Smart Network. Smart Business.

DefensePro Product Family

Software Version 5.11

Security Target

Version 0.4

February 26, 2012

Prepared for:

Radware Ltd.
22 Raoul Wallenberg St.,
Tel-Aviv, Israel 69710

Prepared by:

Metatron
Security Services

Metatron Ltd.
66 Yosef St.,
Modiin, Israel 71724

- Confidential - For internal Radware use only –

Document Version Control Log

Version	Date	Author	Description
0.1	August 28, 2010	Nir Naaman	Initial draft.
0.11	September 14, 2010	Nir Naaman	Added footnote excluding cryptographic algorithms from the evaluation.
0.2	January 31, 2011	Nir Naaman	TOE software version updated to 5.11.00. Dropped support for x008 models. Incorporated PETR comments.
0.3	September 20, 2011	Nir Naaman	Updated Security Log size. Signature updates are loaded manually into the TOE. Removed Telnet and HTTP management interfaces from the TOE.
0.4	February 26, 2012	Nir Naaman	Updated TOE identification to 5.11.01. Augmented assurance claim to ALC_FLR.3. Console interface is excluded from TOE.

Table of Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Reference

Title:	DefensePro Product Family Software Version 5.11 Security Target
ST Version:	0.4
ST Date:	February 26, 2012
Author:	Nir Naaman
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009

Evaluation Assurance Level (EAL):

EAL 4, augmented with ALC_FLR.3 (Systematic flaw remediation).

Keywords: Intrusion Detection, IDS, IPS, Denial of Service, DOS, network security

1.2. TOE Reference

TOE Identification:

The TOE is comprised of DefensePro version 5.11.01 (build 39) software, running on one of the following supported Radware models:

- DefensePro DP-x412-NL-D-OZ device (2U with DME)
- DefensePro DP-x016-NL-Q devices (1U)
- DefensePro DP-x016-NL-D-Q devices (2U)
- DefensePro DP-x016-NL-D-QF devices (2U with DME)

1.3. TOE Overview

The DefensePro product family is a set of network devices that are deployed inline in the network, providing real-time network based Intrusion Detection/Prevention System (IDS/IPS) and anti-Denial of Service (DoS) protections for internal applications and infrastructure.

A DefensePro device collects and analyzes network traffic flowing through the device, and can be configured to detect a wide set of attacks and suspected intrusion attempts. Detected events are recorded on the device, and can be configured to trigger reaction mechanisms such as blocking the suspected traffic and generating alarms.

The Target of Evaluation (TOE) includes the DefensePro device. Administrators use standard hardware and software that is outside of the TOE to provide management user interfaces for each of the TOE's administration interfaces. Management interfaces may include:

- SSH client (CLI interface)

- Web browser
- Web Services client software
- SNMPv3 manager software (e.g. Radware APSolute Vision)

User accounts are maintained in an internal database on the DefensePro device. DefensePro can be optionally configured to authenticate users with the support of an external authentication server in the IT environment, using the RADIUS protocol.

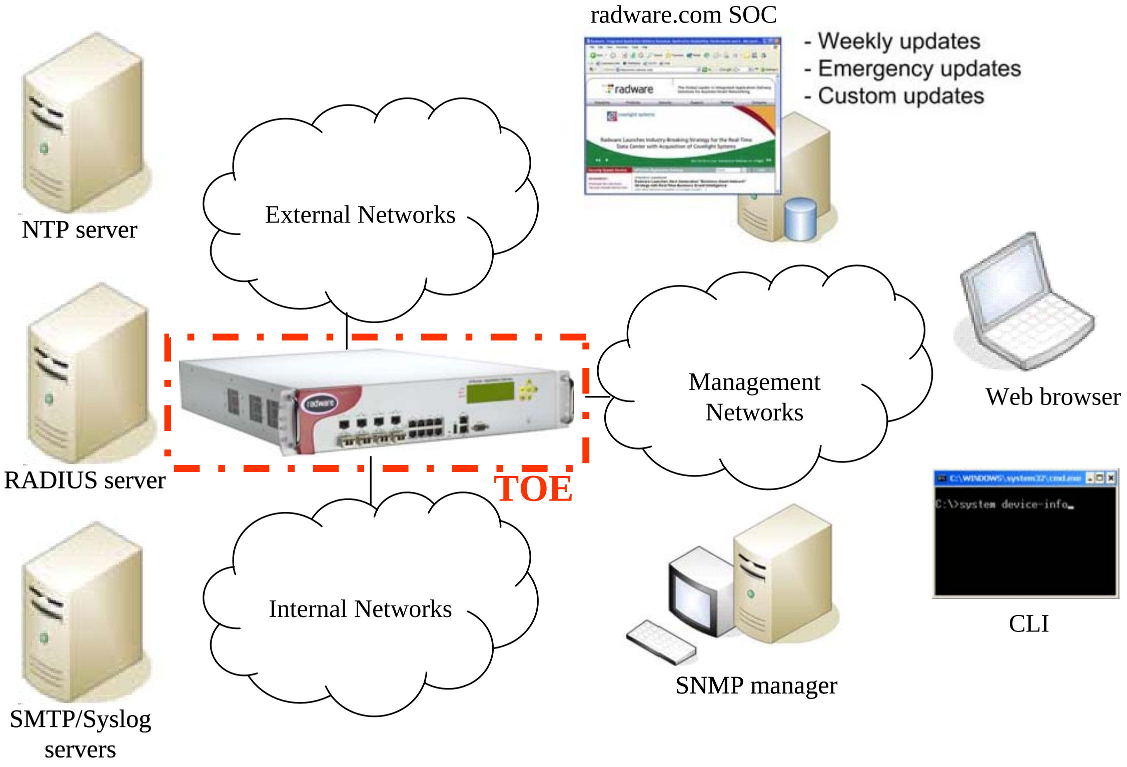
Administrators manage DefensePro devices using Command Line Interpreter (CLI), Web, and/or SNMP-based administration interfaces, after first authenticating by entering a correct user name and password. Authorized System administrators can modify IDS System data collection, analysis, and reaction behavior. The devices can also support restricted administrator accounts that can only manage other product settings.

The device generates an audit trail of all access and configuration change events. Audit records are not maintained on the device. They are delivered to users via SNMP traps and/or displayed on users' terminal interfaces. Administrators can review IDS System data stored on the device.

DefensePro can be configured to generate alarms that may be transmitted to external log and email servers using the Syslog and SMTP protocols, respectively.

DefensePro devices contain an internal hardware clock that provides timestamps for System data and security audit records. In addition, the device can be configured to synchronize its clock with an external time server in the IT environment, using the NTP protocol.

Figure 1-1 - TOE Boundary



```
C:\>system device-info_
```

1.4. Document Organization

Section 1 provides the introductory material for the security target, including ST and TOE references, TOE Overview, and TOE Description.

Section 2 identifies the Common Criteria conformance claims in this security target.

Section 3 describes the security problem solved by the TOE, in terms of the expected operational environment and the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through additional environmental controls identified in the TOE documentation.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 is intended to be used to define any extended requirements claimed in this security target that are not defined in the Common Criteria.

Section 6 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 7 explains how the TOE meets the security requirements defined in section 6, and how it protects itself against bypass, interference and logical tampering.

Section 8 provides supplemental information that is intended to aid the reader, including highlighting conventions, terminology, and external references used in this security target document

1.5. TOE Description

1.5.1. Physical Scope and Boundaries of the TOE

1.5.1.1. TOE Hardware, Firmware, and Software

The TOE consists of the set of DefensePro devices identified in section 1.3 above. Each device is delivered to the customer pre-installed with a real-time operating system and DefensePro software. All device hardware, firmware, and software is included within the TOE.

Some of the DefensePro device models contain hardware accelerators: a DoS Mitigation Engine (DME) to prevent high volume DoS/DDoS flood attacks – without impacting legitimate traffic – and a String Match Engine (SME) to accelerate signature detection. These accelerators are included in the TOE.

Figure 1-2 - DefensePro Device

1.5.1.2. TOE Guidance

The following Radware guidance is considered part of the TOE:

Title	Date	Document ID
DefensePro User Guide Software Version 5.11	February 2011	RDWR-DP-V0511_UG1101
Radware Installation and Maintenance Guide	February 2011	RDWR_IG_1101
DefensePro Product Family Common Criteria Evaluated Configuration Addendum, Software Version 5.11.01	February 26, 2012	Document version 0.3

1.5.2. Logical Scope of the TOE

1.5.2.1. Summary of TOE Security Functionality

DefensePro is a real-time in-line network Intrusion Prevention System (IPS). It employs multiple intrusion detection engines that analyze network traffic flowing through the DefensePro device, in order to detect suspected network-based attacks and to react by generating alarms and blocking suspected traffic. The following types of intrusion analysis engines are applied to network traffic:

- Statistical Network Behavioral Analysis (NBA)
- Signature Matching Engine with proactive updates from Radware’s Security Operations Center (SOC)
- Stateful Protocol Inspection for various application protocols
- Access Control List (ACL) Match – against administrator-configurable ACLs
- Connection Limit protections
- SYN Cookies (DoS protection)

When traffic is categorized as an attack, the product generates IDS System event records that are stored on the device, and generates alarms that can be configured to be delivered over: syslog protocol, SMTP (email), SNMP traps, and/or be displayed as alarms on CLI-based management interfaces. In addition, the device can take action by dropping the traffic and/or sending TCP resets to the source or destination addresses, as appropriate.

