Radware APSolute OS Version 1.0

Security Target Version 2.3

February 17, 2006

Prepared for:

Radware Ltd.,
22 Raoul Wallenberg ST,
Tel Aviv 69710, Israel
http://www.radware.com/

Prepared by:

An Entrust Company

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
2/09/2006	2.0	Dan DePrez	Final Draft
02/10/2006	2.1	Dan DePrez	Modified per Validator's comments
02/13/2006	2.2	D. DePrez	Editorial corrections
02/17/2006	2.3	D. DePrez	Refined objectives for IT environment

TABLE OF CONTENTS

Table of Tables and Figures

Table **Page**

1 Security Target Introduction

1.1 Security Target Identification

Table 1-1 below provides ST Identification Information

Table 1-1 Security Target Identification

TOE Identification:	Radware APSolute OS Version 1.0 (SynApps version 3.402151),
Installed on Models:	WSD v8.21.04, DP v1.32.11
ST Title:	Radware APSolute OS Version 1.0 Security Target
ST Version:	Version 2.3
ST Authors:	Dan DePrez
ST Date:	February 17, 2006
Assurance Level:	EAL3
Strength of Function:	Not applicable
Registration:	VID10083
Keywords:	Network Management, Intrusion Detection, Denial of Service, Network Switch

1.2 Security Target Overview

Radware provides a variety of Intelligent Application Switching (IAS) products that provide high-speed hardware switching with software security services across the International Standards Organisations Open Systems Interconnection Reference Model (OSIRM) seven layer model layers 3-7. Radware APSolute OS Version 1.0 includes the SynApps software module included in Radware IAS products that provides auditing and network traffic filtering according to a set of administrator-defined policies. SynApps is developed and manufactured by Radware Ltd., 22 Raoul Wallenberg ST, Tel Aviv 69710, Israel.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 3 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

2 TOE Description

2.1 TOE Overview

Radware provides Intelligent Application Switching (IAS) products that provide high-speed hardware switching with software security services across layers 3-7. SynApps is a software module included in Radware IAS appliances that provides the following security functions:

- Auditing of certain network attacks specified by the Administrator through setting of filters, filter groups, and attack definitions
- Enforcement of policies that define specific actions to be taken in the event of a defined network attack

The SynApps software module is identical in all Radware products.

The CLI provides Security Management of security attributes and data. The SynApps software module and the CLI together constitute the TOE. The Policy definition file is the interface of the CLI and the SynApps module, and is also included in the TOE. The Radware appliance and operating system, which is in the IT environment, provides additional functionality that allows administrators to be identified and authenticated, provides tools for configuring the TOE and provides reliable time stamps in support of the TOE. IAS products produced by Radware that were included in the evaluation are as follows:

- DefensePro
- Web Server Director

The TOE is depicted within the Radware appliances in diagram in Figure 2-1.

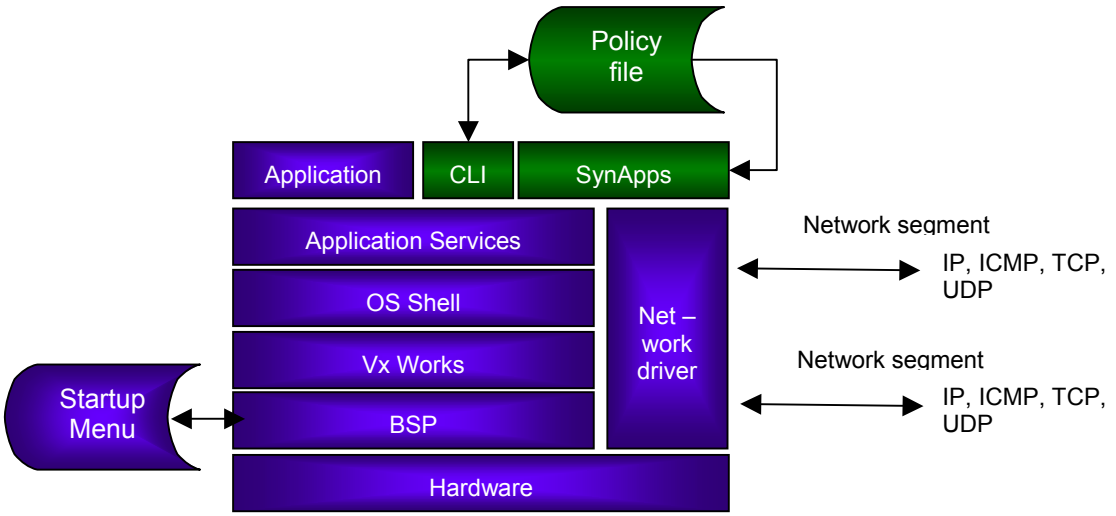


Figure 2-1 – SynApps Module and CLI (the TOE in *green*) within the Radware appliance (IT Environment in *purple*)

Each Radware appliance consists of physical interfaces that are network connections over specific physical ports, and custom hardware to facilitate communications information flow through the appliance. Radware appliances perform the same security functions, however, different appliance models provide for additional throughput, capacity, and redundancy. Although the hardware architecture is similar across

platforms, each platform has a unique combination of hardware components that support the specific performance and feature requirements for that platform. These customized hardware components include items such as memory size, CPU, and network connectivity.

The source code base for all platforms is identical. However, the CLI must be tailored and the application code must be compiled and built into different object code for each platform because of application specific and hardware differences. Although larger appliances support a greater number of security policies, every device can establish the same security policy.

The hardware, which is not part of the TOE, is manufactured according to Radware's specifications by sub-contracted manufacturing facilities.

A very brief description of product components that are not included in the TOE is provided below in order to provide context for the TOE:

- **Hardware** – Custom hardware, which varies for each appliance.
- **BSP layer** - Board Support Package, which is the layer of low levels drivers. This layer connects the operating system to the hardware.
- **VxWorks** – The operating system on the appliances.
- **OS Shell** – The layer between the operating system and the application. The OS shell provides portability for the different appliance applications so that the OS can be changed without having an effect on the application code.
- **Application** – The Radware appliance software, which varies by Radware IAS product, e.g., WSD, CSD, LP, FP, etc.
- **Network driver** - the separate driver that receives and transmits Ethernet frames. Each packet arriving through one of the external Ethernet ports is received by the network driver and is forwarded to the SynApps module for processing.

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

2.2 TOE Physical and Logical Boundary

The TOE physical boundary is the SynApps software running in the Radware IAS appliance and the CLI through which the Administrator sets filters, filter groups, and policies. The Policy Definition file is also included in the TOE. The SynApps software runs as an application on the OS.

The TOE logical boundary consists of the SynApps module performing audit functionality and information flow control and the CLI supporting security management functionality running as part of the Radware IAS Appliance. The default information flow policy is permissive.

Although the TOE does not include administrator authentication, the evaluated configuration excludes remote administrator authentication.

