Juniper Networks, Inc.
Juniper Networks Security Appliances
CCEVS-VR-05-0138

National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks, Inc.

Juniper Networks Security Appliances

Report Number: **CCEVS-VR-05-0138**
Dated: **December 23, 2005**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Timothy J. Bergendahl
The MITRE Corporation
Bedford, MA 01730

The Validation Team thanks Mr. Kenneth Elliott for his work as Senior Validator.

Common Criteria Testing Laboratory

Science Applications International Corporation
7125 Gateway Drive
Columbia, MD 21046

Evaluation Team

Cynthia Reese
Tammy Compton
Quang Trinh

Table of Contents

1 Executive Summary

The purpose of this Validation Report (VR) is to document the results of the EAL4 evaluation of `Juniper Networks Security Appliances` (hereafter `Security Appliances`), products of Juniper Networks, Inc., Sunnyvale, CA.

The evaluated `Security Appliances`, each of which runs ScreenOS 5.0.0r9, a proprietary operating system of Juniper Networks, Inc., are:

- Juniper Networks NetScreen-5GT
- Juniper Networks NetScreen-5XT
- Juniper Networks NetScreen-25
- Juniper Networks NetScreen-50
- Juniper Networks NetScreen-204
- Juniper Networks NetScreen-208
- Juniper Networks NetScreen-500
- Juniper Networks ISG 1000
- Juniper Networks ISG 2000
- Juniper Networks NetScreen 5200
- Juniper Networks NetScreen 5400

This Validation Report is not an endorsement of the Juniper `Security Appliances` by any agency of the United States Government, and no warranty of the products is either expressed or implied.

Evaluation of the `Security Appliances` at EAL4, was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL), Columbia, MD. Evaluation results identified in this validation report (VR) were drawn from the Evaluation Technical Report (ETR) prepared by the SAIC CCTL.

The Juniper evaluated `Security Appliances` identified above are integrated security appliances that control traffic flow through a network and operate as the central security hub in a network configuration. The appliances integrate stateful packet inspection firewall, virtual private networking (VPN), and traffic management features. All have hardware-accelerated VPN encryption and very low latency, allowing them to fit into any network. Installing and managing the appliances is accomplished using a command line interface (CLI).

Each evaluated model consists of hardware and firmware, and each runs ScreenOS 5.0.0r9 in firmware, a Juniper Networks proprietary operating system. The model differences have no affect on the security functions claimed in the Security Target

The TOE generates audit records corresponding to traffic flow, administrator actions, and identification and authentication. The TOE provides interfaces that allow the administrator to review the audit records, including the ability to search and sort the audit records. Additionally, the TOE provides the ability to protect the audit records and limit the loss of records due to storage exhaustion.

The TOE enforces an information flow policy that is enforced upon all packets attempting to traverse a Juniper Networks appliance. The policy is configurable by the administrator and is based on the presumed IP source address, destination IP address, protocol, source and destination interface, and service. The TOE has a packet buffer for temporary storage of packet information. All temporary storage is accounted for in that the size of the temporary storage relative to every packet is known, thus ensuring that the TOE does not reuse any previous packet information. Additionally, the TOE provides encryption/decryption capabilities for VPN sessions.

Administrators are the only users of the TOE and are forced to be identified and authenticated by the TOE before they are allowed to invoke any administrator commands. Although the TOE includes the console port, the actual console used is not part of the TOE, but is part of the environment. The Security Target includes an assumption that a VT-100 terminal, or any device that can emulate a VT-100 terminal, is required for use as a locally-connected console.

The security functions of the TOE are protected in two ways. First, untrusted users do not have a direct interface to these functions; they are limited to sending packets to the device. Second, the administrative interface is a separate interface that is not connected to the network and, therefore, not susceptible to many of the general threats on the network such as packet sniffing or attempts to log into a public administrative interface. The administrative interface allows an administrator (when properly identified and authenticated) to configure the Juniper Networks appliance. The security management functions are not available to non-administrator users. Additionally, the TOE includes a system clock that can only be set and modified by the administrator, providing reliable timestamps for audit information.

The overall Strength of Function (SOF) claim for the TOE is SOF-medium.

The following Juniper Networks Security Appliances have received FIPS 140-2 certification: NetScreen-5400 (Certificate No. 605); NetScreen-5200 (Certificate No. 603); NetScreen-500 (Certificate No. 604); NetScreen-208 (Certificate No. 607); NetScreen-204 (Certificate No. 607); NetScreen-5GT (Certificate No. 629); and NetScreen-5XT (Certificate No. 606).

For this evaluation, it was appropriate for the Security Target to claim compliance with the external standard for DES, TDES, AES, and SHA for the Juniper Networks ISG 1000

and ISG 2000 products; and to claim compliance with the external standard for AES, TDES, DES, DSA, SHS, RSA, HMAC, and RNG for the Juniper Networks NetScreen-25 and NetScreen-50 products. There are many ways of determining compliance with a standard. Juniper Networks has chosen to make a developer claim of compliance. This means there has been no independent verification (by either the evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithm actually meets the claimed standard. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements.

Each of the evaluated `Security Appliances` conforms to the *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, April 1999.

The Juniper `Security Appliances` TOE was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408. [CCV2.1] and the *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999, CEM-99/045. [CEMV1.0]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4].

The Security Target (ST) for the Juniper `Security Appliances` is contained within the document *Juniper Networks Security Appliances Security Target: EAL4,* Revision L, P/N-093-0896-000, December 19, 2005. [ST_AP_Rev_L].

The project, which also involved evaluation of the associated Security Target, was completed on December 23, 2005.

1.1 Interpretations

National and International Interpretations that pertain to this evaluation are identified in Table 2, Evaluation identifiers.

1.2 Threats to Security

The threats the evaluated product addresses are displayed in Table 1.

Threat	Description
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.