Administrators manage DefensePro devices using a variety of management interfaces, supporting effective management of security functions and data. Management interfaces may include: remote CLI access via SSH, Web-based access using HTTPS, Web Services API over HTTPS, or SNMPv3-based access by management server software. Administrators are always identified and authenticated by user name and password before they can perform any action on the device.

An audit facility can be configured to generate audit records for all administrator access to the device. Audit records are timestamped using a reliable hardware clock in the device. Administrators can review audit records via multiple administration interfaces. The responsibility for storage and of audit records and for selectable review of audit data including sorting of audit data is levied on the IT environment.

Administrators can review IDS System data stored on the device. DefensePro devices protect stored IDS System data from unauthorized access. An alarm is generated when IDS System data storage capacity is reached.

1.5.2.2. *Network Behavioral Analysis*

DefensePro’s multi-dimension Fuzzy Logic NBA decision engine collects traffic characteristics parameters and assigns them an anomaly weight according to an adaptive fuzzy membership function. It then correlates these parameter weights and produces real-time decisions represented by a “degree of attack (or anomaly)” value. Based on these degrees of attack figures, the system is then able to introduce counter-measures that actively repel a perceived threat.

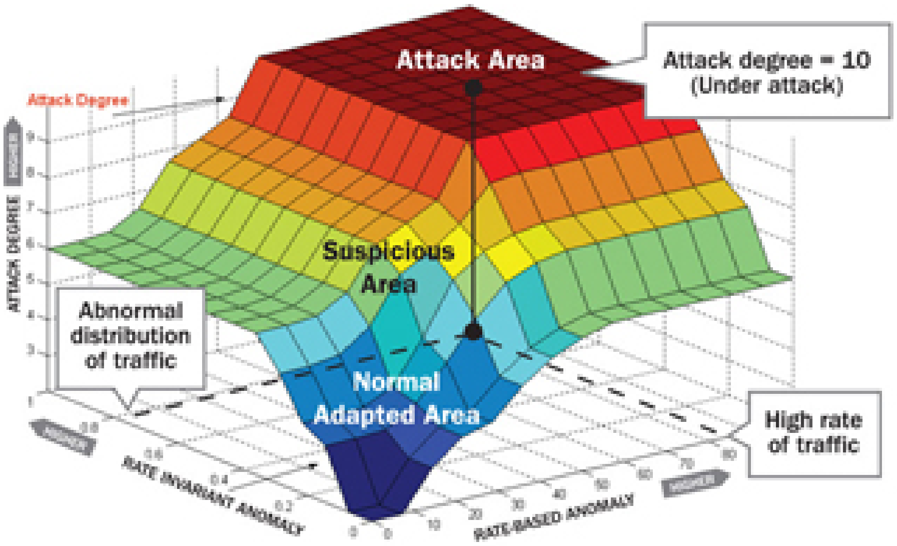
The Fuzzy Logic Module includes adaptive capabilities. The sensitivity of the module is being continuously tuned in order to match the characteristics of the protected network. The adaptive algorithms include Infinite Impulse Response (IIR) filters that continually average traffic parameters and shape the Fuzzy Logic membership functions accordingly.

For each required protection type, the Fuzzy Logic decision collects and learns traffic parameters that are needed in order to best characterize the threat that should be identified and mitigated. Typically, the fuzzy logic decision engine uses two categories of traffic behavioral parameters to generate a degree of attack:

- **Rate-based** behavioral parameters such as packet rate, Mbps, connection rate, application request rate, application response rate etc.
- **Rate invariant** behavioral parameters such as protocol breakdown, TCP flag distributions, ratio between inbound and outbound traffic, application request/response ratio, connections distribution, URL hits probability functions and more.

Figure 1-3 below depicts an example Fuzzy Logic decision surface. The XY plane shows the fuzzy input (rate-based input and rate-invariant input). The z-axis represents the degree of attack (or anomaly).

Figure 1-3 - Fuzzy Logic Decision Surface



1.5.2.3. Elimination of False Positives

In order to eliminate false positive decisions and misdetections, the Fuzzy Logic engine correlates between both rate and rate-invariant parameters.

To illustrate this point, consider the frequent legitimate behavior of a mass crowd entering a news website in an unexpected manner. This behavior immediately causes rate-based behavioral parameters to significantly increase, thus making it look like an anomaly. If the detection engine relies only on rate-based behavioral parameters, this completely legitimate behavior will be flagged as an attack, and will be blocked. However, because rate-invariant parameters will remain unchanged (within certain boundaries) during such legitimate mass crowd behavior, correlating between both types of parameters allows the engine to flag this occurrence as a false positive.

1.5.2.4. Automatic Real-Time Signature Generation

When the Fuzzy Logic engine detects an anomaly, the system activates the automatic attack signature generation mechanism in order to find characteristic parameters of the ongoing anomaly, by distinguishing between expected and unexpected repetition of protocol-specific parameters that were studied (statistically) according to the network environment. The automatic signature generation mechanism flags unexpected values as "possible" pieces of the attack signature that represents the ongoing detected anomaly.

Once values of these parameters are flagged as “abnormal”, the system transits into a signature optimization state that activates a closed-feedback loop mechanism.

The closed-feedback module is responsible for creating the narrowest, but still effective, signature blocking rule. Each one of the analyzed parameters types can include multiple values, detected by the automatic signature generation mechanism. The closed-feedback module tailors these values through AND and OR logical relationships. The more AND logical relationships that are constructed between different values and parameter types, the narrower and more accurate the blocking signature rule is considered to be.

In order to create the logical relationship rules between the detected signature values, the closed-feedback module uses the following feedback cases:

- **Positive feedback**: The traffic anomaly was reduced as a result of the decided blocking signature rules created by the module, the system continues to use the same action and tailors more attack characteristic parameters (i.e., signature types and values) through as many AND logical relationships as possible.
- **Negative feedback**: Meaning that the degree of traffic anomaly was not changed or was increased, the system stops using the last blocking signature rules and continues to search for more appropriate ones.
- **Attack stopped feedback**: If the attack stops, then the system will stop all countermeasures immediately, i.e., remove the signature rule.

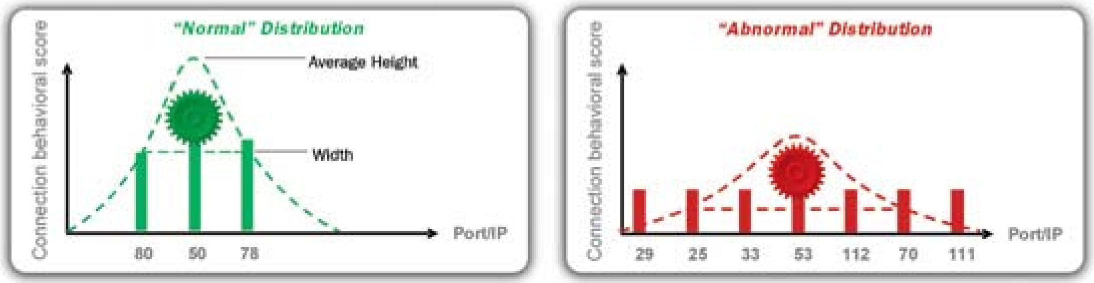
1.5.2.5. *NBA Profiles*

DefensePro includes predefined NBA profiles that optimize detection and mitigation of the following types of attacks:

- DoS/DDoS flood attacks
- Self-propagating worms
- Horizontal and vertical scans
- Misuse of Web application resources
- Server cracking attacks (scans, brute-force, and dictionary attacks)
- Infected clients

For example, Figure 1-4 depicts on the left a normal distribution curve, which represents a normal client's traffic behavior patterns. The figure on the right represents traffic that indicates an attack (e.g. malware propagation). The distribution curves are generated by the decision engine using statistical analysis of multiple clients' traffic parameters.

Figure 1-4 - Infected Client Detection



1.5.2.6. *IPS Signature Analysis*

For to the more deterministic types of threats, such as known application vulnerability exploitation attacks for which a signature is already available, Radware's 24x7 Security Operations Center (SOC) provides subscribers with an automated, weekly delivery of new attack signature filters as well as emergency and custom delivery of signatures. The signature files can be loaded manually by the authorized System administrator into the device's attack database, in the form of regular expressions.

1.5.2.7. *Stateful Protocol Inspection*

Stateful Inspection protection provides additional protection for application level attacks by ensuring that transmission and application stateful rules are enforced based on the protocol Requests for Comments (RFCs). Stateful Inspection tracks protocol state-machines and enforces RFC compliance for each protocol.

