NitroSecurity Intrusion Prevention System 8.0.0

Security Target

Version 1.0

13 October 2009

Prepared for:
NitroSecurity, Inc

12030 Sunrise Valley Drive, Suite 180
Reston, VA. 20191

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is NitroSecurity Intrusion Prevention System provided by NitroSecurity, Inc. The TOE provides a scalable enterprise security solution that provides intrusion prevention, and detection, network behavior analysis, and security event management that enables administrators to secure their networks with real-time[1] threat mitigation.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by the TOE and operational environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and operational environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and details the security assurance requirements (SAR).
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfies the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE Reference, and CC Identification

ST Title – NitroSecurity Intrusion Prevention System 8.0.0 Security Target

ST Version – Version 1.0

ST Date – 13 October 2009

TOE Identification[2] –

- NitroSecurity IPS 8.0.0 running on any one of the following supported appliance models:
  - NS-IPS-150-2BTX, NS-IPS-300-2BTX, NS-IPS-300-4BTX, NS-IPS-300-2SX, NS-IPS-300-4SX, NS-IPS-300R-2BTX, NS-IPS-300R-4BTX, NS-IPS-300R-2SX, NS-IPS-300R-2BSX, NS-IPS-300R-4SX, NS-IPS-300R-4BSX, NS-IPS-620R-2BTX, NS-IPS-620R-4BTX, NS-IPS-620R-8BTX, NS-IPS-620R-2SX, NS-IPS-620R-2BSX, NS-IPS-620R-4SX, NS-IPS-620R-4BSX, NS-IPS-623-R-4C, NS-IPS-623-R-8C, NS-IPS-623-R-4F, NS-IPS-623-R-4BF, NS-IPS-625-R-4C, NS-IPS-625-R-8C, NS-IPS-625-R-4F, NS-IPS-625-R-4F, NS-IPS-645-R-4C, NS-IPS-645-R-8C, NS-IPS-645-R-4F, NS-IPS-4245-R-4BF, NS-IPS-1160-2BTX, NS-IPS-1220-2BTX, NS-IPS-1220-4BTX, NS-IPS-1220-2SX, NS-IPS-1220-2BSX, NS-IPS-1220-4SX, NS-IPS-1220-4BSX, NS-IPS-2230-R-2BTX, NS-IPS-2230-R-4BTX, NS-IPS-2230-R-8BTX, NS-IPS-2230-R-2SX,

[1] 'real time' in this instance is referring to the actual time during which a process takes place or an event occurs and not a technical timing capability.

[2] The differences in the models include the number of ports, copper verses fiber optic cabling, throughput and processing speed, memory and storage. The specific appliance information is available in the product documentation identified in Section 1.1 and from NitroSecurity website, www.nitrosecurity.com.

NS-IPS-2230-R-2BSX, NS-IPS-2230-R-4SX, NS-IPS-2230-R-4BSX, NS-IPS-2250-R-2BTX, NS-IPS-2250-R-4BTX, NS-IPS-2250-R-8BTX, NS-IPS-2250-R-2SX, NS-IPS-2250-R-2BSX, NS-IPS-2250-R-4SX, NS-IPS-2250-R-4BSX, NS-IPS-4245-R-2BTX, NS-IPS-4245-R-4BTX, NS-IPS-4245-R-8BTX, NS-IPS-4245-R-2SX, NS-IPS-4245-R-2BSX, NS-IPS-4245-R-4SX, NS-IPS-4245-R-4BSX, NS-IPS-620R-4C-B,NS-IPS-1220R-4C-2F-B, NS-IPS-1220R-6C-B, NS-IPS-620R-4C-BFS

- NitroSecurity ESM 8.0.0 running on any one of the following supported appliance models:
  - NS-ESS-623-R, NS-ESS-625-R, NS-ESS-2230, NS-ESS-2250-R, NS-ESM-625-R, NS-ESM-645-R, NS-ESM-675-R, NS-ESM-2260-R, NS-ESM-4245-R, NS-ESS-5205-R, NS-ESM-5205-R, NS-ESM-5510-R, NS-ESM-5750-R, NS-ESMR-4200R
- NitroView Receiver 8.0.0 running on any one of the following supported appliance models:
  - NS-NRC-1220, NS-NRC-2230-R, NS-NRC-2250-R, NS-NRC-623-R, NS-NRC-625-R
- NitroView Combo 8.0.0 running on the following supported appliance model:
  - NS-ESMRCV-5205-R
  - NS-ESMRCV-2250-R
  - NS-ESMRCV-625-R
  - NS-ESMRCV-652-R

TOE Developer – NitroSecurity, Inc.

Evaluation Sponsor – NitroSecurity, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 2, September 2007.

NitroSecurity offers a series of documents that describe the installation of TOE (NitroSecurity IPS, NitroSecurity ESM, and NitroView Receiver) as well as guidance for subsequent use and administration of the applicable security features, NitroSecurity NitroView User Guide Version 8.0.0 and NitroSecurity NitroView Installation Guide Version 8.0.0.

1.2 Conformance Claims

This TOE is conformant to the following Common Criteria (CC) specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 2, September 2007.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 2, September 2007.
  - Part 3 Conformant
  - EAL 3 augmented with ALC_FLR.2

The TOE is further conformant to the following Protection Profile (PP):

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

1.3 Conventions

This section specifies the formatting information used in the ST.

The following conventions have been applied in this document:

- Security Functional Requirements (SFRs) – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXT)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. Example: Analyzer analysis (EXT) (IDS_ANL.1)
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The TOE is NitroSecurity's NitroView and NitroGuard network security system version 8.0.0. The TOE includes the software and three hardware appliance components called the NitroSecurity IPS (also called "NitroSecurity NitroGuard IPS", "NitroGuard", "NitroSecurity Intrusion Prevention System", or "IPS"), the NitroSecurity ESM (also called "NitroSecurity NitroView ESM", or "ESM", or "Enterprise Security Manager"), and the NitroSecurity NitroView Receiver (also called "NitroView Receiver" or just "Receiver"). The evaluated configuration includes one or more ESM, one or more NitroGuards, and one or more Receivers.

The TOE provides a scalable enterprise security solution that provides intrusion prevention or intrusion detection, network event and/or flow data acquisition, network behavior analysis, and security event management that enables administrators to secure their networks with real-time[3] threat mitigation. The TOE's NitroGuard component can pass, drop, and log packets as they arrive, based on administrator-configurable rules. When NitroGuard is performing intrusion detection, it is said to be operating in an "IDS mode", when performing intrusion prevention, it is said to be operating in an "IPS mode". Additionally, NitroGuard has an IPS alerts-only mode that is supported when it is operated in an in-line mode. Additionally, the TOE's Receiver can actively and/or passively acquire network event and/or flow data information from various data sources within the network environment (e.g. Windows servers, switches, routers, syslog senders), and correlate all available alerts and flows to detect behaviorally anomalous network activities. In addition, the ESM polls the NitroGuard and Receivers for their data and after some processing, the ESM may send the data to any Receivers it knows about that has the correlation engine enabled for correlation.

The general concept of operation of the TOE includes one or more NitroGuard devices, each in an in-line network location operating in either an IPS mode or in an IPS alerts-only mode, one or more optional Receiver devices, each actively and/or passively collecting network event and/or flow data, and one, or optionally more, ESM devices aggregating, analyzing and reporting on all the collected data. This is depicted in the figure below:

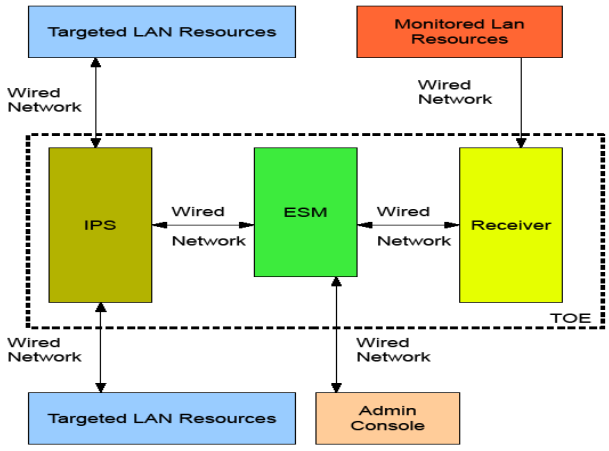

Figure 1: In-line network location of NitroGuard, a Receiver, and ESM

[3] 'real time' in this instance is referring to the actual time during which a process takes place or an event occurs and not a technical timing capability.