2.3 TSF Data and User Data

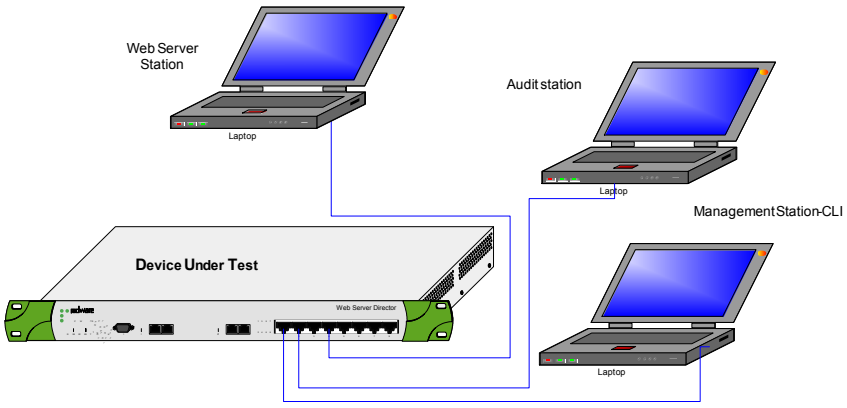
Within the TOE, TSF data is considered to be the security attributes, including filters, filter groups, and policies defined by the Administrator, that control the flow of data and generation of audit records and alerts by the TOE. No user data exists on the TOE.

2.4 IT Security Environment and Evaluated Configuration

SynApps is a software security module included in Radware IAS products. The target of evaluation (TOE) includes the SynApps software module, and the included products' CLI modules. The Policy Definition file is also included in the TOE. For the purposes of this ST and Common Criteria evaluation, Web Server Director Application Switch II (version WSD v8.21.04) and DefensePro Application Switch III (version DP v1.32.11) were tested.

The test configuration as shown in the figure below includes a management station where the TOE's administrative interface (CLI) is installed. Although Administrator authentication is not included in the claimed TOE functionality, the TOE configuration excludes remote administrator authentication. The only means of Administrator authentication that is compatible with the TOE is through the connected console port. Hence, to authenticate as an administrator, a user must have physical access to the TOE and posses a valid user identifier and authenticator.

The test configuration also includes a web server station and an audit station. A set up identical to the figure below has been used to test both the Web Server Director Application Switch II (version WSD v8.21.04) and DefensePro Application Switch III (version DP v1.32.11)



The tested configuration did not include any enabled hardware accelerators or high bandwidth fiber connections.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

Item	Assumption	Description
A1	A.Admin	It is assumed that the TOE Administrator will install, configure, and operate the TOE according to the instructions provided by the TOE documentation and that administrators are not malicious.
A2	A.Physical	It is assumed that the Radware appliance, the Management Station, and the connection between the Radware appliance and the Management Station will be located in a controlled access facility that prevents unauthorized physical access.

3.2 Threats to the TOE

The threats included in the table below are defined for the TOE. The TOE is a software module running on an appliance designed to monitor network traffic and protect against network attacks. For all threats to the TOE:

- The assets under attack are the network traffic and devices, which may be compromised or put out of service by an attack. Examples include: a network device could be flooded with spam email, causing a denial of service for receipt of legitimate email; network traffic may be captured and modified causing the data to be erroneous, thereby stopping legitimate data from being delivered to the intended recipient.
- Expertise, resources, and opportunity are unknown for unknown attackers and unauthorized users. Since the asset under attack is data on an unknown network or unknown network resources and since the value of those assets is unknown, it is not possible to predict the level of expertise, resources, or opportunity that might be applied in an attack. The worst-case scenario is an expert attacker or unauthorized user, i.e., someone knowledgeable about the network traffic, with unlimited resources and opportunity that can compromise network data or cause denial of service.
- The motivation for an unknown attacker or unauthorized user is to compromise network data or resources and/or cause denial of service.

Threat agent and attack are included in the definition of the threat, as shown in Table 3-2.

Table 3-2 Threats

Item	Threat	Description
1	T.No_Alarm	A network administrator may not detect an attack or may detect it only after significant damage has been done if immediate notification of an attack is not provided.
2	T.Attack	An unknown attacker may intercept network data and insert malicious code, causing a denial of service and/or compromise of network data.
3	T.No_Policy	An unknown attacker may intercept network data and insert malicious code in order to compromise network data or resources or cause a denial of service if an adequate policy is not implemented to monitor network operation and detect attacks.
4	T.Mismanage	An unauthorized user may modify security attributes and cause the TOE to malfunction or to allow network attacks to go undetected.
5	T.Mismanage_Ops	An unauthorized user may shutdown the TOE, modify security function policies, or modify the definition of audited events, thereby causing the TOE to malfunction or to allow network attacks to go undetected.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 Security Objectives for TOE

Item	Objective for TOE	Description
1	O.Alarms	The TOE shall send notification when an attack is detected.
2	O.Audit_Analysis	The TOE shall provide the capability to monitor network operations and indicate when an attack is identified.
3	O.Flow	The TOE shall enforce a Security Function Policy, as defined by the Administrator, on data flowing through the TOE.
4	O.Flow_Attributes	The TOE shall enforce a Security Function Policy using defined security attributes for network operations.
5	O.Manage_Attributes	The TOE shall allow only the Administrator to modify security attributes defined within the Security Function Policy.
6	O.Manage_Ops	The TOE shall allow only the Administrator to perform startup and shutdown, modification of the Security Function Policy, and modification of the definition of audited events.

4.2 Security Objectives for the Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for IT Environment

Item	Objective for IT Environment	Description
1E	OE.Install	The IT environment and TOE shall be properly installed. Specifically the Network driver must pass network traffic only to and from the TOE.
2E	OE.I&A	The IT Environment shall require user identification and authentication prior to any action.
3E	OE.Time	The IT Environment shall provide reliable time stamps.
4E	OE.NonBypass	The IT environment must ensure the network driver passes every well formed packet to the TOE.
5E	OE.Protect	The IT environment shall include physical protection for the Radware appliance, the Management Station, and the connection between the Radware appliance and the Management Station such that unauthorized personnel cannot tamper with the TOE or the Administrative connection to the TOE.
6E	OE.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
7E	OE.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations, and explicit functional components derived from the CC components.

The notation, formatting, and conventions used in this security target (ST) are consistent with the Common Criteria. The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner: assignments, refinements, and selections specified by the ST author are in ***italicized bold text***. There are no iterations.

Explicitly Stated Requirements, i.e., requirements that are not included in the CC, are noted with a "_EXP" added to the component name. Application notes are included with some requirements and provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.1 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicitly stated, summarized in the Table 5-1 below.