Stateful Inspection profiles prevent the injection of packets out of session and the misuse of protocol header fields.

Protocol compliance enforcement capabilities are available for the IP, ICMP, TCP, DNS, HTTP, HTTPS, SMTP, POP3, IMAP, FTP, and SSH protocols.

1.5.2.8. ACL Matching

The Access Control List (ACL) engine matches traffic against stateful access control policies that allow or block sessions according to presumed source and destination addresses, protocol, requested service, physical interface, and VLAN tags.

System administrators can view and modify the set of ACLs.

1.5.2.9. DoS Protection

DefensePro provides an extensive set of anti-DoS protections, based on both the Signature Match engine (DoS Shield) and the NBA engines (Behavioral DoS Protection).

In addition, Connection Limit profiles defend against session-based attacks, such as half open SYN attacks, request attacks, and full connection attacks. The profiles contain attacks defined for groups of TCP or UDP application ports. DefensePro counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client + server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the threshold set defining an attack, any session/connection over the threshold is dropped.

DefensePro can defend against SYN floods by sending SYN cookies: particular choices of initial TCP sequence numbers, based on an device-selected secret function. Instead of forwarding client SYN requests to the server, the device generates a SYN cookie and returns it to the client. The device does not allocate resources to queue the SYN requests, thereby protecting itself and the target server from a potential SYN flood. A valid client will complete the TCP handshake, returning the SYN cookie to the device. The device validates the cookie, and then starts forwarding the traffic (as a transparent proxy) between the client and the server.

1.5.2.10. Management

DefensePro supports[1] multiple administration interfaces, including:

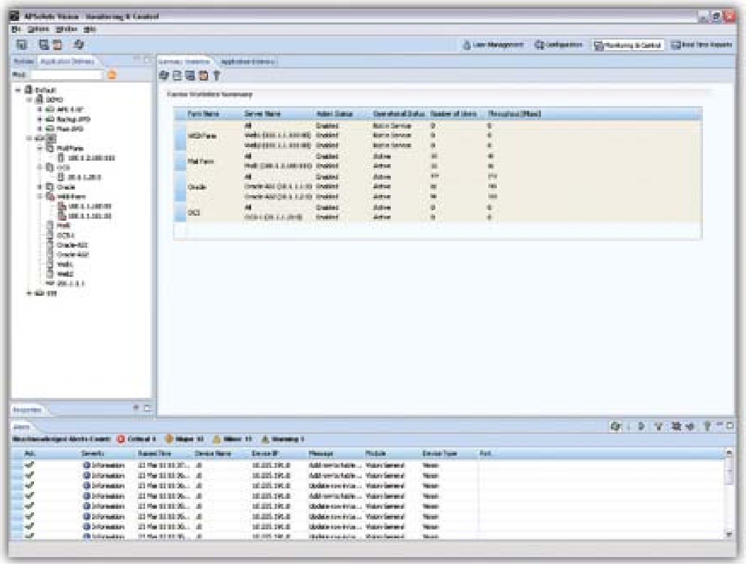
- SSH access to CLI
- HTTPS access to Web-based interface (WBM)
- Web Services API over HTTPS
- SNMPv3

[1] The SSH, HTTPS, and SNMPv3 protocols are supported management interfaces. The protocol definitions for these interfaces include the use of cryptographic algorithms; however, no cryptographic mechanisms are being claimed in this ST as security functionality, and no cryptographic algorithms or protocols are being evaluated in the context of this ST.

All management interfaces interact with the DefensePro MIB stored on the device, and provide equivalent functionality.

Figure 1-5 below is a screen shot from Radware's APSolute Vision management software, which uses the SNMPv3 protocol to access the DefensePro MIB and to receive and display SNMP traps generated as DefensePro alarms. Note that APSolute Vision (or any other management client) is supported by the TOE but considered to be outside of the TOE boundary.

Figure 1-5 - APSolute Vision SNMP-based Management Software



All administrator interfaces require the user to authenticate using a password prior to allowing access to the device. Password verification can be configured locally, or by querying a RADIUS server in the IT Environment.

1.5.2.11. Security Audit

DefensePro can be selectively configured to generate security audit records for all access attempts to the device, and for all configuration changes, via any management interface. The records are delivered to users via SNMP traps and/or displayed on users' terminal interfaces (i.e. SSH sessions).

1.5.2.12. Time Synchronization

DefensePro devices contain a reliable hardware clock that provides secure timestamps for audit records and for IDS System data records. In order to provide support for clock synchronization of multiple TOE devices and/or external IT entities, DefensePro includes an NTP polling agent that can be configured to interact with a remote time synchronization server in the IT environment.

1.5.2.13. Functionality Excluded from the TOE Evaluated Configuration

The following DefensePro functionality is excluded from the evaluated configuration:

- **Bypass Modes** - the DefensePro product supports bypass modes that provide degraded security functionality when the device is overloaded or powered down. TOE evaluated configuration guidance requires that these modes be disabled, in order to ensure that claimed security functionality cannot be bypassed.
- **SNMPv1 and SNMPv2** – while the DefensePro product supports SNMPv1, SNMPv2, and SNMPv3 as administration interfaces, only SNMPv3 User Security Model (USM) may be enabled in the evaluated configuration, because it supports the IDS System Protection Profile requirements for user identification and authentication.
- **Telnet and HTTP Management Interfaces** – DefensePro devices can be managed over the Telnet protocol, using a CLI interface, and over the HTTP protocol, using a Web browser. These two protocols are disabled by default, and should not be enabled in the evaluated configuration. Equivalent management functionality can be obtained using the SSH and HTTPS protocols, respectively.
- **Statistics Reporting Protocol (SRP)** – the DefensePro product supports a proprietary monitoring protocol for efficient transmission of statistical data from the device to Radware APSolute Vision management servers. This interface is disabled by default, and should not be enabled in the evaluated configuration.
- **Out-of-Path Deployment** – DefensePro devices can be deployed out-of-path as an IDS, receiving traffic from a switch mirror port. Out-of-path deployment, inspecting mirrored traffic, is not included in the evaluated configuration, in order to be able to provide a traffic blocking reaction capability.

2. Conformance Claims

2.1. CC Conformance Claim

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002, extended (CC Part 2 extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, conformant (CC Part 3 Conformant)

2.2. Assurance Package Conformance

The TOE is package-name augmented with the following assurance package:

- Evaluation Assurance Level (EAL) 4 - augmented with ALC_FLR.3.

2.3. PP Conformance

The TOE is Protection Profile Conformant with the following Protection Profile:

- U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007

2.4. Conformance Rationale

2.4.1. Introduction

This section is intended to demonstrate that the statements of the security problem definition, security objectives, and security requirements in this ST are consistent with the PP for which conformance is being claimed: [IDSSPP].

The claimed protection profile is a CCv3.1 PP that require demonstrable PP conformance.

2.4.2. Consistency of the Security Problem Definition

The security problem definition in this ST is equivalent to the security problem definition of the claimed PP. This is established by reproducing all of the assumptions, threats, and OSPs defined in the claimed PP in this ST, with the following exceptions:

- The [IDSSPP] identifies three threats that are to be defined only if the TOE contains a Scanner: T.SCNCFG, T.SCNMLC, and T.SCNVUL. As the TOE does not contain a Scanner, these threats have not been included in this ST.

2.4.3. Security Objectives Conformance

The statement of security objectives in this ST is equivalent to the security objectives defined in [IDSSPP]. This is established by reproducing all of the security objectives for the TOE and for the environment defined in the claimed PP in this ST, with the following exceptions:

- O.IDSCAN - The [IDSSPP] requires that a conformant TOE must include at least one Sensor or Scanner (see [IDSSPP] application note for IDS_SDC.1), but not both. DefensePro provides a Sensor that inspects traffic flowing through the TOE, but does not actively scan protected hosts for vulnerabilities.
- O.EXPORT - Omitted as per the guidance given by [PD-0097].
- OE.IDAUTH – Introduced in support of O.IDAUTH for configurations in which the TOE authenticates users with the support of an external authentication server in the IT environment. This is consistent with the guidance given by [PD-0151] as well as [PD-0115].

2.4.4. Security Functional Requirements Conformance

The TOE demonstrably meets and exceeds all security requirements of the claimed [IDSSPP], except for the FAU_STG.4, FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 requirements that are inapplicable to the TOE, and for FAU_SAR.3 and FAU_STG.2 which are treated in this ST as IT Environment SFRs (see rationale below).

All security requirements from the claimed PP have been restated in this ST, except for the SFRs listed above as exceptions. For some requirements, a hierarchical component was selected in place of one or more of the PPs' requirements; by definition a TOE meeting the hierarchical requirement would meet the original requirement as well. Similarly, requirements have been qualified, within the bounds set by the PPs. Permitted operations performed on PP security functional requirements are identified in Table 6-1.

The following subsections provide conformance rationale for individual SFRs that were omitted as exceptions or refined in respect to the claimed PP, clarifying the relationship of an SFR to the claimed PP.

