National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

NetIQ Security Manager Version 5.5

Report Number: CCEVS-VR-07-0058
Dated: 9 August 2007
Version: 1.2

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

Santosh Chokhani
Ken Eggers
Orion Security Solutions, Inc.
McLean, VA

Common Criteria Testing Laboratory
Shukrat Abbas
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary 1
1.1 Evaluation Details 1
1.2 Interpretations 3
1.3 Threats to Security 3
2 Identification 3
3 Security Policy 3
3.1 Identification and Authentication 3
3.2 Security Management. 4
3.3 Protection of the TSF 5
3.4 Intrusion Detection and Event Correlation 5
4 Assumptions 6
4.1 Personnel Assumptions 6
4.2 Physical Assumptions 7
4.3 Intended Usage Assumptions 7
4.4 Clarification of Scope 7
5 Architectural Information 8
6 Documentation 9
7 IT Product Testing 9
8 Evaluated Configuration 10
9 Results of the Evaluation 10
10 Validator Comments/Recommendations 10
11 Annexes 10
12 Security Target 10
13 Glossary 10
Bibliography 11

List of Tables

Table 1 – Threats 3
Table 2 – Personnel Assumptions 6
Table 3 – Physical Assumptions 7
Table 4 – Intended Use Assumptions 7

1 Executive Summary

The evaluation of **NetIQ Security Manager 5.5** was performed by Science Applications International Corporation (SAIC), in the United States (US) and was completed in May 2007. The evaluation was carried out in accordance with the US Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the NetIQ TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 12, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 1.0.

SAIC determined that the evaluation assurance level (EAL) for the product is the EAL 2 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the NetIQ Security Manager 5.5 Security Target.

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 NetIQ Security Manager product by any agency of the US Government and no warranty of the product is either expressed or implied.

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 validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non – TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The technical information included in this report was obtained from the Evaluation Technical Report for NetIQ Security Manager 5.5 (ETR) Parts 1 and 2 produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	**NetIQ Security Manager 5.5**
Sponsor & Developer:	NetIQ, Incorporated 1233 West Loop South, Suite 1800 Houston, Texas 77027

CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	May 2007
CC:	**Common Criteria for Information Technology Security Evaluation, Version 2.3**
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 2
Description	The NetIQ Security Manager is an application that can act as an intrusion detection system for intrusion detection systems as well as for operating systems, firewalls, and antivirus applications. The TOE provides the ability to collect, standardize, and archive collected data from disparate monitored system. The TOE also provides the capability to review the collected data and generate reports. All communications between the TOE distributed components are encrypted. The TOE collects and reacts to event data from targeted IT systems using administrator configurable rules. The TOE agents collect real-time and log data from the targeted IT systems based on the configured rules. The central computer (CC) component receives the data from the agents and stores it in a database in the IT environment. The CC applies correlation rules to the collected data, generates responses when a rule match occurs; and performs trend analysis on the collected data. The Console component provides the GUI interfaces for all configuration and management operations. The console is used for reviewing the collected data and to generate and review summary and trend reports.
Disclaimer	The information contained in this Validation Report is not an endorsement of the NetIQ Security Manager product by any agency of the U.S. Government and no warranty of the NetIQ Security Manager product is either expressed or implied.
PP:	none

1.2 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

T.ADMIN_ERROR	Authorized user	Ineffective security mechanisms
T.MASQUERADE	Unauthorized user	Illegal access to TOE resources
T.TSF_COMPROMISE	Malicious user	Illegal access to the TOE and its data

2 Identification

The product being evaluated is NetIQ Security Manager 5.5. Note that the actual target of evaluation is defined to be only certain parts of the whole product.

3 Security Policy

The NetIQ Security Manager 5.5 TOE enforces the following security policies as described in the Security Target.

