National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Profiler Blade System Version 5.0

Report Number: CCEVS-VR-05-0125
Version 1.0
10 October 2005

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Maureen Cheheyl
The MITRE Corporation
Bedford, Massachusetts

Jandria Alexander
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Booz Allen Hamilton Common Criteria Test Laboratory
Linthicum, Maryland

Table of Contents

1 Executive Summary

The evaluation of the Mazu® Profiler Blade System Version 5.0 was performed by the Booz Allen Hamilton Common Criteria Test Laboratory in the United States and was completed on 10 October 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2 and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation, Version 2.2, for conformance to the Common Criteria for IT Security Evaluation, Version 2.2. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Profiler Blade System product by any agency of the US Government and no warranty of the product is either expressed or implied.

The Booz Allen Hamilton Common Criteria Test Laboratory evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

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

The 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 the command line interface, importing audit data from NetFlow-enabled Routers and NETScout Probes, authenticating users via a RADIUS Server, or receiving lease information from a DHCP Server to track hosts whose IP address has changed.

The technical information included in this report was obtained from the Evaluation Technical Report for Profiler Blade System Version 5.0 produced by Booz Allen Hamilton Common Criteria Test Laboratory.

1.1 Evaluation Details

Evaluated Product	Mazu® Profiler Blade System Version 5.0
Sponsor & Developer	Mazu Networks, Inc., Cambridge, Massachusetts
CCTL	Booz Allen Hamilton, Linthicum, Maryland

Completion Date	10 October 2005
CC	*Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004
Evaluation Class	EAL 2
Description	The Mazu® Profiler Blade System Version 5.0 Target of Evaluation (TOE) is a distributed behavior-based network security solution that is designed to protect the critical, core applications and services inside the enterprise network. The Profiler Blade System analyzes the behavior of hosts in the network rather than threat signatures to detect threats.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Profiler Blade System product by any agency of the U.S. Government, and no warranty of the Profiler Blade System product is either expressed or implied.
PP	None
Evaluation Personnel	Ken Bailey Wilhelm Burger Mark Landon Tiffani Parsons Bruce Potter Brian Rickle Eric Winterton
Validation Team	Maureen Cheheyl The MITRE Corporation Bedford, Massachusetts Jandria Alexander The Aerospace Corporation Columbia, Maryland

1.2 Interpretations

As of the kickoff meeting held on 15 July 2004, there were no CCIMB interpretations that apply to Version 2.2 of the Common Criteria; NIAP interpretations were not used in this evaluation.

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations issue.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 – Threats

Threats Addressed by the TOE	
T.ACCESS	A user could attempt to establish an unauthorised session with the TOE.
T.COLLECT	An unauthorised user could remove or modify statistical data collected by the TOE that is used for analysing the behaviour of normal network activity.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.
Threats Addressed by the Environment	
T.E.SENSOR	A user on an internal or external network could perform hostile actions on the internal network without having such actions captured for analysis and review.
T.E.TIME	A user may attempt to spoof timestamp values provided by an NTP server thereby causing the TOE and/or IT components with which the TOE communicates to maintain deferring time values.

2 Identification

The product being evaluated is the Mazu® Profiler Blade System Version 5.0. Note that the actual target of evaluation defined includes only certain parts of the whole product.

3 Security Policy

There are no security policies for the product.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

A.CONFIG The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation.

A.NOEVIL The authorized users 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 be accessed only by authorized users.

A.PASSWD The authorized users of the TOE will use best commercial practices when establishing passwords.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

A.LOCATE The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unauthorised physical access.

4.3 Logical Assumptions

The following logical assumptions are identified in the Security Target:

A.PEER IT Components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

5 Architectural Information

5.1 Logical Boundary

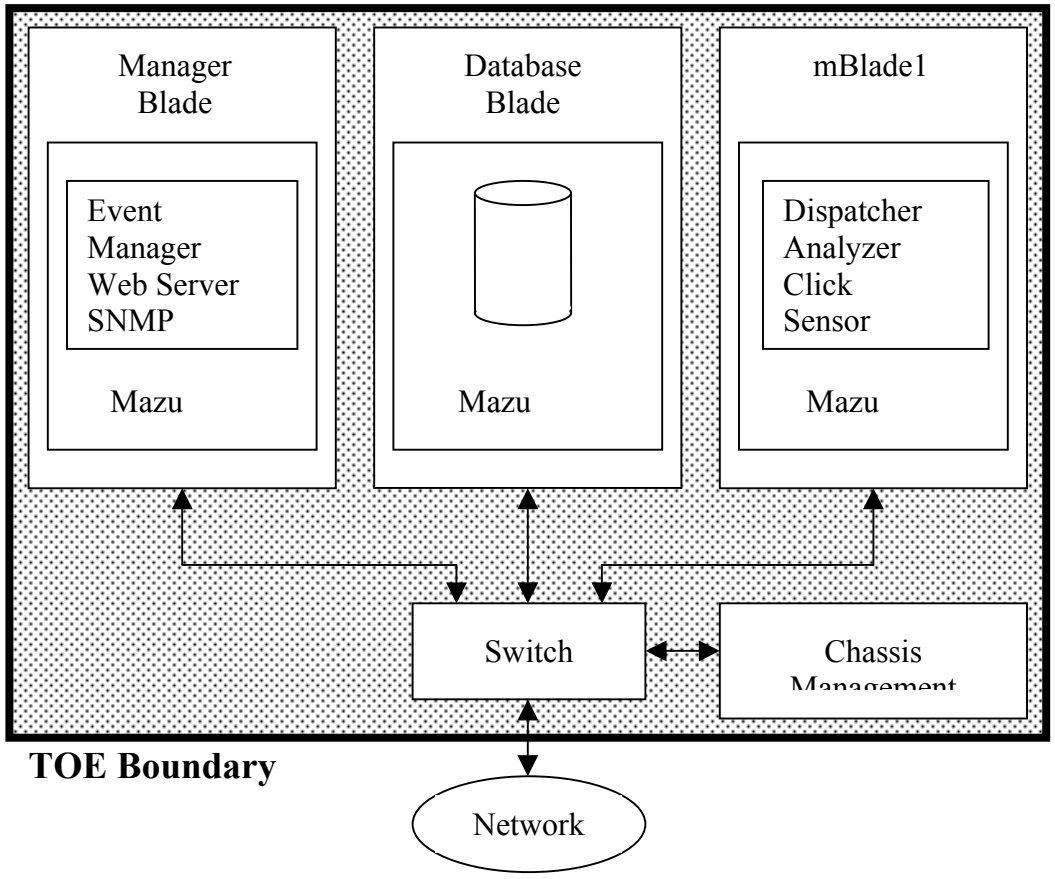

Figure 1 TOE Logical Boundary

The software structures of the TOE are discussed in the following sub-sections.

5.1.1 Security Audit

The TOE receives audit data that has been collected and generated by a Mazu Sensor via the MPCP. In addition, the communication link between the Mazu Sensor and the TOE is established through the use of a shared secret. Once the TOE has received audit data, it stores the information in a profile. Complex heuristics are then applied to the profile to identify anomalous behaviour on the network that deviates from normal activity. The TOE then generates alerts based upon triggered events that have surpassed a configured threshold rating.

5.1.2 Identification and Authentication

The TOE provides an HTTPS interface that is used to access its security functions. During initial configuration, a user establishes a connection to the TOE using their local web browser running on the Admin Terminal. Next, the user is prompted to provide the identification and authentication credentials required to log onto the TOE under the Administrator role. Once the user has successfully assumed the Administrator role, that

user can then create additional roles that the TOE will recognize when other users attempt to identify and authenticate themselves over the HTTPS interface from the Admin Terminal.

5.1.3 Security Management

The TOE provides for the management of its security functions via the HTTPS interface from the Admin Terminal. Once a user has been successfully identified and authenticated, they will then be granted access to the TOE that is limited based upon the role that the user has been assigned. The roles supported by the TOE have varying levels of access rights with respect to viewing or modifying the way in which the security functions of the TOE behave. These roles include the Administrator, Operator, Monitor, and Event Viewer.

5.1.4 Protection

Since the TOE is an appliance-based system, most of the protection features are implemented in its hardware and software structures. These structures provide for process execution as well as process separation. In addition, management of the TOE is enforced by limiting user access by requiring each user to identify and authenticate prior to being granted access over the HTTPS interface. Additional aspects related to protection of the TOE are addressed via assumption statements identified in the Security Target, Section 4.