2.4.4.1. FAU_SAR.3

The [IDSSPP] levies the FAU_SAR.3 Selectable audit review requirement for the ability to perform sorting of audit data on the TOE; however, this contradicts the mapped [IDSSPP] objective OE.AUDIT_SORT, which states that the sorting capability shall be provided by the IT environment. This ST will treat FAU_SAR.3 as an IT Environment SFR.

This interpretation is compatible with the Errata Sheets appended to [IDSSPPv1.6] (from which the [IDSSPP] was derived), which state that the FAU_SAR.3 requirement may be moved to the IT environment, and OE.AUDIT_SORT be levied on the IT environment.

Note: [PD-0152] discusses an equivalent [IDSSPP] inconsistency relating to FPT_STM.1 and OE.TIME. It allows the designation of FPT_STM.1 to the IT Environment.

2.4.4.2. FAU_STG.2

The [IDSSPP] levies the FAU_STG.2 Guarantees of audit data availability requirement for the protection of stored audit records on the TOE; however, this contradicts the mapped [IDSSPP] objective OE.AUDIT_PROTECTION, which states that the IT Environment shall be responsible for protecting audit data. This ST will treat FAU_STG.3 as an IT Environment SFR.

This interpretation is compatible with the Errata Sheets appended to [IDSSPPv1.6] (from which the [IDSSPP] was derived), which state that the FAU_STG.2 requirement may be moved to the IT environment, and OE.AUDIT_PROTECTION be levied on the IT environment.

See also corresponding discussion above in relation to FAU_SAR.3.

2.4.4.3. FAU_STG.4

The [IDSSPP] FAU_STG.4 Prevention of audit data loss requirement is intended to uphold the O.OFLOWS and O.AUDITS security objectives for the TOE.

O.OFLOWS states that the TOE must appropriately handle potential audit storage overflows. O.AUDITS states that the TOE must record audit records. Although the TOE does record audit records (see FAU_GEN.1), it does not store them within the TOE, but provides them to users for storage outside the TOE. See discussion above in relation to FAU_STG.2 for why this is demonstrably conformant with the [IDSSPP].

Because audit records are not stored within the TOE, there is no potential for audit storage overflows, and FAU_STG.4 is therefore not applicable to the TOE. This ST will treat FAU_STG.4 as an IT Environment SFR.

2.4.4.4. FIA_AFL.1

The [IDSSPP] FIA_AFL.1 Authentication failure handling requirement relates to external IT products that might authenticate to the TOE.

This SFR has been omitted as per the guidance given in [PD-0097], which states that this requirement was incorrectly included in the system PP.

2.4.4.5. FIA_UID.1 and FIA_UAU.1

This ST claims FIA_UID.2 and FIA_UAU.2, which are hierarchical to the corresponding [IDSSPP] FIA_UID.1 and FIA_UAU.1 SFRs.

2.4.4.6. FMT_SMF.1

FMT_SMF.1 has been included in this ST to satisfy FMT class dependencies.

2.4.4.7. FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1

These SFRs have been omitted as per the guidance given in [PD-0097], which states that these requirements were incorrectly included in the system PP.

2.4.4.8. Applicable NIAP Precedent Decisions

The following precedent decisions have been used as guidance for interpreting demonstrable conformance with the claimed PP, in relation to claimed SFRs:

Table 2-1- References to Guidance on the Interpretation of Claimed PPs

Reference	Affected SFRs and objectives	Description
[PD-0097]	O.EXPORT, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FIA_AFL.1	Incorrectly included in the System PP – must be removed from the PP
[PD-0152]	FAU_SAR.3, FAU_STG.2	Inconsistency in the [IDSSPP] tracing TOE SFRs to objectives for the IT Environment – FAU_SAR.3 and FAU_STG.2 are treated in this ST as being levied on the IT Environment.

2.4.5. Security Assurance Requirements Conformance

The claimed [IDSSPP] requires a minimum assurance level of EAL 2, augmented with ALC_FLR.3.

The level of assurance chosen for this ST is that of EAL 4, augmented with ALC_FLR.3. The assurance requirements in this ST are therefore clearly hierarchically stronger than the ones required by the claimed PP.

3. Security Problem Definition

3.1. Threats

This section describes the threats that are addressed either by the TOE or the environment (identical[2] to the corresponding threats described in [IDSSPP], provided here for the benefit of the reader of the ST):

3.1.1. TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System’s collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

3.1.2. IT System Threats

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

[2] The [IDSSPP] identifies three threats that are to be defined only if the TOE contains a Scanner: T.SCNCFG, T.SCNMLC, and T.SCNVUL. As the TOE does not contain a Scanner, these threats have not been included in this ST.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2. Assumptions

The following conditions are assumed to exist in the operational environment (identical to the set of assumptions made in [IDSSPP], provided here for the benefit of the reader of the ST):

3.2.1. Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors[3].

3.2.2. Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2.3. Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

[3] A.ASCOPE is an assumption that is upheld by the OE.INTROP objective for the environment. Per the guidance given in [PD-0118], this assumption is given in the wording used in [IDSSPP].

3.3. Organizational Security Policies

The following OSPs are defined in [IDSSPP]. [IDSSPP] does not identify which organization and which organizational security policy any of these OSPs are drawn from.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

4.1. Security Objectives for the TOE

This section describes the TOE security objectives (identical[4] to the corresponding set of TOE security objectives described in [IDSSPP], provided here for the benefit of the reader of the ST):

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

[4] [IDSSPP] security objectives omitted from this ST: O.IDSCAN was omitted because the TOE does not contain a Scanner. O.EXPORT was omitted per the guidance given in [PD-0097].

4.2. Security Objectives for the Operational Environment

4.2.1. IT Security Objectives for the Environment

The following security objectives for the IT Environment are defined in [IDSSPP]:

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.

In addition, the following objective for the IT environment is introduced in support of O.IDAUTH for configurations in which the TOE authenticates users with the support of an external authentication server in the IT environment:

OE.IDAUTH	The IT Environment must be able to authenticate users prior to allowing access to TOE functions and data.

4.2.2. Security Objectives for the Environment Upholding Assumptions

The assumptions made in this ST about the TOE's operational environment must be upheld by corresponding security objectives for the environment.

The following security objectives are intended to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they are intended to be satisfied largely through application of procedural or administrative measures.

OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.

4.3. Security Objectives Rationale

4.3.1. IT Security Objectives Rationale

The security problem description and security objectives in this ST are equivalent to the corresponding elements stated in the [IDSSPP], as established in sections 2.4.2 and 2.4.3 above. See section 6.1 of [IDSSPP] for the IT security objectives rationale.

OE.IDAUTH has been introduced in this ST in support of O.IDAUTH for configurations in which the TOE authenticates users with the support of an external authentication server in the IT environment. OE.IDAUTH thus acts in support of O.IDAUTH in relation to threats T.COMINT, T.COMDIS, T.LOSSOF, T.NOHALT, T.PRIVIL, T.IMPCON, and to OSPs P.MANAGE, P.ACCESS, and P.ACCACT.

4.3.2. Non-IT Security Objectives Rationale

See section 6.2 of [IDSSPP].

5. Extended Components Definition

This security target contains the following extended security requirements defined in [IDSSPP]: IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, IDS_STG.2.

Extended security functional requirements are not drawn from [CC] Part 2 components. The [IDSSPP] provides the following explanation for why these requirements cannot be clearly expressed using existing components, and in particular why the FAU class could not be refined to achieve the same result. Note that FAU deals with events that are internal to the TOE, whereas IDS deals with events occurring in the IT environment.

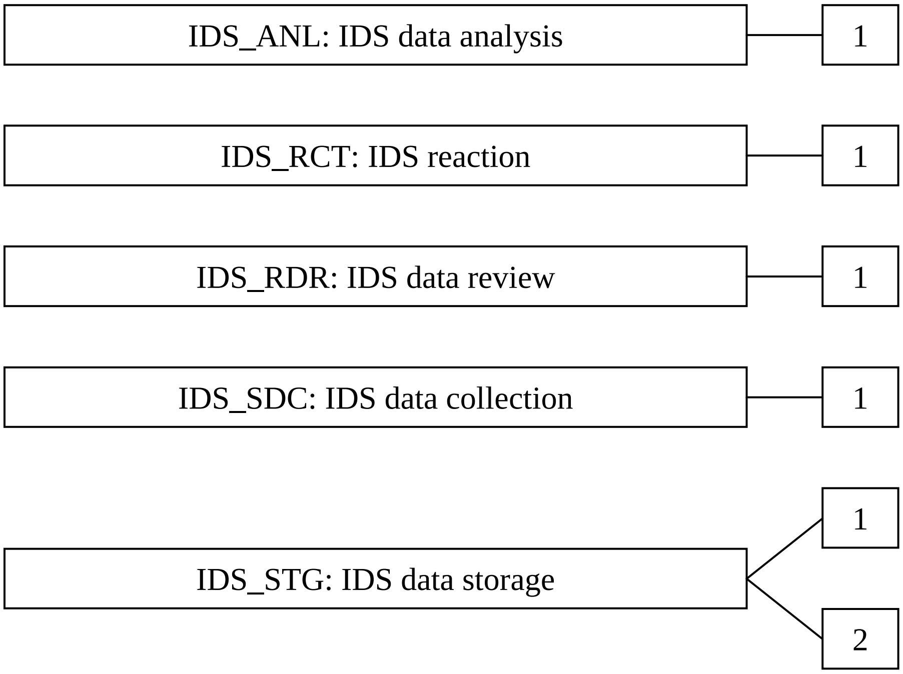
> *"A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data."*

The Extended Components Definition presented here defines an extended component for each extended security requirement, using the existing CC components, families, classes, and methodology as a model for presentation.

