Certification Report

EAL 2

Evaluation of

Arbor Networks, Inc.

Pravail APS
2100 Series Appliances
Version 5.4

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	***10.04.2014***
Version of Report	***1.0***
Author	***Kerem KEMANECİ***
Technical Responsible	***Mustafa YILMAZ***
Approved	***Mariye Umay AKKAYA***
Date Approved	***10.04.2014***
Certification Number	***21.0.01/14-008***
Sponsor and Developer	***Arbor Networks, Inc.***
Evaluation Lab	***Cygnacom Solutions***
TOE	***Arbor Networks Pravail Availability Protection System (APS) 2100 series appliances v5.4***
Pages	***24***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
V 0.1	***08.04.2014***	***All***	***Initial***
V 1.0	***10.04.2014***	***All***	***Final***

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1,revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision. CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by Cygnacom Solutions, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Arbor Networks Pravail Availability Protection System (APS) 2100 series appliances (product version: v5.4) whose evaluation was completed on 07.04.2014 and whose evaluation technical report was drawn up by Cygnacom solutions (as CCTL), and with the Security Target document with version no V 2.0 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

Evaluated IT Product Name: Arbor Networks Pravail Availability Protection System (APS) 2100 series appliances v5.4

Developer: Arbor Networks, Inc.
Name of CCTL: Cygnacom Solutions
Assurance Package: EAL 2
Completion Date of Evaluation: 07.04.2014

The Target of Evaluation (TOE) is Arbor Networks Pravail Availability Protection System (APS) 2100 Series appliances. The Pravail APS secures the Internet data center's edge from threats against availability — specifically from application-layer, distributed denial of service (DDoS) attacks. The appliance is a single, stand-alone device that deploys at ingress points to an enterprise to detect, block, and report on key categories of Distributed Denial of Service (DDoS) attacks.

In addition to the detection and mitigation of DDoS attacks, the appliance provides security audit, enforcement of identification and authentication before providing access, role based security management, protection of the TSF, and requires secure communications for remote management capabilities.

The Pravail APS appliance is bypass capable. If power failures, hardware failures, or software issues affect the Pravail APS appliance, the network traffic can pass through the appliance unaffected.

The following network connectivity models describe the options for connecting Pravail APS within a network.

Pravail APS can be connected in the following ways:

- Inline with or without mitigations enabled (inline mode)
- Out-of-line through a span port or network tap, with no mitigations (monitor mode)

In monitor mode, Pravail APS is deployed out-of-line through a span port or network tap, which collectively are referred to as monitor ports. The router or switch sends the traffic along its original path and also copies, or mirrors, the traffic to Pravail APS. Pravail APS analyzes the traffic, detects possible attacks, and suggests mitigations but it does not forward traffic.

In an inline deployment, Pravail APS acts as a physical cable between the Internet and the protected network. All of the traffic that traverses the network flows through Pravail APS. Pravail APS analyzes the traffic, detects attacks, and mitigates the attacks before it sends the traffic to its destination.

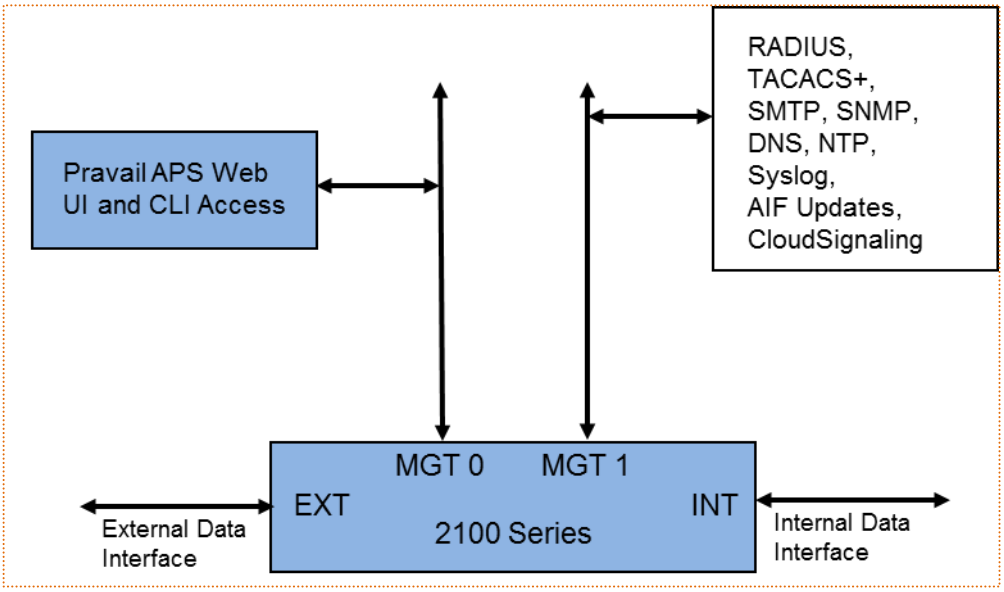


Figure-1: TOE Physical Boundary (Blue components)

The physical boundary of the TOE is the entire appliance. The appliance was evaluated in the "inline mode" deployment scenario.

