National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

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

NitroSecurity Intrusion Prevention System 8.0.0

Report Number: CCEVS-VR-VID10312-2009

Dated: 27 October 2009

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Daniel P. Faigin, CISSP
The Aerospace Corporation
El Segundo, California

Jerome F. Myers
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Shukrat Abbas
Katie Sykes
Quang Trinh

Science Applications International Corporation
Columbia, Maryland

This report contains material that was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report are extracted from the NitroSecurity Intrusion Prevention System 8.0.0 Security Target.

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

The evaluation of NitroSecurity Intrusion Prevention System (IPS) version 8.0.0 was performed by Science Applications International Corporation (SAIC) in the United States and was completed in October 2009. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the NitroSecurity Target of Evaluation (TOE) was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2 and International Interpretations effective on 21 April 2008. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2. The TOE claims and meets conformance to the Intrusion Detection System System Protection Profile, Version 1.7, July 25, 2007 (IDSSPP).

SAIC determined that the evaluation assurance level (EAL) for the product is EAL 3 augmented with ALC_FLR.2 assurance requirements. The product, when configured as specified in the installation and user guides, satisfies all of the security functional requirements stated in the NitroSecurity Intrusion Prevention System Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the NitroSecurity Intrusion Prevention System product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

The evaluated configuration supports both Federal Information Process Standard (FIPS) mode and non-FIPS mode of encryption. If the TOE is configured in FIPS mode, all the control protocol traffic is tunneled through a FIPS 140-2 certified Virtual Private Network (VPN) tunnel connected between distributed components of the TOE, and the HTTP traffic over SSL (HTTPS) uses a FIPS 140-2-certified crypto function. In non-FIPS mode, the cryptography used has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. In non-FIPS mode, cryptography has only been asserted as tested by the vendor.

The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) for NitroSecurity Intrusion Prevention System Parts 1 and 2 produced by SAIC.

1 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	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, 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-

Item	Identifier
	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
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.7, July 25, 2007 (IDSSPP)
ST:	NitroSecurity Intrusion Prevention System version 8.0.0, Version 1.0, October 13, 2009
Evaluation Technical Report	Evaluation Technical Report For NitroSecurity Intrusion Prevention System version 8.0.0 (Proprietary), Version 1.0, October 13, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	NitroSecurity, Inc
Developer	NitroSecurity, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, Maryland
CCEVS Validators	Daniel P. Faigin, The Aerospace Corporation, El Segundo, California Jerome F. Myers, The Aerospace Corporation, Columbia, Maryland

2 SECURITY POLICY

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 ESMs, one or more NitroGuards, and one or more Receivers.

This section identifies the security functions that the TSF provides:

- **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.

- **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 ESM appliance 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.

- **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 can is also be used to manage audit data and users 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.

- **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 TOE Security Policy (TSP) is enforced and to provide for domain separation. In Non-FIPS mode, the cryptography used has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards; rather, it has only been asserted as tested by the vendor.

- **Intrusion detection**. The NitroSecurity Intrusion Prevention System 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 different types of IDS and IPS/alerts-only modes.

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

3.1 Assumptions

The following assumptions were made during the evaluation of NitroSecurity Intrusion Prevention System version 8.0.0:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can be accessed only by authorized users.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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

- External authentication services will be available via RADIUS server

3.2 Operating Environment

The TOE consists of the following components:

- NitroSecurity IPS 8.0.0 running on any of the supported appliance models as identified in Section 1
- NitroSecurity ESM 8.0.0 running on any of the supported appliance models as identified in Section 1.
- NitroSecurity NitroView Receiver 8.0.0 running on any of the supported appliance models as identified in Section 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 and from the NitroSecurity website, www.nitrosecurity.com.