Threat	Description
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 flows 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. *Note*: While the associated *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, April 1999, assumes that administrators may access the TOE remotely, the PP also explicitly allows this capability to be optional. Hence while remote administrator access could be allowed, the TOE does not provide any support for this feature.
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.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.
T.PROTECTION	The data transmitted from the TOE to a peer TOE via encryption may be accessed by an unauthorized person.

Table 1. Threats to security.

2 Identification

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative involving the National Institute of Standards and Technology (NIST) and the National

Security Agency (NSA). The Common Criteria Evaluation and Validation Scheme (CCEVS) is an activity of the NIAP.

The focus of the CCEVS is to establish a national program for the evaluation of information technology products for conformance to the *International Common Criteria for Information Technology Security Evaluation* (*Common Criteria*).

The CCEVS Validation Body approves the participation of Common Criteria Testing Laboratories (CCTLs) for the purpose of performing evaluations of IT products or Protection Profiles. During the course of an evaluation, the Validation Body provides technical guidance to the CCTL and validates the results of the evaluation for conformance to the *Common Criteria*.

When appropriate, the Validation Body issues a Common Criteria Certificate. The Certificate, together with its associated Validation Report (VR), confirms that an IT product or Protection Profile has been evaluated at an accredited CCTL using the *Common Evaluation Methodology* for conformance to the *Common Criteria*.

Table 1 provides the information needed to completely identify the evaluated 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 organizations and individuals participating in the evaluation.

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Juniper Networks NetScreen-5GT, -5XT, -25, -50, -204, -208, and -500; Juniper Networks ISG 1000 and ISG 2000; Juniper Networks NetScreen 5200 and 5400. (5GT runs ScreenOS 5.0.0r9.r; ISG 1000 and 2000 run 5.0.0r9.y; all other platforms run 5.0.0r9.o).
Security Target	*Juniper Networks Security Appliances Security Target: EAL4,* Revision L, P/N-093-0896-000, December 19, 2005. [ST_AP_Rev_L].
CC Identification	*Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408. [CCV2.1]
Interpretations	National: English Language Refinements (0405) – ASE; Residual Protection (0350) – ASE, ADV; FAU_GEN modified

Item	Identifier
	(0347, 0410); PP Differences (0426) – ASE; Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (0418) – ASE; Clarification Of ``Audit Records'' (0422) – ASE, ADV; Association Of Information Flow Attributes W/Subjects And Information (0417) – ASE; Some Modifications To The Audit Trail Are Authorized (0423) – ASE, ADV; American English Is An Acceptable Refinement (0405); PP Notes Informative Only (0421) – ASE; Empty Assignments (0407) – ASE; A Completely Evaluated ST Is Not Required When TOE (0393) – ASE; Guidance Documentation (0411) – AGD. International: Separate objectives for TOE and environment (084) – ASE; Level of detail required for hardware descriptions (025) – ADV; Unique Configuration of CIs (003) – ACM; Underlying Hardware and Firmware (006) – ADV; Augmented and Conformant Overlap (008) – ASE; Deliver procedures may include confidentiality (016) – ADO; Evidence is required of entire TOE (024) – ADV; Events and actions (027) – AGD; Vulnerabilities not in TOE not applicable (031) – AVA; SOF analysis need not be in ST (032); CM applicable to TOE (037) – ACM; CM requirement modified (038) – ASE; ADO_IGS and AVA_VLA requirements modified (051) – ASE; FMT_SMR (new requirement) as a dependency of FMT_MOF – ASE, ADV.
CEM Identification	*Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999, CEM-99/045. [CEMV1.0]
Evaluation Technical Report	Provided by the SAIC Evaluation Team, December 2005.
Conformance Result (CC)	Security Target, [ST_AP_Rev_L], [CCV2.1] conformant; TOE (Juniper Networks NetScreen-5GT, -5XT, -25, -50, -204, -208, and -500; Juniper Networks NetScreen ISG 1000 and ISG 2000; Juniper Networks NetScreen 5200 and 5400. All platforms run S creenOS 5.0.0r9), [CCV2.1] Part 2 and Part 3 conformant.
Conformance Result (PP)	The TOE is conformant to the *U.S. Government Traffic-Filter Protection Profile for Low-Risk Environments*, Version 1.1, April 1999.
Sponsor	Juniper Networks, Inc., Sunnyvale, CA
Developer	Juniper Networks, Inc., Sunnyvale, CA
Evaluators	Cynthia Reese, Tammy Compton, and Quang Trinh, Science Applications International Corporation (SAIC), Columbia, MD

Item	Identifier
Validator	Timothy J. Bergendahl, The MITRE Corporation, Bedford, MA

Table 2. Evaluation identifiers.

3 Security Policy

The security policy for the Juniper `Security Appliances` TOE encompasses the following *Common Criteria* [CCV2.1] security functional classes:

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

The security functional components for each security functional class that pertains to the `Security Appliances` TOE are described in detail in Section 5.0 of the ST [ST_AP_Rev_L].

In addition, Section 5 of this Validation Report and Section 2.0 of the ST [ST_AP_Rev_L] describe the security policy in detail.

4 Assumptions

Assumptions about the environment of the TOE are displayed in Table 3.

Assumption	Description
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.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.CONSOLE	A VT-100 terminal or any device that can emulate a VT-100 terminal is required for use as a locally connected console. The VT-100 terminal/emulator is part of the IT environment and is expected to correctly display what is sent to it from the TOE.
A.LOCATE	The management console (VT-100 terminal/emulator) access will be restricted to authorized administrators.
A.PHYSEC	The TOE is physically secure.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

Assumption	Description
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.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PUBLIC	The TOE does not host public data.
A.NOREMO	Human users who are not authorized administrators cannot 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. *Note*: While the associated *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, April 1999, assumes that administrators may access the TOE remotely, the PP also explicitly allows this capability to be optional. Hence while remote administrator access could be allowed, the TOE does not provide any support for this feature.

Table 3. Assumptions.

5 Architectural Information

5.1 Architectural description

An image of the Juniper Networks NetScreen 5400 appliance is shown in Figure 1. When running ScreenOS 5.0.0r9 (5GT runs 5.0.0r9.r; ISG 1000 and 2000 run 5.0.0r9.y; all other platforms run 5.0.0r9.0.o), the NetScreen 5400 is one of the evaluated products.

