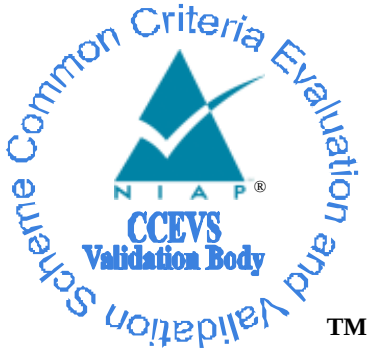
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Juniper Networks Security Appliances

Report Number: CCEVS-VR-10452-2012
Dated: 28 June 2012
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jandria S. Alexander
The Aerospace Corporation

Dr. Patrick W. Mallett
The MITRE Corporation

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

1 Executive Summary

The evaluation of Juniper Networks Security Appliances was performed by SAIC, in the United States and was completed in June 2012. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Juniper Networks Security Appliances TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

Science Applications International Corporation (SAIC) determined that the product satisfies evaluation assurance level "EAL 2 augmented with ALC_FLR.2" as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Juniper Networks Security Appliances Security Target, Version 0.8, April 6, 2012.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is Juniper Networks Security Appliances.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) 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 Juniper Networks Security Appliances by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional 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 For Juniper Networks Security Appliances* Parts 1 and 2 and the *Evaluation Team Test Report For Juniper Networks Security Appliances* produced by SAIC.

1.1 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
Evaluation Facility:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	May 2011
Completion Date:	June 2012
CC:	Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009
Evaluation Class:	EAL 2 augmented with ALC_FLR.2
Description:	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. The TOE consists of one or more of the following security appliances running the specified ScreenOS firmware version: The TOE is administered via a command line interface (CLI). During normal operation, the CLI is accessed remotely over a Secure Shell (SSH) connection.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Juniper Networks Security Appliances by any agency of the U.S. Government and no warranty of Juniper Networks Security Appliances is either expressed or implied.
PP:	*U.S. Government Protection Profile for Traffic-Filter Firewall in Basic Robustness Environments*, version 1.1, July 25, 2007
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The following threats, defined in the U.S. Government Protection Profile for Traffic-Filter Firewall in Basic Robustness Environments, are mitigated by the TOE.

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

1.4 Organizational Security Policies

The following organizational policies are fulfilled by the TOE.

P.INTEGRITY	The TOE shall support the IETF Internet Protocol Security Encapsulating Security Payload (IPSEC ESP) as specified in RFC 2406. Sensitive information transmitted to a peer TOE shall apply integrity mechanisms as specified in Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404)

2 Identification

The evaluated product is as follows:

Security Target: Juniper Networks Security Appliances Security Target, Version 0.7, March 7, 2012

TOE Identification: The TOE consists of 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	6.3.0r6
Juniper Networks NetScreen ISG 2000	NS-ISG-2000, NS-ISG-2000-DC, NS-ISG-2000B, NS-ISG-2000B-DC	6.3.0r6
Juniper Networks NetScreen 5200	NS-5200, NS-5200-DC	6.3.0r6
Juniper Networks NetScreen 5400	NS-5400, NS-5400-DC	6.3.0r6
Juniper Networks SSG5 Secure Services Gateway	SSG-5-SB, SSG-5-SH	6.3.0r6
Juniper Networks SSG20 Secure Services Gateway	SSG-20-SB, SSG-20-SH	6.3.0r6
Juniper Networks SSG140 Secure Services Gateway	SSG-140-SB, SSG-140-SH	6.3.0r6
Juniper Networks SSG320M Secure Services Gateway	SSG-320M-SH, SSG-320M-SH-N-TAA, SSG-320M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG350M Secure Services Gateway	SSG-350M-SH, SSG-350M-SH-N-TAA, SSG-350M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG520M Secure Services Gateway	SSG-520M-SH, SSG-520M-SH-N-TAA, SSG-520M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG550M Secure Services Gateway	SSG-550M-SH, SSG-550M-SH-N-TAA, SSG-550M-SH-DC-N-TAA	6.3.0r6

TOE Environment:

The TOE is a self-contained network appliance.

