National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Enterasys Networks, Inc.

Report Number: CCEVS-VR-04-0075

Dated: 7 September 2004

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

Validator

James Brosey
Mitretek Systems
3150 Fairview Park Drive South
Falls Church, Virginia 22042

Common Criteria Testing Laboratory

Cable & Wireless
NVLAP Lab Code 200429
45901 Nokes Boulevard
Sterling, Virginia 20166

Table of Contents

Table of Figures

Table of Tables

1. Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0, at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Cable & Wireless, Sterling, Virginia, and was completed 9 August 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by Cable & Wireless and submitted to the Validator. The evaluation determined the product conforms to the CC Version 2.1, Part 2 extended and Part 3 conformant to meet the requirements of Evaluation Assurance Level (EAL) 2. This Validation Report is not an endorsement of the Enterasys Networks product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by Cable & Wireless.

The Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 is a self-contained, appliance-based Intrusion Defense System with host-based and network-based sensors as well as management, and reporting features. It is a commercial off the shelf (COTS) product manufactured by Enterasys Networks. Features of this TOE describe an Intrusion Detection System capability including the following:

- Integrated network based intrusion detection, host-based intrusion detection, and enterprise management
- Cross technology security monitoring of third-party routers, switches, firewalls, applications, web servers, and even other intrusion detection products
- Centralized policy management, analysis, and reporting using Dragon Enterprise Management Server
- High visibility into the state of the network with real-time reporting and historical forensics
- Executive-level reporting with summarized, printable network security reports for easy interpretation
- Multi-method detection including pattern matching, protocol decoding, and anomaly detection
- Large signature base can be updated continuously and posted regularly for detection of new attacks immediately after threat becomes known

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, 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 EAL 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 desire 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 CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Evaluation Identifiers for Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0
Protection Profile	N/A
Security Target	Enterasys Dragon-EAL™ Intrusion Defense System Security Target, Version 11, dated August 31, 2004
Evaluation Technical Report	ASE Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System Version 1.6, dated 27 August 2004
Conformance Result	Part 2 extended, Part 3 conformant at EAL2

Evaluation Identifiers for Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0	
Version of CC	CC Version 2.1 [1], [2], [3], [4], and all applicable NIAP CCEVS and International Interpretations effective on March 26, 2003
Version of CEM	CEM Part 1 Version 0.6 [5] and Part 2 Version 1.0 [6], and all applicable NIAP CCEVS and International Interpretations effective on March 26, 2003
Sponsor	Same as Developer
Developer	**Enterasys Networks** 50 Minuteman Rd. Andover, MA 01810 USA
Evaluator(s)	**Cable & Wireless** Diann Carpenter Alicia Squires Rick West Laura Stubbs Joe Cudby Ken Dill
Validator(s)	**NIAP CCEVS** James Brosey

Applicable Interpretations

Based on a kick-off date of March 26, 2003, the Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation: 3, 8, 9, 16, 24, 25, 27, 31, 32, 43, 49, 51, 64, 65, 75, 80, 84, 85, 116, 127, and 138.

3. Security Policy.

The Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 does not implement a security policy in the traditional sense of enforcing a set of access control rules. The TOE collects, stores and manages all IDS System records. The TOE targets the following Security Objectives as outlined in the ST:

- The TOE must protect itself from unauthorized modifications and access to its functions and data.
- The TOE must respond appropriately to analytical conclusions.
- The TOE must include a set of functions that allow effective management of its functions and data.

- The TOE must allow authorized users to access only appropriate TOE functions and data.
- The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- The TOE must not overwrite existing data when system data storage is full.
- The TOE must record audit records for data accesses and use of the System functions.
- The TOE must ensure the integrity of all audit and System data.
- The TOE must protect the confidentiality of its dialog with a remotely connected authorized administrators.
- The TOE must ensure the confidentiality of the System data when any IDS component makes its data available to another IDS component.
- The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of the TOE.
- The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
- The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

3.1 Roles.

The product supports three roles: *Root administrators* who manage the OS, *dragon administrators* who manage the IDS System, and *analysts* who are users authorized to query the system data.

- Root administrators– This role is able to manage the users of the TOE, to view and or modify the configuration of the operating system and to view any TSF data. This role is implemented by the *root* account on the operating system.

- Dragon Administrators: These administrators manage IDS functions of the TOE. This includes the host and network sensor components of the TOE and the IDS functions of the Enterprise Management System. A Dragon administrator account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

- Analysts: This role is able to view reporting data in the TOE, but is not permitted to modify any information. An analyst account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

3.2 Security Management.

There are two types of management functions in this TOE: management of IDS security functions and management of TOE security functions.