Included in the TOE:
The scope of the evaluation includes the following product components and/or functionality:
Pravail APS 2100 Series Appliances (APS 2104, APS 2105, APS 2107, APS 2108) and its user interfaces:

- Pravail APS Web UI
- Pravail CLI

TOE major security features for operational use:

Security Audit: The TOE's auditing capabilities include recording information about system processing and users' access to the TOE. Subject identity (user login name) and outcome are recorded for each event audited. The audit records generated by the TOE are protected by the TOE. The audit trail is comprised of the Pravail APS Change Log and the syslog.

The audit records can be offloaded for long term storage via syslog interface.

Identification and Authentication: Each user must be successfully identified and authenticated with a username and password by the TSF or the external authentication mechanism invoked by the TOE before access is allowed to the TSF. The TOE provides a password based authentication mechanism to administrators.
Access to security functions and data is prohibited until a user is identified and authenticated.

Security Management: The TOE allows only authorized users with appropriate privileges to administer and manage the TOE. Only authorized administrators with appropriate privileges may

modify the TSF data related to the TSF, security attributes, and authentication data.

The TOE maintains 3 default roles: Admin (Read, Write, & Execute all), User (read-only access from Web UI and limited CLI commands), and None (which is used to lock out users that may have valid accounts on external authentication mechanism).

Resource Utilization (DDoS Protection): The TOE sits at the perimeter of the network, referred to as the edge, to protect Internet Protocol (IP) networks against DDoS attacks by successfully identifying and filtering DDoS attacks, while forwarding normal traffic through the network without impacting service. The TOE can function in ACTIVE (filtering), INACTIVE (monitoring), BYPASS (no filtering, no monitoring) modes. The TOE provides capabilities to filter traffic by multiple means. These means include filtering on Whitelist, Blacklist, Fragmentation Control, Rate Limits, malformed HTTP, and TCP SYN Rate configuration specifications to name a few.

Visual alerts Web UI users and notices can be configured to warn the recipient of an event or action that has taken place. The formats can take the form of an email, SNMP trap, or syslog message.

Protection of TSF: The TOE transfers all packets passing through the TOE only after processing the traffic based on traffic attributes. If a hardware failure occurs and the Platform does not repair itself, the Platform goes into a hardware bypass mode. This shunts the "ext#" and "int#" ports, maintaining all traffic flow through the equipment. Thus, the DDoS filtering function may be unavailable, but the flow of traffic will not be impeded. The communication between the remote manager and Platform are protected from disclosure and modification. The TOE provides reliable timestamps on its own or with the support of an NTP Server in the IT environment.

The TSF is protected because the hardware, the OS and the application are part of the TOE and there in a protected physical environment. The logical access to the TOE is controlled by the identification and authentication functionality provided by the TOE.

Trusted Channel/Path: The Pravail APS requires the establishment of an HTTPS (SSL/TLS) connection from the remote administrator's browser. HTTP is not supported.

The Pravail APS also requires the establishment of an SSH connection in order to access the TOE remotely to use the CLI. Telnet is disabled by default.
The TOE communicates with external authentication mechanisms via trusted channel. The TOE provides a communication channel between itself and the external authentication mechanisms that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

TOE configuration conditions for evaluation:

- Inline Mode
- Telnet must not be turned on for remote management.
- Default passwords must be changed during installation.
- No customized groups (roles)

Excluded from the TOE:
The following assets are included in the IT Environment and are not part of the TOE:

- Optional NTP Server (highly recommended for enterprise time synching)
- Optional DNS Server (highly recommended for simplification of configuration and reading reports, reading host names vs just IP addresses)
- Optional SNMP browser/Server (for notifications and management polling of appliance)
- Optional SMTP Server (for notifications)
- Optional Syslog Server (for notifications and syslog offload for central storage and management)
- Web browser (and its host platform) are not included in the TOE boundary
- Optional External authentication mechanisms supported by TOE: RADIUS, TACACS+ servers
- The network assets communicating on the network proving data flow through the TOE
- ISP or MSSP used for Cloud-Signaling Mitigation
- Pravail's AIF Update Server

The following functionality is not included in the scope of the evaluation:

- Pravail APS Programmable API
- Integration with another separately available product from Arbor Networks called vInspector. The vInspector appliance is an SSL proxy that deploys transparently with no changes required to clients or other network equipment. The vInspector provides decrypted plaintext flows to Pravail APS for inspection.