3 Security Policy

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

- Security audit

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF

> ***Note:*** *The ST should be consulted for more description of these and other security functions of the TOE.*

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 our 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. Both audit events and traffic messages can be further defined depending on the severity of the message and/or event. Logs are protected and a searching/sorting mechanism of these logs is offered to administrators.

3.2 Cryptographic support

The Juniper Networks Security Appliances are FIPS 140-2 validated as multi-chip standalone modules. All support the use of AES with SSH using key sizes greater than or equal to 128-bits.

3.3 User data protection

The user data protection provided by the Security Appliance is provided though 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.

Traffic from one network node in a zone will only be forwarded to a node in another zone if the connection requests and the traffic satisfy the information flow policies configured in the security appliance. If data is received by an appliance that does not conform to those policies, it will be discarded and an audit record will be sent to the traffic log.

A zone is a logical abstraction on which a security appliance 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).

See the Security Target for more information about zones.

3.4 Identification and authentication

The security appliances provide an authentication mechanism for administrative users through an internal authentication database. Administrative login is supported through the locally connected console for initial configuration, or remotely via an SSH protected communication channel. The

TOE operates in a mode that has been certified to FIPS 140-2 level 2 overall, and supports AES encryption for the SSH protected communication channel.

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 security appliance. Excessive failed login attempts while initiating a remote administration session can cause the session being created to be closed.

3.5 Security management

Every security appliance provides a command line administrative interface and supports remote administration through an SSH command line interface. SSH provides for the protection of remote administration activity from both disclosure and modification. Neither the web interface nor the Network and Security Manager are part of the evaluated configuration. To execute the CLI, the administrator can establish a trusted SSH connection to the security appliance. The authorized administrator must be successfully identified and authenticated before they are permitted to perform any security management functions on the TOE.

The Security Appliances also support distinct administrative roles: Root Administrator, 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. All of these roles are considered to be authorized administrators.

More details about these management operations available to administrators can be found in Section 6.1.5, 'Security management'.

3.6 Protection of the TSF

Each security appliance 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 security appliance itself. The TOE also utilizes a hardware clock to maintain and provide reliable time stamps.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.

A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

4.1 Clarification of Scope

The Target of Evaluation (TOE) is the Juniper Networks Security Appliances previously identified. All models comprising the TOE have been validated to FIPS 140-2 Security Level 2.

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
- SNMP is excluded from the evaluated TOE. SNMP security features are not consistent with those identified in the ST (
- The IPv6 capabilities of the product were not subject to evaluation to simplify the evaluation and testing.
- The ST specifically indicates that ALG is not supported in a PAT configuration. The client port translation through NAT will not work. The NAT process on the firewall will always pick a high number port for source port translation, which will be subsequently denied by the rsh server. This is an application design issue and not a result of the ALG implementation
- Virtual Systems were excluded to simply the evaluation.

5 Architectural Information

Juniper Networks Security Appliances all share a very similar hardware architecture and packet flow. All run ScreenOS with common core features across all products. All security appliances perform the same security functions and export the same types of interfaces. A sample of the differences between these products is listed below.

- The SSG 5 and SSG 20 use an Intel IXP625 ASIC; the SSG 140 uses the Intel IXP2325. The Intel IXP ASICs provide acceleration of AES, and SHA-1. The remaining cryptographic and firewall functionality is performed in software.
- The 320M, 350M, 520M and 550M use the Cavium Nitrox Lite ASIC to accelerate AES, SHA-1 and modular exponentiation operations. The remaining cryptographic and firewall functionality is performed in software.
- The Juniper Networks NetScreen-5200, NetScreen-5400, NetScreen-ISG1000 and NetScreen-ISG2000 use one or more custom GigaScreen3 ASICs. The GigaScreen3 ASIC is capable of providing most of the firewall and cryptographic functionality, and uses the CPU as a co-processor for handling management traffic and first packet inspections (policy lookups). The GigaScreen3 ASIC can process an incoming packet, perform a session lookup, NAT, TCP/IP sequence checking, and can then send the packet back out of the device without ever being processed by the system CPU. The only time the CPU is used is for first packet inspection, management traffic, and packet fragment reassembly for inspection. These platforms use the Cavium Nitrox Lite ASIC for acceleration of modular exponentiation operations.