Table 5-1 Functional Components for TOE

Item	Component	Component Name	Part 2 or Explicitly Stated
1	FAU_ARP.1	Security alarms	Part 2
2	FAU_SAA.4	Complex attack heuristics	Part 2
3	FDP_IFC.1	Subset information flow control	Part 2
4	FDP_IFF.1	Simple security attributes	Part 2
5	FMT_MOF.1	Management of security functions behaviour	Part 2
6	FMT_MSA.1	Management of security attributes	Part 2
7	FMT_MSA.3	Static attribute initialisation	Part 2
8	FMT_SMF.1	Specification of management functions	Part 2

FAU_ARP.1 Security alarms

Hierarchical to: No other components

FAU_ARP.1.1 The TSF shall take the action specified in the condition that matches the system activity, where the possible actions are:

1. ***display console message, and***
2. ***record event in alert table***

upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_SAA.4 Complex attack heuristics

Hierarchical to: FAU_SAA.1

FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios

1. ***Receipt of sequence of network datagrams where:***
    a. ***Each datagram in the sequence matches the same condition specified by an administrator,***
    b. ***Number of datagrams in the sequence exceeds a threshold set by an administrator, and***
    c. ***Sequence of datagrams is received within a time interval set by an administrator.***

and the following signature events

1. ***Receipt of a network datagram matching an atomic condition specified by an administrator;***
2. ***Receipt of a network datagram matching a conjoined condition specified by an administrator, and***
3. ***Receipt of a network datagram matching any atomic or conjoined condition in a named group of conditions specified by an administrator.***

that may indicate a potential violation of the TSP.

FAU_SAA.4.2 The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of

1. ***For all network datagrams:***
    a. ***Source IP address of network datagram, which matches event when the address is in a range specified by an administrator***
    b. ***Destination IP address of network datagram, which matches an event when the address is in a range specified by an administrator***
    c. ***Direction of network pattern (i.e. one-way or two-way)***
    d. ***IP Packets encapsulating a fragmented URL request must contain a minimum URL size of at least 50 bytes long..***
    e. ***IP Packets encapsulating a URL request must contains URI size of no more than 500 bytes long..***
    f. ***Fragmented packets must be at lease 512 bytes long***
2. ***For all atomic conditions:***
    a. ***Optionally, Protocol of network datagram, which matches event protocol specified by an administrator (one of IP, ICMP, TCP, or UDP),***

b. ***Optionally, a Bit pattern contained within network datagram, which matches an event when***
    i. ***The bit pattern appears within the datagram at a location specified by an administrator (location is specified by base, offset, and pattern length)***
    ii. ***After applying an administrator-specified mask, the bit pattern meets a condition specified by an administrator (one of equal, notEqual, greaterThan, or lessThan)***
c. ***Optionally, but exclusive of "b" above, Text pattern contained within network datagram, which matches an event when***
    i. ***The text pattern appears within the datagram within locations specified by an administrator (locations are specified by starting offset within network packet and maximum length of content)***
    ii. ***The text pattern matches the type specified by an administrator (type is one of Text, Regular Expression, HTTP types, or SMTP types)***
        1. ***HTTP types are: URL, Host name, HTTP header field, Header Type, File Type, and Cookie Data***
            a. ***Header type equals a field value***
            b. ***HTTP cookie equals a cookie value***
            c. ***Or not applicable***
        2. ***SMTP types are: Mail Domain, Mail To, Mail From, and Mail Subject***
    iii. ***The text pattern matches a pattern specified by an administrator including***
        1. ***Encoding of text pattern (one of none, case sensitive, case insensitive, HEX, or international),***
        2. ***Character set of specified pattern***

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

FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when system activity is found to match a signature event or event sequence that indicates a potential violation of the TSP.

Dependencies: No Dependencies

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the ***SynApps Application Security SFP*** on

- ***Subjects – interface table for each physical port from which network traffic is passed through the TOE;***
- ***Information – network traffic sent through the TOE from one subject to another;***
- ***Operations – block or pass network traffic.***

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the ***SynApps Application Security SFP*** based on the following types of subject and information security attributes:

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

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:

- ***A policy rule has not been established to deny the information flow, and all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from combinations of the values of the information flow security attributes, created by the Administrator;***

FDP_IFF.1.3 The TSF shall enforce the ***following rules***

1. ***Receipt of a network datagram matching an atomic condition specified by an administrator.***
2. ***Receipt of a network datagram matching a conjoined condition specified by an administrator, and***

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

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

1. *For all network datagrams:*
    a. *Source IP address of network datagram, which matches event when the address is in a range specified by an administrator*
    b. *Destination IP address of network datagram, which matches an event when the address is in a range specified by an administrator*
    c. *Direction of network pattern (i.e. one-way or two-way)*
2. *For all atomic conditions:*
    a. *Optionally, Protocol of network datagram, which matches event protocol specified by an administrator (one of IP, ICMP, TCP, or UDP),*
    b. *Optionally, a Bit pattern contained within network datagram, which matches an event when*
        i. *The bit pattern appears within the datagram at a location specified by an administrator (location is specified by base, offset, and pattern length)*
        ii. *After applying an administrator-specified mask, the bit pattern meets a condition specified by an administrator (one of equal, notEqual, greaterThan, or lessThan)*
    c. *Optionally, but exclusive of "b" above, Text pattern contained within network datagram, which matches an event when*
        i. *The text pattern appears within the datagram within locations specified by an administrator (locations are specified by starting offset within network packet and maximum length of content)*
        ii. *The text pattern matches the type specified by an administrator (type is one of Text, Regular Expression, HTTP types, or SMTP types)*
            1. *HTTP types are: URL, Host name, HTTP header field, Header Type, File Type, and Cookie Data*
                a. *Header type equals a field value*

b. HTTP cookie equals a cookie value

c. Or not applicable

2. SMTP types are: Mail Domain, Mail To, Mail From, and Mail Subject

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

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

2. Character set of specified pattern

3. For atomic conditions on TCP streams and UDP datagrams:

a. Source port of network datagram, which matches an event when the port is in a range specified by an administrator,

b. Destination port of network datagram, which matches an event when the port is in a range specified by an administrator,

4. For conjoined conditions:

a. Network datagram, which matches when it matches all of the atomic conditions that comprise the conjoined condition.

FDP_IFF.1.4 The TSF shall provide the following ***no other capabilities***.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: ***no other rules.***

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

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

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialization

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behaviour of*** the functions

- ***SynApps Information Flow Control SFP;***
- ***Auditing of attacks.***

to ***the Administrator***.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the ***SynApps Application Security SFP*** to restrict the ability to ***modify*** the security attributes:

- ***information flow rules as described in FDP_IFF.1***
- ***Filter Name***
- ***Description***

to ***the Administrator***.

Dependencies: FMT_SMR.1 Security roles, FDP_IFC.1 Subset information flow control; FMT_SMF.1 Specification of management functions

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

FMT_MSA.3.1 The TSF shall enforce the ***SynApps Application Security 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*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_SMR.1 Security roles, FMT_MSA.1 Management of security attributes

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***Restrict the ability to determine TSF security policy and management behaviour; restrict the ability to modify security attributes; provide default values for security attributes***.

Dependencies: No Dependencies

5.2 Security Requirements for the IT Environment

The security functional requirements for the IT Environment are summarized in Table 5-2.

