

DEFENSEPRO AND APSOLUTE VISION SECURITY TARGET

Author: Yariv Katz
Date: April 16, 2024

Version Control

Version	Comments	Date
1.0	First document release	August 2021
1.1	Added table and figure titles Changed document style to match Radware	May 6 th 2022
1.2	Changes introduced to align with DefensePro and APSolute Vision documentation: <ul style="list-style-type: none"> - Heavily modified section 2.3, along with its subsections to align the specification of TOE images and components. 	June 7 th 2022
1.3	Changes introduced: <ul style="list-style-type: none"> - Removed disclosure section. 	September 7 th , 2022
1.4	Changes introduced: <ul style="list-style-type: none"> - Updated TOE delivery 	October 6 th , 2022
1.5	Changes introduced: <ul style="list-style-type: none"> - Fixed invalid reference to the release date in the front page. - Clarified the acronyms of the functionality outside of the scope in section 2.2. - Updated section 9 to include the missing acronyms. - Fixed the section numbers of the subsections inside the Physical Scope (2.3.1.X). - Fixed an errata in section 2.2.1 where it only listed the maximum capacity as 160 Gbps instead of 200 Gbps. - Reformulated the assumptions (4.4) to be more focused and concise. - Updated the SPD (5.2 and 5.3) to accommodate the updated assumptions. - Reworded the Physical Scope (2.3.1) to more concisely reflect the composition of the TOE as a series of images for each component and platform. Additionally, the internal and management network have been merged in order to simplify the security scenario. - Updated the TOE name (2.1) to include the type of product. - Reformulated the TOE Overview (2.2) and TOE Description (2.3) to include a description on how the TOE is a series of products. 	June 15 th , 2023

Version	Comments	Date
	<ul style="list-style-type: none"> - Updated section 7.2 to clarify that no extended component is being used. - Removed FPT_STM.1 and replaced with a new assumption and security objective for the operational environment A.SYSTEM_TIME, which more accurately reflects that the system date is dependent on the underlying platform. - Updated the TOE Summary Specification (8) to reflect the merge between internal and management network. Additionally, the description of the audit storage has been updated to remove the invalid statement for the DP. 	
1.6	<p>Changes introduced:</p> <ul style="list-style-type: none"> - INT.01: Added section 2.2.3.6 to clarify the need for software licenses in order to operate with the TOE. - INT.02: Changed column “Document ID” to “Version” in table 7, since CC-specific documents do not have ID. - INT.03: Removed section 2.3.2.5 Protection of the TSF, since version 1.5 already removed the only requirement covering it (FPT_STM.1). - OBJ.02: Updated the security objectives for the operational environment (5.2) to clarify their interpretation and applicability. - GEN.01: Clarified in sections 2.3.1.6 and 2.3.1.7 that the guidance documentation, including the CC-specific guide, are delivered via the developer web portal. - PRE.03: Updated the list of guidance documentation in section 2.3.1.6. - FSP.01: Removed ambiguous language when defining the usage of interfaces in section 2.3.1.8. 	October 11 th , 2023
1.7	<p>Changes introduced:</p> <ul style="list-style-type: none"> - OR005-OPE.01: Updated section 2.3.1.8 to match the updated guidance configuration of the interfaces. - Updated section 2.2 to remove an invalid reference to Protection of the TSF. - Updated section 2.2 to clarify a statement about TOE users being administrators. 	January 10 th , 2024

Version	Comments	Date
	<ul style="list-style-type: none"> - Updated section 5.2.1 to clarify that the operational parameters are also accounted for as part of OE.PHYSICAL_PROTECTION. - Updated section 2.3.1.6 to account for the newer version of the CC guide. 	
1.8	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Fixed errata in section 5.3.3 when referencing the OE.Physical_Protection objective. - Removed an invalid assignment of when audit events are generated (FAU_GEN.1) that does not take place. - OR006-IND.02: Removed FTA_SSL.3 due to the erratic behaviour discovered in ATE. - Updated section 2.3.1.6 to account for the newer version of the CC guide. 	January 25 th , 2024
1.9	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Removed a potentially conflicting description of the audit storage implementation in section 8.1.1. - OR008-REQ.01: No changes made, since the issue is related to a misinterpretation of the FDP_IFF.1 definition. Network addresses, traffic bandwidth, quota values and query rates are attributes of unauthenticated users or entities that transmit traffic through the TOE. - OR008-REQ.02: Added profile action as a configurable attribute in FMT_MSA.1. 	April 1 st , 2024
2.0	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Updated the description of the evaluated configuration to be more explicit in how the administrators must not use certain interfaces. - Added application note to FMT_MSA.3 for clarifying the meaning of permissive values. - Changed the document identifier to be consistent with the document title. - Updated the hashes of the Common Criteria guides 	April 16 th , 2024



Version	Comments	Date
	- The numbering of some sections has been updated to be consistent with the document numbering.	



Table of Contents

1. Scope of the Document	9
2. Introduction	10
2.1 Identification	10
2.2 TOE Overview	10
2.2.1 TOE Usage	11
2.2.2 TOE Type	11
2.2.3 Non-TOE Hardware/Firmware/Software	11
2.3 TOE description	13
2.3.1 Physical Scope	14
2.3.2 Logical Scope	20
3. Conformance Claims	22
3.1 Common Criteria Conformance Claim	22
3.2 Protection Profile Conformance Claim	22
3.3 Package Claim	22
3.4 Conformance rationale	22
4. Security Problem Definition	23
4.1 TOE Assets	23
4.1.1 AS.CONFIGURATION	23
4.1.2 AS.LEGITIMATE_TRAFFIC	23
4.1.3 AS.CORE_FUNCTIONALITY	23
4.2 Threats	23
4.2.1 T.DOS	23
4.2.2 T.ATTACK_MITIGATION_BYPASS	23
4.3 Organizational Policies	23
4.3.1 OSP.ROLES	23
4.3.2 OSP.LOGS	23
4.3.3 OSP.ACCOUNTABILITY	24
4.3.4 OSP.TRUSTED_ADMINISTRATORS	24



4.4	Assumptions	24
4.4.1	A.PHYSICAL_PROTECTION	24
4.4.2	A.MANAGEMENT_SEPARATION	24
4.4.3	A.TRUSTED_PLATFORM	24
4.4.4	A.LIMITED_FUNCTIONALITY	24
4.4.5	A.NO_EVIL	24
4.4.6	A.SYSTEM_TIME	24
5.	Security Objectives	25
5.1	Security Objectives for the TOE	25
5.1.1	O.ACCESS	25
5.1.2	O.ADMINISTRATION	25
5.1.3	O.AUDIT	25
5.1.4	O.ATTACK_MITIGATION	25
5.2	Security Objectives for the Operational Environment	25
5.2.1	OE.PHYSICAL_PROTECTION	25
5.2.2	OE.MANAGEMENT_SEPARATION	25
5.2.3	OE.TRUSTED_PLATFORM	26
5.2.4	OE.NO_GENERAL_PURPOSE	26
5.2.5	OE.TRUSTED_ADMIN	26
5.2.6	OE.SYSTEM_TIME	26
5.3	Security Objectives Rationale	26
5.3.1	Threats	27
5.3.2	Organizational Security Policies	27
5.3.3	Assumptions	28
6.	Extended components definition	29
6.1	Security functional requirements	29
6.2	Security Assurance Requirements	29
7.	Security Requirements	30
7.1	Conventions	30



7.2	Security Functional Requirements	30
7.2.1	Security Audit (FAU).....	31
7.2.2	Identification and Authentication (FIA)	32
7.2.3	User Data Protection (FDP)	33
7.2.4	Security Management (FMT)	34
7.2.5	TOE Access (FTA)	36
7.3	Assurance Security Requirements.....	36
7.4	Security Requirements Rationale	37
7.4.1	Security Functional Requirements Rationale.....	37
7.4.2	Security Assurance Requirements Rationale	41
8.	TOE Summary Specification.....	42
8.1	Description on how toe meets each sFR	42
8.1.1	Security Audit.....	42
8.1.2	Identification and Authentication.....	42
8.1.3	User Data Protection.....	42
8.1.4	Security Management.....	43
8.1.5	TOE Access	44
8.2	Functionality Outside of the Scope	44
9.	Acronyms	45
10.	References	46



1. Scope of the Document

The aim of this document is to define the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements.