The management of the functions that are used to collect, analyze, and react to IDS data is managed by the dragon administrator. The behavior of the system data collection, analysis, and reaction functions is controlled by configuration files. The dragon administrator accesses these configuration files by the Policy Manager web interface, which has the ability to modify these configuration files and hence impact or modify the behavior of these functions.

The management of TOE security functions is the responsibility of the root administrator. These security functions include management of accounts, groups, and other TOE management functions. The behavior of the TOE security management functions are controlled by role enforcement on the use of the functions and on the data they impact.

4. Assumptions and Clarification of Scope

Usage Assumptions

The evaluation made the following assumption concerning intended product usage:

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

Clarification of Scope

Although not compliant with the Intrusion Detection System System Protection Profile (IDSSPP), Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 incorporates much of its elements and design. A comparison of the ST for the TOE to the IDSSPP reveals:

- All the same assumptions on the IT environment and personnel
- Several of the threats and objectives in the ST have been rewritten to reflect the TOE capabilities. T.FACCNT, T.SCNCFG, and T.SCNMLC were modified and T.SCNVUL was removed.
- The P.PROTCT policy was modified

- The objectives O.IDSCAN, O.OFLOWS, O.EXPORT were changed and O.RMTENC was added
- The following requirements were changed from the IDSSPP to reflect the TOE's security functionality:

FAU_GEN.1	Changed "basic level of audit" to "not specified level of audit" and removed some of the functionality from the table due to an inability to explicitly track unsuccessful attempts to read information from the audit records.
FAU_STG.2	Replaced with FAU_STG.1 since the TOE does not ensure that a specific percentage of audit records are maintained during audit exhaustion.
FAU_STG.4	This requirement was made explicit because the alert is made on disk capacity not on audit trail capacity.
FIA_AFL.1	Changed "a settable, non-zero number" to "3" and made specific to the product's response at the three different login locations to make the requirement more specific to the TOE.
FMT_MTD.1	Replaced selection existing in PP with a table of different selections and settings specific to the TOE.
FMT_SMR.1	Replaced roles in the PP with roles specific to system.
IDS_SDC.1	Removed some of the rows from the table of "Details" that are being collected, and removed "outcome (success or failure)" from IDS_SDC.1.2. The TOE does not track " success or failure of events"
IDS_STG.1	Removed the third element of the requirement, IDS_STG.1.3 since the TOE does not ensure that a specific percentage of IDS records are maintained during audit exhaustion.

5. Architectural Information.

Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 is a

TOE Overview

The TOE is the Dragon-EAL™ Intrusion Defense System (IDS), a self-contained appliance manufactured by Enterasys Networks. The TOE is an Intrusion Detection System, which uses scanners and sensors to collect information about target systems and/or networks, and an analyzer component to support interpretation of the data and initiate actions in response to its findings.

The TOE provides integrated network and host intrusion detection. It supports monitoring of routers, switches, firewalls, applications, web servers, the appliance itself, and other intrusion detection products. The Host Sensor monitors activity on the TOE, collecting information about events. The Network Sensor collects network packets from configured network connections. The data collected is processed by analyzer functions. Analysis methods include pattern matching, protocol decoding, and anomaly detection.. TOE users called analysts access the collected and interpreted data to do forensic and trending analysis.

The Dragon Enterprise Management System (EMS) provides policy management and centralized management of monitoring data collection and analysis. It provides high visibility into the state of the network and historical forensics. The reporting system provides executive-level reporting with summarized, printable network security

reports for easy interpretation. Enterasys frequently updates its IDS signatures. These signature updates can be downloaded from the Enterasys Dragon website automatically from the EMS. When automatic signature updates are enabled, signatures are downloaded through an Internet connection directly to the EMS using HTTPS. Updates are then pushed to the sensors.

The TOE consists of an enclosed hardware appliance with the Enterasys-modified operating system DAR, and the installed single host configuration of the Dragon 6.3 application software. All components are contained on the TOE appliance. The TOE is to be installed in accordance with the installation instructions in the Dragon-EAL Configuration Guide. This ensures that only the functionality necessary for the single host configuration of the Dragon 6.3 software is installed on the system.