3.1 Identification and Authentication

The TOE relies on the IT Environment, specifically the operating system (OS) and the database (DB) server, to perform identification and authentication for each individual user. The OS maintains access control group names that map to the following four TOE authorization names:

OnePointOp Reporting,
OnePointOp Users,
OnePointOp Operators, and
OnePointOp ConfgAdms.

Similarly, the DB server maintains access control group names that map to the following three TOE authorization names:

EeaDasLocator,
EeaReportViewer, and
VigilEntUserAccess.

The TOE restricts user access to security management functions based on these NetIQ Security Manager authorizations.

3.2 Security Management.

The TOE Console application implements the following security management components:

- The ***Monitor Console*** allows the authorized administrator OS account with OnePointOp Users and EeaDasLocator authorizations to monitor real-time events and alerts for a configuration group and to configure Security Manager settings for a configuration group. Some tasks require the user to have other OnePointOp authorizations in addition to OnePointOp Users.

- The ***Incident Console*** allows the authorized administrator OS account with OnePointOp Users and EeaDasLocator authorizations to monitor alerts about real-time events across multiple configuration groups.

- The ***Development Console*** allows the authorized administrator OS account with OnePointOp Operators and EeaDasLocator authorizations to:

    - Display Windows computer groups, processing rule groups, notification groups, and advanced rule functionality for one configuration group;
    - Create or modify computer groups and processing rules; and
    - Create or modify notification groups, scripts, and data providers, which can be used when creating processing rules.

- The ***Configuration Snap-in*** allows the authorized administrator OS account with OnePointOp ConfgAdms and EeaDasLocator authorizations to:

    - Manage Windows agents and NetIQ Security Manager settings within a single configuration group;
    - View and modify global configuration group settings;
    - Configure settings for individual NetIQ Security Managers or agents;
    - Add operators to a notification group;
    - View and approve Windows agents before they are automatically installed on computers within the configuration group; and
    - Disapprove Windows agents before they are automatically uninstalled from computers within the configuration group.

- The ***Analysis Console*** allows the authorized administrator OS account with OnePointOp Reporting, EeaDasLocator, EeaReportViewer, and VigilEntUserAccess authorizations to:

    - Create, view, and print reports of data collected from computers, servers, devices, routers, and switches in the monitored enterprise;
    - Work with reports for one configuration group; and

- Change the configuration group for an analysis console.

- The ***Web Console*** allows the authorized administrator OS account with OnePointOp Users and EeaDasLocator authorizations to view real-time data and summary reports remotely from any Windows platform that supports Internet Explorer.

- The ***UNIX™ Manager*** allows the authorized administrator of the OS hosting the UNIX™ Manager application to configure rules for UNIX™ agents. The authorized administrator must enter a passphrase to gain access to this capability.

3.3 Protection of the TSF

The NetIQ Security Manager console allows authenticated administrators access to its interfaces according to authorizations corresponding to the set of operating system and database roles that NetIQ Security Manager console recognizes. The NetIQ Security Manager console checks that the IT environment has authenticated administrators before allowing access to its interfaces.

- The application-based console interfaces perform this check when they are invoked using operating system interfaces.
- The web-based console interfaces perform this check after an HTTPS connection has been established using a web browser in the environment.

The TOE relies on the operating system in the environment to protect its application components and to provide a secure runtime environment.

The TOE encrypts communication between Security Manager central computer and agent components and relies on the web server in the environment to provide HTTPS to protect communication between Security Manager console and the web browser.

The TOE relies on the database in the environment to protect collected event data and TOE configuration data.

3.4 Intrusion Detection and Event Correlation

Each TOE security agents is configured, using the Console application, with rules that describe potential security events that may occur on the targeted IT system resources (e.g., intrusion detection systems, operating systems, firewalls, antivirus applications) monitored by the security agent. These rules can be configured to detect changes to both targeted IT system resource operation or configuration changes. When the agent evaluates the rules and identifies a match, it sends an alert to the NetIQ Security Manager along with the security event data related to the alert. The communication between agent and manager relies on the IT Environment's SSL encryption mechanism to protect the data in transit.

