National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, RealSecure Network Sensor 7.0, and SiteProtector 2.0 Service Pack 4

Report Number: CCEVS-VR-06-0029
Version 1.0
16 May 2006

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Maureen Cheheyl
The MITRE Corporation
Bedford, Massachusetts

Jandria Alexander, Senior Validator
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Lab
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0-2003.24 (for Linux), RealSecure Network Sensor Version 7.0-2002.155 (for Windows), and SiteProtector 2.0 Service Pack 4 was performed by the COACT CAFÉ Lab in the United States. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2, and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP-approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation, Version 2.2, for conformance to the Common Criteria for IT Security Evaluation, Version 2.2. This Validation Report applies only to the specific version of the TOE as evaluated. 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 adduced. This Validation Report is not an endorsement of the ISS Proventia product by any agency of the US Government and no warranty of the product is either expressed or implied.

The COACT evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The RealSecure Network Sensor and Site Protector both are sold as software products and run on standard computer platforms. The sensors Proventia A and Proventia G, in contrast, are sold as appliances, hardware platforms that include the operating system and ISS software. In both cases, the platform, including hardware and OS, is not part of the TOE but is considered part of the environment.

Two components of the TOE 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

The Proventia G system is configured as an IDS system at system installation.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 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 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.

2.1 Evaluation Details

Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0-2003.24 (for Linux), RealSecure Network Sensor Version 7.0-2002.155 (for Windows), and SiteProtector 2.0 Service Pack 4
Protection Profile	None
Security Target	ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Security Target, Version 2.25, 11 April 2006
Evaluation Technical Report	Evaluation Technical Report for ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, RealSecure Network Sensor 7.0, and SiteProtector 2.0 Service Pack 4 Target of Evaluation, May 16, 2006
CC	*Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004
Interpretations	All applicable NIAP and International Interpretations effective on 30 November 2005.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004
Evaluation Class	EAL 2

Sponsor & Developer	Internet Security Systems, Atlanta, Georgia
CCTL	COACT CAFÉ Lab, Columbia, Maryland
Evaluation Personnel	Dawn Adams Ching Lee Robert West
Validation Team	Maureen Cheheyl The MITRE Corporation Bedford, Massachusetts Jandria Alexander, Senior Validator The Aerospace Corporation Columbia, Maryland

2.2 TOE Components

The ISS Proventia TOE is an automated real-time intrusion detection system (IDS) designed to protect 10/100/1000 Mbps copper and 1000 Mbps SX network segments by analysing and responding to activity across the network. The TOE is a software-only TOE made up of these components:

A) Proventia A Version 7.0-2003.167 application software

B) Proventia G Version 8.0-2004.219 application software

C) RealSecure Network Sensor Version 7.0

D) SiteProtector 2.0 Service Pack 4

E) Sensor-resident signature files, current active Policy File, commands, and audit records (before transfer to the SiteProtector)

F) SiteProtector-resident default Policy Files and audit data

G) Patches RSNetSnsr70_Linux_XXX_ST_4_3, RSNetSnsr70_MU_20_19, RSNetSnsr70_MU_24_2, RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11.

Three of the TOE components, Proventia A, Proventia G, and RealSecure Network Sensor, referred to as Sensors, provide the IDS functionality; each monitors a network or networks and compares incoming packets against known packet patterns that indicate a potential security violation. If a match occurs, the Sensor will create an audit record. The fourth component of the TOE, SiteProtector, provides management, monitoring, and configuration functions to users.

The RealSecure Network Sensor and Site Protector both are sold as software products and run on standard computer platforms. The sensors Proventia A and Proventia G, in contrast, are sold as appliances, hardware platforms that include the operating system and

ISS software. For all four products, the platform, including hardware and OS, is not part of the TOE but is considered part of the environment.

Two components in the TOE 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

2.3 IT Environment

The IT environment requires the following:

A) Appliance hardware for the Proventia A Version 7.0-2003.167 or Proventia G Version 8.0-2004.219.

B) Workstation hardware for each RealSecure Network Sensor Version 7.0 or SiteProtector subcomponent.

C) Proventia A Version 7.0-2003.167 and Proventia G Version 8.0-2004.219 appliance operating system, Red Hat 8.0.