2. Introduction

2.1 IDENTIFICATION

Document Identifier:	DefensePro and APSolute Vision Security Target
Document Version:	2.0
TOE Name:	DefensePro & APSolute Vision Attack Mitigation System
TOE Version:	APSolute Vision 4.85.00 DefensePro 8.26.1.0
TOE Type:	Attack Mitigation System
Evaluation Type:	Series of products
Created By:	Yariv Katz
Publication Date:	April 16, 2024

TABLE 1 - TOE IDENTIFICATION

2.2 TOE OVERVIEW


The TOE is a series of products which themselves are composed of two independent components: the DefensePro 8.26.1.0 and the APSolute Vision 4.85.00. Either of them can be running directly on a hardware appliance, or on a virtualized environment (Virtual Appliance). For each of the supported platforms, be it the hardware appliances or the virtualized environments, the TOE has a corresponding TOE component image which allows the installation of one of the components. Therefore, the series of products consist of all pair combinations of the different component images.

The TOE is designed to act as a real-time perimeter attack mitigation system, securing organizations against emerging network attacks, Denial of Service (DoS) and Distributed-DoS (DDoS).

The DefensePro 8.26.1.0 acts as a transparent proxy located at the edge of the data center. Meanwhile, the usage of the APSolute Vision 4.85.00 is required in order to be more easily managed, configured and monitored. Given the nature of the TOE, all of the TOE users are administrators with different level of privileges that interact with the TOE, thus hence forward they will be referenced as the *TOE Administrators*.

Additionally, the TOE allows the following major security features:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access



On the other hand, the TOE allows the following functionalities outside of the scope the evaluation:

- ADC: Used to balance the traffic among servers and filter or block traffic associated with a DDoS attack.
- AVR: Used to identify and verify malicious or suspicious traffic at the application layer.
- APM: Used to monitor and analyse real-time application performance, it helps to identify and mitigate the negative effects of a DDoS attack.
- DPM: Used to administrate and coordinate various devices such as firewalls, routers, ADCs, among others, for unified and effective response to a DDoS attack.
- DefenseFlow: Is a network DDoS attack prevention and cyber control application.
- AppWall: Is a web application firewall used to protect against web applications attacks.

2.2.1 TOE USAGE

The TOE makes use of network tapping techniques to observe and catalogue traffic, in order to interrupt attacks. It separates the networks of the customer infrastructure in an unprotected network and a protected network, then monitor traffic and block attacks coming from the unprotected network to the protected network, detecting attacks from layer 3 to layer 7.

Traffic up to 200 Gbps can be monitored by using the DefensePro appliances, or up to 40 Gbps on a virtualized environment.

2.2.2 TOE TYPE

The TOE is a real-time Denial of Service (DoS) and Distributed-DoS (DDoS) attack mitigation system.

2.2.3 NON-TOE HARDWARE/FIRMWARE/SOFTWARE

The following components are required for operation of the TOE in CC-evaluated configuration:

2.2.3.1 DEFENSEPRO 8.26.1.0 PHYSICAL APPLIANCES

The TOE is deployed on physical appliances or on virtual appliances, both of which are outside of the scope of the evaluation.

For bare-metal installations, at least one of the following appliances is required:

- DefensePro 6
- DefensePro 20
- DefensePro 60
- DefensePro 110
- DefensePro 200

- DefensePro 220
- DefensePro 400

Note: the total DDoS protection throughput will be dependent on the specific hardware appliance and the acquired license.

2.2.3.2 DEFENSEPRO 8.26.1.0 VIRTUAL APPLIANCES

For Virtual Appliance (VA) installations, the following minimum specs apply.

- Supported Virtualization Platforms:
 - KVM
 - VMWare
- System Requirements:
 - vCPU: 2
 - Recommended Intel server-grade processors: Westmere, Sandy-bridge, Ivy-bridge, Haswell, Broadwell, Skylake
 - RAM: 4 GB per vCPU + 5 GB (16 GB minimum recommended)
 - Disk space: 10 GB
 - Network Interfaces: 3

For pass-through operation (non-virtualized interfaces on virtual machines), the following Network Interface Cards are recommended:

- Intel® Ethernet Server Adapter X520, 10 GbE
- Intel® Ethernet Controller XL710, 40 GbE
- Intel® Ethernet Network Adapter XXV710, 10/25 GbE

Note: the total DDoS protection throughput will be dependent on the specific virtual platform hardware capabilities and the acquired license.

2.2.3.3 APSOLUTE VISION 4.85.00 PHYSICAL APPLIANCES

For bare-metal installations, the following appliance is required:

- APSolute Vision Server ODS-VL2

2.2.3.4 APSOLUTE VISION 4.85.00 VIRTUAL APPLIANCES

For Virtual Appliance (VA) installations, the following minimum specs apply:

Virtualization platform:

- VMWare
- KVM
- KVM (OpenStack)
- Hyper-V

System Requirements:

- vCPU: 8
- RAM: 32 GB
- Disk space: 500 GB
- NICs: 3

2.2.3.5 WEB BROWSER

In order to access the TOE via management Interfaces (HTTPS-AP) the following web browser can be used:

- Chrome
- Firefox
- MS Edge

2.2.3.6 SOFTWARE LICENSES

In order to use the TOE the user needs to provide software licenses which determine, in conjunction with the underlying platform, the throughput capacity of the TOE. For example, a hardware appliance DefensePro 6 may be used with a throughput license of 1Gbps which would limit the processing throughput to that amount.

Other type of licenses includes the number of CPUs, the number of managed devices, etc. Nonetheless, the capabilities offered by the TOE, DoS protection, would still be the same in terms of security features. Each component, DefensePro and APSolute Vision, need their own licenses and they are acquired from the developer after purchase of the TOE.

2.3 TOE DESCRIPTION

The TOE is composed of the **DefensePro 8.26.1.0** (running on DefensePro appliances or in a Virtual Appliance) and **APSolute Vision 4.85.00** (running on APSolute Vision appliances or in a Virtual Appliance). If the TOE is configured on bare-metal hardware, using the appliances defined in section 2.2.3, the following diagram relates the evaluated elements.

