National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Juniper Networks Security Appliances

Report Number:	**CCEVS-VR-VID10301-2010**
Dated:	**26 March 2010**
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

Validation Team

Senior Validator

Jandria Alexander

The Aerospace Corporation

Columbia, Md

Lead Validator

Rick Murphy

Noblis
Falls Church, VA

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Juniper Networks Security Appliances product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in March 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, Revision 2. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The evaluation team determined that the product satisfies conformance claims of Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4, augmented with ADV_FSP.5, ADV_INT.3, ADV_TDS.4, ALC_FLR.2 and ATE_DPT.3. The information in this Validation Report is largely derived from the Security Target, the Evaluation Technical Report (ETR) and associated test reports produced during the evaluation. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The Juniper Networks Security Appliances comprise a range of network appliances that primarily support the definition and enforcement of information flow policies among network nodes. Each Security Appliance provides for stateful inspection of every packet that attempts to traverse the network via the appliance. The appliance provides capabilities to manage the security policy enforced by the appliance. All information flow from one network node to another passes through a security appliance. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the security appliance ensures that security relevant activity is audited and that its own functions are protected from potential attacks.

Juniper Networks Security Appliances, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Juniper Networks Security Appliances Security Target.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Juniper Networks Security Appliances
Sponsor:	Juniper Networks 1194 North Mathilda Ave. Sunnyvale, CA 94089-1206
Developer:	Juniper Networks 1194 North Mathilda Ave. Sunnyvale, CA 94089-1206

CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	December 18, 2007
Completion Date:	March 22, 2010
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1 Revision 2, September 2007.
Evaluation Class:	EAL 4, augmented with ADV_FSP.5, ADV_INT.3, ADV_TDS.4, ALC_FLR.2, and ATE_DPT.3
Description:	The Juniper Networks Security Appliances comprise a range of network appliances that primarily support the definition and enforcement of information flow policies among network nodes, using stateful inspection.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Juniper Networks Security Appliances product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Dawn Campbell Cynthia Reese Katie Sykes Quang Trinh
Validation Body:	National Information Assurance Partnership CCEVS
Validation Personnel:	Jandria Alexander, The Aerospace Corporation Rick Murphy, Noblis

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.ADDRESS_MASQUERADE A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.ADMIN_ROGUE An administrator’s intentions may become malicious resulting in user or TSF data being compromised.

T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user’s action.

T.CRYPTO_COMPROMISE A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.

T.FLAWED_DESIGN Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.

T.FLAWED_IMPLEMENTATION Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.

T.MALICIOUS_TSF_COMPROMISE A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.MASQUERADE A user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.

T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.

T.REPLAY A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).

T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

T.RESOURCE_EXHAUSTION A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.

T.SPOOFING An entity may misrepresent itself as the TOE to obtain authentication data.

T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.

T.UNAUTHORIZED_ACCESS A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.

T.UNAUTHORIZED_PEER An unauthorized IT entity may attempt to establish a security association with the TOE.

T.UNIDENTIFIED_ACTIONS The administrator may fail to notice potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach.

T.UNKNOWN_STATE When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

2 Identification

The evaluated product is one or more of the following security appliances running the specified ScreenOS firmware version:

Product	**Part Numbers**	**Firmware Version**
Juniper Networks NetScreen ISG 1000	NS-ISG-1000, NS-ISG-1000-DC, NS-ISG-1000B, NS-ISG-1000B-DC	6.2.0r3a
Juniper Networks NetScreen ISG 2000	NS-ISG-2000, NS-ISG-2000-DC, NS-ISG-2000B, NS-ISG-2000B-DC	6.2.0r3a
Juniper Networks NetScreen 5200	NS-5200, NS-5200-DC	6.2.0r3a
Juniper Networks NetScreen 5400	NS-5400, NS-5400-DC	6.2.0r3a

