National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Lancope StealthWatch NC Appliance and StealthWatch Xe Appliance containing StealthWatch version 5.6.1 and StealthWatch Management Console version 5.6.1.

Report Number: CCEVS-VR-VID10243-2008
Dated: 12 May 2008
Version: 1.1

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

Table of Contents

1. Executive Summary

The Target of Evaluation (TOE) is the Lancope StealthWatch NC Appliance and StealthWatch Xe Appliance containing StealthWatch version 5.6.1 intrusion detection software and StealthWatch Management Console (SMC) version 5.6.1. The TOE was evaluated by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in the United States and completed January 2008. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2. The evaluation was conducted in conformance with the Common Criteria (CC) for Information Technology Security Evaluation and the Common Evaluation Methodology for Information Technology Security (CEM), version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

StealthWatch NC and StealthWatch Xe appliances each consist of applications and data files that provide intrusion detection related functions and associated security management functions, an Intel CPU-based hardware platform, and a Linux operating system.

The SMC can optionally be used in conjunction with the other TOE appliances identified above. The SMC is an appliance and a corresponding java application that executes on a commercial workstation and offers the ability to manage multiple appliances (NC or Xe) from a single interface. The java application implements the SMC client interface and is downloaded onto the client's machine every time a client user logs into the SMC. This SMC client interface serves as a TOE management interface, offering a richer set of security management capabilities. The analytical capabilities are not addressed in the context of this evaluation.

The TOE claims and meets conformance to the Intrusion Detection System (IDS) System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP).

The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. The Lancope StealthWatch Version 5.6.1 Security Target (ST) version 1.0 dated March 5, 2008, identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Lancope StealthWatch product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

1.1. Evaluation Highlights

Dates of Evaluation:	January 9, 2007 through January 25, 2008
Evaluated Product:	Lancope StealthWatch NC Appliance and StealthWatch Xe Appliance containing StealthWatch version 5.6.1 intrusion detection software and StealthWatch Management Console (SMC) version 5.6.1
Developer:	Lancope Incorporated, 3650 Brookside Parkway, Suite 400, Alpharetta, Georgia, 30022
CCTL:	SAIC, 7125 Columbia Gateway Drive, Suite 300, Columbia, Maryland 21046
Evaluation Class:	EAL2 augmented with ALC_FLR.2
PPs Claimed:	Intrusion Detection System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP)
Validation Body:	National Information Assurance Partnership CCEVS

2. Product Identification

ST: Lancope StealthWatch Version 5.6.1 Security Target v1.0, dated 5 March 2008

TOE Identification – Lancope StealthWatch NC Appliance (Model numbers M45. M250, M250X, G1, G1C, G1X, G1CX, and G1CFX) and StealthWatch Xe Appliance (Model numbers XE1000 and XE2000) containing StealthWatch version 5.6.1 and StealthWatch Management Console version 5.6.1.

The StealthWatch appliances (NC or Xe) consist of applications and data files that provide the intrusion detection related functions and associated security management functions, an Intel CPU-based hardware platform, and a Linux operating system.

The StealthWatch Management Console (SMC) can optionally be used in conjunction with the

other TOE appliances identified above. The SMC is an appliance and a corresponding java application that executes on a commercial workstation and offers the ability to manage multiple appliances (NC or Xe) from a single interface. The java application implements the SMC client interface and is downloaded onto the client's machine every time a client user logs into the SMC. This SMC client interface serves as a TOE management interface, offering a richer set of security management capabilities. The analytical capabilities are not addressed in the context of this evaluation.

3. Security Policy

The TOE is a network-based intrusion detection system that monitors, records, analyzes, displays, detects and alerts to security breaches and internal misuse on IP based networks. The TOE approaches intrusion detection and network management through a behavior-based architecture that provides protection from unknown threats, network policy management, activity tracking, and forensics tools for a proactive approach to managing threats. It characterizes and analyzes the data that flows between Internet Protocol (IP) devices on the network to differentiate abnormal network behavior from normal network behavior without examining the contents of each packet that traverses the network

The TOE implements the following security policies:

Identification and Authentication Policy:
All users of the TOE must enter a valid user identity and password before the user can access any TOE functionality. The StealthWatch Appliances have 3 types of accounts, Administrator, Web Administrator, and Technician. Administrative guidance defines the assignment of these user identities. The SMC has a single pre-defined Administrator role. The SMC Administrator (and other SMC users granted a role allowing the creation of users) can define additional users – assigning them unique identities, passwords, and applicable SMC roles.