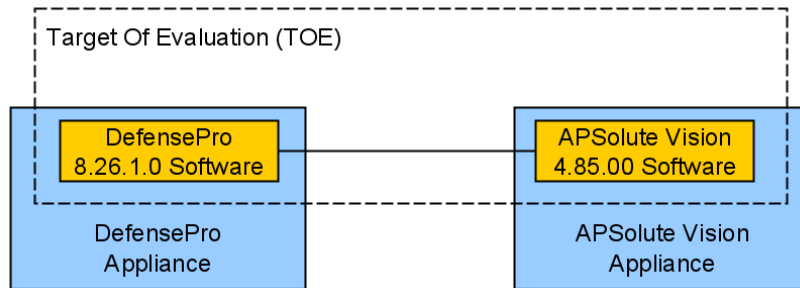


FIGURE 1 - PHYSICAL SCOPE ON APPLIANCES

In case the TOE is running on a Virtual Appliance (VA), the TOE evaluated elements behave under a logically equivalent diagram:

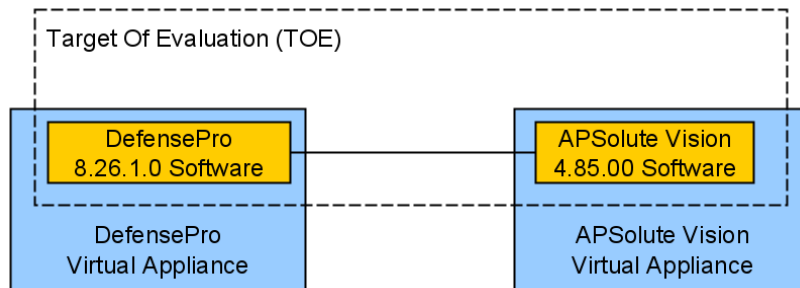


FIGURE 2 - PHYSICAL SCOPE ON VA

The differences between the bare-metal and the Virtual Appliance configurations of the TOE are only related to the throughput capacity, as the bare-metal system has specifically-selected hardware that executes the filtering at a Layer 2/3 level, whereas the Virtual Appliances perform the full filtering on the virtual NICs. In both cases the filtering results and the algorithms, which determine whether the traffic is benign or not, are functionally equivalent. The hardware acceleration is just performed on a specialized ASIC instead of the CPU to ensure a high-performance throughput can be achieved, for carrier grade solutions. Therefore, even mixed deployments, hardware AP and virtual DP, or vice versa, are equivalent and can be considered another instance of the series of products.

2.3.1 PHYSICAL SCOPE

This section outlines the physical scope of the TOE and all of the complementary parts needed for the proper usage of the TOE.

Radware maintains a single code base where all of the product features (TSF included) are implemented. The code base is then compiled and packaged specifically for each of the supported underlying platforms, resulting in multiple images. Thus, any change to the code base is observable and applicable to all platforms, guaranteeing the complete equivalency at the functional and security level.

2.3.1.1 DEFENSEPRO 8.26.1.0 PHYSICAL APPLIANCES

The physical appliances may not include the correct version of the TOE, hence when the appliance is received the end user must perform an upgrade process in order to upgrade the TOE to its correct version.

#	File Name	Hardware Platform	SHA-256
1	DefensePro_6-20-60-110-220-200-400_v8-26-1-0-b93.tgz	DefensePro 6 DefensePro 20 DefensePro 60 DefensePro 110 DefensePro 200 DefensePro 220 DefensePro 400	47F14F430F662E7416AC999CFB1AB9E4B61B01146B11105F1D0690BE19800BD2

TABLE 2 - DEFENSEPRO 8.26.1.0 PHYSICAL APPLIANCE IMAGES

2.3.1.2 APSOLUTE VISION 4.85.00 PHYSICAL APPLIANCES

The physical appliances may not include the correct version of the TOE hence when the appliance is received, the end user must perform a re-installation process in order to setup the TOE to its correct version.

#	File Name	Hardware Platform	SHA-256
1	APSoluteVision-USB-4-85-00-40-x86_64.iso	APSolute Vision Server ODS-VL2	ECBA902692528E3995693B385C5BC8649021BC09FEAE1EBFA45E760835EB3922

TABLE 3 - APSOLUTE VISION 4.85.00 PHYSICAL APPLIANCE IMAGES

2.3.1.3 DEFENSEPRO 8.26.1.0 VIRTUAL APPLIANCES

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the DefensePro 8.26.1.0. The VAs always come as a complete DefensePro 8.26.1.0 instance for each supported platform and/or format:

#	File Name	Virtualization Platform	SHA-256
1	DefensePro_VA_v8-26-1-0-b93_ISO_KVM.iso	KVM (ISO Format)	193F3E67CC56F7A6A2A880F74E2F452395A3308271C8B703491EF0F84FD26A24
2	DefensePro_VA_v8-26-1-0-b93_Full_Install_KVM.tgz	KVM (tgz Format)	B8D0D68695159AF3AFCE304295C78D9D6223E9C0C6E8767A81AB7E3B8498CA33

#	File Name	Virtualization Platform	SHA-256
3	DefensePro_VA_v8-26-1-0-b93_Full_Install_VMware.ova	VMWare	E1546ED74372058425AFC8D674AA741CF3D77E93E071BB9386742CA7E6458034

TABLE 4 DEFENSEPRO 8.26.1.0 VIRTUAL APPLIANCES IMAGES

Note: For the KVM platform two installation options are included, one for emulating an optical disc image; and the other one including supporting scripts to create the entire VM.

2.3.1.4 APSOLUTE VISION 4.85.00 VIRTUAL APPLIANCES

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the APSolute Vision 4.85.00. The VAs always come as a complete APSolute Vision 4.85.00 instance for each supported platform and/or format:

#	File Name	Virtualization Platform	SHA-256
1	APSoluteVision-4-85-00-43-x86_64.iso	Generic	AB37D4EC44A998BB3976851AE543FE9933A303EC2CDE97591158CE0E65412256
2	Vision-4-85-00-KVM_43_prod.qcow2	KVM (OpenStack)	4AB4579C0BA21C8AF7E0D6F9D54CADB96841FAFB1846E404FB403F03D58F9005
3	Vision-4-85-00-VMware_43_Basic.ova	VMWare(OVA Format)	2C251F27F8E5CBF0A12B0CAC043604FAD8A41268C776FA4541BC38BB974F0A44

TABLE 5 APSOLUTE VISION 4.85.00 VIRTUAL APPLIANCES IMAGES

Note: The generic image is in ISO format which emulates an optical disc image and can be used to install on various platforms such as Hyper-V, KVM and VMWare.

2.3.1.5 SUPPORTING SOFTWARE FOR APSOLUTE VISION 4.85.00

The APSolute Vision 4.85.00 physical appliances need some software scripts to allow it to create a bootable USB.

#	File Name	Hardware Platform	SHA-256
1	Vision-4-85-00-usb-boot-ODSVL2-43.tar.gz	APSolute Vision Server ODS-VL2	CC929F1285C967BA9665FE27BF1E009C50DF02E95AF81E80612F47FF7FAF3403

TABLE 6 - APSOLUTE VISION 4.85.00 USB BOOT SOFTWARE

Note: The software provided is applicable to both variants of the physical appliance.