The following description of the `Juniper Networks Security Appliances` architecture is based on the description presented in (a) Final Evaluation Technical Report for the Juniper Networks Security Appliances Product, EAL4, Part 1 (Non-Proprietary), Version 0.2, December 19, 2005 and (b) the ST [ST_AP_Rev_L].

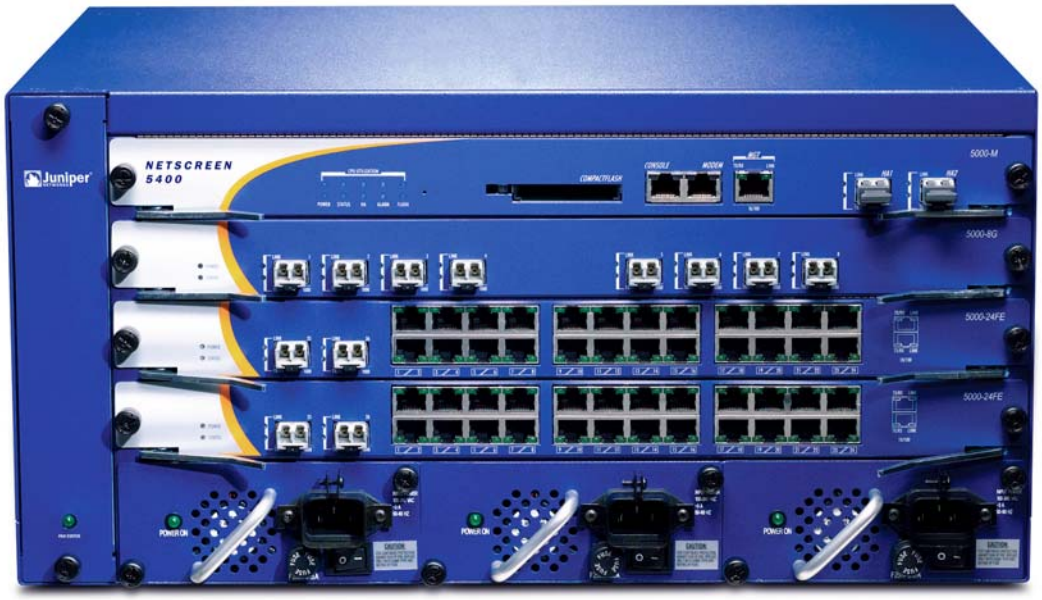

Figure 1. Juniper Networks NetScreen 5400.

5.1.1 Product Description

Juniper Networks NetScreen-5GT, 5XT, 25, 50, 204, 208, 500, ISG 1000, ISG 2000, 5200, and 5400 all share a very similar hardware architecture and packet flow. All utilize custom Application-Specific Integrated Circuits (ASICs) for policy lookup acceleration, while a CPU is used as the main processor. 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 Juniper Networks NetScreen-5GT, 5XT, 25, 50, 204, 208, and 500 use a version of the GigaScreen ASIC that accelerates policy look-ups.
- The Juniper Networks NetScreen-204, 208, and 500 utilize dual-port memory for faster processing and faster packet flow.
- The Juniper Networks NetScreen-ISG100 and ISG 2000 utilizes a Cavium Nitrox Lite ASIC, which serves requests from 100 Mbps up to 1 Gbps of data.
- The Juniper Networks NetScreen-5200 and 5400 are different than the rest of the products. They utilize one or more GigaScreen-II ASICs, which provide significantly more functionality than the GigaScreen ASIC. The GigaScreen-II ASIC is capable of providing most of the functionality, and uses the CPU as a co-processor for handling management traffic and first packet inspections (policy lookups). As a result, the GigaScreen-II 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 the CPU every seeing it. The only time

the CPU is used is for first packet inspection, management traffic, and packet fragment reassembly for inspection.

5.1.2 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 because of the large storage capabilities.

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.

5.1.3 ScreenOS

ScreenOS firmware powers the entire system. At its core is a custom-designed, real time operating system that provides an integrated platform for its many functions, including:

- Stateful inspection firewall
- Traffic management
- Site-to-Site VPN using manual key authentication

ScreenOS does not support a programming environment.

5.1.4 Policies

`Juniper Networks Security Appliances` enforce information flow control decisions by defining policies which permit, deny, or tunnel information flows in accordance with the rules defined in each policy. All policies on a security appliance include the following attributes:

- Direction – The direction of traffic between two security zones (from a source zone to a destination zone)
- Source address – The address from which traffic initiates
- Destination address – The address to which traffic is sent
- Service – The type of traffic transmitted
- Action – The action that the security appliance performs when it receives traffic meeting the first four criteria: permit, deny, nat, or tunnel

The `Security Appliances` provide three different types of policies which support the information flow control decisions enforced by the TOE. This includes Interzone Policies, Intrazone Policies, and Global Policies.

5.1.4.1 Interzone policies

Interzone policies provide traffic control between security zones. You can set interzone policies to permit, deny, or tunnel traffic from one zone to another. Using stateful inspection techniques, the TOE maintains a table of active TCP sessions and active UDP "pseudo" sessions so that it can allow replies to service requests.

5.1.4.2 Intrazone Policies

Intrazone policies provide traffic control between interfaces bound to the same security zone. The source and destination addresses are in the same security zone, but reached via different interfaces on the TOE. Like interzone policies, intrazone policies control traffic flowing unidirectionally. To allow traffic initiated at either end of a data path, you must create two policies—one policy for each direction.

Intrazone policies do not support VPN tunnels or source network address translation (NAT-src) when it is set at the interface level (**set interface** *interface* **nat**). However, intrazone policies do support policy-based NAT-src and NAT-dst. They also support destination address translation when the policy references a mapped IP (MIP) as the destination address. A mapped IP address is a direct one-to-one mapping of traffic destined for one IP address to another IP address.

