National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module

Report Number: CCEVS-VID10276-2010

Dated: 4 November 2010

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

Jerry Myers
Ken Eggers
Dave Dignan

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 6 May 2010. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.3, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The Target of Evaluation (TOE) is the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module.

The TOE is an automated real-time intrusion detection system (IDS) designed to protect 10/100/1000 Mbps copper and 1000 Mbps SX network segments. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE comprises two components:

A) Proventia G 1.3 appliance (hereafter referred to as Proventia G 1.3, Proventia GX, Sensor or Agent).

B) SiteProtector 2.0 Service Pack 6.1 with Reporting Module. (hereafter referred to as SiteProtector 2.0 Service Pack 6.1 with Reporting Module or SiteProtector)

The Proventia GX TOE component provides the IDS functionality. This Sensor monitors a network or networks and compares incoming packets against known packets and packet patterns that indicate a potential security violation. If a match occurs, Proventia GX will create an audit record. The SiteProtector 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators.

The Sensor monitors one or more 10/100/1000 Mbps copper or 1000 Mbps SX fibre network segments (the sensed, monitored network).

The SiteProtector Version 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation is connected to the appliance via TLS session, and is only used by authorized administrators for the management of the appliance.

Audit Security Function: The TOE's Audit Security Function provides audit data generation, selective auditing, audit data viewing and selective audit data viewing.

Intrusion Detection Security Function: The TOE provides Intrusion Detection Security Functionality by continuously monitoring network traffic, comparing this traffic to signatures, and reporting any match that may indicate an intrusion.

Self Protection Security Function: The TOE Self Protection Security Functionality provides functionality that protects its TSF Data and TOE functions from unauthorized access.

Management Security Function: The TOE's Management Security Function provides an interface that enables an authorized user to manage and monitor the TOE.

Reaction Security Function: The TOE's Reaction Security Function provides the actions taken in response to a detected intrusion attempt.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted information technology product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories, called Common Criteria Testing Laboratories (CCTLs), using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module
Protection Profile	N/A
Security Target	IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Security Target, dated May 10, 2010.
Evaluation Technical Report	Evaluation Technical Report for the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module, Document No. E2-0110-007, dated May 10, 2010.
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.3 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on December 6, 2006.
Version of CEM	CEM Version 2.3 and all applicable NIAP and International Interpretations effective on December 6, 2006.

IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module	
Sponsor	IBM Internet Security Systems, Inc. 6303 Barfield Road Atlanta, GA 30328
Developer	IBM Internet Security Systems, Inc. 6303 Barfield Road Atlanta, GA 30328
Evaluator(s)	**COACT Incorporated** Bob Roland Greg Beaver Pascal Patin Brian Pleffner
Validator(s)	**NIAP CCEVS** Jerry Myers Ken Eggers David Dignan

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 TOE Description

The TOE is an automated real-time intrusion detection system (IDS) designed to protect 10/100/1000 Mbps copper and 1000 Mbps SX network segments. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE comprises two components:

A) Proventia G 1.3 appliance (hereafter referred to as Proventia G 1.3, Proventia GX, Sensor or Agent).

B) SiteProtector 2.0 Service Pack 6.1 with Reporting Module. (hereafter referred to as SiteProtector 2.0 Service Pack 6.1 with Reporting Module or SiteProtector)

The Proventia GX TOE component provides the IDS functionality. This Sensor monitors a network or networks and compares incoming packets against known packets and packet patterns that indicate a potential security violation. If a match occurs, Proventia GX will create

an audit record. The SiteProtector 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators.

The Sensor monitors one or more 10/100/1000 Mbps copper or 1000 Mbps SX fibre network segments (the sensed, monitored network).

The SiteProtector Version 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation is connected to the appliance via TLS session, and is only used by authorized administrators for the management of the appliance.

Audit Security Function: The TOE's Audit Security Function provides audit data generation, selective auditing, audit data viewing and selective audit data viewing.

