

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

NitroSecurity Intrusion Prevention System v7.1.3

Report Number: CCEVS-VR-07-0035
Dated: 11 June 2007
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 6740
Fort George G. Meade, MD 20755-6740

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

ACKNOWLEDGEMENTS

Validation Personnel

**Jean Hung
Paul Bicknell**

**MITRE Corporation
Bedford, Massachusetts**

Common Criteria Testing Laboratory

**SAIC, Inc.
Columbia, Maryland**

Table of Contents

1	Executive Summary	1
1.1	Evaluation Details	2
1.2	Interpretations	3
1.3	Threats to Security	3
2	Identification	4
3	Security Policy	4
4	Assumptions.....	5
4.1	Personnel Assumptions	5
4.2	Physical Assumptions	5
5	Architectural Information	5
6	Documentation.....	8
7	IT Product Testing	9
8	Evaluated Configuration	9
9	Results of the Evaluation	10
10	Validator Comments/Recommendations	10
11	Annexes.....	10
12	Security Target.....	10
13	Glossary	10
14	Bibliography	11

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

1 Executive Summary

The evaluation NitroSecurity Intrusion Prevention System v7.1.3 was performed by SAIC, in the United States and was completed in April 2007. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the NitroSecurity TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 15 October 2005. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 1.0. The TOE claims and meets conformance to the Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP).

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 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 NitroSecurity Intrusion Prevention System v7.1.3 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 NitroSecurity Intrusion Prevention System v7.1.3 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 parts of the TOE 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.

The technical information included in this report was obtained from the Evaluation Technical Report for NitroSecurity Intrusion Prevention System (ETR) v7.1.3 Parts 1 and 2 produced by SAIC.

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

1.1 Evaluation Details

Evaluated Product:	NitroSecurity Intrusion Prevention System v7.1.3.
Sponsor & Developer:	NitroSecurity, Inc 12030 Sunrise Valley Drive, Suite 180 Reston, VA. 20191
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	April 2007
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005
Evaluation Class:	EAL 3
Description	The TOE is an intrusion detection and prevention system that can detect network intrusion attempts and react by actively recording and/or blocking such attempts. The TOE can pass, drop, and log packets as they arrive, based on administrator-configurable rules. When the TOE is performing intrusion detection, it is said to be operating in an “IDS mode”. When the TOE is performing intrusion prevention, it is said to be operating in an “IPS” mode.
Disclaimer	The information contained in this Validation Report is not an endorsement of the NitroSecurity Intrusion Prevention System v7.1.3 by any agency of the U.S. Government and no warranty of the NitroSecurity Intrusion Prevention System v7.1.3 is either expressed or implied.
PP:	U.S. Government Intrusion Detection System System Protection Profile(IDSSPP), Version 1.6, April 4, 2006
Evaluation Personnel	Shukrat Abbas John Boone
Validation Personnel	Jean Hung, Paul Bicknell

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:

1.3.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

1.3.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

2 Identification

The product being evaluated is NitroSecurity Intrusion Prevention System v7.1.3. The models evaluated are identified in the NitroSecurity Intrusion Prevention System Security Target. Note that the actual target of evaluation is defined to be two components of the whole product.

3 Security Policy

P.DETECT 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.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Assumptions

4.1 Intended Usage Assumptions

The following intended usage assumptions are identified in the Security Target:

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.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

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.

A.NOTRST The TOE can only be accessed by authorized users.

4.3 Physical Assumptions

The following physical assumptions are identified in the Security Target:

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

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

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 3 in this case).

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

2. As with all EAL 3 evaluations, this evaluation did not specifically search for vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM); seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. The TOE consists of distributed components that exchange information across encrypted channels. The encryption capability has not been FIPS validated..