The TOE appliance provides ports that support connection to network switches or to networks to be monitored. When a network switch is used, the Dragon-EAL™ monitors traffic from everything attached to the switch. Figure 1, below, shows an example of how the TOE could be placed in a target configuration. The TOE can be used by root administrators, who configure and maintain the appliance via the OS, dragon administrators, who configure and maintain the sensors via EMS, and by analysts who can access intrusion detection reporting data via the EMS. This reporting data includes raw data collected from monitored networks and systems as well as the results of analysis of such data. The root administrators can access the TOE from the physically co-located administrative console, using a command-line interface (CLI) to the OS and via SSH. Dragon administrators and analysts access the TOE remotely through encrypted logical connections via the EMS.

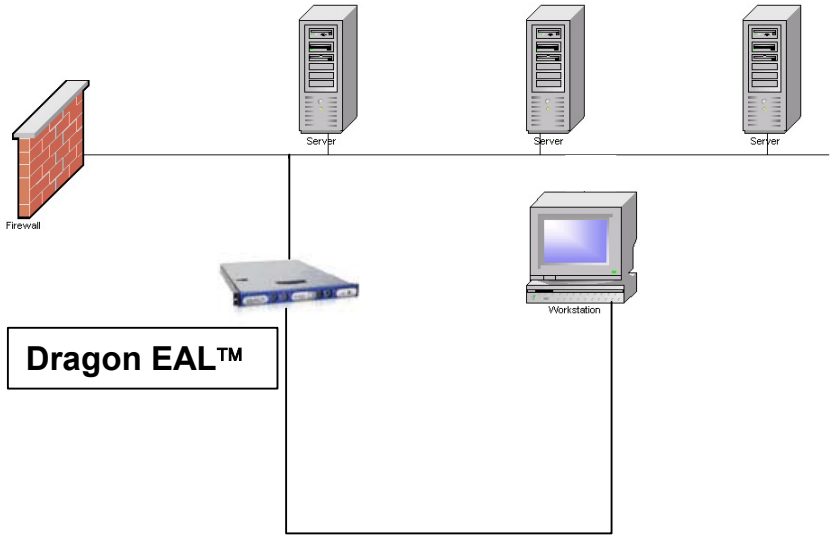

Figure 1: TOE in Sample Network Architecture

The administrative network and the network being monitored should be separate networks. The monitoring interface does not have a protocol stack bound to it, therefore it does not have an IP address and is not an active participant in the network. The administrative interface should have an IP address that is not accessible

from outside of the organization. This can be accomplished by placing the administrative network behind a firewall or by other means.

Dragon responds in a number of ways from simple administrator notification to automated responses to protect systems. Notification occurs on the administrative network while automated responses occur on the monitored network.

Dragon can utilize a SPAN (switch port analyzer) to monitor network traffic. In order to use the Sniper functionality the SPAN port must be capable of receiving inbound traffic on the SPAN destination port. If the IDS sensor is using a network TAP to receive traffic, the TAP must be capable of allowing the IDS to transparently inject TCP Resets back into the network.

The TOE has a hardware component and two software components. The Software components consist of the Enterasys proprietary operating system DAR, and the Dragon 6.3 application software (e.g., sensors, EMS, and Dragon Agents). Figure 2, below shows the hardware and software components of the TOE as well as its potential external physical connections.

Note there is some flexibility in the configuration of the TOE, and the following diagram represents a single instance. This diagram reflects a configuration where OS management is provided by a local terminal, and only one external network is being monitored. Options in configurations are described briefly in the discussion following the diagram.