5.2 TOE Exclusions

The evaluated configuration does not include user access to the Profiler command-line interface. Therefore, the following features described in the user manual are outside the evaluated configuration:

- Using an external script to write DHCP information to the Profiler
- Manually modifying the etc/hosts file that is internal to the Profiler
- Importing a specification file for a rule-based event
- Performing backup and restore operations

The following additional TOE functionality is also beyond the scope of this evaluation:

- Importing audit data collected and generated by NetFlow-enabled Routers and NETScout Probes
- Authenticating users via a RADIUS Server
- Receiving lease information from a DHCP Server to track the behaviour of hosts when they have been assigned a new IP address

6 Documentation

The following documents are delivered to customers and are pertinent to the installation, configuration, and operation of the TOE.

1. Mazu Networks Configuration Guide for Profiler 5.0
2. Mazu Networks Mazu Profiler 5.0 Release Notes

3. Mazu Networks Profiler Blade System Installation Process Description version 1.0
4. Mazu Networks Profiler Version 5.0 User Manual version 5.0-2
5. IBM eServer BladeCenter HS20, Type 8832 Installation and User's Guide
6. IBM eServer HS20, SCSI Storage Expansion Unit
7. IBM eServer BladeCenter, Type 8677 Installation and User's Guide
8. IBM BladeCenter 4-Port Gb Ethernet Switch Module Installation Guide
9. IBM Distributed Power Interconnect Front-end Power Distribution Unit Installation & Maintenance Guide
10. Mazu Networks Support Services Handbook

7 IT Product Testing

7.1 Test Approach

The test team's test approach was to test the security mechanisms of the Mazu Profiler Blade System V5.0 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface is described in Mazu's design documentation in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, High-Level Design (HLD), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all EAL2 requirements for all security-relevant TOE external interfaces. TOE external interfaces that were determined to be security relevant are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be appropriate to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen also performed vulnerability assessment and penetration testing.

7.2 Test Methodology

The evaluation team used three types of tests. They were:

- Ixia Machine Testing
- Manual testing
- Nessus Intelligent Scanning

7.2.1 IXIA Machine Testing

The functional tests were conducted on a test network with an IXIA machine attached to generate specific traffic patterns.

This included interactive scripts executed via the IXIA machine. Each script consisted of specific traffic-generation parameters to simulate activity normally associated with destructive events such as worm or virus infestation and denial-of-service activities. Each script was in a separate file which was executed using the IXIA GUI as the controller. These scripts generated traffic as if the TOE were on an active network.

The IXIA appliance is a machine that generates specific traffic at specific rates for specific network segments. The intent was to use the IXIA appliance to simulate the activity that is typical of worms, denial-of-service schemes, and viruses. The IXIA process allows execution of traffic generation either interactively or through execution of a script. When executed interactively the IXIA GUI is used to change traffic patterns or behavior. Execution of a script is done by setting up a profile of the traffic requirements necessary and saving these parameters as a profile.

The results of execution appear in the IXIA window. The results can then be copied to an OS file and compared to the results contained in the script documentation.

7.2.2 Manual Testing

The test team created manual testing procedures to test various functional claims of the Mazu Profiler Blade System v5.0. These tests included rebooting the Mazu sensor, causing the sensor to go down or to not respond, adding a new host to the network, removing a host from the network, starting a new service on the network. All of these events were designed to trigger alerts generated by Mazu Profiler Blade System v5.0.

7.2.3 Nessus Intelligent Scanning

Nessus allows remote audit of a given network to determine whether intruders can break into it or misuse it in some way. Unlike many other security scanners, Nessus does not assume that a given service is running on a fixed port; that is, if a web server runs on port 1234, Nessus will detect it and test its security. It will also not determine that a security vulnerability is present by simply checking the version number of the remote service, but will actually attempt to exploit the vulnerability.

7.3 Developer Testing

The vendor provided a complete set of test results for analysis. The evaluation team analyzed the vendor test procedures to determine if there was adequate coverage of the SFRs and to determine if the interfaces between subsystems behaved as expected. The Evaluation Team determined that the developer's actual test results matched the expected results.

7.4 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset of the tests that the developer performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed the security functions.

