National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme Validation Report

IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module

Report Number: CCEVS-VR-VID10320-2011

Dated: 31 May 2011

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Kenneth Elliott
Mario Tinto

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 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 1 June 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 3.1, Revision 2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2+ Augmented with ALC_FLR.2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module.

The TOE is an automated real-time intrusion detection system designed to protect network segments from unauthorized activity. The GX6116 features two copper 10/100/1000Mbps ports for management, one for console access, and sixteen (1,000 TX/SX/LX) network ports for detection of potential security violations, which are reported to a managed central console called SiteProtector. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE is comprised of two components:

1. The Proventia GX6116 TOE component (hereafter referred to as the appliance, Sensor, Agent, or as stated) provides IDS security functionality. This component includes the Proventia GX6116 appliance hardware, the appliance resident Red Hat Operating System (OS) and the Proventia GX application software image.

2. The SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module component of the TOE (hereafter referred to as SiteProtector or as stated) is a software product that runs on a Microsoft Windows-based workstation and enables administrators to monitor and manage the Sensor components of the TOE.

The Proventia GX6116 TOE component provides the IDS functionality; it monitors a network or networks and compares incoming packet or packets against known packets and packet patterns that indicate a potential security violation. If a match occurs, the Proventia GX6116 will create an audit record. The SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation connects to the appliance via TLS session, and this workstation is only used by authorized administrators for the management of the appliance.

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.

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

- Manages and monitors Sensors and SiteProtector sub-components;
- Enables an administrator to view TOE component configuration data;
- Displays audit and system data records; and
- Monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

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:

  - Vulnerability Assessment reports
  - Attack Activity reports
  - User Audit reports
  - Content Filtering reports
  - User Permission reports

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.

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.

1 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 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 GX6116 Security Appliance Version 2.2 and SiteProtector 2.0 Service Pack 7.0 with Reporting Module	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module
Protection Profile	Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSPP).
Security Target	IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module Security Target, dated November 10, 2010.
Evaluation Technical Report	Evaluation Technical Report for the IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module , Document No. F2-1210-001, Dated 3 February 2011.
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 3.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on December 17, 2008.
Version of CEM	CEM Version 3.1 and all applicable NIAP and International Interpretations effective on December 17, 2008.
Sponsor	IBM Internet Security Systems, Inc. 6303 Barfield Road

IBM Proventia GX6116 Security Appliance Version 2.2 and SiteProtector 2.0 Service Pack 7.0 with Reporting Module	
	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** Kenneth Eggers Kenneth Elliott Mario Tinto

1.1 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

2 TOE Description

The TOE is an automated real-time intrusion detection system (IDS) designed to monitor and protect up to eight in-line Network Intrusion Protection System (NIPS) network segments or sixteen passive mode (IDS) network segments. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE is comprised of two components:

1. The Proventia GX6116 TOE component (hereafter referred to as the appliance, Sensor, Agent, or as stated) provides IDS security functionality. This component includes the Proventia GX6116 appliance hardware, the appliance resident Red Hat operating system (OS) and the Proventia GX application software image.

2. The SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module component of the TOE (hereafter referred to as SiteProtector or as stated) is a software product that runs on a Microsoft Windows-based workstation and enables administrators to monitor and manage the Sensor components of the TOE.

The Proventia GX6116 TOE component provides the IDS functionality; it monitors a network or networks and compares incoming packet or packets against known packets and packet patterns that indicate a potential security violation. If a match occurs, the Proventia GX6116 will create an audit record. The SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation connects to the appliance via TLS session, and this workstation is only used by authorized administrators for the management of the appliance.

3 Assumptions

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

Table 2 - Assumptions

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.

4 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.

Table 3 - Threats

T.SCNCFG	Improper security configuration settings 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.
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.

5 Clarification of Scope

The Proventia GX6116 and SiteProtector TOE components are described in the following sections:

Proventia GX6116

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 Version 2.0 Service Pack 7.0 with Reporting Module

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

- Manages and monitors Sensors and SiteProtector sub-components;
- Enables an administrator to view TOE component configuration data;
- Displays audit and system data records; and
- Monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

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

- 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:
    - Vulnerability Assessment reports
    - Attack Activity reports
    - User Audit reports
    - Content Filtering reports
    - User Permission reports

- 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.