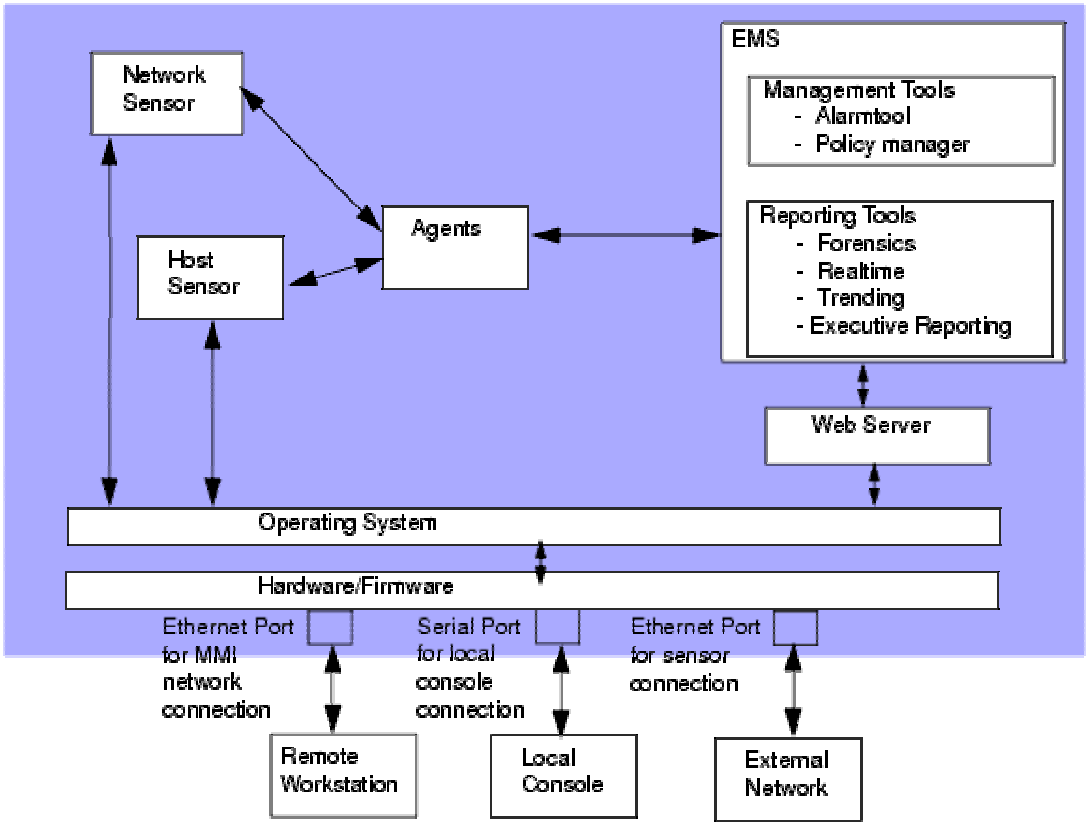

Figure 2: Dragon-EAL™ Component Architecture

TOE Physical Boundaries

The TOE is identical to the Dragon-EAL™ appliance. The TOE physical boundary is described in the table below.

Table 2: Physical Boundaries

Component	TOE or TOE Environment
Dragon-EAL™ version 1 hardware appliance	TOE
The DAR operating system version 2.1	TOE
Installed Dragon 6.3 in single server configuration	TOE
Target networks and Systems	TOE Environment
OS Administrative console: VT100 or VT100 emulator, any compatible mouse, screen, and keyboard.	TOE Environment
Remote management and analysis workstations	TOE environment

TOE Logical Boundaries

The TOE logical boundary includes the following security functions:

- Security Audit
- Identification and Authentication and Roles
- Security Management
- TOE Protection
- IDS data collection, analysis, and reaction
- System data management

Security Audit

The Security Audit function makes provisions for audit data generation, restricted and selectable audit review. The auditing feature is provided by a combination of functions from the web server, the operating system kernel, and the host sensor. The TOE uses a reliable time stamp mechanism provided by the TOE protection function. This makes it possible to determine the time and order of security relevant events that have been audited.

Identification and Authentication and roles

The Identification and Authentication function is based on user attributes, and ensures that users are identified and authenticated prior to any use of TOE functions. Identification and authentication occurs on the OS or from the web server. Users who are permitted to log into the OS can do this via a local console or remotely via the MMI. Web server users can only log in remotely via the MMI.

Security roles are defined for *Root administrators* who manage the OS, *dragon administrators* who manage the IDS System, and *analysts* who are users authorized to query the system data.

Security Management

The security management function contains the functionality to control and manage the IDS and the functionality to control and manage other TOE issues such as system log configurations, accounts and groups. Management and configuration of the IDS system is performed by the dragon administrator via the GUI. Other TOE management is performed by the root administrator from the operating system interface (either via the local console or remotely via the MMI).

TOE Protection

The TOE protects itself by providing a domain for its own execution that cannot be accessed by untrusted subjects, and by ensuring that the TSF cannot be bypassed. A TOE execution domain is provided by a combination of physical protection of the TOE, TSF that prevent access by unauthorized users, and lack of visibility to non TOE devices or users as well as entities on the systems being monitored. Non-bypassability of the TSF is provided by forbidding unauthorized users to access the TOE and by role enforcement.

The TOE provides a reliable time stamp mechanism for its own use.

The TOE also protects communication between analysts or dragon administrators and the TOE using SSL in an HTTPS session. HTTP access is not permitted. OS access can be provided via a local console or remotely. Remote root administrator sessions are protected by SSH.