Table 5-2 Security Functional Requirements for the IT Environment

Item	Component	Component Name	Part 2 or Explicitly Stated
1E	FIA_UAU.2	User authentication before any action	Part 2
2E	FIA_UID.2	User identification before any action	Part 2
3E	FPT_STM.1	Reliable time stamps	Part 2

Item	Component	Component Name	Part 2 or Explicitly Stated
4E	FPT_RVM_EXP.1	Non-bypassability of the TSP: IT	Explicitly Stated
5E	FPT_SEP_EXP.1	TSF domain separation: IT	Explicitly Stated

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The ***IT Environment*** shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for ***the TOE's*** use.

Dependencies: No dependencies

FPT_RVM_EXP.1 Non-bypassability of the TSP: IT

Hierarchical to: No other components.

FPT_RVM_EXP.1.1 The security functions of the IT environment shall ensure that the network drive passes every well formed packet it receives to the TOE.

Dependencies: No dependencies.

FPT_SEP_EXP.1 TSF domain separation: IT

Hierarchical to: No other components.

FPT_SEP_EXP.1.1 The security functions of the IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope and control of the IT environment.

FPT_SEP_EXP.1.2 The security functions of the IT environment shall enforce separation between the security domains of subjects in the scope of control of the IT environment.

Dependencies: No dependencies.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in the following table.

Table 5-3 Assurance Requirements: EAL3

Assurance Class	Assurance Components		
Configuration management	1	ACM_CAP.3	Authorisation controls
	2	ACM_SCP.1	TOE CM coverage
Delivery and operation	3	ADO_DEL.1	Delivery procedures
	4	ADO_IGS.1	Installation, generation, and start-up procedures
Development	5	ADV_FSP.1	Informal functional specification
	6	ADV_HLD.2	Security enforcing high-level design
	7	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	8	AGD_ADM.1	Administrator guidance
	9	AGD_USR.1	User guidance
Life cycle support	10	ALC_DVS.1	Identification of security measures
Tests	11	ATE_COV.2	Analysis of coverage
	12	ATE_DPT.1	Testing: high-level design
	13	ATE_FUN.1	Functional testing
	14	ATE_IND.2	Independent testing - sample
Vulnerability assessment	15	AVA_MSU.1	Examination of guidance
	16	AVA_SOF.1	Strength of TOE security function evaluation (Not Applicable)
	17	AVA_VLA.1	Developer vulnerability analysis

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

6 TOE Summary Specification

6.1 IT Security Functions

The TOE performs the following security functions:

- Audit
- Information Flow Control
- Security Management

These three IT security functions and their mapping to security functional requirements from Section 5 of this ST are described below and are summarized in Table 6-1.

Table 6-1 Mapping of IT Security Functions to SFRs

IT Security Function	Security Functional Requirement
Audit	FAU_ARP.1 FAU_SAA.4
Information Flow Control	FDP_IFC.1 FDP_IFF.1
Security Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1

6.1.1 Audit

SynApps creates Alerts and stores them in the Alerts Table within flash memory when certain events are detected. By default no events create alerts, the administrator must define the events that create alerts. An alert contains:

- Attack Index: the sequence number of the audit event
- Attack name: the name of the Administrator defined policy and filter
- Attack source address: the IP source address
- Attack destination address: the IP destination address
- Attack status: always “blocked” in the TOE
- Attack time: the timestamp of the event

Since a timestamp is included in the Alert, there is a dependency on the IT environment to provide reliable timestamps to the TOE.

This functionality meets the requirement FAU_ARP.1.

Although this is a layer 2 device that does not perform stateful network processing, SynApps maintains an internal representation of administrator defined event sequences of known intrusion scenarios and signature events. A detailed discussion of the method by which the administrator may define event sequences is contained in Section 6.1.2 and Table 6-2, which relies on the same method of defining event sequences to determine which network packets are dropped. In summary, to support the Auditing functions the SynApps module examines the Layer 2 network traffic and compares the

record of the system activity against the signature events and event sequences and indicates a violation of the policy if the system activity matches any of the signature events and event sequences. This functionality meets the requirement FAU_SAA.4.

6.1.2 Information Flow Control

SynApps passes all network traffic unless the traffic is blocked by a filter configured by an administrator. SynApps controls the network traffic (packets) flowing through the SynApps module by the definition of filters, filter groups, and policies, explained in the following:

There are three filter types:

1. Regular filter – basic filter and the smallest building block. It contains information about protocol, ports, OMPC attributes and content attributes. This supports the functionality described as an atomic condition.
2. Advanced Filter – contains number of basic filters. There is a logical “AND“ between the basic filters. This supports the functionality described as a co-joined condition.
3. Group Filter – contains number of basic filters. There is a logical “OR“ between the basic filters. This supports the functionality described as a named group.

The administrator defines Profiles which are a link between a profile name and a filter. The administrator can define Networks to manage as an IP address or range of IP address.

Profiles and Networks are combined into a Policy to define the device's security management policies including source networks, the desired action (filtering to be performed) and the destination network. A policy provides a means to define:

- the Policy Name,
- the Policy Service (the name of the filter group bound to the policy),
- the Source Address network from which incoming traffic will be inspected,
- the Destination Address network to which outgoing traffic will be inspected,
- the Direction of the traffic (one-way, or two-way),
- the Policy State of active or inactive, and
- the Inbound Physical Port group from which traffic will be inspected. Basic filters can be combined with logical conditions to implement more sophisticated filters

for the groups of filters that are associated with it. The SynApps Application Security SFP, which is defined by the Administrator at system installation, can be updated by the Administrator at any time. Each Basic Filter is built from the following fields by the Administrator. The following are included in all basic filters, either explicitly or as a default value:

- Filter Name: The Administrator-defined name of the filter.
- Description: The Administrator-defined description of the filter.
- Protocol: The protocol used, which is IP, UDP, TCP, or ICMP.

- Destination Port Range From: The first port in the range of destination ports for UDP and TCP traffic only.
- Destination Port Range To: The last port in the range of destination ports for UDP and TCP traffic only.
- Source Port Range From: The first port in the range of source ports for UDP and TCP traffic only.
- Source Port Range To: The last port in the range of source ports for UDP and TCP traffic only. This allows the administrator to configure filters for various bit patterns in packets.
- Filter Type: Can be “Regular”, “Static” or “Application Security”. “Application Security” filters are the only filters enforced by the SynApps module. The filter type must to be set "Application Security" for administrator defined filters.

There are two incompatible methods by which binary or text data may be tested in the packets. The first method based on binary data relies on the following parameters:

- OMPC Length: The length of the OMPC data can be N/A, one Byte, two Bytes, three Bytes, or four Bytes.
- OMPC Offset: The offset in the packet where the OMPC is checked.
- OMPC Pattern: The OMPC pattern searched for in the packet in hexadecimal.
- OMPC Mask: Mask for the OMPC data in hexadecimal.
- OMPC Condition: Can be either N/A, equal, not Equal, greater Than or less Than.
- OMPC Offset Relative To: Can be either None, IP Header, IP Data, or TCP Data.

