# Pravail APS

# 2100 Series Appliances

# Version 5.4

# Security Target

**Version 2.0**

**Mar 10, 2014**

**Prepared For**

ARBOR NETWORKS

**Arbor Networks, Inc.**
**76 Blanchard road**
**Burlington, MA 01803**
**http://www.arbornetworks.com/**

**Prepared By**

CYGNACOM SOLUTIONS

## Revision History

| Date | Version | Author | Description |
|---|---|---|---|
| 07/29/2013 | 0.1 | Herb Markle | First Draft |
| 8/8/2013 | 0.2 | Herb Markle | Input Arbornet Comments |
| 8/29/2013 | 0.3 | Herb Markle | Input Arbornet Comments round 2 |
| 9/23/2013 | 0.4 | Herb Markle | Input Arbornet Comments round 3 |
| 9/30/2013 | 1.0 | Herb Markle | Initial Submission |
| 12/27/2013 | 1.1 | Herb Markle | Updates per Eval/Val |
| 03/10/2014 | 2.0 | Herb Markle | Updated References |

## TABLE OF CONTENTS

## Table of Tables and Figures

**Table / Figure** **Page**

# 1 Security Target Introduction

## *1.1 Security Target Reference*

| | |
|---|---|
| **ST Title:** | Pravail APS 2100 Series Appliances, Version 5.4 Security Target |
| **ST Version:** | v2.0 |
| **ST Author:** | CygnaCom Solutions |
| **ST Date:** | Mar 10, 2014 |

## *1.2 TOE Reference*

| | |
|---|---|
| **TOE Identification:** | Pravail APS 2100 Series Appliances, Version 5.4 |
| **TOE Vendor:** | Arbor Networks, Inc. |

## *1.3 TOE Overview*

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.

*This Security Target (ST) defines the Information Technology (IT) security requirements for the TOE. The TOE is being evaluated at assurance level EAL2.*

### 1.3.1 TOE Type

The TOE is a Distributed Denial of Service (DDoS) detection and mitigation appliance.

## *1.4 TOE Description*

### 1.4.1 Acronyms

Table 1-1 and Table 1-2 define product specific and CC specific acronyms respectively.

**Table 1-1: Product Specific Acronyms**

| Acronym | Definition |
|---|---|
| **AAA** | Authentication, Authorization, & Accounting |
| **AIF** | ATLAS Intelligence Feed |
| **API** | Application Programming Interface |
| **APS** | Availability Protection System |
| **ATLAS** | Active Threat Level Analysis System |
| **CDN** | Content Delivery Network |
| **CIDR** | Classless Inter-Domain Routing |
| **CLI** | Command Line Interface |
| **CSV** | Comma Separated Value |
| **DDoS** | Distributed Denial of Service |
| **DNS** | Domain Name Server |
| **FCAP** | Flow Capture fingerprint expression language |
| **FQDN** | Fully Qualified Domain Name |
| **GUI** | Graphical User Interface |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **ICMP** | Internet Control Message Protocol |
| **ISP** | Internet Service Provider |
| **LAN** | Local Area Network |
| **MSSP** | Managed Security Service Provider |
| **NIC** | Network Interface Card |
| **NTP** | Network Time Protocol |
| **PPS** | Packets Per Second |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **RDN** | Registered Domain Name |
| **SIP** | Standard Initiation Protocol |
| **SMTP** | Simple Mail Transport Protocol |
| **SNMP** | Simple Network Management Protocol |
| **SSH** | Secure Shell |
| **SSL** | Secure Socket Layer |
| **TACACS+** | Terminal Access Controller Access-Control System Plus |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol |
| **TLS** | Transport Security Layer |
| **UDP** | User Datagram Protocol |
| **UI** | User Interface |
| **URL** | Uniform Resource Locator |
| **VoIP** | Voice over Internet Protocol |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |

### Table 1-2: CC Specific Acronyms

| Acronym | Definition |
|---|---|
| **CC** | Common Criteria [for IT Security Evaluation] |
| **EAL** | Evaluation Assurance Level |
| **IT** | Information Technology |
| **OSP** | Organizational Security Policy |
| **PP** | Protection Profile |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSFI** | TOE Security Functions Interface |
| **TSP** | TOE Security Policy |

### 1.4.2 Description

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.

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.

Pravail APS is available in several models and licensing options. The licensing options determine the maximum traffic rate that Pravail APS can accommodate.

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.

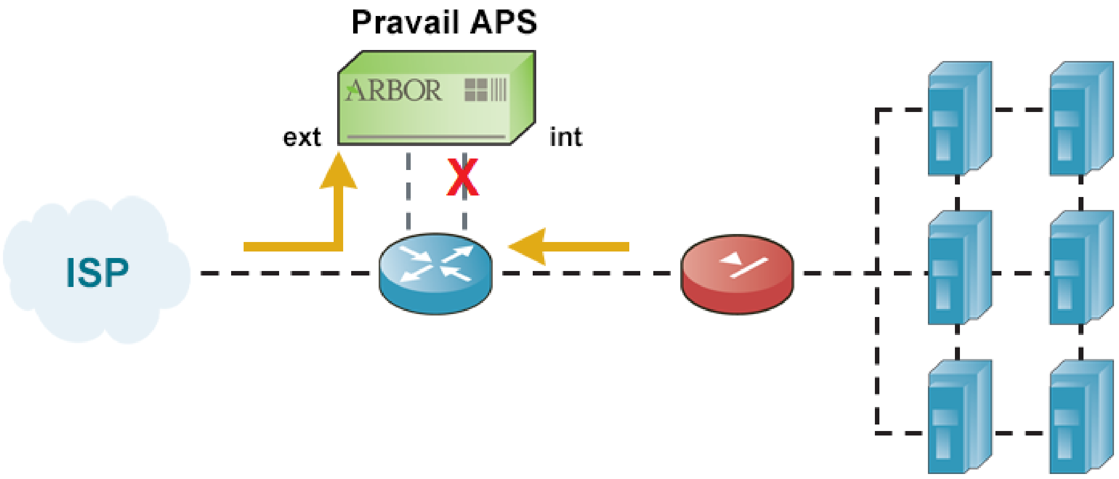
The monitor ports for the traffic that is received from the Internet are connected to the "ext" interfaces on Pravail APS. The network traffic is analyzed but no mitigation takes place. Because Pravail APS never forwards traffic in monitor mode, the mirrored traffic is not re-injected to the "int" port in the pair. The monitor ports for the traffic that is bound for the Internet is connected to the "int" interfaces if desired (connection not required). This internal traffic is blocked from going through the TOE and is not analyzed.

Monitor mode is most commonly used in trial implementations. For example, before deploying Pravail APS inline and allowing it to affect the enterprise network traffic, it can be deployed in monitor mode for evaluation purposes. The resulting information can be used to set the enterprise policies for attack detection and mitigation.

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.

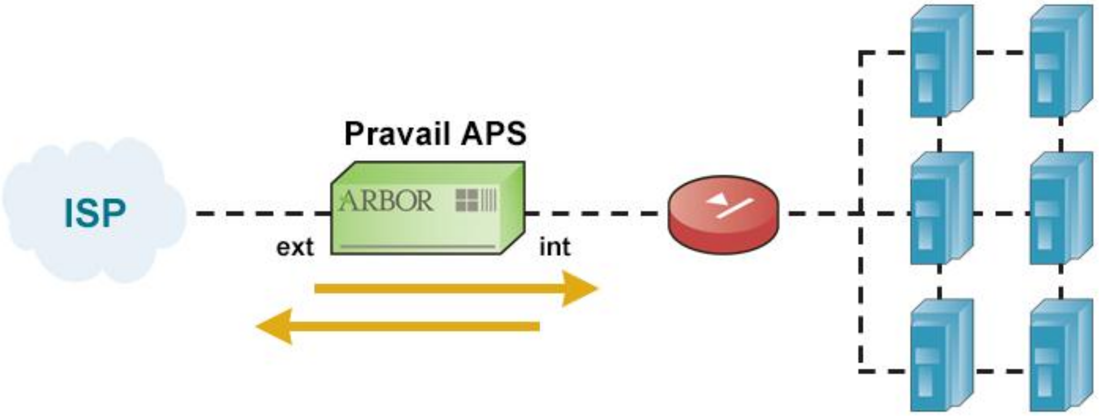
In an inline deployment, Pravail APS and two Ethernet cables directly replace an existing Ethernet cable. An Ethernet cable from an upstream router or the service provider's equipment is connected to an "ext" interface on Pravail APS. The matching "int" interface on Pravail APS is connected to the downstream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

**Figure 1-1: Monitor Mode Deployment**



Pravail APS inline mode can be operated in an “inactive” protection mode, in which it analyzes traffic and detects attacks without performing mitigations. The resulting information can be used to set/customize the APS policies for attack detection and mitigation. When the APS policy is ready for operational implementation, the administrator can change the protection mode to “active” and allow the APS to mitigate attacks.

**Figure 1-2: Inline Mode Deployment**



An additional option that Pravail APS supports is Cloud Signaling. Cloud Signaling is the process of requesting and receiving cloud-based mitigation of volumetric attacks in real time from an upstream service provider. In short, if the Pravail APS determines that thresholds for rate-based attacks are met, the TOE will signal the ISP or MSSP (via trusted channel) and the ISP or MSSP then mitigates the attack and then routes the cleaned traffic back to the protected network. To use this option the following conditions must be true:

- the end user must have an ISP or MSSP (Managed Security Service Provider) that supports cloud-based protection
- a purchase agreement with ISP or MSSP
- username / password used for the TOE to connect to the ISP or MSSP

### 1.4.2.1 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.

**Table 1-3: Pravail APS Appliance Common Features**

| **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<br>• Firefox 21 • Internet Explorer 10<br>• Safari 6 • Google Chrome 27 |
| Depth: 24 in (61 cm) | |
| Weight: 41 lbs. (18.5 kg) | |

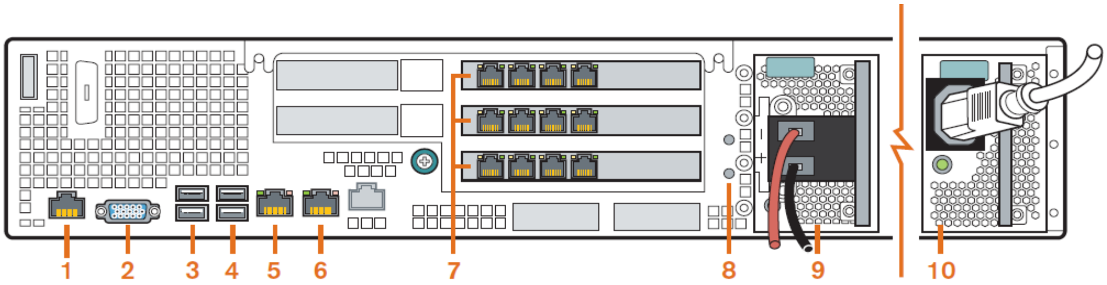
The table below presents a comprehensive description of the similarities and differences between the Platform types.

**Table 1-4: Pravail APS Model Comparison**

| **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 |

**Figure 1-3: Back panel of the Pravail APS appliance with 1G copper interfaces**



1 RJ45 Serial console port (Cisco pinouts)

2 VGA connector for a monitor

3 USB0 and USB1 (1 on the top, 0 on the bottom)

4 USB2 and USB3 (3 on the top, 2 on the bottom)

5 Management port 0, mgt0 (GbE NIC 1 connector)

6 Management port 1, mgt1 (GbE NIC 2 connector)

7 Protection ports (1G copper is shown) 1G and 10G Fiber are available
The protection ports are configured as port pairs. Each pair consists of an external (ext) port and an internal (int) port.

8 Two ground studs for DC-input system

9 Power supply 2 (DC module is shown; the -48V (-) terminal is on the top and the return terminal (+) is on the bottom)

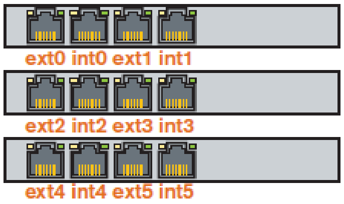
10 Power supply 1 (AC module is shown)
Both types of power supplies are shown for illustration purposes only. Each appliance has either two AC power supplies or two DC power supplies.

* The Pravail APS appliance might be different from this diagram, depending on the model that is purchased.

The following diagrams show how the protection ports are numbered for each of the available interfaces:

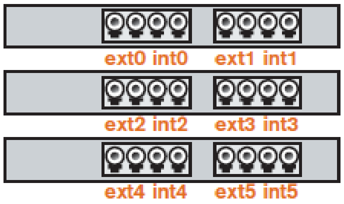
Interface panel, 1G copper

Contains 3 four-port copper NICs.



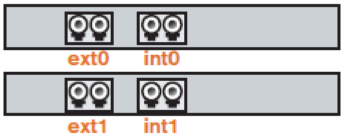
Interface panel, 1G fiber

Contains 3 four-port fiber NICs.



Interface panel, 10G fiber

Contains 2 two-port fiber NICs.



The network path to be protected is connected to any two like-numbered interfaces. The “ext” interface always faces an external Internet connection, and the “int” interface always faces the internal network, as shown in Figure 1-2: Inline mode Deployment. Do not send outbound traffic from the internal network to an “ext” interface. Pravail treats all traffic on “ext” interfaces as external.

### 1.4.3 User Description

User groups provide the means to organize Pravail APS users into different levels of permitted system access. When a user account is created, it must be assigned to a group. The owner of that account inherits the access levels that are assigned to that group once the owner has been successfully identified and authenticated. Pravail APS contains the following predefined groups.