Intrusion Detection Security Function: The TOE provides Intrusion Detection Security Functionality by continuously monitoring network traffic, comparing this traffic to signatures, and reporting any match that may indicate an intrusion.

Self Protection Security Function: The TOE Self Protection Security Functionality provides functionality that protects its TSF Data and TOE functions from unauthorized access.

Management Security Function: The TOE's Management Security Function provides an interface that enables an authorized user to manage and monitor the TOE.

Reaction Security Function: The TOE's Reaction Security Function provides the actions taken in response to a detected intrusion attempt.

4 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

5 Threats

The threats identified in the following table sections are addressed by the TOE and/or Operating Environment. The following threats are addressed by the TOE and IT environment, respectively.

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.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
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.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.SCNCFG	Improper security configuration setting may exist in the IT System the TOE monitors.
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.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or 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.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

6 Clarification of Scope

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia G 1.3) and one instance of a workstation running SiteProtector 2.0 Service Pack 6.1 with Reporting Module.

Excluded Functionality

The following list itemizes configuration options excluded from the TOE for the evaluated configuration:

1. Telnet server support in the Sensors is not included. Telnet is disabled on the sensor by default, and it must remain disabled for the evaluated configuration.

2. Incidents and Exceptions are disabled.

3. The evaluated configuration of SiteProtector does not have Internet access to the ISS website. Automatic retrieval is disabled. Therefore, SiteProtector will not periodically check the ISS website for new software updates and automatically retrieve and store the updates on the SiteProtector system.

4. Intrusion Prevention and firewall functionality provided by Proventia GX is not included in the evaluated configuration.

5. Remote SiteProtector Console is not supported in the evaluated configuration.

6. Management via local management or web interface directly to the Proventia GX is not included in the evaluated configuration. Local management by the Console port and the Proventia Manager Web interface are used for initial installation and configuration only. These two interfaces are not to be used after the TOE has been placed into the evaluated configuration.

SiteProtector Host Minimum Requirements

The minimum requirements for the SiteProtector Host (supplied by the IT Environment) are described in the following table.

Table 2 - SiteProtector Component Requirements

Minimum Requirements	
Processor	1 GHz Pentium III
Memory	1 GB
Disk Space	8 GB
Operating System	Windows 2000 Server with Service Pack 4 or later, or Windows 2000 Advanced Server with Service Pack 4 or later, or Windows Server 2003 with or without Service Pack 1, or Windows Enterprise Server 2003 with Service Pack 1
DBMS	SQL Server 2000 Desktop Engine (MSDE) with Service Pack 3a and Security Patch 03-031 or SQL Server 2000 with Service Pack 3a and SQL Security Patch MS03-031 or SQL Server 2000 with Service Pack 4
Additional Software	Microsoft Internet Explorer 5.0 or higher Microsoft Data Access Components (MDAC) 2.8 or later Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.5.0_06 Adobe Acrobat Reader 6.0 or later OpenSSL 0.9.7d
Network Configuration	Static IP address
Disk Partition Formats	NTFS

In larger configurations, TOE components may be distributed across multiple systems. In such cases, the distributed components must meet the following evaluated configuration restrictions:

1. SiteProtector components and the DBMS implementation must reside on one workstation.

2. Proventia GX and SiteProtector must communicate via TLS.

3. SSL or encrypted SQL must be used for the communication between SiteProtector and the DBMS. SSL encryption can be manually configured by the user for each component that connects to the DB. The SiteProtector documentation includes steps to manually

configure SSL. Neither data nor database code is encrypted, encryption occurs only in the communications to the DB.

4. The SiteProtector Reporting Module add-on must be installed and configured. The Reporting Module is licensed to allow viewing of Audit Reports; it does not generate audit data. The Reporting Module requires the end user to purchase a license to unlock this functionality within the TOE.

Exclusions from TOE Security Functions

This section presents a delineation of components that are in the TOE, but do not contribute to meeting any of the Security Functional Requirements (SFRs) and hence are excluded from the TOE Security Functions (TSF).

