National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Securify^{TM} V6.0

Report Number: **CCEVS-VR-VID10316-2009**

Dated: **August 21, 2009**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Ms. Jean J. Hung
The MITRE Corporation
McLean, VA

Ms. Deborah Downs
Aerospace Corporation
El Segundo, CA

Ms. Jean Petty
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Mr. Sai Pulugurtha
CygnaCom Solutions
McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Securify^{TM} 6.0 Security Target.

Table of Contents

List of Figures

List of Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Securify v6.0.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

McAfee Network User Behavior Analysis v6.0 (Securify^{TM} v6.0 or TOE) is an appliance-based security product which monitors network access and behavior across systems and networks. SecurifyTM provides visibility as to who is doing what and where they are doing it across the network.

Securify™ v6.0 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.

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.

The TOE is intended for use in computing environments where there is a low level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in August 2009. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R2 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 extended from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, [CEM]. 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).

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document Securify v6.0 Security Target

2. Identification

Target of Evaluation: Securify^{TM} Version 6.0

Evaluated Software and Hardware:

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)

Developer: McAfee, Inc. (Securify, Inc.)

CCTL: CygnaCom Solutions
7925 Jones Branch Dr, Suite 5200
McLean, VA 22102-3321

Evaluators: Sai Pulugurtha

Validation Scheme: National Information Assurance Partnership CCEVS

Validators: Jean Hung, Deborah Downs, Jean Petty

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007

CEM Identification: Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 6.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

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.

Summary

A summary of the SFRs for the TOE are included in the following tables. Note that _EXP in the SFR ID indicates explicitly specified requirements.

Table 1 TOE Security Functional Requirements

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

TOE Security Functional Components		
No.	**Component**	**Component Name**
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

Table 2 Objectives for the Operational Environment

Security Objectives for the Operational Environment		
1	OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
2	OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information
3	OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
4	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.
5	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.
6	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.
7	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
8	OE.INTROP	The TOE is interoperable with the IT System it monitors.

4. Assumptions and Clarification of Scope

Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures

Assumptions

Table 3 Assumptions

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

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.

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.

Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. 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.

5. 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.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

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. 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.

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

  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: the SV Manager role is required to download Application Logs and the Account Manager role is required to download User Logs. It is important to note that each Monitor allows the Enterprise Manager that manages it to pull both Application and User Logs.

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.

- **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 Enterprize Manager Provides the following functionality:

  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 provides 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 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. 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.

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.

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

  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.

Securify System Configurations and Inter-connections

- **Stand-alone Monitor**

  This configuration consists of the following Securify components:

  - Securify Studio
  - One Securify Monitor

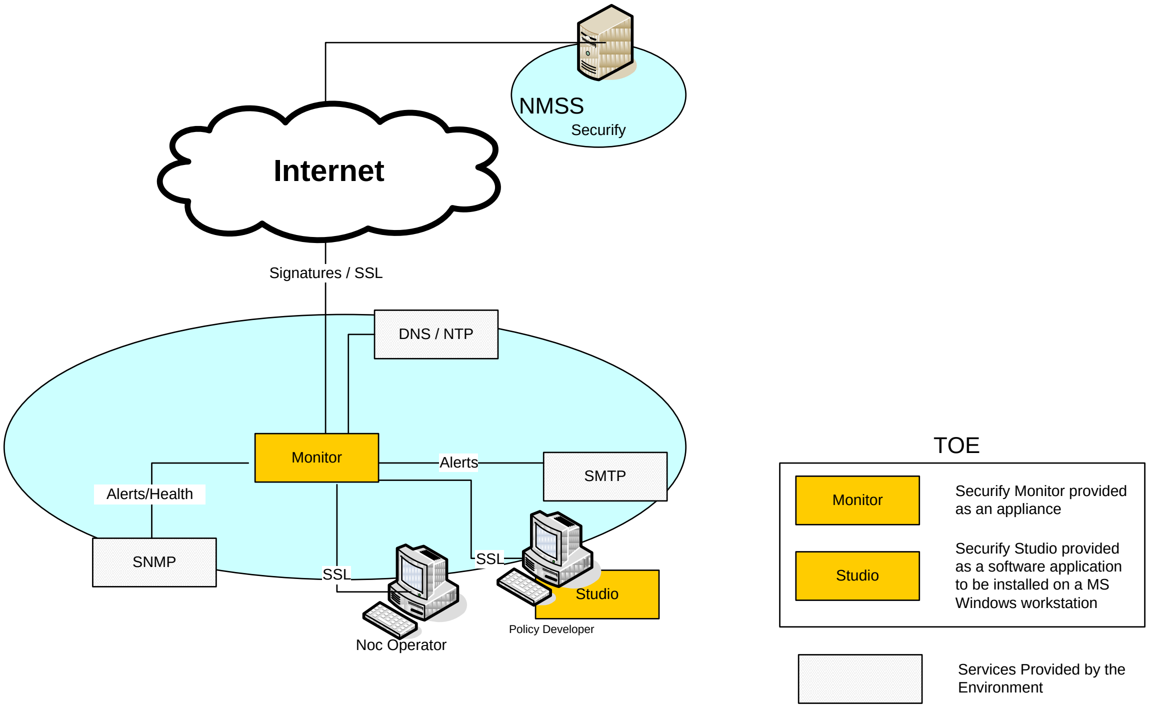
NMSS
Securify
Internet
Signatures / SSL
DNS / NTP
Monitor
Alerts
SMTP
Alerts/Health
SNMP
SSL
SSL
Studio
Noc Operator
Policy Developer
TOE
Monitor
Securify Monitor provided as an appliance
Studio
Securify Studio provided as a software application to be installed on a MS Windows workstation
Services Provided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

Figure 5-1 Securify Deployment Single 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.

- **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)

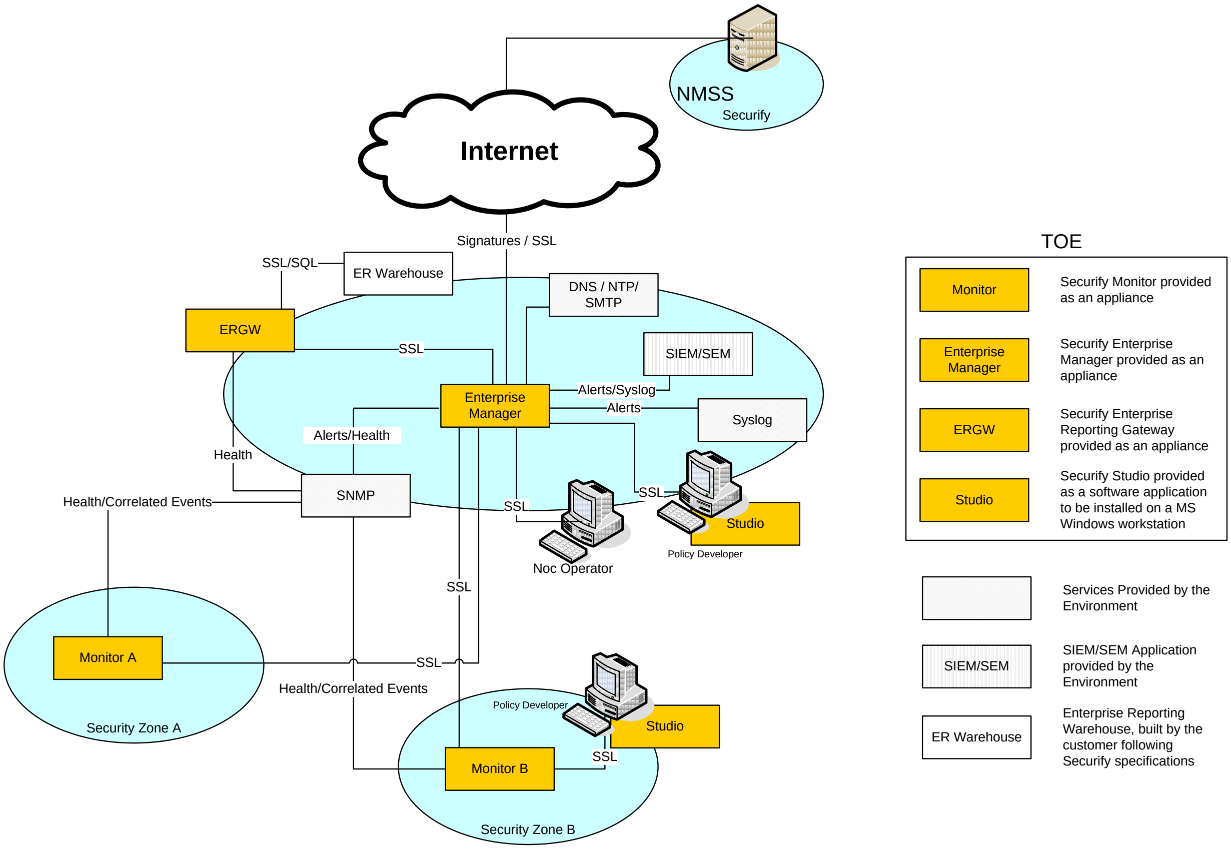
NMSS
Securify
Internet
Signatures / SSL
SSL/SQL
ER Warehouse
DNS / NTP/ SMTP
ERGW
SSL
SIEM/SEM
Enterprise Manager
Alerts/Syslog
Alerts
Syslog
Alerts/Health
Health
SNMP
Health/Correlated Events
SSL
SSL
Studio
Noc Operator
Policy Developer
SSL
Monitor A
SSL
Security Zone A
Health/Correlated Events
Policy 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 5-2 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.