5.1.4.3 Global Policies

Unlike interzone and intrazone policies, global policies do not reference specific source and destination zones. Global policies reference user-defined Global zone addresses or the predefined Global zone address "any". These addresses can span multiple security zones. For example, if you want to provide access to or from multiple zones, you can create a global policy with the Global zone address "any", which encompasses all addresses in all zones.

5.1.4.4.1 Order of Invocation

When the TOE initiates a policy lookup, it first checks to see if the security zones are the same or different. If the zones are different, the TOE performs a policy lookup in the interzone policy set list. If the zones match, the TOE performs a policy lookup in the intrazone policy set. If a policy is not found within either the interzone or intrazone set lists, the TOE performs a policy lookup in the global policy set list.

5.1.4.4.1 Services

The `Security Appliances` enforce policies based on a service. A service specifies the protocol (TCP or UDP), the port number, the service group, the timeout and the flag associated to a specific service and maps the service to a defined name.

5.1.5 Security functionality

The `Security Appliances` offer the following security functions:

- *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. Both audit events and traffic messages can be further defined depending on the severity of the message and/or event.
- *Information Flow Policy*: Traffic flow from one network node to another network node is controlled by an information flow policy. This policy controls the flow of network traffic based solely upon the administratively configured rule set and information within network traffic and about the port upon which it arrives. If an authenticated information flow policy is enforced, then the information flow policy additionally utilizes cryptographic support for the authentication and protection of the information flows associated with the information flow policy.
- *Identification & Authentication*: The security appliances provide an authentication mechanism for administrative users through an internal authentication database. Administrative login is only supported through the locally connected console. The only authentication mechanisms supported by the TOE is passwords.
- *Security Management*: Every security appliance provides a command line administrative interface. To execute the CLI, an administrator must use a locally connected VT-100 terminal or workstation providing VT-100 terminal emulation to manage a security appliance through a direct serial connection. The authorized administrator must be successfully identified and authenticated before they are permitted to perform any security functions on the TOE.
- *TOE Protection*: Each security appliance is a hardware 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 preserves its configuration for a trusted recovery in the event that the configuration has been modified and not saved or if the security appliance has been ungracefully shutdown. The TOE additionally protects the session table by enforcing destination-based session limits and applying procedures to limit the lifetime of sessions when the session table reaches the defined watermark.

5.1.6 TOE configurations

The TOE supports a variety of configurations. The TOE provides three possible ways to configure a network interface. A network interface may be configured to operate in Transparent Mode, NAT Mode, or Route Mode. In addition, the TOE also supports Site-to-Site VPNs using a pre-shared key for authentication. These various configurations are further described below.

5.1.6.1 Interface Modes

The TOE supports three types of interface modes. These interface modes include a Transparent Mode, NAT Mode, and Route Mode each of which determine how packets are routed and filtered by the TOE. Each instance of the TOE can include one, a combination of, or all three interface modes. However, each individual network interface may only be configured with one interface mode and may not share a combination of or all three interface modes with one physical network interface. Each interface mode consistently satisfies all of the TOE security functional requirement claims identified in this ST. These three interface modes are further described below.

5.1.6.1.1 Transparent mode

When the TOE is configured in Transparent Mode, the TOE filters packets traversing the firewall without modifying any of the source or destination information in the IP packet header. All interfaces behave as though they are part of the same network, with the TOE acting much like a Layer 2 switch or bridge. In Transparent mode, the IP addresses of interfaces are set at 0.0.0.0, making the presence of the TOE invisible, or "transparent," to users.

Only Authenticated Transparent mode is supported by the TOE. Non-Authenticated Transparent mode is not supported by the TOE and should not be used.

5.1.6.1.2 NAT mode

When an ingress interface is in Network Address Translation (NAT) mode, the security appliance, acting like a Layer 3 switch (or router), translates two components in the header of an outgoing IP packet destined for the Untrust zone: its source IP address and source port number. The security appliance replaces the source IP address of the originating host with the IP address of the Untrust zone interface. Also, it replaces the source port number with another random port number generated by the security appliance.

When the reply packet arrives at the security appliance, the device translates two components in the IP header of the incoming packet: the destination address and port number, which are translated back to the original numbers.

The security appliance then forwards the packet to its destination. NAT adds a level of security not provided in Transparent mode: The addresses of hosts sending traffic through an ingress interface in NAT mode (such as a Trust zone interface) are never exposed to hosts in the egress zone (such as the Untrust zone) unless the two zones are in the same virtual routing domain and the security appliance is advertising routes to peers through a dynamic routing protocol (DRP). Even then, the Trust zone addresses are only reachable if you have a policy permitting inbound traffic to them. (If you want to keep the Trust zone addresses hidden while using a DRP, then put the Untrust zone in the untrust-vr and the Trust zone in the trust-vr, and do not export routes for internal addresses in the trust-vr to the untrust-vr.) If the security appliance uses static routing and just one virtual

router, the internal addresses remain hidden when traffic is outbound, due to interface-based NAT. The policies you configure control inbound traffic. If you use only mapped IP (MIP) and virtual IP (VIP) addresses as the destinations in your inbound policies, the internal addresses still remain hidden.

5.1.6.1.3 Route mode

When an interface is in Route mode, the security appliance routes traffic between different zones without performing source NAT (NAT-src); that is, the source address and port number in the IP packet header remain unchanged as it traverses the security appliance. Unlike NAT-src, you do not need to establish mapped IP (MIP) and virtual IP (VIP) addresses to allow inbound traffic to reach hosts when the destination zone interface is in Route mode. Unlike Transparent mode, the interfaces in each zone are on different subnets.

You do not have to apply source network address translation ("NAT-src") at the interface level so that all source addresses initiating outgoing traffic get translated to the IP address of the destination zone interface. Instead, you can perform NAT-src selectively at the policy level. You can determine which traffic to route and on which traffic to perform NAT-src by creating policies that enable NAT-src for specified source addresses on either incoming or outgoing traffic. For network traffic, NAT can use the IP address or addresses of the destination zone interface from a Dynamic IP (DIP) pool, which is in the same subnet as the destination zone interface. For VPN traffic, NAT can use a tunnel interface IP address or an address from its associated DIP pool.