5.1. Class IDS: Intrusion Detection

This class is used to satisfy security objectives that pertain to intrusion detection and prevention (IDS/IPS) systems. These include data collection and analysis, automatic reaction capabilities, review, and protection of IDS System data.

Figure 5-1 - IDS: Intrusion detection class decomposition


IDS_ANL: IDS data analysis
1
IDS_RCT: IDS reaction
1
IDS_RDR: IDS data review
1
IDS_SDC: IDS data collection
1
1
IDS_STG: IDS data storage
2

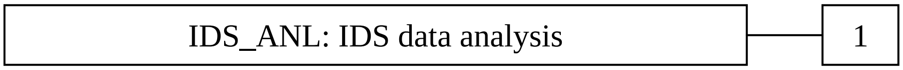
5.1.1. IDS data analysis (IDS_ANL)

Family Behaviour

This family defines requirements for automated means that analyse IDS System data looking for possible or real security violations.

The actions to be taken based on the detection can be specified using the IDS reaction (IDS_RCT) family as desired.

Component levelling



In IDS_ANL.1 Analyser analysis, statistical, signature, or integrity based analysis is required.

Management: IDS_ANL.1

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

a) maintenance (deletion, modification, addition) of the parameters of the analytical functions.

Audit: IDS_ANL.1

The following actions should be auditable if IDS_ANL IDS data analysis is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

5.1.1.1. IDS_ANL.1 Analyser analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [selection: *statistical*, *signature*, *integrity*]; and

b) [assignment: *any other analytical functions*].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

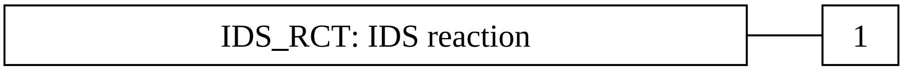
b) [assignment: *any other security relevant information about the result*].

5.1.2. IDS reaction (IDS_RCT)

Family Behaviour

This family defines the response to be taken in case when an intrusion is detected.

Component levelling



At IDS_RCT.1 IDS reaction, the TSF shall send an alarm and take action when an intrusion is detected.

Management: IDS_RCT.1

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

a) the management (addition, removal, or modification) of actions.

Audit: IDS_RCT.1

The following actions should be auditable if IDS_RCT IDS reaction is included in the PP/ST:

a) Minimal: Actions taken due to detected intrusions.

5.1.2.1. IDS_RCT.1 Analyser react

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser analysis

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

5.1.3. IDS data review (IDS_RDR)

Family Behaviour

This family defines the requirements for tools that should be available to authorised users to assist in the review of IDS System data.

Component levelling

IDS_RDR.1 IDS data review, provides the capability to read information from the System data and requires that there are no other users except those that have been identified as authorised users that can read the information.

Management: IDS_RDR.1

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data.

Audit: IDS_RDR.1

The following actions should be auditable if IDS_RDR IDS data review is included in the PP/ST:

a) Basic: Reading of information from the System data.

b) Basic: Unsuccessful attempts to read information from the System data.

5.1.3.1. *IDS_RDR.1 Restricted data review*

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.1.4. IDS data collection (IDS_SDC)

Family Behaviour

This family defines requirements for recording information from the targeted IT System resource(s).

Component levelling

IDS_SDC.1 IDS data collection, defines the information to be collected from the targeted IT System resource(s), and specifies the data that shall be recorded in each record.

Management: IDS_SDC.1

There are no management activities foreseen.

Audit: IDS_SDC.1

There are no auditable events foreseen.

5.1.4.1. *IDS_SDC.1 System data collection*

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

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

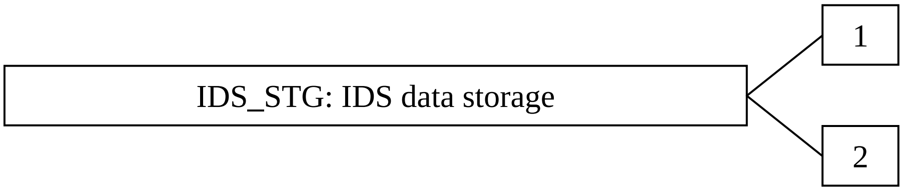
b) [assignment: *other additional information*].

5.1.5. IDS data storage (IDS_STG)

Family Behaviour

This family defines requirements for protecting IDS System data after it is recorded and stored by the TOE.

Component levelling



At IDS_STG.1 Guarantees of System data availability, specifies the guarantees that the TSF maintains over the system data given the occurrence of an undesired condition.

IDS_STG.2 Prevention of System data loss, specifies actions in case of exceeded storage capacity.

Management: IDS_STG.1

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

a) maintenance (deletion, modification, addition) of the actions to be taken in case of storage failure.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

5.1.5.1. IDS_STG.1 Guarantees of System data availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_STG.1.2 The System shall protect the stored System data from modification.

IDS_STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion*, *failure*, *attack*].

5.1.5.2. IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_STG.1 Guarantees of system data availability

IDS_STG.2.1 The System shall [selection: '*ignore System data*', '*prevent System data, except those taken by the authorised user with special rights*', '*overwrite the oldest stored System data* '] and [assignment: *other actions to be taken in case of storage failure*] if the storage capacity has been reached.

6. Security Requirements

6.1. Security Functional Requirements

The functional security requirements (SFRs) for this ST consist of the following components from CC Part 2, summarized in Table 6-1. All SFRs were taken from [IDSSPP], except for FMT_SMF.1, which was introduced in this ST in order to satisfy FMT class dependencies.

Subjects, objects, and operations are as defined in the [IDSSPP].

The CC defined operations of assignment, selection, and refinement were applied in relation to the PP requirements as described in column 3 of Table 6-1 below.

Table 6-1 –Security functional requirement components

Functional Component		CC Operations Applied
FAU_GEN.1	Audit data generation	None
FAU_SAR.1	Audit review	Assignment
FAU_SAR.2	Restricted audit review	None
FAU_SEL.1	Selective audit	Assignment
FIA_ATD.1	User attribute definition	Assignment, refinement
FIA_UAU.2	User authentication before any action	Hierarchical
FIA_UID.2	User identification before any action	Hierarchical
FMT_MOF.1	Management of security functions behaviour	None
FMT_MTD.1	Management of TSF data	Assignment
FMT_SMF.1	Specification of management functions	Assignment
FMT_SMR.1	Security roles	Assignment, refinement
FPT_STM.1	Reliable time stamps	None
IDS_ANL.1	Analyser analysis	Selection, assignment
IDS_RCT.1	Analyser react	Assignment
IDS_RDR.1	Restricted Data Review	Assignment
IDS_SDC.1	System Data Collection	Selection, assignment
IDS_STG.1	Guarantee of System Data Availability	Assignment, selection
IDS_STG.2	Prevention of System data loss	Selection

6.1.1. Security Audit (FAU)

6.1.1.1. Audit data generation (FAU_GEN.1)

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 basic[5] level of audit; and

c) Access to the System and access to the TOE and System data.

Table 6-2 - Auditable Events

Functional Component	Auditable Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System Data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.2	Any use of the authentication mechanism.	User identity, location
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role.	User identity

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, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the additional information specified in the Details column of Table 6-2 - Auditable Events.

[5] The **basic** level of audit is defined in [IDSSPP] as the auditable events included in Table 6-2 - Auditable Events.

6.1.1.2. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authorised administrators and authorised System administrators** with the capability to read **all audit information** from the audit records.

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

6.1.1.3. Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.4. Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type;

b) **severity**.

6.1.2. Identification and authentication (FIA)

6.1.2.1. User attribute definition (FIA_ATD.1)

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

a) User identity;

b) Authentication data; **and**

c) Authorisations[6].

6.1.2.2. User authentication before any action (FIA_UAU.2)

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.

6.1.2.3. User identification before any action (FIA_UID.2)

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

[6] FIA_ATD.1.1 subsection d) assignment ‘any other security attributes’ is completed as ‘None’; the component has been refined to omit subsection d) for clarity.

6.1.3. Security Management (FMT)

6.1.3.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions of System data collection, analysis and reaction to authorised System administrators[7].

6.1.3.2. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to query and add System and audit data, and shall restrict the ability to query and modify all other TOE data to **authorized roles as specified in Table 6-3 below**.

