3)
M-AUD-7	Monitor is able to include or exclude auditable events from the set of audited events based on event type. This is done by means of a console text-based audit configurator that is available only to users with root access. (FAU_SEL.1)
M-AUD-8	Monitor protects audit records from unauthorized deletion and modification. Monitor ensures that at least 1 GB worth of audit records is maintained when audit storage exhaustion occurs. (FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3)
M-AUD-9	Monitor overwrites the oldest stored audit records if the audit trail is full. A daily cron job assesses whether the drive space is filling. If this were the case, this routine finds what the oldest record is and deletes it, while making sure it keeps the last 1 GB. If resources are still scarce it would delete the oldest file. If the disk is full, Monitor sends an SMTP and/or SNMP alert (depending on configuration). (FAU_STG.4.1)

Monitor Self Protection Function	
M-SPF-1	Monitor only establishes connections with Enterprise Manager and/or Studio when they are all properly authenticated with each other. This communication is client/server side SSL/TLS protected and the trust relationship must have been already established by the SV Manager user manually accepting the certificates. (FPT_ITT.1, FCS_COP.1.1)
M-SPF-2	Monitor is able to maintain its internal clock upon which all timestamps are based. In addition it can synchronize to an external NTP server. (FPT_STM.1)
M-SPF-3	Monitor is able to synchronize its clock with an Enterprise Manager, once trust has been established between the Monitor and the Enterprise Manager. (FPT_STM.1)

Monitor IDS System Function	
M-IDS-1	Monitor is able to collect the information listed below from an IPv4 and/or IPv6 network. Monitor does so by parsing network traffic and applying deep protocol decoding. The Monitor reconstructs network transactions into network events and signature events. Both events are written into DME files. DME streams are processed next by the Policy Engine. The user has the option of saving DME streams into the file system. (IDS_SDC_EXT.1.1, IDS_SDC_EXT_1.2) For all events, the following is recorded: Host identity Service Protocol Protocol attributes Timestamp Identification and Authentication events: • Kerberos: Name of Kerberos ticket holder. User@Domain and Machine@Domain for user and machine. • FTP: user name when authenticated • POP: user name when authenticated • SMTP: user name when authenticated • SSL: client certificate subject name • YIM & AOL: Yahoo IM and AOL IM authenticated handle • SIP: user name when authenticated Data Accesses: • HTTP: URLs, methods • TCP: Data Connection • FTP: Data Connection, list directories, file management, • DNS: zone transfers, queries. Service Requests: • Destination/source ports for TCP/UDP ○ Services as defined in Policy ○ Services as defined by IANA ○ Protocol/port number Detected signatures **Note**: For signatures to be applied, they must have been previously uploaded to the Monitor either through Studio or through the Securify NMSS service. Monitors would automatically connect to the NMSS service and download the most up-to-date set of signatures.

Monitor IDS System Function	
M-IDS-2	Monitor is able to evaluate network traffic against the Securify Policy and the signature engine. Once packets have been reassembled (where applicable), they are processed by both the signature engine and the DME process. The signature engine communicates to the DME process whether there have been matches to any of the configured signatures. The result when there is a positive match is included as part of the DME stream. Once the DME stream has been put together, it is passed to the Policy Engine. The Policy Engine follows a ‘most specific’ algorithm to establish the best matching rule to evaluate any given network transaction. It also evaluates the signature if present to the characteristics of the target system and the application protocol as decoded by the Monitor. In most cases, this mitigates the number of false positives. The rule chosen by the Policy Engine already has the severity assigned to such events. When signatures are present, the event always produces a signature event, even when the Policy about such traffic is set to be classified as an OK event. If the traffic is both a violation to Policy and it has a signature positive match, it generates both a violation event and a signature event. (IDS_ANL_EXT.1.1)
M-IDS-3	Monitor records the following information about the detected violations of Policy and signatures (once the Policy is applied, the set of information is known as a network event; if a signature is found, it is known as a signature event) (IDS_ANL_EXT.1.2): The following information is stored for a violation network event: Host identity Service Protocol Protocol attributes Timestamp Hostname Service name Outcome name Event severity Policy Category IP address for source and destination Target port Count The following information is stored for a signature event SSID – Signature identifier Signature Description – Name of the attack Signature Set – Name of the set to which the signature belongs to Severity Protocol – Application Protocol detected Outcome Behavior Security Zone Count
M-IDS-4	Monitor stores network events in a database accessible to the user for review and analysis, but not for modification or deletion. (IDS_RCT_EXT.1)
M-IDS-5	Monitor can be configured to send an SMTP message based on the correlation of one or more network events (otherwise known as Correlated Events). (IDS_RCT_EXT.)