2.3.1.6 TOE GUIDANCE

The main CC documentation that is provided as part of the TOE delivery is:

#	Document Name	Version	SHA-256
1	DefensePro and APSolute Vision Common Criteria Guide	1.8	393cad5378801691a3ec871d880792dc3b601dd960dadebd7041481adb10fdc1

TABLE 7 - CC GUIDANCE DOCUMENTATION

Additionally, the following complementary documentation is also provided as part of the TOE delivery:

#	Document Name	Document ID	SHA-256
1	APSolute Vision Installation and Maintenance Guide	RDWR_APSV_V485_IG2203	FDCC14CEC98F7D073F0B57CF8D88099F4707F0D918FA583D4CC65B073DC0D597
2	APSolute Vision User Guide	RDWR-APSV-V048500_UG2203	C71F598A108EDAE18293288B0267FD39CFB28C38083EB09258E06AC2DCB67DEA
3	DefensePro Installation and Maintenance Guide	RDWR_DP_IG_2309	F3C37B7486942BF93B9BAFB7CB9E9681FC83A1CCF26237F8908B7D3356E17930
4	DefensePro User Guide	RDWR-DP-V082610_UG2112	53B45E7C5444589494CC87F260780276365B932535790169390D3CCE14EF6B1A
5	DefensePro VA Installation and Maintenance Guide	RDWR-DPVA_IG2112	A6EE6AFFD7CF0CCDCA03A7008E32774C8B9E53445A006858F839044272EAC419

TABLE 8 - GENERAL GUIDANCE DOCUMENTATION

The listed documentation, CC-specific and complementary, can be found in PDF format via Radware website. Furthermore, the TOE includes via its Web Management Interface (HTTPS-AP) complementary information describing each parameter. This Online Help is delivered as part of the APSolute Vision 4.85.00 and can be accessed through its Web Management Interface (HTTPS-AP) by clicking on the “?” button.

2.3.1.7 TOE DELIVERY

As described previously, the different TOE component images are used to install the TOE components onto the different supported platforms. As such, the TOE is a pure software solution comprised of a series of component images that are distributed digitally via the developer (Radware) web portal.

The users acquire the TOE from Radware by buying the available hardware or virtual appliances. In either case the user will be provided with access to Radware web portal, from where it can download the TOE component images along with the guidance documentation.

Once downloaded, the user can validate that the images and documentation are the correct ones by calculating the secure hash value (SHA-256) of each element and contrasting it with the ones provided in the previous sections of the Physical Scope.

2.3.1.8 EVALUATED CONFIGURATION

The TOE is composed of two components, APSolute Vision 4.85.00 and DefensePro 8.26.1.0, which work together to provide the security functionality. The DefensePro 8.26.1.0 is the main component which implements the core functionality, while the APSolute Vision 4.85.00 provides the management interfaces (HTTPS-AP) for managing the operational parameters.

Although the DefensePro 8.26.1.0 is capable of running on two deployment scenarios (in-line/transparent and out-of-path), in the evaluated configuration only the in-line mode will be used.

For the evaluated configuration the TOE requires a network segmentation as follows:

- A Management Network for management purpose and internal communication between APSolute Vision 4.85.00 and DefensePro 8.26.1.0.
- An in-bound (ingress) Unprotected Network for all traffic to which protection rules will be applied.
- An out-bound (egress) Protected Network for traffic that has been filtered.
- The in-bound and out-bound networks are disconnected from each other and only bridged via the DefensePro.
- The Management Network is also disconnected from both, the in-bound and out-bound networks.
- The client machines used by the TOE Administrators are connected to the Management Network.

The following diagram illustrate the evaluated configuration deployment:

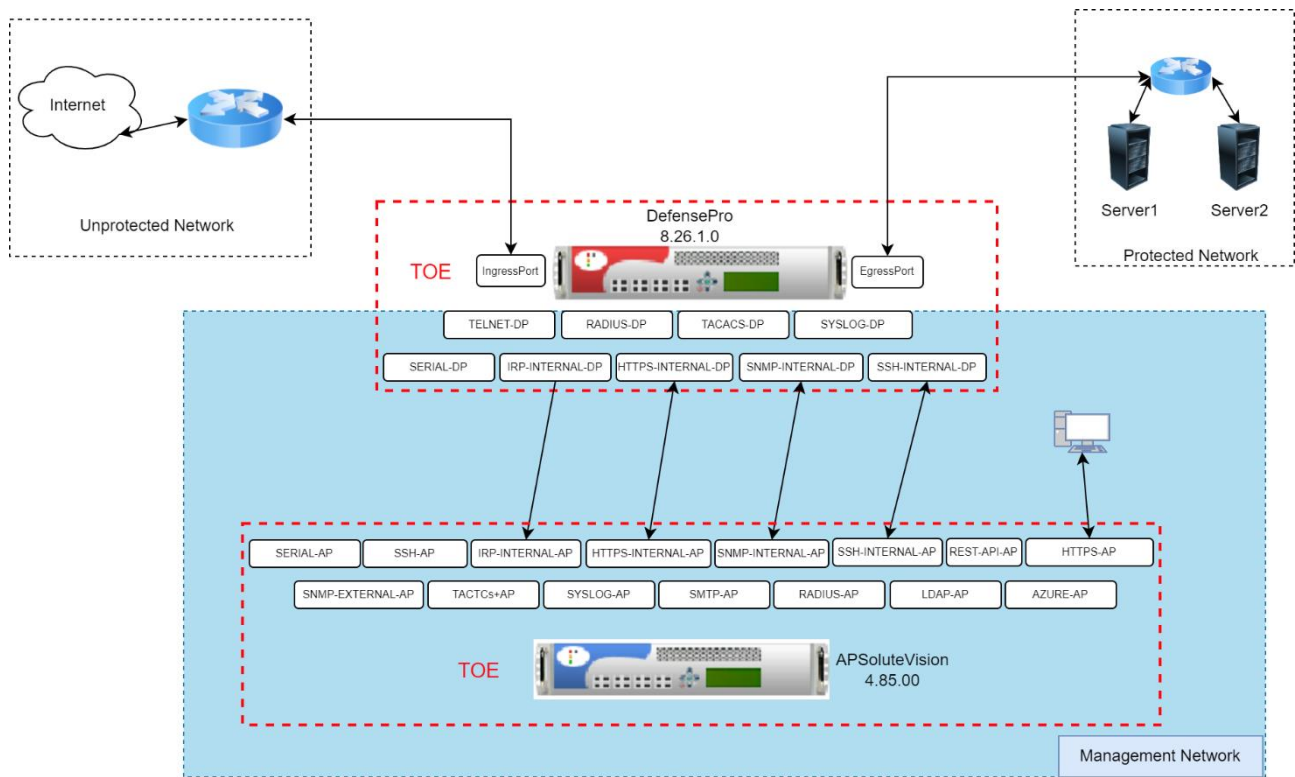


FIGURE 3 - EVALUATED CONFIGURATION

Note that in the evaluated configuration (in-line/transparent mode) the Protected Network and Unprotected Network share the same network segment. That is to say, the TOE is not performing traffic routing.

As illustrated in Figure 3 - EVALUATED CONFIGURATION, there are a series of internal interfaces (IRP-INTERNAL-DP, IRP-INTERNAL-AP, HTTPS-INTERNAL-DP, HTTPS-INTERNAL-AP, SNMP-INTERNAL-DP, SNMP-INTERNAL-AP, SSH-INTERNAL-DP and SSH-INTERNAL-AP) that facilitate the connection between the APSolute Vision 4.85.00 and DefensePro 8.26.1.0. These interfaces are connected through the Management Network. They serve as communication channels between the APSolute Vision 4.85.00 and DefensePro 8.26.1.0, enabling data transfer and interaction.