D) RealSecure Network Sensor Version 7.0 operating system (Microsoft Windows 2000 or Red Hat Linux 7.3).

E) SiteProtector 2.0 Service Pack 4 workstation operating system (Microsoft Windows 2000 Server).

F) Database Management System (Microsoft SQL Server 2000).

G) SiteProtector Console workstation's Web browser (Microsoft Internet Explorer 5.0 or higher) and Java RTE.

H) Network software and hardware on each TOE component that provides a connection to the secure management network for communication between the Sensors and the SiteProtector.

I) Network software and hardware that provides a connection to the sensed, monitored network for Proventia A appliance(s), Proventia G appliance(s) and/or RealSecure Network Sensor host(s).

J) An IT Environment-supplied timer that is used by the components of SiteProtector.

K) Patches RSNetSnsr70_Linux_2.4.18-10smp_ST_4_1, RSNetSnsr70_Linux_2.4.18-10smp_ST_4_2, SPIA_POLICY_20050208, SPNS_POLICY_20050208, DB_SR_1_1_20040915, DB_SR_1_2_20041020, DB_SR_1_3_20041022, DB_XPU_1_44_20040628, DB_XPU_1_45_20040719, DB_XPU_1_46_20040812, DB_XPU_1_47_20040915, DB_XPU_1_48_20041014, DB_XPU_1_49_20041111 DB_XPU_1_50_20041221, and DB_XPU_1_51_20050119

3 Security Policy

3.1 Sensors

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 (audit record). This audit data is sent to the TOE's SiteProtector, which enables a user to view and analyze the audit information.

Signatures are configured on the Sensors by Policy Files. Policy Files identify a subset 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 a user to disable or enable signatures in a Sensor's current Policy File or select and apply a new Policy File selected from the set of Policy Files.

3.2 SiteProtector

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 records

D) Initiates and maintains the network connection between SiteProtector and the Sensors it is configured to monitor

SiteProtector relies on its host OS in performing identification and authentication (I&A) of users. For a user of the TOE to properly gain access to SiteProtector the user roles on the host OS and the roles maintained by SiteProtector need to be insync with each other. SiteProtector User Groups (User Roles) are automatically created during the installation of SiteProtector. The installation procedures create the three roles supported by SiteProtector: Operator, Analyst and Administrator. The IT Environment Administrator is responsible for defining user names, passwords and associating the User Groups to the user name/password pairs to enable successful SiteProtector login.

SiteProtector relies on the host OS to verify the user name and password entered into the SiteProtector GUI login screen. The login screen is invoked by users and requires users to identify and authenticate themselves. If the user name/password pair is not successfully verified by the host OS, the SiteProtector login screen refreshes by clearing the entered user name and password and not allowing any further actions. If the user name and password are successfully verified, SiteProtector obtains from the host OS the User Group associated with the user name/password pair. If the User Group (User Role) is a non-supported SiteProtector User Role, SiteProtector will not allow any further actions. If the User Role is a supported SiteProtector role, SiteProtector uses this User Role to determine the privilege level of the user. Users assigned the User Role of Analyst or

Administrator are considered privileged users and have access to all GUIs. Users assigned the User Role of Operator have limited privileges. Operators can view TSF Data but cannot modify TSF Data or invoke any functions that affect the TSF.

4 Assumptions

4.1 IT Environment Assumptions

A.DBASE The IT environment's DBMS implementation will be properly configured, reliable, protected, and securely administered.

A.DEDICATE The TOE components will be installed on dedicated systems. A dedicated system is a computer system that contains no other software other than the TOE component(s), the ISS network driver support software and the required supporting third party software, as defined by the evaluated configuration.

A.I&A The operating systems of the computers the TOE is installed on require identification and authentication of users.

A.NETWORK The IT environment will provide a secure network dedicated to communication between SiteProtector and the Sensors.

4.2 Personnel Assumptions

A.INSTALL The authorised administrator will install the hardware, operating systems and software required for the TOE in a manner that maintains IT security with the proper network and configured according to ISS installation guides.

A.NOEVIL The authorised administrators of the TOE will not be careless, wilfully negligent, or hostile.

