National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Radware APSolute OS Version 1.0

Report Number: **CCEVS-VR-06-0007**
Dated: **March 23, 2006**
Version: **1.02**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Radware

Evaluation Personnel:
CygnaCom Solutions, McLean VA
Nancy Gow
Peter Kukura
Nithya Rachamadugu
Kris Rogers
Deepak Somesula
Mossadeq Zia

Validation Personnel:
Scott Shorter, Orion Security Solutions
James Donndelinger, Aerospace

Table of Contents

Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Radware APSolute OS Version 1.0. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Radware APSolute OS Version 1.0 was performed by the CygnaCom Solutions Common Criteria Testing Laboratory in the United States and was completed in February 2006. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was prepared by CygnaCom Solutions. The ETR and test report used in developing this validation report were written by CygnaCom Solutions. The evaluation team determined the product to be Part 2 and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 have been met.

Radware provides Intelligent Application Switching (IAS) products that provide high-speed hardware switching with software security services across layers 3-7. The Target of Evaluation (TOE) for this effort consists of the SynApps module that performs information flow control and security alert notification as a component of the overall appliance, as well as the Command Line Interface (CLI) module that manages the SynApps module and the Policy Definition File (PDF) that stores the configuration.

The Radware appliance itself forms the IT Environment of the TOE, and the TOE relies on it for services including user authentication, timestamps, non-bypassability and domain separation. None of these services were analyzed or tested. An assumption that administrators would log in via local console access allows the device to rely on physical protection to prevent unauthorized administrative access. Trusted administrators (the other assumption) are a necessity, as the device performs no auditing of management activities, either in the TOE or in the IT Environment.

The information flow control and security alert notification are based on a set of security attributes of the traffic being examined, including simple attributes like packed length, source or destination IP address or port, as well as more complex attributes that, when combined, can examine the content of packets to catch particular attach scenarios. It should be noted that the more complex attributes are more likely to be provided in configurations supplied by the vendor than independently created and managed by Administrators.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 evaluation. Therefore the validation team concludes that the CygnaCom CCTL findings are accurate, and the conclusions justified.

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 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 desiring a security evaluation contract with a CCTL pay a fee for their product's NIAP 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; and
- 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
Target of Evaluation	Radware APSolute OS Version 1.0 (SynApps version 3.402151)
Installed on Models	WSD v8.21.04, DP v1.32.11
Security Target	*Radware APSolute OS Version 1.0 Security Target*, Version 2.3, February 17, 2006.
Protection Profiles	N/A
Evaluated Hardware	DefensePro Web Server Director
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation Radware APSolute OS Version 1.0*; Version 2.3, February 17, 2006.
Conformance Result	CC Part 2 extended, CC Part 3 conformant, EAL 3
Sponsor	Radware
Common Criteria Testing Lab (CCTL)	CygnaCom/Entrust 7925 Jones Branch Drive Suite 5200 McLean, VA 22102-3321

Item	Identifier
CCEVS Validator(s)	Scott Shorter, Orion Security Solutions James Donndelinger, Aerospace

Security Policy

The security policy enforced by the TOE consists of the *SynApps Application Security SFP* that determines whether traffic is permitted to be passed through the appliance. Based on that policy, the TOE shall permit or deny external IT entities to pass traffic from one group of physical ports to another group of physical ports based upon the following security attributes:

- Source IP address,
- Destination IP address,
- Direction (one way or two way filtering),
- IP Fragment Offset Field,
- Packet total length,
- Protocol,
- Bit pattern,
- Text pattern,
- Destination port, and
- Source port.

The flow shall be permitted if no policy rule has been established to deny the information flow, and all security attribute values are unambiguously permitted by the information flow security policy rules, as created by an Administrator.

1. Receipt of a network datagram matching an atomic condition specified by an administrator.
2. Receipt of a network datagram matching a conjoined condition specified by an administrator, and
3. Receipt of a network datagram matching any atomic or conjoined condition in a named group of conditions specified by an administrator.
4. Receipt of sequence of network datagrams where:
    a. Each datagram in the sequence matches the same condition specified by an administrator,
    b. Number of datagrams in the sequence exceeds a threshold set by an administrator, and
    c. Sequence of datagrams is received within a time interval set by an administrator.