The intended operational environment of the TOE contains 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 graphical user interface (GUI) interfaces. Note, for FIPS mode only, the supported Web browsers are Microsoft Internet Explorer 7 or higher and Firefox 1.5.0.4 or later.
- *Adobe Flash Player v9.0.124.0 or later.* A web browser plug-in that is required to access the ESM.
- *NTP server.* Network Time Protocol server that is used to set the ESM system clock.
- *RADIUS server.* An external Remote Authentication Dial In User Service (RADIUS) server used to support external authentication services.
- *SMTP server.* An external server used to receive email alerts generated by the TOE.
- *SNMP server.* An external server used to receive Simple Network Management Protocol (SNMP) alerts generated by the TOE.
- *Syslog servers.* An external server used to receive log message alerts generated by the TOE.
- *Certificate authority server.* An external server that provides digital certificates to support the web-based GUI.

- *DNS Server.* An external server used to govern the DNS records and implement the name-service protocol.

3.3 Clarification of Scope

Users of this product must be clear that the following product features were 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"
- **Third-party Smart Dashboard**. This is Check Point's management system that can be used to manage various devices within an organization's network.
- **Third-party Snort Barnyard**. This 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.

Additionally, although the TOE provides a Network Discovery function, the correct operation of this function was not considered security relevant from the point of view of this TOE, and was not covered by the evaluation.

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

The NitroSecurity Users Manual discusses reports meeting compliance aspects of BASEL II, FISMA, HIPAA, and other laws. Note that compliance of reports to legal or governmental standards was not a covered evaluation claim.

Public material on this product makes a number of claims related to availability that are not covered by the evaluation, such as claims related to high throughput, a high number of concurrent sessions, and reliability.

The evaluation did not assess the quality of the pre-supplied rule definitions with respect to adequacy to task.

Although the product provides a command-line interface (CLI), this interface is not considered security relevant. These commands are to be used in a maintenance mode and only under the direction of NitroSecurity Support personnel for emergency situations. CLI command usage is restricted to the Administrator and the CLI commands are not used for any management required by the ST.

4 ARCHITECTURAL INFORMATION

Note: The following architectural description is based on the description presented in the Security Target.

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[1] 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 Figure 1, below.

[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.

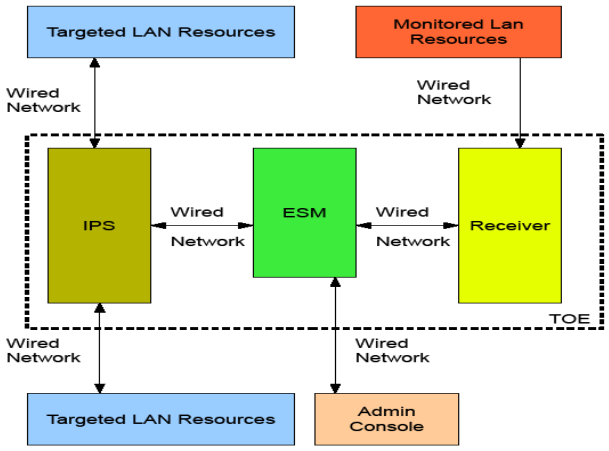

Figure 1. In-line network location of NitroGuard, a Receiver, and ESM

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 Figure 2, below:

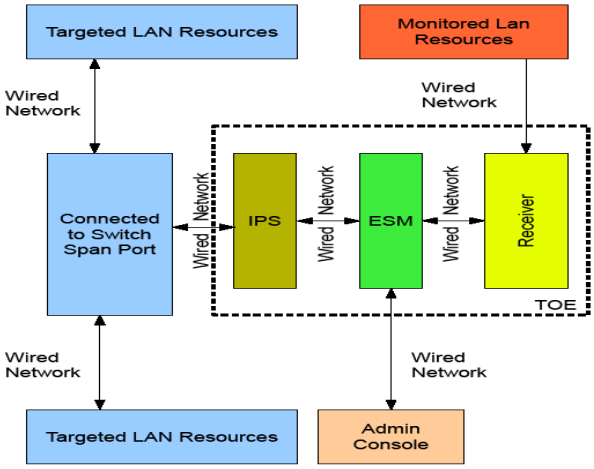

Figure 2. In-tap network location of NitroGuard, a Receiver, and ESM

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.