4.3 Physical Assumptions

A ENVIRON The hardware running the TOE is located in an environment that provides controlled physical access. Only authorized personnel have physical access to the hardware running the TOE. Additionally, the environment provides reliable power and air conditioning controls to insure reliable operation of the hardware.

5 Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, or

RealSecure Network Sensor Version 7.0 TOE component) and one instance of SiteProtector 2.0 Service Pack 4. In addition, the IT environment requires the items listed in Section 2 above.

The following list itemizes configuration requirements for the TOE for the evaluated configuration along with TOE IT Environment resources and configuration used by the TOE when the TOE is in the evaluated configuration:

1. All Sensors are configured (by default) with the Response Field in Policy Files set to LOGDB and Display. All Sensors are configured (by default) with the options RSKill, Log Evidence, and View session disabled in the Response Field in the Policy Files.

2. Telnet server support in the Sensors is disabled by default. Incidents and Exceptions is disabled by selection of ‘Show Uncategorized’ in the Incidents/Exception pane because the evaluated configuration of the TOE does not support Incidents and Exceptions.

3. 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 automatic retrieve and store the updates on the SiteProtector system.

4. Intrusion Prevention functionality provided by Proventia G Version 8.0-2004.219 is not included in the evaluated configuration.

5. SiteProtector components reside on a single workstation (a remote SiteProtector Console is not supported in the evaluated configuration). The SiteProtector host requires Windows 2000 Server OS, Microsoft SQL Server 2000 for the DBMS, and both Microsoft Internet Explorer and Java RTE to support the SiteProtector Console GUI interface.

6. The IT Environment-supplied Secure Sockets Layer (SSL) is used for the communication between the Sensors and SiteProtector.

7. SSL or encrypted SQL is used for the communication between SiteProtector and the DBMS.

6 Architectural Description of the TOE

The ISS Proventia TOE is an automated real-time intrusion detection system (IDS) designed to protect 10/100/1000 Mbps copper and 1000 Mbps SX network segments by analysing and responding to activity across the network. The TOE is made up of four components:

A) Proventia A Version 7.0-2003.167 with patch RSNetSnsr70_MU_24_2

B) Proventia G Version 8.0-2004.219 with patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_Linux_XXX_ST_4_3

C) RealSecure Network Sensor Version 7.0 with patches, RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19

D) SiteProtector 2.0 Service Pack 4 with patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_1

Three of the TOE components, Proventia A, Proventia G, and RealSecure Network Sensor, referred to as Sensors, provide the IDS functionality; each monitors a network or networks and compares incoming packets against known packet patterns that indicate a potential security violation. If a match occurs, the Sensor will create an audit record. Proventia A, Proventia G, and RealSecure Network Sensor each provide the same security functionality. The fourth component of the TOE, SiteProtector, provides management, monitoring, and configuration functions to users.

The Sensors monitor one or more 10/100/1000 Mbps copper or 1000 Mbps SX fiber network segments (the sensed, monitored network). Each Sensor deployed is also connected to a secure network, the secure management network, for dedicated communication to a SiteProtector.

Several patches are applied to the TOE and to the IT Environment of the TOE. The patches applied to the TOE have been done to help in the mitigation of vulnerabilities discovered in the TOE. Patches have been applied to the IT Environment of the TOE to help in configuring the TOE's IT Environment to support the functioning of the TOE and to help put the IT Environment in a state that can help in the protection of the TOE. The patches for the TOE are RSNetSnsr70_Linux_XXX_ST_4_3, RSNetSnsr70_MU_20_19, RSNetSnsr70_MU_24_2, RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11.

The patches for the IT Environment are RSNetSnsr70_Linux_2.4.18-10smp_ST_4_1, RSNetSnsr70_Linux_2.4.18-10smp_ST_4_2, SPIA_POLICY_20050208, SPNS_POLICY_20050208, DB_SR_1_1_20040915, DB_SR_1_2_20041020, DB_SR_1_3_20041022, DB_XPU_1_44_20040628, DB_XPU_1_45_20040719, DB_XPU_1_46_20040812, DB_XPU_1_47_20040915, DB_XPU_1_48_20041014, DB_XPU_1_49_20041111 DB_XPU_1_50_20041221, and DB_XPU_1_51_20050119.