Where the conditions that may be specified by the administrator are:

1. For all network datagrams:
    a. Source IP address of network datagram, which matches event when the address is in a range specified by an administrator
    b. Destination IP address of network datagram, which matches an event when the address is in a range specified by an administrator
    c. Direction of network pattern (i.e. one-way or two-way)
2. For all atomic conditions:
    a. Optionally, Protocol of network datagram, which matches event protocol specified by an administrator (one of IP, ICMP, TCP, or UDP),
    b. Optionally, a Bit pattern contained within network datagram, which matches an event when
        i. The bit pattern appears within the datagram at a location specified by an administrator (location is specified by base, offset, and pattern length)

ii. After applying an administrator-specified mask, the bit pattern meets a condition specified by an administrator (one of equal, notEqual, greaterThan, or lessThan)

c. Optionally, but exclusive of “b” above, Text pattern contained within network datagram, which matches an event when

i. The text pattern appears within the datagram within locations specified by an administrator (locations are specified by starting offset within network packet and maximum length of content)

ii. The text pattern matches the type specified by an administrator (type is one of Text, Regular Expression, HTTP types, or SMTP types)

1. HTTP types are: URL, Host name, HTTP header field, Header Type, File Type, and Cookie Data
    a. Header type equals a field value
    b. HTTP cookie equals a cookie value
    c. Or not applicable
2. SMTP types are: Mail Domain, Mail To, Mail From, and Mail Subject

iii. The text pattern matches a pattern specified by an administrator including

1. Encoding of text pattern (one of none, case sensitive, case insensitive, HEX, or international),
2. Character set of specified pattern

3. For atomic conditions on TCP streams and UDP datagrams:
    a. Source port of network datagram, which matches an event when the port is in a range specified by an administrator,
    b. Destination port of network datagram, which matches an event when the port is in a range specified by an administrator,
4. For conjoined conditions:
    a. Network datagram, which matches when it matches all of the atomic conditions that comprise the conjoined condition.

Furthermore, the TOE shall explicitly deny an information flow based on the following rules:

1. IP Packets encapsulating a fragmented URL request must contain a minimum URI size of at least 50 bytes long.
2. IP Packets encapsulating a URL request must contain a URL size of no more than 500 bytes long.
3. Fragmented packets must be at least 512 bytes long.

Assumptions

The following assumptions were made in the Security Target:

- The TOE Administrator will install, configure, and operate the TOE according to the instructions provided by the TOE documentation and that administrators are not malicious.
- The Radware appliance, the Management Station, and the connection between the Radware appliance and the Management Station will be located in a controlled access facility that prevents unauthorized physical access.

The validators consider these assumptions to be reasonable for the operational environments to which this product is targeted. The nature of network equipment is consistent with trusted administrators and physical protection.

Architecture

The SynApps module consists of a single subsystem, which performs audit and policy enforcement. Audit functions include generating alarms and complex attack heuristics. Policy enforcement functions include information flow control and security management. The policy enforcement functions require support from the Radware Appliance Software Application for policy configuration by the administrator. The CLI supports the Administrator in setting filters, filter groups, and policies.

Figure 1 shows the TOE (shaded grey) in the context of the overall Radware appliance that forms the IT Environment of the TOE (white).