The second method based on text data provides an alternative means of specifying application layer network processing:

- Content Offset: The offset in the packet where the content is checked.
- Content: Refers to the search for the content in the packet. It can be N/A, URL, or text.
- Content Type: Enable the user to search for the specific content type, for HTTP, URL, hostname, text or HTTP header field; for SMTP, Mail Domain, Mail to, Mail form, Mail Subject, or a Regular Expression.
- Content Max. Length: the maximum length to be searched within the selected Content Type.
- Content Data: The actual value of the content search.
- Content Encoding: Can be either None, Case Insensitive, Case Sensitive, HEX, or International.
- Content Data Encoding: Can be either None, Case Insensitive, Case Sensitive, HEX, or International.

The CLI processes both the binary and text data methods into an identical internal format so that all filters are in the same format insofar as the SynApps module is concerned.

In addition to the Basic Filter parameters, the following advanced parameters may be configured for a filter:

- Tracking Time: Time during which a given Threshold must be exceeded
- Threshold: The number of packets that match the attack signature, within the Tracking Time period, that are recognized as legitimate traffic.
- Tracking Type: Defines how traffic is to be treated when under an attack of this type, Drop All, Target Count, or Source and Target Count.

The interdependencies of these fields are shown in the following table:

Table 6-2 Filter Parameter Relationships

Context	Interfaces to test	Interdependency
Method 1 of defining a basic filter. Cannot be used with Method 2 fields.	**Group A** • Offset Mask Pattern Condition (OMPC) Length • OMPC Pattern • OMPC Mask • OMPC Condition • OMPC Offset • OMPC Offset Relative To	These fields are always used together, except *OMPC Offset* and *OMPC Offset Relative To*, which are alternative methods of specifying an offset.
Method 2 of defining a basic filter. This included Groups **B**, **C**, and **D**. This method is intended as an easy method to define basic filters. Cannot be used with Group A fields.	**Group B** • Content	This field is required for all basic filters specified by this method.
	Group C (optional) • Content Data • Content Type	*Content Type* has a pre-defined set of values given in the User Guidance. *Content Data* depends on *Content Type* and is a subset of *Content*.
	Group D (depends on Group C) • Content Offset (from-to) • Content Encoding • Content Data Encoding • Content Max Length	*Content Offset* depends on *Content Type*. *Content Max Length* depends on *Content Offset*. *Content Encoding* depends on *Content*, while *Content Data Encoding* depends on for *Content Data.*
These fields may be used with Basic Filters specified either by Method 1 or 2.	**Group E** • Destination Port (Range: From, To) • Source Port (Range: From, To) • Direction	*Destination* and *Source Port* may only be used when filtering Transport Layer protocols. *Direction* can be applied to any Network Protocol.

Advanced filter. These are built from Basic filters.	**Group F** • Tracking Time • Threshold • Tracking Type	These fields may all be used independently, but only with one or more basic filters defined by either Method 1 or Method 2.

By using policies the SynApps module prevents or allows traffic from flowing between unauthenticated external IT entities to one another. The policies also determine whether alerts or audit records are written and any other action that may be required to thwart or respond to an attack.

SynApps operates at layer 2 of the OSIRM seven layer models. As such, it operates upon packets. Although packets are normally thought of as corresponding to an IP datagram, when an IP datagram is too large for the maximum transmission unit (MTU) of the underlying data link layer technology used for the next leg of its journey, it must be fragmented before it can be sent across the network. The higher-layer message to be transmitted is not sent in a single IP datagram but rather broken down into pieces called fragments that are sent separately. In some cases, the fragments themselves may need to be fragmented further. In this circumstance, SynApps applies the specified filtering for OSI layers 4-7 to the fragment in the IP datagram which includes the layer 4-7 protocol header (e.g.: nominally the first fragment), while filtering rules for layer 3 may be applied to every fragment (frame).

By default, the Radware product filters fragmented packets based on packet size. The default filtering parameters are:

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

In the evaluated configuration the above defined packet lengths may not be modified. The filtering of fragmented packets with respect to size is based on the actual packet size, not the Total length field in the packet header.

This functionality meets the requirements FDP_IFC.1 and FDP_IFF.1.

6.1.3 Security Management

SynApps performs the following security management functions:

- Management of security functions behaviour,
- Management of security attributes,
- Definition of defaults for security attributes.

The only access to set filters, filter groups, and policies is through a Command Line Interface (CLI) that is only accessible to an Administrator. The CLI accesses policy definition file that stores the policy and filter settings. SynApps accesses the policy definition files and implements the settings in those files. Please note that identification and authentication is not part of the TOE.

SynApps performs Management of security functions behavior by restricting definition of information flow and audit policies that to the Administrator. This functionality meets FMT_MOF.1

Management of security attributes, i.e., defining global parameters and policies which are the security attributes within the TOE, is restricted to the Administrator, who sets the policies though the CLI, which are then accessed and implemented by SynApps. The Administrator is sets all global parameters, filters, filter groups, and policies. This functionality meets FMT_MSA.1.

SynApps passes all network traffic that is not blocked by a filter specified by the Administrator. FMT_MSA.3 concerns itself with managing the permissive or restrictive setting of default values for a given access control SFP. Therefore, the default property of the access control attribute is permissive.
The Radware product has only one security role: the administrator. There is no untrusted user role or user data. In the evaluated configuration remote administration is disabled. Therefore, any user who can physically access the Radware product and possess a valid user account name and password may authenticate as an administrator.

SynApps provides security management functionality to enforce security policies, to modify security attributes, and provide default values for security attributes, which meets the requirement FMT_SMF.1.

6.2 SOF Claims

There are no permutational or probabilistic mechanisms included in the TOE, therefore strength of function is not applicable.

6.3 Assurance Measures

The TOE satisfies the assurance requirements for Evaluation Assurance Level EAL3.

Refer to Table 8-9 in Section 8.3.2 for the evaluation evidence provided to satisfy the EAL3 assurance requirements.

7 PP Claims

This Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Mapping Threats to Objectives for the TOE

Table 8-1 shows that all the identified threats to security are countered by at least one security objective for the TOE.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Threat Description	Objective
1	T.No_Alarm	A network administrator may not detect an attack or may detect it only after significant damage has been done if immediate notification of an attack is not provided.	O.Alarms, OE.Person, OE.Time
2	T.Attack	An unknown attacker may intercept network data and insert malicious code, causing a denial of service and/or compromise of network data.	O.Audit_Analysis
3	T.No_Policy	An unknown attacker may intercept network data and insert malicious code in order to compromise network data or resources or cause a denial of service if an adequate policy is not implemented to monitor network operation and detect attacks.	O.Flow O.Flow_Attributes
4	T.Mismanage	An unauthorized user may modify security attributes and cause the TOE to malfunction or to allow network attacks to go undetected.	O.Manage_Attributes, OE.Install, OE.Operations, OE.Protect, OE.NonBypass
5	T.Mismanage_Ops	An unauthorized user may shutdown the TOE, modify security function policies, or modify the definition of audited events, thereby causing the TOE to malfunction or to allow network attacks to go undetected.	O.Manage_Ops, OE.Install, OE.Operations, OE.Protect, OE.NonBypass OE.I&A

Table 8-2 shows that all Security Objectives for the TOE are mapped to at least one threat. Rationale for the mappings in Tables 8-1 and 8-2 are provided in the text below.