5.1.7 VPN

Site-to-Site VPNs allow an organization to securely connect to a remotely connected network. The TOE supports and defines security claims for Transparent Mode, Route Mode and NAT Mode for utilizing Site-to-Site VPN connections using pre-shared key (PSK) authentication. In order to meet these security functional requirement claims, the TOE must have the appropriate VPN tunnels and permit filters allowing such connectivity and have the appropriate pre-shared key authentication credentials configured. The product supports various methods for VPN connectivity (i.e. Dialup VPN, L2TP VPN, Site-to-Site VPN), authentication (i.e. Manual Key, AutoKey), IPSEC Modes (i.e. Transport, Tunnel), and cryptographic algorithms (i.e. MD5, SHA-1, HMAC, DES, 3DES, AES). However, the evaluated configuration of the TOE requires that VPN connections are only configured as Site-to-Site VPNs using Manual Key authentication, also known as Pre-Shared Key authentication, using the IPSEC Tunnel Mode, and one of the following algorithms; MD5, SHA-1, HMAC, DES, 3DES, AES.

While the TOE defines security claims for Site-to-Site VPN connections, an organization is not bound to having VPN configured to meet the evaluated configuration of the TOE. If an organization does not wish to implement the Site-to-Site VPN functionality, then they may exclude it from their configuration of the TOE by ensuring that no VPN tunnels, permit filters, and pre-shared key credentials are established for such

connectivity. However in doing so, the organization will not be able to implement the security functionality of the TOE that satisfies the AUTHENTICATED TRANSPARENT MODE SFP or the AUTHENTICATED ROUTE MODE SFP defined in the ST [ST_AP_Rev_L].

5.1.7.1 Policy-Based VPN

Policy-Based VPNs define VPN tunnels through a "tunnel" policy action. A "tunnel" policy action always permits traffic to flow for traffic matching the related routes and services of the VPN tunnel policy.

5.1.7.2 Route-Based VPN

Route-Based VPNs define VPN tunnels using the routing table. For each VPN tunnel, a route is identified to where the VPN tunnel is invoked. Policies can be used in conjunction with the Route-Based VPN to explicitly permit or deny VPN tunnel access based on specified attributes, whereas the Policy-Based VPN only allows the capability to permit specific traffic to a VPN tunnel. Route-Based VPN's are not supported in Transparent mode and only Policy-Based VPN's can be used.

5.2 TOE Boundaries

The TOE includes both physical and logical boundaries.

5.2.1 Physical Boundaries

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

The security appliance attaches to a physical network that has been separated into zones through port interfaces.

Security appliances come in eleven models: 5GT, 5XT, 25, 50, 204, 208, 500, 1000, 2000, 5200, and 5400. Each model differs in the performance capability, however all provide the same security functionality. Each appliance enforces a security policy for all connection request and traffic flow between any two network zones. There are no direct connections between nodes in two separate zones except through the security appliance.

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 administrative console, which must be a VT-100 terminal or any device that can emulate a VT-100 terminal. The console is part of the TOE environment and it expected to correctly display what is sent to it from ScreenOS.

The physical boundary for the TOE is the physical port connections on the outside of the appliance's cabinet. One such port is the management port for the administrative console.

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 the security appliance, and from the security appliance to the receiving node in another network zone if the security policy allows the information flow.

Traffic from one network node in a zone will only be forward 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.

5.2.2 Logical Boundaries

The logical boundaries of the security appliances include the interfaces to communicate between the network nodes in one zone with network nodes in other zones. Security policies are applied to interzone and intrazone information flows.

5.2.2.1 Zone

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).

5.2.2.1.1 Security Zone

A security zone is a segment of network space to which security measures are applied. Multiple security zones can be configured on a single security appliance by sectioning the network into segments to which various security policies may be applied to satisfy the needs of each segment. At a minimum, two security zones must be identified, basically to protect one area of the network from the other. Many security zones can also be established to bring finer granularity to a network security design, without deploying multiple security appliances to do so.

Each security appliance is also configured with a Global Zone. A Global Zone is a security zone without a security zone interface. The Global zone serves as a storage area for mapped IP (MIP) and virtual IP (VIP) addresses. The predefined Global zone address "Any" applies to all MIPs, VIPs, and other user-defined addresses set in the Global zone. Because traffic going to these addresses is mapped to other addresses, the Global zone does not require an interface for traffic to flow through it.

5.2.2.1.1.1 Security Zone Interface

A security zone interface is an interface in which information can be sent to and from a security zone. Security zones support five types of security zone interfaces, which include physical interfaces, subinterfaces, aggregate interfaces, redundant interfaces, and virtual

security interfaces. However, the evaluated configuration of the TOE may only utilize the physical interfaces, aggregate interfaces, and redundant interfaces.

5.2.2.1.1.1.1 Physical Interface

Each physical network port on the security appliance represents a physical interface, and the name of the interface is predefined. The name of a physical interface is composed of the media type, slot number (for some security appliances), and port number, for example, ethernet3/2 or ethernet2. A physical interface can bind to any security zone where it acts as a doorway through which traffic enters and exits the zone. Without a physical interface, no traffic can access the zone or leave it.

5.2.2.1.1.1.2 Aggregate Interface

The Juniper Networks NetScreen-5000 series supports aggregate interfaces. An aggregate interface is the accumulation of two or more physical interfaces, each of which shares the traffic load directed to the IP address of the aggregate interface equally among them. By using an aggregate interface, the amount of bandwidth available to a single IP address can be increased. Also, if one member of an aggregate interface fails, the other member or members can continue processing traffic, although with less bandwidth than previously available.