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 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.

6. Documentation

Table 4 Evaluation Documentation and Evidence

Securify v6.0 Enterprise Reporting Operations Guide	SV-ER-600-06-08
Securify v6.0 Studio User Guide	SV-SG-600-06-08
Securify v6.0 Web Application	SV-OG-600-06-08
Securify v6.0 Deployment Guide	SV-DG-600-06-08
Securify v6.0 Installation Guide	SV-IG-600-06-08
Securify v6.0 ADV (ADV_FSP.2 and ADV_TDS.1)	3.2
Securify v6.0 ADV_TDS.1 Addendum	1.0
Securify v6.0 ADV_ARC.1	1.0
Securify v6.0 AGD_PRE.1	3.0
Securify V6.0 CM Capabilities and Scope (ALC_CMC.2 and ALC_CMS.2)	1.1
Securify v60.0 Delivery Procedure (ALC_DEL.1)	1.0
Securify v6.0 Flaw Remediation and Reporting Procedures (ALC_FLR.2)	1.0
Securify v6.0 List of Controlled Files (ALC)	1.0
Securify v6.0 Common Criteria Addendum	2.0
Securify v6.0 Tests (ATE_COV.1)	1.2
Securify V6.0_ATE_FUN.1_Supplemental_IDS_References.xls	2.0
Securify v6.0 TM-Monitor (ATE_FUN.1)	1.3
Securify v6.0 TM-EnterpriseManager (ATE_FUN.1)	1.3
Securify v6.0 TM-Studio (ATE_FUN.1)	1.3
Securify v6.0 TM-ERGW (ATE_FUN.1)	1.3
Securify v6.0 TM-Sentinel (ATE_FUN.1)	1.2
Securify V6.0_MappingOfWebInterfaceObjects.xls (ATE_FUN.1)	1.0
Securify v6.0 TM-AccountLockout (ATE_FUN.1)	1.2
Securify v6.0 CI List	8.2
Securify v6.0 Administrator Addendum	3.0
Security Target	3.2

IT Product Testing

At EAL 2, the overall purpose of the testing activity is “independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests” (ATE_IND.2, 14.6.2.1 [CEM])

At EAL 2, the developer’s test evidence must “show the correspondence between the tests provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all TSFI have been tested, or that all externally-visible interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during the independent testing.” (ATE_COV.1, 14.3.1.3 [CEM])

This section describes the testing efforts of the vendor and the evaluation team.