Table 8-2 All Objectives Mapped to at Least One Threat

Item	Objective Name	Objective Description	Threat
1	O.Alarms	The TOE shall send notification when an attack is detected.	T.No_Alarm

Item	Objective Name	Objective Description	Threat
2	O.Audit_Analysis	The TOE shall provide the capability to monitor network operations and indicate when an attack is identified.	T.Attack
3	O.Flow	The TOE shall enforce a Security Function Policy, as defined by the Administrator, on data flowing through the TOE.	T.No_Policy
4	O.Flow_Attributes	The TOE shall enforce a Security Function Policy using defined security attributes for network operations.	T.No_Policy
5	O.Manage_Attributes	The TOE shall allow only the Administrator to modify security attributes defined within the Security Function Policy.	T.Mismanage
6	O.Manage_Ops	The TOE shall allow only the Administrator to perform startup and shutdown, modification of the Security Function Policy, and modification of the definition of audited events.	T.Mismanage_Ops

T.No_Alarm - A network administrator may not detect an attack or may detect it only after significant damage has been done if immediate notification of an attack is not provided. This threat is countered by O.Alarms, which states that the TOE shall send notification when an attack is detected. The need of a timestamp for the alarms is supported by OE.Time. OE.Person states that personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system and hence will configure the TOE to provide timely notification of attacks.

T.Attack - An unknown attacker may intercept network data and insert malicious code, causing a denial of service and/or compromise of network data. This threat is countered by O.Audit_Analysis, which states that the TOE shall provide the capability to monitor network operations and indicate when an attack is identified.

T.No_Policy - An unknown attacker may intercept network data and insert malicious code in order to compromise network data or resources or cause a denial of service if an adequate policy is not implemented to monitor network operation and detect attacks. This threat is countered by O.Flow, which states that the TOE shall enforce a Security Function Policy, as defined by the Administrator, on data flowing through the TOE.

T.Mismanage - An unauthorized user may modify security attributes and cause the TOE to malfunction or to allow network attacks to go undetected. This threat is countered by O.Manage_Attributes, which states that the TOE shall allow only the Administrator to modify security attributes defined within the Security Function Policy. OE.Install and OE.Protect insure that the product is properly installed so the TOE SynApps module is invoked by the IT environment and the IT Environment shall include physical protection for the TOE such that unauthorized personnel cannot tamper with the TOE. OE.Operations insures that the TOE is operated in a secure manner consistent with administrative guidance. OE.NonBypass insures that the network driver passes every well formed packet it receives to the TOE.

T.Mismanage_Ops - An unauthorized user may shutdown the TOE, modify security function policies, or modify the definition of audited events, thereby causing the TOE to

malfunction or to allow network attacks to go undetected. This threat is countered by O.Manage_Ops, which states that the TOE shall allow only the Administrator to perform startup and shutdown, modification of the Security Function Policy, and modification of the definition of audited events. OE.Install and OE.Protect insure that the product is properly installed so the TOE SynApps module is invoked by the IT environment and the IT Environment shall include physical protection for the TOE such that unauthorized personnel cannot tamper with the TOE. OE.Operations insures that the TOE is operated in a secure manner consistent with administrative guidance. OE.NonBypass insures that the network driver passes every well formed packet it receives to the TOE. OE.I&A ensures that a user must possess a valid user identifier and password prior to assuming the administrative role.

8.1.2 Mapping Assumptions to Objectives for the IT Environment

Table 8-3 shows that all of the assumptions are addressed by security objectives for the IT Environment. The rationale for the mappings is provided below.

Table 8-3. Assumptions Mapped to Objectives for the IT Environment

Item	Assumption	Assumption Description	Objective for the IT Environment
A1	A.Admin	It is assumed that the TOE Administrator will install, configure, and operate the TOE according to the instructions provided by the TOE documentation, and that administrators are not malicious.	OE.Install, OE.Operations, OE.Person
A2	A.Physical	It is assumed that the Radware appliance, the Management Station, and the connection between the Radware appliance and the Management Station will be located in a controlled access facility that prevents unauthorized physical access.	OE.Protect

A.Admin - This assumption is met by OE.Install, which states that the IT environment and TOE shall be properly installed so that the TOE SynApps module is invoked by the IT environment. OE.Operations insures that the TOE is operated in a secure manner consistent with administrative guidance. OE.Person provides that Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.

A.Physical - This assumption is met by OE.Protect, which states that the IT Environment shall include physical protection for the Radware appliance hosting the TOE, the Management Station thru which the CLI is accessed and the connection between Radware appliance and the Management Station such that unauthorized personnel cannot tamper with the TOE or the administrative connection to the TOE.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives of the TOE are satisfied by at least one security functional requirement and Table 8-5 shows that all security functional requirements map to at least one security objective for the TOE. The rationale for the mappings is provided in the text below.

Table 8-4. Mapping of Security Objectives to SFRs for the TOE

Item	Objective Name	Objective Description	SFR
1	O.Alarms	The TOE shall send notification when an attack is detected.	FAU_ARP.1
2	O.Audit_Analysis	The TOE shall provide the capability to monitor network operations and indicate when an attack is identified.	FAU_SAA.4
3	O.Flow	The TOE shall enforce a Security Function Policy, as defined by the Administrator, on data flowing through the TOE.	FDP_IFC.1
4	O.Flow_Attributes	The TOE shall enforce a Security Function Policy using defined security attributes for network operations.	FDP_IFF.1
5	O.Manage_Attributes	The TOE shall allow only the Administrator to modify security attributes defined within the Security Function Policy.	FMT_MSA.1 FMT_SMF.1 FMT_MSA.3
6	O.Manage_Ops	The TOE shall allow only the Administrator to perform startup and shutdown, modification of the Security Function Policy, and modification of the definition of audited events.	FMT_MOF.1 FMT_SMF.1 FMT_MSA.3

Table 8-5. Mapping of SFRs to Security Objectives

Item	SFR	Description	Maps to Objective
1	FAU_ARP.1	Security alarms	O.Alarms
2	FAU_SAA.4	Complex attack heuristics	O.Audit_Analysis
3	FDP_IFC.1	Subset information flow control	O.Flow
4	FDP_IFF.1	Simple security attributes	O.Flow_Attributes
5	FMT_MOF.1	Management of security functions behaviour	O.Manage_Ops
6	FMT_MSA.1	Management of security attributes	O.Manage_Attributes
7	FMT_MSA.3	Static attribute initialisation	O.Manage_Ops O.Manage_Attributes
8	FMT_SMF.1	Specification of management functions	O.Manage_Ops O.Manage_Attributes

O.Alarms - The TOE shall send notification when an attack is detected. This objective is met by FAU_ARP.1, which states that the TOE shall generate security alarms for events defined by the Administrator. This will include specific filters, filter groups, and policies that the TOE allows the Administrator to define.