When the TOE collects data from these agents, it manages them using any of the following four "datastreams" or work flows.

- The ***Real-time datastream*** first determines whether the applicable rule requires notification of an authorized administrator. If so, the TOE delivers an alarm using the configured notification mechanism. In either event, the TOE stores the alert and event data to the real-time database. The NetIQ Security Manager console monitors changes to the database and initially displays an alert. Authorized administrators can then perform further analysis of the alert.

- The ***Correlation datastream*** applies configured event correlation rules to collected data i.e., alerts and events from targeted IT system resources. When a correlation rule is matched, the TOE responds as specified in the rule (which could involve the generation of "correlation" alerts) and sends the source events and resulting alerts to the database server.

- The ***Log management datastream*** normalizes event data collected from the targeted IT system resources and sends the normalized data to the database. The retention period for this log data is configurable, but defaults to 90 days. In the event that the database becomes full, any new information is ignored and a warning is displayed to the Monitor Console. Whenever log data exceeds the configured retention period, the TOE creates additional space by deleting this data from the database. The Log Management datastream also periodically summarizes the collected data and assembles dimension information for trend analysis reports.

- The ***Reporting and trend analysis datastream*** is initiated when the Log management datastream finishes summarization of the collected data. The summary and dimension information are retrieved from the database and the trend analysis data cube, which includes historical summary data, is updated with the new dimension information. After completion of the summary and trend analysis processing, authorized administrators can view and publish trend analysis and summary reports via the Console interfaces.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 2 – Personnel Assumptions

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, willfully negligent, or hostile, and will follow and abide by the

	instructions provided by the TOE documentation.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3 Intended Usage Assumptions

The following physical assumptions are identified in the Security Target:

Table 4 – Intended Usage 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

4.4 Clarification of Scope

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

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 in this case).
2. As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. Encryption of communications using SSL between the agents and the central computer components and between the web console and the central computer is required. The evaluation team did verify the SSL communication between the central computer component and the agents and console components. Testing confirmed the presence of encrypted communication.

5 Architectural Information

The NetIQ Security Manager is an application that can act as an intrusion detection system for intrusion detection systems as well as for operating systems, firewalls, and antivirus applications. The TOE provides the ability to collect, standardize, and archive collected data from disparate monitored system. The TOE also provides the capability to review the collected and generate reports. All communications between the TOE distributed components are encrypted.

The TOE collects and reacts to event data from targeted IT systems using administrator configurable rules. The TOE agents collect real-time and log data from the targeted IT systems based on the configured rules. The central computer (CC) component receives the data from the agents and stores it in a database in the IT environment. The CC applies correlation rules to the collected data, generates responses when a rule match occurs; and performs trend analysis on the collected data. The Console component provides the GUI interfaces for all configuration and management operations. The console is used for reviewing the collected data and to generate and review summary and trend reports.

The Supported Targeted IT systems from which the TOE can collects events include the following:

- Firewalls
  - Check Point FireWall-1 NG (FP 1, 2, and 3)
  - Check Point FireWall-1 NG with Application Intelligence
  - Check Point Provider-1 NG (FP 1, 2, and 3)
  - Check Point Provider-1 NG with Application Intelligence
  - Check Point SiteManager-1 NG (FP 1, 2, and 3)
  - Check Point SiteManager-1 NG with Application Intelligence
  - Check Point VPN-1 NG (FP 1, 2, and 3)
  - Check Point VPN-1 NG with Application Intelligence
  - Cisco Secure PIX Firewall versions 5.3 to 6.3
  - Microsoft Internet Security and Acceleration Server 2000 (Event Manager Only)
  - NetScreen Firewalls with ScreenOS 4.0x
  - Secure Computing Sidewinder version 5.2x
  - Secure Computing Sidewinder version G2 6.0