Security Audit Policy:
The TOE generates audit data for administrative and management actions taken on the system. This audit is unrelated to the system data that is collected about the monitored networks. The actions audited by the TOE include start-up and shutdown of the system, system access, access to collected system and audit data, modification to the auditing configuration, modifications to configuration data, and adding or removing users. Access to the security audit log is provided through the administrative interface via a secure connection from a web browser.

Security Management Policy:

The TOE provides a secure web-based (utilizing SSL) management interface for all three classes of users performing administrative tasks.

In the StealthWatch appliances, the Administrator and Web Administrator accounts are provided with the ability to modify the behavior of the analysis and reporting functions by allowing them to modify the policies and thresholds of a host that is being monitored by the TOE. The Administrator and Web Administrator classes comprise the authorized System administrator role, while the Technician class comprises the authorized administrator role.

In the SMC, there is a single pre-defined Administrator role. The SMC supports the notion of Data and Function roles that can be assigned to users. Data roles dictate whether the associated user can only perform read or query operations or alternately whether the user is allowed to make changes within the TOE. Function roles serve to group specific TOE functions. SMC users are assigned a Data and Function role which together serve to define (and limit) the set of TOE functions available to that user. SMC users can also be explicitly designated as SMC administrators enabling the applicable administrative privileges.

Protection of the TOE Security Functions Policy:

The TOE protects its own security functions through a variety of mechanisms. A principle protection is the identification and TOE authentication of each user before any administrative operation can be performed. The data transferred between the TOE and the administrative user is protected by using SSL to encrypt and verify the communication.

The data collection interface of the TOE is protected from the monitored network by operating in a completely passive mode. The TOE does not respond to any traffic received from the monitored networks. The TOE cannot receive any management requests or input from the monitored network interfaces. Management requests can only be received via a physically separate network management port.

The TOE SMC java application is protected by its hosting IT environment from potential bypass and tampering while the application is active. The application is re-loaded from the SMC appliance onto the client machine during each client login. This mitigates the necessity of protecting the application between sessions.

The TOE protects its ability to continuously record audit data by periodically purging data, starting with the oldest data first. If there is adequate storage space, audit data is preserved for 30 days. If storage space is exhausted prior to 30 days, the oldest records are overwritten with new data on a first-in / first-out basis. This ensures that there is always storage available for recording current audit events.

System Data Collection Policy:
The TOE collects communications flow information about all monitored network activity. The system data collection policy will be either auto-tuned by monitoring normal activity on the network for a pre-defined period of time or constructed manually using the zone and host policies found under System Data Analysis and Reaction Policy.

System Data Analysis and Reaction Policy:
The TOE monitors all network traffic against predefined thresholds called Concern Indices (CIs) and policies, set at the granularity of a host or a zone (i.e., a collection of hosts), to detect potential intrusions and to generate alarms when an event is detected. Extensive analysis tools to view system data are provided through the Administrative interface.

System Data Review, Availability, and Loss Policy:
The TOE protects the data it collects by limiting access. It limits access in two ways:

1. Only authorized administrators are permitted to read system data.
2. The only interface provided to the data store is read only.

The TOE ensures availability and limits loss of system data by periodically purging data, starting with the oldest data first. In a situation where there is adequate storage space, system data is preserved for 30 days. If storage space is exhausted prior to 30 days, the oldest records are overwritten with new data on a first-in / first-out basis, and an alarm is sent to the authorized administrator. This ensures that there is always storage available for recording current system data.

4. Assumptions and Threats, Clarification of Scope and Interpretations

4.1 Usage Assumptions and Threats

The assumptions, threats and organizational security policies are reproduced from the IDSSPP and the related errata sheet.