**Table 1-5: Predefined user groups**

| Group | Access |
|---|---|
| system_admin | Users in this group have full read and write access on all pages of the Web UI and can run all of the command line interface (CLI) commands. |
| system_user | Users in this group have read-only access to most of the Web UI pages and can edit and update their own user account settings. They can log on to the CLI and run limited CLI commands. For example, they can view the status of the system.<br>Users in this group cannot change any settings. |
| system_none | Users in this group have no access to Pravail APS.<br>When the organization uses RADIUS or TACACS+ authentication, it is possible for all users who have an account on the authentication server to access Pravail APS. Use this group as the default to lock out the unwanted users, and then assign users who need to access Pravail APS to the other groups. |

This grouping of users into categories of privileges to restrict/permit TSF functionality is referred to in Common Criteria as “roles”.

The TOE does provide the ability to create customized roles via the command line interface. However, the CC evaluated configuration does not include customized roles only those “out-of-the-box” roles described in Table 1-5.

### 1.4.4 User Interfaces

#### 1.4.4.1 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:

**Table 1-6: 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 |

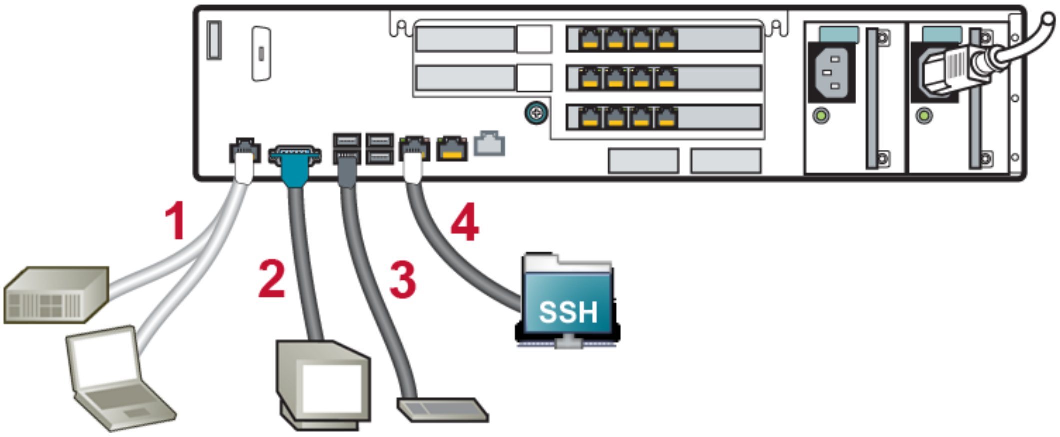
The Platform is self-running and does not require operator intervention to perform DDoS filtering functions. The Web UI displays multiple views of network traffic and DDoS attack statistics.

### 1.4.4.2 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 1-4: Options for connecting to the CLI**



The following table describes the connections in the figure:

**Table 1-7: 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.

### 1.4.5 TOE Data Description

**TSF Data** includes information used by the TSF in making decisions. It includes the systems parameters set by administrators to configure the security of the TOE Security attributes, authentication data and traffic control attributes. Examples of TSF Data include administrative roles and audit logging parameters.

**User Data** includes the Data created by external and internal IT entities that do not affect the operation of the TSP. User Data is separate from the TSF data. The information flows created by Clients and Servers are examples of User Data.

### 1.4.6 Product Guidance

The following product guidance documents are provided with the TOE:

### Table 1-8: TOE User Guidance Documents

| Reference Title | ID |
|---|---|
| Pravail APS User Guide, Version 5.4, APS-UG-540-2013/09 | [ADMIN] |
| Pravail APS 2100 Series Mixed Interface Appliance, APS-QSC-MIA-EN-2013/06 | [INSTALL-MIAQSC] |
| Pravail APS 2100 Series Quick Start Card, APS-QSC-EN-2100-2013/06 | [INSTALL-QSC] |
| Pravail APS 5.4 Release Notes, APS-RN-540-2014/02 | [RELEASE] |

### 1.4.7 Physical Scope of the TOE

The physical boundary of the TOE is the entire appliance. The appliance will be evaluated in the “inline mode” deployment scenario.

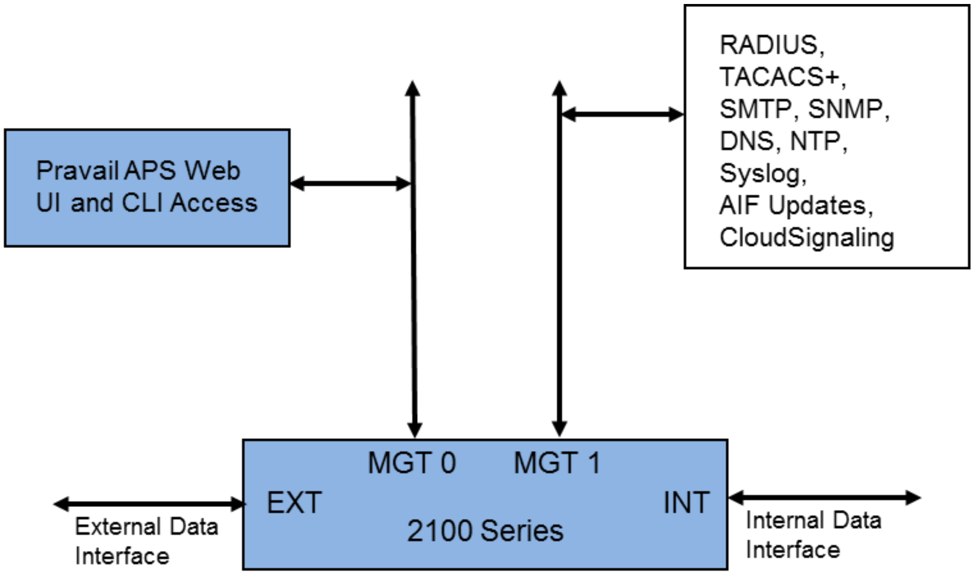


**Figure 1-5: TOE Physical Boundary (Blue components)**

#### 1.4.7.1 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 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)
- Use of CLIs are scoped to those functions described in Section 1.4.4.2

#### 1.4.7.2 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.

### 1.4.8 Logical Scope of the TOE

Pravail APS provides the following security functionality:

- **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.

  See the corresponding section in the TSS for more detailed information

- **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.

# 2 Conformance Claims

## 2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 3.1 R4.

This document conforms to the Common Criteria (CC) for Information Technology (IT) Security Evaluation, Version 3.1, Revision 4, dated September 2012.

## 2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

## 2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2.

# 3 Security Problem Definition

## 3.1 Threats

The TOE must counter the threats to security listed in Table 3-1. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

| Item | Threat ID | Threat Description |
|---|---|---|
| 1 | T.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. |
| 2 | T.DDoSATTACK | 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. |
| 3 | T.FAILURE | A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable. |
| 4 | T.MANAGE | An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE |
| 5 | T.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. |
| 6 | T.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. |

**Table 3-1: TOE Threats**

## 3.2 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are listed in Table 3-2.

| Item | Assumption ID | Assumption Description |
|---|---|---|
| 1 | A.BACKUP | Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost. |
| 2 | A.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. |
| 3 | A.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, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. |
| 4 | A.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. |

**Table 3-2: Assumptions**

### *3.3 Organizational Security Policies*

There are no Organizational Security Policies defined for the TOE.

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

**Table 4-1: TOE Security Objectives**

| Item | Objective ID | Description |
|---|---|---|
| 1 | O.AUDIT | The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security. |
| 2 | O.DDoSALERT | The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors. |
| 3 | O.DDoSMITIGATE | The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources. |
| 4 | O.FAILSAFE | The failure of the TOE must not interrupt the flow of traffic through the TOE between networks. |
| 5 | O.IDAUTH | The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions. |
| 6 | O.MANAGE | The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. |
| 7 | O.PROCOM | The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the Pravail APS Web UI or remote access to the CLI |

## 4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

**Table 4-2: Security Objectives for the Operational Environment**

| Item | Environment Objective | Description |
|---|---|---|
| 8 | OE.AUDIT | The IT environment must provide a long term audit and alert store for the TOE. |
| 9 | OE.BACKUP | Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost. |
| 10 | OE.CONNECT | Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE. |

| Item | Environment Objective | Description |
|---|---|---|
| 11 | OE.NOEVIL | Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. |
| 12 | OE.PHYSICAL | Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |

## *4.3 Security Objectives Rationale*

**Table 4-3: Mapping of TOE Security Objectives to Threats/Policies**

| Item | TOE Objective | Threat |
|---|---|---|
| 1 | O.AUDIT | T.AUDIT |
| 2 | O.DDoSALERT | T.MANAGE |
| 3 | O.DDoSMITIGATE | T.DDoSATTACK |
| 4 | O.FAILSAFE | T.FAILURE |
| 5 | O.IDAUTH | T.NOAUTH |
| 6 | O.MANAGE | T.MANAGE |
| 7 | O.PROCOM | T.PROCOM |

**Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions**

| Item | Environment Objective | Threat/Policy/Assumption |
|---|---|---|
| 8 | OE.AUDIT | T.AUDIT |
| 9 | OE.BACKUP | A.BACKUP |
| 10 | OE.CONNECT | A.CONNECT |
| 11 | OE.NOEVIL | A.NOEVIL |
| 12 | OE.PHYSICAL | A.PHYSICAL |

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

### Table 4-5: All Threats to Security Countered

| Item | Threat ID | Objective | Rationale |
|---|---|---|---|
| 1 | T.AUDIT<br>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. | O.AUDIT<br>The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security. | This threat is mitigated by O.AUDIT which requires that the TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security thus providing administrators the ability to investigate incidences. |
| | | OE.AUDIT<br>The IT environment must provide a long term audit for the TOE. | OE.AUDIT requires that IT environment must provide a long term audit store for the TOE thus providing administrators with a longer history to investigate incidences with. |
| 2 | T.DDoSATTACK<br>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. | O.DDoSMITIGATE<br>The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources. | This threat is mitigated by O.DDoSMITIGATE, which requires that the TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS attacks). The TOE must also be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DOS and DDoS attacks, and authorized users who may overuse resources. |
| 3 | T.FAILURE<br>A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable. | O.FAILSAFE<br>The failure of the TOE must not interrupt the flow of traffic through the TOE between networks. | This threat is mitigated by O.FAILSAFE which ensures that the flow of traffic through the TOE is not interrupted during TOE failure creating a DoS scenario. |
| 4 | T.MANAGE<br>An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE | O.MANAGE<br>The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. | This threat is mitigated by O.MANAGE, which requires that The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion. The TOE provides role based access control to management functions and enforces I&A prior to obtaining any access. |
| | | O.DDoSALERT<br>The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors. | This threat is mitigated by O.DDoSALERT which provides the alerting required to warn administrators about events that happened or are happening that may require further management intervention. |

| | | | |
|---|---|---|---|
| 5 | T.NOAUTH<br>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. | O.IDAUTH<br>The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions. | This threat is mitigated by O.IDAUTH, which provides for unique identification and authentication of administrative users. |
| 6 | T.PROCOM<br>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. | O.PROCOM<br>The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the Pravail APS Web UI or remote access to the CLI. | This threat is mitigated by O.PROCOM which requires that the TSF must provide a secure session for communication between the TOE and the remote administrator's web browser trying to access the Pravail APS Web UI or remotely accessing the CLI. |

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

**Table 4-6: All Assumptions Upheld**

| Item | Assumption ID | Objective | Rationale |
|---|---|---|---|
| 1 | A.BACKUP<br>Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost. | OE.BACKUP<br>Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost. | This objective provides for the backup of the TOE audit and configuration files by administrators to ensure data loss minimization due to hardware or software errors. |
| 2 | A.CONNECT<br>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. | OE.CONNECT<br>Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE. | This objective provides for placing the TOE at the network perimeter and ensuring that information flow cannot flow between internal and external networks without TOE inspection. |

| Item | Assumption ID | Objective | Rationale |
|---|---|---|---|
| 3 | A.NOEVIL<br>There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. | OE.NOEVIL<br>Those responsible for the TOE must ensure that  there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. | This objective provides for competent and non-hostile personnel to administer the TOE. This objective ensures the TOE is delivered, installed, managed, and operated by competent individuals. |
| 4 | A.PHYSICAL<br>The TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. | OE.PHYSICAL<br>Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. | This objective provides for the protection of the TOE from untrusted software and users. This objective provides for the physical protection of the TOE software. |

# 5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding “_EXT” in the component name.

**Table 5-1: Extended Components**

| Item | SFR ID | SFR Title |
|---|---|---|
| 1 | FIA_UAU_EXT.2 | User authentication before any action |
| 2 | DDoS_DEF_EXT.1 | DDoS Defense |
| 3 | DDoS_NOT_EXT.1 | Security Notifications |

## *5.1 FIA_UAU_EXT.2 User authentication before any action*

### 5.1.1 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4.

### 5.1.2 Family: User authentication (FIA_UAU)

#### 5.1.2.1 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

#### 5.1.2.2 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

#### 5.1.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

### 5.1.3 Definition

**FIA_UAU_EXT.2 User authentication before any action**

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

### 5.1.4 Rationale

FIA_UAU_EXT.2 is modeled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXT.2 needed to be defined as an extended component because the standard component was broadened by adding the text *“either by the TSF or by an authentication service in the Operational Environment invoked by the TSF”.*

*Note: The definition and use of the wording in FIA_UAU_EXT.2.1 was approved by the validation team for FAU_UAU_EXT.2 in a previous CygnaCom evaluation.*

## *5.2 DDoS_DEF_EXT.1 DDoS Defense*

### 5.2.1 Class: DDoS: Distributed Denial of Service

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a DDoS detection and mitigation product. While this SFR was modeled on exiting FRU requirements in the CC Part 2, these requirements needed further modification to meet the specific needs of DDoS detection and mitigation implementation rather than intrusion detection.

### 5.2.2 Family: DDoS Defense (DDoS_DEF)

#### 5.2.2.1 Family Behaviour

This family provides requirements for the TSF enforcement of detection and mitigation of DDoS attacks. The requirements of this family ensure that the TOE will protect networks against DDoS attacks.