In contrast to the necessary internal interfaces, some of the TOE interfaces must not be used (be it by not configuring them or by explicitly disabling them) in order to be in the evaluated configuration. The TOE Administrator must not make use of:

- Telnet-DP
- RADIUS-DP
- TACACS+DP
- RADIUS-AP
- TACACS+AP
- LDAP-AP

- AZURE-AP
- SMTP-AP
- SNMP-EXTERNAL-AP
- SYSLOG-DP
- SYSLOG-AP

Finally, the rest of the interfaces SSH-AP, REST-API-AP, HTTPS-AP, SERIAL-AP and SERIAL-DP are enabled by default and their usage is not restricted by configuration. However, these interfaces are not intended to be used, rather the TOE Administrators should only make use of the HTTPS-AP interface to perform all management activities with the TOE.

2.3.2 LOGICAL SCOPE

This section summarizes the logical scope of the TOE.

2.3.2.1 SECURITY AUDIT

The TOE generates audit records for security-related events which are stored in the APSolute Vision 4.85.00 and DefensePro 8.26.1.0. In addition, the security-related logs generated in the DefensePro 8.26.1.0 are sent to the APSolute Vision 4.85.00.

The audit logs are protected from unauthorized modification and deletion.

2.3.2.2 USER DATA PROTECTION

The TOE achieves information flow control applying different policies and rules to the traffic that passes through its interfaces. Information flow control is used by the TOE to mitigate denial of service attacks.

2.3.2.3 IDENTIFICATION AND AUTHENTICATION

The different parts of the TOE present a different set of roles. The TOE requires that the users associated with those roles must be identified and authenticated before granting them access to the TOE and its security functions. Users can authenticate through the different management interfaces using their username and password, but in the evaluated configuration all access and management will be done through the AP.

2.3.2.4 SECURITY MANAGEMENT

The APSolute Vision 4.85.00 provides remote management capabilities of the TOE via the management interfaces (HTTPS-AP). The security management functionality allows to configure users, roles and all of the other configuration objects (policies and profiles) needed to manage the data flow control.

2.3.2.5 TOE ACCESS

The TOE allows user-initiated session termination for its management interfaces (HTTPS-AP).

2.3.2.6 FUNCTIONALITY OUTSIDE OF THE SCOPE

The following TOE functionality falls outside of the scope of the evaluation and will not be evaluated:

- Non-DP protection and analysis features:
 - ADC
 - AVR
 - APM
 - DPM
 - DefenseFlow
 - AppWall

3. Conformance Claims

3.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target is conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

Being:

- CC Part 2 conformant
- CC Part 3 conformant

And claiming conformance with Evaluation Assurance Level 2 (EAL2).

3.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2.

3.4 CONFORMANCE RATIONALE

The TOE for this ST does not claim conformance with any PP, therefore a conformance rationale is not applicable.

4. Security Problem Definition

4.1 TOE ASSETS

The following assets are to be protected by the TOE.

4.1.1 AS.CONFIGURATION

The authenticity and integrity of the TOE configuration.

4.1.2 AS.LEGITIMATE_TRAFFIC

The legitimacy of the filtered traffic outputted by the TOE.

4.1.3 AS.CORE_FUNCTIONALITY

The integrity of the TOE attack mitigation capabilities.

4.2 THREATS

The following threats are addressed by the TOE. Each threat is described in terms of agents and the actions they can use to compromise the assets described in the previous sections.

4.2.1 T.DOS

Attackers may employ different types of Denial of Services (DoS) attacks to prevent legitimate traffic (**AS.LEGITIMATE_TRAFFIC**) from reaching the user's services.

4.2.2 T.ATTACK_MITIGATION_BYPASS

An attacker may take advantage of an error on the TOE implementation to prevent the attack mitigation functionality from being enforced. Bypassing or tampering with the TOE means that an attacker would compromise the TOE security capabilities (**AS.CONFIGURATION**, **AS.CORE_FUNCTIONALITY**).


4.3 ORGANIZATIONAL POLICIES

The Organizational Security Policies (OSPs) are a set of rules, procedures or guidelines imposed by an organization in the operational environment. Alternatively, the OSPs can also be laid down by legislative or regulatory bodies.

4.3.1 OSP.ROLES

The TOE shall support and implement user management based on user roles.

4.3.2 OSP.LOGS



All management actions must be registered in the audit log.

4.3.3 OSP.ACCOUNTABILITY

All users shall be accountable for their actions within the TOE.

4.3.4 OSP.TRUSTED_ADMINISTRATORS

Only approved and capable individuals shall have administrative access to the TOE.

4.4 ASSUMPTIONS

4.4.1 A.PHYSICAL_PROTECTION

The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks nor provide physical access to unauthorized users.

4.4.2 A.MANAGEMENT_SEPARATION

The Management Network, which is used for communication between the parts of the TOE and the TOE administrators, is assumed to be completely separated from the data path network; only accessible to authorized personnel; and can be considered trustworthy.

4.4.3 A.TRUSTED_PLATFORM

The supporting platform of the TOE, be it the hardware appliances or the virtualized platform, are assumed to be secure, trustworthy and capable of providing the necessary functionality according to the needs of the TOE.

4.4.4 A.LIMITED_FUNCTIONALITY

The TOE is assumed to be used to provide only its core functionality as an Attack Mitigation System and not to provide functionality/services that could be deemed as general purpose computing.

4.4.5 A.NO_EVIL

The TOE administrators are assumed to be properly trained, not careless, wilfully negligent, or hostile, and will follow all administrative guidance.

4.4.6 A.SYSTEM_TIME

It is assumed that the Operational Environment will provide reliable time data to the TOE.

5. Security Objectives

5.1 SECURITY OBJECTIVES FOR THE TOE

5.1.1 O.ACCESS

The TOE must only allow authorized users access to the management capabilities of the TOE and provide the security mechanism to protect the credentials used to provide said access.

5.1.2 O.ADMINISTRATION

The TOE must restrict the functionality available to the users based on their associated role and limit the actions available to all users.

5.1.3 O.AUDIT

The TOE must provide auditing functionality in the form of:

1. Generating audit logs.
2. Storing audit logs.

For all actions performed in the TOE related to the TSF, and be capable of storing the necessary information associated with said actions (user, time, results, etc.).

5.1.4 O.ATTACK_MITIGATION

The TOE must ensure that the attack mitigation functionality is being properly applied to the traffic passing through the data paths as per the user configuration and the allowed license throughput. Thus, guaranteeing that only legitimate traffic is egressed from the TOE.

Furthermore, the TOE will ensure that no other functionality is offered through the data paths.


5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

5.2.1 OE.PHYSICAL_PROTECTION

The TOE must be located in a secure physical location which prevent any access from non-authorized users. Meaning that the operational environment will ensure that:

- The underlying platform, hardware appliances or virtualization hardware, is located in a restricted area with access control measures.
- The only personnel allowed to access the restricted area are the TOE Administrators.
- The operational parameters are controlled and properly managed.

5.2.2 OE.MANAGEMENT_SEPARATION



The TOE management interfaces must be connected to a secure Management Network with the appropriate security measure to ensure no access is given to non-authorized users. Meaning that the operational environment will ensure that:

- The management network is physically and logically dedicated to the interconnection of the TOE components and the management client, with no other element connected to it.
- The management network components (cables, switch, etc.) are physically located in the same secure location as the underlying platform in its entirety.