5.2.2.1.1.1.3 Redundant Interface

A redundant interface consists of binding two physical interfaces together to create one redundant interface, which you can then bind to a security zone. One of the two physical interfaces acts as the primary interface and handles all the traffic directed to the redundant interface. The other physical interface acts as the secondary interface and stands by in case the active interface experiences a failure. If that occurs, traffic to the redundant interface fails over to the secondary interface, which becomes the new primary interface. The use of redundant interfaces provides a first line of redundancy before escalating a failover to the device level.

5.2.2.1.2 Tunnel Zone

A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is conceptually affiliated with a security zone in a “child-parent” relationship. The security zone acting as the “parent”, provides the firewall protection to the encapsulated traffic. The tunnel zone provides packet encapsulation/decapsulation, and by supporting tunnel interfaces with IP addresses and netmasks that can host mapped IP (MIP) addresses and dynamic IP (DIP) pools, can also provide policy-based NAT services. The security appliance uses the routing information for the carrier zone to direct traffic to the tunnel endpoint. The default tunnel zone is Untrust-Tun, and it is associated with the Untrust zone. Other tunnel zones can be created and bound to other security zones, with a maximum of one tunnel zone per carrier zone per virtual system. Virtual systems, however, are outside the scope of the evaluated configuration.

5.2.2.1.2.1 Tunnel Interfaces

A tunnel interface acts as a doorway to a VPN tunnel. Traffic enters and exits a VPN tunnel via a tunnel interface.

When you bind a tunnel interface to a VPN tunnel, you can reference that tunnel interface in a route to a specific destination and then reference that destination in one or more policies. With this approach, you can finely control the flow of traffic through the tunnel. It also provides dynamic routing support for VPN traffic. When there is no tunnel interface bound to a VPN tunnel, you must specify the tunnel in the policy itself and choose **tunnel** as the action.

Outbound traffic enters the tunnel zone via the tunnel interface, is encapsulated, and exits via the security zone interface. Inbound traffic enters via the security zone interface, is decapsulated in the tunnel zone, and exits via the tunnel interface.

5.2.2.1.3 Function Zone

The function zone is a zone that performs a specific function. Functional zones support five types of zones, which include null zones, MGT zones, HA zones, self zones, and VLAN zones. However, the evaluated configuration of the TOE may only utilize the null zones and self zones. Each zone exists for a single purpose, as explained below.

5.2.2.1.3.1 Null Zone

This zone serves as temporary storage for any interfaces that are not bound to any other zone.

5.2.2.1.3.2 Self Zone

This zone hosts the interface for remote management connections. When you connect to the security appliance via HTTP, SCS, or Telnet, you connect to the Self zone. Remote management is not supported in the evaluated configuration of the TOE and therefore, also excludes Self Zones.

5.2.2.2 Loopback Interfaces

A loopback interface is a virtual interface that can be used either as a redundancy feature for binding a logical interface to more than one physical network interface, or as a management feature for providing an interface that can be dedicated to provide specific hosts the capability to manage the TOE. Since the evaluated configuration of the TOE restricts the use of remote management, loopback interfaces cannot be used to provide remote management of the TOE. However, loopback interfaces can be used to provide redundancy between to physical network interfaces which can assist in the enforcement of the information flow policies defined.

5.2.2.3 Audit

Security appliances categorize auditing information into three categories, 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. When logging and counting are enabled for a policy, all traffic will be logged to the traffic log. Self logs store information on traffic that is dropped and traffic that is sent to the device. For example, if you disable some management options on an interface—such as WebUI, SNMP, and ping—and HTTP, SNMP, or ICMP traffic is sent to that interface, entries appear in the self log for each dropped packet.

Buffer storage on the device is broken into the following categories. There are two buffers for event logs, one for basic logs and one for alarms. There are also two buffers for traffic & self logs, one for traffic/self logs for traffic information and one for traffic/self events or alarms. The first tracks network traffic while the second stores information on alarms. Traffic/self alarms can be set in the policy such that when more traffic matches the policy than is configured in the policy alarm field, then an alarm will be logged.

The audit logs are stored in memory because of the large storage capacity. Security appliances also can simultaneously send audit records to SDRAM and a remote syslog as a backup device to the audit log and an administrator controls this backup. The platform and storage device that control the syslog are not part of the TOE.

5.2.2.4 Information Flow Protection

By default, a security appliance denies all traffic in all directions. [1] Through the creation of information flow policies, traffic flow across an interface can be controlled by defining the kinds of traffic permitted to pass from one security zone to another. In addition, the NAT and Route mode configurations also control traffic across an interface by defining the kinds of traffic permitted to pass between hosts within the same security zone.

The information flow policy is supported by allowing an administrator to define information flow policies that specify which network nodes within a specific zone can communicate with which other network nodes in other zones or within the same zone. Once a connection is established, access that is granted to another network node is controlled by an information flow policy. At a minimum, this information flow policy enforces a policy based on the following:

- Addresses (source and destination),
- Service[2] (port or groups of ports, such as port 80 for HTTP, or service name such as FTP, or service data type such as ftp-get), and
- Network Interface (i.e. from zone and to zone, direction).

Additionally, if a security appliance attempts to connect to another security appliance using Site-to-Site VPN, the security appliance establishing the connection must use a manual key consistent with the manual key configured on the destination security

[1] When ScreenOS is installed on all security appliance models, no traffic flow is the default except for the Juniper Networks NetScreen-5GT, and 5XT, which will allow traffic from the Trust network to the Untrust network by default, therefore during the install process an administrator is instructed to establish traffic flow parameters to specifically allow intentional flows and to disallow all other information flows. Since this setup occurs before the NetScreen appliance is operational and begins enforcing the SFP, the default that provides no information flow without explicit approval holds true.

[2] A service also specifies the protocol (TCP or UDP) used for the specific type of service defined.

appliance before access is granted to establish the VPN tunnel. Once a VPN tunnel is successfully established, the information flow policy is enforced.

While the information flow policies stated in FDP_IFC.1a, FDP_IFC.1b, and FDP_IFC.1c of the ST [ST_AP_Rev_L] are indicated to be optional, at least one of the three information flow policies identified must be enforced to remain within the evaluated configuration and compliant to the TFFPP requirements.