In another deployment scenario, of the operation of the TOE's NitroGuard is in an in-tap network location operating in an IDS mode, and is depicted in the figure below:

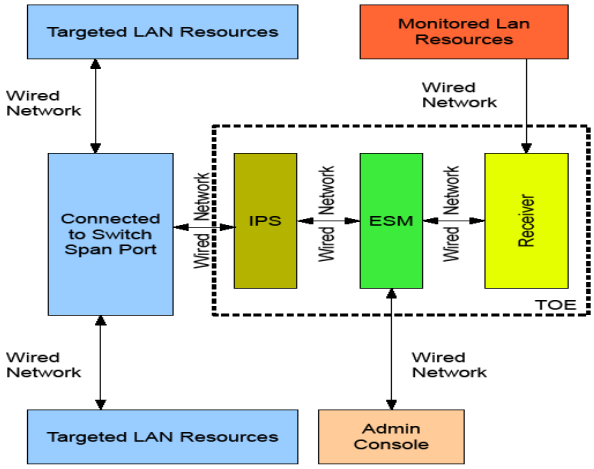

Figure 2: In-tap network location of NitroGuard, a Receiver, and ESM

The TOE is also capable of running in "stealth mode" whether placed in an 'in-tap' or 'in-line' deployment scenario. When configured to run in stealth mode, the IPS device does not require an IP address. The device will not respond to pings, trace routes, or any other high-level mechanics, nor will it respond to ARP requests or any other low level mechanics. It is extremely difficult to detect the presence of the device within a network, effectively reducing the risk of attack against the IPS device itself.

2.1 TOE Overview

The TOE is not a Firewall; it is an IPS that includes a firewall module and it is that module which all network traffic passes. The TOE's NitroGuard passes, drops, and logs packets as they arrive, based on configurable rules. Each NitroGuard device in a TOE deployment is individually configured with rules, notification definitions, modes, variables and other parameters. Following are the three rule types the IPS supports:

- *Firewall Policy rules* - include those rules that the IPS will test against when a packet is examined. These rules correspond to iptables (these include both standard and custom firewall policy rules). The firewall policy rules are adjusted as needed to control the iptables instance running within the IPS component. There are standard firewall rules and custom firewall rules within the policy. For the standard rules, the user can adjust the parameters of the rule including enabling or disabling a rule, for custom rules, the user defines the rules and can enable and disable them. .
- *Standard Policy rules* - include deep-packet inspection rules that evaluate the contents of a packet and compare them with the signatures associated with the rules.
- *Custom Policy rules* - include administrator-modified/created firewall policy rules and standard policy rules as described above.

NitroGuard is designed using the layers of the protocol stack present in data-link and TCP/IP protocol definitions. NitroGuard includes an implementation of Snort, which is an open source packet inspection application implementation. The NitroGuard imposes order on packet data by overlaying data structures on the raw network traffic. These decoding routines are called, in order, through the protocol stack, from the data link layer up through the transport layer, finally ending at the application layer.

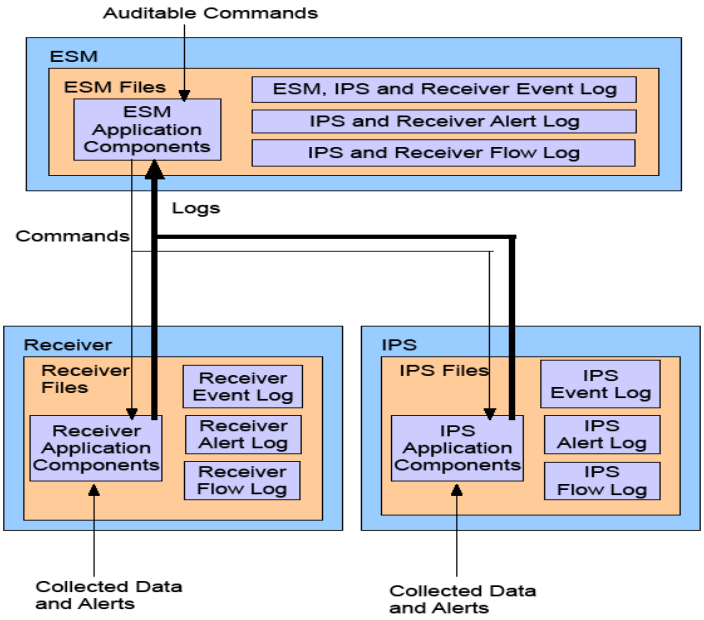

Figure 3: Command and log flow within an ESM, Receiver, and NitroGuard deployment.

When a network packet enters the NitroGuard through one of its physical network interfaces, when it is either in an in-line or an in-tap network location, the packet is first inspected using Linux netfilter/iptables to look for any firewall policy rule matches (packet headers), and to gather flow data information. The first check is done by a netfilter/iptables plug-in that determines if the packet is a control channel packet from the Enterprise Security Manager (ESM) destined for the NitroGuard device. If the packet is a control channel packet it is dropped (The control channel packet is actually processed using a control channel daemon that acquires the packet from the network interface promiscuously). If the packet is NOT a control channel packet, and a match is found that will cause an alert the information is passed to a daemon in the alert module for logging to the alerts database. Additionally, the netfilter/iptables capabilities are used to acquire flow information that is passed to a daemon in the flow module for logging to the flows database. If the packet was not dropped, the NitroGuard passes it to one, of potentially several, Snort instances, each with its own set of inspection rules to be matched against a packets content, running on the NitroGuard device. If a match is found, Snort has a custom plug-in, which enables it to send the alert to the alerts database in the alert module for logging. If the packet has gone through both firewall and deep packet inspection without being dropped, it is sent out of the NitroGuard device through the second physical interface of that traffic path.

As for the TOE's Receiver, it too has netfilter/iptables running on it as its firewall, but this firewall generates no alerts[4]. The Receiver's netfilter/iptables instance is used to 1) limit the flow of packets into the Receiver to those packets of interest (e.g. If the Receiver is supposed to accept syslog packets from IP address 1.2.3.4, then netfilter/iptables will be configured to allow syslog packets in from 1.2.3.4), 2) detect and drop control channel packets, and 3) to acquire flow data. Note that the Receiver processes control channel packets and acquires flow data in exactly the same manner described for the TOE's IPS.

The evaluated configuration does not allow the use of the bypass feature that allows all traffic to pass, even malicious traffic.

[4] The TOE is not a Firewall, it is an IPS. When configured in IPS mode, the rules could be defined as simple firewall flow control rules. Its integration with snort traffic analysis rules are what distinguishes this product in IPS mode from a simple Traffic Filter Firewall. No firewall functionality was evaluated.

2.2 TOE Architecture

The TOE can be described in terms of the following components:

- NitroSecurity IPS (NitroGuard) – A hardware appliance that provides network intrusion prevention or detection services for an enterprise type network. The component detects network intrusion attempts and actively records and/or thwarts such attempts. The component selectively passes, drops, and logs packets as they arrive, based on an administrator configurable rules. Additionally, the component provides blacklisting functions, and the collection of flow data information.
    - Includes the following sub-components:
        - NitroSecurity hardware appliance
        - NitroSecurity software that includes
            - Linux operating system[5]
            - User- and Kernel-mode components that perform IDS and IPS functions and flow data information collection.
- NitroSecurity ESM – A hardware appliance that provides web-based administrator console interface that can be used to manage NitroGuard and Receiver device services and collected data that are accessible using a web browser in the operational environment. The ESM is the central point of administration for data, settings, and configuration.
    - Includes the following sub-components:
        - NitroSecurity hardware appliance
        - NitroSecurity software that includes
            - Linux operating system
            - User- and Kernel-mode components that provide web-based GUI administrative interfaces
- NitroSecurity NitroView Receiver – A hardware appliance that enables the collection of network infrastructure, and end station events, and network flow data from multiple vendor sources including firewalls, VPNs, routers, IPS/IDS, NetFlow, sFlow and others. This provides data acquisition functions across multiple vendors' devices, such as Cisco, Checkpoint and Juniper firewalls, NitroSecurity and McAfee IPS devices, and Cisco and Foundry routers. The NitroView Receiver analyzes the raw acquired data to categorize and normalize it, creates alerts and inserts them into its alerts database. The NitroView Receiver passively and actively acquires data. Additionally, the Receiver has a "correlation engine" running on it, which actively analyzes data sent from the NitroSecurity ESM, which originated on NitroGuard devices and this or other Receivers, looking for interesting patterns it is configured to report on.
    - Includes the following sub-components:
        - NitroSecurity hardware appliance
        - NitroSecurity software that includes
            - Linux operating system
            - User- and Kernel-mode components that perform data acquisition and correlation functions

The Linux operating system has been customized for use with the NitroSecurity components. The version of Linux is based on the 2.6 series of the Linux Kernel and has been updated with patches that address identified security concerns. The Linux operating system does not provide a general-purpose computing environment. The Linux operating system includes support for additional hardware, implementation of network protocols, enhancements to network connection tracking and statistics, custom iptables extensions, and packet forwarding improvements when operating in IDS mode.

The Receiver and IPS (NitroGuard) devices are accessed and modified (i.e. configured) by the ESM using a control protocol that is transmitted between them using their network stack OS interfaces. Authorized administrators access

[5] The Linux operating system is embedded in the device to support Nitro appliance functionality.

and manage all aspects of IPS devices via their web browsers. Communication is secured via the HTTPS protocol, between their computers and the ESM device.