It is important to be clear that the TOE is not a firewall; rather, it is an IPS that includes a firewall module and it is that module through which all network traffic passes. The TOE's NitroGuard device 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. The IPS supports the following three rule types:

- *Firewall Policy rules.* The IPS tests against these rules when a packet is examined. These rules correspond to those typically enforced by iptables (a common Linux packet-filtering module—e.g., 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.* These 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.* These 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, 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 protocol stack order, from the data-link layer up through the transport layer, finally ending at the application layer.

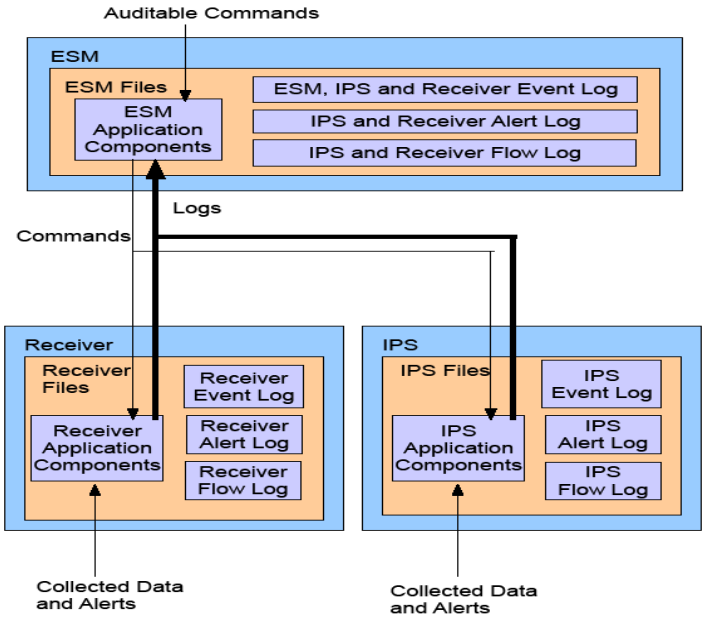

Figure 3. Command and log flow within an ESM, Receiver, and NitroGuard deployment

When a NitroGuard device is in either an in-line or an in-tap network location, a network packet enters through one of the device's physical network interfaces. 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 (this occurs because 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 generate 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 packet's content, running on the NitroGuard device. If a match is found, Snort has a custom plug-in that 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 NitroView Receiver, it also has netfilter/iptables running on it as its firewall, but this firewall does not generate alerts[2]. The Receiver's netfilter/iptables instance is used to (a) 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); (b) detect and drop control channel packets; and (c) 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 product's bypass feature, which allows all traffic to pass through the device (even malicious traffic).

The TOE consists 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. The NitroGuard consists of the NitroSecurity hardware appliance and the NitroSecurity software (which includes a modified Linux operating system together with 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. The ESM consists of the NitroSecurity hardware appliance and NitroSecurity software (which includes a modified Linux operating system and 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

[2] 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.

acquires data. Additionally, the Receiver has a "correlation engine" running on it that actively analyzes data sent from the NitroSecurity ESM, which originated on NitroGuard devices and this or other Receivers, looking for interesting patterns. The Receiver consists of the NitroSecurity hardware appliance and the NitroSecurity software (which includes a modified Linux operating system and User- and Kernel-mode components that perform data acquisition and correlation functions).

All three components include a modified version of the Linux operating system that 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 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 140-2 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 ability to use these commands is restricted to the Administrator and they are not used for any management required by the ST.

5 DOCUMENTATION

The following documentation was used as evidence for the evaluation of the TOE. Documents that are publically available are shown in **boldface.** All **boldface** documents are delivered with the product with the exception of the Security Target.

5.1 Design Documentation

Document	Revision	Date
NitroSecurity™ (NitroGuard™ IPS, NitroView™ ESM, NitroView™ Receiver, NitroView™ ESM/Receiver Combo) User Guide, Release 8.0. Part № NS-75602001800.	No Version Number	© 2008
NitroSecurity Installation and Setup Guide: NitroGuard™ IPS, NitroView™ ESM, NitroView™ Receiver, and NitroView™ ESM/Receiver Combo. Document № NS-75602002800.	No Version Number	© 2008
NitroSecurity 8.0.0 Design	13	2009-10-13
NitroSecurity Intrusion Prevention System 8.0.0 Security Target	1.0	2009-10-13