5.2.3 OE.TRUSTED_PLATFORM

The hardware appliances and the virtualization platforms supporting the TOE must be acquired and managed in a secure way, such that it provides a secure and trustworthy operational environment for the TOE.

5.2.4 OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. The TOE is not configured to provide any non-TSF related service or functionality.

5.2.5 OE.TRUSTED_ADMIN

The TOE Administrators must be properly trained and trusted to follow all guidance documentation in a trusted manner. In addition, the TOE Administration will not do anything that may reduce security of the TOE or its operational environment, e.g. granting access of the TOE to unauthorized users.

5.2.6 OE.SYSTEM_TIME

The hardware appliances and the virtualization platforms will provide reliable time data to the TOE.

5.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.DOS	T.ATTACK_MITIGATION_BYPASS	OSP.ROLES	OSP.LOGS	OSP.ACCOUNTABILITY	OSP.TRUSTED_ADMINISTRATOR	A.PHYSICAL_PROTECTION	A.MANAGEMENT_SEPARATION	A.TRUSTED_PLATFORM	A.LIMITED_FUNCTIONALITY	A.NO_EVIL	A.SYSTEM_TIME
O.ACCESS						X						
O.ADMINISTRATION			X			X						
O.AUDIT				X	X							
O.ATTACK_MITIGATION	X	X										
OE.PHYSICAL_PROTECTION							X					
OE.MANAGEMENT_SEPARATION								X				
OE.TRUSTED_PLATFORM									X			
OE.NO_GENERAL_PURPOSE										X		
OE.TRUSTED_ADMIN						X					X	
OE.SYSTEM_TIME												X

TABLE 9 - SECURITY PROBLEM DEFINITION MAPPING


5.3.1 THREATS

T.DOS: Attacks intended to disrupt legitimate traffic by flooding with invalid traffic packets are addressed with the security objective **O.ATTACK_MITIGATION** which enforces the set of protection rules defined by the users.

T.ATTACK_MITIGATION_BYPASS: This threat is addressed by establishing the necessary mechanism to define and manage the data paths such that the TOE is completely transparent to the user's traffic. This is implemented by means of the security objective **O.ATTACK_MITIGATION**.

5.3.2 ORGANIZATIONAL SECURITY POLICIES

OSP.ROLES: This organizational security policy enforces the usage of role-based user management and it is implemented via the security objective **O.ADMINISTRATION**.



OSP.LOGS: This organizational security policy requires the implementation of an audit management system. The TOE is required to generate and store audit logs generated during operation as dictated by the security objective **O.AUDIT**.

OSP.ACCOUNTABILITY: This organizational security policy requires the association between actions performed in the TOE and the users who performed them. The TOE fulfils this policy by means of the security objective **O.AUDIT** which implements an audit management system which stores all relevant information, including user information, for all TSF-relevant events.

OSP.TRUSTED_ADMINISTRATORS: This organizational security policy requires that all administrative actions are performed only by capable and authorized users. The security objectives **O.ACCESS** and **O.ADMINISTRATION** contribute to enforce this policy by implementing the security mechanism necessary to restrict access to the TOE and it's functionality to the appropriate users.

This is further compounded by the security objective for the operational environment **OE.TRUSTED_ADMIN** which ensures that the TOE administrators will be properly trained and be responsible.

5.3.3 ASSUMPTIONS

A.PHYSICAL_PROTECTION: This assumptions is fully covered by the security objective for the operational environment **OE.PHYSICAL_PROTECTION** which ensures that no physical access will be given to unauthorized users.

A.MANAGEMENT_SEPARATION: This assumption is fully covered by the security objective for the operational environment **OE.MANAGEMENT_SEPARATION** which ensures the management network will be secured by the users.

A.TRUSTED_PLATFORM: This assumption is fully covered by the security objective for the operational environment **OE.TRUSTED_PLATFORM**, which ensures that the supporting platform (hardware or virtual) will be trustworthy and be capable of supporting the TOE.

A.LIMITED_FUNCTIONALITY: This assumption is fully covered by the security objective for the operational environment **OE.NO_GENERAL_PURPOSE** which ensures that the TOE will not be used for other functions or services that are not related to its core capabilities.

A.NO_EVIL: This assumption is covered by the security objectives for the operational environment **OE.TRUSTED_ADMIN**, which ensures that the TOE administrators are properly trained and will follow all administrative guidelines.

A.SYSTEM_TIME: This assumption is covered using the system time provided from the hardware appliance or virtualization platform. It is fully covered by the security objective for the operational environment **OE.SYSTEM_TIME** which ensures that the underlying platform must provide with accurate time data.



6. Extended components definition

6.1 SECURITY FUNCTIONAL REQUIREMENTS

This Security Target does not include extended Security Functional Requirements.

6.2 SECURITY ASSURANCE REQUIREMENTS

This Security Target does not include extended Security Assurance Requirements.

7. Security Requirements

7.1 CONVENTIONS

In accordance with Part 1 of the Common Criteria standard, there are four types of operation applicable for SFRs and SARs. For each type of operation, the following typographical distinctions will apply:

1. Iteration: iterations will have a text extension (with format “/” + “label”) added at the end of the component name as well as by modifying the functional component title (adding the same text extension between brackets) to distinguish between iterations. For example, FCS_CKM.1/RSA Cryptographic Key Generation (RSA) and FCS_CKM.1/EC Cryptographic Key Generation (EC).
2. Assignment: assignments are surrounded by brackets and the inner text will be in italics. For example, [*assigned item*].
3. Selection: selections are surrounded by brackets. For example, [selected item].
4. Refinement: refinements are marked depending on their type. For added information the text will be in **bold**; meanwhile, any removed text will be ~~strikeout~~. For example, users will provide ~~original item~~ **new item** when...

7.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, all summarized in the following table.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	Timing of identification
User Data Protection (FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization

Class	Identifier	Name
	FMT_SMF.1	Specification of management functions
	FMT_SMR.2	Restrictions on security roles
TOE Access (FTA)	FTA_SSL.4	User-initiated termination

TABLE 10 - SECURITY FUNCTIONAL REQUIREMENT SUMMARY

7.2.1 SECURITY AUDIT (FAU)

7.2.1.1 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 events:*
 - *User login*
 - *User logout*
 - *Modifications made to the TOE configuration.*
 - *Modifications to users and user roles.*
 - *User account status-related events.*

].

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, [none].

7.2.1.2 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.

7.2.1.3 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 audit records in the audit trail from unauthorised deletion.

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

7.2.1.4 FAU_STG.4: PREVENTION OF AUDIT DATA LOSS

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other action*] if the audit trail is full.

7.2.2 IDENTIFICATION AND AUTHENTICATION (FIA)

7.2.2.1 FIA_AFL.1: AUTHENTICATION FAILURE HANDLING

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [3 and 10]] unsuccessful authentication attempts occur related to [*user login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user account until it is unlocked by a user with an authorized role*].

Application Note: This SFR only applies to the APSolute Vision part of the TOE, whose users will be locked after a configurable number of authentication attempts. The authentication in the DefensePro 8.26.1.0 is only used as an internal interface protection between DefensePro 8.26.1.0 and APSolute Vision 4.85.00.

7.2.2.2 FIA_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION



Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

7.2.2.3 FIA_UID.2: TIMING OF IDENTIFICATION

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.