- The Intrusion Prevention System (IPS) Component
- The Incident and Exception Component
- Firewall capabilities
- Administrator access to the Proventia GX other than through SiteProtector.

7 Architecture

The Proventia GX and SiteProtector TOE components are described in the following sections:

Proventia GX TOE Component

The Proventia GX TOE component provides IDS security functionality. The Proventia GX TOE component consists of Proventia G 1.3 firmware and is made up of one of the following appliances GX4002, GX4004, GX5008 C, CF and SFP (Copper, Copper/Fibre and small form factor pluggable port configuration), GX5208 and GX5108 (C, CF and SFP) appliances. The Proventia GX TOE component includes the Proventia GX appliance hardware, the appliance resident Red Hat operating system (OS) and the Proventia GX application software image.

Proventia GX Sensors monitor packets on a sensed, monitored network or networks and compare the incoming packets against signatures. Signatures are known packets or packet patterns that indicate a possible attack or intrusion against hosts or network segments. If a match occurs, the Sensors create an event (system data record). This data is sent to the TOE's SiteProtector which enables an administrator to view and analyze the information.

Signatures are configured on the Sensors by Policy Files. Policy Files identify a sub-set of signatures based on attack type. At TOE installation time, the SiteProtector is installed with a set of Policy Files and the Sensors are configured with one default Policy File and the signature files that apply to all Policy Files. SiteProtector enables an administrator to disable/enable signatures in a Sensor's current Policy File or select and apply a new Policy File selected from the set of Policy Files.

SiteProtector 2.0 Service Pack 6.1 TOE Component

The SiteProtector 2.0 Service Pack 6.1 with Reporting Module component of the TOE is a software product that runs on a Windows based workstation. The SiteProtector enables

administrators to monitor and manage the Sensor components of the TOE. The SiteProtector TOE component includes the SiteProtector 2.0 Service Pack 6.1 with Reporting Module software.

The SiteProtector is used as the central controlling point for Sensors deployed on the network. The SiteProtector performs the following functionality:

A) Manages and monitors Sensors and SiteProtector sub-components;

B) Enables an administrator to view TOE component configuration data;

C) Displays audit and system data records; and

D) Monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

The SiteProtector is divided into the following software sub-components:

a) SiteProtector Console – The SiteProtector Console is a graphical user interface (GUI) that provides an interface that enables an Administrator to configure and monitor the Sensors. The add-on Reporting Module provides the ability to generate a wide range of reports in a variety of formats, including the following:

1. Vulnerability Assessment reports
2. Attack Activity reports
3. User Audit reports
4. Content Filtering reports
5. User Permission reports

b) SiteProtector Event Collector – The SiteProtector Event Collector is a software process that is responsible for receiving data from the Sensors and storing the data in the database via the DBMS.

c) SiteProtector Application Server – The SiteProtector Application Server is a software process that is responsible for providing the communication path between the DBMS and all other SiteProtector software components.

SiteProtector Sensor Controller – The SiteProtector Sensor Controller is a software process that is responsible for processing command and control information from the SiteProtector Console and the database (via the SiteProtector Application Server) and sending the command and control information to the Sensors or the SiteProtector Event Collector.

8 Security Policy

The Security Functional Policies (SFPs) implemented by Proventia GX and SiteProtector are based on the set of security policies that support intrusion detection, audit, management, self protection, and reaction.

Note: Much of the description of the Proventia GX and SiteProtector security policy has been extracted and reworked from the Proventia GX and SiteProtector Security Target.

8.1 Intrusion Detection Security Function

The TOE Intrusion Detection Security Function continuously monitors network traffic; comparing packets to signatures identified in the Sensor's Policy File. Signatures identify packets and packet patterns that indicate the presence of a potential security violation on a device accessible by the Sensor's monitored network. The Sensor detects a security violation when an incoming packet matches a signature defined in a Sensor's Policy File. When this occurs, the Sensor creates a system data record (event) that includes the date and time of the event, type of event, subject identity, event outcome (success or failure), protocol, and source and destination IP addresses.