Product	Part Numbers	Firmware Version
Juniper Networks SSG5 Secure Services Gateway	SSG-5-SB, SSG-5-SH	6.2.0r3
Juniper Networks SSG20 Secure Services Gateway	SSG-20-SB, SSG-20-SH	6.2.0r3
Juniper Networks SSG140 Secure Services Gateway	SSG-140-SB SSG-140-SH	6.2.0r3
Juniper Networks SSG320M Secure Services Gateway	SSG-320M-SH, SSG-320M-SH-N-TAA, SSG-320M-SH-DC-N-TAA	6.2.0r3
Juniper Networks SSG350M Secure Services Gateway	SSG-350M-SH, SSG-350M-SH-N-TAA, SSG-350M-SH-DC-N-TAA	6.2.0r3
Juniper Networks SSG520M Secure Services Gateway	SSG-520M-SH, SSG-520M-SH-N-TAA, SSG-520M-SH-DC-N-TAA	6.2.0r3
Juniper Networks SSG550M Secure Services Gateway	SSG-550M-SH, SSG-550M-SH-N-TAA, SSG-550M-SH-DC-N-TAA	6.2.0r3

The TOE is administered via a command line interface (CLI). During normal operation, the CLI is accessed remotely over a Secure Shell (SSH) connection. For initial configuration, a device that can emulate a VT-100 terminal is connected directly to the appliance as a local console. Once initial configuration is completed and the TOE is in the evaluated configuration, the local console remains connected to the TOE only to monitor alarms generated by the TOE. It is not to be used for entering commands or any other input. This is described in the administrative guidance documentation provided as part of the TOE.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

3.1 Security Audit

Audit data is stored in memory and is separated into three types of logs: events; traffic logs; and self logs. Events are system-level notifications and alarms which are generated by the system to indicate events such as configuration changes, network attacks detected, or administrators logging in or out of the device. Traffic logs are directly driven by policies that allow traffic to go through the device. Self logs store information on traffic that is dropped and traffic that is sent to the device. Logs are protected and a searching/sorting mechanism of these logs is offered to administrators.

The TOE monitors events and can apply rules to those monitored events to identify potential security violations. If the TOE detects a potential security violation, it displays an alarm at the local console, at remote administrator sessions that currently exist, and at remote administrator sessions that are initiated before the alarm has been acknowledged. Alarms can be configured to be audible.

3.2 Cryptographic Support

The Juniper Networks Security Appliances are FIPS 140-2 validated as multi-chip standalone modules.

3.3 User Data Protection

The TOE enforces information flow control policies based on the concept of zones. Security policies are applied to the flow of information from network nodes in one zone to network nodes in other zones. These policies control interzone and intrazone information flows.

A zone is a logical abstraction on which the TOE provides services that are typically configurable by the administrator. A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or logical entity that performs a specific function (a function zone).

3.4 Identification and Authentication

The TOE provides an authentication mechanism for administrative users through an internal authentication database. Administrative login is supported at the local console for initial configuration, and remotely via an SSH protected communication channel. FIPS 140-2 level 3 operator authentication requirements preclude the use of external authentication servers. Thus, to operate the TOE in a FIPS certified manner, only local administrator authentication is permitted in the evaluated configuration.

A known administrator user id and its corresponding authentication data must be entered correctly in order for the administrator to successfully logon and thereafter gain access to administrative functions. For local authentication, all administrator user name and password pairs are managed in a database internal to the TOE. Excessive failed login attempts while initiating a remote administration session can cause the session being created to be closed.

3.5 Security Management

After initial configuration, administrators manage the TOE remotely using a CLI communicating over the SSH protocol. The TOE also implements a web interface, but this is not part of the evaluated configuration.

To execute the CLI, the administrator can establish a trusted SSH connection to the TOE and utilize the CLI offered through the SSH connection. Regardless of the interface, the authorized administrator must be successfully identified and authenticated before they are permitted to perform any security management functions on the TOE.

The TOE supports three distinct administrative roles: Audit Administrator; Cryptographic Administrator; and Security Administrator. In addition to these administrative roles, an administrator may be given a read-write or read-only attribute that affects that administrator's ability to change the device's configuration data.