The ESM appliance provides a GUI to administer any and all NitroGuard and Receiver devices. It is accessed using a web browser on a system in the operational environment. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. The administrator console can also be used to manage audit data and users. System data consists of results from NitroGuard scanning, sensing, and analyzing tasks. In addition, the ESM collects the data from the Receiver acquired from other networking devices (i.e. firewalls, VPNs, routers). The ESM appliance uses a proprietary control protocol to communicate with the IPS and Receiver devices. When the TOE is configured to run in FIPS mode, all control channel traffic is transmitted over FIPS certified Virtual Private Network (VPN) connection between the ESM and the IPS or Receiver. HTTPS is used to protect the connection between the web browser in the operational environment and the ESM appliance. The ESM offers HTTP v1.1 using TLS v1.0 to web browsers; in FIPS mode, these functions are FIPS certified. The FIPS certificate number for the ESM component is 1103, the certificate number for the NitroGuard component is 1097, the certificate number for the NitroView Receiver component is 1104, and the certificate number for the Combo component is 1138. Note, stealth mode is not available when the TOE is running in FIPS mode.

The ESM and NitroGuard also supports a command line interface, though is not considered security relevant as opposed to the GUI. The terminal commands are used in a maintenance mode and should only be used under the direction of NitroSecurity Support personnel for emergency situations. The use of the commands are restricted to the Administrator and they are not used for any management required by the ST.

The following features are not included in the evaluated configuration:

- SNMPv3 usage of the Blacklist option in FIPS mode – this feature is removed when the system is operating in FIPS mode because it does not comply with FIPS regulations. Following are the settings for the SNMPv3 options when operating in FIPS mode:
  - SNMP configuration GUI tab - Blacklist checkbox and Authentication Mode is always “None”
  - Event Forwarding GUI tab - Authentication Mode is always “None”
  - Profile Management GUI tab - Authentication Mode is always “None”
  - Receiver Properties > Data Sources GUI dialog - Authentication Mode is always “None”
- 3rd-party Smart Dashboard – this is Check Point’s management system that can be used to manage various devices within an organization’s network.
- 3rd-party Snot Barnyard – is an application that keeps up with a 1000 Mbps connection for a unified logging and a unified log reader.
- Remedy Ticket System – this application allows events from the TOE to be sent to Remedy that indicates the event that has been or will be remedied
- Nitro Plug-in Protocol - Nitro Plug-in Protocol is a means to interface with NitroView Receiver. The Nitro Plug-in Protocol provides a means for an external program to insert events into the Receiver’s database.

2.2.1 Physical Boundaries

The TOE consists of the following components:

- NitroSecurity IPS 8.0.0 running on supported appliance models as identified in Section 1.1
- NitroSecurity ESM 8.0.0 running on supported appliance models as identified in Section 1.1
- NitroSecurity NitroView Receiver 8.0.0 running on supported appliance models as identified in Section 1.1

The differences in the models include the number of ports, copper verses fiber optic cabling, throughput and processing speed, memory and storage. The specific appliance information is available in the product documentation identified in Section 1.1 and from NitroSecurity website, www.nitrosecurity.com.

The intended operational environment of the TOE can be described in terms of the following components:

- *Targeted IT systems – Hosts in the environment sending and/or receiving network traffic and/or security relevant network operational data.*

- *Web browser – Used to access ESM GUI interfaces. Note, for FIPS mode only, the supported Web browsers are IE 7 or higher and FireFox 1.5.0.4 or later.*
- *Adobe Flash Player v9.0.124.0 or later - required to access the ESM.*
- *NTP server – Used to set ESM system clock.*
- *RADIUS server – Used to support external authentication services.*
- *SMTP server – Used to receive email alerts generated by the TOE*
- *SNMP server – Used to receive SNMP alerts generated by the TOE*
- *Syslog servers – Used to receive log message alerts generated by the TOE*
- *Certificate authority server – Provides digital certificates to support the web-based GUI*
- *DNS Server – Used to governs the DNS records and implement the name-service protocol*

2.2.2 Logical Boundaries

The logical boundaries of the TOE include the security functions implemented at the TOE interfaces. These functions include:

- Security audit
- Identification and authentication
- Security management
- TSF protection
- Intrusion detection

2.2.2.1 Security audit

All three TOE appliances; NitroGuard, ESM, and Receiver generate audit records when security-relevant events occur. Auditable events generated by the IPS and Receiver are sent at regular administrator-configured intervals for storage and review by the ESM appliance. Audit records are stored in an audit trail on the ESM appliance. The audit trail is physically protected by the ESM appliance hardware. The audit trail is protected from unauthorized access by restricting access to the ESM web-based GUI interface used to read from the audit trail.

2.2.2.2 Identification and authentication

The NitroGuard and Receiver appliances cannot be accessed directly. Their system data collection interfaces are invoked upon receipt of monitored network traffic. They are managed using the ESM appliance, which can only be accessed after an authorized user successfully logs into the ESM web-based GUI interface using a valid username and password. The TOE also provides a mechanism to lock or disable a user account after a configured number of consecutive failed attempts to logon.

Authentication services can be handled either internally (fixed passwords) or through a RADIUS (Remote Authentication Dial In User Service) authentication server in the operational environment. The external authentication server is considered outside the scope of the TOE.

2.2.2.3 Security management

The ESM appliance provides a GUI interface to administer the NitroGuard and Receiver appliances. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction. System data consists of results from NitroGuard scanning, sensing, and analyzing tasks, as well as the data from the Receiver on other networking devices (i.e. firewalls, VPNs, routers). The administrator console is also used to manage audit data and user accounts.

The TOE also provides the capability to see the physical locations where events have occurred in the network, which increases the ability of tracking down events through the Network Discovery function. The TOE restricts access to this function via the GUI interface. The actual function of Network Discovery is not considered security relevant from the point of view of this TOE, and was not covered by the evaluation..

2.2.2.4 TSF protection

The TOE restricts access to its interfaces by requiring authorized users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the NitroGuard and Receiver appliances. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM appliance. In FIPS mode, the TOE tunnels all traffic between the ESM and NitroGuard/Receiver through a FIPS certified VPN tunnel, and uses a FIPS certified HTTPS crypto function. The FIPS certificate number for the ESM component is 1103, the certificate number for the NitroGuard component is 1097, the certificate number for the NitroView Receiver component is 1104, and the certificate number for the Combo component is 1138.

The TOE relies on NitroSecurity appliance hardware in general to ensure the TSP is enforced and to provide for domain separation.

2.2.2.5 Intrusion detection

The TOE can detect different types of intrusion attempts by performing analysis of network traffic packets depending on location within a network. The TOE supports installation in different locations in the network architecture of the TOE operational environment by providing the ability to operate in different types of IDS and IPS/alerts-only modes.

The evaluated configuration does not allow the use of the bypass feature that allows all traffic to pass, even malicious traffic.

3. Security Problem Definition

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Modifications to the security environment as described in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, to which this ST claims compliance are identified in Section 7 Protection Profile Claims.

3.1 Assumptions

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

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 Operational Environment Assumption

A.COMPROT The operational environment will provide protection of TSF data transmitted between the TOE and external entities (such as a RADIUS server and NitroSecurity).

A.EAUTH External authentication services will be available via RADIUS server.

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 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.

3.2.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

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.

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.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

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

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs. Modifications to the security objectives as described in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, to which this ST claims compliance are identified in Section 7 Protection Profile Claims.

4.1 Information Technology (IT) Security Objectives

The following are the TOE security objectives.

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

O.IDSCAN The Scanner must collect and store 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.

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.

O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

The TOEs operational environment must satisfy the following objectives.

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

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.

OE.EAUTH A RADIUS server must be available for external authentication services.

OE.COMPROT The operational environment will provide protection of TSF data transmitted between the TOE and external entities (such as a RADIUS server and NitroSecurity).

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 2 and the Protection Profile (PP) identified in Protection Profile Claims section.

This ST includes a number of extended requirements. Each of the extended requirements is defined in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments. The extended requirements can be identified by the use of the keyword "EXT" in the title.

Every SFR included in the PP is addressed in this Security Target. Each SFR, except as noted in Section 7, was copied from the PP. Each SFR was changed in this ST to complete operations left incomplete by the PP or to make necessary refinements so that the intent of each SFR remains as specified in the PP. Each SFR was also changed, when necessary, to conform to International Interpretations and the version of the CC being claimed.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SAR.3: Selectable Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.2: Guarantees of Audit Data Availability
	FAU_STG.4: Prevention of Audit Data Loss
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User Attribute Definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TOE Security Functions	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_STM.1: Reliable time stamps
IDS: IDS Component requirements	IDS_ANL.1: Analyzer analysis (EXT)
	IDS_RCT.1: Analyzer react (EXT)
	IDS_RDR.1: Restricted Data Review (EXT)
	IDS_SDC.1: System Data Collection (EXT)
	IDS_STG.1: Guarantee of System Data Availability (EXT)
	IDS_STG.2: Prevention of System data loss (EXT)

Table 1: TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 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***] level of audit; and c) [**Access to the System and access to the TOE and System data**].[FAU_GEN.1.1]

Application Note: The auditable events for the basic level of auditing are included in Table 2 Auditable Events.