Monitor IDS System Function	
M-IDS-6	Monitor provides the Operator, Analyst, and Developer roles with the ability to review network events. Monitor prevents access to this data by other roles maintained by the system. (IDS_RDR_EXT.1.1, IDS_RDR_EXT.1.3)
M-IDS-7	Monitor provides network event records in a manner suitable for authorized users to interpret the information. (IDS_RDR_EXT.1.2)
M-IDS-8	Monitor provides no interface for deleting or modifying network event records once they are stored in the database. (IDS_STG_EXT.1.1, IDS_STG_EXT.1.2)
M-IDS-9	Monitor ensures that 10 GB of network events are stored, even when system data storage exhaustion is reached. (IDS_STG_EXT.1.3)
M-IDS-10	Monitor overwrites the oldest record store whenever it is approaching its limit of storage. (IDS_STG_EXT.2.1, IDS_STG_EXT.1)

7.3.3 Securify^{TM} Enterprise Manager

Enterprise Manager User Access Function	
E-MUA-1	Enterprise Manager maintains the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. Enterprise Manager also maintains an authorized identifier for the Monitor(s) that it's managing. The trust relationship with the Monitor(s) is established by accepting the self-signed certificates manually. (FIA_ATD.1.1)
E-MUA-2	Enterprise Manager restricts the ability to access data as specified in Table 6-4. (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)
E-MUA-3	Enterprise Manager maintains the roles of Operator, Analyst, Developer, SV Manager, and Account Manager. (FMT_SMR.1.1, FMT_SMR.1.2)
E-MUA-4	Enterprise Manager allows SV Managers to set and configure the parameters of the account lockout feature (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)

Enterprise Manager User Login function	
E-UL-1	Enterprise Manager requires each user to identify themselves before they are allowed to perform any other actions. Enterprise Manager compares the credentials (username/password or hash of the certificate) to a locally maintained database. Enterprise Manager does not maintain passwords in clear text. It maintains a salted hash of the password or the certificate. (FIA_UID.1.1, FIA_UID.1.2)
E-UL-2	Enterprise Manager requires each user to successfully authenticate with either a password or certificate before they are allowed to perform any other actions. Authentication/authorization is granted after the server-side SSL connection has been established between the user's browser or Studio and Enterprise Manager itself. (FIA_UAU.1.1, FIA_UAU.1.2, FCS_COP.1.1)
E-UL-3	Enterprise Manager locks user accounts when consecutive failed login attempts are performed on a given account. By default, accounts are lockout for a 30 min period after 3 failed attempts. (FIA_AFL.1.1, FIA_AFL.1.2)

Enterprise Manager Audit Function	
E-AUD-1	Enterprise Manager is able to generate audit records. (FAU_GEN.1.1) Application logs: Start-up and shutdown of audit functions Access to System Modifications to the audit function Modifications Use of authentication mechanism User logs: Access to System Access to the TOE and System data Download audit records (whomever can download can view) Unsuccessful attempts to read audit records Use of the user authentication mechanism
E-AUD-2	Enterprise Manager records the following information for all auditable events: date and time, type of event, subject identity (where applicable), success or failure, system from which a given request were made (where applicable). (FAU_GEN.1.2).
E-AUD-3	Monitor allows users with Authorized System Administrator role (root) access to read svstrace and svsuser by means of a console text-based application. (FAU_SAR.1.1)
E-AUD-4	Enterprise Manager provides audit records in text format (FAU_SAR.1.2).
E-AUD-5	Enterprise Manager denies all users read access to the audit records, except those who have been granted explicit read access. (FAU_SAR.2.1)
E-AUD-6	Enterprise Manager provides administrators with root access with the ability to perform searches, sorting, and ordering of the audit data, based on date and time and event type. This is done by means of a console text-based application. (FAU_SAR.3)
E-AUD-7	Enterprise Manager is able to include or exclude auditable events from the set of audited events based on event type. This is done by means of a console text-based audit configurator that is available only to users with root access. (FAU_SEL.1)
E-AUD-8	Enterprise Manager protects audit records from unauthorized deletion and modification. Enterprise Manager ensures that at least 1 GB worth of audit records is maintained even when audit storage exhaustion occurs. (FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3)
E-AUD-9	Enterprise Manager overwrites the oldest stored audit records if the audit trail is full. A daily cron job assesses whether the drive space is filling. If this is the case, the cron job determines what is the oldest record and deletes it, while ensuring it keeps the last 1 GB. If resources are still scarce it deletes the oldest file. If the disk is full, Enterprise Manager sends an SMTP and/or SNMP alert (depending on configuration) (FAU_STG.4.1)

Enterprise Manager Self Protection Function	
E-SPF-1	Enterprise Manager only establishes connections with Monitor, ERGW and Studio when they are all properly authenticated with each other. This communication is client/server side SSL/TLS protected and the trust relationship must have been already established by the SV Manager user manually accepting the certificates (FPT_ITT.1, FCS_COP.1.1)