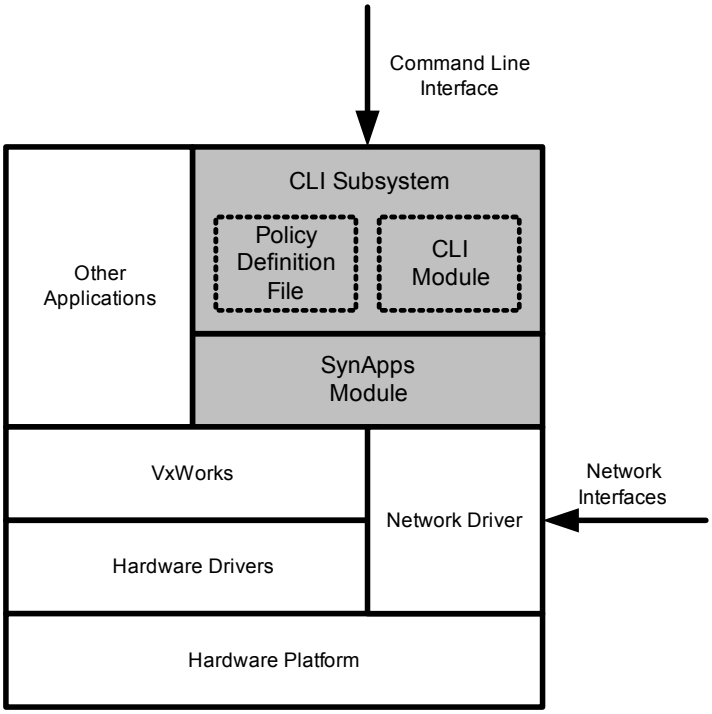

Figure 1 - TOE Architecture

The Radware appliance consists of a physical hardware platform with platform specific hardware drivers, running a VxWorks operating system. A set of RJ-45 and Small Form-factor Pluggable

(SFP) ports provide network interfaces, although only the RJ-45 ports were used in the evaluated configuration.

SynApps Module

The SynApps module is the component that enforces the TOE's security policy at run-time. The SynApps Module reads the Policy Definition File via the VxWorks OS interface, and that forms the basis of the security policy used by the SynApps Module. The IT Environment ensures information from one group of physical ports to another cannot bypass the SynApps module, therefore the security policy is applied to all information flowing through the appliance. The NIC drivers are linked directly to the SynApps module by use of callback functions, and the SynApps module then forwards traffic, when permitted by policy, via calls to the NIC drivers.

It should be noted that the information flow security policy is applied at the level of Ethernet frames received directly from the NIC drivers – IP datagrams are not assembled, nor is any state retained beyond that required to determine if a condition's threshold has been met. The Radware appliance also does not further fragment Ethernet frames – if they are permitted, they pass unchanged.

In addition to the traffic filtering capabilities, the SynApps module also supports security alarms based on a configurable threshold of traffic filtering events. These security alarms are displayed on the console and stored in an internal alert table that may be displayed via the CLI, and may optionally be transmitted as SNMP alerts or syslog records.

Command Line Interface Subsystem

The Command Line Interface subsystem consists of two modules, the CLI module and the Policy Definition File. The CLI is accessed via a serial port connection, and is used to configure the SynApps Module (via the Policy Definition File), to review the alert table, and to display alerts as they occur.

Commands may be entered via the CLI to create atomic conditions, conjoined conditions, and groups of conditions per the security policy, and to set the thresholds of the detection of those conditions that will result either in the traffic flow being denied or security alarms being raised. Errors in command line syntax will result in reasonably intelligible messages being returned to the users, so misconfiguration will not occur without some warning.

Documentation

The following documentation is provided to the consumer along with the product:

- Radware APSolute OS WSD Pro/WSD Pro+/WSD Pro AS WSD-DS/WSD-NP User Guide
- Radware APSolute OS DefensePro User Guide
- Radware APSolute OS Addendum for Installers for the Evaluated Configuration

As there are no non-administrative users of the TOE, all of the above documents are considered administrator guidance, and were evaluated as such. The documents were found to have sufficient information for an Administrator to properly manage the TOE, and to configure it in the evaluated configuration. The Addendum describes the Command Line Interface, supplemented by the users guides.

The CLI is described in terms of the commands that can be used to manage the TOE, the security attributes that can be set in each of those commands, valid values for those security attributes, and the effects of the commands.