#### 5.2.2.2 Management

The following actions could be considered for the management functions in FMT:

- Management of TSF data.

#### 5.2.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Detection and Actions taken due to detected potential attacks.

### 5.2.3 Definition

**DDoS_DEF_EXT.1 DDoS Defense**

Hierarchical to: No other components.

Dependencies: No other components

**DDoS_DEF_EXT.1.1 The TSF shall be able to detect the following type of DDoS attacks**

***[***

***Assignment: Types of DDoS Attacks.***

***]***

**DDoS_DEF_EXT.1.2 The TSF shall be able to mitigate the detected DDoS attacks.**

**DDoS_DEF _EXT.1.3 The TSF shall provide the following additional information flow control capabilities**

***[***

***Assignment: Additional Traffic Control Capabilities.***

***]***

### 5.2.4 Rationale

DDoS_DEF_EXT.1 had to be explicitly stated because the CC Part 2 does not have any DDoS mitigation related SFRs that can describe the functions of the TOE. DDoS_DEF is modeled as a Family of the standard class FRU (Resource Utilization) as it is the only class that deals with availability and prioritization of resources.

## *5.3 DDoS_NOT_EXT.1 Explicit: Security Notifications*

### 5.3.1 Class: DDoS: Distributed Denial of Service

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a DDoS detection and mitigation product. While this SFR was modeled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of DDoS detection and mitigation implementation rather than intrusion detection.

### 5.3.2 Family: Security Notifications (DDoS_NOT)

#### 5.3.2.1 Family Behaviour

This family defines the notifications generated by the TSF as a result of trigger events that happen while the TSF is detecting and mitigating DDoS attacks. This family also defines the destination(s) of the notifications that are generated. The scanners would generally collect static configuration information and send that onto an analytical component which would cause the notifications to be generated.

#### 5.3.2.2 Management

The following actions could be considered for the management functions in FMT:

- Configuration of the notification destination by an administrator

#### 5.3.2.3 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: time notification generated, source and destination of notification, notification type

### 5.3.3 Definition

**DDoS_NOT_EXT.1 Explicit: Security Notifications**

Hierarchical to: No other components

Dependencies: DDoS_DEF_EXT.1

**DDoS_NOT_EXT.1.1 The TSF shall send a visual notification to *[assignment: list where visual notifications are displayed]* when *[assignment: list of events]* occurs during the assessment process.**

**DDoS_NOT_EXT.1.2 The TSF shall send a *[assignment: list notification types]* notification to *[assignment: list notification recipients]* when *[assignment: list of events or category of alerts]* occurs during the assessment process.**

### 5.3.4 Rationale

DDoS_NOT_EXT.1 is modeled on IDS_RCT.1 Analyzer react (EXP) as defined in IDS System Protection Profile Version 1.7 July 25, 2007. This SFR was modified to apply to the various events that can be generated by any detection and mitigation type system rather than only the detection of an intrusion. This SFR uses the term “notification” rather than “alert” because there is no guarantee that the recipient will acknowledge or read the event information in a timely manner. For example, if the TOE sends this information via email (SMTP Server or native messaging within the product) there is no guarantee that the recipient will acknowledge or read the event information in a timely manner. Nor is the TOE expected to handle incoming responses such as an acknowledged receipt or read.

# 6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

## 6.1 Security Functional Requirements for the TOE

### Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

iteration: allows a component to be used more than once with varying operations;

assignment: allows the specification of parameters;

selection: allows the specification of one or more items from a list; and

refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text]****.*
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *Extended components* defined in Section 5 have been denoted with the suffix "_EXT" following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5, and summarized in Table 6-11 below.

**Table 6-1: Functional Components**

| Item | SFR ID | SFR Title |
|---|---|---|
| 1 | FAU_GEN.1 | Audit data generation |
| 2 | FAU_GEN.2 | User identity association |
| 3 | FAU_SAR.1 | Audit review |
| 4 | FAU_SAR.3 | Selectable audit review |
| 5 | FAU_STG.1 | Protected audit trail storage |
| 6 | FIA_ATD.1 | User attribute definition |

| | | |
|---|---|---|
| 7 | FIA_SOS.1 | Verification of Secrets |
| 8 | FIA_UAU.5 | Multiple authentication mechanism |
| 9 | FIA_UAU_EXT.2 | User authentication before any action |
| 10 | FIA_UID.2 | User identification before any action |
| 11 | FMT_MTD.1 | Management of TSF data |
| 12 | FMT_SMF.1 | Specification of management functions |
| 13 | FMT_SMR.1 | Security roles |
| 14 | FPT_FLS.1 | Failure with Preservation of  Secure State |
| 15 | FPT_STM.1 | Reliable Time Stamps |
| 16 | DDoS_DEF_EXT.1 | DDoS Defense |
| 17 | DDoS_NOT_EXT.1 | Security Notifications |
| 18 | FTP_ITC.1 | Inter-TSF trusted Channel |
| 19 | FTP_TRP.1 | Trusted Path/Channel |

### 6.1.1 Class FAU: Security Audit

#### 6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[not specified]*** level of audit; and

**c)** ***[the following auditable events: events listed in column 3 of Table 6-2 ]***

**Table 6-2: Functional Components**

| Item | SFR ID | SFR Title |
|---|---|---|
| 1 | FAU_GEN.1 | None |
| 2 | FAU_GEN.2 | None |
| 3 | FAU_SAR.1 | None |
| 4 | FAU_SAR.3 | None |
| 5 | FAU_STG.1 | Disk usage is getting full. |
| 6 | FIA_ATD.1 | None |
| 7 | FIA_SOS.1 | None |
| 8 | FIA_UAU.5 | None |
| 9 | FIA_UAU_EXT.2 | User login and logout |

| | | |
|---|---|---|
| 10 | FIA_UID.2 | User login and logout |
| 11 | FMT_MTD.1 | Configuration or updates to any of the Pravail APS Settings<br>CLI commands |
| 12 | FMT_SMF.1 | All Actions defined in FMT_MTD.1 |
| 13 | FMT_SMR.1 | None |
| 14 | FPT_FLS.1 | Failure with Preservation of  Secure State |
| 15 | FPT_STM.1 | None |
| 16 | DDoS_DEF_EXT.1* | Triggers for Cloud Signaling (event happened)<br>AIF updates (success and failure) |
| 17 | DDoS_NOT_EXT.1 | Security Notifications |
| 18 | FTP_ITC.1 | None |
| 19 | FTP_TRP.1 | None |

**Application Note: The Pravail APS records DDoS events in a separate log file, Blocked Host Log, which is not part of the audit trail and is available to view via a different function in the Web UI.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[the additional information identified in Table 6-3]***.

**Table 6-3: Audit Record Information**

| Information | Description |
|---|---|
| Username | The user who made the change, or “system” if it is a system-generated change. |
| Sub-System | The sub-system that made the change. ATLAS, CLI, deployment, diagnostics, file system, mitigation, notifications, system, and user accounts. |
| Protection Group | The name of the protection group to which the entry corresponds, if the entry is the results of a protection group change. |
| Description | A description of the change. For example, if a protection group is created, the description displays the settings that are configured. |

*Application Note: The “…outcome (success or failure) of the event” will only be included if applicable.*

### 6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other component

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[Administrators]*** with the capability to read ***[all audit data]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

*Application Note: Only the current Change Log (Audit data) that resides on the TOE can be reviewed by using the local audit review GUI. Audit data collected by Syslog servers and SNMP servers cannot be reviewed using the local audit review GUI.*

### 6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[searching]*** of audit data based on ***[***

***All possible combinations of the following fields:***

- ***Username***
- ***TimeStamp***
- ***Sub-system***
- ***Protection Group***
- ***Description***

***]***

### 6.1.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***[prevent]*** unauthorized modifications to the audit records in the audit trail.

## 6.1.2 Class FIA: Identification and authentication

### 6.1.2.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

***[***

- ***Username***
- ***Password***
- ***Group assignment (role)***

***]***

### 6.1.2.2 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the parameters of the Pravail Password Policy (See Table 6-4)].***

**Table 6-4: Pravail Password Policy Rules**

| Password Criteria |
|---|
| must be at least 7 characters long |
| must be no more than 72 characters long |
| can include special characters, spaces, and quotation marks |
| cannot be all digits |
| cannot be all lowercase letters or all uppercase letters |
| cannot be only letters followed by only digits (for example, abcd123) |
| cannot be only digits followed by only letters (for example, 123abcd) |
| cannot consist of alternating letter-digit combinations (for example, 1a3A4c1 or a2B4c1d) |

### 6.1.2.3 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide ***[Local Password Authentication and ability to invoke external authentication mechanism when configured]*** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the ***[***

***Following rules:***

- ***IF no external authentication server is configured (default mode) then the TOE uses Use Local Password Mechanism only until either an success or failure decision***

- ***IF an external authentication server is configured the TOE will invoke the configured external authentication mechanism(s) based on the following:***
    - ***IF Exclusive Authentication is Disabled: The TOE invokes each authentication mechanism according to the administratively configured precedence order until either a success or until all methods fail (i.e. Failure from: RADIUS, TACACS+, LOCAL = Login Failure, Failure from: RADIUS, TACACS+ but Success from: LOCAL = Login Success)***

    - ***IF Exclusive Authentication is Enabled and the external authentication mechanism IS operational and reachable:***
        - ***The TOE invokes only the Exclusively configured authentication mechanism for immediate success or failure decision.***
        - ***The TOE does not try any other authentication mechanism in the precedence list.***

    - ***IF Exclusive Authentication is Enabled and external authentication mechanism IS NOT operational or not reachable:***
        - ***The TOE invokes the next authentication mechanism according to the administratively configured precedence order until either a success or failure is returned (i.e. if precedence order is RADIUS, TACACS+, LOCAL and RADIUS Server is down : Failure from: TACACS+ = Login Failure, Success from TACACS+ = Login Success, LOCAL is never attempted unless TACACS+ server is also down)***

***].***

*Application Note: The external authentication servers are NOT part of the TOE. The TOE only claims compatibility with RADIUS and TACACS+ servers).*

#### 6.1.2.4 FIA_UAU_EXT.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

#### 6.1.2.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### 6.1.3 Class FMT: Security Management

#### 6.1.3.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[change_default, query, modify, delete, and [other operations as specified in Table 6-5]*** the ***[TSF Data as specified in Table 6-5]*** to ***[the role as specified in Table 6-5].***

**Table 6-5: Management of TSF Data**

| **Operations** | **TSF Data or object** | **Role** | |
|---|---|---|---|
| Login to CLI (Access) | the CLI environment | ADMIN | USER |
| Login to Web UI (Access) | the Pravail APS Web UI | ADMIN | USER |
| Capture | the network packets in real time | ADMIN | USER |
| Change | the global protection level | ADMIN | |
| Configure, Run, Restore | the backup and restore data | ADMIN | |
| Create | diagnostic packages | ADMIN | |
| Edit | the user accounts attributes | ADMIN | USER* |
| Edit | the AIF connection settings | ADMIN | |
| Edit | the Cloud Signaling configuration settings | ADMIN | |
| Edit | the IP interface configuration settings | ADMIN | |
| Edit | the routing configuration settings | ADMIN | |
| Edit | the local user and authentication | ADMIN | |

| | | | |
|---|---|---|---|
| Edit | the authorization configuration settings | ADMIN | |
| Edit | the accounting AAA configuration settings | ADMIN | |
| Edit | the DNS configuration settings | ADMIN | |
| Edit | the HTTP configuration settings | ADMIN | |
| Edit and View | the logging configuration settings | ADMIN | |
| View | the server log | ADMIN | |
| Edit | the NTP configuration settings | ADMIN | |
| Edit | the SSH configuration settings | ADMIN | |
| Edit | the system attributes | ADMIN | |
| Edit  and Apply | the IP access rules (Policy) | ADMIN | |
| Explore | historical blocked hosts log | ADMIN | USER |
| Import | a configuration file/package from disk | ADMIN | |
| Install and uninstall | software packages | ADMIN | |
| Edit | the Pravail APS system files | ADMIN | |
| Manage | the General Configuration Settings | ADMIN | |
| Manage | the Inline Active State Setting | ADMIN | |
| Manage | the notification configuration settings | ADMIN | |
| Manage | the protection groups configuration settings | ADMIN | |
| Manage | the system events configuration settings | ADMIN | |
| Manage | the SSH keys | ADMIN | |
| Manage | the system disks | ADMIN | |
| View | the Pravail APS system files | ADMIN | |
| Modify | the Address Resolution Protocol (ARP) information | ADMIN | |
| Restore | Restore the default protection settings | ADMIN | |
| Save and Export | the running configuration settings | ADMIN | |
| Set | the system clock | ADMIN | |
| Show | the running or saved configuration settings | ADMIN | USER |
| Shutdown | the Pravail APS system | ADMIN | |
| Start and Stop | the Pravail APS services | ADMIN | |
| View | the protection groups configuration settings | ADMIN | USER |
| View | the Pravail APS change log | ADMIN | |

*USER can only edit own account attributes for updating password or email attributes. A USER cannot change his own Group assignment or his Username.

### 6.1.3.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

***[***

- ***operations as specified in Table 6-5 on the TSF Data as specified in Table 6-5 (See FMT_MTD.1)***

***]***

### 6.1.3.3 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[ADMIN, USER, NONE]*****.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

*Application Note: The "None" role only applies when remote authentication (RADIUS and TACACS+) is used.*

## 6.1.4 Class FPT: Protection of TSF

### 6.1.4.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: None

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

***[***

- ***Power Failure***
- ***Hardware Failure***
- ***Software Failure***

***]***

#### 6.1.4.2 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: None

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

### 6.1.5 Class DDoS: Distributed Denial of Service

#### 6.1.5.1 DDoS_DEF_EXT.1 DDoS Defense

Hierarchical to: No other components.