The patches applied to the TOE do not affect the version number of the TOE. The patches are listed in the TOE after installation of the TOE has occurred so that an end user knows that they have the evaluated configuration with the patches applied.

6.1 TOE Components

The RealSecure Network Sensor and Site Protector both are sold as software products and run on standard computer platforms. The sensors Proventia A and Proventia G, in contrast, are sold as appliances, hardware platforms that include the operating system and

ISS software. For all four products, the platform, including hardware and OS, is not part of the TOE but is considered part of the environment.

6.1.1 Proventia A Version 7.0-2003.167 TOE Component

The Proventia A Version 7.0-2003.167 component of the TOE is one of three components of the TOE that provide IDS security functionality. The Proventia A Version 7.0-2003.167 software is included with any of the following appliances: Proventia A201, Proventia A604, Proventia A604-200, Proventia A1204, Proventia A1204F, Proventia A1204F-400. The following parts are also included in the TOE delivery:

A) Appliance face plate with 2 keys
B) Power Cable
C) Serial Console Cable (RJ45-DB9)
D) PS2/Mouse Y-Cable Splitter
E) Quick Start Guide
F) Appliance Recovery CD

6.1.2 Proventia G Version 8.0-2004.219 TOE Component

The Proventia G Version 8.0-2004.219 component of the TOE is one of three components of the TOE that provide IDS security functionality. The Proventia G Version 8.0-2004.219 is included with any of the following appliances: Proventia G100, Proventia G200, Proventia G1000, Proventia G1000F, Proventia G1200, Proventia G1200CF, or the Proventia G1200F. The following parts are also included in the TOE delivery:

A) Appliance face plate with 2 keys
B) Power Cable
C) Quick Start Guide
D) Cat 6 Coupler Crossover
E) Ethernet Cable 1ft
F) Appliance Recovery CD
G) Appliance Addendum Worksheet
H) Hardware Warranty
I) Appliance Bypass Unit Sheet
J) Pigtail (for keyboard/mouse)
K) Serial Console Cable (RJ45-DB9)
L) Rack Mount Kit (Mid Mount)
M) Slide Rail Kit

6.1.3 RealSecure Network Sensor Version 7.0 TOE Component

The RealSecure Network Sensor component of the TOE is one of three components of the TOE that provide IDS security functionality. The RealSecure Network Sensor Version 7.0 is offered by one of the following products:

a) RealSecure Gigabit Network Sensor 7.0 for Windows

b) RealSecure Gigabit Network Sensor 7.0 for Red Hat Linux

c) RealSecure Network Sensor 7.0 for Windows

d) RealSecure Network Sensor 7.0 for Red Had Linux

Each of these software products is a variant of RealSecure Network Sensor 7.0. Although the products offer different network interfaces and operate on different operating systems, the operating system and network drivers are not included in the security functionality claimed by the TOE. Therefore, all of the above appliances offer the same RealSecure Network Sensor 7.0 TOE component.

6.1.4 SiteProtector 2.0 Service Pack 4 TOE Component

The SiteProtector 2.0 Service Pack 4 component of the TOE is a software product that enables users to monitor and manage the Sensor components of the TOE.

Two components in the TOE 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

7 Assurance Requirements

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target.

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing-sample

AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

8 Security Functional Requirements

This section documents the SFRs on both the TOE and the environment. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the ST.

8.1 TOE Security Functional Requirements

Functional Component ID	Functional Component Name
Class FAU: Security Audit	
FAU_SAA.3	Simple Attack Heuristics
FAU_SAR.1	Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
Class FDP: User Data Protection	
FDP_ACC.1(1)	Subset Access Control
FDP_ACF.1(1)	Security Attributes Based Access Control
Class FMT: Security Management	
FMT_MOF.1	Management of Security Functions Behavior
FMT_MTD.1	Management of TSF Data
FMT_SMF.1(1)	Specification of Management Functions
FMT_SMR.1(1)	Security Roles
Explicitly Stated SFRs for the TOE	
FAU_GEN_EXP.1	Audit Data Generation - Explicit
FPT_RVM_SFT_EXP.1	Non-Bypassability of the TSP for Software TOEs - Explicit
FPT_SEP_SFT_EXP.1	TSF Domain Separation for Software TOEs - Explicit