O.Audit_Analysis - The TOE shall provide the capability to monitor network operations and indicate when an attack is identified. This objective is met by FAU_SAA.4, which requires that the TOE be capable of monitoring the network traffic and indicate an attack when the record of system activity matches an internal representation of specific event sequences of known intrusion scenarios and signature events[details found in FAU_SAA.4] maintained by the TOE.

O.Flow - The TOE shall enforce a Security Function Policy, as defined by the Administrator, on data flowing through the TOE. This objective is met by FDP_IFC.1, which requires that the TOE be capable of enforcing the SynApps Application Security SFP as defined by the Administrator, on subjects, information, and objects, i.e., network entities passing data, network data traffic, and network operations.

O.Flow_Attributes - The TOE shall enforce a Security Function Policy using defined security attributes for network operations. This objective is met by FDP_IFF.1, which requires that the TOE enforce the SynApps Application Security SFP for the defined security attributes, including global attributes and specific policies.

O.Manage_Attributes - The TOE shall allow only the Administrator to modify security attributes defined within the SFP. This objective is met by FMT_MSA.1, which states that the listed security attributes may only be modified by the Administrator, FMT_MSA.3, which defines the default behaviour of the SFP, and FMT_SMF.1, which states that such security management capabilities shall be provided by the TOE.

O.Manage_Ops - The TOE shall allow only the Administrator to perform startup and shutdown, modification of the SFP, and modification of the definition of audited events. This objective is met by FMT_MOF.1, which states that startup and shutdown of the TOE, the definition of security policies, and auditing functionality shall be under the control of the Administrator, FMT_MSA.3, which defines the default behaviour of the SFP, and by FMT_SMF.1, which states that such security management capabilities shall be provided by the TOE.

8.2.2 Functional Requirements for the IT Environment

Table 8-6 shows the mapping of security objectives for the IT Environment to SFRs for the IT Environment. The rationale is provided in the text below.

Table 8-6. Mapping of Functional Requirements for the IT Environment to Objectives

Item	SFR	Description	Objective
1E	FIA_UAU.2	User authentication before any action	OE.I&A
2E	FIA_UID.2	User identification before any action	OE.I&A
3E	FPT_STM.1	Reliable time stamps	OE.Time
4E	FPT_RVM_EXP.1	Non-bypassability of the TSP: IT	OE.NonBypass

Item	SFR	Description	Objective
5E	FPT_SEP_EXP.1	TSF domain separation: IT	OE.Install, OE.Protect, OE.Operations. OE.Person

OE.I&A - The IT Environment shall require user identification and authentication prior to any user action. This objective is met by FIA_UID.2 and FIA_UAU.2, which require that the user be authenticated and identified before any function may be accessed.

OE.Time – The IT Environment shall provide reliable time stamps. This objective is met by FPT_STM.1, which requires that the IT environment be able to supply the TOE with reliable time stamps.

OE.NonBypass – The IT environment must ensure the network driver passes every well formed packet it receives to the TOE. This objective is met by FPT_RVM_EXP.1 which provides that the security functions of the IT environment shall ensure that the network driver passes every well formed packet it receives to the TOE.

OE.Install– The TOE and IT environment shall be properly installed. The IT environment must ensure the IT environment's security functional policy is invoked and succeeds before allowing another IT environment function to proceed and that the TOE SynApps module is invoked by the IT environment. Specifically the Network driver must pass network traffic only to and from the TOE. This objective is met by FPT_SEP_EXP.1 which provides that the IT environment will support the IT environments self protection functions, including the network driver which will be configured to pass network traffic to the TOE for filtering, and back from the TOE towards the destination IP address.

OE.Protect– The IT environment shall include physical protection for the TOE such that unauthorized personnel cannot tamper with the TOE. This objective is met by FPT_SEP_EXP.1 which provides that the IT environment will support the IT environments self protection functions.

OE.Operations – The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. This objective is met by FPT_SEP_EXP.1 which provides that the IT environment will support the IT environments self protection functions.

OE.Person - Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective is met by FPT_SEP_EXP.1 which provides that the IT environment will support the IT environments self protection functions.

8.2.3 Dependencies

Table 8-7 shows the dependencies between the functional requirements for the TOE and the IT Environment. All dependencies are satisfied.

Table 8-7 TOE Dependencies Satisfied

Item	Component	Component Name	Dependencies	Reference
1	FAU_ARP.1	Security alarms	FAU_SAA.1	2 (H)
2	FAU_SAA.4	Complex attack heuristics	No dependencies	None
3	FDP_IFC.1	Subset information flow control	FDP_IFF.1	4

Item	Component	Component Name	Dependencies	Reference
4	FDP_IFF.1	Simple security attributes	FDP_IFC.1 FMT_MSA.3	3 7
5	FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 FMT_SMF.1	None 8
6	FMT_MSA.1	Management of security attributes	FMT_SMR.1 FDP_IFC.1 FMT_SMF.1	None 3 8
7	FMT_MSA.3	Static attribute initialisation	FMT_SMR.1 FMT_MSA.1	None 6
8	FMT_SMF.1	Specification of management functions	None	None
1E	FIA_UAU.2	Timing of authentication	FIA_UID.1	2E (H)
2E	FIA_UID.2	Timing of identification	No dependencies	None
3E	FPT_STM.1	Reliable time stamps	No dependencies	None
4E	FPT_RVM_EXP.1	Non-bypassability of the TSP: IT	No dependencies	None
5E	FPT_SEP_EXP.1	TSF domain separation: IT	No dependencies	None

The dependency of FMT_MSA.1, FMT_MSA.3 and FMT_MOF.1 on FMT_SMR.1 is not applicable to this evaluation because the product (and hence the TOE) only has one role, the administrative role. There is no untrusted user role, or user data on the Radware product.

8.2.4 Strength of Function Rationale

There are no permutational or probabilistic functions within the TOE, therefore SOF is not applicable and a rationale is not required.

8.2.5 Assurance Rationale

Evaluation Assurance Level (EAL) 3 was chosen because it provides appropriate assurance measures for the expected application of the product. EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behavior. EAL3 provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures. EAL3 also requires a moderate level of independently assured security. AVA_VLA.1 includes an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

FPT_RVM_EXP.1 Non-bypassability of the TSP. External users are not permitted to access the TOE's Administrative interface, except thru a specially configured, physically protected interface, because of configuration of the IT environment. Only once an external user is identified and authenticated with the IT environment does the IT environment permit them to access the TOE's administrative interface. Publicly accessible device ports are configured to prevent external users from accessing or invoking the IT environments security functions.