7.2.3 USER DATA PROTECTION (FDP)

7.2.3.1 FDP_IFC.1: SUBSET INFORMATION FLOW CONTROL

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*unauthenticated information flow control SFP*] on [

- *Subjects: Unauthenticated users and IT entities that sent and receive information through the TOE.*
- *Information: Network traffic sent through the TOE.*
- *Operations: Allow or deny the flow of information passing through the TOE.*

].

7.2.3.2 FDP_IFF.1: SIMPLE SECURITY ATTRIBUTES

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*unauthenticated information flow control SFP*] based on the following types of subject and information security attributes: [

- *Subjects:*
 - *Unauthenticated users and IT entities.*
 - *Network Addresses*

].



- *Traffic Bandwidth and Quota values*
 - *Query Rate*
- *Information:*
 - *Network traffic.*
 - *Source and Destination Ports*
 - *Flood Protection Type*
 - *Protocol (TCP, UDP, ICMP, IGMP)*
 - *Protocol state and packet flags*
 - *Traffic Footprints and Signatures*
 - *Profile Action (Report Only, Block and Report)*

].

- FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *[information can flow through the TOE to another connected network if all the information security attribute values are unambiguously permitted by the configured information flow security policy rules, where such rules may be composed from the combinations of the values of the information flow security attributes]*.
- FDP_IFF.1.3** The TSF shall enforce ~~the~~ *[no additional rules]*.
- FDP_IFF.1.4** The TSF shall explicitly authorize an information flow based on the following rules: *[none]*.
- FDP_IFF.1.5** The TSF shall explicitly deny an information flow based on the following rules: *[none]*.

7.2.4 SECURITY MANAGEMENT (FMT)

7.2.4.1 FMT_MSA.1 MANAGEMENT OF SECURITY ATTRIBUTES

- Hierarchical to: No other components.
- Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1

The TSF shall enforce the [*unauthenticated information flow control SFP*] to restrict the ability to [modify] the security attributes [*of protection policies attributes*]:

- *Network Addresses*
- *Source and Destination Ports*
- *Flood Protection Type*
- *Protocol (TCP, UDP, ICMP, IGMP)*
- *Protocol state and packet flags*
- *Traffic Footprints and Signatures*
- *Profile Action (Report Only, Block and Report)*
- *Traffic Bandwidth and Quota values*
- *Query Rate*

] to [

- *Administrator*
- *Device Administrator*
- *Security Administrator*
- *Vision Administrator*

].

7.2.4.2 FMT_MSA.3: STATIC ATTRIBUTE INITIALISATION

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles.

FMT_MSA.3.1

The TSF shall enforce the [*unauthenticated information flow control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Administrator, Device Administrator, Security Administrator, Vision Administrator*] to specify alternative initial values to override the default values when an object or information is created.

Application note: The permissive values refer to the default parameter values found during the creation of protection profiles, which must be configured to the degree desired by the administrator.

7.2.4.3 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 management functions:
[
• *Management of TOE users*
• *Management of security attributes of protection rules*
].

Application note: Management functionality refers to the ability to create, modify and delete objects related to each particular function (e.g. create users, create rules, etc.).

7.2.4.4 FMT_SMR.2: RESTRICTIONS ON SECURITY ROLES

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [*Administrator, Vision Administrator, Device Administrator, Security Administrator, System User, Security Monitor, Vision Reporter, Device Configurator, Device Viewer*].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [
• *users may only have one role*
] are satisfied.

7.2.5 TOE ACCESS (FTA)

7.2.5.1 FTA_SSL.4: USER-INITIATED TERMINATION

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

7.3 ASSURANCE SECURITY REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3.

The Security Assurance Requirements (SARs) are summarized in the following table:

Assurance Class	SAR ID	SAR Name
Class ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Class AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class 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
Class ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	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
Class ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

TABLE 11 - SECURITY ASSURANCE REQUIREMENT SUMMARY

7.4 SECURITY REQUIREMENTS RATIONALE

7.4.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following table provides a mapping between SFRs and Security Objectives.

	O.ACCESS	O.ADMINISTRATION	O.AUDIT	O.ATTACK_MITIGATION
FAU_GEN.1			X	
FAU_GEN.2			X	

FAU_STG.1			X	
FAU_STG.4			X	
FIA_AFL.1	X			
FIA_UAU.2	X	X		
FIA_UID.2	X	X		
FDP_IFC.1				X
FDP_IFF.1				X
FMT_MSA.1				X
FMT_MSA.3				X
FMT_SMF.1		X		
FMT_SMR.2		X		
FTA_SSL.4	X			

TABLE 12 - SECURITY REQUIREMENT RATIONALE MAPPING

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: O.ACCESS	The TOE must only allow authorized users access to the management capabilities of the TOE and provide the security mechanism to protect the credentials used to provide said access.
Security Functional Requirements	FIA_AFL.1, FIA_UAU.2, FIA_UID.2 and FTA_SSL.4
Rationale	FIA_AFL.1 support the objective by locking a user account after a specified number of unsuccessful authentication attempts, thereby protecting the TOE against a brute force attack. FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated prior to being granted access to the management capabilities of the TOE. FTA_SSL.4 supports the objective by ensuring that open sessions can be closed manually to reduce the risk of an attacker using an open session.

TABLE 13 - RATIONALE FOR O.ACCESS

Objective: O.ADMINISTRATION	The TOE must restrict the functionality available to the users based on their associated role and limit the actions available to all users.
Security Functional Requirements	FIA_UAU.2, FIA_UID.2, FMT_SMF.1, FMT_SMR.2
Rationale	FMT_SMF.1 supports this objective by defining the list of management functions that can be performed in the TOE by the authorized administrators. FMT_SMR.2 cover this objective by defining the roles which are used to



	<p>provide access to the TOE security functionality in the different parts of the TOE.</p> <p>FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated prior to being granted access to the actions available to each user of the TOE.</p>
--	--

TABLE 14 - RATIONALE FOR O.ADMINISTRATION

<p>Objective: O.AUDIT</p>	<p>The TOE must provide auditing functionality in the form of:</p> <ol style="list-style-type: none"> 1. Generating audit logs. 2. Storing audit logs. <p>For all actions performed in the TOE related to the TSF, and be capable of storing the necessary information associated with said actions (user, time, results, etc.).</p>
--------------------------------------	--

<p>Security Functional Requirements</p>	FAU_GEN.1, FAU_GEN.2, FAU_STG.1 and FAU_STG.4
--	---

<p>Rationale</p>	<p>FAU_GEN.1 and FAU_GEN.2 meet this objective by ensuring that the TOE generates audit records for the specified set of auditable events and that the audit records associate a user identity with the auditable event.</p> <p>FAU_STG.1 supports this objective by ensuring that the audit trail is protected against deletion and modification.</p> <p>FAU_STG.4 supports this objective specifying how audit data is treated when the audit trail is full.</p>
-------------------------	--

TABLE 15 - RATIONALE FOR O.AUDIT

<p>Objective: O.ATTACK_MITIGATION</p>	<p>The TOE must ensure that the attack mitigation functionality is being properly applied to the traffic passing through the data paths as per the user configuration and the allowed license throughput. Thus, guaranteeing that only legitimate traffic is egressed from the TOE. Furthermore, the TOE will ensure that no other functionality is offered through the data paths.</p>
--	---

<p>Security Functional Requirements</p>	FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3
--	--

<p>Rationale</p>	<p>FDP_IFC.1 and FDP_IFF.1 cover this objective specifying the subjects, operations and security attributes that can be applied and used by the TOE to perform the flow control functionality used to mitigate attacks.</p> <p>FMT_MSA.1 supports this objective by specifying the user roles and operations that can be performed over the security attributes used to manage the flow control policies.</p> <p>FMT_MSA.3 supports this objective by specifying the characteristics of the</p>
-------------------------	---

security attributes initialization and the user roles that can specify alternative initial values for such attributes.

