National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61

Report Number: CCEVS-VR-VID10275-2008
Dated: 10 December 2008
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

Mike Allen (Lead Validator)
Jandria Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

COACT Café Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 at Evaluation Assurance Level 2(EAL2). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target and supplemental installation guidance.

The evaluation of the IBM Proventia Network Enterprise Scanner 1.3 was performed by COACT Café Laboratory Common Criteria Testing Laboratory in the United States and was completed on 28 October 2008.

The information in this report is largely derived from the Security Target (ST), the Evaluation Technical Report (ETR) and associated test report. The ST was written by COACT for IBM. The ETR and test report used in developing this validation report were written by COACT. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005. The product, when configured as specified in the supplemental installation guide and user guide, satisfies all of the security functional requirements stated in the IBM Proventia Network Enterprise Scanner 1.3 Security Target. The evaluation team determined the product to be Part 2 and Part 3 conformant, and meets the assurance requirements of EAL 2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61. The TOE is a vulnerability assessment system designed to scan specified targets for vulnerabilities and includes a management system that provides management and monitoring functionality.

The TOE consists of two main components:

A) The Enterprise Scanner that scans any Internet Protocol version 4 addressable device connected to the scanning network (operational network) and discovers assets and determines the assets' services and known vulnerabilities. Vulnerabilities are known weaknesses in a system allowing an attacker to violate

the integrity, confidentiality, access control, availability, consistency or audit mechanism of the system or the data and applications it hosts. The Enterprise Scanner identifies vulnerabilities such as:

1) improperly configured desktops, servers, Web servers, routers or firewalls;
2) hosts running unauthorized services;
3) weak or no password protection; and
4) unpatched or outdated versions of operating systems.

B) SiteProtector with Reporting Module is used as the central controlling point for Enterprise Scanners deployed on the network. The Reporting Module is embedded within SiteProtector, but its functionality must be enabled via a separate license. The SiteProtector performs the following functionality:

1) Manages and monitors all associated Enterprise Scanners;
2) Manages and monitors SiteProtector and
3) displays audit data and system data events.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence reviewed.

During this evaluation, the Validators monitored the activities of the COACT evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validators conclude that the COACT findings are accurate, the conclusions justified, and the conformance claims correct.

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 product evaluations. Under this program, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring 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's 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 Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61
Protection Profile	None
Security Target	*IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 Security Target*, Version 1.6, 25 November 2008
Dates of evaluation	January 11, 2007 through October 28, 2008
Evaluation Technical Report	*Evaluation Technical Report for IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61*, Document No. F2-1108-001, Dated 16 December 2008
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 11, 2006
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 11, 2006
Sponsor	IBM Internet Security Systems, Inc., 6303 Barfield Rd., Atlanta, GA 30328
Developer	IBM Internet Security Systems, Inc., 6303 Barfield Rd., Atlanta, GA 30328
Common Criteria Testing Lab	COACT Café Laboratory, Inc., Columbia, MD
Evaluators	Bob Roland, Greg Beaver, Pascal Patin and Brian Pleffner of COACT
Validation Team	Jandria Alexander and Mike Allen of The Aerospace Corporation

2.1 Applicable Interpretations

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

2.1.1 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

2.1.2 International Interpretations

None

3 Organizational Security Policy

The TOE is a vulnerability management system designed to scan specified targets for vulnerabilities and includes a management system that provides management and monitoring functionality.

Enterprise Scanner consists of two main components:

A) The Enterprise Scanner scans any Internet Protocol version 4 addressable device connected to the scanning network (operational network) and discovers assets and determines the assets' services and known vulnerabilities. Vulnerabilities are known weaknesses in a system allowing an attacker to violate the integrity, confidentiality, access control, availability, consistency or audit mechanism of the system or the data and applications it hosts. The Enterprise Scanner identifies vulnerabilities such as:
   1) improperly configured desktops, servers, Web servers, routers or firewalls;
   2) hosts running unauthorized services;
   3) weak or no password protection; and
   4) unpatched or outdated versions of operating systems.