The use of physical protection and administrative user authentication ensures that the TSF functions are accessed and invoked only after the IT environment security policy enforcement functions have been invoked and succeeded and only by authenticated administrators, thus preventing an untrusted user from modifying the IT environment so as to disable or bypass the TOE.

Furthermore, since the Radware product is a preinstalled network appliance, the security functions of the IT environment ensure that the network driver passes all well formed packets it receives to the TOE, and that no network driver function within the scope of control of the IT environment is will bypass the TOE.

FPT_SEP_EXP.1 TSF domain separation, ensures that TSF executes in its separated security domain, which is protected from interference and tampering by untrusted subjects.

Each publicly accessible network segment connected to the TOE is connected thru a unique configured port. The port configuration does not permit a user on a network segment to make a connection directly with the TOE, but only from a client on one network segment to a client on another connected network segment. The configured port passes network traffic to the network driver which in turn passes that traffic to the TOE. The TOE processes the network traffic and then conditionally passes the network traffic back to the network driver for its next hop towards the IP destination address thru a (different) configured port. The TOE and IT environment is configured to require network traffic to pass thru the TOE before flowing between two clients on different network segments.

8.2.7 Explicitly Stated Requirements Rationale

The explicitly stated requirements FPT_RVM_EXP.1 Non-bypassability of the TSP: IT environment, and FPT_SEP_EXP.1 TSF domain separation: IT environment, were added because the TOE relies upon the IT environment to support non-bypassability and domain separation.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-8 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-8 Mapping of TOE Functional Requirements to TOE Summary Specification

Item	SFR	Security Function	Rationale

1	FAU_ARP.1	Audit	SynApps detects violations of security policy and generates alarms.
2	FAU_SAA.4		SynApps maintains an internal representation of specific set event sequences of known intrusion scenarios and signature events. SynApps module examines the network traffic and compares the record of the system activity against the signature events and event sequences and indicates violation of the policy if the system activity matches any of the signature events and event sequences .
3	FDP_IFC.1	Information Flow Control	SynApps performs information flow control by the definition of filters, filter groups, and policies, which define the controls on the network traffic flowing through the SynApps module
4	FDP_IFF.1		
5	FMT_MOF.1	Security Management	The CLI supports Management of security functions behavior by restricting definition of information flow and audit policies to the Administrator.
6	FMT_MSA.1		Management of security attributes, i.e., defining global parameters and policies which are the security attributes within the TOE, is restricted to the Administrator, since it is contained in SynApps, which is accessible only to the Administrator. The Administrator is sets all global parameters, filters, filter groups, and policies.
7	FMT_MSA.3		SynApps passes all network traffic by default. The Administrator selectively blocks network traffic by specifying filters through the CLI. Filters are specified in FDP_IFF.1.
8	FMT_SMF.1		SynApps performs management functions as specified in FMT_MSA.1 and FMT_MOF.1.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-9.

Table 8-9 Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.3	CM Documentation CM Plan Configuration Item List	Radware SynApps Configuration Management Plan	This evidence was written to address the configuration management documentation. This includes identifying the evaluated TOE and providing a configuration list with configuration items that have been uniquely identified and the method used to identify them.
2	ACM_SCP.1	CM Plan	Radware SynApps Configuration Management Plan	This evidence was written to address the configuration management documentation. This includes identifying the evaluated TOE and providing a configuration list with configuration items that have been uniquely identified and the method used to identify them.
3	ADO_DEL.1	Delivery Procedures	Radware SynApps Configuration Management Plan	This evidence addresses delivery procedures for the TOE and documents how the TOE is securely provided to the customer.
4	ADO_IGS.1	Installation, Generation, and Startup procedures	WSD Pro / WSD Pro+ / WSD Pro AS / WSD-DS / WSD-NP User Guide, Software Version 8.0 DefensePro User Guide, Software Version 1.21 Radware APSolute OS Addendum for Installers for the Evaluated Configuration	This evidence addresses Installation, Generation, and Startup procedures for the evaluated TOE. This includes that the TOE is installed, generated, and started as the developers intended with the assurance that each time it is done the securely and the same way.
5	ADV_FSP.1	Functional Specification	Radware APSolute OS EAL3 Common Criteria Evaluation Propriety Development Specification	This evidence addresses the security functions of the TOE. This includes identifying and describing the external TOE security function interfaces.

Item	Component	Evidence Requirements	How Satisfied	Rationale
6	ADV_HLD.2	High-Level Design	Radware APSolute OS EAL3 Common Criteria Evaluation Propriety Development Specification	This evidence describes the security functionality of the TOE and supporting protection mechanisms implemented.
7	ADV_RCR.1	Representation Correspondence	Radware APSolute OS EAL3 Common Criteria Evaluation Propriety Development Specification	This evidence was written to show a correspondence analysis between the ST and the functional specification; and between the functional specification and the high level design.
8	AGD_ADM.1	Administrator Guidance	WSD Pro / WSD Pro+ / WSD Pro AS / WSD-DS / WSD-NP User Guide, Software Version 8.0 DefensePro User Guide, Software Version 1.21 Radware APSolute OS Addendum for Installers for the Evaluated Configuration	This evidence addresses administrator guidance. It describes how to securely administer the TOE.
9	AGD_USR.1	User Guidance	Not Applicable	No Non-Administrative Users
10	ALC_DVS.1	Development Security Documentation	Radware APSolute OS Development Security	This evidence describes the developer's security controls on the development environment and demonstrates that they are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.
11	ATE_COV.2	Test Coverage Analysis	Radware APSolute OS Test Coverage Analysis	This evidence demonstrates that the tests provided systematically test the TSF against the functional specification.

Item	Component	Evidence Requirements	How Satisfied	Rationale
12	ATE_DPT.1	Depth of Testing analysis	Radware APSolute OS Test Coverage Analysis	This evidence demonstrates that the tests provided systematically test the TSF against the high-level design.
13	ATE_FUN.1	Test Documentation	Test Plan for SynApps Radware Test Plan and Report EAL 3 Evaluation Radware SynApps version 3.402151	This evidence provides tests that demonstrate that the TOE security functions operate as described in the ST and development documentation.
14	ATE_IND.2	TOE for Testing	TOE provided for testing	
15	AVA_MSU.1	Misuse Analysis	WSD Pro / WSD Pro+ / WSD Pro AS / WSD-DS / WSD-NP User Guide, Software Version 8.0 DefensePro User Guide, Software Version 1.21 Radware APSolute OS Addendum for Installers for the Evaluated Configuration Radware APsolute OS Misuse Analysis of Guidance Documentation	This evidence provides guidance to securely administer, operate, and use the TOE.
16	AVA_SOF.1	SOF Analysis	Not Applicable	No Strength of Function is claimed for the TOE
17	AVA_VLA.1	Vulnerability Analysis	CC EAL 3 Vulnerability Analysis For Radware SynApps Release 3.402151	This evidence describes obvious vulnerabilities applicable to the TOE and describes how those vulnerabilities are addressed.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.