Component	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	
FAU_STG.4[6]	Actions taken due to the audit storage failure.	
FIA_UAU.2	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	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_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 2: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity **(if applicable)**, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**, [the additional information specified in the Details column of Table 2 Auditable Events].** FAU_GEN.1.2

Application Note: Given that auditing is always enabled on the devices (NitroGuard, ESM, and Receiver) and the system audits the TOE device startup and shutdown, therefore auditing startup and shutdown of the audit mechanism.

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[authorized administrator, authorized System administrators]** with the capability to read **[all audit information]** from the audit records. FAU_SAR.1.1

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

Application note: Permissions that may be assigned general users by system administrators such as Event Management and Reporting permissions that allow access to audit information are defined in section 6.1.2.

[6] It appears the PP inadvertently omitted FAU_STG.4 from the table.

5.1.1.3 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.[FAU_SAR.2.1]

5.1.1.4 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to ~~perform~~ **apply** [**sorting**] of audit data based on [**date and time, subject identity, type of event, and success or failure of related event**].[FAU_SAR.3.1]

Application note: The administrator console interfaces that can be used to sort audit data do not include a separate type of event field. However, there is a "status" field provided by the administrator console that corresponds to IPS component type of event field (which include critical, warning, and informational event types).

5.1.1.5 Selective Audit (FAU_SEL.1)

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

a) [***event type***;]
b) [**no additional attributes**].[FAU_SEL.1.1]

Application note: The auditable event types are grouped into categories that can be enabled or disabled. The categories and corresponding auditable events are listed in Section 6.1.1 Security Audit.

5.1.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records **in the audit trail** from unauthorized deletion.[FAU_STG.2.1]

FAU_STG.2.2 The TSF shall be able to [***detect***] modifications to the audit records.[FAU_STG.2.2]

FAU_STG.2.3 The TSF shall ensure that [**most recent, up to 1 million records**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***]**.**[FAU_STG2.3]

5.1.1.7 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and **[send an alarm]**[7] if the audit trail is full**.**[FAU_STG.4.1]

Application note: Actions the TOE takes if the audit trail becomes full are defined in section 6.1.1.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when a settable, [**non-zero number of**] unsuccessful authentication attempts occur related to [**TOE users attempting to authenticate**]. [FIA_AFL.1.1]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**prevent the offending TOE users from successfully authenticating until an authorised administrator takes some action to make authentication possible for the TOE users in question**]. [FIA_AFL.1.2]

5.1.2.2 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;

[7] The PP indicates this operation as a selection, when in fact it is an assignment. The ST author has indicated the correct operation performed.

c) Authorisations;
d) Group; and
e) Alarm notification data].[FIA_ATD.1.1]

5.1.2.3 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.[FIA_UAU.2.1]

5.1.2.4 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.[FIA_UID.2.1]

5.1.3 Security Management (FMT)

5.1.3.1 Management of Security Functions Behavior (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 [**authorized administrator, authorized System administrators**].[FMT_MOF.1.1]

5.1.3.2 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query*** [**and add System data and audit data, and shall restrict the ability to query and modify all other TOE data**] to [**authorized administrator, authorized System administrators**].[FMT_MTD.1.1]

5.1.3.3 Specification of Management Functions (FMT_SMF.1)

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

a.) **Add/Delete general users – Add/remove general user accounts**
b.) **Assign/Remove general user permissions – Assign/remove permissions to/from general user accounts**
c.) **Add/Delete Devices - Add/remove NitroGuard devices to/from the system.**
d.) **Add/Delete Policies - Add/remove/rollback rule policies to/from the system.**
e.) **Custom Rules and Variables - Add, modify and delete custom rules, blacklist, and variables.**
f.) **Device Management - Configure settings and perform operations on NitroGuard and Receiver devices.**
g.) **ESM Configuration - Configure settings and perform operations on the ESM device.**
h.) **Event Management - Management of alert and flow data in addition to all rights of Reporting.**
i.) **Notifications - Add, modify and delete notifications and event forwarding destinations.**
j.) **Policy Administration - Manage policy settings for NitroGuard and Receiver devices.**
k.) **Reporting - Execute reports and retrieve alert, flow and log data from the NitroGuard and Receiver devices.**
l.) **System Management - Configure system wide security settings.**
m.) **View Management - Add, modify and delete views in addition to all rights of Reporting**
n.) **Network Port Control – Ability to reconfigure ports on network infrastructure devices (e.g. disable port)**
o.) **FIPS Self-Test – Ability to initiate a FIPS self-test on the ESM, NitroGuard and Receiver.**][FMT_SMF.1.1]

5.1.3.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the **following** roles [**authorized administrator, authorized System administrators, and** [**general users**]].[FMT_SMR.1.1]

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

Application note: The authorized administrator role corresponds to the single system administrator account that can be used to create general user accounts. The authorized System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

5.1.4 Protection of the TOE Security Functions (FPT)

5.1.4.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.[FPT_ITT.1.1]

5.1.4.2 Reliable time stamps (FPT_STM.1)

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

5.1.5 IDS Component requirements (IDS)

5.1.5.1 Analyzer analysis (EXT) (IDS_ANL.1)

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

a) [***signature***]; and

b) [**the following additional traffic analysis techniques:**

- **Protocol anomaly analysis**
- **Behavioral anomaly analysis**
- **Stateful protocol analysis**]. (EXT) [IDS_ANL.1.1]

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) [**no additional information about the result**]. (EXT)[IDS_ANL.1.2]

5.1.5.2 Analyzer react (EXT) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to [**one or more of the following alarm destinations:**

a) **Email**

b) **Syslog**

c) **SNMP**]

and take [**one or more of the following actions:**

a) **Drop packet**

b) **Drop session**

c) **Log packet data**]

when an intrusion is detected. (EXT)[IDS_RCT.1.1]

5.1.5.3 Restricted Data Review (EXT) (IDS_RDR.1)

IDS_RDR.1.1 The System shall provide [**authorized administrator, authorized System administrators**] with the capability to read [**all System data**] from the System data. (EXT)[IDS_RDR.1.1]

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information. (EXT)[IDS_RDR.1.2]

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. (EXT)[IDS_RDR.1.3]

Application note: Permissions that may be assigned general users by system administrators such as Event Management and Reporting permissions that allow access to audit information are defined in section 6.1.2.

5.1.5.4 System Data Collection (EXT) (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) [***network traffic***]; and
b) [**no other defined events**]. (EXT)[IDS_SDC.1.1]

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 the following table, System Events. (EXT)[IDS_SDC.1.2]

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 3: System Events

5.1.5.5 Guarantee of System Data Availability (EXT) (IDS_STG.1)

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion. (EXT)[IDS_STG.1.1]

IDS_STG.1.2 The System shall protect the stored System data from modification. (EXT)[IDS_STG.1.2]

IDS_STG.1.3 The System shall ensure that [**most recent, up to 1 million records**] System data will be maintained when the following conditions occur: [***System data storage exhaustion***]. (EXT)[IDS_STG.1.3]

5.1.5.6 Prevention of System data loss (EXT) (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.[IDS_STG.2.1]

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL3 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. Note that the EAL3 requirements that exceed EAL 2 are indicated in italics in the following table. No operations are applied to the assurance components. The SARs have been changed, when necessary, to conform to International Interpretations.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Architectural Design with domain separation and non-bypassability
	ADV_FSP.3: Functional specification with complete summary
	ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	*ALC_CMC.3: Authorisation controls*
	ALC_CMS.3: Implementation representation CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
ATE: Tests	*ATE_COV.2: Analysis of coverage*
	ATE_DPT.1: Testing: basic design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4: EAL 3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 Functional specification with complete summary (ADV_FSP.3)

ADV_FSP.3.1d The developer shall provide a functional specification.

ADV_FSP.3.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.3.1c The functional specification shall completely represent the TSF.

ADV_FSP.3.2c The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.3.3c The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.3.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.3.5c For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.
ADV_FSP.3.6c The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.
ADV_FSP.3.7c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.3.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Architectural design (ADV_TDS.2)

ADV_TDS.2.1d The developer shall provide the design of the TOE.
ADV_TDS.2.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.2.1c The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.2.2c The design shall identify all subsystems of the TSF.
ADV_TDS.2.3c The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.
ADV_TDS.2.4c The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.5c The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.6c The design shall summarise the behaviour of the SFR-supporting subsystems.
ADV_TDS.2.7c The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.2.8c The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.
ADV_TDS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.2.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Authorisation controls (ALC_CMC.3)

ALC_CMC.3.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.3.2d The developer shall provide the CM documentation.
ALC_CMC.3.3d The developer shall use a CM system.
ALC_CMC.3.1c The TOE shall be labelled with its unique reference.
ALC_CMC.3.2c The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.3.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.3.4c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ALC_CMC.3.5c The CM documentation shall include a CM plan.
ALC_CMC.3.6c The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.3.7c The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.3.8c The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.
ALC_CMC.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Implementation representation CM coverage (ALC_CMS.3)

ALC_CMS.3.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.3.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.
ALC_CMS.3.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.3.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.

ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.2.3.5 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.6 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 Testing: basic design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.
ATE_DPT.1.2c The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.
AVA_VAN.2.1c The TOE shall be suitable for testing.
AVA_VAN.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

The IPS, Receiver and ESM subsystems each generate three types of logs. These logs are used to store audit records (in the event log) and to store collected data event information (in the traffic alert log and in the traffic flow log). The event log contains records not related to traffic alerts or traffic flow such as TOE management events. The event log is the TOE's log containing the audit trail.

- *event log*
  - Generated by ESM (when using GUI) and Receiver and NitroGuard (when receiving commands from ESM)
  - Records generated by Receiver and NitroGuard are sent to ESM periodically in batches for storage and review on ESM. The records are protected during transmission using the proprietary stackless control protocol called SEM (Secure Encrypted Management). The communication between the ESM and the NitroGuard and Receiver is always initiated by the ESM. The audit trail is protected by the ESM subsystem and is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.
  - Maximum event log size on NitroGuard, ESM, and Receiver is one million records on all supported NitroGuard, ESM, and Receiver appliance models

Note: Maximum log sizes are not configurable. Maximum log sizes depend on appliance model.

The audit records received by the ESM are stored in the ESM subsystem's event log. The ESM subsystem's event log is also known as the audit trail. The audit trail is protected by the ESM subsystem. The audit trail is protected from unauthorized logical access by restricting access to the ESM web-based GUI interface that is used to read from the audit trail. There are no interfaces (not ESM web-based GUI interfaces or otherwise) to modify audit records stored in the audit trail.

The ESM provides web-based GUI interfaces to configure auditable events. Events are grouped into categories that correspond to sets of ESM GUI dialogs, menus, and screens. Each category will have a checkbox that allows the user to enable/disable logging of each event category. If a category is disabled, no events that are a part of that category will be logged. The auditable event types include:

- Authentication category - Login, logout, and any user account changes
- Backup category - Database backup process
- Blacklist category - Sending blacklist entries to the device
- Device category - Any device changes or communications such as getting events, flows and logs
- Event Forwarding category - Event forwarding changes or errors
- Health Monitor category - Device status events
- Notifications category - Notification changes or errors
- Policy category - Policy management and applying policies
- Rule Server category - Download and validation of rules downloaded from the rule server
- System category - System setting changes and table rollover logging
- Views category - Changes to views and queries

In addition to the list of events above, it should be noted that audit is always on and hence the start-up and shutdown audit is fulfilled vacuously, however there is a system log that identifies the start and stop of various TOE components.

The ESM provides the only administrative interface to all audit events related to system management that occur on the ESM. The IPS and Receiver subsystems role in creating audit records is limited to responding to audit storage failure and other exception based audited activity.

The ESM web-based GUI interfaces that can be used to read from the event log allow for selecting events to display within an administrator-configurable time period. When event log records (i.e., audit records) are displayed after a time period has been selected, the following information is displayed for each record:

- time of the event
- user name
- status of the event (IPS and Receiver events only), which can be any one of:
  - critical
  - warning
  - informational
- location (i.e. IPS, Receiver or ESM identifier) of the event (is blank if ESM)
- description (details) of the event

When the event log reaches its maximum size, it begins overwriting the oldest stored records. There is an alarm mechanism to alert the administrator when the log runs out of space.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for the basic level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., System data).
- FAU_SAR.1: The TOE provides administrator console interfaces that can be used by authorized administrators and general users that possess permissions that allow access to read the audit trail.
- FAU_SAR.2: The TOE restricts access to the audit trail to authorized administrators and general users that possess permissions that allow access to read the audit trail using administrator console interfaces.
- FAU_SAR.3: The TOE provides administrator console interfaces that can be used to sort audit data. The administrator console interfaces that can be used to sort audit data do not include a separate type of event field. However, there is a "status" field provided by the administrator console that corresponds to NitroGuard and Receiver component status event types (which include critical, warning, and informational event types).
- FAU_SEL.1: The TOE provides administrator console interfaces that can be include or exclude auditable events based on event type. Note the event type is the audit categories.
- FAU_STG.2: The TOE restricts administrator console interfaces that can be used to delete audit data. The TOE provides administrator console interfaces that can be used to detect modifications (administrators can compare system activity reports based on audit data generated at different points in time).
- FAU_STG.4: The TOE generates an alarm using a configured mechanism (see section 6.1.5 for a description of notification mechanisms), and begins overwriting the oldest stored audit records when the audit trail becomes full. Note that the TOE does not stop collecting or producing System data.

6.1.2 Identification and Authentication

There is a single system administrator account that can be used to create what are called general user accounts. The system administrator may grant general users other privileges by creating access groups and assigning users to these groups. However, there are operations such as creating general user accounts that only the system administrator account can perform even if a general user were to be assigned all available privileges. Group membership and the permissions assigned to the group by the administrator determine what ESM web-based GUI interfaces a user may access. The ESM appliance stores user account information on the ESM appliance. User account information is

physically protected by the ESM appliance hardware and logically protected by the access control mechanism. User account information includes username, password, and group information. Note the terms permissions and privileges are synonymous with authorizations.

Assignable permissions include:

- Add/Delete Devices - Add/remove NitroGuard devices to/from the system.
- Add/Delete Policies - Add/remove/rollback rule policies to/from the system.
- Custom Rules and Variables - Add, modify and delete custom rules, blacklist, and variables.
- Device Management - Configure settings and perform operations on NitroGuard and Receiver devices.
- ESM Configuration - Configure settings and perform operations on the ESM device.
- Event Management - Management of alert and flow data in addition to all rights of Reporting.
- Notifications - Add, modify and delete notifications and event forwarding destinations.
- Policy Administration - Manage policy settings for NitroGuard and Receiver devices.
- Reporting - Execute reports and retrieve alert, flow and log data from the NitroGuard and Receiver devices.
- System Management - Configure system wide settings.
- View Management - Add, modify and delete views in addition to all rights of Reporting.
- Network Port Control – Ability to reconfigure ports on network infrastructure devices (e.g. disable port).
- FIPS Self-Test – Ability to initiate a FIPS self-test on the ESM, NitroGuard and Receiver.

When a user attempts to log into the ESM web-based GUI interface, a username and password are required. If the identification and authentication method specified is defined locally, the TOE will identify and authenticate the user provided the username and password matches the stored attributes. Alternately, if the TOE is configured to work with a RADIUS server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until the user has been successfully identified and authenticated.

The authorized administrator can set the Allowed Failed Login Attempts value specifies the number of consecutive unsuccessful logins that will be allowed in a single session before the user attempting to login has their account locked. Once a user has their account locked, the system administrator must unlock their account via the Users and Groups section, before that user will be allowed to login again. The default value is three (3).

The ESM web-based GUI interface provides interfaces for users to change their own passwords. The ESM appliance requires passwords to be at least eight characters from the printable character set. Passwords must also include at least one uppercase letter, at least one numeric digit (i.e. 0 thru 9), and at least one non-letter/non-digit (i.e. symbols and/or punctuation marks). The ESM appliance GUI enforces these password composition rules.

The NitroGuard and Receiver appliances cannot be accessed directly. Their system data collection interfaces are invoked upon receipt of monitored network traffic. The NitroGuard and Receiver appliances are managed using the ESM appliance, which can only be accessed after a user successfully logs into the ESM appliance using a username and password.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The TOE enforces the number of failed login attempts and locks the users account once that threshold has been reached.
- FIA_ATD.1: The TOE maintains user identities (user id), authentication data (passwords), authorization (permission/privileges), group information (group/role membership), and alert notification data (e-mail address for alert notification).
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security Management

The ESM appliance provides a GUI to administer the NitroGuard and Receiver appliances. Administrator console interfaces are provided for managing functions related to system data collection, analysis, and reaction as well as the data that is collected from the devices that are monitored by the Receiver. System data consists of results from

NitroGuard scanning, sensing and analyzing tasks, and Receiver active/passive network event acquisition, flow data information and data correlation. The administrator can use the default policies and rules or using the Policy Manager, the administrator can add new rules and policies, edit the rules and policies, import policies, delete policies, change the rule history, etc. For a complete list of functions and capabilities, see the NitroSecurity NitroView User Guide.

The administrator console can also be used to manage audit data and user accounts. Management functions correspond to the list of assignable permissions that can be found in section 6.1.2, and include the functions of creating and deleting general users accounts and assigning and removing permissions by the system administrator.