TABLE 16 - RATIONALE FOR O.ATTACK_MITIGATION

7.4.1.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCY RATIONALE

The following table lists the dependencies for each security functional requirement included in this Security Target, indicating how each dependency has been satisfied.

SFR	Dependency	Fulfilled By	Rationale
FAU_GEN.1	FPT_STM.1	OE.SYSTEM_TIME	Covered by OE.SYSTEM_TIME
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	FAU_GEN.1 has been included in this ST
	FIA_UID.1	FIA_UID.2	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	FAU_GEN.1 has been included in this ST
FAU_STG.4	FAU_STG.1	FAU_STG.1	FAU_STG.1 has been included in this ST
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	Satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UID.2	No dependencies	N/A	N/A
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	FDP_IFF.1 has been included in this ST.
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1	FDP_IFC.1 has been included in this ST.
	FMT_MSA.3	FMT_MSA.3	FMT_MSA.3 has been included in this ST.
FMT_MSA.1	FDP_ACC.1, or FDP_IFC.1	FDP_IFC.1	FDP_IFC.1 has been included in this ST.
	FMT_SMR.1	FMT_SMR.2	Satisfied by FMT_SMR.2, which is hierarchical to FMT_SMR.1.
	FMT_SMF.1	FMT_SMF.1	FMT_SMF.1 has been included in this ST.
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	FMT_MSA.1 has been included in this ST.
	FMT_SMR.1	FMT_SMR.2	Satisfied by FMT_SMR.2, which is hierarchical to FMT_SMR.1.
FMT_SMF.1	No dependencies	N/A	N/A
FMT_SMR.2	FIA_UID.1	FIA_UID.2	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1

SFR	Dependency	Fulfilled By	Rationale
FTA_SSL.4	No dependencies	N/A	N/A

TABLE 17 - SFR DEPENDENCIES

7.4.2 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3. The EAL 2 package was selected to fulfil the required market level for this kind of products.

Since all the SARs included in this Security Target have been taken from a self-sufficient assurance package (EAL 2), there are no dependencies missing for the selected security assurance requirements.

8. TOE Summary Specification

This section provides a high-level description on how the TOE meets each SFR.

8.1 DESCRIPTION ON HOW TOE MEETS EACH SFR

8.1.1 SECURITY AUDIT

The TOE generates audit records for any modification made to the TOE configuration, including user management or any security-related configuration. The TOE associates events resulting from actions of identified users with the identity of the user that caused the event.

The TOE presents only a limited functionality to its users and the audit trail cannot be deleted or modified in any way through its management interfaces (HTTPS-AP). When the storage files are full the TOE replaces the oldest ones with the newer ones, thus overwriting older records.

TOE Security Functional Requirements covered: FAU_GEN.1, FAU_GEN.2, FAU_STG.1, and FAU_STG.4.

8.1.2 IDENTIFICATION AND AUTHENTICATION

The TOE requires identification and authentication of user's prior granting access to any resource or management function.


Both parts of the TOE (APSolute Vision and DefensePro) require user identification and authentication through their interfaces (HTTPS, SNMP, SSH, IRP). However, in the evaluated configuration only the HTTPS-AP interface of the APSolute Vision is used as a management interface for the TOE users.

Thus, the management interface (HTTPS-AP) are found in the APSolute Vision, where users are authenticated and managed. The administrator can set a lockout threshold between 3 and 10 authentication attempts. Once an APSolute Vision user accounts get locked only a user with an authorized role can unlock said account.

TOE Security Functional Requirements covered: FIA_AFL.1, FIA_UAU.2 and FIA_UID.2.

8.1.3 USER DATA PROTECTION

The TOE acts as a transparent proxy between an external network and the network it protects. By default, the TOE allows all the traffic to pass between both networks until an attack is detected. Users with the right role can configure a set of rules and policies that will determine when TOE detects that an attack is taking place.



The TOE allows the configuration of different protection policies, which at the same time are composed of different profiles. The main profiles are BDoS, Connection Limit, DNS Flood Protection, HTTPS Protection, Signature protection and SYN Flood protection.

All those profiles can be configured individually and grouped into a policy that can be activated or deactivated by the authorized users.

The TOE includes a set of pre-configured Signature Protection profiles that can be used as they are or can be modified in order to suit the customer needs. Authorized users can also create custom policies for the other profiles (BDoS, DNS Flood Protection, etc.) based on the following security attributes:

- Network Addresses
- Source and Destination Ports
- Flood Protection Type
- Protocol (TCP, UDP, ICMP, IGMP)
- Protocol state and packet flags.
- Traffic Footprints and Signatures.
- Traffic Bandwidth and Quota values.
- Query Rate.
- Profile Action (Report Only, Block and Report).

Based on the policies and profiles that have been configured by the administrator, the TOE examines the traffic passing from one network to another and determines whether an attack is taking place or not. If an attack is detected, the TOE performs the action selected in the *Profile Action* security attribute, which can consist on denying all the malicious traffic or only reporting the detected attack.

TOE Security Functional Requirements covered: FDP_IFC.1, and FDP_IFF.1.

8.1.4 SECURITY MANAGEMENT

The TOE allows role-based access control to features. These roles are predefined and can be assigned to users by the administrator.

The guidance documentation provides an exhaustive mapping between the existing roles and the software features available. This information can be found under the *Feature-Accessibility per Role* section of the APSolute Vision online help.

Nonetheless, the core security feature, protection policy management, is only available to the Administrator-type roles:

- Administrator
- Device Administrator
- Security Administrator

- Vision Administrator

TOE Security Functional Requirements covered: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.2.

8.1.5 TOE ACCESS

TOE users can perform user-initiated session termination for its management interfaces (HTTPS-AP). The APSolute Vision 4.85.00 management interface (HTTPS-AP) contains a “Logout” button that can be used by authenticated users to close its session.

Once a session is closed the TOE will not allow any user interaction through that session.

TOE Security Functional Requirements covered: FTA_SSL.4.

8.2 FUNCTIONALITY OUTSIDE OF THE SCOPE

The following TOE functionality falls outside of the scope of the evaluation and will not be evaluated:

- Non-DP protection and analysis features:
 - ADC
 - AVR
 - APM
 - DPM
 - DefenseFlow
 - AppWall

9. Acronyms

Acronym	Meaning
CC	Common Criteria
DoS	Denial of Service
DDoS	Distributed DoS
EC	Elliptic Curve
ESXi	Elastic Sky X Integrated
HTTPS	HyperText Transfer Protocol Secure
IPsec	Internet Protocol Security
MAC	Media Access Control
NIC	Network Interface Controller
PP	Protection Profile
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSS	TOE Summary Specification
VA	Virtual Appliance
ADC	Application Delivery Controller
AVR	Application Layer DDoS Verification
APM	Application Performance Monitor
DPM	Distributed Protection Management
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol

10. References

[CEM]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 3.1 Revision 5
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1, 2 and 3 Version 3.1, Revision 5

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666

© 2022 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A.