6.1.3.3. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **as specified in Table 6-3**.

Table 6-3- Specification of Management Functions

Component	Management Function	Required Authorisations
FMT_MOF.1	**Modify the behaviour of the functions of System data collection, analysis and reaction**	**Authorised System administrator (administrator assigned Read-Write permissions)**
FMT_MTD.1	**Query audit data**	**All administrator roles**
	Query System data	**All administrator roles**
	Add System and Audit data	**No authorized role**
	Query all other (non-System and audit) TOE data	**All administrator roles**
	Modify all other TOE data	**Authorised System administrator**
FMT_SMR.1	**Modify the group of users that are part of a role**	**Authorised System administrator**

6.1.3.4. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following roles**:** authorised administrator, authorised System administrators[8].

[7] In this ST, the authorised System administrator role is defined as an administrator role that is assigned Read/Write permissions on applicable objects, in relation to FMT_MOF.1, FMT_MTD.1, and FMT_SMR.1.

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

6.1.4. Protection of the TSF (FPT)

6.1.4.1. Reliable time stamps (FPT_STM.1)

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

6.1.5. IDS Component Requirements (IDS)

6.1.5.1. System Data Collection (IDS_SDC.1)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) service requests, network traffic[9].

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

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

b) The additional information specified in the Details column of Table 6-4 – System Events.

Table 6-4 - System Events

Component	Event	Details
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address

6.1.5.2. Analyser analysis (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) statistical, signature; and

b) **stateful protocol inspection;**

c) **ACL match;**

d) **Connection Limiting; and**

e) **SYN cookies**.

[8] FMT_SMR.1.1 assignment ‘other authorised identified roles’ is completed as ‘None’; the component has been refined to omit this assignment for clarity.

[9] IDS_SDC.1.1 subsection b) assignment ‘other specifically defined events’ is completed as ‘None’; the component has been refined to omit subsection b) for clarity. In addition, Table 6-4 has been tailored to omit all PP event descriptions not selected for IDS_SDC.1.1 a).

Application Note: Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences.

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

c) Date and time of the result, type of result, identification of data source;

d) **Identification of destination address;**

e) **Severity;**

f) **Action taken;** and

g) **Attack details**.

6.1.5.3. Analyser react (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to **authorised System administrator-defined syslog, SMTP, SNMP, or terminal alarm destinations** and take **action to block and/or reset applicable network traffic** when an intrusion is detected.

6.1.5.4. Restricted Data Review (IDS_RDR.1)

IDS_RDR.1.1 The System shall provide **authorised administrators and authorised System administrators** with the capability to read **all information** from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.5.5. Guarantee of System Data Availability (IDS_STG.1)

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_STG.1.2 The System shall protect the stored System data from modification.

IDS_STG.1.3 The System shall ensure that **up to 2.500 log record entries of** System data will be maintained when the following conditions occur: System data storage exhaustion.

6.1.5.6. Prevention of System data loss (IDS_STG.2)

IDS_STG.2.1 The System shall overwrite the oldest stored System data and send an alarm if the storage capacity has been reached.

6.2. Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 4 components defined in Part 3 of the Common Criteria, augmented with the Part 3 component ALC_FLR.3.

No operations are applied to any assurance component.

Table 6-5- TOE Security Assurance Requirements

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools

Assurance Class	**Assurance Components**	
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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

See section 6.3 of [IDSSPP] for the rationale for all PP-derived SFRs. The following is rationale for the SFRs added to this ST in addition to [IDSSPP] SFRs:

- FMT_SMF.1 was introduced to satisfy CCv 3.1 dependencies for FMT_MOF.1 and FMT_MTD.1, as identified in Table 6-7. It can therefore be seen to support the security objective O.ACCESS in which these two requirements are grounded. FMT_SMF.1 also directly supports O.EADMIN, in that it includes a set of functions that allow effective management of TOE functions and data.

Table 6-6 summarizes the rationale. It maps security functional requirements to security objectives described in section 4.1. The table clearly demonstrates that each objective is met by at least one SFR and that each SFR meets at least one objective.

Table 6-6- Tracing of SFRs to security objectives for the TOE

	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_GEN.1									✓	
FAU_SAR.1					✓					
FAU_SAR.2						✓	✓			
FAU_SEL.1					✓				✓	
FIA_ATD.1							✓			
FIA_UAU.2						✓	✓			
FIA_UID.2						✓	✓			
FMT_MOF.1	✓					✓	✓			
FMT_MTD.1	✓					✓	✓			✓
FMT_SMF.1					✓	✓				
FMT_SMR.1							✓			
FPT_STM.1									✓	
IDS_SDC.1		✓								
IDS_ANL.1			✓							
IDS_RCT.1				✓						

	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
IDS_RDR.1					✓	✓	✓			
IDS_STG.1	✓					✓	✓	✓		✓
IDS_STG.2								✓		

6.3.2. Security Assurance Requirements Rationale

The level of assurance chosen for this ST is that of Evaluation Assurance Level (EAL) 4, as defined in CC Part 3, augmented with the CC Part 3 component ALC_FLR.3.

EAL 4 ensures that the product has been methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security.

In addition, the assurance requirements have been augmented with ALC_FLR.3 (Systematic flaw remediation) to provide assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE, and providing guidance to TOE users for how to submit security flaw reports to the developer and for how to register themselves with the developer so that they may receive corrective fixes.

6.3.3. Dependency Rationale

Table 6-7 depicts the satisfaction of all security requirement dependencies. For each security requirement included in the ST, the CC dependencies are identified in the column “CC dependency”, and the satisfied dependencies are identified in the “ST dependency” column. Iterated components are identified to help determine exactly which specific iteration is dependent on which SFR or SAR.

Dependencies that are satisfied by hierarchically higher or alternative components are given in **boldface**, and explained in the “Dependency description” column.

Table 6-7- Security Requirements Dependency Mapping

SFR	CC dependency	ST component	Justification (where needed)
FAU_GEN.1	FPT_STM.1	FPT_STM.1	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1	

SFR	CC dependency	ST component	Justification (where needed)
FIA_ATD.1	None		
FIA_UAU.2	FIA_UID.1	**FIA_UID.2**	
FIA_UID.2	None		
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_SMF.1	None		
FMT_SMR.1	FIA_UID.1	FIA_UID.1	
FPT_STM.1	None		
IDS_SDC.1	None		
IDS_ANL.1	None		
IDS_RCT.1	None		
IDS_RDR.1	None		
IDS_STG.1	None		
IDS_STG.2	None		
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	**ADV_FSP.4,** **ADV_TDS.3**	Consistent with EAL4
ADV_FSP.4	ADV_TDS.1	**ADV_TDS.3**	Consistent with EAL4
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_TDS.3, ALC_TAT.1	
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4	
AGD_OPE.1	ADV_FSP.1	**ADV_FSP.4**	Consistent with EAL4
AGD_PRE.1			
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	**ALC_CMS.4,** ALC_DVS.1, ALC_LCD.1	Consistent with EAL4
ALC_CMS.4	None		
ALC_DEL.1	None		
ALC_DVS.1	None		
ALC_FLR.3	None		

SFR	**CC dependency**	**ST component**	**Justification (where needed)**
ALC_LCD.1	None		
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1	
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	**ADV_FSP.4,** ATE_FUN.1	Consistent with EAL4
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, **ADV_TDS.3**, ATE_FUN.1	Consistent with EAL4
ATE_FUN.1	ATE_COV.1	**ATE_COV.2**	Consistent with EAL4
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	**ADV_FSP.4**, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	Consistent with EAL4
AVA_VAN.3	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, **ADV_FSP.4,** ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1	Consistent with EAL4

7. TOE Summary Specification

7.1. SFR Mapping

Table 7-1 provides a description of the general technical mechanisms that the TOE uses to satisfy each SFR defined in section 6. The table includes the description of security functionality given in each SFR by reference, and provides a high-level view of their implementation in the TOE, referencing section 1.5.1 and 1.5.2 for descriptions of the physical and logical components of the TOE, respectively.

Table 7-1 - TOE Summary Specification SFR Mapping

Component	Description of mechanism
7.1.1. Security Audit (FAU)	
FAU_GEN.1	DefensePro generates audit records for each successful and unsuccessful access to the TOE, for all management interfaces. The information recorded includes the date and time of the event, type of management interface, source IP address, user name (where available), and the outcome of the event (success or failure). When Configuration Auditing is enabled, an audit record is generated whenever a configuration variable is modified through any management interface. The audit record contains the following information (as applicable): date and time of the event, type of management interface, source IP address, user name, name of MIB variable that was changed or action performed, the new value for the variable, and the old value. Table 7-2 below, derived from Table 6-2, provides more details on how the TOE meets each auditable event requirement in FAU_GEN.1.