Sensors are shipped with a default Policy File that includes pre-defined signatures for detection of denial of service, unauthorized access attempts, pre-attack probes, and suspicious activity. An authorized user may customize a Sensor Policy File by enabling or disabling the signatures present in the Policy file. Reactions taken for specific events (e.g., generating an email and/or SNMP trap) are also configured via the Policy Files.

8.2 Audit Security Function

The TOE Audit Security Functional records both audit records and system data records (events). The Audit Security Function includes audit data generation and system data generation; audit data selective generation; audit and system data viewing; audit and system data selective viewing; audit and system data storage; and viewing of TOE generated alerts.

Audit Data Generation: Audit data records are generated as the result of administrator execution of management functions. These functions are generated locally on the SiteProtector host and include starting and stopping Sensors, applying sensor policy files, and receipt of completion indications from Sensors reporting the completion of these events.

System Data Generation: The System Data Generation reports possible security violations as the result of collecting and analyzing network traffic. A System Data event is generated by the Intrusion Detection Security Function when a security violation is detected as a result of network traffic matching a signature in the Sensor's Policy File. Data included in the Event is date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, protocol and source and destination IP address.

Audit Data and System Data Viewing
The TOE provides the same functionality for viewing audit data and viewing system data using the DBMS to retrieve the audit and system data. Data records include date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, protocol, and source and destination IP address (if applicable). A SiteProtector Administrator must explicitly configure Windows users to the SiteProtector database to allow access to audit and system data. Audit data is viewable only through administrator-created Audit Detail Reports, each of which is accessible only to administrators with appropriate permissions for the group. Administrators with appropriate global permissions may enable or disable individual audit events. Authorized users with appropriate audit and system data permission may sort data, by event, type of event, subject identity, and the outcome (success or failure) of the event after the information has been retrieved database by the DBMS.

Alert Viewing
Alarms are messages displayed in a SiteProtector Console window to any user who has successfully logged onto the SiteProtector. These are generated when DBMS audit storage is full when attempting to store a new record or when a potential intrusion is detected.

Audit Data Selective Auditing
An Administrator may include or exclude auditable events from the set of auditable events based on event type. All management actions defined in the Management Security Function are auditable and all audits may be disabled or enabled based on event type.

Audit Data and System Data Storage
Audit and system data are stored in the database via the DBMS. The IT Environment provides protection from unauthorized deletion or modification from interfaces outside the TSC for the records stored in the DBMS. If the database becomes full, the DBMS notifies the TOE, which sends an alarm to the SiteProtector Console, then the DBMS continues storing audit records; overwriting the oldest records in the database.

8.3 Management Security Function

The Management Security Function facilitates management of TOE components using through SiteProtector's GUI interface. User accounts are defined as part of the IT Environment (Windows). Users authenticate through the SiteProtector GUI, which passes the authentication information to Windows to determine whether the user has been successfully authenticated.

If the user has been authenticated to Windows, SiteProtector acquires the user's permissions from the database. Otherwise, it terminates the session. Permissions give the possessing user the capability to perform specific administrative actions. Permissions are individually configurable, but may be assigned to User Accounts or to groups, comprising one or more users. The GUI enforces permissions by enabling only those actions covered by permissions associated with the user or a group of which the user is a member.

The Apply Policy GUI allows users to customize Policy Files and apply these to Sensors. Policy File customization allows authorized users to enable or disable signatures, affecting the security violation patterns that may be recognized by the Sensors, and to configure Reactions (e.g., email notifications or SNMP traps) in response to specific events. Once customized, a separate user action is required to apply the Policy File to a Sensor. Additional GUI screens also enable an authorized user to control the starting and stopping the sensing capability of the Sensors.

The Management Security Function also includes the modification of the system data collection, analysis and reaction capabilities of the TOE. These capabilities manage how the TOE collects, analyzes and reacts to data collected from the monitored network. Only an authorized Administrator (e.g., modify permission for the signatures) has the ability to modify or add system data (i.e., enable signatures in a policy files). An administrator with view permission for reports is allowed to query TSF data (i.e., view the audit trail).