5.1 Hardware

The hardware is manufactured to Juniper's specifications by sub-contracted manufacturing facilities. Juniper's custom OS, ScreenOS, runs in firmware. The security appliances provide no extended permanent storage like disk drives and no abstractions like 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 supported network interfaces that carry network traffic include support for Gigabit or 10/100Mbps copper-based connections as well as Fibre channel connections. All devices support 10/100Mbps ethernet connectivity, while some also provide a management interface through an RJ-45 serial port.

5.2 ScreenOS

ScreenOS 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 general-purpose, computing environment.

5.3 Physical Boundaries

The physical boundary of the security appliances is the physical appliance. The console, which is part of the TOE operational environment, provides the visual I/O for the administrative interface.

After the TOE is placed into the evaluated configuration, the administrative interface is provided over an SSH connection using encryption.

The security appliance attaches to physical networks that have been separated into zones through port interfaces.

Security appliances come in several models. Each model differs in the performance capabilities; however all provide the same security functions. Each appliance enforces a security policy for all connection request and traffic flow between any two network zones.

All hardware on which each security appliance operates is part of the TOE. Each security appliance has a custom operating system that is part of the TOE. The operating system, ScreenOS, runs completely in firmware. There is one assumption pertaining to the correct operation of the TOE and that is for the console, which must be a device that can emulate a VT-100 terminal. The console is part of the TOE environment and is expected to correctly display what is sent to it from ScreenOS. Also within the TOE environment are optional servers that can provide time keeping or syslog services. These servers communicate with the TOE over trusted channels using certificate-based authentication and encryption.

The physical boundaries of the security appliance include the interfaces to communicate between an appliance and a network node assigned to a network zone. All network communication flow goes from the sender network node in one zone, through a security appliance, and from a security appliance to the receiving node in another network zone, if the security policy allows the information flow.

Please refer to the Security Target for more technical details about the product and its associated security claims and functions.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE (note that the first is Common Criteria specific and is normative while the others are generally informative) is as follows:

- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 1: Overview
- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 2: Fundamentals
- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 3: Administration
- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 4: Attack Detection
- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 5: VPNs
- ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 8: Address Translation
- ScreenOS CLI Reference Guide: IPv4 Command Descriptions
- ScreenOS 6.3.0 Message Log Reference Guide
- Juniper Networks ScreenOS 6.3 Evaluated Configuration for Common Criteria, EAL4

- 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

Note: *Several sections of the ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide are NOT included as part of the TOE documentation. These sections were excluded because this ST makes no claims regarding the functionality within these sections. Operation of the TOE with these features is not part of this evaluation.*

6.2 Evaluation Evidence

The following tables identify the additional documentation submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents are proprietary and not available to the general public.

- Juniper Networks Security Appliances Security Target, Version 0.8, April 6, 2012
- Functional Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [FSP]
- Juniper Networks Security Appliances Security Architecture Document, Revision 0.5, May 31, 2011 Tracings for BRPP Evaluation.xlsx [Tracings]
- Administrator Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [Admin]
- Audit Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [Audit]
- Authentication Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [Authentication]
- File System Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- Hardware Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- Initialization Subsystem TOE Design Specification Specification, Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- Kernel Services Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [Kernel Services]