3.6 Protection of the TSF

The TOE is a hardware and firmware device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. ScreenOS is a special purpose OS that provides no general purpose programming capability. All network traffic from one network zone to another or between two networks within the same network zone passes through the TOE; however, no protocol services are provided for user communication with the TOE itself. The TOE also preserves its configuration for trusted recovery in the event that the configuration has been modified and not saved or if the TOE has been ungracefully shutdown.

The TOE provides a recovery and self testing mechanism. The recovery mechanism allows administrators to return the TOE to a secure state, while the self test mechanism allows administrators to verify the integrity of the TOE and its cryptographic functions.

3.7 Resource Utilization

The TOE provides features to protect itself from Denial of Service attacks. These features limit TCP connections and offer administrators the ability to limit the number of resources a particular address or set of addresses can use over a specified time period.

3.8 TOE Access

The TOE provides the ability to restrict the establishment of an administrative session based on a schedule or based upon the originating source IP address (or subnet). The TOE also provides inactivity timeouts and logon banners that can be configured by administrators.

3.9 Trusted Path/Channels

Remote administration of the TOE can be accomplished using SSH to protect the communication of a remote administrator and the TOE. SSH provides for the protection of remote administration activity from both disclosure and modification. An IPSEC tunnel is used to provide encryption and integrity for trusted channels to external servers (e.g., an NTP server).

4 Assumptions

The following assumptions are identified in the ST:

A.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

A.NO_TOE_BYPASS Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is the Juniper Networks Security Appliances.

All models comprising the TOE have been validated to FIPS 140-2 Security Level 2, and to Security Level 3 for:

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Cryptographic Key Management
- Design Assurance.

As a consequence of this validation, and in order to ensure the evaluated configuration of the TOE satisfies its security requirements, the following clarifications are noted:

- The TOE appliance should be configured for FIPS 140 mode to operate in the evaluated configuration
- External authentication servers are not permitted in the evaluated configuration
- Use of the Web interface for security management is not permitted in the evaluated configuration
- Use of the local console for security management is restricted to initial configuration. Once initial configuration is completed and the TOE is in FIPS mode, the local console can remain connected to the TOE only to monitor alarms generated by the TOE. It is not to be used for entering commands. This is described clearly in the administrative guidance documentation provided as part of the TOE
- Once the necessary administrator accounts (Security, Audit, Crypto) have been created, the Root account should not be used, except to manage (modify, delete) administrator accounts.

5 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks Security Appliances, a line of integrated security network devices combining firewall, virtual private networking (VPN), and traffic management functions.

All security appliances have hardware accelerated IPSec encryption and very low latency, allowing them to fit into any network. Installing and managing appliances is accomplished using a command line interface (CLI).

The security appliances use a technique known as ‘stateful inspection’ rather than an ‘application proxy’, as stateful inspection offers the combination of security and performance. Stateful inspection firewalls examine each packet, and track application-layer information for each connection, by setting up a state table that spans multiple packets. This is used to determine whether incoming packets are legitimate. It eliminates the requirement to establish a TCP session with the firewall itself to access a service on the other side of the firewall (i.e., proxy the service).

The TOE hardware is manufactured to Juniper's specifications by sub-contracted manufacturing facilities. Juniper's custom operating system, ScreenOS, runs in firmware. The security appliances provide no extended permanent storage such as disk drives and no abstractions such as files. Audit information is stored in memory. The main components of a security appliance are the processor, ASIC, memory, interfaces, and surrounding chassis and components. The differences between security appliances are the types of processor(s), traffic interfaces, management interfaces, number of power supplies, type of ASIC, and redundancy to ensure high availability. The architectural differences are summarized in the following table:

Model	**Crypto Support**	**Processor Architecture**
SSG-5	Intel IXP625	Intel IXP625
SSG-20	Intel IXP625	Intel IXP625
SSG-140	Intel IXP2325	Intel IXP2325
SSG-320M	Cavium CN1010	Intel Celeron
SSG-350M	Cavium CN1010	Intel Celeron
SSG-520M	Cavium CN1010	Intel Pentium 4
SSG-550M	Cavium CN1010	Intel Pentium 4
ISG 1000	GigaScreen3 ASIC	GigaScreen3 ASIC, PowerPC MPC7447(2)
ISG 2000	GigaScreen3 ASIC	GigaScreen3 ASIC, PowerPC MPC7447(2)
NS-5200	GigaScreen3 ASIC	GigaScreen3 ASIC, PowerPC MPC7447(2)
NS-5400	GigaScreen3 ASIC	GigaScreen3 ASIC, PowerPC MPC7447(2)

ScreenOS firmware powers the entire system. At its core is a custom-designed, real time operating system built from the outset to deliver security and performance. ScreenOS provides an integrated platform for its functions, including:

- Stateful inspection firewall
- Traffic management
- Site-to-Site VPN.

ScreenOS does not support a programming environment.

The TOE design decomposes ScreenOS into 14 subsystems, each of which is further decomposed into one or more related modules. Each subsystem is responsible for a specific area of the operation of the TOE, as follows:

- Administration—implements the administrative interface to the TOE (the Command Line Interface), including the SSH server to support remote administration, and enforces role-based restrictions on access to specific commands
- Authentication—responsible for authentication of users attempting to gain access to the TOE, including enforcement of restrictions on when and from where administrative sessions can be established
- Audit—responsible for the configuration and operation of the audit security function, generating audit events and traffic and self logs on behalf of all other subsystems

- VPN—responsible for the TOE’s VPN capability, including IKE and all cryptographic functionality
- Packet Flow Processing—processes all network packets arriving on the TOE’s network interfaces, whether addressed to the TOE or intended to traverse the TOE, thus implementing the TOE’s firewall capabilities, including detection of attempted network-based attacks
- Traffic Management—provides traffic-shaping support (non-TSF)
- TCP/IP Stack—implements the TOE’s TCP/IP stack for receiving and transmitting network packets (non-TSF)
- Routing—implements the TOE’s routing tables and supports the VPN and Packet Flow Processing subsystems
- NSRP—implements the TOE’s High-Availability functionality (non-TSF)
- Kernel—implements kernel services to support the operation of the other subsystems, such as task management, inter-process communication, and interrupt handling
- Initialization—responsible for bringing the TOE up from the initial power-on state to full operation
- Memory Management—implements the TOE’s virtual memory management system to support the other subsystems
- File System—implements a simple file system for storage of TOE configuration data
- Hardware—provides the underlying hardware support, including the system clock.

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- Juniper Networks Concepts and Examples ScreenOS Reference Guide Volumes 1 – 14, Release 6.2.0, Rev. 01
- Juniper Networks Security Products ScreenOS CLI Reference Guide: IPv4 Command Descriptions, Release 6.2.0, Rev 01
- Juniper Networks Security Products ScreenOS CLI Reference Guide: IPv6 Command Descriptions, Release 6.2.0, Rev 01
- ScreenOS Message Log Reference Guide, release 6.2.0, Rev. 1
- Juniper Networks ScreenOS 6.2 Evaluated Configuration for Common Criteria, EAL4, Version 1.0, 20 March 2010
- Juniper Networks Security Products Upgrade Guide ScreenOS Release 6.2.0, Rev. 03
- SSG 5 Hardware Installation and Configuration Guide
- SSG 20 Hardware Installation and Configuration Guide
- SSG 140 Hardware Installation and Configuration Guide
- SSG 300M-series Hardware Installation and Configuration Guide
- SSG 500M-series Hardware Installation and Configuration Guide
- ISG 1000 Hardware Installation and Configuration Guide
- ISG 2000 Hardware Installation and Configuration Guide

- NetScreen-5000 Series Hardware Installation and Configuration Guide

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for Juniper Networks Security Appliances.

Evaluation team testing was conducted at the vendor’s development site in January 2010.