2100 Series Platform

The Platform is a hardware appliance with embedded Pravail APS software. It is available in 2104, 2105, 2107, 2108 Models. Each series is available with copper Ethernet, single-mode fiber, and multi-mode fiber interfaces.
A hardened Linux (RHEL6 kernel) is used for the operating system of the APS appliance. All Open Source software is in source control of Arbor Networks and is compiled by Arbor Networks.
The table below presents common environmental considerations among all of the models.

Power Options	**Environmental**
600W AC or DC hot-swap, redundant power supplies with PMBus support. The use of the second power supply is optional.	Temperature, operating: 50º to 95ºF (10º to 35ºC)
	Temperature, non-operating: -40º to 158ºF (-40º to 70ºC)
AC: 100 to 127 VAC, 50 to 60 Hz, 6 A max	Humidity, operating: 5% to 85%
200 to 240 VAC, 50 to 60 Hz, 3 A max	Humidity, non-operating: 95%, non-condensing at temperatures of
DC: -48 to -60 VDC, 13 A Max	73º to 104ºF (23º to 40ºC)
Physical Dimensions	**Compatibility: Monitoring**
Chassis: 2U rack height	Integrates with management consoles supporting SNMP v2 or SNMP V3
Height: 3.45 in (8.76 cm)	**Compatibility: Web-based UI**
Width: 17.4 in (43.53 cm)	• Firefox ESR 17 • Internet Explorer 9 • Firefox 21 • Internet Explorer 10 • Safari 6 • Google Chrome 27
Depth: 24 in (61 cm)	
Weight: 41 lbs. (18.5 kg)	

The table below presents a comprehensive description of the similarities and differences between the Platform types.

APS 2100 Series	**Model APS 2104**	**Model APS 2105**
Memory	24 GB	24 GB
Inspected Throughput	Up to 2 Gbps	Up to 4 Gbps
HTTP(s) Connections per Second	368K at recommended protection level; 613K filter list only protection	368K at recommended protection level; 613K filter list only protection
Processor	2 Intel Xeon CPU	2 Intel Xeon CPU
Protection Interface Options	• 12 x 10/100/1000 BaseT Copper	• 12 x 10/100/1000 BaseT Copper
	• 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber	• 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber
	• 12 x GE SX Fiber	• 12 x GE SX Fiber
	• 12 x GE LX Fiber	• 12 x GE LX Fiber
	• 4 x 10 GE SR Fiber	• 4 x 10 GE SR Fiber
	• 4 x 10 GE LR Fiber	• 4 x 10 GE LR Fiber
Bypass Options	• Integrated hardware bypass	• Integrated hardware bypass
	• Internal “software” bypass to pass traffic without inspection	• Internal “software” bypass to pass traffic without inspection
APS 2100 Series	**Model APS 2107**	**Model APS 2108**
Memory	24 GB	24 GB
Inspected Throughput	Up to 8 Gbps	Up to 10 Gbps
HTTP(s) Connections per Second	368K at recommended protection level; 613K filter list only protection	368K at recommended protection level; 613K filter list only protection
Processor	2 Intel Xeon CPU	2 Intel Xeon CPU
Protection Interface Options	• 12 x 10/100/1000 BaseT Copper	• 12 x 10/100/1000 BaseT Copper
	• 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber	• 4 x 10/100/1000 BaseT Copper, 4 x GE SX Fiber, 4 x GE LX Fiber
	• 12 x GE SX Fiber	• 12 x GE SX Fiber
	• 12 x GE LX Fiber	• 12 x GE LX Fiber
	• 4 x 10 GE SR Fiber	• 4 x 10 GE SR Fiber
	• 4 x 10 GE LR Fiber	• 4 x 10 GE LR Fiber
Bypass Options	• Integrated hardware bypass	• Integrated hardware bypass
	• Internal “software” bypass to pass traffic without inspection	• Internal “software” bypass to pass traffic without inspection

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	***TSE-CCCS-020***
TOE Name and Version	***Arbor Networks Pravail Availability Protection System (APS) 2100 series appliances v5.4***
Security Target Document Title	***Arbor Networks ST***
Security Target Document Version	***2.0***
Security Target Document Date	***10.03.2014***
Assurance Level	***EAL 2***
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
Methodology	• Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4
Protection Profile Conformance	***None***
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
Sponsor and Developer	***Arbor Networks, Inc***
Evaluation Facility	***Cygnacom Solutions***
Certification Scheme	***Turkish Standards Institution*** ***Common Criteria Certification Scheme***

2.2 Security Policy

The TOE does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. The consumers who plan to use the product should consider the **assumptions** below.