The TOE has three user accounts: authorized administrator, system administrators, and general user. The authorized administrator role corresponds to the single system administrator account that can be used to create general user accounts. The authorized System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the NitroGuard and Receiver appliances. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM appliance. If the TOE is configured in FIPS mode then all traffic between the ESM and NitroGuard/Receiver is tunneled through a FIPS certified VPN tunnel and the HTTPS uses a FIPS certified crypto function. The evaluated configuration supports both FIPS mode and non-FIPS mode.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE restricts the ability to modify the behavior of the functions of System data collection, analysis and reaction by restricting access to administrator console interfaces.
- FMT_MTD.1: The TOE restricts the ability to query and add System data and audit data to authorized administrators. Note that only authorized administrators can query or modify any other types of TOE data, as well.
- FMT_SMF.1: The TOE provides authorized administrators with the ability to manage functions and data related to scanning, sensing, and analyzing tasks, as well as the ability to manage audit data and user accounts.
- FMT_SMR.1: The authorized administrator role corresponds to the single system administrator account that can be used to create general user accounts. The authorized System administrator role corresponds to general user accounts that have been assigned one or more permissions by the authorized administrator. The general user role corresponds to general user accounts that have not been assigned any permissions by the authorized administrator.

6.1.4 Protection of the TSF

The TOE restricts access to its interfaces by requiring users to log into the ESM appliance using its GUI, and by encrypting commands sent from the ESM appliance to the NitroGuard and Receiver appliances. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM appliance. The ESM supports HTTP v1.1 using TLS v1.0. The TOE relies on NitroSecurity appliance hardware to ensure the TSP is enforced and to provide for domain separation. The TOE additionally encrypts communication between Console, Receiver, and IPS appliances using a proprietary stackless control protocol called SEM (Secure Encrypted Management), which uses encrypted commands packaged in packet payloads, together with a specific token in the payload that indicates the packet is a control packet. The communication between the ESM and the NitroGuard and Receiver is always initiated by the ESM. If the TOE is configured in FIPS mode, all the control protocol traffic is tunneled through a FIPS certified VPN tunnel connected between the Console and NitroGuard/Receiver device, and the HTTPS uses a FIPS certified crypto function. The evaluated configuration supports both FIPS mode and non-FIPS mode.

The following table summarizes the cryptographic security functions of FIPS mode.

Security Function	*Purpose or Use*	*Certificate*
Approved Security Functions		
AES (FIPS PUB 197) CBC(e/d; 128)	TLS and SSH encryption and decryption.	668
Triple-DES (FIPS PUB 46.3)	Support for ANSI X9.31 PRNG	613
SHA-1 (FIPS PUB 180-2) (BYTE-only)	TLS and SSH signature verification, data integrity	701
HMAC-SHA1	Data integrity and data authentication within SSH	352 (HMAC), 701 (SHS)
RNG (ANSI X9.31 PRNG, Appendix A.2.4)	Key generation	387
RSA (FIPS PUB 186-2) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048, SHS: SHA-1	TLS and SSH key transport, signature verification	310
Allowed Security Functions		
Diffie Hellman (key agreement and key establishment methodology provides a minimum of 80 bits of encryption strength)	Key agreement within SSH	Vendor Affirmed

Security Function	*Purpose or Use*	*Certificate*
Approved Security Functions		
AES (FIPS PUB 197) CBC(e/d; 128)	TLS and SSH encryption and decryption.	668
Triple-DES (FIPS PUB 46.3)	Support for ANSI X9.31 PRNG	613
SHA-1 (FIPS PUB 180-2) (BYTE-only)	TLS and SSH signature verification, data integrity	701
HMAC-SHA1	Data integrity and data authentication within SSH	352 (HMAC), 701 (SHS)
RNG (ANSI X9.31 PRNG, Appendix A.2.4)	Key generation	387
RSA (FIPS PUB 186-2) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048, SHS: SHA-1	TLS and SSH key transport, signature verification	310
Allowed Security Functions		

Security Function	*Purpose or Use*	*Certificate*
Diffie Hellman (key agreement and key establishment methodology provides a minimum of 80 bits of encryption strength)	Key agreement within SSH	Vendor Affirmed

Before the TOE is installed and configured, the NitroGuard and ESM and the Receiver and ESM appliances are preconfigured with different types of cryptographic keys for use with SEM and with HTTPS. During TOE installation and configuration, the keys are replaced with newly generated ones. During TOE installation and initial configuration, NitroGuard keys on both NitroGuard and ESM appliances are replaced with newly generated keys as are the Receiver and the ESM. The SSL keys and certificate are also replaced with newly generated keys and certificate during TOE installation and initial configuration. The evaluated configuration supports both FIPS mode and non-FIPS mode. When the TOE is operated in non FIPS-mode, the cryptographic support is vendor affirmed.

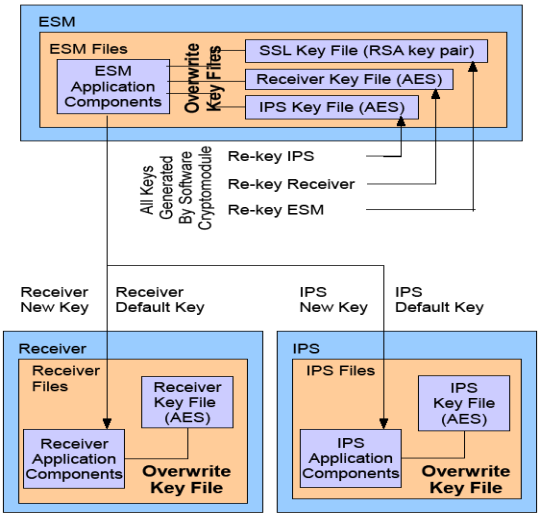

Figure 4: NitroGuard, Receiver, and ESM Keying

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TOE encrypts commands sent from the ESM appliance to the NitroGuard and Receiver appliances. HTTPS is also used to protect the connection between the web browser in the operational environment and the ESM appliance.
- FPT_STM.1: The hardware for each subsystem includes its own hardware clock that provides reliable time stamps for use in audit and collected data records generated by that subsystem. The clock in the IPS subsystem and the Receiver subsystem can only be set by a command from the ESM. The clock in the ESM subsystem can be set by an administrator using the GUI or by an NTP server configured by the administrator.

6.1.5 Intrusion detection (EXT)

NitroGuard is an Open System Interconnection (OSI) Layer 2 device and can be configured without an IP address, if the TOE is not in FIPS mode. Without an IP address, the device will not respond to pings, traceroutes, or any other high-level mechanics, nor will it respond to ARP requests or any other low-level mechanics.

The Receiver can sit anywhere within the network architecture. The only constraint is that Receiver data sources must be able to 1) send data to the Receiver, or 2) be accessed by the Receiver. For security reasons, it makes most sense to put the Receiver in the "most secure" part of the network that meets the two constraints mentioned above. The Receiver has a correlation engine that enables the Receive to correlate the network, log, and event data from any source. The Receiver collects data from virtually any third party device, such as firewalls, VPNs, routers, IPS/IDS, NetFlow, sFlow and others. This provides data acquisition functions across multiple vendors' devices, such as Cisco, Checkpoint and Juniper firewalls, NitroSecurity and McAfee IPS devices, and Cisco and Foundry routers.

The TOE can be installed in the following locations in the network architecture of the operational environment:

- *Outside the firewall location* – The TOE is placed between the external interface of the firewall and the border router.
- *DMZ location* – The TOE is placed between the DMZ interface on the firewall and whatever network exists as part of the DMZ.
- *VPN concentrator in DMZ location* – The TOE is placed between the internal interface of the concentrator and the internal switch into which it feeds. This is the only way to examine unencrypted traffic of VPN users on networks set up in this manner.
- *Inside the firewall location* – The TOE is placed between the internal interface of the firewall and the internal switch into which it feeds.
- *IDS Mode location* – The TOE is placed on a mirrored port in any network location.

NitroGuard can detect different types of intrusion attempts by performing analysis of network traffic packets depending on location within a network. The TOE supports installation in different locations in the network architecture of the TOE environment by providing the ability to operate in one of three modes:

- IPS mode (supported when the TOE is located *in-line*)
- Alerts-only mode (supported when the TOE is located *in-line*)
- IDS mode (supported when the TOE is located *in-tap*)

When NitroGuard is located in-line it can operate in what is called an *IPS mode*. IPS mode consists of the device being located in-line while functioning as an IPS, i.e. the device can drop, pass, reject network traffic according to policy. NitroGuard is placed inline between two devices (i.e., a firewall and a switch) using network cables. All traffic that enters NitroGuard through its physical network interfaces is picked up by iptables for firewall policy rule inspection. The firewall policy rules are checked in order of resulting action in the following order: pass, reject, drop, and alert. If the packet was not passed, rejected, or dropped, it is passed to Snort for deep packet inspection (i.e. payload). The Snort rules are checked in the same order as the firewall rules: pass, reject, drop, and alert.

As for the Receiver, it does have iptables running on it as its firewall, but no deep packet inspection is done on the Receiver. The Receivers' iptables instance is used simply to limit the flow of packets into the Receiver to those packets of interest to the Receiver (e.g. If the Receiver is supposed to accept syslog packets from IP address 1.2.3.4, then iptables will be configured to allow syslog packets in from 1.2.3.4).