4.2 Clarification of Scope

The following SFRs from the PP have not been included in this ST: FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. They were dropped because the TOE monitors but does not transmit information to external IT products and the SFRs were deemed unnecessary. To further support the exclusion of these SFRs, PD-0097 (http://niap.nist.gov/cc-scheme/PD/0097.html) states the inter-TSF related requirements (FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1) were erroneously included in the PP. PD-0097 also states that the O.EXPORT objective was erroneously replicated into the IDSSPP. Therefore, this ST deleted the O.EXPORT objective in order to be consistent with PD-0097. Additionally, PD-0097 also indicates that FPT_ITT.1 should be included when the TOE is a

distributed TOE.

4.3 Interpretations

Based on International Interpretations, changes were made within the ST. These interpretations had no impact on conformance to the IDSSPP since they only served to clarify assurance claims. The following sections provide the title and number of the applicable interpretations and the CEM class in which they were considered.

1. Separate objectives for TOE and environment (084) - ASE
2. Level of detail required for hardware descriptions (025) - ADV
3. Unique Configuration of CIs (003) – ACM
4. Underlying Hardware and Firmware (006) – ADV
5. Augmented and Conformant Overlap (008) – ASE
6. Deliver procedures may include confidentiality (016) - ADO
7. Evidence is required of entire TOE (024) – ADV
8. Events and actions (027) – AGD
9. Vulnerabilities not in TOE not applicable (031) – AVA
10. SOF analysis need not be in ST (032)
11. CM applicable to TOE (037) – ACM
12. CM requirement modified (038) – ASE
13. ADO_IGS and AVA_VLA requirements modified (051) – ASE
14. FMT_SMR (new requirement) as a dependency of FMT_MOF (065) – ASE, ADV
15. FAU_STG.2 modified (141) – ASE, ADV
16. FAU_GEN.1 permits the selection of only one options (202) – ASE, ADV

5. Architectural Information

5.1 Physical Boundaries

The TOE is physically comprised of an Intel based hardware platform. The TOE relies on process, disk, and memory management services provided by the base operating system and hardware to manage itself. The TOE also uses network communication services to monitor network traffic and to communicate between the StealthWatch appliance and the web-based administrative interface. The only security relevant function allocated to the operating system and underlying hardware is making reliable time information available to the StealthWatch application software.

The TOE also includes a StealthWatch Management Console (SMC). The SMC consists of an appliance and a java application executing on a commercial workstation in the IT environment. The SMC appliance provides services to support the corresponding java application. The java

application, the SMC Client Interface, is downloaded to the client's computer whenever the client user logs into the SMC appliance via a web browser. The SMC client interacts with the SMC appliance, which in turn interacts with the other TOE appliances using TLSv1 using a network. (The vendor recommends that this should be a separate network, dedicated to SMC interaction with SMC Clients.)

The TOE environment includes the host of the SMC Java application and the network being monitored. Note that the SMC is not required for the secure use of any of the other TOE appliances, but is an available option within the evaluated configuration.

5.2 Logical Boundaries

The logical boundaries of the TOE fall into two categories. The first deals with security and administration of the system as a whole (Security Audit, Identification and Authentication, Security Management, and Protection of Security Functions). The second deals with collection and analysis of data on the monitored networks (System Data Collection; System Data Analysis and Reaction; and System Data Review, Availability, and Loss).

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators

in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Examination of Vendor Tests

Testing of the TOE security functions was performed using a series of manual tests provided by the vendor, Lancope. These tests demonstrated the security-relevant behavior of the TOE for the external interfaces defined in the Functional Specification and High-Level Design. The goal of these tests was to demonstrate that the TOE meets the security functional requirements specified in the Security Target. The security functions tested were Security Audit, User Data Protection; Identification and Authentication; Security Management; Protection of TOE Security Functions; and Intrusion Detection System.

The developer's testing approach was to test all the security functional requirements described in the functional specification. Each test procedure identified the steps necessary to stimulate the required functionality and the results expected based on the documented stimuli. The developer's test configuration included two TOE administrative interface systems, a monitored network, and a network resident system to generate packets intended to stimulate the required TOE functionality. The actual results indicate that the expected result was achieved for each test procedure.

7.2 Evaluation Team Independent Tests

The evaluation team performed a subset of the developer's functional test suite as well as the team independent test suite using the developer's test configuration. The independent test suite included additional tests developed in response to perceived gaps or areas of weakness in the developer's test suite based on the team's coverage and depth analyses. Each actual test result was found to be consistent with the expected results for each test case.