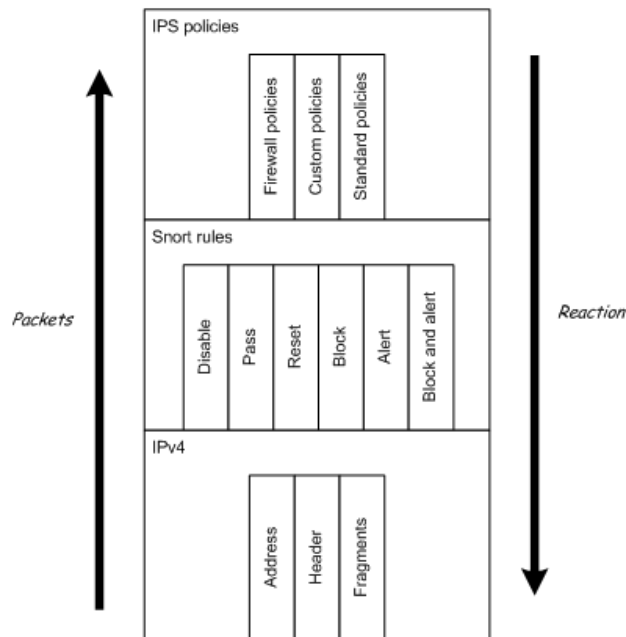
5 Architectural Information

The TOE passes, drops, and logs packets as they arrive, based on configurable rules. The TOE may be individually configured with rules, notification definitions, modes, variables and other parameters. There are three rule types:

- *Firewall Policy rules* include those the IPS will test against when a packet is examined for network traffic analysis
- *Standard Policy rules* include deep-packet inspection rules that evaluate the contents of a packet and compare them with the signatures associated with the rule.
- *Custom Policy rules* include administrator-modified firewall and standard policy rules.

The TOE is designed using the layers of the protocol stack present in data-link and TCP/IP protocol definitions. The TOE includes an implementation of Snort, an open source IDS type application implementation. The TOE imposes order on packet data by overlaying data structures on the raw network traffic. These decoding routines are called in order through the protocol stack, from the data link layer up through the transport layer, finally ending at the application layer.

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3



When a network packet enters the TOE through one of the physical network interfaces when the TOE is either in an in-line or an in-tap network location, the packet is first inspected to look for any firewall rule matches (packet headers). If a match is found that will cause an alert, the information is logged in the alerts database. If the packet was not dropped, it is passed to the inspection engine for deeper inspection (packet contents). The first check determines if the packet is a control channel packet from the ESM destined for this IPS. Otherwise, it begins trying to match the policy rules. If a match is found, the information is logged in the alerts database. If the packet has gone through both firewall and deep packet inspection without being dropped, it is sent out of the TOE through the second physical interface of that traffic path.

The TOE can be described in terms of the following components:

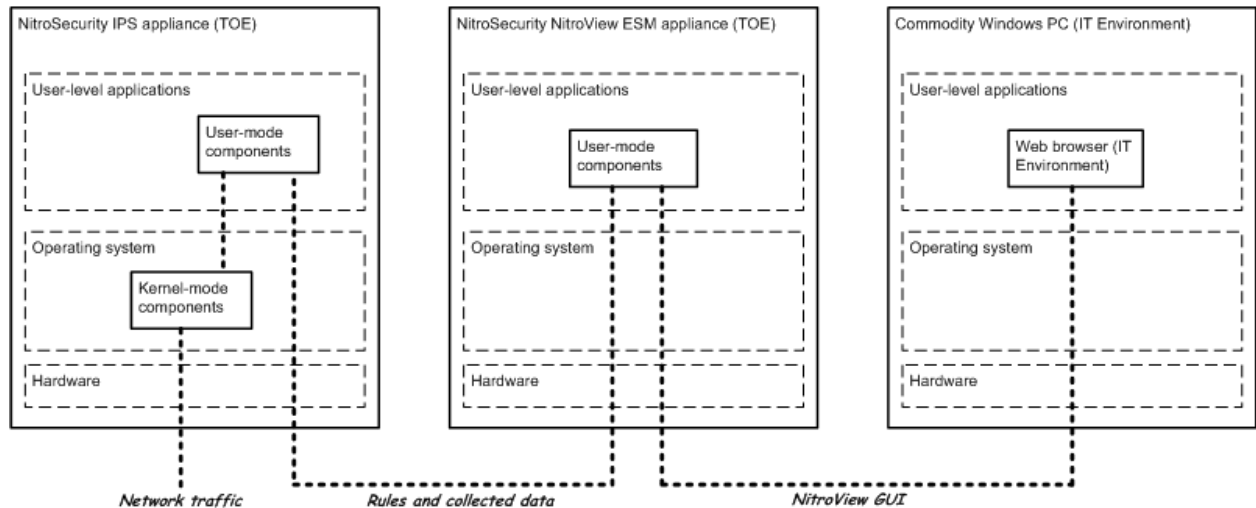
- *NitroSecurity IPS*¹ – A hardware appliance that provides network intrusion detection and prevention services for an enterprise type network. Includes the following components:
 - NitroSecurity hardware appliance
 - NitroSecurity Hardened Linux operating system
 - User- and Kernel-mode components that perform IDS and IPS functions
- *NitroSecurity ESM*² – A hardware appliance that provides web-based administrator console interfaces that can be used to manage NitroSecurity IPS services and collected data that are accessible using a web browser in the IT Environment. Includes the following components:

¹ Also called “NitroSecurity Intrusion Protection System”, or “IPS”.

² Also called “NitroSecurity NitroView ESM”, or “ESM”, or “Enterprise Security Manager”.

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

- NitroSecurity hardware appliance
- NitroSecurity Hardened Linux operating system
- User-mode components that provide web-based GUI administrative interfaces



The intended environment of the TOE can be described in terms of the following components:

Targeted IT systems – send and receive monitored network traffic

Web browser – used to access TOE administrative interfaces, including displaying alerts

SMTP, SNMP, syslog servers – can receive alerts generated by the TOE

Certificate authority server – Provides digital certificates to support the web-based GUI

NTP server – Used to set TOE hardware clock (specifically, the ESM appliance clock)

The ESM appliance provides a GUI to administer the IPS. It is accessed using a web browser on a system in the IT Environment. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. The administrator console can also be used to manage audit data and users. System data consists of results from IDS scanning, sensing, and analyzing tasks. The ESM appliance encrypts commands using a proprietary stackless control protocol sent from the ESM to the IPS. HTTPS is also used to protect the connection between the web browser in the IT Environment and the ESM appliance.

6 Documentation

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

VALIDATION REPORT
NitroSecurity Intrusion Prevention System v7.1.3

- Quick Start guide,
- NitroView user guide,
- Software License,
- Rack Installation manual
- NitroSecurity Hardware Warranty

- NitroSecurity Installation and Setup Guide, NS-75602002713 (hardcopy)

The security target used is:

- NitroSecurity Intrusion Prevention System Security Target (Version 1.0), 2007/04/27.

7 IT Product Testing

The evaluation team applied each EAL 3 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 the entire 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:

- TOE Platform: NitroSecurity Intrusion Prevention System v7.1.3 on IPS models: NS-IPS-1220R, NS-IPS-300, NS-IPS-620R, NS-IPS-300R and ESM models: NS-ESS-10, NS-ESSR-100
- Client Platform: Windows XP SP2 and Java-enabled web browser (IE and Mozilla)

The test configurations include the TOE in in-line configuration and in-tap configuration with the test machine that will generate traffic. The following tasks were performed by the evaluation team:

The developer test suite was examined and found to provide adequate coverage of 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.

Tests devised from postulated vulnerabilities in the I&A mechanism revealed no problems.

8 Evaluated Configuration

The evaluated configuration is two duplicate configurations of the TOE placed on the network in-line for IPS mode and in-tap for IDS mode. The ESMs are accessed over a network from Web browsers (IE and Mozilla).

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 the entire 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

The cryptography used in this product has not been FIPS validated. All cryptography has only been asserted as tested by the vendor.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **NitroSecurity Intrusion Prevention System v7.1.3 Security Target (Version 1.0), 05/25/2007**.

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 2: Evaluation Methodology, dated August 2005, version 2.3.
- [6] Evaluation Technical Report for NitroSecurity Intrusion Prevention System Product Part II, version 1.0, April 30, 2007
- [7] NitroSecurity Intrusion Prevention System Security Target (Version 1.0), 2007/05/25.
- [8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001