5.2.2.5 Identification & Authentication

The following three administrative roles are included in the evaluated configuration,[3] although they are treated collectively as a single "authorized administrator" role:

- Root administrator
- Read/Write Administrator
- Read-only Administrator

Each administrator must log on using the console locally connected to the security appliance. A known administrator user name and its corresponding password must be entered correctly in order for the administrator to successfully logon and thereafter gain access to administrative functions. All administrator user name and password pairs are managed in a database internal to the security appliance.

5.2.2.6 Security Management

Every security appliance provides a command line administrative interface. A locally connected console; a VT-100 terminal or a workstation providing VT-100 terminal emulation may be used to enter administrative commands. The console used to enter administrative commands is in the environment and not part of the TOE. No other management connections are supported as part of the TOE.

Security management functions are restricted to administrators by supporting only administrator accounts and also by requiring that administrators log into their accounts prior to gaining access to those functions.

5.2.2.7 TOE Self Protection

Some of the TOE self-protection (e.g., against physical tampering) is ensured by its environment. In particular, it is assumed that security appliances will remain attached to the physical connections made by an administrator so that an appliance cannot be bypassed. Each security appliance is completely self-contained in that the hardware and firmware developed by Juniper provide all the services necessary to implement the TOE. There are no external interfaces into the TOE other than the well-defined physical ports. There is no general purpose computing capabilities that might offer an opportunity for a user to bypass or otherwise corrupt the TOE.

[3] There are also two VSYS administrative roles (VSYS Administrator and VSYS Read-only Administrator), but these are not in the evaluated configuration, and administrators are directed not to use these if they wish to remain in the evaluated configuration.

The TOE configuration protects its management functions by isolating them using identification and authentication and by limiting them exclusively to the local console port.

Logically, each security appliance is protected largely by virtue of the fact that its interface supports network traffic, but none of that traffic is interpreted as being directed at the security appliance itself. For example, there is no support for remote administration of the TOE that would effectively open a logical interface from the untrusted user environment to the TOE itself.

Additionally, the TOE protects its session table by enforcing destination-based session limits and watermarks for limiting the time a session may live when the session table reaches the specified watermark. The TOE also provides a trusted recovery function for cases when the configuration is modified or the system is ungracefully shutdown.

5.3 Documentation

The following documentation supported the evaluation of the TOE.

Guidance documentation

Reference Guide

Juniper Networks NetScreen CLI Reference Guide, Version 5.0.0 Command Descriptions, P/N 093-1352-000, Rev A

Concepts and Examples Document Set

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 2

Fundamentals Screen OS 5.0.0 P/N 093-1345-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 3

Administration, P/N 093-1346-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: Attack Detection and Defense Mechanisms, P/N 093-1347-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 5: VPNs, P/N 093-1348-000, Revision A

Audit Record Description Document

NetScreen Message Log Reference Guide, ScreenOS Version 5.0.0, P/N 093-1353-000, Revision A

User's Guides

NetScreen-5XT User's Guide, Version 5.0, P/N 093-1323-000, Revision A NetScreen-25 User's Guide, Version 5.0, P/N 093-1245-000, Revision A NetScreen-50 User's Guide, Version 5.0, P/N 093-1249-000, Revision A NetScreen-200 Series User's Guide, Version 5.0, P/N 093-1253-000, Revision A NetScreen-500 User's Guide, Version 5.0, P/N 093-0973-000, Revision A NetScreen-5000 User's Guide, Version 5.0, P/N 093-1216-000, Revision A <u>Release Notes</u> NetScreen Release Notes ScreenOS 5.0.0r9, P/N 093-1459-000, Revision A
Delivery and Operation documentation Juniper Networks Common Criteria EAL4 Delivery of the Product to Buyer, Document Number 093-1557-000, Revision C
Design documentation Juniper Networks Security Appliances Functional Specification for Common Criteria for EAL4 & EAL4+, Document Number 093-1548-000, Revision G, 10/17/2005 Juniper Networks Security Appliances High Level Design Document for Common Criteria for EAL4 & EAL4+, Document Number 093-1549-000, Revision E, 10/17/2005 Juniper Networks Common Criteria LLD Master, P/N 093-1550-000, Revision F, 10/18/2005 Juniper Networks Correspondence Matrix for Common Criteria EAL4, Document Number 093-1551-000, Revision E, 10/18/2005 Juniper Networks Audit Loss Mitigation, 093-0853-000, Revision B, 5/27/2005 Juniper Networks Security Appliances Informal Security Policy Model for Common Criteria EAL4 & EAL4+, Document Number 093-1552-000, Revision D, 10/18/2005
Configuration Management documentation Juniper Networks Common Criteria EAL4 Configuration Management Plan, Document Number 093-1527-000, Revision B
Life Cycle documentation

Juniper Networks Life Cycle Process for Common Criteria, Document Number 093-1550-000, Draft A, 2/16/2005
Test documentation Juniper Networks Correspondence Matrix for Common Criteria, P/N 093-1551-000, Revision E Juniper Networks Screen OS 5.0 Test Plan, Procedures, Results And Correspondence, P/N 093-1554-000, Revision H
Vulnerability Assessment documentation Juniper Networks Security Appliances NetScreen Vulnerability Assessment Plan and Report for Common Criteria, Document Number 093-1556-000, Revision B, 7/12/2005 Misuse Document for Common Criteria, Document Number 093-1558-000, Revision A
Security Target Juniper Networks Security Appliances Security Target EAL4, P/N 093-0896-000, Revision L, December 19, 2005

Table 4. Documentation

6 IT Product Testing

Testing of the Juniper `Security Appliances` took place at Juniper Networks, Inc., Sunnyvale, CA, during November 2005.

The SAIC evaluation team executed a subset of the developer tests, as well as tests they devised. Testing covered each security functional component claimed for the TOE, and demonstrated the validity of each component.

The SAIC evaluation team also performed penetration testing as required at EAL4.