B) SiteProtector with Reporting Module is used as the central controlling point for Enterprise Scanners deployed on the network. The Reporting Module is embedded within SiteProtector, but its functionality must be enabled via a separate license. The SiteProtector performs the following functionality:
   1) Manages and monitors Enterprise Scanners;
   2) Manages and monitors SiteProtector and
   3) displays audit data and system data events.

The Following are the Security Policies that the TOE enforces.

3.1 Scanning

The TOE performs scanning of designated systems to detect known vulnerabilities on those systems. The TOE is designed to automate the process of cyclically discovering and assessing assets (background scanning), while accommodating ad hoc scans as well. Background scans are well suited to minimize impact on operational systems since their execution can be tailored for times when operational usage of the systems and networks is low.
Scanning is broken into two categories: discovery and assessment. Discovery scans are initially used to discover assets on the network (so that they may subsequently be assessed). On-going discovery scans highlight changes to the assets and detect unauthorized systems on the network. Assessment scans perform in-depth searches for vulnerabilities on previously discovered systems.

Results of the scans are stored in the DBMS (IT Environment) located on the same system as the SiteProtector software.

3.2 System Data Generation

The TOE's System Data Generation Security Function provides functionality to generate and store system data related to scans performed by the TOE. The TOE's system data includes three types of system data: scan events; analysis views; and system data reports.
The first two types of system data are saved via the SiteProtector database via the DBMS supplied by the IT Environment, while the system data reports are saved on disk using the OS file I/O functionality (IT Environment).

3.3 System Data Viewing

The TOE's System Data Viewing Security Function provides administrator support functionality that enables authorized administrators to view system data records (e.g., detected vulnerabilities) in human readable format via the SiteProtector Console. Data included in system data records and available for viewing are the specific vulnerability, associated severity, timestamp, IP name and address of the asset on which the vulnerability was detected, scanner from which the scan was performed, and the service protocol (if applicable) associated with the vulnerability.

The TOE retrieves system data from the SiteProtector database via the DBMS or from a file on disk via the OS file I/O functionality supplied by the IT Environment.

3.4 Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the roles (and therefore permissions) are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE which prevents tampering or interference with the TOE for those users that are within the TSC.

Since the SiteProtector component of the TOE consists of a set of applications, the TOE cannot provide complete self-protection for itself. The TOE depends on the operating system and hardware (IT Environment) on the SiteProtector platform to protect the TOE from interference or bypass from users or processes outside the TSC.

TLS is used to protect communication between the TOE components. The TLS functionality is provided by the TOE on the Enterprise Scanners and by the IT Environment on the SiteProtector platform.

3.5 Management

Management of the TOE may be performed via SiteProtector Console on the SiteProtector platform. All management of the TOE components is performed via SiteProtector.
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.

3.6 Audit

The TOE's Audit Data Generation and Viewing Security Function provides administrator support functionality that records the administrator commands and enables authorized administrators to view audit data records in human readable format via the SiteProtector Console.

The TOE stores audit records into the SiteProtector database via the DBMS supplied by the IT Environment. The audit records are retrieved from the database and saved as a report via the OS file system (IT Environment) for audit viewing.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

4.1 Environmental Assumptions

Following are the assumptions identified in the Security Target:

1) The TOE has access to all the IT System data it needs to perform its functions.
2) The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
3) The TOE is appropriately scalable to the IT System the TOE monitors.
4) The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
5) The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
6) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
7) The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation with respect to their roles, permissions and ownership.
8) The TOE can only be accessed by authorized users.

4.2 Organizational Security Policies

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

1) Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2) Analytical processes and information to derive conclusions about vulnerabilities must be applied to incoming Scanner network data and appropriate notification provided.
3) The TOE shall only be managed by authorized users.
4) All data collected and produced by the TOE shall only be used for authorized purposes.
5) Users of the TOE shall be accountable for their actions within the TOE.
6) Data collected and produced by the TOE shall be protected from modification.
7) The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4.3 Threats Countered by the TOE

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

1) An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
2) An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
3) An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
4) An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
5) An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
6) An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
7) An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
8) Unauthorized attempts to access TOE data or security functions may go undetected.
9) Improper security configuration settings may exist in the IT System the TOE monitors.
10) 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.
11) Vulnerabilities may exist in the IT System the TOE monitors.
12) The TOE may fail to recognize vulnerabilities based on the network data received from each data source.
13) The TOE may fail to identify vulnerabilities based on association of the network data received from all data sources.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This section covers some of the more important limitations and clarifications of this evaluation. Note that to use the product in the evaluated configuration the following restrictions apply:

1) Network Time Protocol support must be disabled. The Enterprise Scanner appliance generates its own time stamps and the operating system on which the SiteProtector resides generates the timestamps for the SiteProtector.
2) SSH functionality for connecting to the Scanners must be disabled.
3) The Authentication Level configured on all Enterprise Scanners must be "first time trust."
4) Automatic retrieve of X-Press updates (XPUs) must be disabled.

5) SiteProtector components are resident on one workstation and a remote SiteProtector Console is not supported in the evaluated configuration.

6) SSL/TLS must be used for the communication between Scanners and SiteProtector. The IT Environment supplies the SSL/TLS on the SiteProtector Host. SSL/TLS on the Scanner is supplied by the TOE.

The following functionality included in the TOE boundary was not included as part of the evaluation:

1) Active Directory Import Data - SiteProtector provides authorized users the ability to import assets from Active Directory. All assets must be discovered or created by a SiteProtector administrator.
2) Tickets - The SiteProtector ticketing functionality enables an administrator to generate a ticket that reports a known vulnerability discovered by the Scanners. The ST does not claim this functionality as security relevant.
3) Web Access - SiteProtector provides a read-only Web-based interface. This interface is not claimed as a monitoring interface in the ST and must be disabled at TOE installation.
4) X-Press Update Server - The X-Press Update Server is a means to update the TOE software. This functionality must not be used since it would change the TOE from the evaluated version.
5) Proventia Manager - The Proventia Manager is a Network Enterprise Scanner resident web-based interface used for Enterprise Scanner installation configuration and start-up. This interface is not used for an operational TOE and all management and monitoring functionality is performed via the SiteProtector Console.

5 Architectural Information

The evaluated configuration of the TOE consists of:

- One instance of SiteProtector with Reporting Module enabled on a Windows computer dedicated to that purpose. The DBMS, supplied by the IT Environment, is hosted on the same platform.

- One or more instances of Enterprise Scanners.

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 (The SQL Server version will be 8.00.818 after you apply this patch.) or SQL Server 2000 with Service Pack 4
Additional Software	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 0.9.7c
Network Configuration	Static IP address
Disk Partition Formats	NTFS

The Enterprise Scanners of the system are connected to the SiteProtector Host over the monitored network. All communications between the Scanners and the Host employs TLS encryption and certificates.

6 Documentation

The TOE consists of downloaded software and documentation as well as one or more appliances. Once a purchase of the TOE has been processed through the IBM order processing system, an account on the MyISS web site is created for the user (if it doesn't already exist) and the user is authorized to download Proventia Network Enterprise Scanner software from the web site. The MyISS account information is communicated to the user via email. At the same time, shipment of any purchased scanners is scheduled.

Documentation may be downloaded from the web site at any time. Sales personnel work with the user to ensure the appropriate documentation is obtained. This includes an installation document specific to the evaluated version of the TOE ("IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 [Version 2.684/1/24/008] Installation Supplement Version 1.1, November 25, 2008"). This document informs the user which software files need to be downloaded.

Special download files have been provided on the MyISS download center for the EAL2 evaluated version. The user may select either the ES750_NIAP.zip file or the ES1500_NIAP.zip file (or both) to download. Both files include the same SiteProtector files, which is all the software required to install the evaluated version of SiteProtector from scratch. The download files differ only in the software packages provided for the scanners.

IBM utilizes third-party vendors for order fulfillment of the appliances. These vendors assemble the components for the appliances, install the most recent version of released software, and ship the systems per instructions from IBM. Note that IBM cannot guarantee that the version of software installed on the appliances is the evaluated version. Therefore, the installation instructions specific to the evaluated version direct the user to install the evaluated version from the download file onto each appliance.