BACK UP	Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.
CONNECT	The TOE will separate the network on which it is installed and operates into external and internal networks. Information cannot flow between the external and internal networks without passing through the TOE.
NOEVIL	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, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
PHYSICAL	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

TOE is evaluated to meet all assurance requirements to provide security against Basic Level (EAL2) attackers with the scope of the **threats** listed below:

AUDIT	Unauthorized attempts by users and external IT entities to access network resources through the TOE, TOE data or TOE security functions may go undetected because the actions they conduct are not audited or audit records are not reviewed, thus allowing an attacker to escape detection.
DDoS ATTACK	An External IT Entity or group of External IT Entities may exhaust service resources of the TOE or Internal IT Entities by passing information flows through the TOE by DDoS attacks thus making the resources unavailable to its intended users.
FAILURE	A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable.
MANAGE	An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE
NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as

to access and use security functions and/or non-security functions provided by the TOE.

PROCOM An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

2.4 Architectural Information

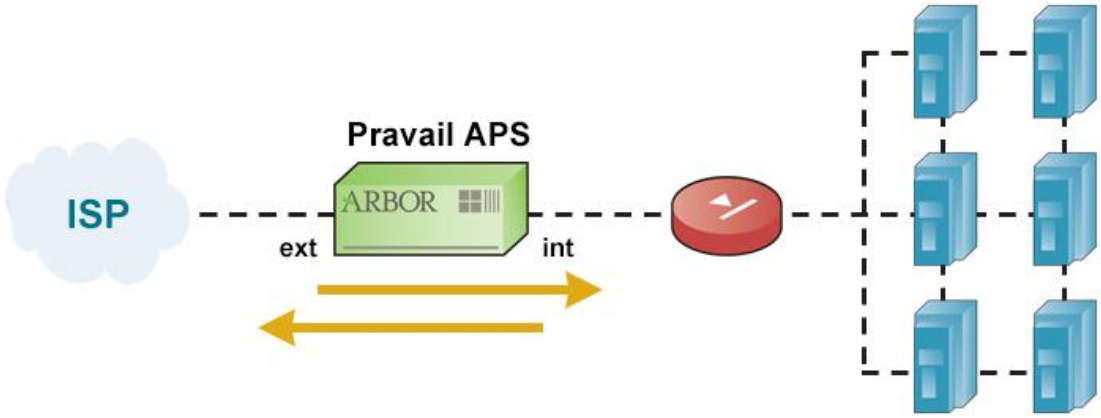


Figure-2: Inline Mode Deployment (Evaluated configuration)

In an inline deployment, Pravail APS acts as a physical cable between the Internet and the protected network. All of the traffic that traverses the network flows through Pravail APS. Pravail APS analyzes the traffic, detects attacks, and mitigates the attacks before it sends the traffic to its destination.

In an inline deployment, Pravail APS and two Ethernet cables directly replace an existing Ethernet cable. An Ethernet cable from an upstream router or the service provider's equipment is connected to an “ext” interface on Pravail APS. The matching “int” interface on Pravail APS is connected to the downstream network equipment. Usually, this network connection is an Internet-facing port on a firewall, but it could be a router or a switch.

The typical network scenarios for the TOE are shown below.