The configurations used to test the TOE were:

Standalone Appliances:

- StealthWatch Appliance Model NC G1,
- StealthWatch Appliance Model Xe2000,

SMC and Appliances:

- StealthWatch Appliance Model NC M45,
- StealthWatch Appliance Model Xe1000,
- StealthWatch Management Console

IT Environment:

- Three Standard PC-computer laptop or desktop machines
    - Two PC computers running Windows XP,
    - One PC computer running Linux to generated network packets,
- Two Hubs,
- Monitor and keyboard, - used for directed connection to TOE-embedded appliance,
- Network cables

7.3 Strength of Function

The ST claims the strength of function for the Identification and Authentication (i.e., password) mechanism to be SOF-basic. The vendor's strength of function analysis and the evaluator assessment of the analysis substantiate this claim.

7.4 Vulnerability Analysis

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, and the evaluation team's performance of penetration tests.

8. Evaluated Configuration

The evaluated versions and model numbers of the TOE were:

- Lancope StealthWatch NC Appliance with StealthWatch version 5.6.1:
  - Model numbers: M45. M250, M250X, G1, G1C, G1X, G1CX, and G1CFX
- Lancope StealthWatch Xe Appliance with StealthWatch version 5.6.1:
  - Model numbers: XE1000 and XE2000
- Lancope StealthWatch Management Console version 5.6.1

9. Results of the Evaluation

The evaluation was conducted based upon version 2.3 of the CC and the CEM. The verdict for an assurance component is determined based on the verdicts assigned by the evaluation team to each of the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2" certificate rating be issued for Lancope StealthWatch NC Appliance and StealthWatch Xe Appliance containing StealthWatch version 5.6.1 intrusion detection software and StealthWatch Management Console (SMC) version 5.6.1.

The assurance components are shown in the table below:

EAL2 Augmented with ALC_FLR.2 Assurance Requirements

Assurance Class	Assurance Components

Configuration Management (ACM)	ACM_CAP.2 Configuration items
Delivery and Operation (ADO)	ADO_DEL.1 Delivery Procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life Cycle Support (ALC)	ALC_FLR.2 Flaw reporting procedures
Tests (ATE)	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

10.Validator Comments/Recommendations

None.

11. Security Target

The Security Target is provided separately.

ST: Lancope StealthWatch Version 5.6.1 Security Target v1.0, dated 5 March 2008.

12. List Of Acronyms And Glossary Of Terms

The following acronyms are provided for reference:

ACM	Assurance Configuration Management
ADO	Assurance Delivery and Operation
AGD	Assurance Guidance Documents
ADV	Assurance Development
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CI	Concern Index
DOS	Denial Of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	Hyper Text Transmission Protocol
HTTPS	Hyper Text Transmission Protocol, Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IDS	Intrusion Detection System
IDSSPP	IDS System Protection Profile
I/O	Input/Output
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol (RFC 1305)
PP	Protection Profile
RPC	Remote Procedure Call
SAIC	Science Applications International Corporation
SF	Security Functions
SFR	Security Functional Requirements
SFP	Security Function Policy
ST	Security Target
SWA	StealthWatch Appliance
SW+T	StealthWatch + Therminator
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	Target of Evaluation Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

UI	User Interface
URI	Uniform Resource Identifier

The following terms are provided for reference:

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

13. Documentation

The following end-user documents were examined for the evaluation:

SWA:

- The StealthWatch Appliance Configuration Guide Includes StealthWatch NC and StealthWatch Xe For v5.6
- SWA Quick Start Checklist
- StealthWatch v5.6.1 Help
- The StealthWatch Appliance Configuration Guide Includes StealthWatch NC and StealthWatch Xe For v5.6

SMC:

- SMC Installation Checklist
- SMC Configuration Guide For v5.6.1
- SMC Admin v5.6.1 Online Help
- SMC Help File for v5.6.1
- SMC User's Guide For v5.6
- SMC Configuration Guide For v5.6.1

14. Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Lancope Inc. (http://www.lancope.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security*, *version 2.3,* August 2005.

Security Target:

- *Lancope StealthWatch Version 5.6.1 Security Target v1.0*, dated 5 March 2008.