Enterprise Manager Self Protection Function	
E-SPF-2	Enterprise Manager is able to maintain its own internal clock upon which all timestamps are based. In addition it can synchronize to an external NTP server (FPT_STM.1)
E-SPF-3	Enterprise Manager pushes time configuration to a Monitor once trust has been established between the Monitor and the Enterprise Manager. (FPT_STM.1)

Enterprise Manager IDS System Function	
E-IDS-1	Enterprise Manager stores a summary of network events from the trusted Monitors in a database accessible to the user for review and analysis. The Enterprise Manager retrieves data (stored in proprietary files) from each Monitor every 5 minutes. (IDS_RCT_EXT.1)
E-IDS-2	Enterprise Manager provides the Operator, Analyst, and Developer roles with the ability to review network events. Enterprise Manager prevents access to this data by other roles maintained by the system (IDS_RDR_EXT.1.1, IDS_RDR_EXT.1.3)
E-IDS-3	Enterprise Manager provides network event records in a manner suitable for authorized users to interpret the information (IDS_RDR_EXT.1.2)
E-IDS-4	Enterprise Manager provides no interface for deleting or modifying network event records once they are stored in the database.(IDS_STG_EXT.1.1, IDS_STG_EXT.1.2)
E-IDS-5	Enterprise Manager ensures that 10 GB of network events are stored, even when system data storage exhaustion is reached. (IDS_STG_EXT.2.1, IDS_STG_EXT.1.3)
E-IDS-6	Enterprise Manager overwrites the oldest record store whenever it is approaching its limit of storage.(IDS_STG_EXT.1)
E-IDS-7	Enterprise Manager can be configured to export both network and signature events. It can export in SNMP and/or Syslog format. It can be configured to send all events, or it can be configured to send only those with a specified severity (for example, only critical events). The system can be configured to send all events or to send a maximum number of events per minute. Events exported through Syslog comply with CEF (Common Exchange Format).(IDS_RCT_EXT.1)

7.3.4 Securify^{TM} Enterprise Reporting Gateway

Enterprise Reporting Gateway (ERGW) Manage User Access Function	
ER-MUA-1	ERGW maintains the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. ERGW also maintains an authorized identifier for the Enterprise Manager(s) from which it is collecting data. The trust relationship with the Enterprise Manager(s) is established by accepting the self-signed certificates manually.((FIA_ATD.1.1)
ER-MUA-2	ERGW restricts the ability to access data as specified in Table 6-4. (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)
ER-MUA-3	ERGW maintains the roles ER SV Manager and ER Account Manager. (FMT_SMR.1.1, FMT_SMR.1.2)

Enterprise Reporting Gateway (ERGW) Manage User Access Function	
ER-MUA-4	ERGW allows ER SV Managers to set and configure the parameters of the account lockout feature (FMT_MTD.1.1, FMT_MOF.1.1, FMT_SMF.1)

Enterprise Reporting Gateway (ERGW) User Login function	
ER-UL-1	ERGW requires each user to identify themselves before they are allowed to perform any other actions. ERGW compares the credentials (username/password or hash of the certificate) to a locally maintained database. ERGW does not maintain passwords in clear text. It maintains a salted hash of the password or the certificate. (FIA_UID.1.1, FIA_UID.1.2)
ER-UL-2	ERGW requires each user to successfully authenticate with either a password or certificate before they are allowed to perform any other actions. Authentication/authorization is granted after the server-side SSL connection has been established between the users and ERGW itself. (FIA_UAU.1.1, FIA_UAU.1.2, FCS_COP.1.1)
ER-UL-3	ERGW locks user accounts when consecutive failed login attempts are performed on a given account (FIA_AFL.1.1, FIA_AFL.1.2)

Enterprise Reporting Gateway (ERGW) Audit Function	
ER-AUD-1	ERGW is able to generate audit records. (FAU_GEN.1.1) Application logs: Start-up and shutdown of audit functions Access to System Modifications to the audit function Modifications Use of authentication mechanism User logs: Access to System Download audit records (whomever can download can view) Unsuccessful attempts to read audit records Use of the user authentication mechanism
ER-AUD-2	ERGW records the following information for all auditable events: date and time, type of event, subject identity (where applicable), success or failure, system from which a given request were made (where applicable). (FAU_GEN.1.2).
ER-AUD-3	Monitor allows users with Authorized System Administrator role (root) access to read svstrace and svsuser by means of a console text-based application. (FAU_SAR.1.1)
ER-AUD-4	ERGW provides audit records in text format (FAU_SAR.1.2).
ER-AUD-5	ERGW denies all users read access to the audit records, except those who have been granted explicit read access. (FAU_SAR.2.1)
ER-AUD-6	ERGW provides administrators with root access with the ability to perform searches, sorting, and ordering of the audit data, based on date and time and event type. This is done by means of a console text-based application. (FAU_SAR.3)
ER-AUD-7	ERGW is able to include or exclude auditable events from the set of audited events based on event type. This is done by means of a console text-based audit configurator that is available only to users with root access. (FAU_SEL.1)