8.2 Security Functional Requirements for the IT Environment

Security Functional Requirement Component	IT Environment Security Functional Requirement Component Name
Class FAU: Security Audit	
FAU_STG.1	Protected Audit Trail Storage
Class FDP: User Data Protection	
FDP_ACC.1(2)	Subset Access Control
FDP_ACF.1(2)	Security Attributes Based Access Control
Class FIA: Identification and authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMF.1(2)	Specification of Management Functions
FMT_SMR.1(2)	Security Roles
Class FPT: Protection of the TSF	
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable Time Stamps
Explicitly Stated SFRs for the IT Environment	
FAU_GEN.1-NIAP-0347	Audit data generation
FPT_RVM_OS_DBMS_EXP.1	Non-Bypassability of the TSP of the TSP for the OSs and DBMS - Explicit
FPT_SEP_OS_EXP.1	TSF Domain Separation for the OSs - Explicit

9 IT Product Testing

9.1 Test Configuration

The test configuration for all product tests was composed of five Windows computers, one Linux workstation, one Proventia A appliance, and one Proventia G appliance. The equipment was set up as two networks, a management network and a sensed network. The management network connected SiteProtector, RealSecure Network Sensor

(Windows), RealSecure Network Sensor (Linux), Proventia A, and Proventia G. The sensed network connected the attack computer, the target, and the sensors.

Each sensor has two network interfaces, one connected to the management network and the other to the sensed network. The management interfaces are connected to the Ethernet switch and the other to the network hub. The Ethernet hub is used to ensure the sensors are able to "see" all the network traffic. The management network is configured as 10.1.0.x and the sensed network is 192.168.1.x. Each of the sensor interfaces on the sensed network are configured in "stealth" mode and are not visible to other devices on the network.

For all tests,

A) The TOE is installed in its evaluated configuration

B) An Administrator account is created in Windows 2000 Server SP4

Table 1 - Configuration Details

System	Hardware	Software
SiteProtector	1.7 GHz Processor 386 MB RAM 20 Gig Hard Drive	Windows 2000 Server SP4 SQL Server 2000 SP3a Internet Explorer 6.0 SP1 SiteProtector 2.0 SP4
RealSecure Network Sensor (Windows)	P3 733 MHz Processor 256 MB RAM 19 Gig Hard Drive 2 Network cards	Windows 2000 Server SP4 Internet Explorer 6.0 SP1 WinZip RealSecure Network Sensor 7.0
RealSecure Network Sensor (Linux)	1.6 GHz Processor 256 MB RAM 20 Gig Hard Drive	2 Network cards Red Hat Linux 7.3 RealSecure Network Sensor 7.0
Attack Host	1.6 Ghz Processor 512 MB RAM 20 Gig Hard Drive	Windows XP Professional SP2 Internet Explorer 6.0 SP1 WinZip NMAP 3.00 (GUI 1.31) NEWT 2.0
Target Host	General Purpose PC	Windows Server 2000 SP4

9.2 Developer Testing

The evaluators determined that the developer's tests covered all of the TOE security functions (Audit, Detect, Protect, and Management) and exercised all but two of the TSFIs. They determined in addition that the developer's test configuration matched the evaluated configuration. The evaluators sampled the developer's test procedures to ensure that they were consistent with the test plan and reproducible, and that the actual test results were consistent with the expected results.

9.3 Evaluator Independent Testing

The evaluators verified a sampling of the developers test results and independently tested a portion of the TSF subset as defined in the ISS PROVENTIA| A Version 7.0-2003.167, PROVENTIA| G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0, and SiteProtector 2.0 Service Pack 4 Security Target.

The tests chosen for the independent testing were those functions for which the vendor did not provide tests and procedures. Several of the TSFIs with no procedures in the test plan were invoked to ensure that evaluator testing was complete. In addition, the evaluator also selected some tests that checked to verify that protocols disabled in the installation procedures were indeed disabled.