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE_IND.2, Independent testing – sample [CC]).

Developer Testing

The test approach consists of manual tests and automated tests that were grouped together under the TOE component being tested. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan and procedures do not cover every possible combination of parameters for a given interface and every possible combination of parameters for a given security function. However, the test plan and procedures do stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The evaluator determined that the developer’s approach to testing the TSFs was adequate for an EAL2 evaluation.

Evaluator Independent Testing

CygnaCom has selected approximately 60% of the tests Securify provided as evaluation evidence. The tests were selected to exercise security functions from the externally visible TSFI.

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised
- All Security Functional Requirements are tested.

Since the product is a Intrusion Detection System emphasis was on the IDS functionality along with Security Management (SM), Identification and Authentication functionality (I & A). The test provided by the developer and the test sample of the developer tests selected tested security functions at appropriate level of rigor commensurate with EAL2. The evaluator augmented the IDS_* SFR tests to test the signature based detection and protocol behaviour detection functionality. CygnaCom’s independent tests augment and supplement the tests Securify provided as evaluation evidence.

More emphasis is laid on the Network Interface (Where the IDS functionality is implemented) being tested. The evaluator ensured that the test sample contains a good representative sample of the protocols and policy violations referenced in the Functional Specification and user guidance documents.

7. Evaluated Configuration

The following Evaluated Configuration(s) (consistent with the ST) are used for testing:

- Single Monitor Mode
- Full Configuraion

8. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.2 Use of a CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample
- AVA_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached PASS verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.

The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9. Validators Comments/Recommendations

The validators recommend that the TOE be certified as meeting Common Criteria version 3.1 R2 [CC] Part 2 extended and Part 3 conformant, and assurance requirements of EAL 2 extended from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R2.

10. Security Target

The Securify V6.0 Security Target is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

11. Glossary

The following is an acronym list used within this validation report other evaluation evidence such as the ST.

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

This section defines the Common Criteria terms. Not all of these terms are used in this document.

Assignment The specification of an identified parameter in a component.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent’s expertise, resources and motivation.

Augmentation The addition of one or more assurance component(s) to a package.

Authentication data Information used to verify the claimed identity of a user.

Authorised user A user who may, in accordance with the SFR, perform an operation.

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements on which requirements may be based.

Connectivity The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package..

Element An indivisible security requirement.

Evaluation Assessment of a PP, an ST, or a TOE against defined criteria.

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.

Evaluation scheme The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External entity Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Identity A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal Expressed in natural language.

Inter-TSF transfers Communicating data between the TOE and the security functions of other trusted IT products.

Internal communication channel A communication channel between separated parts of TOE.

Internal TOE transfer Communicating data between separated parts of the TOE.

Iteration The use of the same component to express two or more distinct requirements.

Object A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Organizational security policies A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.

Package A named set of either functional or assurance requirements (e.g. EAL 3).

Protection Profile (PP) An implementation-independent statement of security needs for a TOE type.

Prove This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, "prove" is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.

Refinement The addition of details to a component.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Secure state A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

Security attribute A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP) A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

Security Target (ST) An implementation-dependent statement of security needs for a specific identified TOE.

Selection The specification of one or more items from a list in a component.

Semiformal Expressed in a restricted syntax language with defined semantics.

Subject An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE) A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE resource Anything useable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

Transfers outside TSF TSF mediated communication of data to entities not under control of the TSF.

Trusted channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted path a means by which a user and a TSF can communicate with necessary confidence.

TSF data Data created by and for the TOE, that might affect the operation of the TOE.

TSF interface (TSFI) A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

User See **external entity**

User data Data created by and for the user that does not affect the operation of the TSF.

12. 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.

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- McAfee, Inc. (http://www.mcafee.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007.

Other Documents

- [ST] Securify^{TM} V6.0 Security Target