Dependencies: None

DDoS_DEF_EXT.1.1 The TSF shall be able to detect the following types of DDoS attacks

***[***

- ***Botnet***
- ***Generic Bandwidth***
- ***Slow HTTP***
- ***Malformed HTTP***
- ***HTTP Cache Abuse***

***]***

DDoS_DEF_EXT.1.2 The TSF shall be able to mitigate the detected DDoS attacks.

DDoS_DEF_EXT.1.3 The TSF shall provide the following additional information flow control capabilities

***[***

***Capability to:***

- ***Configure TOE to function in ACTIVE (filter), INACTIVE (Monitor) or BYPASS modes***
- ***Configurable Protection Level (low, medium, high) enforcement***
- ***Request for Cloud Mitigation based on threshold settings***

***]***

*Note: See Section 8 for terminology and more details on ACTIVE (filtering), INACTIVE (monitoring), BYPASS, Whitelist, Blacklist, Service Definitions, Fragmentation Control and TCP SYN Rate Config, etc..*

*For additional details on description of DDoS attack types and mitigation mechanisms, see Section 7.6.*

#### 6.1.5.2 DDoS_NOT_EXT.1 Explicit: Security Notifications

Hierarchical to: No other components

Dependencies: DDoS_DEF_EXT.1

DDoS_NOT_EXT.1.1 The TSF shall send a visual notification to ***[Pravail APS Web UI Summary Page and Management Tab display]*** when ***[the event(s) listed in Table 6-6 ]*** occurs during the assessment process.

DDoS_NOT_EXT.1.2 The TSF shall send a ***[email, SNMP Trap, syslog message, and/or Cloud Signaling Mitigation Request]*** notification to ***[the assigned event notification recipient's Email ID, configured SNMP manager, configured syslog server, or Cloud Signaling Mitigation Request recipient (ISP or MSSP)]*** when ***[the Alert type(s) listed in Table 6-6 ]*** occurs during the assessment process.

**Table 6-6: Security Notifications**

| ***Alert Type*** | ***Causes*** |
|---|---|
| ***System*** | Hardware or system component events and other events that affect the system's health. For example, a system alert is created when an interface goes down. |
| ***Cloud*** | Notifications for Specific Cloud Signaling events can be sent in addition to the Cloud Signaling Mitigation Request being sent to the ISP or MSSP. For example, cloud alerts occur when traffic exceeds the configured threshold or when a communication error occurs between the network and the Cloud Signaling Server. |
| ***Protection*** | Someone changes the global protection level or a protection group's protection level. |
| ***Deployment*** | The deployment mode is changed. |
| ***Blocked Host*** | Source hosts are blocked. |
| ***Bandwidth*** | A protection group's traffic exceeds one or more traffic thresholds, or the system's traffic exceeds 90 percent of its licensed throughput limit. |

### 6.1.6 Class FTP: Trusted Path/Channels

#### 6.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product 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.

FTP_ITC.1.2 The TSF shall permit ***[the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[authentication decision handling, downloading of AIF Updates, and Cloud Signaling].***

#### 6.1.6.2 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***[remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[modification and disclosure]*****.**

FTP_TRP.1.2 The TSF shall permit ***[remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[initial user authentication, [and all remote user actions]].***

### *6.2 Security Assurance Requirements for the TOE*

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 6-5.

**Table 6-7: EAL2 Assurance Components**

| Assurance Class | Assurance components |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.2 Security-enforcing functional specification |
| | ADV_TDS.1 Basic design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.2 Use of a CM system |
| | ALC_CMS.2 Parts of the TOE CM coverage |
| | ALC_DEL.1 Delivery procedures |
| ASE: Security Target | ASE_CCL.1 Conformance claims |

| | |
|---|---|
| evaluation | ASE_ECD.1 Extended components definition |
| | ASE_INT.1 ST introduction |
| | ASE_OBJ.2 Security objectives |
| | ASE_REQ.2 Derived security requirements |
| | ASE_SPD.1 Security problem definition |
| | ASE_TSS.1 TOE summary specification |
| ATE: Tests | ATE_COV.1 Evidence of coverage |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.2 Vulnerability analysis |

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

## *6.3 Security Requirements Rationale*

### 6.3.1 Assurance Rationale

EAL 2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and protected by other products designed to address threats that correspond with the intended environment. At EAL *2*, the TOE will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

### 6.3.2 Dependencies Satisfaction Rationale

Table 6-8 shows the dependencies between the functional requirements including the extended components defined in Section 5.  Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

**Table 6-8: TOE Dependencies Satisfied**

| Item | SFR ID | SFR Title | Dependencies | Reference |
|---|---|---|---|---|
| 1 | FAU_GEN.1 | Audit data generation | FPT_STM.1 | 15 |
| 2 | FAU_GEN.2 | User identity association | FAU_GEN.1 | 1 |
| 2 | FAU_GEN.2 | User identity association | FIA_UID.1 | |

| | | | | |
|---|---|---|---|---|
| 3 | FAU_SAR.1 | Audit review | FAU_GEN.1 | 1 |
| 4 | FAU_SAR.3 | Selectable audit review | FAU_GEN.1 | 1 |
| 5 | FAU_STG.1 | Protected audit trail storage | FAU_SAR.1 | 3 |
| 6 | FIA_ATD.1 | User attribute definition | None | |
| 7 | FIA_SOS.1 | Verification of Secrets | None | |
| 8 | FIA_UAU.5 | Multiple authentication mechanism | None | |
| 9 | FIA_UAU_EXT.2 | User authentication before any action | FIA_UID.1 | 10 |
| 10 | FIA_UID.2 | User identification before any action | None | |
| 11 | FMT_MTD.1 | Management of TSF data | FMT_SMF.1 | 12 |
| 11 | FMT_MTD.1 | Management of TSF data | FMT_SMR.1 | 13 |
| 12 | FMT_SMF.1 | Specification of management functions | None | |
| 13 | FMT_SMR.1 | Security roles | FIA_UID.1 | 10 |
| 14 | FPT_FLS.1 | Failure with Preservation of Secure State | None | |
| 15 | FPT_STM.1 | Reliable Time Stamps | None | |
| 16 | DDoS_DEF_EXT.1 | DDoS Defense | None | |
| 17 | DDoS_NOT_EXT.1 | Security Notification | DDoS_DEF_EXT.1 | 16 |
| 18 | FTP_ITC.1 | Inter-TSF trusted Channel | None | |
| 19 | FTP_TRP.1 | Trusted Path/Channel | None | |

### 6.3.3 Functional Requirements vs Objectives Satisfaction Rationale

Table 6-9 traces each SFR back to the security objectives for the TOE demonstrating that ALL SFRs map to ALL security objectives for the TOE.

**Table 6-9: Mapping of TOE SFRs to TOE Security Objectives**

| Item | SFR ID | SFR Title | Objectives |
|---|---|---|---|

|  |  |  |  |
|---|---|---|---|
| 1 | FAU_GEN.1 | Audit data generation | O.AUDIT |
| 2 | FAU_GEN.2 | User identity association | O.AUDIT |
| 3 | FAU_SAR.1 | Audit review | O.AUDIT |
| 4 | FAU_SAR.3 | Selectable audit review | O.AUDIT |
| 5 | FAU_STG.1 | Protected audit trail storage | O.AUDIT |
| 6 | FIA_ATD.1 | User attribute definition | O.IDAUTH |
| 7 | FIA_SOS.1 | Verification of Secrets | O.IDAUTH |
| 8 | FIA_UAU.5 | Multiple authentication mechanism | O.IDAUTH |
| 9 | FIA_UAU_EXT.2 | User authentication before any action | O.IDAUTH |
| 10 | FIA_UID.2 | User identification before any action | O.IDAUTH |
| 11 | FMT_MTD.1 | Management of TSF data | O.MANAGE |
| 12 | FMT_SMF.1 | Specification of management functions | O.MANAGE |
| 13 | FMT_SMR.1 | Security roles | O.MANAGE |
| 14 | FPT_FLS.1 | Failure with Preservation of Secure State | O.FAILSAFE |
| 15 | FPT_STM.1 | Reliable Time Stamps | O.AUDIT |
| 16 | DDoS_DEF_EXT.1 | DDoS Defense | O.DDoSMITIGATE |
| 17 | DDoS_NOT_EXT.1 | Security Notifications | O.DDoSALERT |
| 18 | FTP_ITC.1 | Inter-TSF trusted Channel | O.PROTCOM |
| 18 | FTP_ITC.1 | Inter-TSF trusted Channel | O.IDAUTH |
| 19 | FTP_TRP.1 | Trusted Path/Channel | O.PROTCOM |
| 19 | FTP_TRP.1 | Trusted Path/Channel | O.MANAGE |

The Table 6-10 provides the rationale for how each objective is satisfied by the TOE.

**Table 6-10: All TOE Objectives Met by Security Functional Requirements**

| Item | Objective ID | SFR ID/Title | Rationale |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | O.AUDIT<br>The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security. | FAU_GEN.1 | Audit records are generated for security-relevant events. |
| | | FAU_GEN.2 | The user/source is associated with the audit events is recorded. |
| | | FAU_SAR.1 | The TOE provides the ability to review and manage the audit trail of the system. |
| | | FAU_SAR.3 | The TOE is capable of providing searching capabilities of the audit records. The TOE is capable of providing selection capabilities for auditing to include or exclude auditable events from the set of audited events |
| | | FAU_STG.1 | The TOE is able to protect audit records stored internally. |
| | | FPT_STM.1 | The TOE provides the timestamp required for the audit record. The TOE supports the setting of the time manually or configuring an external NTP server. |
| 2 | O.DDoSALERT<br>The TOE will provide the capability to alert administrators when DDoS attacks are detected and other customizable events, conditions, and system errors. | DDoS_NOT_EXT.1 | The TOE is capable of generating notifications based upon administratively defined set of events, conditions, or system errors. The notifications can be sent via email, SNMP trap, or syslog message. |
| 3 | O.DDoSMITIGATE<br>The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources. | DDoS_DEF_EXT.1 | The TOE protect Internet Protocol (IP) networks against DDoS attacks by successfully identifying and mitigating attacks via mechanisms such as filtering, Whitelists, Blacklists, TCP SYN rate monitoring, etc. |
| 4 | O.FAILSAFE<br>The failure of the TOE must not interrupt the flow of traffic through the TOE between networks. | FPT_FLS.1 | FPT_FLS.1 ensures that the TOE preserves a secure state when there is a hardware, software or power failure. |
| 5 | O.IDAUTH<br>The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions. | FIA_ATD.1 | User attributes required for identification and authentication are stored by the TOE. |
| | | FIA_UAU.5 | Provides for local authentication and the invocation of an external authentication mechanism (only claiming the ability to interface with RADIUS and TACACS+ servers). |

| | | | |
|---|---|---|---|
| | | FIA_UAU_EXT.2 | All authorized users are successfully authenticated before allowing any management actions on behalf of that user. |
| | | FIA_UID.2 | All users are successfully identified before allowing any other TSF-mediated actions on behalf of that user. |
| | | FIA_SOS.1 | Provides the enforced password policy for native password authentication. |
| | | FTP_ITC.1 | Provides trusted communications to the external authentication mechanisms that can optionally be used to identify and authenticate the requesting user. |
| 6 | O.MANAGE<br>The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. | FMT_MTD.1 | The TOE allows for the appropriate management TSF data within each Security function. |
| | | FMT_SMF.1 | Ensures that the TOE security Function data may only be modified by an appropriate administrator. |
| | | FMT_SMR.1 | This objective is met by supporting multiple management roles (ADMIN and USER, and NONE). |
| | | FTP_TRP.1 | Provides for the trusted path required for remote management of the TOE. |
| 7 | O.PROCOM<br>The TOE will provide a secure session for communication between the TOE and the remote administrator's browser trying to access the Pravail APS Web UI or remote access to the CLI | FTP_ITC.1 | The TOE requires the establishment of an HTTPS (SSL/TLS) connection from the remote administrator's browser. HTTP is not supported. |
| | | FTP_TRP.1 | The TOE requires the establishment of an SSH connection in order to access the TOE remotely to use the CLI. Telnet is disabled by default. |

# 7 TOE Summary Specification

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.10 Logical Scope of the TOE.

The following sub-sections describe how the TOE meets each SFR listed in Section 6.

**Table 7-1: Security Functional Requirements Mapped to Security Functions**

| Security Class | SFRs | Security Functions |
|---|---|---|
| Security audit | FAU_GEN.1 | SA-1 |
| | FAU_GEN.2 | |
| | FAU_SAR.1 | SA-2 |
| | FAU_SAR.3 | |
| | FAU_STG.1 | SA-3 |
| Protection of TSF | FPT_FLS.1 | FPT-1 |
| | FPT_STM.1 | FPT-2 |
| Identification and authentication | FIA_ATD.1 | IA-1 |
| | FIA_SOS.1 | IA-2 |
| | FIA_UAU.5 | |
| | FIA_UAU_EXT.2 | |
| | FIA_UID.2 | |
| Security Management | FMT_MTD.1 | SM-1 |
| | FMT_SMF.1 | SM-2 |
| | FMT_SMR.1 | SM-3 |
| Trusted Communication | FTP_ITC.1 | TC-1 |
| | | TC-2 |
| | | TC-3 |
| | FTP_TRP.1 | TC-4 |
| | | TC-5 |
| Resource Utilization (DDoS Protection) | DDoS_DEF_EXT.1 | DDoS-1<br>DDoS-2 |
| | DDoS_NOT_EXT.1 | DDoS-3 |

## *7.1 Security Audit*

### 7.1.1 SA-1: Audit Generation

**(FAU_GEN.1 and FAU_GEN.2)**

The TOE's audit trail equates to Pravail's Change Log and syslog (2 different files with overlap) which is stored on the appliance.