IT Product Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

In particular, developer testing contained the following types of tests:

- Confirmation of the proper behavior of the SynApps Application Security SFP, by configuring the TOE to block traffic based on each of the available security attributes, and attempting to pass traffic matching the profile of the configuration and traffic that does not match the profile, to confirm that the rule is working properly. For example:
    - Block traffic to a particular IP address
    - Block traffic from a particular source port
    - Prior tests, with a threshold added, e.g. block the traffic after the third attempt
    - Block traffic based on content based attributes, such as content encoding, content data/mask/offset, content max length, etc.
- Confirmation of the proper behavior of the security alarm complex attack heuristics, by configuring the TOE to initiate security alarms in response to each of the available security attributes and observing that security alarms are generated as expected. Security alarms were observed as console messages, alert table records, and syslog messages.
- Confirmation of the proper management capabilities of the TOE was captured in the course of the same testing, as the CLI was exercised with a wide range of commands and security attributes in different configurations in the course of setting up the TOE for each test.

The above list is not intended to be comprehensive, but merely representative.

The validator witnessed the testing, and considered the testing to comprehensively cover the different attributes that compose the information flow control policy.

Evaluated Configuration

The evaluated configuration of the TOE consists of the Web Server Director Application Switch II (version WSD v8.21.04) and DefensePro Application Switch III (version DP v1.32.11), configured according to the guidance *Radware APSolute OS Addendum for Installers for the Evaluated Configuration*. The evaluated configuration includes a management station that exercises the TOE's administrative interface (CLI) via a console port interface. Although Administrator authentication is not included in the claimed TOE functionality, the TOE configuration excludes remote administrator authentication. The evaluated configuration did not include any enabled hardware accelerators or high bandwidth fiber connections.

The test bed environment used for product testing consisted of a client machine, server machine, and audit server running syslogd, in addition to the TOE operating in evaluated configuration.

Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

CygnaCom Solutions has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 3. A team of validators, on behalf of the

CCEVS Validation Body, monitored the evaluation. The evaluation was completed in February 2006.

Validator Comments

The evaluated configuration of the TOE is a useful and usable product that provides traffic filter and security alarm capabilities. The omission of remote administration does make for a product that is more challenging to administer (a dedicated administrative workstation, physically connected to the TOE, is required for the evaluated configuration), but it does not impact the overall security.

As witnessed during testing, the CLI management interface is somewhat cumbersome, however that is probably a necessary consequence of not permitting the HTTP based GUI management interface available beyond the evaluated configuration. An experienced administrator should be able to use the CLI with relative ease after a period of familiarization with the product.

The vulnerability analysis did not find any issues that could not be addressed by operating the TOE in accordance with the evaluated configuration and CC addendum instructions. The search for security vulnerabilities of similar products in public databases did not turn up any problems, however since the TOE is not a product that can be neatly categorized as a switch or a firewall, perhaps the limited number of similar products may result in a relatively shallow level of knowledge of such products in the public databases.

Note that remote administration and other non-evaluated functionality were left out of the evaluated product to simplify the evaluation process. Furthermore because I&A of administrators was relegated to the IT Environment, that mechanism was not tested (although it was of course exercised in the course of testing.) In addition, because administrator actions are not audited, there is no individual accountability for management activities.

Due to the reduced scope of the evaluation, end-users should be aware of the possibility of potential vulnerabilities in the IT Environment of the TOE. For example, they should test to see what services are available to VxWorks and determine whether they pose a risk in their environment.

Security Target

Radware APSolute OS Version 1.0 Security Target, Version 2.3, February 17, 2006.

Bibliography

The validation team used the following documents to prepare the validation report.

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.
3. Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.
4. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.
5. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.
6. Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

7. Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, Radware APSolute OS Version 1.0, Security Target version 2.3, ETR Version 2.3, February 17, 2006
8. Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Radware APSolute OS Version 1.0, Security Target version 2.3, ETR Version 2.3, February 17, 2006
9. Test Plan and Report, EAL 3 Evaluation, Radware SynApps version 3.402151, Version 1.4, December 28, 2005
10. Radware APSolute OS Version 1.0 Security Target, Version 2.3, February 17, 2006.
11. Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.