- 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.

6 Security Functions

The TOE's Security Functions are:

6.1 Security Audit Function

The TOE's Audit Security Functionality combines both audit data record and system data records functionality. The Audit Security Function includes audit 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.

6.2 Identification and Authentication Function

The TOE requires operators to be successfully authenticated before any actions can be performed. User accounts must be defined in Windows (in the IT Environment). SiteProtector collects userid and password information through a GUI and passes that information to Windows to authenticate the user. If Windows indicates that the user is authenticated, SiteProtector looks up that userid in its database to determine the permissions associated with the user. If Windows indicates that the user is not authenticated, SiteProtector terminates the session.

6.3 Security Management Function

The TOE's Management Security Function provides administrator support functionality that enables a human user to manage the TOE via a GUI interface (SiteProtector Console). After installation, all management of the TOE components occurs through SiteProtector.

6.4 Traffic Analysis Function

The TOE continuously monitors network traffic and compares the packets to signatures identified in the Sensor's Policy File. Signatures identify packet and packet patterns that indicate a potential security violation to a device accessible by the Sensor's monitored network. The Sensors are shipped with a default Policy File that includes pre-defined signatures that include detection of denial of service, unauthorized access attempts, pre-attack probes, and suspicious activity.

6.5 Protection of Management Function

TLS 1.0 is used to protect communication between the Sensors and SiteProtector. The TLS implementation (via OpenSSL 1.1.2) is included in the TOE boundary. The cipher suite used for the TLS session is TLS_RSA_WITH_3DES_EDE_CBC_SHA. The Sensor initiates the connection with SiteProtector. SiteProtector responds with its RSA certificate (tested by CCTL); the Sensors authenticate the server (SiteProtector) by comparing the SiteProtector-supplied certificate to the certificate saved on the Server during installation. The pre-master secret is generated with the Sensor's random number generator and sent back to SiteProtector encrypted with the public key from the certificate, then both sides complete the key establishment phase. Subsequent data traffic is encrypted with TDES operating with 168 bit keys in CBC mode (tested by CCTL). SHA-1 (tested by CCTL) is used for message integrity checking. Session keys held in memory are zeroized (tested by CCTL) when a session ends. RSA certificates are generated by the IT Environment during installation of the TOE.

7 Architecture Information

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia GX6116) and one instance of a workstation running SiteProtector 7.0.
The following list itemizes configuration options for the TOE for the evaluated configuration:

1. Telnet server support in the Sensors is not included. Incidents and Exceptions are disabled.
2. The evaluated configuration of SiteProtector does not have Internet access to the ISS website. An automatic retrieve 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.
3. SiteProtector components are resident on one workstation (a remote SiteProtector Console is not supported in the evaluated configuration).
4. SiteProtector components and the DBMS implementation reside on one workstation.
5. Proventia GX and SiteProtector communicate via TLS.
6. After the initial configuration, management via local console is not included in the evaluated configuration.
7. SiteProtector must run on a Common Criteria evaluated version of Microsoft Windows.
8. The Console Port must not be used after the initial configuration. All subsequent configuration occurs via SiteProtector.
9. Management via Proventia Manager is not included in the evaluation, and Proventia Manager should not be used in evaluated configuration. All management of the TOE occurs through the SiteProtector application.
10. The SiteProtector Reporting Module add-on must be installed and configured.

Note that the SiteProtector runs on a dedicated workstation; applications not essential to the operation of the TOE are not installed on the workstation.