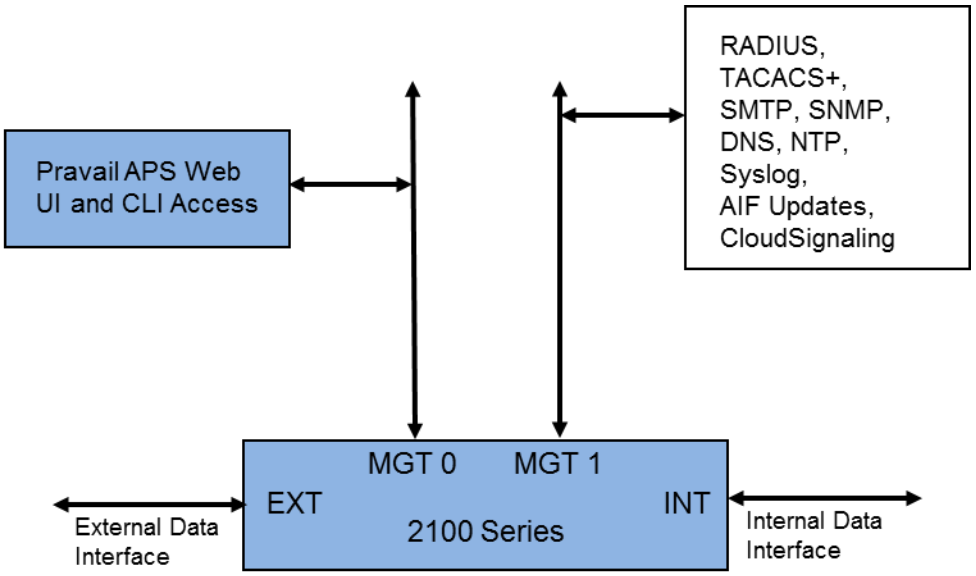


Figure-3: Typical Configuration of TOE (Blue) Ethernet interfaces

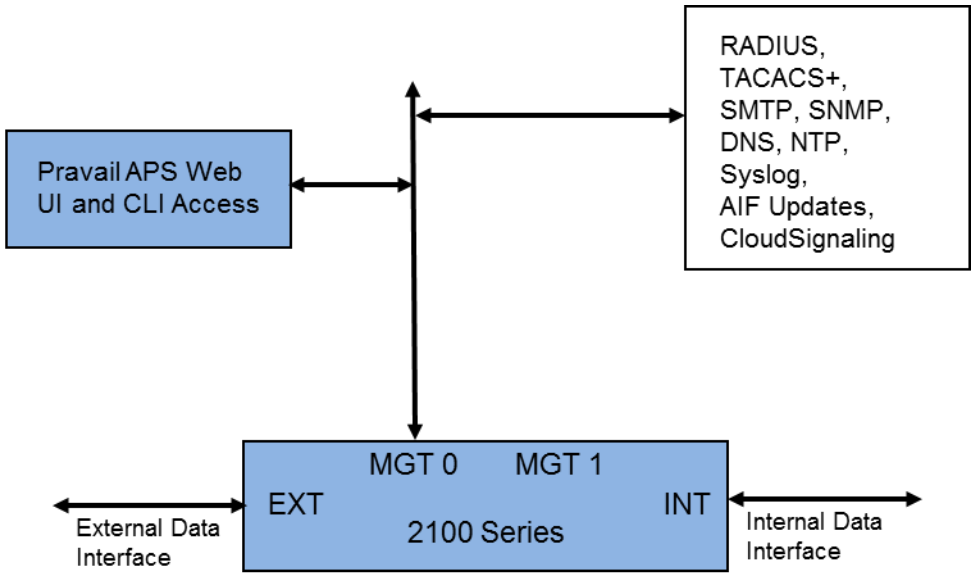


Figure-4: Typical Configuration of TOE (Blue) Ethernet interfaces

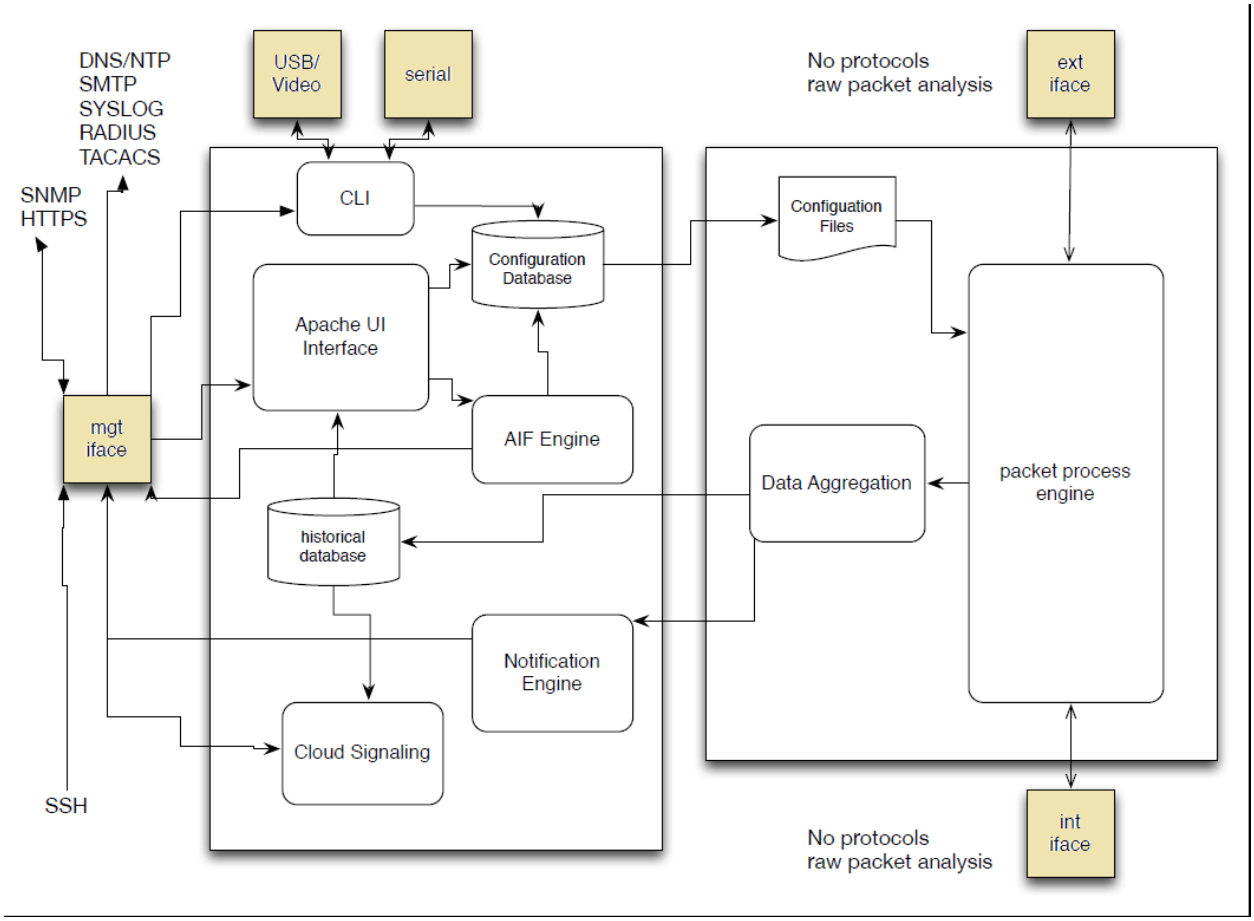


Figure-5 : Pravail APS Component Subsystems

The two larger boxes represent the 2 domains of the TOE: Management domain (box on the left) and Network domain (box on the right). The TOE resides on the OS which is considered as another subsystem itself.

The Management domain includes the following subsystems:

1. CLI
2. Apache UI
3. Cloud Signaling
4. Notification Engine
5. AIF Engine
6. Configuration Database.
7. Historical Database

The physical Ethernet interfaces (shown by the shaded boxes)

- Management Interface (mgmt. iface)
- Serial Interface
- USB/Video interface

The Network domain includes the following subsystems

1. Configuration files
2. Data Aggregation
3. Packet Process Engine
4. The physical Ethernet interfaces (shown by the shaded boxes)

    - External Interface (ext iface)
    - Internal Interface (int iface)

Pravail APS Web UI

The main administrative interface after the TOE has been installed is a web based UI that is access by connecting to the Pravail APS and successfully authenticating. The Pravail APS Web UI uses the