Table 7-2- TSS Mapping for FAU_GEN.1

Functional Component	Auditable Event	Mapping
FAU_GEN.1	Start-up and shutdown of audit functions	Enabling and disabling audit functions is a configuration change that is audited by the Configuration Auditing facility.
FAU_GEN.1	Access to System	All access attempts to the device are audited for all management interfaces.
FAU_GEN.1	Access to the TOE and System Data	Access to the device and all configuration changes are audited for all management interfaces. Configuration Auditing records object IDs and requested access.
FAU_SAR.1	Reading of information from the audit records	Audit records are pushed to users; therefore this requirement is satisfied by auditing user logons.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Unsuccessful access attempts to the device are audited.
FAU_SEL.1	All modifications to the audit configuration	Configuration Auditing audits all audit configuration changes that occur while the audit

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>that occur while the audit collection functions are operating</td><td>collection functions are operating.</td></tr>
<tr><td>FIA_UAU.2</td><td>Any use of the authentication mechanism.</td><td>All access attempts to the device are audited for all management interfaces. Information recorded includes user identity and location.</td></tr>
<tr><td>FIA_UID.2</td><td>All use of the user identification mechanism</td><td>All access attempts to the device are audited for all management interfaces. Information recorded includes user identity and location.</td></tr>
<tr><td>FMT_MOF.1</td><td>All modifications in the behavior of the functions of the TSF</td><td>Configuration Auditing audits all modifications in the behavior of the functions of the TSF.</td></tr>
<tr><td>FMT_MTD.1</td><td>All modifications to the values of TSF data</td><td>Configuration Auditing audits all modifications to the values of TSF data.</td></tr>
<tr><td>FMT_SMR.1</td><td>Modifications to the group of users that are part of a role.</td><td>Configuration Auditing audits all modifications to user and group database tables. The information recorded includes user identity.</td></tr>
</table>
</td></tr>
<tr><td><b>FAU_SAR.1</b></td><td>Audit records are not maintained on the device. They are delivered to users via SNMP traps and/or displayed on users' terminal interfaces (i.e. SSH). The audit records are delivered in a manner suitable for the user to interpret the information.
In addition, for CLI/Web users that have Configuration Tracing enabled, the device sends an email notification containing Configuration Auditing audit records. All changes made to the same MIB entry within a 60 second window are batched together, for clarity.</td></tr>
<tr><td><b>FAU_SAR.2</b></td><td>Audit records can only be delivered to administrative users. Non-administrators do not have an interface through which they can gain read access to the audit records.</td></tr>
<tr><td><b>FAU_SEL.1</b></td><td>Configuration Auditing can be selectively enabled or disabled. Audit record delivery can also be conditioned on event severity, on a per-user basis.</td></tr>
</table>

7.1.2. User identification and authentication (FIA)

FIA_ATD.1	DefensePro devices contain an internal database. Separate tables are used for storing user accounts for the SNMPv3 management interface, and for the device CLI and Web-based interfaces. The following information is maintained for SNMPv3 users: • User identity: User Name • Authentication Data: Authentication Password, Privacy Password • Authorisations: association with an SNMP Group. SNMP Groups are associated with an access entry, which assigns a Read View and a Write View. (A View defines a subset of the SNMP MIB tree.) The following information is maintained for CLI/Web users: • User identity: User Name • Authentication Data: Password • Authorisations: Access Level (Read-Write, Read-Only, or None)

Component	Description of mechanism
FIA_UAU.2	The device does not provide any unauthenticated external interfaces. All device management interfaces: SSH, HTTPS, and SNMPv3 require the user to authenticate using a password before allowing any actions on behalf of that user.
FIA_UID.2	The user is required to be identified by its user name prior to allowing any actions on behalf of that user.

7.1.3. Security Management (FMT)

Component	Description of mechanism
FMT_MOF.1	When an administrator attempts to modify the behaviour of the functions of System data collection, analysis, and reaction via any management interface, this entails modification of a corresponding MIB variable on the device. Such modification is restricted by the device to users with Read-Write permissions, i.e. to authorised System administrators. As described above for 160HFIA_ATD.1, Read-Write permissions are encoded differently for CLI/Web users and for SNMPv3 users. For the former, the permission is an attribute of the user record in the device database. For the latter type of user, the device determines the permission by computing the Write View for the user's associated groups, and determining whether the requested MIB variable is included within any of those views.
FMT_MTD.1	All administrators may query audit and System data. Non-administrators do not have any external interface that may be used for this purpose. No interface is provided to any authorized role for adding System and audit data to the device. All configuration changes are restricted to the authorised System administrator role as described above for 163HFMT_MOF.1.
FMT_SMF.1	All modifications to TSF behaviour, TOE data, and user accounts are implemented through modifications of the device MIB, whether via CLI, SNMP, or Web-based (including Web Services) interfaces. System data is stored in a cyclical database on the device and may be queried through the appropriate MIB entries. Access to audit data is provided by pushing the audit records to the various administrator interfaces: by displaying the audit records on the CLI terminal, and sending the audit records as SNMP traps to SNMP-interface users. Web-based administration interfaces do not provide access to the audit records.
FMT_SMR.1	The device distinguishes between the authorised administrator and authorised System administrator roles based on the user's Read-Write permissions, as explained above for 160HFIA_ATD.1 and 163HFMT_MOF.1.

7.1.4. Protection of the TSF (FPT)

Component	Description of mechanism
FPT_STM.1	DefensePro devices contain a reliable hardware clock that provides secure timestamps for audit records and for IDS System data records. The device can be configured to periodically synchronize its clock with a remote time synchronization server in the IT environment, using the NTP protocol.

Component	Description of mechanism

7.1.5. Intrusion Detection (IDS)

IDS_ANL.1

DefensePro applies a set of analysis functions on collected IDS System data, as configured by the authorized System administrator. These functions are described in detail in section 1.5.2.

Table 7-3 below provides more details on how the TOE meets each analysis function requirement defined in IDS_ANL.1.

Table 7-3- TSS Mapping for IDS_ANL.1

Analysis function	Section	Description of mechanism
statistical	1.5.2.2 - 1.5.2.5	DefensePro's multi-dimension Fuzzy Logic NBA decision engine generates attack signatures automatically based on perceived traffic anomalies and statistical network behavior analysis. It correlates both rate and rate-invariant parameters in order to reduce false positives, and uses a closed-feedback module for optimizing the signature blocking rules.
signature	1.5.2.6	Traffic is matched against regular expression-encoded attack signatures stored on the DefensePro device. Some device models utilize hardware SME accelerators for signature matching. Signature updates can be downloaded from Radware's SOC, and loaded manually into the device by the authorized System administrator.
stateful protocol inspection	1.5.2.7	Stateful Inspection protection provides additional protection for application level attacks by ensuring that transmission and application stateful rules are enforced based on the protocol RFCs. Stateful Inspection tracks protocol state-machines and enforces RFC compliance for each protocol.
ACL match	1.5.2.8	The Access Control List (ACL) engine matches traffic against stateful access control policies that allow or block sessions according to presumed source and destination addresses, protocol, requested service, physical interface, and VLAN tags.
Connection Limiting	1.5.2.9	DefensePro counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client + server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the threshold set defining an attack, any session/connection over the threshold is dropped.
SYN cookies	1.5.2.9	DefensePro can defend against SYN floods by sending SYN cookies. Client SYN requests are forwarded to the server only after the client successfully completes the TCP handshake.

DefensePro generates a security event record whenever an analysis engine identifies a potential attack. Each security event record contains at least the following information:

- Start Time – date and time of attack start
- Category – threat type, e.g. Intrusions, DoS, Scanning, etc.

Component	Description of mechanism
	• Status – the last-report status of the attack (Started, Occurred, Ongoing, Terminated) • Risk – predefined attack severity level (High, Medium, Low, Info) • Attack Name – the name of the detected attack • Source Address, Destination Address • Protocol, Source L4 Port, Destination L4 Port (service) • Action Type (Forward, Drop, Reset Source, Reset Destination) • Physical Port • Attack Details (different for each attack type)
IDS_RCT.1	When traffic is categorized as an attack, DefensePro generates IDS System event records that are stored on the device, and generates alarms that can be configured to be delivered over: syslog protocol, SMTP (email), SNMP traps, and/or be displayed as alarms on CLI-based management interfaces. In addition, the device can take action by dropping the traffic and/or sending TCP resets to the source or destination addresses, as appropriate.
IDS_RDR.1	DefensePro provides access to the IDS System event file stored on the device via all supported management interfaces. The records are displayed in a manner suitable for the user to interpret the information. There is no unauthenticated interface that allows access to IDS System data.
IDS_SDC.1	All network packets flowing through DefensePro are collected and forwarded to the IDS analysis engines. DefensePro parses the packets and extracts protocol-specific information, including the requested service.
IDS_STG.1	IDS System data is stored on the DefensePro device in a cyclical log file, containing up to 2,500 records. Only the authorized System administrator can clear the file or delete it, using TOE management interfaces. There is no interface provided for modifying the stored data.
IDS_STG.2	When the number of entries exceeds the maximum log file size, the oldest entries are overwritten. Alarms are generated when the file is at 80% and 100% utilization.