IDS Data Collection, Analysis, and Reaction

The TOE provides both sensor and scanner functionality. The Host Sensor provides data collection and analysis capabilities by scanning selected entities on the TOE. The host sensor observes static data to detect attribute modifications, match signatures, or verify integrity. The Network Sensor provides data collection and data analysis using network traffic from configured remote networks. It provides a variety of signature-based analyses. All data from either sensor is stored in the Dragon DB. The EMS provides tools for further analysis. Selected records are collected and stored in a MySQL database, facilitating statistical analysis at high speed. The Alarmtool send alarms or alerts to the administrator when a likely intrusion is detected by any of the data collecting and analyzing functions.

System Data Management

The Intrusion Detection System provides the ability to review the system data via a web interface. system data is available to any administrator or analyst. The IDS also prevents system data loss and ensures of system data availability.

Subsystems

Enterasys Dragon-EAL™ Intrusion Defense System has the following subsystems:

- TOE Management Subsystem; This subsystem provides an external interface for root administrator to log directly into the operating system. The subsystem supports management and sorting of the audit data stored in the syslogs and web logs. It provides a path to the Command Line Interface component of the EMS subsystem to allow the root administrator to manipulate the data and create reports.
- The Host Sensor Subsystem: The Host Sensor provides configurable monitoring capabilities for actions on the Dragon-EAL™ system. This subsystem collects information about actions on the Dragon-EAL™ and ensures that it is written into the Dragon DB.
- The Network Sensor Subsystem: This configurable subsystem is connected to an external network to be monitored. It passively listens to the network traffic and ensures that information is recorded in the Dragon DB.
- The Enterprise Management Server Subsystem: This large subsystem is further broken down into several components. The EMS Configuration Management component provides the external interface for the Dragon administrator to perform configuration management on the Host sensor, network sensor, and Dragon-EAL™ EMS. The EMS Reporting component provides the external interface for analysts to access and manipulate collected data. The Dragon DB stores reporting data and is accessed by the network sensor and host sensor subsystems as well as the reporting components of the EMS. Although accessible via the command line, the command line tools also provide access to the Dragon DB for reporting information. The Dragon agents provide data transfer between the sensors and the reporting tools.
- The Web Server Subsystem: This subsystem consists of the Apache Web Server and the Tomcat™ servlet engine. They provide secure sessions for access to the EMS and perform identification and authentication of users.

6. Delivery and Documentation

6.1 Hardware and Software

Enterasys Dragon-EAL™ Intrusion Defense System Version 1.0 hardware and software is acquired as a system.

The Dragon-EAL consists of the Dragon IDS™ v6.3 software which can reside in one of two hardware models. Models are offered with different physical media types and performance rating, but this does not affect or differentiate the security functions in any way. The physical interfaces are functionally identical across all of the models. These models are identified as follows:

Dragon-EAL-TX
Dragon-EAL-SX
Dragon-E500-TX

Dragon-E500-SX

Dragon-EAL-TX/SX consists of:
Either the DSNSA-GE250-TX or SX appliance, Dragon software version 6.3, DSEMS (EMS Software license)

Dragon-E500-TX/SX consists of:
Either the DSNSA-GE500-TX or SX appliance, Dragon software version 6.3, DSEMS (EMS Software license)

TX versions contain dual port Copper gigabit interface
- SX versions contain dual port Fiber gigabit interface
- EAL-TX and SX perform at 250 Megabits per second
- E500-TX and SX perform at 500 Megabits per second

The following is a list of Documentation provided with the TOE:

6.2 Documentation

Dragon-EAL Version 1.0 Configuration Guide P/N 9033818-05

Plus, a CD-ROM is delivered with the TOE containing the following documentation:

- Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide Installation
- Dragon Intrusion Defense System Software Version 6.3 Customer Release Notes
- Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide
- Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide

7. IT Product Testing

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 product meets its advertised functional requirements. This functional test suite was used to run functional testing.

The Evaluation Team performed all of the Vendor Test Procedures provided by the contractor, in lieu of sampling. Since the entire test suite contains twenty-two total tests, the evaluation team decided that it was worth the time to execute all the test procedures.