Audit records are generated within the TOE by the TSF for the events listed in FAU_GEN.1. Audit records contain a timestamp, the information of the entity triggering the event (username or sub-system), the event (e.g. Cloud Signaling, configuration changes, CLI command usage, AIF updates occur), and a summary of the event as well as the additional information listed in Table 6-2 and Table listed in Section Table 6-3.

There is no separate startup/shutdown of audit as it is all part of the TOE's startup and shutdown procedures.  The startup and shutdown of the system is audited.

### 7.1.2 SA-2: Audit Review

**(FAU_SAR.1, FAU_SAR.3)**

An authorized ADMIN user can read all of the Change Log (audit data) generated using the Pravail APS Web UI as the Administration → Change Log. Once the Change Log page is displayed the ability to search on various information is provided.

**Table 7-2: Audit Search Fields**

| Information | Description |
|---|---|
| Username | The user who made the change, or "system" if it is a system-generated change. |
| Date | The date on which the event occurred. |
| Sub-System | The sub-system that made the change. ATLAS, CLI, deployment, diagnostics, file system, mitigation, notifications, system, and user accounts. |
| Protection Group | The name of the protection group to which the entry corresponds, if the entry is the results of a protection group change. |
| Description | A description of the change. For example, if a protection group is created, the description displays the settings that are configured. |
| **Search** box | Allows one to search on data from any column on the page except the date.<br>Type all or part of a search string, and then click the 🔍 icon<br>To clear the search results, click the **X** in the Search box. |

The TOE displays search results in chronological order with the most recent event displayed first.

The CLI for viewing the syslog would be the / service logging view *logfile*

### 7.1.3 SA-3: Audit Protection

**(FAU_STG.1)**

The TSF protects the stored audit records on the TOE from unauthorized deletion and modifications via the TSFIs. The Audit data resides on the TOE Platform and can only be accessed using the Pravail APS Web UI. The Pravail APS Web UI does not provide an option for users to delete or modify the Change Log (aka audit log), but allows administrators to export the Change Log audit data.

The TOE does automatically delete oldest audit data logfile (syslog) when the maximum number of rotated syslog files to be retained is met (i.e maxlimit is set to 5 then on 6th rollover the oldest rotated file is deleted.  The maxlimit is configurable via the CLI / service logging maxlimit #.

It is highly recommended that the TOE be configured to use an external syslog server to continually off load the audit for long term storage. The TOE supports the manual exporting of the syslog files via the CLI / service logging remote *<IP address>.*

The TOE allows an administrator to export the syslog audit log using the Web UI for persistent storage. These files are in the form of a CSV file or PDF file.  An administrator can also backup the appliance which would include the audit trail along with protection settings, blacklist and whitelist, and configuration settings (excludes network configurations and alerts).

The TOE also supports the manual exporting of the syslog files via the CLI /service logging export command.

The TOE does not allow for the modification or deletion of any of the TOE's audit data (Change Log or syslog) via the CLI commands or the Web UI.

## *7.2 Protection of TSF*

### 7.2.1 FPT-1: Failure with preservation of secure state

**(FPT_FLS.1)**

Secure State for this product is defined as the state when the TOE Platform provides uninterrupted access to resources on the Internal Network to intended users. The failure of the TOE must not make the resources unavailable.

The flow of network traffic is not interfered with, monitored, or filtered, during the boot cycle as the TOE is in bypass mode. The Pravail APS must initialize successfully in order for the TOE to be placed out of bypass mode for operational use.

The Pravail APS appliance is bypass capable. If power failures, hardware failures, or software issues (includes the cryptographic self-check) affect the TOE during operational use, the TOE is placed in bypass mode and the network traffic is passed through the appliance unaffected thus preventing resources being made unavailable.

In the case of a power supply failure, the redundant power architecture (if configured) will take over and maintain safe operation.  In case of complete power supply failure, the Platform passes traffic without any monitoring or filtering in an uninterrupted manner.

### 7.2.2 FPT-2: Reliable Time Stamps

An administrator can set or reset the clock in Pravail APS by using the CLI.

An administrator can optionally configure Pravail APS to use an NTP server using the CLI (uses port 123). The TOE can provide its own timestamp through a system call to the supporting operating system which is part of the appliance.  It is highly recommended that the enterprise network being protected have it’s time synchronized with a NTP server.  The TOE supports the use of an NTP server to update the system’s time clock.  The TOE allows for up to 2 NTP servers to be identified (primary and backup).

## *7.3 Indentification and Authentiation*

### 7.3.1 IA-1: User Attributes

**(FIA_ATD.1)**

The TSF maintains the following security attributes for each individual TOE user for use with local password authentication only:

- Username
- Password
- Group assignment (role)
- Email

### 7.3.2 IA-2: User I&A

**(FIA_UAU.5, FIA_UAU_EXT.2, FIA_UID.2, FIA_SOS.1)**

The TSF requires each user to self-identify before being allowed to perform any other actions. The TSF requires an administrator to be successfully authenticated with a password before being allowed any other management actions. Authentication is handled via local password protection or the TOE invokes an external authentication mechanism (RADIUS or TACACS+) for the authentication decision.  The TOE must be administratively configured to select the authentication method and to talk with the RADIUS or TACACS+ server via the CLI interface after installation.

If it is desired to authenticate users with the RADIUS or TACACS+ authentication service, the administrator must specify which authentication method to use. If the use multiple methods is desired, the administrator must also specify the order in which Pravail APS should try each method. Pravail APS tries each method according to the order in which the administrator listed them, until one method succeeds or until they all fail.  The only 3 choices available: RADIUS, TACACS, LOCAL.  One, two, or three may be specified).

Pravail APS uses LOCAL authentication by default if no method is specified.

This authentication applies to both Web UI access and CLI access.

**About exclusive authentication**

An administrator can also set the authentication method to be exclusive, which specifies the following behavior: Pravail APS tries the defined exclusive method, and if the method is working (for example, the authentication server responds), but the user cannot log on with it, then the user cannot log on at all. For example, if exclusive authentication is used and the TACACS+ server is operational, but the user does not have a TACACS+ account, then that user cannot log on at all. Pravail APS only tries to authenticate with the next method listed if the TACACS+ server is not operational or is unreachable on the network.

However, if the TACACS+ server is down then the next method in the precedence list is tried. When using the exclusivity feature the precedence list must contain LOCAL as one of the mechanisms. Meaning at least 2 methods must be declared in the precedence list (TACACS+ and LOCAL). One can declare RADIUS as the backup method however LOCAL would still need to be declared (TACACS+, RADIUS, LOCAL).

This exclusive method is also set at the CLI mode by and administrator. Exclusivity is disabled by default.

Below is a table of scenarios to help in understanding the authentication enforcement described above. The top left corner sets the scenario as to whether exclusivity has been enabled or is disabled. The Method Status is indicating whether the TOE/external authentication mechanisms are Available (operational and network reachable) or are NOT available (not reachable on network). The precedence order set shows the order in which an administrator may configure the TOE. The Final Outcome / Method row shows the final decision the TOE would enforce and which authentication server was the final decision maker.

**Table 7-3: Authentication Scenario Examples**

| **Exclusive: Disabled**<br>**Method Status: Available**<br>**Precedence Order Set: Not Set (default)** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | LOCAL (TOE) | Success | Stops | Failure | Stops | N/A | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| | **Overall Outcome / Method** | **Success** | **LOCAL** | **Failure** | **LOCAL** | | | | |

| **Exclusive: Disabled**<br>**Method Status: Available**<br>**Precedence Order Set: T, R, L** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TACACS+ | Success | Stops | Failure | Next | Failure | Next | Failure | Next |
| 2 | RADIUS | | | Success | Stops | Failure | Next | Failure | Next |
| 3 | LOCAL | | | | | Success | Stops | Failure | Stops |
| | **Overall Outcome / Method** | **Success** | **TACACS+** | **Success** | **RADIUS** | **Success** | **LOCAL** | **Failure** | **LOCAL** |

| **Exclusive: Enabled = TACACS+**<br>**Method Status: Available**<br>**Precedence Order Set: T, R, L** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TACACS+ | Success | Stops | Failure | Stops | N/A | | | |
| 2 | RADIUS | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | LOCAL | | | | | | | | |
| | **Overall Outcome / Method** | **Success** | **TACACS+** | **Failure** | **TACACS+** | | | | |

| **Exclusive: Enabled = TACACS+**<br>**Method Status: NOT Available**<br>**Precedence Order Set: T, L, R** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TACACS+ | Network Error | | Network Error | | N/A | | | |
| 2 | LOCAL | Success | Stops | Failure | Stops | | | | |
| 3 | RADIUS | | | | | | | | |
| | **Overall Outcome / Method** | **Success** | **LOCAL** | **Failure** | **LOCAL** | | | | |

| **Exclusive: Enabled = TACACS+**<br>**Method Status: NOT Available**<br>**Precedence Order Set: T, R, L** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TACACS+ | Network Error | | Network Error | | N/A | | | |
| 2 | RADIUS | Success | Stops | Failure | Stops | | | | |
| 3 | LOCAL | | | | | | | | |
| | **Overall Outcome / Method** | **Success** | **RADIUS** | **Failure** | **RADIUS** | | | | |

| **Exclusive: Enabled = TACACS+**<br>**Method Status: NOT Available**<br>**Precedence Order Set: R, T, L** | | **Scenario 1** | | **Scenario 2** | | **Scenario 3** | | **Scenario 4** | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TACACS+ | Network Error | | Network Error | | N/A | | | |
| 2 | LOCAL | Success | Stops | Failure | Stops | | | | |
| | **Overall Outcome / Method** | **Success** | **LOCAL** | **Failure** | **LOCAL** | | | | |

### Pravail APS Password Policy

Local passwords have a software enforced password policy.  The password policy is within the user manual. The requirements are:

- must be at least 7 characters long
- must be no more than 72 characters long
- can include special characters, spaces, and quotation marks
- cannot be all digits
- cannot be all lowercase letters or all uppercase letters
- cannot be only letters followed by only digits (for example, abcd123)
- cannot be only digits followed by only letters (for example, 123abcd)
- cannot consist of alternating letter-digit combinations (for example, 1a3A4c1 or a2B4c1d)

Additionally information:

> **WARNING: Default username and password**
> For accessing the CLI for the very first time, one must use the default username and password. The default username is ***admin***. The default password is ***arbor***.
>
> It is imperative for security purposes that this password be changed after the first time logging into the system.

## *7.4 Security Management*

### 7.4.1 SM-1: Management of TSF Data

**(FMT_MTD.1)**

The allowed operations on TSF Data and the administrative roles required to execute them are defined in Table 6-6: Management of TSF Data (See Section 6.1.3.1 FMT_MTD.1 Management of TSF data).

### 7.4.2 SM-2: Specification of Management Functions

**(FMT_SMF.1)**

The TOE is capable of performing the security management functions as defined in Table 6-5: Management of TSF Data of Section 6.1.3.1 FMT_MTD.1 Management of TSF data. The functions defined for FMT_SMF are exactly the same as the functions defined in the FMT_MTD requirement.

All management functions and access rights are limited by role based management as defined in Section 7.1.3.3 SM-3: Security Roles below.

When accessing the management functions via the Pravail APS Web UI:

A successfully authenticated user can navigate menus and pages by using typical navigational controls. The Web UI menu bar indicates which menu is active or inactive and only allows the user to access those menus based on the privileges inherited from the user's assigned group.

The menu bar is divided into the following menus: Summary, Explore, Protection Groups, & Administration (details of which were given in the introduction section).  An ADMIN has access to all the web menus. A USER only has access to the Administration menu functions that allow the user to change his/her own password and e-mail address. A user with the role of NONE won't have access to any of the menus and is pushed back to the login page.

The functions defined in the FMT_MTD.1 Table 6-5 are divided amongst the 4 web menus (predominately in the Administration) and are either submenus (provide further division) or pages that display the actual data such as list of users or a page of a particular user's attributes.

Additionally there are some administrative functions that can only be handled by using CLIs.  Typically, the CLI is used for installing and upgrading the software and completing the initial configuration. However there are additional advanced functions that can only be configured using the CLI.

### 7.4.3 SM-3: Security Roles

**(FMT_SMR.1)**

The TOE supports the 3 roles listed below:

Group Access

- ADMIN: Users in this group have full read and write access on all pages of the Web UI and can run all of the command line interface (CLI) commands.
- USER: Users in this group have read-only access to most of the Web UI pages and can edit and update their own user account settings. They can log on to the CLI and run limited CLI commands. For example, they can view the status of the system. Users in this group cannot change any settings.
- NONE: Users in this group have no access to Pravail APS. When an organization uses RADIUS or TACACS+ authentication, it is possible for all users who have an account on the authentication server to access Pravail APS. Use this group as the default to lock out the unwanted users, and then assign users who need to access Pravail APS to the other groups.

When using RADIUS or TACACS+ to authenticate Pravail APS users, the user group for those users must be set the respective RADIUS or TACACS+ server. Any user who is not assigned to a user group on the RADIUS or TACACS+ server is assigned to the default user group in Pravail APS. Initially, the default user group is the predefined group system_user (i.e USER role). If the system_user group's authorizations are inappropriate for the RADIUS or TACACS+ users, the default group to which they are assigned can be changed.

See Section 6.1.5.2 FMT_MTD.1 Management of TSF data table for details on the specific function available to each role.

## *7.5 Trusted Communications*

### 7.5.1 TC-1: Trusted Channel for Authentication

Transactions between the TOE and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the TOE and RADIUS server. This eliminates the possibility that someone snooping on an unsecured network could determine a user's password. The TOE uses port 1812 for RADIUS Authentication by default. This port may be customized during installation.