- Memory Management Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 26, 2011
- NSRP Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- Packet Flow Processing Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.1, August 29, 2011 [Packet Flow Processing]
- Routing Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- TCP/IP Stack Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- Traffic Management Subsystem TOE Design Specification Juniper Networks Security Appliances, Version 2.0, May 31, 2011
- VPN Subsystem TOE Design Specification, Juniper Networks Security Appliances, Version 2.0, August 29, 2011 [VPN]
- Juniper Networks ScreenOS 6.3 Evaluated Configuration for Common Criteria, EAL4, Version 1.0, March 8, 2012 [ECCC]
- Other product guidance available for the TOE on the developer product website (http://www.juniper.net/techpubs/en_US/screenos6.3.0/information-products/pathway-pages/screenos/index.html)
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 1: Overview, Release 6.3.0, Rev. 01 [RG1]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 2: Fundamentals, Release 6.3.0, Rev. 01 [RG2]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 3: Administration, Release 6.3.0, Rev. 01 [RG3]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 4: Attack Detection and Defense Mechanisms, Release 6.3.0, Rev. 01 [RG4]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 5: VPNs, Release 6.3.0, Rev. 01 [RG5]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 6: Voice-over-Internet Protocol, Release 6.3.0, Rev. 01 [RG6]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 7: Routing, Release 6.3.0, Rev. 01 [RG7]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 8: Address Translation, Release 6.3.0, Rev. 01 [RG8]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 9: User Authentication, Release 6.3.0, Rev. 01 [RG9]
    - Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 11: High Availability, Release 6.3.0, Rev. 01 [RG11]

- Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 12: WAN, ADSL, Dial, and Wireless, Release 6.3.0, Rev. 01 [RG12]
- Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 13: General Packet Radio Service, Release 6.3.0, Rev. 01 [RG13]
- Juniper Networks ScreenOS 6.3.0 Concepts and Example, ScreenOS Reference Guide, Volume 14: Dual-Stack Architecture with IPv6, Release 6.3.0, Rev. 01 [RG14]
- Juniper Networks ScreenOS Reference Guide: IPv4 Command Descriptions, Release 6.3.0, Rev. 01 [CD4]
- Juniper Networks ScreenOS Reference Guide: IPv6 Command Descriptions, Release 6.3.0, Rev. 01 [CD6]
- Juniper Networks Secure Delivery Processes and Procedures, Revision D, December 1, 2009 [DEL]
- SSG 5 Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems60/HW_SSG5_600.pdf)
- SSG 20 Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems60/HW_SSG20_600.pdf)
- SSG 140 Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems60/HW_SSG140_600.pdf)
- SSG 300M-series Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems60/HW_SSG300M_600.pdf)
- SSG 500M-series Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems54/UG_SSG500M.pdf)
- ISG 1000 Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems61/HW_ISG1000_610.pdf)
- ISG 2000 Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems61/HW_ISG2000_610.pdf)
- NetScreen-5000 Series Hardware Installation and Configuration Guide, Juniper Networks (http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems50/hw_ns5000_610.pdf)

- ScreenOS Configuration Items, Revision C, April 11, 2011 (JNPR_ScreenOS_62_CC_MRPP_Configuration_Items.xml)
- ScreenOS Maintenance Release QA Process, Version 1.1, August 17, 2009 [Maintenance]

- Configuration Management Plan, Revision D, December 4, 2009 [CMP]
- Secure Delivery Processes and Procedures, Revision E, March 8, 2012 [DEL]
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 1 – Introduction & Overview, Document Number: SPEC-9242, Revision: 2.0, Date: Jan 1, 2012
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 2 - General Test Cases, Document Number: SPEC-9243, Revision: 2.0, Date: Jan 1, 2012
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 3 – More General Tests, Document Number: SPEC-9244, Revision: 2.0, Date: Jan 1, 2012
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 4 – Transparent Mode VPN Tests, Document Number: SPEC-9245, Revision: 2.0, Date: Jan 1, 2012
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 5 – Route Mode VPN Tests, Document Number: SPEC-9246, Revision: 2.0, Date: Jan 1, 2012
- Juniper Networks ScreenOS 6.3 Common Criteria Test Plan, Volume 7 – Transparent Mode Firewall Tests, Document Number: SPEC-9248, Revision: 2.0, Date: Jan 1, 2012
- Test Results

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 Technical Report For Juniper Networks Security Appliances Part 1, 0.1, 3/7/2012.

Evaluation team testing was conducted at the vendor's development site in Sunnyvale, CA during the week of February 27, 2012.