- Intrusion Detection Systems
  - Cisco IDS version 4.0
  - Snort 1.9 and 2.0
  - Tripwire for Servers version 3.0 on Microsoft Windows 2000 Server

- Antivirus Applications
  - Network Associates McAfee Groupshield versions 4.5 and 5.0
  - Network Associates McAfee NetShield version 4.5
  - Network Associates McAfee VirusScan Enterprise version 7.0 and 8.0i
  - Symantec Norton AntiVirus Corporation Edition versions 7.x and 8.x
  - Symantec Norton Antivirus version 2.1 for Exchange 5.5
  - Symantec Norton Antivirus version 2.1 for Exchange 2000
  - Trend Micro ScanMail for Microsoft Exchange 5.5 versions 3.52 and 3.8
  - Trend Micro ScanMail for Microsoft Exchange 2000 version 6.0
  - Trend Micro Server Protect version 5.1

- Routers and Switches
  - Cisco Internet Operating System (IOS) versions 12.2 to 12.3

- Operating Systems
  - Windows NT 4.0 with Service Pack 6a
  - Windows 2000
  - Windows XP
  - Windows 2003
  - Compaq Tru64 UNIX 4.0f and 5.1a
  - HP-UX versions 11.0, 11.11
  - IBM-AIX versions 4.3.3, 5.1, 5.2
  - IBM iSeries hosting SuSE Linux 7.1
  - Red Hat Enterprise Linux AS 2.1 and 3.0
  - Silicon Graphics IRIX 6.5
  - Sun Solaris 7, 8, 9
  - Novell SuSE Linux Enterprise 7.1
  - iServers Servers running OS/400 version V5R1 or later

6 Documentation

Following is a list of useful documents supplied by the developer on a CD shipped with the product.

- NetIQ Security Manager Installation Guide, March 15, 2006
- NetIQ Security Manager Programming Guide, March 7, 2006
- NetIQ Security Manager User Guide, March 16, 2007
- NetIQ Unix Agent Installation and Configuration Guide Security Manager Vulnerability Manager, March 8, 2006
- NetIQ Installation Guide NetIQ Security Solutions for iSeries, July 25, 2005
- Release Notes – contains an overall description of the product and basic system requirements

The security target used is:

- NetIQ Security Manager 5.5 Security Target, version 0.83, May 23, 2007.

7 IT Product Testing

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

1. Central Computer applications and console applications: installed on Windows 2003 Server SP1
2. Agents applications components: Manual agents for Windows 2003 SP1, Windows XP, iSeries running OS/400, Red Hat Linux Advance Server 3.0, Solaris9. Managed agents for

Cisco IDS 4.1, Check Point NG –R55, Cisco Secure Pix Firewall, Symantec Antivirus Corporate Edition 9.x.

3. Network devices: Windows 2003 server, Windows XP, Red Hat Linux, iSeries computer running OS/400, Solaris 9, Symantic Antivirus Corporate Edition 9.x, Cisco IDS 4210 running Cisco IDS 4.1, Check Point NG-R55 software, Cisco Secure Pix Firewall running on Cisco Pix (OS) version 6.3.

The basic test configuration is running the console applications to access the central computer applications; to configure the data collection rules used by the agents and to manipulate the system data collected by the agents.

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions.

A selection of the developer tests were run and the results found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

8 Evaluated Configuration

The evaluated configuration is a single central computer component with console installed on one machine, the console components installed separately (i.e. two consoles); and manual agents, and managed agents.

9 Results of the Evaluation

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

None

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **NetIQ Security Manager 5.5 Security Target**, Version 0.9, July 9, 2007.

13 Glossary

There were no definitions used other than those used in the CC or CEM.

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, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Evaluation Technical Report for NetIQ Security Manager 5.5 Part II, version 1.0, May 25, 2007

[8] NetIQ Security Manager 5.5 Security Target, Version 0.9, July 9, 2007.

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