The following table identifies the minimum hardware and software requirements for components provided by the IT Environment:

Table 4 - Hardware and Software Requirements for IT Environment

Component	Minimum Requirement
Processor	1 GHz Pentium III
Memory	1 GB
Disk Space	8 GB

Component	Minimum Requirement
Operating System[1]	• Windows Server 2003 with Service Pack 1 or Service Pack 2 • Windows Server 2003 R2 • Windows Server 2003 R2 with Service Pack 2 • Windows Enterprise Server 2003 with Service Pack 1 or Service Pack 2 • Windows Enterprise Server 2003 R2 • Windows Enterprise Server 2003 R2 with Service Pack 2 • Windows 2000 Server with Service Pack 4 or later (only supported for upgrades to SiteProtector 2.0, Service Pack 7.0) • Windows 2000 Advanced Server with Service Pack 4 or later (only supported for upgrades to SiteProtector 2.0, Service Pack 7.0)
Additional Software	• Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.6.0_03 (required to run the SiteProtector Console GUI) • Internet Explorer 6.0 or 7.0 for Windows Server 2003 and Windows Enterprise Server 2003 users • Internet Explorer 6.0 with Service Pack 1 or later for all other users • Adobe Acrobat Reader 6.0 or later • SQL Server 2000 with Service Pack 4 (only supported for upgrades to SiteProtector 2.0, Service Pack 7.0) OR SQL Server 2005, Standard and Enterprise editions, with Service Pack 2 or earlier
Network Configuration	Static IP address
Disk Partition Formats	NTFS

8 Product Delivery

The GX6116 component is delivered to the customer's location either by FedEx or UPS. Signature confirmation of delivery is required.
The following steps outline the internal process of shipping a GX6116 product to a customer:

1. Affix ISS sticker to the Proventia GX product associated with the part number (PN) and serial number (SN) of the product being shipped.
2. Package all products shipped to customer in ISS imprinted boxes.
   Regardless of the shipping carrier chosen to ship the GX6116, the appliance and supporting materials are packaged in boxes that are imprinted with the ISS trademarked logo. Imprinted boxes with the ISS trademarked logo are used so customers have confidence that either the GX6116 product was packaged and shipped by an ISS distribution center.
3. Affix an ISS sticker to the shipping box associated with the PN and SN of the product being shipped in the shipping box.
   A sticker is applied to one of the sides of the shipping box that contains the Proventia GX product. The sticker is imprinted with the ISS trademarked logo. The sticker contains two fields. The first field is a product number (PN). The PN imprinted on the label is both in human readable characters and as a bar scan. The PN imprinted on the sticker is also included in the e-mail sent to the customer who orders the product. The PN allows the end customer to determine if they have received a GX6116. The second field is a serial number (SN). The SN is imprinted on the sticker in both human readable characters and as a bar code. The SN imprinted on the sticker is also included in the e-mail sent to the customer who orders the product.
   The end customer may determine if they have received a GX6116 product by looking at the first character of the PN.
4. Place the GX6116 in the shipping box such that the PN and SN sticker on the product corresponds to the PN and SN sticker applied to the shipping box.
5. Seal all shipping boxes with clear packaging tape and staples.
   The top, bottoms, and all corners of the shipping box except one are sealed using clear packaging tape. One corner side seam of the box is stapled shut.
6. Transfer package to third party shipping company.
7. Send a product shipment confirmation e-mail to the customer's e-mail address.
   After shipment, the customer is sent an e-mail by ISS which itemizes the product(s) purchased. The FedEx or UPS shipment tracking numbers are included. The e-mail contains the full SN and PN of the products that they have ordered.
   The full PN and SN are included in the e-mail sent to the customer so that this information can be used to check that the PN and SN in the e-mail match the PN and SN on the sticker applied to the packing box(es) as well as the sticker(s) on the appliance(s) to determine that they have received the proper product(s).
   The customer should note that it is possible that the sticker applied to the appliance with the PN and SN may be difficult to locate. The customer should look at the inside ridges back by the power cord if the sticker is not in plain view on any of the sides of the delivered appliance.
   If the customer finds a discrepancy with any PN or SN in the shipment, ISS must be contacted immediately.

8.1 Delivery of Downloadable Components

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 customer password must be changed. The ISS Customer Portal is protected by 128-bit SSL encryption. The certificate that is being used to help implement the 128-bit SSL can be verified as an ISS certificate through the security features of the web browser used to connect to the ISS Customer Portal. For example, using 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. The user must keep their user ID and password, to whatever they changed it to, so that they can download the software they desire.
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.