When NitroGuard is located in-line it can operate in what is called an *alerts-only mode*. Alerts-only operating mode consists of NitroGuard being located in-line while functioning as an IDS, i.e. the device can monitor network traffic but not affect it. NitroGuard is placed inline between two devices (i.e., a firewall and a switch) using network cables. All traffic that enters NitroGuard through its physical network interfaces is picked up by iptables for firewall policy rule inspection. The firewall rules are checked in order of resulting action in the following order: pass, reject, drop, and alert. However, in alerts-only mode, pass, reject, and drop actions for each rule are replaced with the alert action. The packet is then always passed to Snort for deep packet inspection. The Snort rules are checked in the same order as the firewall policy rules: pass, reject, drop, alert. However, as with firewall policy rules, in alerts-only mode, the deep packet inspection policy check rule actions are replaced with the alert action and the packet is always passed thru.

When NitroGuard is located in-tap it can operate in what is called an *IDS mode*. IDS mode (also called passive operating mode) consists of the device being located in-tap while functioning as an IDS, i.e. the TOE can monitor network traffic but not affect it. NitroGuard is placed on a span port of a switch using a network cable. Any traffic that enters the switch is passed through the span port, as well as the actual output port. All traffic that enters

NitroGuard through the physical network interface is picked up by iptables for firewall rule inspection. Because the device is not inline, no action other than alert can be taken. After firewall policy rules are checked, the packets are passed on to Snort for checking against the deep packet inspection policy rules.

NitroGuard performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes. The TOE retrieves authenticated and encrypted signature updates from the NitroSecurity central server via an encrypted communication mechanism. Mechanisms, both hardware and software based, are in place to ensure that devices are managed only from properly authorized NitroViews

- *Signature analysis* of network traffic packets consists of identifying deviations from normal patterns of behavior using patterns corresponding to known attacks or misuses, e.g. comparing user activity against a database of known attacks
- *Protocol anomaly analysis* of network traffic packets filters each packet to identify deviations from normal patterns of behavior
- *Behavioral anomaly analysis* of network traffic packets consists of identifying deviations from normal patterns of behavior using tracking of all packet statistics including burst rates, bytes and packets per second, threshold limit alerts, source and destination IP addresses and ports, and protocols
- *Stateful protocol analysis* and what is called connection tracking of network traffic packets consists of identifying deviations from normal patterns of behavior by monitoring and analyzing all packets within a connection or session

The TOE's ESM administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion. The NitroGuard, Receiver, and ESM appliances generate three types of logs to store collected data event information:

- *traffic alert log* – these are events that occur when packets match a rule, i.e. this is collected data
  - Records generated by NitroGuard and Receiver are sent to ESM periodically in batches for storage on ESM.
  - Maximum log size on NitroGuard, Receiver, and ESM depends on appliance model:
    - Maximum traffic alert log size on all supported NitroGuard and Receiver models is ten million records
    - Maximum traffic alert log size on supported ESM models depends on model, ranging from 250 million to 750 million records.
- *traffic flow log* – these are events that occur when connections are made between targeted IT systems in general (i.e. a flow is not associated with an IDS rule), i.e. this is collected data
  - Records generated by NitroGuard and Receiver are sent to ESM periodically in batches for storage on ESM
  - Maximum log size on NitroGuard, Receiver, and ESM depends on appliance model:
    - Maximum traffic flow log size on all supported IPS and Receiver models is ten million records
    - Maximum traffic flow log size on supported ESM models depends on model, ranging from 250 million to 750 million records.
- *device location log* – this data is associated with the location of network infrastructure and end-station devices automatically discovered by, and manually entered into, the ESM
  - There's no practical maximum log size
  - All location data is stored
  - Maximum log size on ESM depends on appliance model:
    - Maximum device location log size on all supported ESM models is ten million records
    - Maximum device location log size on supported ESM models depends on model, ranging from 250 million to 750 million records.

Note: Maximum log sizes are not configurable. Maximum log sizes depend on appliance model.

The NitroGuard and Receiver devices receive requests for alerts and flows from the ESM containing the date of the last retrieval. All requested data since the date passed are retrieved and passed back to the ESM. NitroGuard and Receiver can also be configured to automatically send out Syslog messages and SNMP traps when an alert is triggered. NitroGuard and Receiver devices receive configuration data for Syslog servers and SNMP managers from the ESM, including an alert rate. This data is used for sending Syslog messages and SNMP traps whenever an alert is logged, not to exceed the specified rate. The ESM can generate email SNMP traps, syslog, and text log files. To setup the notifications, the user must be assigned to the System administrator role. The user can configure the conditions/events that will cause a notification to be generated. Conditions or events can include, specified event rate, specified date/time, FIPS compliance failure, device failure, etc. When sending notifications via e-mail, SNMP or syslog, a recipient must be identified. For e-mail, the e-mail address of the person or group that will receive the e-mail must be entered. Recipients can be added or removed as necessary. SNMP uses User Datagram Protocol (UDP) as the transport protocol. It should be noted that due to size limitations of the SNMP trap packets, each line of the notification report is sent in a separate trap. Syslog uses the standard for forwarding log messages in an IP network. Notifications can also be appended to a text file that is stored on the ESM. The information contained in a notification can consist of the results of any query for any combination of devices over any desired time range. The alarm mechanisms used when reacting to collected data may also be used when reacting to audit mechanism events, if the TOE has been configured to do so.

When either of the logs reaches their respective maximum size, they begin overwriting the oldest stored records. There is an alarm mechanism to alert the administrator when the logs run out of space.

The IDS function is designed to satisfy the following security functional requirements:

- IDS_SDC.1: The TOE collects network traffic data for use in scanning, sensing, and analyzing functions, acting as an IDS sensor. Note that different types of network traffic can be collected depending on the TOE's location within a network. Also, note that host-based events may be collected for network switches.
- IDS_ANL.1: The TOE performs signature analysis, protocol anomaly analysis, behavioral anomaly analysis, and stateful protocol analysis on collected network traffic data and records corresponding network traffic event data when operating in any one of its operating modes. . Note that the administrator console provides the ability to examine analytical conclusions drawn by the TOE that describe the conclusion and identifies the information used to reach the conclusion.
- IDS_RCT.1: The TOE provides the ability to generate alert and notify an authorized administrator using a configured notification mechanism when an intrusion is detected. The TOE also provides the ability to automatically pass or reject packets (and connections) based on rule configuration when an intrusion is detected.
- IDS_RDR.1: The TOE provides authorized administrators and general users that possess permissions that allow access the ability to review results from IDS scanning, sensing, and analyzing tasks (i.e., System data) using the administrator console.
- IDS_STG.1: The TOE ensures that the most recent system data is always able to be recorded, when the system data storage space is exhausted, the oldest events stored in the system data store will be overwritten.
- IDS_STG.2: The TOE prevents loss in new/current event data by overwriting the oldest events stored in the log when the system data storage capacity is exhausted. When this occurs, an alarm is generated and sent to the authorized administrator using a configured notification mechanism.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007. In addition, NitroSecurity has elected to pursue a more vigorous assurance level as depicted in Section 1.2, Conformance Claims.

Section 1.3 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007 states "…STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance…". This ST is a suitable solution to the generic security problem described in the PP. Following are the changes to the PP defined security problem definition, security objectives, and security requirements. All changes in the ST are equivalent to or more restrictive than stated in the PP.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim, except as noted below.

> The assumption, A.EAUTH was added to support external authentication services via a RADIUS server. The assumption is mapped to the corresponding security objective, OE.EAUTH.
>
> The assumption, A.COMPROT was added to support the protection of transmitted TSF data between the TOE and external entities, such as the RADIUS server and NitroSecurity for signature updates.

This Security Target includes all of the Security Objectives from the PP, verbatim, except as noted below.

> The security objective, OE.EAUTH was added to support external authentication services via a RADIUS server. The security objective is mapped to the corresponding assumption, A.EAUTH.
>
> The security objective, OE.COMPROT was added to support the protection of transmitted TSF data between the TOE and external entities, such as the RADIUS server and NitroSecurity for signature updates. The security objective is mapped to the corresponding assumption, A.COMPROT.

This Security Target includes all of the Security Objectives for the Environment from the PP, verbatim, except as noted below.

> The operational environment security objectives OE.AUDIT_PROTECTION and OE.AUDIT_SORT are not applicable to the environment for this TOE and were removed from the ST. The security objectives for the TOE provide the ability to sort the audit logs and provide protection of the audit trail.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP verbatim, except as noted below.

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FAU_GEN.1	Refined to be compliant with CC v3.1, Revision 2.
FAU_SAR.1	*Assignment* – completed the assignment.
FAU_SAR.2	No changes.
FAU_SAR.3	Refined to be compliant with CC v3.1, Revision 2.
FAU_SEL.1	Refined to be compliant with CC v3.1, Revision 2.
FAU_STG.2	*Selection* – completed the selection. *Assignment* – completed the assignment. Refined to be compliant with CC v3.1, Revision 2.
FAU_STG.4	*Selection* – completed the selection. *Assignment* – completed the assignment. In addition, the PP indicates this operation as a selection, when in fact the operation is an assignment. The ST author has indicated the correct operation performed.

