National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

NETSCOUT Arbor Edge Defense and APS Systems

Report Number: CCEVS-VR-VID10925-2019
Version 1.0
December 30, 2019

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior Validator
Randy Heimann, ECR Team
Linda Morrison, Lead Validator

MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle
Alex Massi
Christopher Rakaczky
Courtney Simon

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the NETSCOUT Arbor Edge Defense and APS Systems provided by NETSCOUT, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in December 2019. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* (NDcPP).

The TOE is the NETSCOUT Arbor Edge Defense and APS Systems containing the models APS2600, APS2800, AED2600, and AED2800. Each TOE appliance operates with APS or AED software version 6.2.2. Note that the AED/APS software is built on top of Arbux internal OS v7.0 (ArbOS). The NETSCOUT Arbor Edge Defense and APS Systems (AED/APS) are used to secure the internet data center's edge from threats against availability, specifically from application-layer distributed denial of service (DDoS) attacks. AED/APS deploys at ingress points to an enterprise to detect, block, and report on key categories of Distributed Denial of Service (DDoS) attacks. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The 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 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. 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 technical information included in this report was obtained from the *NETSCOUT Arbor Edge Defense and APS Systems Security Target v1.1*, dated December 12, 2019 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring 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's Product Compliant 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 Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	NETSCOUT Arbor Edge Defense and APS Systems running software version 6.2.2. Refer to Table 2 for Model Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	NETSCOUT Arbor Edge Defense and APS Systems Security Target V1.1, December 12, 2019
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "NETSCOUT Arbor Edge Defense and APS Systems" Evaluation Technical Report v1.1 dated December 12, 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	NETSCOUT, Inc.
Developer	NETSCOUT, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Paul Bicknell, Randy Heimann, Linda Morison

3 Assumptions and Clarification of Scope

3.1 Assumptions

The assumptions are drawn directly from the [NDcPP].

3.2 Threats

The threats are drawn directly from the [NDcPP].

3.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314*, 14 March 2018, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the Security Management Platform's capabilities to collect network traffic and events, correlate the data collected to detect threats, and provide recommendations for responses to safeguard the network against cyberattacks described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The evaluated configuration of the TOE is the APS2600, APS2800, AED2600, and AED2800 described in Table 2 running software version 6.2.2. In the evaluated configuration, the TOE uses TLS/HTTPS to secure remote web-based administration, SSH to secure remote command-line administration. and TLS to secure transmissions of security-relevant data from the TOE to an external syslog server. The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Model	APS2600/AED2600	APS2800/AED2800
Processor	Intel E5-2608L v3 - 2.00GHz	Intel E5-2648L v3 - 1.80GHz
Sockets	2	2
Memory	32 GB	64 GB
OS SSD Capacity	240 GB	240 GB
Cores Per CPU	6	12

Table 2 – Hardware

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Component	Definition
Certification Authority / OCSP Responder	A server that acts as a trusted issuer of digital certificates and hosts the OCSP Responders that identifies revoked certificates.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or a web browser (Microsoft Internet Explorer 10 or 11, Google Chrome 44, Firefox ESR 31 or 40) to access the web GUI, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
Syslog Server	The syslog server connects to the TOE and allows the TOE to send syslog messages to it for remote storage. This is used to send

	copies of audit data to be stored in a remote location for data redundancy purposes.
Update Server	A general-purpose computer that is used to store software update packages that can be retrieved by the Security Administrator and downloaded via the management workstation. Software updates, including new versions, are made available to licensed clients through an Electronic Software Distribution system. Access to the ESD server is controlled by the NETSCOUT client services organization and limited to actively licensed clients. Updates are transferred from the management workstation to the TOE via the web GUI upload tool from the management workstation. The TOE does not directly communicate with the update server and is not considered a TOE external interface.

Table 5 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

Audit records are generated for various types of management activities and events. The audit records include the date and time stamp of the event, the event type and subject identity. In the evaluated configuration, the TSF is configured to transmit audit data to a remote syslog server using TLS. Audit data is also stored locally to ensure availability of the data if communications with the syslog server becomes unavailable. Local audit records are stored in files which are rotated to ensure a maximum limit of disk usage is enforced.

5.1.2 Cryptographic Support

The TOE uses sufficient security measures to protect its data in transmission by implementing cryptographic methods and trusted channels. The TOE uses SSHv2 and TLS/HTTPS to secure the trusted path to the Remote CLI and the web GUI respectively. The TOE also uses TLS to secure the trusted channel to the remote syslog server.

The cryptographic algorithms are provided by a NETSCOUT FIPS Object Module (CERT 3457). Cryptographic keys are generated using the CTR_DRBG provided by this module. The TOE erases all plaintext secret and private keys that reside in both RAM and non-volatile storage by overwriting them with random data. In the evaluated configuration, the TOE operates in "FIPS mode" which is used to restrict algorithms to meet the PP requirements.

5.1.3 Identification and Authentication

All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE. This is true of users accessing the TOE via the local console, or protected paths using the remote CLI via SSH or web GUI via TLS 1.2/HTTPS. Users authenticate to the TOE using one of the following methods:

- Username/password (defined on the TOE)
- Username/public key (SSH only)

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked until a Security Administrator unlocks it. This behavior is configurable and shared by the CLI and by the web GUI. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers, and special characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates to the device, a configurable warning banner is displayed.