HTTPS protocol for secure sessions over one of the two Management LAN (port mgt0 or mgt1) connections. This is not available through the "int" or "ext" interfaces. The certificate is based on Arbor Networks' Certificate Authority (CA); however, the TOE can be configured to use the end-user's enterprise certificate. The first time Pravail APS is accessed, the user must accept the SSL certificate to complete the secure connection.

The Web UI menu bar indicates which menu is active and provides the ability to navigate the Web UI menus and pages. The menus that are available depend on the user group to which the authorized user is assigned.

The menu bar is divided into the following menus:

Menu Bar of Pravail APS Web UI

Menu	Description
Summary	Displays the current health of Pravail APS and provides traffic forensics in real time.
Explore	Displays information about the traffic that Pravail APS monitors and mitigates.
Protection Groups	Provides ability to view, configure, and manage protection groups.
Administration	Provides the functions to configure and maintain Pravail APS

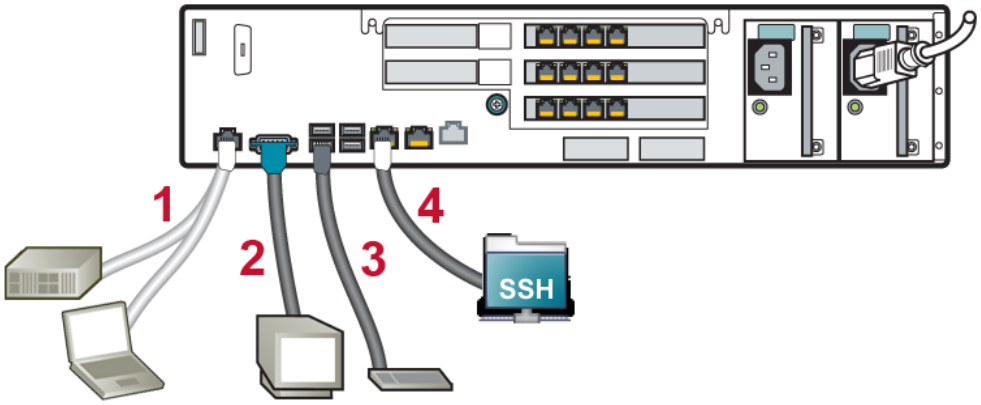
The Platform is self-running and does not require operator intervention to perform DDoS filtering functions. The Web UI displays multiple views of network traffic and DDoS attack statistics.