The developers Test Plan and Test Procedures were documented in *Enterasys Dragon-EAL ™ IDS Version 1.0 EAL 2 Team Test Report*, Version 1.6, dated 23 July 2004. in this document, the SFRs and TSFIs that were tested during functional testing were mapped to vendor test cases. The Test Cases provide a description of the test functionality tested and test setup. The Test Cases were mapped to one or more Test Procedures. The Test Procedures provided detailed instructions for the tester as well as expected and actual test results.

The evaluation team identified areas within the evaluation that were not explicitly tested by the vendor. These include the FPT_SEP and FPT_RVM test areas. The evaluation team evaluated these areas through a combination of independent functional test procedures and an overall analysis of the testing effort.

7.2 Evaluator Independent Testing

For Independent testing, the CCTL developed a set of functional tests designed to augment the vendor testing. These tests have been developed to test specific functional requirements and they are detailed in *Enterasys Dragon-EAL ™ IDS Version 1.0 EAL 2 Team Test Report*, Version 1.6, 23 July 2004, section 4.3. The lab gave additional attention to the IDS Component Requirements Function, because it is the primary function of the product. The evaluation team tested as many of the specific IDS signatures as were reasonably possible against a test designed Windows victim, which limited the types of attacks that could be simulated. The test purpose was to successfully identify and trigger approximately 20 signatures to indicate positive IDS performance

The evaluation team chose several tools based on past IDS evaluation experience. Tools were included because of their ability to use a suite of attacks, which the evaluation team found to include many of the most dangerous attacks known today. The evaluation team used these tools to design tests applicable to the functionality of the TOE.

In addition, the evaluation team augmented the vendor testing by adding tests that cover three additional TSFIs, five additional SFRs, and more specific IDS signatures.

Comprehensive independent testing was not done for this product, however the team conducted a coverage mapping of the vendor functional tests to security functions and interfaces, and then devised the independent tests to cover several of the weak areas were functions and interfaces either were not tested or they were not tested sufficiently.

7.3 Penetration Testing

The evaluation team targeted the administration interface on the TOE, because port scanning during independent testing confirmed that no ports were open and no IP addresses on the sensing interface. The configuration used for penetration testing is the same as the network configuration used for functional and independent testing, but the SlackAttack box was put on the administrative hub and given an IP of 192.168.100.110.

The depth of testing chosen by the evaluation team was focused on the administrative interface and relative to confirming or attempting to disprove claims made by the developer's vulnerability analysis. Additional web server exploits were attempted.

The only additional vulnerability discovered by the evaluation team was that "the SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack." This vulnerability exists only on the administrative interface. Since the administrative interface on the evaluated configuration is assumed to be on a protected network (A.LOCATE) with authorized administrators are not careless, willfully negligent, or hostile (A.NOEVIL), this vulnerability will be mitigated.

8. Evaluated Configuration

TOE Identification

The TOE is identified as Enterasys Dragon-EAL Version 1.0. The evaluation team has verified that the TOE is labeled consistently with this unique identifier.

TOE Installation

The evaluation team used the Enterasys Dragon-EAL installation manuals to ensure that all steps needed to bring the TOE up into a known state on each platform are used and confirmed:

- Dragon-EAL Configuration Guide P/N 903318-05
- Documents referenced by the EAL Configuration Guide

Testing involved team installation and configuration of a sampling of systems in the documented configuration. All systems were installed from original media, using default configurations, by the evaluation team.

TOE Configurations

The configuration of the network used to test the TOE was created by the CCTL. This configuration is documented in Figure 3 below, and it was used to execute the developer tests, evaluator independent tests, and penetration tests.