Licenses required to operate SiteProtector and the scanners are distributed to the user via email or are obtained online from the MyISS web site.
.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

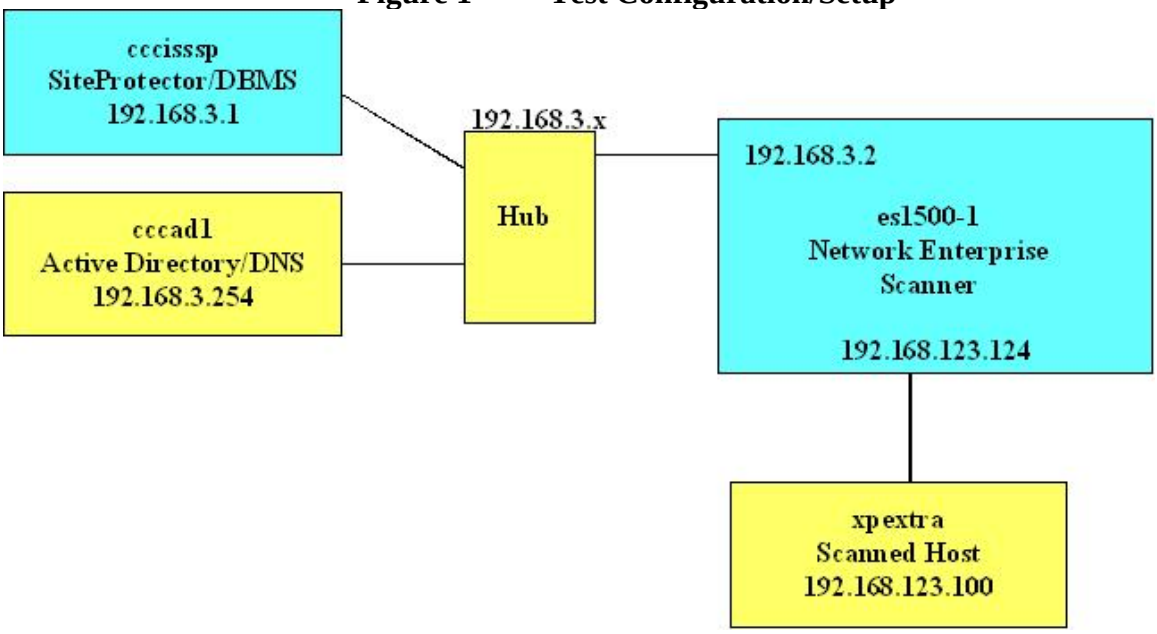
7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Functional Testing 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
cccisssp	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 cccad1.
cccad1	In DNS, records should be configured for each of the systems shown in the figure above. The name es1500-1 maps to address 192.168.3, while the name es1500-1-scan1 maps to address 192.168.4.1.
xpextra	This is a PC with Windows XP Professional SP2 installed; no other

System	Purpose
	Microsoft patches or updates are installed. If any firewall software is installed, it must be disabled. The system services should not be configured to allow remote connections. The domain should be configured for DOMAIN3, although no Active Directory servers are reachable. Only the Administrator account is required on this system.
es1500-1	This is a single ES1500 Network Enterprise Scanner.

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

Table 4 - cccisssp Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft SQL Server 2000 SP4 Microsoft Internet Explorer 6.0 SP1 Sun Java 2 Runtime Environment (JRE), Standard Edition, Version 1.5.0_09 Adobe Reader Version 8.0 WinZip Version 10.0 or later SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008)
Configuration	Static IP address 192.168.3.1/24 DNS Server 192.168.3.254 FQDN cccisssp.domain3.cccllc.com

Table 5 - cccad1 Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4
Configuration	Static IP address 192.168.3.254/24 FQDN cccad1.domain3.cccllc.com Primary Domain Controller for domain3.cccllc.com DNS Server for domain3.cccllc.com with records for all systems identified in the test configuration DOMAIN3\Users defined for SPAdmin, SPAudit, SPView1and SPView2

Table 6 - xpextra Details

System	Installed Components
Installed software	Microsoft Windows XP Professional SP2
Configuration	Static IP address 192.168.123.100/24 FQDN xpextra.domain3.cccllc.com