8.4 Self Protection Security Function

The TOE's Self Protection Security Functional provides domain separation and non-bypassability for functions within the TSC and part of the protection mechanism for intra-TOE communication.

Proventia GX Component

The Proventia GX (Sensor) TOE component comprises all hardware and software making up the Sensor appliance, including all functions that provide IDS functionality to the monitored network. It maintains its security domain through well defined monitoring and management interfaces and by allowing only a strictly controlled set of TSP-enforcing functions through these interfaces. It provides non-bypassability by mediating access to its own interfaces and ensuring that any TSF-mediated action proceeds only after the TOE security policy is invoked and successful. The strictly controlled functionality provided by the interfaces protects the Sensor component security domain from interference and tampering.

Sensor components include monitoring (or "sensing") interfaces that connect to the monitored network. These interfaces monitor the network packets based on the Sensor's Policy File signatures. No other functionality (programmatic or user-accessible) is available through the monitoring interface to either authorized or un-authorized subjects.

The Sensor management interface communicates with SiteProtector. This interface ensures that all enforcement functions successfully succeed before allowing any other Sensor component management actions to proceed. Only authorized subjects are allowed to connect and communicate with the Sensor management interface.

Inter-TOE Communications

The TOE uses TLS 1.0 to protect communication between the Sensors and SiteProtector using the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite and SHA-1 for message integrity. The TLS implementation is included inside the TOE boundary in the Sensors and is part of the IT Environment (using OpenSSL 0.9.7d) with SiteProtector. Session keys held in memory are zeroized (overwritten with all zeros) when a session ends. RSA certificates are generated by the IT Environment during installation of the TOE.

SiteProtector Component

The SiteProtector TOE component relies on the operating system to protect itself from interference from users outside the TSC. Within the TSC, SiteProtector provides for self protection and non-bypassability of functions. SiteProtector provides access by multiple administrators concurrently; maintaining a separate session for each administrator. Within each session, SiteProtector ensures that proper access restrictions are applied to each session based on individual administrator's permissions. Through the use of separate administrative sessions, the SiteProtector ensures that security functions within the TSC cannot be bypassed.

SiteProtector provides graphical user interfaces (GUIs) to manage and monitor the Sensor(s). These GUIs provide strictly controlled functionality to the users within the TSC, protecting the TOE from corruption or compromise from these users. Human users must be authenticated by SiteProtector before they may carry out any action within the TSC (see Section 7.3, Management Security Function).

The network and application interfaces of SiteProtector are used solely to collect data from and communicate with the Proventia GX Sensors. When invoked, the SiteProtector interfaces execute the TSP enforcement functions prior to permitting any subsequent SiteProtector action.

SiteProtector maintains a separate domain for itself that prevents it from being interfered with or tampered with by those users that are within the TSC. This is implemented using the following features:

- Protected storage for TSF data,
- Well-defined GUI and network and application communications interfaces,
- Strictly controlled set of functionality through these interfaces, and
- No general purpose computing or programming capabilities.

8.5 Reaction Security Function

The Reaction Security Function provides the TOE's reaction capabilities when the Sensor has detected an intrusion (See Section 7.1, Intrusion Detection Security Function). When this happens, the Sensor will send an alarm to the SiteProtector where it can be viewed on the Console by an authorized user. The Sensor can also be configured in conjunction with SiteProtector to perform the following types of responses for detected intrusions:

- Email Response,
- Log Evidence Response,
- Quarantine Response
- SNMP Trap Response, and
- User Specified Response

Delivery of responses is the responsibility of the IT Environment.

9 Documentation and Delivery

The Proventia GX product is delivered to the customer's location by the preferred carrier, DHL. Signature confirmation of delivery is required. The delivery contains a Proventia GX hardware appliance already loaded with the Proventia GX 1.3 firmware.

For the remaining delivery procedures, the customer is instructed to download components from the ISS website. Software products are delivered to the customer via download after purchase of the software from ISS.