7.5 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the penetration test team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

8 Evaluated Configuration

The evaluated configuration of the TOE includes the Profiler Blade System Version 5.0 appliance that is comprised of the following:

- Hardware:
    - One IBM eServer BladeCenter Type 8677 7U chassis hardware platform
    - One or more Analyser mBlades (IBM eServer BladeCenter HS 20, Type 8832 blade server plug-in module): each Analyzer mBlade provides support to monitor between 20,000-40,000 hosts on the network.
    - One Database mBlade (IBM eServer BladeCenter HS20, Type 8832 blade server plug-in module)
    - One Manager mBlade (IBM eServer BladeCenter HS 20, Type 8832 blade server plug-in module)
    - One IBM eServer BladeCenter HS20, SCSI Storage Expansion Unit
    - One IBM eServer BladeCenter 4-Port Gb Ethernet Switch Module
    - Two IBM Distributed Power Interconnect Front-end Power Distribution Units
- Software:
    - Mazu Profiler Version 5.0 that includes:
        - Linux version 2.4.25 – with Mazu patches
        - openssh-3.7.1 – Secure Shell
        - openssl-0.9.7d – Secure Socket Layer
        - ntp-4.1.2 – Network Time
        - ucd-snmp-4.2.3 – SNMP
        - apache-2.0.49 – Web Server
        - php-4.3.8 – Scripting Language.

The evaluated configuration does not include the following features described in the user manual:

- User access to the Profiler command-line interface
- Using an external script to write DHCP information to the Profiler
- Manually modifying the etc/hosts file that is internal to the Profiler
- Importing a specification file for a rule-based event
- Performing backup and restore operations
- Importing audit data collected and generated by NetFlow-enabled Routers and NETScout Probes
- Authenticating users via a RADIUS Server
- Receiving lease information from a DHCP Server to track the behaviour of hosts when they have been assigned a new IP address

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the Profiler Blade System Version 5.0 TOE meets the security requirements contained in the Security Target.

The criteria against which the Profiler Blade System Version 5.0 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the Profiler Blade System Version 5.0 TOE is EAL 2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

A Validator on behalf of the CCEVS Validation Body monitored the evaluation carried out by Booz Allen Hamilton. The evaluation was completed in October 2005. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

10 Validator Comments/Recommendations

The Mazu® Profiler Blade System is a distributed behavior-based network security solution that is designed to protect the critical, core applications and services inside the enterprise network. The Profiler Blade System analyzes the behavior of hosts in the network rather than threat signatures to detect threats.

Note that the TOE is not the complete product. Specific functions have not been evaluated, even though those might be useful in operational use. Unevaluated functions include:

- User access to the Profiler command-line interface
- Using an external script to write DHCP information to the Profiler
- Manually modifying the etc/hosts file that is internal to the Profiler
- Importing a specification file for a rule-based event
- Performing backup and restore operations
- Importing audit data collected and generated by NetFlow-enabled Routers and NETScout Probes
- Authenticating users via a RADIUS Server
- Receiving lease information from a DHCP Server to track the behaviour of hosts when they have been assigned a new IP address

Furthermore, the correct operation of the Profiler depends heavily on the correct operation of the Mazu Sensor that collects the audit data but is not included in the TOE.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is *Profiler Blade System Version 5.0 Security Target*, *Version 1.0,* August 16, 2005.

13 List of Acronyms

The following acronyms are used in this report:

CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CEM	
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAL	Evaluation Assurance Level
HTTPS	HyperText Transfer Protocol Secure
IT	Information Technology
MPCP	Mazu Profiler Communication Protocol
NTP	Network Time Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

14 Glossary

The following definitions may be used in this document:

- Administrator: A role recognized by the TOE that can change settings but not manage user accounts.
- Event Viewer: A role recognized by the TOE that can only view event reports.
- Monitor: A role recognized by the TOE that can view all pages, but can change only the display settings.
- Superuser: A role recognized by the TOE that can change settings and manage user accounts.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Parts 1, 2, and 3.
- Common Criteria Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations,* Scheme Publication #3, Version 2.2, January 2002.
- *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004
- *Profiler Blade System Version 5.0 Security Target,* Version 1.0, August 16, 2005
- *Profiler Blade System Version 5.0 Evaluation Technical Report (ETR)*, Version 1.0, August 17, 2005
- Evaluation Team Test Plan for the Mazu Profiler Blade System, V5.0, Version 1.0, July 2005