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, 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 subset of vendor tests selected was spread out over all of the TOE models, which includes coverage for five of the 18 test beds defined in the vendor's test suite. The evaluators selected the test cases so that there was at least 20% test coverage for each functional requirement. However, since some of the test cases are mapped to multiple requirements, the overall independent test coverage was over 30%. This sample was successfully exercised substantiating the vendor's own more comprehensive test results.

The evaluators devised a series of independent tests corresponding to the security functions as follows:

- Audit Data Generation
- Audit Review
- Audit Sorting
- Cryptographic Operation for remote sessions
- Cryptographic Operation for VPN sessions
- NAT Mode firewall protection
- Interzone and Global Zone Policy enforcement
- Single-use Authentication Mechanisms
- Management of Security Functions Behavior for User Security Attributes
- Management of Security Functions Behavior for Configuration Backup
- Management of Security Functions Behavior for SYSLOG Configuration
- Management of Security Functions Behavior for Remote Administration

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, no reported vulnerabilities are relevant to the TOE in its evaluated configuration.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a 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.

Finally, the evaluators ran comprehensive ports scans in order to ensure that all opened ports were expected and their purposes understood.

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL 2 augmented with ALC_FLR.2 are fulfilled.

8 Evaluated Configuration

As identified in the Juniper Networks Security Appliances Security Target, Version 0.7, March 7, 2012 the evaluated configuration consists of the following TOE components. Ultimately the guidance identified previously describes specifically how each of the identified components needs to be installed and used in order to operate the evaluated products in their evaluated configuration.

Product	Part Numbers	Firmware Version
Juniper Networks NetScreen ISG 1000	NS-ISG-1000, NS-ISG-1000-DC, NS-ISG-1000B, NS-ISG-1000B-DC	6.3.0r6
Juniper Networks NetScreen ISG 2000	NS-ISG-2000, NS-ISG-2000-DC, NS-ISG-2000B, NS-ISG-2000B-DC	6.3.0r6
Juniper Networks NetScreen 5200	NS-5200, NS-5200-DC	6.3.0r6
Juniper Networks NetScreen 5400	NS-5400, NS-5400-DC	6.3.0r6
Juniper Networks SSG5 Secure Services Gateway	SSG-5-SB, SSG-5-SH	6.3.0r6
Juniper Networks SSG20 Secure Services Gateway	SSG-20-SB, SSG-20-SH	6.3.0r6
Juniper Networks SSG140 Secure Services Gateway	SSG-140-SB, SSG-140-SH	6.3.0r6
Juniper Networks SSG320M Secure Services Gateway	SSG-320M-SH, SSG-320M-SH-N-TAA, SSG-320M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG350M Secure Services Gateway	SSG-350M-SH, SSG-350M-SH-N-TAA, SSG-350M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG520M Secure Services Gateway	SSG-520M-SH, SSG-520M-SH-N-TAA, SSG-520M-SH-DC-N-TAA	6.3.0r6
Juniper Networks SSG550M Secure Services Gateway	SSG-550M-SH, SSG-550M-SH-N-TAA, SSG-550M-SH-DC-N-TAA	6.3.0r6

9 Results of the Evaluation

The evaluation was conducted based upon Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. 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 an "EAL 2 augmented with ALC_FLR.2" certificate rating be issued for Juniper Networks Security Appliances.

The details of the evaluation are recorded in the *Evaluation Technical Report For Juniper Networks Security Appliances* Parts 1 and 2 and the *Evaluation Team Test Report For Juniper Networks Security Appliances*, which are controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

TOE Security Assurance Requirements

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

10 Validator Comments/Recommendations

See Section 4.1 Clarification of Scope.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Juniper Networks Security Appliances Security Target, Version 0.8, April 6, 2012.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5] Juniper Networks Security Appliances Security Target, Version 0.8, April 6, 2012.

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Juniper Networks Security Appliances Part 1, 0.1, 3/7/2012.

[8] Evaluation Technical Report For Juniper Networks Security Appliances Part 2, 0.2, 3/7/2012.

[9] Evaluation Team Test Report For Juniper Networks Security Appliances, version 0.1 3/7/2012.