8.2 SiteProtector Download Procedure

In order to comply with the TOE configuration, the only following should be used: . If the pre-loaded software version differs from the version required for the TOE configuration, the administrator should load the correct version:

1. Log in to the ISS support site at https://webapp.iss.net/myiss/login.jsp
2. Select **Downloads** from the menu
3. Choose **NIAP EAL2PP - Prov. GX6116 ver.2.2, Site Protector 2.0 Service Pack 7.0** from the **Select a Product** dropdown menu and then select **Go**
4. Select **NIAP - GX6116 version 2.2** from the **Version** dropdown menu then select **Go**
5. Select **Other Updates** and select **Continue** next to the bundle listing for the software
6. Accept the Export Agreement and the End User License and select **Submit**
7. Download **DeploymentManager-Setup.exe** (SiteProtector Installation), **Proventia_Network_IPS_FW2.2_Readme.htm**, and **GX6116Bootsrv.2.2_2008.0523_14.17.00.iso** (the GX6116 software)

8.3 Verifying Integrity of Downloaded Components

Once the customer has finished downloading the components they should verify the MD5 or SHA-1 hashes to ensure integrity of the components. The hash values are presented for convenience on the DLC.
The customer should use an MD5 or SHA-1 hash utility on the system they have downloaded the components to in order to compute the hash values of the downloaded software components. Computing the hash value on the downloaded software component serves two purposes. It determines if the integrity of the downloaded software component is compromised

and it also allows the customer to identify that they have the proper software that was evaluated. SHA-1 and MD5 hash values should then be compared to the DLC.
If the customer finds a problem when verifying the hashes, they should be instructed to contact ISS immediately.