Communication between the TOE and TACACS+ Server require that the entire data payload of the packet is encrypted, leaving only the standard TACACS+ header in cleartext and encrypts the user's password between the TOE and TACACS+ Server. TACACS+ reserves TCP port 49 by default. This port may be customized during installation.

### 7.5.2 TC-2: Trusted Channel for AIF Updates

During an AIF update, Pravail APS uses HTTPS (Port 443) to download the latest AIF threat feed. By default, the AIF updates run automatically every 24 hours. An administrator can change the frequency of the updates and can request an update at any time. The automatic updates can also be disabled, but then AIF must be updated manually. The TOE using FIPS validated Red Hat Enterprise Linux 5 (RHEL) OpenSSL Cryptographic Module (0.9.8e-26.el5_9.1.src.rpm, supports the following cipher suites for this communications channel:

- RC4-SHA
- RC4-MD5
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

### 7.5.3 TC-3: Trusted Channel for Cloud Signaling

Cloud Signaling is the process of requesting and receiving cloud-based mitigation of volumetric attacks in real time from an upstream service provider. The end user must purchase the cloud-based protection from an ISP or MSSP (Managed Security Service Provider) that supports Cloud Signaling. The ISP or MSSP would be considered an external trusted entity that is not in scope of this evaluation. However, the communication channel between the TOE and this trusted entity is in scope of the evaluation. This communication channel is protected using the HTTPS with certificate based identification and ID and Password authentication to the ISP/MSSP's Cloud Signaling Server. The TOE using FIPS validated Red Hat Enterprise Linux 5 (RHEL) OpenSSL Cryptographic Module (0.9.8e-26.el5_9.1.src.rpm, supports the following cipher suites for this communications channel:

- RC4-SHA
- RCRC4-MD5
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

### 7.5.4 TC-4: Trusted Path for Web UI Access

The Pravail APS requires the establishment of an HTTPS (TLSv1) connection from the remote administrator's Web UI (Port 443). The channel is established via the Apache/Tomcat Web Server (v2.2.22) which is part of the OS. The remote platform connects to the TOE using a standard browser that supports TLS. The remote platform and the TOE negotiate a common cipher suite between the 2 platforms. The TOE using FIPS validated Red Hat Enterprise Linux 5 (RHEL) OpenSSL Cryptographic Module (0.9.8e-26.el5_9.1.src.rpm, supports the following cipher suites for this communications channel:

- RC4-SHA
- RC4-MD5
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

HTTP is not acceptable in the evaluated configuration and must be disabled as a separate step during installation or can be manually disabled if accidentally turned on during installation.

### 7.5.5 TC-5: Trusted Path for CLI Access

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 remote platform connects to the TOE using the standard SSH-2 protocol through OpenSSH version 5.5 p1 which provides confidentiality and integrity of data over an insecure network. The remote user's host platform must therefore be on a network where it can access TCP Port 22, or a custom configured port such as 8022

The crypto cipher suites supported are:

- aes128-cbc,
- 3des-cbc,
- aes192-cbc,
- aes256-cbc and
- hmac-md5,
- hmac-sha1,
- umac-64@openssh.com,
- hmac-ripemd160,
- hmac-sha1-96,
- hmac-md5-96

Telnet by default is disabled and to maintain CC configuration must not be used during operational use.

## *7.6 Resource Utilization (DDoS Protection)*

### 7.6.1 DDoS-1: DDoS Detect

**BOTNET attacks**

A DDoS botnet is a large set of compromised computers that are controlled remotely by a server. The controlling server is known as a CnC (command-and-control) server. Usually, the computers in a botnet, which are known as bots, become compromised without their users' knowledge. The bots are infected with malware that enables them to generate a high-volume traffic attack that targets a victim server. Victim servers can include Web, DNS, and SMTP servers.

The bots can use a variety of protocols, including HTTP, IRC, and other proprietary protocols, to communicate with the CnC server and other bots. For example, a bot can send information about itself, receive attack commands from the CnC server, or share "hello" messages between itself and other bots.

Depending on the botnet family, the messages themselves can be in plain text or encoded. The botnet family also determines the type of attacks that are supported. These attacks can include one or more of the following types of floods: HTTP, UDP, TCP, and ICMP. When the bots receive commands from the CnC server, such as the attack method and target IP addresses, they collectively engage in DDoS attacks against the specified targets.

Some botnets are available for hire, whereby an individual can purchase the services of a botnet for a specific period. The service allows the individual to choose one or more target servers for the entire botnet to attack.

A voluntary botnet is one in which users allow their computers to become part of the botnet with the intention of attacking a victim server. When a computer becomes a member of the botnet, it accepts commands from the CnC server; for example, the attack method and target IP address. The bot joins the rest of the botnet to flood the victim server with traffic.

Some of the tools that attackers use contain a feature whereby users can allow their computers to become part of a botnet.

To prevent botnet attacks, Pravail APS performs the following tests:

- **Basic Botnet Prevention filtering**:
  When enabled the TOE checks the packet headers for incomplete fields, known as malformed HTTP filtering. Pravail APS blocks any packets whose headers are incomplete and temporarily blocks the source host.

  The fields that are checked vary by protection level, as follows:

  | **Protection level** | **Checks** |
  |---|---|
  | Low | Analyzes the Host field in HTTP 1.1 requests |
  | Medium | Analyzes the Host field in HTTP 1.1 requests |
  | High | Analyzes the following fields in all requests:<br>• Host<br>• User-Agent<br>• Connection |

  NOTE: the Basic Botnet Prevention works only if Malformed HTTP Filtering is also enabled.

- **AIF Botnet Signatures filtering**

  When enabled, the TOE uses the AIF signatures to detect DDoS botnet attacks, voluntary botnet attacks, and slow HTTP attacks. It is essential to keep the AIF signature listing updated in order to mitigate and detect emerging DDoS attacks.

  Pravail APS inspects all of the HTTP traffic and compares each AIF signature separately to each line of the HTTP headers. When a packet's HTTP header matches an AIF signature, Pravail APS records the traffic statistics for that packet. If the AIF signature's protection level matches or is lower than the global protection level or protection group protection level, Pravail APS blocks the packet. It also temporarily blocks the source host. For example, if the global protection level is medium, Pravail APS blocks any packet that matches the medium or low signatures.

- **Prevent Slow Request Attacks filtering**

  When enabled, the TOE checks for HTTP requests that contain less than 500 bytes of data and do not end with *\n*. Pravail APS blocks the requests and temporarily blocks the source host of any requests that match these criteria because they are likely to be part of a slow HTTP attack.

  During a slow HTTP attack, the attacker makes several connections and, on each connection, sends a partial request for data to the victim server. In response, the server allocates resources such as memory to each connection and waits for subsequent requests to arrive. The attacker sends a very small portion of the request at a rate almost equal to, but less than, the server's timeout setting. Therefore, the server stays busy processing the small requests but it takes a long time to time out. Eventually, the server starts to deny legitimate connection requests from other clients.

  For example, if the server's timeout period is 300 seconds, the attacker sends 5 bytes of a 500-byte request every 299 seconds (just before the server times out). The attack occupies the server's resources on that connection for 29,900 seconds (299 * 500/5).

  The Prevent Slow Request Attacks filtering is enhanced when it works in conjunction with the TCP Connection Reset settings which tracks established TCP connections and blocks the traffic when a connection remains idle for too long. Traffic is also blocked when the bit rate for a single request drops below a configured minimum.

### Generic Bandwidth Flood Attacks

An HTTP flood is a continuous submission of the same HTTP request or a set of HTTP request messages to a victim Web server's resources. Typically, the attacker sends the requests at a high rate and forces the Web server to respond to each request. As a result, the Web server remains busy and denies service to legitimate requests.

Floods can originate from malware or from an attack tool that uses underlying operating system facilities to connect to the victim, create HTTP requests, and perform the attack. Some attack methods can provide flexibility in creating a traffic pattern (for example, randomized payloads), while others can provide better performance in terms of speed. The method that the attacker uses to construct the requests determines the nature of the attack, which in turn affects how the DDoS traffic is mitigated.

Many of the protection settings help to prevent this type of attack. Examples of these settings are as follows:

- The ICMP Flood Detection settings detect ICMP (ping) flood attacks.
- The Malformed HTTP Filtering settings protect against attacks that flood a server with invalid or blank HTTP requests.
- The Rate-based Blocking settings protect against floods by enforcing traffic thresholds.
- The Spoofed SYN Flood Prevention settings and the TCP SYN Flood Detection settings detect certain SYN flood attacks.

**Malformed HTTP attacks**

Malformed HTTP attacks exploit the way that Web servers handle HTTP requests that do not conform to protocol standards. For example, an early version of IIS server was vulnerable to HTTP requests that contained a specially crafted header. This header contained multiple, duplicate Host fields of a certain length that appeared a certain number of times. The attack consumed all of the server's memory.

Some malware and attack tools generate large amounts of TCP payload data that targets a Web server without including legitimate HTTP header information. These requests force the Web server to send a response, such as an error message, to the attacker for each request it receives. These attacks exhaust the Web server's resources.

To prevent this kind of attack the TOE implements the Malformed HTTP Filtering settings to influence how the TOE detects attacks that send invalid or blank HTTP requests.

**HTTP Cache Abuse attacks**

A Web server can store responses in cache memory to improve performance. The HTTP protocol supports several elements to make caching work. Some of these elements can be misused to make the server vulnerable to cache abuse attacks.

For example, an attacker repeatedly sends HTTP requests in a way that prevents the Web server from using the cache. The attacker can achieve this by using some of the cache control specific headers in the HTTP request message. This kind of attack can force the Web server to repeatedly reload the same page or load less frequently used pages, causing significant load on the server. As a result, the Web server can start to deny services to legitimate clients.

### 7.6.2 DDoS-2 Additional Filter Control

Pravail APS monitors the network traffic and mitigates attacks by using the protection settings that are defined for one or more protection groups.  A protection group represents one or more hosts that need to be protected. Each protection group is associated with a server type and one or more host servers of that type. For example, a protection group can represent a single Web server or a specific group of DNS servers.

The server type represents a class of hosts that a specific protection group protects. Each protection group is associated with a server type; each server type can be associated with multiple protection groups. The server type determines which protection settings are available for that protection group and which application-specific data is collected and displayed for that group. Pravail APS contains predefined, standard server types whose protection settings cover most situations.

Certain protection settings are available for all protection groups. Other settings include application-specific behavior and are available only if a protection group is associated with that type of application server. For example, the HTTP Rate Limiting settings are available for a Web Server protection group but not for a DNS Server protection group.

The categories of protection settings that are available for each of the standard server types are as follows:

**Table 7-4: Available protection settings for each standard server type**

| **Protection Settings Category** | **Server Type** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Generic Server** | **DNS Server** | **File Server** | **Mail Server** | **RLogin Server** | **VoIP Server** | **VPN Server** | **Web Server** |
| Application Misbehavior | x | | x | x | x | | x | x |
| Block Malformed DNS Traffic | x | x | | | | | | |
| Block Malformed SIP Traffic | x | | | | | x | | |
| Botnet Prevention | x | | | | | x | | x |
| CDN and Proxy Support | x | | | | | | | x |
| DNS Authentication | x | x | | | | | | |
| DNS NXDomain Rate Limiting | x | x | | | | | | |
| DNS Rate Limiting | x | x | | | | | | |
| DNS Regular Expression | x | x | | | | | | |
| Filter List | x | x | x | x | x | x | x | x |
| Fragment Detection | x | x | x | x | x | x | x | x |
| HTTP Header Regular Expressions | x | | | x | | x | | x |
| HTTP Rate Limiting | x | | | x | | x | | x |
| HTTP Reporting | x | | | | | x | | x |
| ICMP Flood Detection | x | x | x | x | x | x | x | x |
| Malformed HTTP Filtering | x | | | | | x | | x |
| Multicast Blocking | x | x | x | x | x | x | x | x |
| Payload Regular Expression | x | x | x | x | x | x | x | x |
| Private Address Blocking | x | x | x | x | x | x | x | x |
| Rate-based Blocking | x | x | x | x | x | x | x | x |
| SIP Request Limiting | x | | | | | x | | |
| Spoofed SYN Flood Prevention | x | x | x | x | x | x | x | x |
| TCP Connection Limiting | x | | x | x | | | | x |
| TCP Connection Reset | x | x | x | x | x | x | x | x |
| TCP SYN Flood Detection | x | x | x | x | x | x | x | x |
| TLS Attack Prevention | x | | x | x | | | x | x |
| Traffic Shaping | x | x | x | x | x | x | x | x |
| UDP Flood Detection | x | x | x | x | x | x | x | x |
| WebCrawler Support | x | x | | | | | | x |

The TOE can be put into 3 different modes Active (filtering), Inactive (monitoring), and BYPASS (no filtering or monitoring). The **active mode** is a state within the inline deployment mode, in which Pravail APS mitigates attacks in addition to monitoring traffic and detecting attacks. The **inactive mode** is a state within the inline deployment mode, in which Pravail APS analyzes traffic and detects attacks without performing mitigations. The **bypass mode** is state in which Pravail APS neither mitigates attacks, monitors traffic, or detects attacks. This mode is automatically entered when the Pravail APS goes into a fault mode.

The TOE also provides mitigation enforcement by means of Cloud signaling. **Cloud Signaling** is the process of requesting and receiving cloud-based mitigation of volumetric attacks in real time from an upstream service provider.

Key points for the traffic filtering:

a) The TOE support ALL protocol on Ethernet - they either get forwarded or dropped

b) Product inspects for DDoS in the following: TCP, UDP and ICMP

c) The packets inspected must be IPv4 but can have GRE and VLAN tags

d) IPv6 and ARP are always forwarded

e) All other traffic can be dropped or forward based on configuration

f) There is no filtering from the LAN to the WAN network traffic

The following table describes the filter types, settings, and DDoS classification that the filter supports.