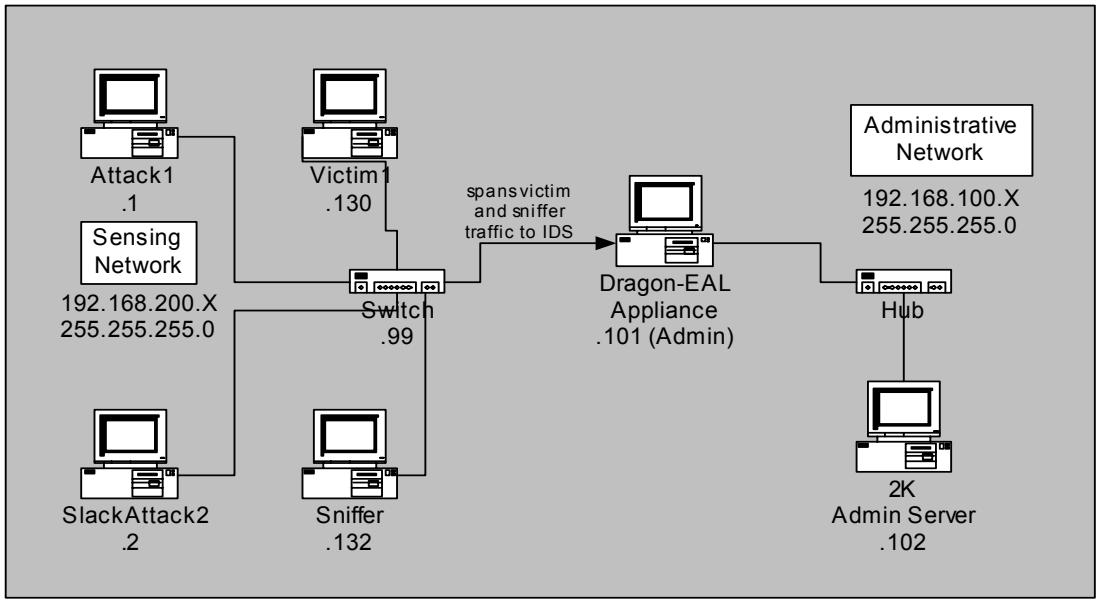

Figure 3: Enterasys Dragon-EAL testing environment

Table 3: Configurations

System Configuration Name	Hardware Platform	Software Platform	NICS	RAM
Enterasys Dragon-EAL IDS	Dragon-E500-SX	Enterasys Dragon-EAL running software version 6.3	10/100/1000	
Victim	Compaq Proliant 1850R	Windows 2K Advanced Server	10/100	256
Windows 2K Admin Server	Compaq Proliant 1850R	Windows 2K Advanced Server	10/100	128
FreeBSD Attack1 Box	Gateway	Free BSD 4.7	10/100	
Slackware Attack2	Dell	Slackware 9.1	10/100	
Sniffer	Dell	Slackware 9.1	10/100	256

The TOE that was tested was the 500 Appliance (all models are functionally equivalent in terms of security functionality) with the dual port Fiber interface running Dragon software version 6.3. Customers will be able to order this configuration by the part number Dragon-E500 SX at the completion of the evaluation. The other models of the TOE are the Dragon-EAL-TX, Dragon-EAL-SX, and the Dragon-E500-TX. The TX versions contain a dual port Copper gigabit interface, while the SX versions contain a dual port Fiber gigabit interface. The 250 in the model identifier indicates that intrusion detection is performed at 250 Megabits per second, while the 500 indicates that intrusion detection is performed at 500 Megabits per second. The models are offered with different physical media types and performance rating, but this does not affect or differentiate the security functions in any way. The physical interfaces are functionally identical across all of the models; therefore testing could have been conducted against any of the models. Successful test results obtained by the lab on the Dragon-E500-SX apply to all four models.

Physical Boundaries of TOE

The TOE is identical to the Dragon-EAL™ appliance. The TOE physical boundary is described in the table below.

Table 4: Physical Boundaries

Component	TOE or TOE Environment
Dragon-EAL™ version 1 hardware appliance	TOE
The DAR operating system version 2.1	TOE
Installed Dragon 6.3 in single server configuration	TOE
Target networks and Systems	TOE Environment
OS Administrative console: VT100 or VT100 emulator, any compatible mouse, screen, and keyboard.	TOE Environment
Remote management and analysis workstations	TOE environment

Logical Boundaries of TOE

The TOE logical boundary includes the following security services and features:

- Security Audit
- Identification and Authentication and Roles
- Security Management
- TOE Protection
- IDS data collection, analysis, and reaction
- System data management

9. Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable NIAP CCEVS and International Interpretations in effect on March 26, 2003.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 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. Section 4, Results of Evaluation, from the following documents, contains the verdict of "PASS" for all the work units:

- ASE Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.6, August 27, 2004.
- ACM_CAP.2 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.3, 6 August 2004.
- ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.1, 3 August 2004.
- ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 24 August 2004.
- AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 25 August 2004.
- ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.3, 25 August 2004.
- AVA_SOF.1; AVA_VLA.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 5 August 2004.

The evaluation determined the product to be Part 2-extended and Part 3 conformant, meeting the Security Assurance Requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Cable & Wireless.

Therefore, when configured according to the following guidance documentation:

- Dragon-EAL Version 1.0 Configuration Guide P/N 9033818-05
- Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide Installation
- Dragon Intrusion Defense System Software Version 6.3 Customer Release Notes
- Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide
- Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide

Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 is CC compliant and satisfies the ST, *Enterasys Dragon-EAL™ Intrusion Defense System Security Target*, Version 11, August 31, 2004.