10 Documentation

The following documents were used as evidence for the evaluation; all were issued by ISS:

- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Security Target, Version 2.25, 11 April 2006
- Configuration management Documentation for ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4, Version 1.3, 10 October 2005
- Installation Procedure Supplement For ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4, Version 1.4, 14 February 2006
- Installation Procedure Supplement Errata Sheet For For ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4, Version 1.0, 13 June 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Functional Specification, Version 1.9, 7 October 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 High Level Design, Version 0.12, 14 December 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Developer's Functional Test Documentation, Test Results, Version 1.2, 16 November 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4
- Developer's Function Test Documentation Version 1.2, 16 November 2005

- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Administrator Guide, Version 1.3, 12 October 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 User Guide, Version 1.2, 12 October 2005
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Vulnerability Analysis, Version 1.1, 12 September 2005
- SiteProtector Installation and Configuration Guide – Version 2.0, Service Pack 4, June 2, 2004
- RealSecure Network Sensor and Gigibit Network Sensor Installation and Configuration Guide 7.0, March 2003
- Proventia A604 Appliances QuickStart Card, MA-PRO-A604-QSC-002
- Proventia A604, A1024, and A1024F Appliance User Guide, June 18, 2003
- Proventia G Series Appliances QuickStart Card, MA-PRO-GSeries_QSC-002
- Proventia G Series Appliances User Guide, June 22, 2004
- Delivery Procedure for Proventia A 7.0-2003.167 software, Proventia G 8.0-2004.219 software, SiteProtector™ 2.0 Service Pack 4, and RealSecure Network Sensor 7.0 Version 4.7 June 14, 2005.

11 Validator Comments/Recommendations

The ISS Proventia TOE is made up of four application software components. Two of these components, SiteProtector and NetworkSensor are purchased alone for installation on standard workstations. Two others, Proventia A and Proventia G, are each supplied as part of an appliance consisting of hardware, operating system, and applications software that is the TOE component. The products are used in various combinations of one SiteProtector with one of more Sensors that can be NetworkSensors or Proventia A or Proventia G appliances. The testing covered only representative combinations of these products, and so it is possible that some problems remain in configurations that were not tested.

The TOE includes only application software and excludes the hardware, operating system, and utility software such as the web browser and the DBMS. Consequently, much of the burden for maintaining security falls to the environment, and many of the security functional requirements were put on the environment rather than the TOE, where they are subjected to much less scrutiny than the TOE components.

Because auditing is done not by the TOE itself but by the operating system, the TSF is unable to audit startup and shutdown of the audit function as called for in FAU_GEN.1. Consequently, the ST calls for an explicit requirement, FAU_GEN_EXP.1 instead, which omits the reference to startup and shutdown of the audit function. Thus a rogue user could shut down TSF auditing to cover some malfeasance, and the shutdown would not appear in the (environment) audit record. Furthermore, the explicit requirement does not fulfill the dependency requirement for FAU_SAR.1 and FAU_SEL.1

12 Glossary

Abbreviation	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CPU	Central Processing Unit
DBMS	Database Management System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High Level Design
IDS	Intrusion Detection System
ISS	Internet Security Systems
IT	Information Technology
Mbps	Megabits per second
NIC	Network Interface Card
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

13 Bibliography

The following documents were used in the preparation of this Validation Report.

- Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, version 2.2, CCIMB-2004-01-001.
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, version 2.2, CCIMB-2004-01-002.

- Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, version 2.2, CCIMB-2004-01-003.
- Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, dated January 2004, version 2.2.
- Common Criteria Evaluation and Validation Scheme for Information Technology Security: Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002
- ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, RealSecure Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 Security Target, Version 2.25, 11 April 2006
- Evaluation Technical Report for ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, RealSecure Network Sensor 7.0, and SiteProtector 2.0 Service Pack 4 Target of Evaluation, COACT CAFÉ Lab, Document No. F2-0206-006(2), May 16, 2006
- Internet Security Systems, Inc. Proventia A and G Functional Test Report, COACT CAFÉ Lab, Document No. F2-0206-001, February 22, 2006
- Internet Security Systems, Inc. Proventia A and G Penetration Testing Report, COACT CAFÉ Lab, Document No F2-0206-005, February 22, 2006