As part of establishing trusted remote communications, the TOE provides X.509 certificate functionality. In addition to verifying the validity of certificates, the TSF can check their revocation status using Online Certificate Status Protocol (OCSP). The TSF can also generate a Certificate Signing Request in order to obtain a signed certificate to install for its own use as a TLS server.

5.1.4 Security Management

The TOE defines three roles: System Administrator, DDoS Admin, and System User. Each of these roles has varying levels of fixed privilege to interact with the TSF. The System Administrator role is able to perform all security-relevant management functionality (such as user management, password policy configuration, application of software updates, and configuration of cryptographic settings). Therefore, a user that is assigned this role is considered to be a Security Administrator of the TSF. Management functions can be performed using the local CLI, remote CLI, or web GUI. All software updates to the TOE are performed manually.

5.1.5 Protection of the TSF

The TOE stores usernames and passwords in a password file that cannot be viewed by any user on the TOE regardless of the user's role. The passwords are hashed using SHA-512. Public keys are stored in the configuration database which is integrity checked at boot time. Key data is stored in plaintext on the hard drive but cannot be accessed by any user. The TOE has an underlying hardware clock that is used for keeping time. The time must be manually set in evaluated configuration. Power-on self-tests are executed automatically when the FIPS validated cryptographic module is loaded into memory. The FIPS cryptographic module verifies its own integrity using an HMAC-SHA1 digest computed at build time.

The version of the TOE (both the currently executing version and the installed/updated version, if different) can be verified from any of the administrative interfaces provided by the TSF. All updates are downloaded to a local machine from the vendor website and then loaded on to the TOE. The updated image is verified via a digital signature before installation completes.

5.1.6 TOE Access

The TOE can terminate inactive local console, remote CLI or web GUI sessions after a specified time period. Users can also terminate their own interactive sessions. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE displays an administratively configured banner on the local console or remote CLI and the web GUI prior to allowing any administrative access to the TOE.

5.1.7 Trusted Path/Channels

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a remote syslog server using TLS to encrypt the audit data that traverses the channel. When accessing the TOE remotely, administrators interact with the TSF using a trusted path. The remote CLI is protected via SSHv2 and the web GUI is protected by TLS/HTTPS.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Assurance Activities Report for a Target of Evaluation NETSCOUT Arbor Edge Defense and APS Systems v1.1, December 12, 2019
- NETSCOUT Arbor Edge Defense and APS Systems Security Target v1.1, December 12, 2019
- NETSCOUT Arbor Edge Defense and APS Systems Supplemental Administrative Guidance for Common Criteria- v1.1, December 12, 2019

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, are the TOE models APS2600, APS 2800, AED2600, and AED2800, running the software version 6.2.2.

Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, each TOE model is configured to communicate with the following environment components:

- Management Workstation for local and remote administration and pulling TOE updates from NETSCOUT update server.
- Syslog Server for recording of audit data
- OCSP Responder for confirming the validity and revocation status of certificates

To use the product in the evaluated configuration, the product must be configured as specified in the *NETSCOUT Arbor Edge Defense and APS Systems Supplemental Administrative Guidance for Common Criteria Version 1.1, December 12, 2019* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "NETSCOUT Arbor Edge Defense and APS Systems" Assurance Activities Report v1.1* dated December 12, 2019.

8.1 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.2 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces.

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 tested each interface for all relevant behavior of the TOE that applied to that interface.

8.3 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD.
These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources.

All search activities were conducted prior to the execution of the vulnerability testing activities. The public search was updated December 12, 2019 with no further vulnerabilities discovered.

System penetration tests were also conducted and this testing showed that there were no vulnerabilities that could be leveraged by a malicious user when installed according to the NETSCOUT Arbor Edge Defense and APS Systems Supplemental Administrative Guidance for Common Criteria Version 1.1 [AGD].

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

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 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Security Management Platform product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in

describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in *NETSCOUT Arbor Edge Defense and APS Systems Supplemental Administrative Guidance for Common Criteria Version 1.1, December 12, 2019* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *NETSCOUT Arbor Edge Defense and APS Systems Security Target version 1.1,* dated December 12, 2019.

13 List of Acronyms

Acronym	Definition
AGD	Administrative Guidance Document
CC	Common Criteria
CPU	Central Processing Unit
ESD	Electronic Software Distribution
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
NIAP	National Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

14 Terminology

Term	Definition
Administrator	A user who is assigned an Administrator role on the TOE and has the ability to manage the TSF.
ArbUX	Arbux internal OS v7.0 (ArbOS) is a Linux based operating system.
Security Administrator	The claimed Protection Profile defines a single Security Administrator role that is authorized to manage the TOE and its data. This TOE defines three separate user roles, but only the most privileged role is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

15 Bibliography

1. Assurance Activities Report for a Target of Evaluation NETSCOUT Arbor Edge Defense and APS Systems, December 12, 2019
2. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
4. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
6. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
7. NETSCOUT Arbor Edge Defense and APS Systems Security Target v1.1, December 12, 2019
8. NETSCOUT Arbor Edge Defense and APS Systems Supplemental Administrative Guidance for Common Criteria- v1.1, December 12, 2019