10. Validator Comments

The Validator observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validator agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 6 and the Conclusions presented in Section 7 of the ASE Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.6, August 27, 2004. The validator considered the findings of the evaluation team and the clarification of scope in section 4 of this document. The Validation Team, therefore, concludes that the evaluation and Pass result for the Enterasys Dragon-EAL™ Intrusion Defense System, version 1.0 ST and TOE are complete and correct.

11. Security Target

The Security Target, *Enterasys Dragon-EAL™ Intrusion Defense System Security Target*, Version 11, August 31, 2004, is included here by reference.

12. Glossary

12.1 Definition of Terms

Authorized Analyst An authorized user who can access System data and use EMS analysis tools to access system data

Authorized Dragon administrator An authorized administrator who manages the IDS functionality of the TOE from the EMS

Authorized User A user that is allowed to perform IDS functions and access data. All authorized users are administrative in nature.

Human User Any person who interacts with the TOE

Intrusion Detection System Analyzer (Analyzer) The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future)

Intrusion Detection System Scanner (Scanner) The component of an IDS that collects 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

Intrusion Detection System Sensor (Sensor) The component of an IDS that collects real time events that may be indicative of vulnerabilities in or misuse of IT resources

IT Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems

Network Two or more machines interconnected for communications

Packet A block of data sent over the network transmitting the identities of the sending and receiving stations, error control information, and message

Packet Sniffer A device or program that monitors the data traveling between computers on a network

Role A predefined set of rules establishing the allowed interactions between a user and the TOE

Root administrator An authorized administrator who manages the IDS functionality of the TOE from the OS

Scanner data Data collected by the Scanner functions

Scanner functions The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data). In this ST, the component named the Host Sensor provides the scanner functions.

Security A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

Sensor data Data collected by the Sensor functions

Sensor functions The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data). In this ST, the component named the Network Sensor provides the sensor functions.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

System data Data collected and produced by the System functions

System functions Functions performed by all IDS component (i.e., Analyzer functions, Scanner functions, and Sensor functions)

Target of Evaluation (TOE) An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation

Threat The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security

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

TSF data Data created by and for the TOE, that might affect the operation of the TOE

TSF Scope of Control (TSC) The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE

Vulnerability Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing

12.2 Definition of Acronyms

API Application Program Interface
ASCII American Standard Code for Information Interchange
CC Common Criteria for Information Technology Security Evaluation
CEM Common Evaluation Methodology
CI Configuration Items
CLI Command Line Interface: In this ST, CLI refers specifically to the ten IDS reporting data manipulation functions that are available to the dragon administrator from the Forensics console and to the root administrator from the operating system. These may also be referred to as command line tools.
CM Configuration Management
DAC Discretionary Access Control
DAR The name of the Enterasys-hardened version of the Linux-based Slackware operating system that is provided with the TOE. There is no expansion.
EAL Evaluation Assurance Level
EGID Effective Group ID
EMS Enterprise Management System
HIDS Host Intrusion Detection System: in this ST, the Host Sensor
NIDS Network Intrusion Detection System; in this ST, the Network Sensor
MMI Man machine interface
OS Operating System. In this ST, the operating system is DAR. The operating systems contains all OS commands and CLI commands. The operating system is accessible through a command line interface (in the traditional sense).
OSP Organizational Security Policy
PEM Privacy Enhanced Mail
SFP Security Function Policy
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
SQL Structured Query Language

SOF Strength of Function
SSL Secure Socket Layer
ST Security Target

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

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

[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 1999, Version 2.1.

[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 1999, version 1.0.

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

[8] 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

[9] Enterasys Dragon-EAL™ Intrusion Defense System Security Target, Version 11, August 31, 2004.

[10] ASE Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.6, August 27, 2004

[11] ACM_CAP.2 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.3, 6 August 2004.

[12] ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.1, 3 August 2004.

[13] ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 24 August 2004.

[14] AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 25 August 2004.

[15] ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.3, 25 August 2004.

[16] AVA_SOF.1; AVA_VLA.1 Evaluation Technical Report for Enterasys Dragon-EAL Intrusion Defense System, version 1.2, 5 August 2004.

[17] Enterasys Dragon-EAL ™ IDS Version 1.0 EAL 2 Team Test Report, Version 1.6, 23 July 2004.