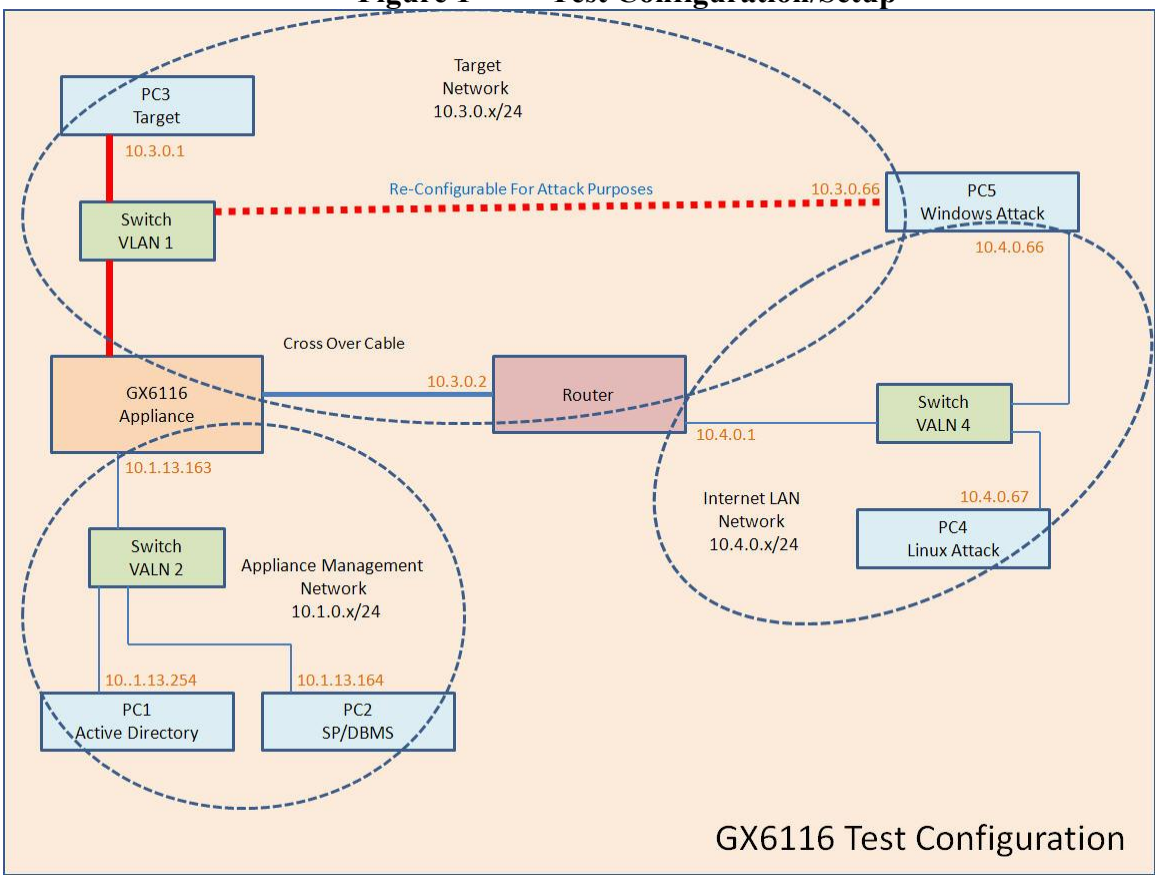
9 IT Product Testing

Testing was completed on May 25, 2010 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

9.1 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 5 - Test Configuration Overview

Component	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 GX6116 maps to address 10.1.13.163. The name SP-DBMS maps to the address 10.1.13.164.
GX6116	The Proventia Intrusion Detection System. Port 10.1.13.163 is the management port.
Windows Attack PC	This is the PC that will be used to attack the Target PC. The

Component	Purpose
	Windows Attack PC will have two network cards. The two network cards will permit communication on the Target Network and the Internet LAN Network.
Linux Attack PC	This is the PC that will be used to attack the Target PC.
Target PC	This is the PC that will be the receipitant of the attacks.
Switch	NetGear GS716T - The switch is configured for three separate VLANs.
Router	LinkSys RVS4000 – The router will connect the network to the simulated Internet. IP Address – Target Network 10.3.0.2 IP Address – Internet LAN Network 10.4.0.1

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

Table 6 - 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 1.6.020 Adobe Acrobat Reader Version 8.0 WinZip Version 10.0 or later SnagIt 8 Version 2.0 Service Pack 7.0 with Reporting Module Outlook Express Microsoft Visual Studio 2005
Configuration	Static IP address 10.1.13.164 DNS Server 10.1.13.254 FQDN SP-DBMS.CoactLab.com

Table 7 - 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 8 - GX6116 Details

Item	Purpose
Installed software	Proventia GX Version 2.2
Configuration	Static IP address 10.1.13.163 FQDN: GX6116.CoactLab.com

Table 9 - Windows Attack PC Details

Item	Purpose
Hardware	Processor: 1 GHz Pentium 4 Memory: 1 GB Disk Space: 8 GB
Installed software	Windows 2000 Professional SP4 Internet Explorer 6.0 SP1 WinZip 10 ZENMAP GUI 4.68 NMAP 4.68 NEWT 3 SnagIt 8 WireShark 1.0.2 Nessus Version 3.0.6.1 Paros Proxy 3.2.13
Configuration	Static IP address 10.3.0.66 Static IP Address 10.4.0.66

Table 10 - Linux Attack PC Details

Item	Purpose
Installed software	Linux RHE 3.0 Metasploit 3.3
Configuration	Static IP address 10.4.0.67

Table 11 - Target PC Details

Item	Purpose
Installed software	Windows 2000 Professional SP4 WireShark 1.0.8
Configuration	Static IP address 10.3.0.1

9.2 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 Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module Test Report, dated May 25, 2010

9.3 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.

9.4 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 any 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.

9.5 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.

10. Results of the Evaluation

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the product for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module Test Report, dated May 25, 2010.

The evaluation determined that the product meets the requirements for EAL 2+ Augmented with ALC_FLR.2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

11. Validator Comments

The CCTL testing for the signatures covered less than 1% of the total signatures recognized by the product. While the vendor claims to have comprehensive test suites that cover all of the signatures recognized by the product, these were not made available to the CCTL during the evaluation process.

12. Security Target

IBM Internet Security Systems GX6116 Security Appliance Version 2.2 and SiteProtector Version 2.0 Service Pack 7.0 with Reporting Module Security Target, dated November 3, 2009.

13. 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

14. 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 3.1, Revision 2, dated September 2007
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 3.1, Revision 2, dated September 2007
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 3.1, Revision 2, dated September 2007
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 3.1, Revision 2, dated September 2007
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 3.1, Revision 2, dated September 2007
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000