Command Line Interface

The command line interface (CLI) allows the authenticated user to enter commands and navigate through the directories on the Pravail APS appliance. Typically, the CLI is used for installing and upgrading the software and completing the initial configuration. However, some advanced functions can only be configured by using the CLI.

The Pravail APS appliance can be connected to either directly or remotely. The following figure shows the options and ports that can be used to connect to the appliance in order to access the CLI.

Figure: Options for connecting to the CLI



The following table describes the connections in the figure:

Connection Options

Item	Connection
1	Serial port with either of the following options (but not both):
	- Serial console server
	- Computer (HyperTerminal)
2	VGA connector with monitor (direct connection)
3	USB port with keyboard (direct connection)
4	Management port mgt0 or mgt1 with SSH or Telnet*+

The boot commands are not available when connected through SSH or Telnet*.
Telnet should not be used in a secure environment. By default the Pravail APS appliance is configured
to only allow SSH connections.

The CLI functionality is limited to:

- Starting and Stopping Pravail APS services (services aps *stop/start*)
- Configuring the authentication mechanism and precedence order
- Viewing Pravail APS configuration (show)
- Setting the Pravail APS License (system license set Pravail *license number*, system license show)
- Setting the System Clock (clock set)
- Setting the Deployment Mode (services aps mode set *inline/monitor*)
- Stopping and Starting the NTP Service (services ntp *stop/start*)
- Advance File Management (system file *copy*, *delete*, *rename* : used for manual updating TOE)
- Configuring Interface Speed and Duplex Mode (ip interfaces media speed options, ip interfaces show, ip interfaces ifconfig *ipaddr* ,*netmask*, *prefix*, and *IP tee*). Note: IP tee is disabled by default and should not be enabled in the evaluated configuration unless required

for integrating the TOE with another Arbor Product.

2.5 Documentation

Document list for customers:

- Arbor Networks ST V2.0
- Arbor Networks Delivery Procedures v1 0__Mar 4-2014
- Arbor Security Architecture Description_V1 0 03-04-2014
- EAL2_ADV_FSP 2 Arbornet v1 0 03-04-2014 (Functional Specification)
- EAL2_ADV_TDS Arbornet v1 0 03-04-2014 (TOE Design)
- Pravail_APS_5.4_User_Guide_English
- Pravail_APS_2100_Quick_Start_Card
- Pravail_APS_5.4_Release_Notes
- Pravail_APS_2100_Mixed_Interface_Quick_Start_Card

2.6 IT Product Testing

Developer Tests:
The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. The test cases were written by the developers or chosen from an existing set of QA tests to exercise the security functionality of the TOE. These test cases were mapped by the evaluator to the SFRs and TSFIs, listed in the [ST] and [FSP].

Test scenarios, expected results and obtained results are listed by Arbor's testers. For each test, expected results are same with obtained test results. Developer tests are explained in Pravail APS Developer Test Plan & Tests and Pravail APS Developer DDoS Tests in detail.

In all the developer submitted 17 test case files consisting of 191 sub-tests.

Evaluator Tests:
The evaluator ran a representative sample of the developer tests to show completeness of the test coverage. The sample included tests to exercise each security function and TSFI. The purpose of running this sample of the tests was to gain confidence in the developer's functional test results. The evaluator compared the results of each test with the corresponding expected results provided by the developer as ATE_FUN.1 evidence.

The evaluator reran 80 out of the 191 developer's QA sub-tests (approximately 42%).
All tests that were rerun by the evaluator passed. All results were visually verified by the evaluator on-site.

Evaluator Defined Tests:
The evaluator's strategy in developing the evaluator-defined tests for the TOE was to supplement the developer's functional tests and the penetration tests.

The evaluator-defined tests were devised to augment the developer's functional tests in order to exercise functionality in greater depth than the developer tests provided. Because of the extensive coverage of the vendor tests, the following five evaluator-defined tests were defined and run to cover functionality not exercised in the vendor tests.

Penetration Tests:
The evaluator considered the following while performing the vulnerability analysis and developing penetration tests:

- All Evidence Deliverables – All evidence deliverables were considered for identifying potential vulnerabilities. An analysis of the design documentation identified no specific vulnerabilities.