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FIA_ATD.1	*Assignment* – completed the assignment.
FIA_UAU.1	*Replaced* – the requirement was removed from the ST and replaced with FIA_UAU.2 given no mediated functions are otherwise available.
FIA_UID.1	*Replaced* – the requirement was removed from the ST and replaced with FIA_UID.2 given no mediated functions are otherwise available.
FMT_MOF.1	No changes.
FMT_MTD.1	*Assignment* – completed the assignment.
FMT_SMF.1	Added - this requirement was added in this Security Target to satisfy a dependency to FMT_MOF.1 and FMT_MTD.1. This requirement was originally included by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included in CC v3.1. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
FMT_SMR.1	*Assignment* – completed the assignment.
FPT_ITA.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable.
FPT_ITC.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable.
FPT_ITI.1	*Removed* – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable.
FPT_ITT.1	Added – Since the TOE does not does not communicate with IDS components outside of the IDS system TOE the FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 SFRs were removed. The requirement, FPT_ITT.1 was added to protect inter-communications between the distributed TOE components. *Selection* – completed the selection.
FPT_STM.1	No changes
IDS_ANL.1	*Selection* – completed the selection. *Assignment* – completed the assignment.
IDS_RCT.1	*Assignment* – completed the assignment.
IDS_RDR.1	*Assignment* – completed the assignment.
IDS_SDC.1	*Selection* – completed the selection. *Assignment* – completed the assignment.
IDS_STG.1	*Selection* – completed the selection *Assignment* – completed the assignment.
IDS_STG.2	*Selection* – completed the selection.
EAL3	Added – the PP requires only EAL2. However, to satisfy the assurance requirements of environment requiring more assurance that the security functions are enforced, this Security Target has adopted the EAL3 security assurance requirements.

Table 5: Modification of Security Functional and Security Assurance Requirements

8. Rationale

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- Extended Requirements;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007.

This Security Target includes all of the Security Objectives from the PP, verbatim, except as noted below.

> The security objective, OE.EAUTH was added to support external authentication services via a RADIUS server. The security objective is mapped to the corresponding assumption, A.EAUTH.
>
> The security objective, OE.COMPROT was added to support the protection of transmitted TSF data between the TOE and external entities, such as the RADIUS server and NitroSecurity for signature updates. The security objective is mapped to the corresponding assumption, A.COMPROT.

This Security Target includes all of the Security Objectives for the Environment from the PP, verbatim, except as noted below.

> The operational environment security objectives OE.AUDIT_PROTECTION and OE.AUDIT_SORT are not applicable to the environment for this TOE and were removed from the ST. The security objectives for the TOE provide the ability to sort the audit logs and provide protection of the audit trail.

The security objective rationale is presented in Section 6.1 and Section 6.2 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

8.2 Security Requirements Rationale

The security requirements rationale is presented in Section 6.3 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

All of the security functional requirements have been reproduced from the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments to this ST, except as noted below:

The following security functional requirements were added to the ST:

- FIA_UAU.2: this requirement was included to replace FIA_UAU.1 since no mediated functions are available prior to login.
- FIA_UID.2: this requirement was included to replace FIA_UID.1 since no mediated functions are available prior to login.

- FMT_SMF.1: this requirement was added to satisfy a dependency to FMT_MOF.1 and FMT_MTD.1. This requirement was originally included by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included in CC v3.1. FMT_SMF.1 requires that a defined set of security management functions are made available so that an administrator can effectively manage the security configuration of the TOE. This security functional requirement provides direct support for the O.EADMIN security objective.
- FPT_ITT.1: Since the TOE does not does not communicate with IDS components outside of the IDS system TOE, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 SFRs were removed. The requirement, FPT_ITT.1 was added to protect inter-communications between the distributed TOE components. This change is based on PD 0097..

The following security functional requirements were removed from the ST:

- FIA_UAU.1: this requirement was removed and replaced by FIA_UAU.2 since there are no mediated functions available prior to login.
- FIA_UID.1: this requirement was removed and replaced by FIA_UID.2 since there are no mediated functions available prior to login.
- FPT_ITA.1: this requirement is intended to specify how audit and system data are made available to external (trusted) IT products that would provide audit and system data services. Since the TOE provides these functions internally, no external IT products are necessary. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. This change is based on PD 0097.
- FPT_ITC.1: this requirement is intended to specify how TSF data is protected while transmitted to external (trusted) IT products. Since the TOE provides all functionality for the System in a self-contained manner, no data is transferred to external products. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. This change is based on PD 0097..
- FPT_ITI.1: this requirement is intended to specify how modifications to TSF data can be detected when it is transmitted to external (trusted) IT products. This includes both integrity checks and detection of modification during transmission. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. This change is based on PD 0097.

Removal of these requirements does not have any impact on other security functional requirements.

The additional SFRs map to existing objectives as follows:

- FMT_SMF.1: Maps to O.EADMIN to summarize provided admin functions.
- FPT_ITT.1: Maps to O.EXPORT to protect communication between TOE components

8.3 Security Assurance Requirements Rationale

NitroSecurity has elected to pursue a more rigorous assurance level, increased from EAL2 augmented with ALC_FLR.2 as specified in U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments to EAL3 augmented with ALC_FLR.2, as specified in section 1.2 of this ST. EAL3 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. In addition, augmentation was chosen to provide the added assurances that result from having flaw remediation procedures and correcting security flaws as they are reported.

The NitroSecurity TOE meets all the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments functional and assurance requirements as so stated for EAL2. Additionally, the

TOE conforms to all the assurance requirements for an EAL3 product. The resulting assurance level is therefore, EAL3 augmented with ALC_FLR.2.

The EAL3 requirements that exceed EAL2 by the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments are rationalized below:

- ADV Development; ADV_FSP.3 Functional specification with complete summary
  - It is important to document the SFR-supporting and SFR-non-interfacing actions and error messages to demonstrate they are not SFR-enforcing.
- ADV Development; ADV_TDS.2 Architectural design
  - It is important to provide sufficient information to determine the TSF boundary and to describe how the TSF implements the security functional requirements.
- ALC Life-cycle support; ALC_CMC.3 Authorisation controls
  - It is important to demonstrate the CM operates in accordance with the CM Plan.
- ALC Life-cycle support; ALC_CMS.3 Implementation representation CM coverage
  - It is important to demonstrate that the parts that comprise the TOE that are under CM control are in fact modified in a controlled manner with proper authorization.
- ALC Life-cycle support; ALC_DVS.1 Identification of security measures
  - It is important to demonstrate the physical security of the development facility as well as personnel, procedural, and other security measures as deemed appropriate.
- ALC Life-cycle support; ALC_LCD.1 Developer defined life-cycle model
  - It is important to demonstrate the controlled development and maintenance of the TOE.
- ATE Tests; ATE_COV.2 Analysis of coverage
  - It is important to demonstrate the TSF has been tested against the functional specification and that the test documentation corresponds to all the TSFIs in the functional specification.
- ATE Tests; ATE_DPT.1 Testing basic design
  - It is important to demonstrate the TSF subsystems behave and interact as described in the architectural description.

8.4 Requirement Dependency Rationale

The dependency requirements rationale is presented in Section 6.7 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This Security Target includes two Security Functional Requirements not included in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments; FMT_SMF.1, and FPT_ITT.1. The requirement, FMT_SMF.1 was included to satisfy a dependency of FMT_MOF.1 and FMT_MTD.1 introduced in by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included CC v3.1. The SFR introduces no additional dependencies itself. The requirement, FPT_ITT.1 was included to support inter-communications in lieu of FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. The requirement FPT_ITT.1 does not introduce any dependency requirements.

8.5 Extended Requirements Rationale

There are no extended requirements beyond those in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

The extended requirements rationale is presented in Section 6.5 of the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The table below demonstrates the relationship between security requirements and security functions.

	Security Audit	Identification and Authentication	Security Management	Protection of the TOE Security Functions	IDS COMPONENT REQUIREMENTS (IDS)
FAU_GEN.1	**x**				
FAU_SAR.1	**x**				
FAU_SAR.2	**x**				
FAU_SAR.3	**x**				
FAU_SEL.1	**x**				
FAU_STG.2	**x**				
FAU_STG.4	**x**				
FIA_AFL.1		**x**			
FIA_ATD.1		**x**			
FIA_UAU.2		**x**			
FIA_UID.2		**x**			
FMT_MOF.1			**x**		
FMT_MTD.1			**x**		
FMT_SMF.1			**x**		
FMT_SMR.1			**x**		
FPT_STM.1				**x**	
IDS_ANL.1					**x**
IDS_RCT.1					**x**
IDS_RDR.1					**x**
IDS_SDC.1					**x**
IDS_STG.1					**x**
IDS_STG.2					**x**

Table 6: Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See Section 7, Protection Profile Claims.