Customers who order software components are sent an e-mail message containing details of their access to the Internet Security Systems True Blue Customer Portal, ISS Customer Portal. The e-mail contains a user id (the registered e-mail of the customer receiving the product), a temporary password, and a link that allows the receiving customer of the e-mail to register with the ISS Customer Portal.

On the initial login the user must change the customer password. The ISS Customer Portal is protected by 128-bit SSL encryption. The certificate can be verified as an ISS certificate using the security features of the web browser used to connect to the ISS Customer Portal. For example, in Microsoft's Internet Explorer (IE) the customer can double click on the pad lock icon on the tool bar at the bottom of the browser on the far right to see the certificate information. Once changed from the customer password, the user must keep their user ID and password unchanged so that they can download the desired software.

To download any of the product components described in the sections below, the customer must login to the ISS website. From the main ISS page, click on the "Downloads" link at the top. From there, click "Sign into the Download Center" in the Business Security Products box which takes the customer to the login screen at

https://www.iss.net/issEn/MYISS/login.jhtml?action=download

Four CDs are delivered with the TOE:

1. GX4000 Series Recovery.
2. Management #1 Deployment Manager/SiteProtector 2.0 Service Pack 6.1 Readme.
3. Management #2 Express.
4. Terms and Conditions.

Also delivered with the TOE is a hardcopy – Getting Started GX4000 Series Appliance (Part Code DOC-QSD-GX4-001.

The following documents are delivered by the Web site TOE download and the Website documentation download site.

TOE Download Link

Proventia Management SiteProtector Installation Guide Version 2.0, Service Pack 6.1, November 29, 2006.

Proventia Network IPS G and GX Appliance User Guide December 1, 2006.

IBM PROVENTIA GX 1.3 and SiteProtector 2.0 Service Pack 6.1 Installation, Generation and Start-Up Supplement Version 3.1, January 21, 2009 .

Documentation Download Link

Proventia Management SiteProtector Installation Guide Version 2.0, Service Pack 6.1, November 29, 2006

Proventia GX5008C Appliance QuickStart Card MSM-ISSQSCGX5008C

Proventia GX5008CF Appliance QuickStart Card MSM-ISSQSCGX5008CF

Proventia GX5108C Appliance QuickStart Card MSM-ISSQSCGX5108C

Proventia GX5108CF Appliance QuickStart Card MSM-ISSQSCGX5108CF

Proventia GX4002 Appliance QuickStart Card PM-PNIPSQRCGX4-0306

Proventia GX4004 Appliance QuickStart Card PM-PNIPSQRCGX4-0306

Proventia Network IPS G and GX Appliance User Guide December 1, 2006

Proventia Management SiteProtector Configuration Guide Version 2.0, Service Pack 6.1, November 21, 2006

Proventia Management SiteProtector User Guide for Security Analysts Version 2.0, Service Pack 6.1, May 9, 2007

Proventia Management SiteProtector Policies and Responses Configuration Guide Version 2.0, Service Pack 6.1, November 10, 2006