5.2 Guidance Documentation

Document	Revision	Date
NitroSecurity™ (NitroGuard™ IPS, NitroView™ ESM, NitroView™ Receiver, NitroView™ ESM/Receiver Combo) User Guide, Release 8.0. Part № NS-75602001800.	No Version Number	© 2008
NitroSecurity Installation and Setup Guide: NitroGuard™ IPS, NitroView™ ESM, NitroView™ Receiver, and NitroView™ ESM/Receiver Combo. Document № NS-75602002800.	No Version Number	© 2008
NitroSecurity Quick Start Guide	No Version Number	No Date

5.3 Life Cycle

Document	Revision	Date
Nitrosecurity Intrusion Prevention System Version 8.0.0 Configuration Management Plan	No Version Number	2008-03-17
Nitrosecurity Intrusion Prevention System Version 8.0.0 Delivery Procedures	No Version Number	2008-03-17
NitroSecurity 8.0.0 Life Cycle Document	4	2008-04-22
NitroSecurity Inc., Flaw Remediation Procedures	0.1	2008-08-01

5.4 Testing

Document	Revision	Date
NitroSecurity 8.0 Test Document	7	2009-09-30
Test Result Outputs: • Automated Test Suite Output.doc • Device Properties Test Suite Output.doc • Event Log Test Suite Output.doc • Policy Manager Test Suite Output.doc • System Properties Test Suite Output.doc • Test Output.pdf • User Authentication Test Suite Output.doc • Users and Groups Test Suite Output.doc • Views Test Suite Output.doc	TBS	TBS

5.5 Security Target

Document	Revision	Date
NitroSecurity Intrusion Prevention System 8.0.0 Security Target	1.0	2009-10-13

6 IT PRODUCT TESTING

6.1 Vendor Testing

NitroSecurity's approach to testing the TOE security functions consisted of a series of manual tests and automated tests. The test documents divided the test cases into a series of suites, which exercised the specific security functions and interfaces described in the User Guide and the design document. The test documentation described the testing environment, the test procedures (including the test steps for each test procedure, the order in which the tests should be performed) and the summarized the test coverage which mapped each test procedure to the security functional requirements. The test documents also provided the test results output. The analysis of the test coverage (documented in the ETR) showed that all the security functions outlined in the TSS section of the ST were adequately tested.

NitroSecurity performed testing on the following TOE models:

- NitroSecurity IPS: 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-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, 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: NS-ESS-2230, NS-ESS-2250-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: NS-NRC-1220, NS-NRC-2230-R, NS-NRC-2250-R
- NitroView Combo: NS-ESMRCV-5205-R, NS-ESMRCV-2250- R

Note that the vendor did not test on all model numbers in the evaluated configuration, as several models were added late in the evaluation. In each instance, the added models are exactly the same as the models already included in the evaluation, and covered by vendor testing. The new model numbers arose because a customer required specific numbering, and thus an existing model was re-numbered.

6.2 Evaluator Testing

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed the entire vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

- NitroSecurity IPS:

  NS-IPS-620R-2BTX

  NS-IPS-300-2BTX

  NS-IPS-1220-4BTX

  NS-IPS-4245-R-4BTX

  NS-IPS-2250-R-4BTX

  NS-IPS-1220-2BTX

- NitroSecurity ESM:

NS-ESM-4245-R

- NitroView Receiver:

  NS-NRC-2230-R

- NitroView Combo

  NS-ESMRCV-5205-R

  NS-ESMRCV-2250-R

The test configuration includes the TOE in in-line and in-tap configurations with the test machine that will generate traffic. The following tasks were performed by the evaluation team:

- The developer test suite was examined and found to provide adequate coverage of the security functions.
- A selection of the developer tests were run and the results found to be consistent with the results generated by the developer.
- No vulnerabilities in the TOE were found during a search of vulnerability databases.