7.1 Developer Testing

The vendor’s approach to testing for the Juniper Networks Security Appliances is based on testing the claimed security functions of the TOE as represented by the SFRs specified in the ST. The vendor has developed a test suite comprising various automated tests designed to demonstrate that the TSF satisfies the SFRs specified in the ST.

The vendor addressed test depth by mapping SFRs to specific subsystems and modules and by simultaneously mapping SFRs to specific test cases. The vendor’s tests are focused on demonstrating the satisfaction of specific SFRs, but the vendor also analyzed the functionalities addressed in the TOE design and also mapped test cases that address those functionalities.

The vendor ran the entire test suite on all TOE models on the test configuration described in the test documentation and gave the evaluation team the actual results. The evaluation team verified the results demonstrated all vendor tests had passed.

The evaluation team noted the vendor’s test suite is comprehensive, including positive and negative test cases and a significant number of vulnerability tests.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite for the TOE per the evaluated configuration as described in the vendor’s test documentation (“NIAP Test Configurations R3” spreadsheet).

The evaluation team executed a sample of the vendor test suite, per the evaluated configuration as described in the Juniper Networks Security Appliances Security Target. The tests were run on a selection of the test configurations described in the vendor test documentation, using the vendor’s test infrastructure.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results. The following models, covering the spectrum of appliance from low to high end, were included in evaluation team testing:

- SSG-5: 72 test cases
- SSG-140: 23 test cases
- SSG-320M: 38 test cases
- SSG-520M: 139 test cases
- ISG 1000: 102 test cases.

The evaluation team performed the following additional functional tests covering the following aspects of the TSF:

- Allowed and excluded user types
- Association of administrative role with user
- Administrative role separation
- Authentication failure handling
- Authentication failure threshold
- Login process and throttling
- Password constraints enforcement
- Administrative role revocation
- Location based access restrictions.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE, identifying five vulnerabilities reported against earlier versions of ScreenOS. The evaluation team determined, through analysis of vulnerability descriptions and consideration of the method of use of the TOE, that two of these reported vulnerabilities are not relevant to the TOE in its evaluated configuration—one relates the Web user interface, which is not permitted, and the other is a documented feature, which has appropriate guidance associated with it in the product guidance documentation. The evaluators additionally confirmed, through examination of the vendor's CM records, that the other vulnerabilities have had fixes developed and applied to ScreenOS and do not exist in the evaluated version of the TOE.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities.

8 Evaluated Configuration

The evaluated version of the TOE is Juniper Networks Security Appliances, model and firmware versions as identified in Section 2.

9 Results of the Evaluation

The evaluation was conducted based upon Version 3.1, Revision 2 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that a certificate rating of EAL4, augmented with ADV_FSP.5, ADV_INT.3, ADV_TDS.4, ALC_FLR.2 and ATE_DPT.3 be issued for Juniper Networks Security Appliances.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	**Assurance Component Name**
ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.1	Implementation representation of the TSF
ADV_INT.3:	Minimally complex internals
ADV_TDS.4	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_FLR.2	Flaw reporting procedures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

10 Validator Comments/Recommendations

The Validator has the following observation:

- The TOE incorporates administrative interfaces including a console. The evaluated configuration requires that, after initial configuration, the console be used only to monitor alarms generated by the TOE. All other administrative actions are performed while using an authenticated Secure Shell (SSH) connection.

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices. The Validator agrees that the CCTL presented appropriate rationales to support the Results of the Evaluation presented in Section 6 of the ETR. Therefore, the Validator concludes that the evaluation and the Pass results for the TOE are complete and correct:

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Juniper Networks Security Appliances Security Target**, Version 2.0, dated 5 March 2010.

13 Glossary

Please consult the CC, CEM and the US Government VPN and Traffic Filter Firewall PPs for Medium Robustness environments for definitions of abbreviations and terms used within this document.

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Juniper Networks, Inc. (http://www.juniper.net)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, Revision 2, September 2007
- *Common Evaluation Methodology for Information Technology Security*, version 3.1, Revision 2, September 2007.

Other Documents:

- *Juniper Networks Security Appliances Security Target*, Version 2.0, 5 March 2010.