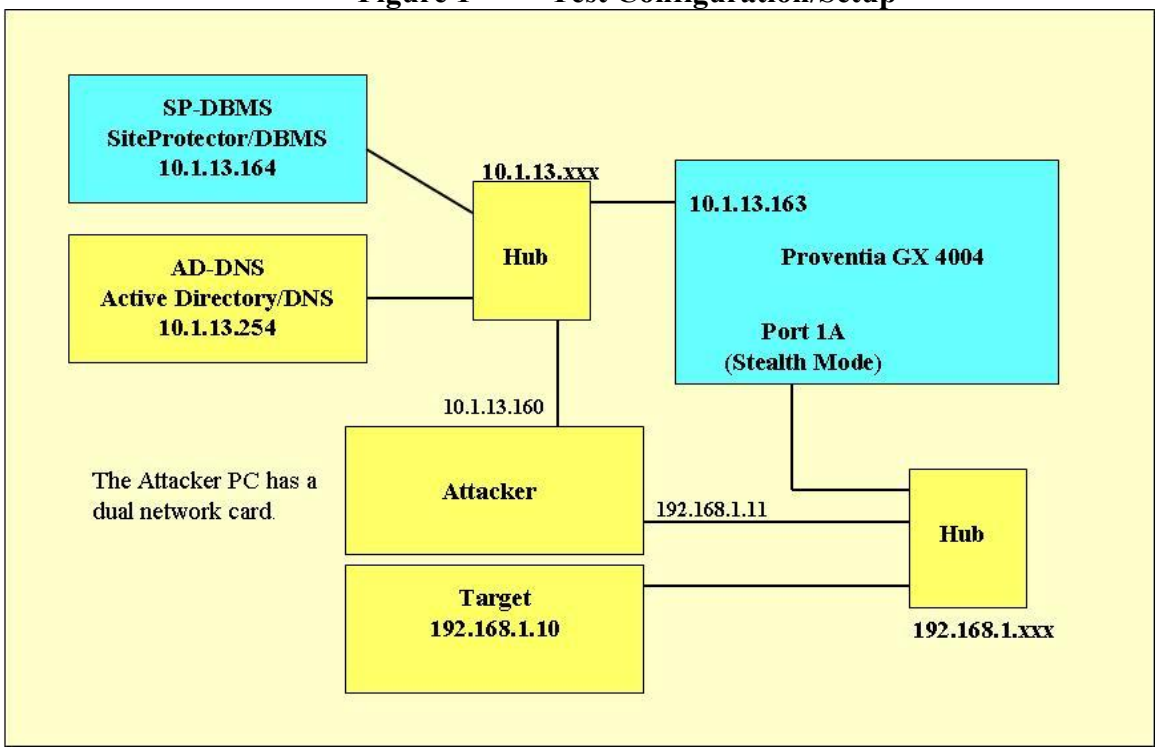
10 IT Product Testing

Testing was completed on June 9, 2009 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

10.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

Figure 1 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 3 - Test Configuration Overview

System	Purpose
SP-DBMS	This system provides the single instance of SiteProtector. It also hosts the DBMS and SiteProtector Console software. The system should be configured per the figure above, with the Active Directory and DNS servers both configured as CoactLab.
AD-DNS	In DNS, records should be configured for each of the systems shown in the figure above. The name GX4004 maps to address 10.1.13.163. The name SP-DBMS maps to the address 10.1.13.164.
GX4004	The Proventia Intrusion Detection System. Port 10.1.13.163 is the management port. Port 1A is the Sensing port, configured in stealth mode.
Attacker	This is the PC that will be used to attack the Target PC, the SiteProtector, and the GX4004 appliance.
Target	This is the PC that will be the receipitant of the attacks.

Specific configuration details for each of the systems are provided in the tables below.

Table 4 - SP-DBMS Details

Item	Purpose
Hardware	Processor: 1 GHz Pentium 4 Memory: 1 GB Disk Space: 8 GB
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Data Access Components (MDAC) Version 2.8 SQL Server 2000 Desktop Engine (MSDE) with Service Pack 3a and Security Patch 03-031 Microsoft Internet Explorer 6.0 SP1 Microsoft Data Access Components (MDAC) 2.8 or later Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.5.0_06 Adobe Acrobat Reader Version 8.0 OpenSSL 0.9.7d WinZip Version 10.0 or later SnagIt 8 SiteProtector 2.0 SP6.1
Configuration	Static IP address 10.1.13.164 DNS Server 10.1.13.254 FQDN SP-DBMS.CoactLab.com

Table 5 - AD-DNS Details

Item	Purpose
Installed software	Microsoft Windows 2000 Server SP4
Configuration	Static IP address 10.1.13.254 FQDN: AD-DNS.CoactLab.com Primary Domain Controller for CoactLab.com DNS Server for CoactLab.com with records for all systems identified in the test configuration CoactLab\Users defined for SPAdmin, SPAudit, SPView1and SPView2

Table 6 - GX4004 Details

Item	Purpose
Installed software	Proventia G 1.3 firmware
Configuration	Static IP address 10.1.13.163 FQDN: GX4004.CoactLab.com