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| application misbehavior | **Interrupt Count box:** Type the number of TCP FIN interruptions that are allowed from a single client before that client is temporarily blocked. To disable this setting, leave this box empty. | | x | | | |
| Blacklist | In the **Blacklisted Hosts box**, an administrator can type a source IP address or a source hostname.<br>In the **Blacklisted Countries list**, select a source country. In the Blacklisted Countries selection list, the countries are listed alphabetically and other, non-specific regions are listed after the countries.<br>In the **Blacklisted Domains box**, type the destination domain name. | x | x | x | x | x |
| Botnet | **Enable Basic Botnet Prevention buttons:** Click one of these buttons to enable or disable the inspection of traffic for missing HTTP header fields, which are a common indicator of botnet attacks.<br>Important: The Basic Botnet Prevention works only if Malformed HTTP Filtering is enabled. If Malformed HTTP Filtering disabled, the Basic Botnet Prevention for the corresponding protection level is disabled also.<br>**Enable AIF Botnet Signatures buttons:** Click one of these buttons to enable or disable the inspection of traffic based on the AIF signatures that define known botnet attacks.<br>**Prevent Slow Request Attacks buttons:** Click one of these buttons to enable or disable the inspection of traffic for requests that are characteristic of slow HTTP attacks. If this option is enabled, Pravail APS checks for HTTP requests that contain less than 500 bytes of data and do not end with \n. | x | | | | |
| CDN and Proxy | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |
| DNS Authentication | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |
| DNS NXDomian Rate Limiting | **DNS NXDomain Rate Limit box:** Type the number of failed queries to allow per second.<br>To disable this setting, leave this box empty. | | x | | | x |
| DNS Rate Limiting | **DNS Query Rate Limit box:** Type the maximum number of DNS queries per second that a source can send before it is blocked. This rate limit represents what is considered to be a reasonable maximum amount of DNS traffic.<br>To disable this setting, leave this box empty. | | x | | | |
| DNS Regular | **DNS Regular Expressions lines:** Type a regular expression to filter out DNS traffic | | x | | | |

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| Expression | with matching requests or headers. Use PCRE format. Type multiple regular expressions. Pravail APS uses the OR operator for multiple regular expressions. | | | | | |
| Filter List | **Filter FCAP Expressions box:** Type an FCAP expression that corresponds to the data that is desired to be matched. Type IP addresses or ranges, DNS names, CIDRs, or case-insensitive descriptive text.<br>Include a drop or pass keyword to specify the action to take on the matched data. If no specified action, Pravail APS uses a drop action. Type one expression per line. To include a comment, type a number sign (#) at the beginning of each comment line. | x | x | | | |
| Fragment Detection | **Enable Fragment Detection buttons:** Click one of these buttons to enable or disable this category.<br>**Maximum bps box:** Type the maximum amount of traffic (in bps) to allow from single source.<br>**Maximum pps box:** Type the maximum amount of traffic (in pps) to allow from a single source. | | x | x | | |
| HTTP Header | **Header Regular Expressions lines:** Type a regular expression to match HTTP requests or headers. Use PCRE format. Type multiple regular expressions. Pravail APS uses the OR operator for multiple regular expressions. | x | | | x | |
| HTTP Rate Limiting | **HTTP Request Limit box:** Type the number of HTTP requests to allow per second. An HTTP request is any type of request such as GET, POST, HEAD, or OPTIONS.<br>To disable this setting, leave this box empty.<br>**HTTP URL Limit box:** Type the number of requests for a unique HTTP object (specific URL) to allow per second. For example, the medium level defaults are 500 for the HTTP Request Limit and 15 for the HTTP URL Limit. If 100 requests for the same URL are received in one second, they are blocked because they exceed the URL limit.<br>To disable this setting, leave this box empty. | x | x | x | | |
| HTTP Reporting | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | x | | | | |
| ICMP Flood Detection | **Enable ICMP Flood Detection buttons:** Click one of these buttons to enable or disable this category.<br>**Maximum Request Rate box:** Type the maximum number of ICMP echo requests per second that a source can send before it is blocked. This rate limit represents what is considered to be a reasonable amount of ICMP traffic.<br>**Maximum bps box:** Type the maximum amount of traffic (in bps) to allow from a single source. | | x | | | |
| Malformed DNS | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this | | x | | | |

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| Traffic | category. | | | | | |
| Malformed HTTP Filtering | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category.<br>Important: The Basic Botnet Prevention works only if Malformed HTTP Filtering is enabled. If Malformed HTTP Filtering is disabled, the Basic Botnet Prevention for the corresponding protection level is disabled also. | | | | x | |
| Malformed SIP Traffic | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |
| Multicast blocking | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |
| Payload regular expression | **Payload Regular Expression TCP Ports:** Type the destination port numbers to define the TCP traffic to inspect. Use spaces or commas to separate multiple port numbers. Pravail APS applies the regular expressions to only the TCP packets that are destined for these ports.<br>**Payload Regular Expression UDP Ports box:** Type the destination port numbers to define the UDP traffic to inspect. Use spaces or commas to separate multiple port numbers. Pravail APS applies the regular expressions to only the UDP packets that are destined for these ports.<br>**Payload Regular Expression box:** Type the regular expression to apply to the payload traffic that matches the appropriate ports. Use PCRE format. Type multiple regular expressions; press ENTER after each one. Pravail APS uses the OR operator for multiple regular expressions. | x | x | | | |
| Private Address Blocking | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |
| Rate-based Blocking | **Bits per Second Threshold box:** Type the maximum rate of traffic in bits that a source can send before it is blocked.<br>**Packets per Second Threshold box:** Type the maximum rate of traffic in packets that a source can send before it is blocked. | | x | | | |
| SIP Request Limiting | **SIP Source Limit box:** Type the maximum number of SIP requests to allow per second.<br>To disable this setting, leave this box empty. | | x | | | |

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| Spoofed SYN Flood Prevention | **Prevent Spoofed SYN Floods buttons:** Click one of the following buttons to enable or disable this category:<br>OFF — Disable this category.<br>TCP — Enable TCP authentication.<br>TCP/HTTP — Enable both TCP authentication and HTTP authentication.<br>The selection determines which protection settings are available for this category.<br><br>**Except on ports box**: For applications that have difficulty with spoofed SYN flood authentication, type the affected application ports so that they are ignored during the authentication process.<br>Caution: If this category is disabled, all of the ports that are specified here are removed. If an administrator later re-enables this category, the ports do not re-appear.<br><br>**TCP Out of Sequence Authentication buttons:** Click one of these buttons to enable or disable the automatic<br>refresh of client connections during TCP SYN authentication.<br><br>**HTTP Authentication Method buttons:** Click one of the following buttons to authenticate the traffic on<br>ports 80 and 8080 before the traffic passes to the server:<br>Redirect: Use HTTP redirects to authenticate the traffic on specific HTTP ports.<br>Soft Reset: Automatically refresh client connections on an application specific basis during TCP SYN authentication. | | x | | | |
| TCP Connection Limiting | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | x | x | x | | x |

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| TCP Connection Reset | **Enable TCP Connection Reset buttons:** Click one of these buttons to enable or disable this category.<br>**Minimum Request Bit Rate box:** Type the minimum rate of bits per second that a host must maintain when sending an individual request. Pravail APS checks several times per minute to verify that the transmitted data does not fall below this limit. The data rate must fall below this limit for a minimum of 60 seconds for Pravail APS to reset the connection or block the host.<br>**TCP Connection Initial Timeout box:** Type the number of seconds that a connection can be idle after it is first established before it is blocked.<br>**Initial Timeout Required Data box:** Type the number of bytes that a host must send within the initial timeout period for the timeout to be canceled.<br>For example, the default TCP Connection Initial Timeout is 10 seconds and the default Initial Timeout Required Data is 1 byte. The connection has 10 seconds in which to send 1 byte of data. If that amount of data is not sent, then the connection is reset.<br>**Consecutive Violations before Blocking Source box**: Type the number of consecutive idle connections to allow before a host is blocked. Adjust this number higher for applications with multiple TCP control connections that might be idle simultaneously due to a single lack of user action. | | | x | | |
| TCP SYN Flood Detection | **Enable SYN Flood Detection buttons:** Click one of these buttons to enable or disable this category.<br>**SYN ACK Delta Rate box**: Type the allowable difference between the number of ACK packets and the number of SYN packets (SYN - ACK = delta). This rate should be lower than the SYN Rate. In legitimate traffic, the number of ACK packets from a specific source should exceed or be slightly less than the number of SYN packets from that source. This threshold represents the allowable difference between the two types of packets and allows Pravail APS to detect attackers that send only SYN packets. To disable this setting, leave this box empty.<br>**SYN Rate box:** Type the number of packets per second that a source can send before it is blocked. In a data center environment, a client typically does not establish a large number of connections per second. This threshold allows Pravail APS to detect very blatant SYN floods based on the number of connection requests from a single source. To disable this setting, leave this box empty. | | x | | | |
| TLS Attack Prevention | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | | x | | | |

| Filter List | Setting: Description | Botnet | Generic Bandwidth | Slow HTTP | Malformed HTTP | HTTP Cache |
|---|---|---|---|---|---|---|
| Traffic Shaping | **Enable Traffic Shaping buttons:** Click one of these buttons to enable or disable this category.<br>**Maximum bps box:** Type the maximum amount of traffic (in bps) to allow.<br>**Maximum pps box:** Type the maximum amount of traffic (in pps) to allow.<br>**Filter box (Optional):** Type an FCAP expression that corresponds to the data that is desired to be matched. Type IP addresses or ranges, DNS names, CIDRs, or case-insensitive descriptive text. Type one expression per line. To include a comment, type a number sign (#) at the beginning of each comment line. |  | x |  |  |  |
| UDP Flood Detection | **Enable UDP Flood Detection buttons:** Click one of these buttons to enable or disable this category.<br>**Maximum bps box:** Type the maximum amount of traffic (in bps) to allow from a single source.<br>**Maximum pps box:** Type the maximum amount of traffic (in pps) to allow from a single source. |  | x |  |  |  |
| Web Crawler | **Enabled and Disabled buttons:** Click one of these buttons to enable or disable this category. | x | x | x | x | x |
| Whitelist | Click the **Whitelist button** to the far right of the item’s name. The host is whitelisted for all protection groups even if it was blacklisted for specific protection groups only. Because only hosts can be whitelisted, this option is only available in the Blacklisted Hosts section. | x | x | x | x | x |

### 7.6.3 DDoS-3 Notification

When Pravail APS detects events, conditions, or errors in the system, it creates alerts to inform the user. Pravail APS can be configured to send notification messages to specified destinations to communicate certain alerts.

The alert type specifies the event category that can trigger a specific notification. An administrator can associate each notification destination with one or more of these alert types.

**Table 7-5: Alert Types**

| ***Alert Type*** | ***Causes*** |
|---|---|
| ***System*** | Hardware or system component events and other events that affect the system's health. For example, a system alert is created when an interface goes down. |
| ***Cloud*** | Specific Cloud Signaling events. For example, cloud alerts occur when traffic exceeds the configured threshold or when a communication error occurs between the network and the Cloud Signaling Server. |
| ***Protection*** | Someone changes the global protection level or a protection group's protection level. |
| ***Deployment*** | The deployment mode is changed. |
| ***Blocked Host*** | Source hosts are blocked. |
| ***Bandwidth*** | A protection group's traffic exceeds one or more traffic thresholds, or the system's traffic exceeds 90 percent of its licensed throughput limit. |

The TOE supports 4 types of notifications:

- Email: Pravail APS sends email notifications to the destination address that is administratively specified. The notifications appear to come from the sender address that is specified. Pravail APS queues email messages for one minute, and then send them in a batch. When an email notification contains multiple alerts, Pravail APS sends one summary email. The notification includes the alert description and the alert type. It also includes the default URL hostname, which is configured on the Configure General Settings page. The recipient can copy and paste the URL into a browser to navigate to the Pravail APS server that sent the alert. Pravail APS sends the email notifications through the SMTP server that is configured using the Configure General Settings page on the Administration menu.

- SNMP: Pravail APS sends notifications to a network management system as SNMP traps. The Arbor SMI MIB and the Pravail APS MIB define the SNMP notification format. Pravail APS supports SNMP version 2 and SNMP version 3 for notifications.

- Syslog: Pravail APS sends notifications to a security event management system as syslog messages. The notification includes the alert description and the alert type. It also includes a URL that the recipient can copy and paste into a browser to navigate directly to the event.

- Cloud Signaling Mitigation Request: Pravail APS signals to the cloud service provider that mitigation help is needed via a trusted channel. The Pravail APS mitigation signal does not depend on a response from the Cloud Signaling Server. Therefore, overwhelming incoming attacks do not prevent the outgoing mitigation requests.

An administrator has the ability to customize the actual notification message to include/not include certain fields.

The TOE also visually displays the alert event on 2 different locations in the Web UI.  The first visual alert is on the Summary Page.  The Summary Page only displays the Active alerts.  The Management Tab shows not only the Active alerts but also allows the administrator to browse/search through the historical listing of alerts.

# 8 Pravail APS Glossary of Terms

## a

**AAA** (Authentication, Authorization, & Accounting) — An acronym that describes the process of authorizing access to a system, authenticating the identity of users, and logging their behaviors.

**active mode** — A state within the inline deployment mode, in which Pravail APS mitigates attacks in addition to monitoring traffic and detecting attacks.

**address** — A coded representation that uniquely identifies a particular network identity.

**AIF** (ATLAS Intelligence Feed) — A service that downloads real-time threat information from Arbor's Active Threat Level Analysis System (ATLAS). This information is used to detect and block emerging botnet attacks and application-layer attacks.

**alert** — A message informing the user that certain events, conditions, or errors in the system have occurred.

**anomaly** — An event or condition in the network that is identified as an abnormality when compared to a predefined illegal traffic pattern.

**API** (Application Programming Interface) — A well-defined set of function calls providing high-level controls for underlying services.