Table 7 - es1500-1 Details

System	Installed Components
Installed software	Network Enterprise Scanner 1.3 with XPU 1.28
Configuration	FQDN es1500-1.domain3.cccllc.com Static IP address 192.168.3.2/24 on the MANAGEMENT port Static IP address 192.168.123.124/24 on the SCAN port DNS Server 192.168.3.254 DNS search path domain3.cccllc.com Default gateway 192.168.3.1 Alternate Update Server cccisssp.domain3.cccllc.com port 3994 SiteProtector cccisssp.domain3.cccllc.com SiteProtector group EnterpriseScanner Agent Manager cccisssp.domain3.cccllc.com port 3995

7.3 Functional Testing Results

The repeated developer test suite includes all of the five 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 ISS Enterprise Scanner Functional Test Report, Document No. F2-1108-002, dated 16 December 2008.

7.4 Evaluation Team Independent Testing

The tests chosen for independent testing allowed the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests was 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 allowed for a finer level of granularity of testing compared to the developer's testing, or provided additional testing of functions that were not exhaustively tested by the developer. The tests allowed specific functions and functionality to be tested. The tests reflected 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.

7.5 Vulnerability Testing

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 included:

A) http://xforce.iss.net/

B) http://cve.mitre.org

C) http://www.securityfocus.com/

D) http://www.ciac.org/

E) http://www.cert.org/

F) http://securitytracker.com

G) http://www.osvdb.org

H) http://www.infobyte.com.ar/

I) http://www.kb.cert.org/vuls/

J) https://rhn.redhat.com/

K) http://www.us-cert.gov/cas/techalerts/TA04-078A.html

L) http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-0079

M) http://www.openssl.org/news/secadv_20040317.txt

N) http://secunia.com/advisories/13827/

O) http://www.microsoft.com/technet/security/bulletin/MS02-040.mspx

P) https://www.openssl.org/news/vulnerabilities.html

The vulnerability search criteria consisted of the following keywords:

A) Adobe 6.0

B) ISS

C) Proventia Network Enterprise Scanner

D) Proventia

E) Network Enterprise Scanner

F) SiteProtector

G) JRE 1.5.0_06

H) SQL Server 2000

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 rationale 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 existed 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 rationale provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

7.6 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.

.

8 Evaluated Configuration

The evaluated configuration requires the SiteProtector software package running on a windows platform and one or more Enterprise Scanners. These devices are connected via a secure communication channel using TLS encryption and certificates. For specific configuration settings required in the evaluated configuration see "IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 [Version 2.684/1/24/008] Installation Supplement Version 1.1, November 25, 2008."

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on January 11, 2006. The evaluation confirmed that the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL 2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008). The product was evaluated and tested against the claims presented in the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) Security Target, Version 1.6, November 25, 2008.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) product meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

Administrators are warned to follow the guidance in the supplemental user guide ("IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 [Version 2.684/1/24/008] Installation Supplement Version 1.1, November 25, 2008") to ensure the product is in the evaluated configuration by applying the following restrictions:

1) Network Time Protocol support must be disabled. The Enterprise Scanner appliance generates its own time stamps and the operating system on which the SiteProtector resides generates the timestamps for the SiteProtector.
2) SSH functionality for connecting to the Scanners must be disabled.
3) The Authentication Level configured on all Enterprise Scanners must be "first time trust."
4) Automatic retrieve of X-Press updates (XPUs) must be disabled.
5) SiteProtector components are resident on one workstation and a remote SiteProtector Console is not supported in the evaluated configuration.
6) SSL/TLS must be used for the communication between Scanners and SiteProtector. The IT Environment supplies the SSL/TLS on the SiteProtector Host. SSL/TLS on the Scanner is supplied by the TOE.

11 Security Target

The Security Target is identified as IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) Security Target Version 1.6, November 25, 2008. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

12 Glossary

The following definitions are used throughout this document:

CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
HTTP	HyperText Transfer Protocol
I/O	Input/Output
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement(s)
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] Evaluation Technical Report for IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61.

[6] IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 Security Target, Version 1.6, November 25, 2008.

[7] IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 Vulnerability Analysis, Version 1.1, August 11, 2008.

[8] Functional Test Report for IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61, December 16, 2008.

[9] Penetration Test Report for IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61, December 16, 2008.

[10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.