Table 7 - Attacker Details

Item	Purpose
Hardware	Processor: 1 GHz Pentium 4 Memory: 1 GB Disk Space: 8 GB

Item	Purpose
Installed software	Windows 2000 Professional SP4 Internet Explorer 6.0 SP1 WinZip 10 ZENMAP GUI 4.68 NEWT 3 SnagIt 8 WireShark 1.0.2 Nessus Version 4.68 Paros Proxy
Configuration	Static IP address 192.168..1.11

Table 8 - Target Details

Item	Purpose
Installed software	Windows 2000 Professional SP4
Configuration	Static IP address 192.168.1.10

10.2 Functional Test Results

The repeated developer test suite includes all of the developer functional tests. Additionally, each of the Security Function and developer tested TSFI are included in the CCTL test suite. Results are found in the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Functional Test Report, Document No. E2-0110-006, dated January 21, 2010.

10.3 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

10.4 Evaluator Penetration Tests

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

a) The Open Source Vulnerabilities Database (OSVDB) (http://www.osvdb.org/)

b) Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org/)
c) Secunia (http://secunia.com/advisories/
d) SecurityFocus (http://www.securityfocus.com/bid/)
e) US-CERT United States Emergency Readiness Team (http://www.kb.cert.org/vuls/)
f) ICAT Metabase (http://icat.nist.gov/)
g) SecurityTracker (http://www.securitytracker.com/)

The vendor used the following keywords to perform their Internet vulnerability search.

a) Proventia GX
b) Proventia G
c) SiteProtector

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify additional vulnerabilities.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

10.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

11 RESULTS OF THE EVALUATION

The evaluation determined that the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module meets the requirements for EAL 2. The work unit requirements upon which the evaluation were based are work units defined in Common Evaluation Methodology for EAL2. Table 9 contains the overall verdicts for each of the evaluation assurance components. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

Table 9 - Component Verdicts

Component	Verdict
CM Capabilities (ACM_CAP.2)	Passed
Delivery (ADO_DEL.1)	Passed
Installation, generation and start-up (ADO_IGS.1)	Passed
Functional specification (ADV_FSP.1)	Passed
High-level design (ADV_HLD.1)	Passed
Representation correspondence (ADV_RCR.1)	Passed
Administrator guidance (AGD_ADM.1)	Passed
User guidance (AGD_USR.1)	Passed
Coverage (ATE_COV.1)	Passed
Functional tests (ATE_FUN.1)	Passed
Independent testing (ATE_IND.2)	Passed
Strength of TOE security functions (AVA_SOF.1)	Passed
Vulnerability analysis (AVA_VLA.1)	Passed
TOE Description (ASE_DES)	Passed
Security Environment (ASE_ENV)	Passed
ST Introduction (ASE_INT)	Passed
Security Objectives (ASE_OBJ)	Passed
PP Claims (ASE_PPC)	Passed
IT Security Requirements (ASE_REQ)	Passed
Explicitly Stated IT Security Requirements (ASE_SRE)	Passed
TOE Summary Specification (ASE_TSS)	Passed

IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Security Target, Version 1.19, dated 23 December 2009. The TOE was assessed against the EAL2 requirements as stated in the *Common Criteria for Information Technology Security Evaluation Version 2.3*.

12 VALIDATOR COMMENTS

None.

13 Security Target

IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Security Target Version 1.19, dated December 23, 2009 is incorporated here by reference.

14 List of Acronyms

CC ……Common Criteria
EAL2 ……Evaluation Assurance Level 2
IT ……..Information Technology
NIAP ……..National Information Assurance Partnership
PP ……Protection Profile
SF ……Security Function
SFP ……..Security Function Policy

SOF ……Strength of Function
ST ……..Security Target
TOE ……Target of Evaluation
TSC ……..TSF Scope of Control
TSF ……..TOE Security Functions
TSFI ……TSF Interface
TSP ……TOE Security Policy

15 Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.3, dated August 2005
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000