**Arbor Smart bar** — An area of the product's user interface that contains icons for performing certain actions.

**ArbOS** — Arbor's proprietary, embedded operating system.

**ASCII** (American Standard Code for Information Interchange) — A coded representation for standard alphabetic, numeric, and punctuation characters, also referred to as "plain text".

**ATLAS** (Active Threat Level Analysis System) — A globally scoped threat analysis network that analyzes data from darknets and the Internet's core backbone to provide information to participating customers about malware, exploits, phishing, and botnets.

**authentication** — An identity verification process.

## b

**blacklist** — A list of hosts and destinations block — To prevent traffic from passing to the network, or to prevent a host from sending traffic. In Pravail APS, blocking occurs for a specific length of time, after which the traffic is allowed to pass again.

**bot** — A program that runs run automated tasks over the Internet.

**botnet** — A set of compromised computers (bots) that respond to a controlling server to generate attack traffic against a victim server.

**bps** — Bits per second.

**bypass mode** — A state in which Pravail APS neither mitigates attacks, monitors traffic, or detects attacks. This mode is automatically entered when the Pravail APS goes into a fault mode.

## c

**CA** (Certificate Authority) — A third party that issues digital certificates for use by other parties. CAs are characteristic of many public key infrastructure (PKI) schemes.

**CDN** (Content Delivery Network) — A collection of Web servers that contain duplicated content and are distributed across multiple locations to deliver content to users based on proximity.

**CIDR** (Classless Inter-Domain Routing) — Method for classifying and grouping Internet addresses.

**CLI** (command line interface) — A user interface that uses a command line, such as a terminal or console (as opposed to a graphical user interface).

**client** — The component of client/server computing that uses a service offered by a server.

**cloud** — A metaphor for the Internet.

**Cloud Signaling** — Cloud Signaling is the process of requesting and receiving cloud-based mitigation of volumetric attacks in real time from an upstream service provider.

**Cloud Signaling widget** — A graphical element in the Web UI that allows the user to monitor the status of the Cloud Signaling connection and mitigations in real time. It also allows the user to enable, activate, and deactivate Cloud Signaling.

**CSV** (comma-separated values) file — A file that stores spreadsheet or database information in plain text, with one record on each line, and each field within the record separated by a comma.
**customer edge** — The location at the customer premises of the router that connects to the provider edge of one or more service provider networks.
**customer edge router** — A router within a customer's network that is connected to an ISP's customer peering edge.

# d

**Dark IP** — Regions of the IP address space that are reserved or known to be unused.
**data center** — A centralized facility that houses computer systems and associated components, such as telecommunications and storage systems, and is used for processing or transmitting data.
**DDoS** (Distributed Denial of Service) — An interruption of network availability typically caused by many, distributed malicious sources.
**deployment mode** — Indicates how Pravail APS is installed in the network: inline or out-of-line through a span port or network tap (monitor).
**DNS** (Domain Name System) — A system that translates numeric IP addresses into meaningful, human consumable names and vice-versa.
**DNS server** — A server that uses the Domain Name System (DNS) to translate or resolve human-readable domain names and hostnames into the machine-readable IP addresses.
**DoS** (Denial of Service) — An interruption of network availability typically caused by malicious sources.

# e

**edge** — The outer perimeter of a network.
**encryption** — The process by which plain text is scrambled in such a way as to hide its content.
**Ethernet** — A series of technologies used for communication on local area networks.
**exploit** — Tools intended to take advantage of security holes or inherent flaws in the design of network applications, devices, or infrastructures.

# f

**failover** — A configuration of two devices so that if one device fails, the second device takes over the duties of the first, ensuring continued service.
**FCAP** — A fingerprint expression language that describes and matches traffic information.
**Fibre Channel** — Gigabit-speed network technology primarily used for storage networking.
**fingerprint** — A pattern or profile of traffic that suggests or represents an attack. Also known as a signature.
**firewall** — A security measure that monitors and controls the types of packets allowed in and out of a network, based on a set of configured rules and filters.
**FQDN** (Fully Qualified Domain Name) — A complete domain name, including both the registered domain name and any preceding node information.
**FTP** (File Transfer Protocol) — A TCP/IP protocol for transferring files across a network.

# g

**Gb** — Gigabit.
**GB** — Gigabyte.
**Gbps** — Gigabits per second.
**global protection level** — Determines which protection settings are in use for the entire system.
**GMT** (Greenwich Mean Time) — A world time standard that is deprecated and replaced by UTC.
**GRE** (Generic Routing Encapsulation) — A protocol that is used to transport packets from one network through another network.
**GRE tunnel** — A logical interface whose endpoints are the tunnel source address and tunnel destination address.

# h

**handshake** — The process or action that establishes communication between two telecommunications devices.

**header** — The data that appears at the beginning of a packet to provide information about the file or the transmission.
**heartbeat** — A periodic signal generated by hardware or software to indicate that it is still running.
**host** — A networked computer (client or server); in contrast to a router or switch.
**HTTP** (HyperText Transfer Protocol) — A protocol used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.
**HTTPS** (HyperText Transfer Protocol over SSL) — The combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism.

## i

**ICMP** (Internet Control Message Protocol) — An IP protocol that delivers error and control messages between **TCP/IP** enabled network devices, for example, ping packets.
**IMAP** (Internet Message Access Protocol) — An application layer Internet protocol that allows a local client to access email on a remote server. (Also known as Internet Mail Access Protocol, Interactive Mail Access Protocol, and Interim Mail Access Protocol.)
**inactive mode** — A state within the inline deployment mode, in which Pravail APS analyzes traffic and detects attacks without performing mitigations.
**inline mode** — A deployment mode in which Pravail APS acts as a physical connection between two end points. All of the traffic that traverses the network flows through Pravail APS.
**interface** — An interconnection between routers, switches, or hosts.
**IP** (Internet Protocol) — A connectionless network layer protocol used for packet delivery between hosts and devices on a TCP/IP network.
**IP address** — A unique identifier for a host or device on a TCP/IP network.
**IPS** (Intrusion Prevention System) — A computer security device that exercises access control to protect computers from exploitation.
**ISP** (Internet Service Provider) — A business or organization that provides to consumers access to the Internet and related services.

## l

**LAN** (Local Area Network) — A typically small network that is confined to a small geographic space.

## k

**Kbps** — Kilobits per second.

## m

**malformed** — Refers to requests or packets that do not conform to the RFC standards for Internet protocol. Such requests or packets are often used in DoS attacks.
**Mbps** — Megabits per second.
**MBps** — Megabytes per second.
**MIB** (Management Information Base) — A database used by the SNMP protocol to manage devices in a network. The SNMP polling device uses this to understand Pravail APS SNMP traps.
**mitigation** — The process of using recommendations to apply policies to the network to reduce the effects of an attack.
**monitor mode** — A deployment mode in which Pravail APS is deployed out-of-line through a span port or network tap. Pravail APS monitors traffic and detects attacks but does not mitigate the attacks.
**MSSP** (Managed Security Service Provider) — An Internet service provider (ISP) that provides an organization with network security management,
**multicast** — Protocols that address multiple IP addresses with a single packet (as opposed to unicast and broadcast protocols).

## n

**netmask** — A dotted quad notation number that routers use to determine which part of the address is the network address and which part is the host address.
**network tap** — A hardware device that sends a copy of network traffic to another attached device for passive monitoring.
**NIC** (Network Interface Card) — A hardware component that maintains a network interface connection. notification — An email message, SNMP trap, or syslog message that is sent to specified destinations to communicate certain alerts.
**NTP** (Network Time Protocol) — A protocol that synchronizes clock times in a network of computers.
**NXDomain** — A response that results when DNS is unable to resolve a domain name.

# o

**out-of-band** — Communication signals that occur outside of the channels that are normally used for data.

# p

**packet** — A unit of data transmitted across the network that includes control information along with actual content.
**password** — A secret code used to gain access to a computer system.
**payload** — The data in a packet that follows the TCP and UDP header data.
**PCAP** (packet capture) file — A file that consists of data packets that have been sent over a network.
**pps** — Packets per second.
**ping** — An ICMP request to determine if a host is responsive.
**policy** — The set of rules that network operators determine to be acceptable or unacceptable for their network.
**POP** (Post Office Protocol) — A TCP/IP email protocol for retrieving messages from a remote server.
**PoP** (Point of Presence) — A physical connection between telecommunications networks.
**port** — A field in TCP and UDP packet headers that corresponds to an application level service (for example TCP port 80 corresponds to HTTP).
**prefix** — The initial part of a network address, which is used in address delegation and routing.
**protection category** — A group of related protection settings that detect a specific type of attack traffic.
**protection group** — A collection of one or more protected hosts that are associated with a specific type of server.
**protection level** — Defines the strength of protection against a network attack and the associated intrusiveness and risk of blocking legitimate traffic. The protection level can be set globally or for specific protection groups.
**protection mode** — A state within the inline deployment mode, in which the mitigations are either active or inactive.
**protection settings** — The criteria by which Pravail APS defines legitimate traffic and attack traffic.
**protocol** — A well-defined language used by networking entities to communicate with one another.

# r

**RADIUS** (Remote Authentication Dial In User Service) — A client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

**rate limit** — The number of requests, packets, bits, or other measurement of data that a host is allowed to send within a specified amount of time.
**RDN** (Registered Domain Name) — A domain name as registered, without any preceding node information (for example, “arbor.net” instead of www.arbor.net).
**real time** — When systems respond or data is supplied as events happen.
**redundancy** — The duplication of devices, services, or connections so that, in the event of a failure, the duplicate item can perform the work of the item that failed.
**refinement** — The process of continually gathering information about anomalous activity that is observed on a network.
**regular expression** — A standard set of rules for matching a specified pattern in text. Often abbreviated as regex or regexp.
**report** — An informational page that presents data about a traffic type or event.
**route** — A path that a packet takes through a network.

**router** — A device that connects one network to another. Packets are forwarded from one router to another until they reach their ultimate destination.

# S

**secret key** — A secret that is shared only between a sender and receiver of data.
**server type** — A class of servers that Pravail APS protects and that is associated with one or more protection groups.
**SIP** (Standard Initiation Protocol) — An IP network protocol that is used for VoIP (Voice Over IP) telephony.
signature — A pattern or profile of traffic that suggests or represents an attack. Also known as a fingerprint.
**SMTP** (Simple Mail Transfer Protocol) — The de facto standard protocol for email transmissions across the Internet.
**SNMP** (Simple Network Management Protocol) — A standard protocol that allows routers and other network devices to export information about their routing tables and other state information.
**span port** — A designated port on a network switch onto which traffic from other ports is mirrored.
**spoofing** — A situation in which one person or program successfully masquerades as another by falsifying data (usually an IP address) and thereby gains an illegitimate advantage.
**SSH** (Secure Shell) — A command line interface and protocol for securely accessing a remote computer. SSH is also known as Secure Socket Shell.
**SSL** (Secure Sockets Layer) — A protocol for secure communications on the Internet for such things as Web browsing, email, instant messaging, and other data transfers.

**SSL certificate** — A file that is installed on a secure Web server to identify a Web site and verify that the Web site is secure and reliable.
**stacked graph** — A graph in an Arbor Networks product that displays multiple types of data in a color-coded stack.
**syslog** — A file that records certain events or all of the events that occur in a particular system. Also, a service for logging data.

# t

**TACACS+** (Terminal Access Controller Access Control System +) — An authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether that user is allowed to access a given system.
**target** — A victim host or network of a malicious denial of service (DoS) attack.
**TCP** (Transmission Control Protocol) — A connection-based, transport protocol that provides reliable delivery of packets across the Internet.
**TCP/IP** — A suite of protocols that controls the delivery of messages across the Internet.
**Telnet** — A TCP protocol used primarily for unencrypted CLI communications (usually deprecated and replaced by SSH).
throughput — The data transfer rate of a network or device.
**TLS** (Transport Layer Security) — An encryption protocol for the secure transmission of data over the Internet.
**TLS** is based on, and has succeeded, SSL.

# u

**UDP** (User Datagram Protocol) — An unreliable, connectionless, communication protocol.
unblock — To remove a source or destination from the temporarily blocked list without adding it to the whitelist.
**UNC** (Universal Naming Convention) — A standard which originated from UNIX for identifying servers, printers, and other resources in a network.
**URI** (Uniform Resource Identifier) — A protocol, login, host, port, path, etc. in a standard format used to reference a network resource, (for example http://arbor.net/).
**URL** (Uniform Resource Locator) — Usually a synonym for URI.
**UTC** (Universal Time Coordinated) — The time zone at zero degrees longitude, which replaces GMT as the world time standard.

# V

**VLAN** (Virtual Local Area Network) — Hosts connected in an infrastructure that simulates a local area network, when the hosts are remotely located, or to segment a physical local network into smaller, virtual pieces.

**VoIP** (Voice over Internet Protocol) — Routing voice communications (such as phone calls) through an IP network.

**volumetric attack** — A type of DDoS attack that is generally high bandwidth and that originates from a large number of geographically distributed bots.

**VPN** (Virtual Private Network) — A private communications network that is often used within a company, or by several companies or organizations, to communicate confidentially over a public network using encrypted tunnels.

**vulnerability** — A security weakness that could potentially be exploited.

# W

**WAN** (Wide Area Network) — A computer network that covers a broad area. (Also Wireless Area Network, meaning a wireless network.)

**Web UI** (User Interface) — A Web-based interface for using an Arbor Networks product.

**whitelist** — A list of hosts whose traffic is passed without further inspection. To add a host to the whitelist.

**widget** — A graphical element in a user interface that displays information about an application and allows the user to interact with the application.

# X

**XML** (eXtensible Markup Language) — A metalanguage written in Standard Generalized Markup Language (SGML) that allows one to design a markup language for easy interchange of documents on the World Wide Web.