Enterprise Reporting Gateway (ERGW) Audit Function	
ER-AUD-8	ERGW protects audit records from unauthorized deletion and modification. ERGW ensures that at least 1 GB worth of audit records is maintained even when audit storage exhaustion occurs. (FAU_STG.2.1, FAU_STG.2.2, FAU_STG.2.3)
ER-AUD-9	ERGW overwrites the oldest stored audit records if the audit trail is full. A daily cron job assesses whether the drive space is filling. If this is the case, the cron job determines what is the oldest record and deletes it, while ensuring it keeps the last 1 GB. If resources are still scarce it deletes the oldest file. If the disk is full ERGW sends an SMTP and/or SNMP alert (depending on configuration). (FAU_STG.4.1)

Enterprise Reporting Gateway (ERGW) Self Protection Function	
ER-SPF-1	ERGW only establishes connections with Enterprise Manager when they are properly authenticated with each other. This communication is client/server side SSL/TLS protected and the trust relationship must have been already established by the SV Manager manually accepting the certificates (FPT_ITT.1, FCS_COP.1.1)
ER-SPF-2	ERGW is able to maintain its own internal clock upon which all timestamps are based. (FPT_STM.1)

Enterprise Reporting Gateway (ERGW) IDS System Function	
ER-IDS-1	ERGW collects summaries of network events as they are made available by the Enterprise Manager to which it is connected. The ERGW retrieves data (stored in proprietary files) from each Enterprise Manager every 10 minutes. (IDS_RCT.1)
ER-IDS-2	ERGW provides no interface for network events to be deleted or modified once they have been stored in its database.(IDS_STG_EXT.1.1, IDS_STG_EXT.1.2)
ER-IDS-3	ERGW ensures that 10 GB of network events are stored, even when system data storage exhaustion occurs. (IDS_STG_EXT.2.1, IDS_STG_EXT.1.3)
ER-IDS-4	ERGW overwrites the oldest record store whenever it is approaching its limit of storage.(IDS_STG_EXT.1)

7.4 Security Requirements Rationale

Table 7-1 shows the dependencies between the functional requirements, including the extended components. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 7-1: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	IT Environment*
2	FAU_SAR.1	Audit review	FAU_GEN.1	1
3	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	13
6	FAU_STG.2	Guarantees of data availabitlity	FAU_GEN.1	1
7	FAU_STG.4	Prevention of audit data loss	FAU_STG.1	6(H)
8	FIA_UAU.1	Timing of authentication	FIA_UID.1	11
9	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	8
10	FIA_ATD.1	User attribute definition	None	None
11	FIA_UID.1	Timing of identification	None	None
12	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	15
			FMT_SMF.1	14
13	FMT_MTD.1	Management of TSF data	FMT_SMF.1	14
14	FMT_SMF.1	Specification of Management Functions	None	None
15	FMT_SMR.1	Security roles	FIA_UID.1	11
16	FPT_ITT.1	Basic internal TSF data transfer protection	None	None
17	IDS_SDC_EXT.1	System Data Collection (EXT)	None	None
18	IDS_ANL_EXT.1	Analyzer analysis (EXT)	IDS_SDC_EXT.1	17
19	IDS_RCT_EXT.1	Analyzer react (EXT)	IDS_SDC_EXT.1	17
20	IDS_RDR_EXT.1	Restricted Data Review (EXT)	IDS_SDC_EXT.1	17
21	IDS_STG_EXT.1	Guarantee of System Data Availability (EXT)	IDS_SDC_EXT.1	17
22	IDS_STG_EXT.2	Prevention of System data loss (EXT)	IDS_SDC_EXT.1	17
23	FCS_COP.1	Cryptographic operation	FCS_CKM.1	See application note below
			FCS_CKM.4	

* Reliable timestamps are provided by the hardware and OS of the platforms that host the TOE components.

Application Note: FCS_CKM.1 Cryptographic key generation and FCS_CKM.4 Cryptographic key destruction are not further expanded for FCS_COP.1 because there are not functional requirements for key management. In particular, no user intervention is involved with the processes of creation, distribution, access and destruction of any cryptographic key for the operation of the TOE.

According to Common Criteria Part 2 “Security Functional Components” version 3.1 revision 2 paragraph 143 on FCS_CKM:

“This family should be included whenever there are functional requirements for the management of cryptographic keys.”