7.2. Protection against Interference and Logical Tampering

7.2.1. Domain Separation

The DefensePro TOE is a self-contained device running a proprietary real-time operating system. The device does not host untrusted software, processes or users. It does not depend on any component in the IT Environment for its protection from interference and tampering by untrusted users.

Administration interfaces are selectively enabled for each device port. Ports and protocols used for operational traffic cannot be used to tamper or interfere with the TSF.

7.2.2. Administrator Authentication

All management interfaces enabled in the evaluated configuration require successful password-based identification and authentication before the user can perform any action.

7.3. Protection against Bypass

7.3.1. Inline Deployment

DefensePro devices are typically deployed inline. Network traffic flows through the device, ensuring that all traffic is collected and analyzed, and that reaction logic that involves blocking suspected traffic cannot be bypassed.

7.3.2. Protocol Normalization

DefensePro devices apply normalization logic on various protocol streams to ensure that intrusion analysis logic interprets the network traffic flowing through the device in the same way that the target can be expected to. This behavior mitigates various IDS evasion attacks that apply transformations on the attack payloads in order to avoid signature-based detection. For example:

- IP packet fragments are cached, and IDS logic is applied on reassembled packets.
- To avoid evasion techniques when classifying HTTP-GET requests, the URL content is transformed into its canonical representation.
- RPC requests are reassembled when Record Marking is used in accordance with RFC 1831, prior to applying analysis logic.
- FTP commands are parsed, normalized, and embedded telnet opcodes stripped.

7.3.3. Bypass Modes

Although the DefensePro product supports bypass modes that provide degraded security functionality when the device is overloaded or powered down, TOE evaluated configuration guidance requires that these modes be disabled, preventing attackers from overloading or disabling the device with the intention to bypass the TSF.

8. Supplemental Information

8.1. References

The following external documents are referenced in this Security Target.

Identifier	Document
CC	Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002, 002 and 003
CEM	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004
[HTTP]	RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1, June 1999
[HTTPS]	RFC 2818 – HTTP over TLS, May 2000
[IDSSPP]	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007
[IDSSPPv1.6]	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.6, April 4, 2006
[NTP]	RFC 1305 – Network Time Protocol (Version 3) – Specification, Implementation and Analysis
[PD-0097]	NIAP Precedent Decision PD-0097: Compliance with IDS System PP Export Requirements
[PD-0115]	NIAP Precedent Decision PD-0115: Third Party Authentication is permitted by the ALFWPP-MR
[PD-0118]	NIAP Precedent Decision PD-0118: Assumptions in the IDS PP v1.4
[PD-0151]	NIAP Precedent Decision PD-0151: Acceptable Demonstrable Assurance for the IDS System PP v1.7 (BR)
[PD-0152]	NIAP Precedent Decision PD-0152: Internal Inconsistency within the IDS System PP regarding FPT_STM
[RADIUS]	RFC 2865 – Remote Authentication Dial In User Service (RADIUS), June 2000
[RPC]	RFC 1831 – RPC: Remote Procedure Call Protocol Specification Version 2, August 1995
[SMTP]	RFC 2821 – Simple Mail Transfer Protocol, April 2001
[SSH]	RFC 4251 – The Secure Shell (SSH) Protocol Architecture
[SNMPv3]	RFC 2570 – Introduction to Version 3 of the Internet-standard Network Management Framework
[TELNET]	RFC 0854 – TELNET Protocol Specification, May 1983

8.2. Conventions

The notation, formatting, and conventions used in this Security Target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

8.2.1. Security Environment Considerations and Objectives

The naming convention for security problem considerations, objectives, and for subjects and objects is as follows:

- Assumptions are denoted by the prefix “A.”, e.g. “A.ACCESS”.
- Threats are denoted by the prefix “T.”, e.g. “T.COMINT”.
- Objectives for the TOE are denoted by the prefix “O.”, e.g. “O.IDAUTH”.
- Objectives for the operational environment are denoted by the prefix “OE.”, e.g. “OE.TIME”.

8.2.2. Security Functional Requirements

The CC permits four functional and assurance requirement component operations: assignment, iteration, refinement, and selection. These operations are defined in the Common Criteria, Part 1, appendix C.4 as:

- Iteration (not used in this ST): allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

8.2.2.1. Assignment

Some components have elements that contain parameters that enable the ST author to specify a set of values for incorporation into the ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter. Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

8.2.2.2. *Selection*

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

8.2.2.3. *Refinement*

For all components, the ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details. In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

- A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the ST;
- In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement;
- The refined requirement does not extend the scope of the original requirement; and
- The refined requirement does not alter the list of dependences of the original requirement.

8.2.3. Other Notations

8.2.3.1. *Application Notes*

Application Notes are used to clarify the author's intent for a given requirement. These are italicized (except where taken directly from a claimed PP) and will appear following the component needing clarification.

8.2.3.2. *Footnotes*

Footnotes[10] are used to provide further clarification for a statement, without breaking the flow of the text. They are also used to identify text that has been omitted from a SFR in the context of a refinement operation.

8.2.3.3. *References*

References to other documents are given using a short name in square brackets, e.g. "[PD-0105]". The identification of the referenced document is provided in Section 8.1.

[10] This is an example of a footnote.

8.2.4. Highlighting Conventions

The conventions for SFRs described above in section 8.2.2 are expressed in chapter 6 by using combinations of bolded, italicized, and underlined text as specified in Table 8-1 below.

Note that as discussed in Section 6.1, highlighting conventions relating to the CC-defined operations of assignment, selection, and refinement were applied in relation to the requirements as stated in the claimed PP(s).

Table 8-1- SFR Highlighting Conventions

Convention	Purpose	Operation
Boldface	Boldface text denotes completed component assignments. Example: *6.1.3.2 Management of TSF data (FMT_MTD.1)* FMT_MTD.1.1 The TSF shall restrict the ability to query and add System and audit data, and shall restrict the ability to query and modify all other TOE data to **authorized roles as specified in Table 6-3 below**.	(completed) Assignment
<u>Underline</u>	Underlined text denotes completed component selections (out of a set of selection options provided in the original CC requirement). Example: *6.1.5.1 System Data Collection (IDS_SDC.1)* IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): a) <u>service requests</u>, <u>network traffic</u>.	(completed) Selection
<u>**Boldface Underline**</u>	Underlined boldface text highlights component refinements. This includes refinement of an operation that was completed in the PP. Example: *6.1.2.1 User attribute definition (FIA_ATD.1)* FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: a) User identity; b) Authentication data; <u>**and**</u> c) Authorisations[11].	Refinement

[11] FIA_ATD.1.1 subsection d) assignment ‘any other security attributes’ is completed as ‘None’; the component has been refined to omit subsection d) for clarity.

8.3. Terminology

In the Common Criteria, many terms are defined in Section 4 of CC Part 1. The following sections are a refined subset of those definitions, listed here to aid the user of this ST. The glossary is augmented with terms that are specific to the DefensePro product.

8.3.1. Glossary

Administrator An entity that has complete trust with respect to all policies implemented by the TSF.

Assets Entities that the owner of the TOE presumably places value upon.

Assurance Grounds for confidence that a TOE meets the SFRs.

Authentication data Information used to verify the claimed identity of a user.

Authorisation Permission, granted by an entity authorised to do so, to perform functions and access data.

Authorised user A user who may, in accordance with the SFRs, perform an operation.

Compromise Violation of a security policy.

Confidentiality A security policy pertaining to disclosure of data.

External entity Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Fuzzy Logic A form of logic that supports approximate reasoning.

Identity A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity A security policy pertaining to the corruption of data and TSF mechanisms.

Interface A means of interaction with a component or module.

Network Two or more machines interconnected for communications.

Object A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation A specific type of action performed by a subject on an object.

Operational Environment The environment in which the TOE is operated.

Packet A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Role a predefined set of rules establishing the allowed interactions between a user and the TOE.

Security attribute A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

Subject An active entity in the TOE that performs operations on objects.

Threat The potential adverse action of a threat agent on an asset.

Threat Agent Entities that can adversely act on assets.

Target of evaluation A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE security functionality A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

Trusted channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted IT product An IT product other than the TOE which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly (e. g. by being separately evaluated).

TSF data Data created by and for the TOE, that might affect the operation of the TOE.

User See **external entity**.

Vulnerability A weakness in the TOE that can be used to violate the SFRs in some environment.

8.3.2. Abbreviations

Abbreviation	Description
ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CLI	Command Language Interpreter
DDoS	Distributed DoS
DME	DoS Mitigation Engine
DoS	Denial of Service
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP (Secure)
IDS	Intrusion Detection System
IIR	Infinite Impulse Response
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
MIB	Management Information Base
NBA	Network Behavioral Analysis
NIC	Network Interface Card
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RPC	Remote Procedure Call
SFR	Security Functional Requirement
SME	String Matching Engine
SMTP	Simple Mail Transfer Protocol

Abbreviation	Description
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UDP	User Datagram Protocol
URL	Universal Resource Locator
USM	User Security Model