- Public Sources – The evaluator performed an independent search for vulnerabilities available from public domains including the NVD and CVE databases. The evaluator also considered vulnerabilities from similar products from public sources. The evaluator will continue to monitor and analyze vulnerabilities until the close of the evaluation.

- TSF based analysis – All Security Functions, Security Functional Requirements and External Interfaces were considered.

- Subject to Threats – Threats considered included Bypass, Tampering, Direct Attacks and Misuse.

All results of the penetration testing were visually verified by the evaluator on-site. All penetration tests that were run by the evaluator passed.

2.7 Evaluated Configuration

The physical boundary of the TOE is the entire appliance. The appliance was evaluated in the "inline mode" deployment scenario. The scope of the evaluation includes the following product components and/or functionality:

Pravail APS 2100 Series Appliances (APS 2104, APS 2105, APS 2107, APS 2108) and its user interfaces:

- Pravail APS Web UI
- Pravail CLI

TOE configuration conditions for evaluation:

- Inline Mode
- Telnet must not be turned on for remote management.
- Default passwords must be changed during installation.
- No customized groups (roles)

The following components are in the Operational Environment and are included in the evaluated test configuration:

- NTP Server
- DNS Server
- SNMP Server
- SMTP Server
- Syslog Server
- Web browser (and its host platform)
- External authentication mechanisms supported by TOE: RADIUS, TACACS+ Servers
- The network assets communicating on the network proving data flow through the TOE
- ISP or MSSP used for Cloud-Signaling Mitigation
- Pravail's AIF Update Server

The CLI functionality is limited to:

- Starting and Stopping Pravail APS services (services aps stop/start)
- Configuring the authentication mechanism and precedence order
- Viewing Pravail APS configuration (show)
- Setting the Pravail APS License (system license set Pravail license number, system license show)
- Setting the System Clock (clock set)
- Setting the Deployment Mode (services aps mode set inline/monitor)
- Stopping and Starting the NTP Service (services ntp stop/start)
- Advance File Management (system file copy, delete, rename : used for manual updating TOE)
- Configuring Interface Speed and Duplex Mode (ip interfaces media speed options, ip interfaces show, ip interfaces ifconfig ipaddr ,netmask, prefix, and IP tee). Note: IP tee is disabled by default and should not be enabled in the evaluated configuration unless required for integrating the TOE with another Arbor Product.

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 2 as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is **PASS**. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to "BASIC LEVEL" attack potential attackers.

Assurance class	**Assurance components**	**VERDICT**
ADV: Development	ADV_ARC.1 Security architecture description	PASS
	ADV_FSP.2 Security enforcing functional specification	PASS
	ADV_TDS.1 Basic design	PASS
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS
	AGD_PRE.1 Preparative procedures	PASS
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage	PASS
	ALC_CMC.2 Use of a CM system	PASS
	ALC_DEL.1 Delivery procedures	PASS
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS
	ASE_ECD.1 Extended components definition	PASS
	ASE_INT.1 ST Introduction	PASS
	ASE_OBJ.2 Security objectives	PASS
	ASE_REQ.2 Derived security requirements	PASS
	ASE_SPD.1 Security Problem Definition	PASS
	ASE_TSS.1 TOE summary specification	PASS
ATE: Tests	ATE_IND.2 Independent testing sample	PASS
	ATE_FUN.1 Functional testing	PASS
	ATE_COV.1 Evidence of coverage	PASS
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of Arbor Networks Pravail Availability Protection System (APS) 2100 series appliances v5.4 product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the fallowing nomenclature:

Title: Arbor Networks ST
Version: V2.0
Date: 10.03.2014

4 GLOSSARY

CCCS:	Common Criteria Certification Scheme (TSE)
CCTL:	Common Criteria Test Laboratory (OKTEM)
CCRA	Common Criteria Recognition Arrangement
CEM:	Common Evaluation Methodology
CLI	Command Line Interface
DNS	Domain Name System
ETR:	Evaluation Technical Report
IT:	Information Technology
ISP:	Internet Service Provider
MSSP:	Managed Security Service Providers
NTP:	Network Time Protocol
STCD:	Software Test and Certification Department
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function
TSFI:	TSF Interface
SFR:	Security Functional Requirement
EAL:	Evaluation Assurance Level
Evaluator:	Cygnacom solutions
Developer:	Arbor Networks, Inc.
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
TSE	Turkish Standards Institutions
DDOS	Distributed Denial of Service attack
TACACS+	Terminal Access Controlller Access-Control System Plus
WEB UI	Web User Interface

5 BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
4. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4

5. YTBD-01-01-TL-01 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.