7 EVALUATED CONFIGURATION

The evaluated product is:

- 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, 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 any of the following supported appliance models:

  NS-ESMRCV-5205-R, NS-ESMRCV-2250-R, NS-ESMRCV-625-R, NS-ESMRCV-652-R

The products must be installed and configured in accordance with the Common Criteria appendix of NitroSecurity™ (NitroGuard™ IPS, NitroView™ ESM, NitroView™ Receiver, NitroView™ ESM/Receiver Combo) User Guide, Release 8.0. Part № NS-75602001800.

8 RESULTS OF THE EVALUATION

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL3 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 and CEM version 3.1 [5], [6]. The evaluation determined the NitroSecurity Intrusion Prevention System version 8.0.0 TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 3) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the NitroSecurity Intrusion Prevention System version 8.0.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, and an architectural design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 3 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely install and administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied the coverage and independent testing CEM work units. . Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite and devised an independent set of team tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Vulnerability Assessment Activity (AVA)

The SAIC evaluation team performed a vulnerability assessment. The vulnerability assessment included a public search for vulnerabilities, an examination of the evidence provided for evaluation for flaws, and development of penetration tests. The product proved to be adequate to withstand an attacker with a basic attack potential.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.6 Summary of Evaluation Results

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 VALIDATOR COMMENTS AND RECOMMENDATIONS

The following are some recommendations and guidance for those integrating this product into a system:

1. Commands issued in terminal mode are not covered by this evaluation. As such, customers should be aware that these commands may not satisfy the ECAR and ECAT IA controls of DOD Instruction 8500.2.
2. The term "firewall" and "firewall rules" are used in this product's documentation. However, there was no evaluation of firewall functionality.
3. The Linux product used internal to the NitroSecurity product cannot be configured by the end-user. It is unknown if the appliance-internal versions of Linux are in STIG-compliant configurations, but their limited accessibility and lack of published vulnerability may provide appropriate mitigations for DOD users.
4. The network discovery functionality was not covered by the evaluation.
5. In order to support interaction with external devices, this product stores usernames and passwords for external services. From the evaluation point of view, this information was protected by the physical protection of the devices. The evaluation team did not assess whether this information is stored encrypted nor the quality of that encryption, if it exists.
6. In the evaluated configuration, password rules are weaker than required by the DOD Instruction 8500.2 IAIA control. It is unclear if the system provides the ability to configure these rules stronger.

7. It appears the product provides capabilities for login frustration, although these were not covered by the evaluation. This may impact the ability to meet the ECLO IA control.

10 SECURITY TARGET

The Security Target is identified as NitroSecurity Intrusion Prevention System 8.0.0 Security Target, Version 1.0, October 13, 2009.

11 GLOSSARY AND ACRONYMS

11.1 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

11.2 Acronyms

ARP	Address Resolution Protocol
CCEVS	Common Criteria Evaluation and Validation Scheme
CISSP	Certified Information Systems Security Professional
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ESM	Enterprise Security Module
ETR	Evaluation Technical Report
FIPS	Federal Information Process Standard
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
IDS	Intrusion Detection System
IDSSPP	Intrusion Detection System System Protection Profile
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
RADIUS	Remote Authentication Dial In User Service
SAIC	Science Applications International Corporation
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transport Protocol
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Security Summary
VPN	Virtual Private Network

12 BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, dated September 2007, Version 3.1 Rev 2.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, dated September 2007, Version 3.1 Rev 2.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, dated September 2007, Version 3.1 Rev 2.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 2.3, August 2005.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, dated September 2007, Version 3.1 Rev 2.

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

[7] Science Applications International Corporation. *Evaluation Technical Report for the NitroSecurity Intrusion Prevention System 8.0.0 Part 1 (Non-Proprietary)*, Version 0.4, October 13, 2009

[8] Science Applications International Corporation. *Evaluation Technical Report for the NitroSecurity Intrusion Prevention System 8.0.0 Part 2 (Proprietary)*, Version 1.0, October 13, 2009.

[9] Science Applications International Corporation. *Evaluation Team Test Report for NitroSecurity Intrusion Prevention System 8.0.0 Part 2 Supplement (SAIC and NitroSecurity Proprietary)*, Version 0.8, October 13, 2009.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] NitroSecurity Intrusion Prevention System 8.0.0 Security Target, Version 1.0, October 13, 2009.