Testing details are SAIC and Juniper Networks, Inc., proprietary and, as such, are not provided in this VR.

The following Juniper Networks Security Appliances have received FIPS 140-2 certification: NetScreen-5400 (Certificate No. 605); NetScreen-5200 (Certificate No. 603); NetScreen-500 (Certificate No. 604); NetScreen-208 (Certificate No. 607); NetScreen-204 (Certificate No. 607); NetScreen-5GT (Certificate No. 629); and

NetScreen-5XT (Certificate No. 606). For this evaluation, it was appropriate for the Security Target to claim compliance with the external standard for DES, TDES, AES, and SHA for the Juniper Networks ISG 1000 and ISG 2000 products; and to claim compliance with the external standard for AES, TDES, DES, DSA, SHS, RSA, HMAC, and RNG for the Juniper Networks NetScreen-25 and NetScreen-50 products. There are many ways of determining compliance with a standard. Juniper Networks has chosen to make a developer claim of compliance. This means there has been no independent verification (by either the evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithm actually meets the claimed standard. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements.

7 Evaluated Configuration

The evaluated configuration of `Juniper Networks Security Appliances` is one or more of the following appliances:

- Juniper Networks NetScreen-5GT (Part number: NS-5GT-00*, NS-5GT-10*, NS-5GT-20*, where * = 1, 3, 5, 7, 8)
    - Firmware version: 5.0.0r9.r
    - Hardware version: 1010
- Juniper Networks NetScreen-5XT (Part number: NS-5XT-00*, NS-5XT-10*, where * = 1, 3, 5, 7, or 9)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 1010
- Juniper Networks NetScreen-25 (Part number: NS-025-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 4010
- Juniper Networks NetScreen-50 (Part number: NS-050-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 4010
- Juniper Networks NetScreen-204 (Part number: NS-204-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 0110

- Juniper Networks NetScreen-208 (Part number: NS-208-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 0110
- Juniper Networks NetScreen-500 (Part number: NS-500-SK1, NS-500ES-GB1-**, NS-500ES-GB2-**, NS-500SP-GB1-**, NS-500SP-GB2-**, NS-500ES-FE1-**, NS-500ES-FE2-**, where ** = AC or DC)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 4110
- Juniper Networks ISG 1000 (Part number: NS-ISG 1000-PO*-S00, NS-ISG 1000B-PO*-S00, where * = 0A, 1A, 2A, or 3A)
    - Firmware version: 5.0.0r9.y
    - Hardware version: 3010
- Juniper Networks ISG 2000 (Part number: NS-ISG 2000-PO*-S00, NS-ISG 2000B-PO*-S00, where * = 0A, 1A, 2A, or 3A)
    - Firmware version: 5.0.0r9.y
    - Hardware version: 3010
- Juniper Networks NetScreen 5200 (Part number: NS-5200-P00*-**, NS-5200-P01*-**, NS-5200-P10*-**, NS-5200-P11*-**, where * = A or D, and ** = S00, S01, or S02)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 3010
- Juniper Networks NetScreen 5400 (Part number: NS-5400-P00*-**, NS-5400-P01*-**, NS-5400-P10*-**, NS-5400-P11*-**, where * = A or D, and ** = S00, S01, or S02)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 3010

8 Results of the Evaluation

The SAIC Evaluation Team followed the procedures outlined in *Guidance to CCEVS Approved Common Criteria Testing Laboratories*, Scheme Publication #4, Version 1.0, March 20, 2001 [CCEVS4].

The Evaluation Team concluded that (a) the ST [ST_AP_Rev_L] is *Common Criteria* V2.1 conformant, and (b) the TOE is *Common Criteria* V2.1 Part 2 and Part 3

conformant, and recommended that an EAL4 certificate rating be issued for the Juniper Networks Security Appliances.

9 Validator Comments/Recommendations

- The Validator attended TOE testing at Juniper Networks, Inc., Sunnyvale, CA, during November 2005.

- The documentation provided by Juniper Networks, Inc., in support of this evaluation, was of excellent quality.

- The following Juniper Networks Security Appliances have received FIPS 140-2 certification: NetScreen-5400 (Certificate No. 605); NetScreen-5200 (Certificate No. 603); NetScreen-500 (Certificate No. 604); NetScreen-208 (Certificate No. 607); NetScreen-204 (Certificate No. 607); NetScreen-5GT (Certificate No. 629); and NetScreen-5XT (Certificate No. 606). For this evaluation, it was appropriate for the Security Target to claim compliance with the external standard for DES, TDES, AES, and SHA for the Juniper Networks ISG 1000 and ISG 2000 products; and to claim compliance with the external standard for AES, TDES, DES, DSA, SHS, RSA, HMAC, and RNG for the Juniper Networks NetScreen-25 and NetScreen-50 products. There are many ways of determining compliance with a standard. Juniper Networks has chosen to make a developer claim of compliance. This means there has been no independent verification (by either the evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithm actually meets the claimed standard. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements.

10 Annex

10.1 *URLs*

- Common Criteria Evaluation and Validation Scheme (CCEVS)
  (www.niap.nist.gov/cc-scheme).

- Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL)
  (www.saic.com/infosec/cctl/)

- Juniper Networks, Inc.
  (www.juniper.net)

10..2 *Common Criteria/CCEVS Documents*

[CCV2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

[CEMV1.0] *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999, CEM-99/045.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, February 2002.

[CCEVS4] *Guidance to CCEVS Approved Common Criteria Testing Laboratories*, Scheme Publication #4, Version 1.0, March 20, 2001.

[PP_Low_Risk] *U.S. Government Traffic-Filter Protection Profile for Low-Risk Environments*, Version 1.1, April 1999.

11 Security Target

[ST_AP_Rev_L] *Juniper Networks Security Appliances Security Target: EAL4,* Revision L, P/N-093-0896-000, December 19, 2005.

12 Glossary

Acronym	Expansion
ASIC	Application-Specific Integrated Circuit
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.1, August 1999.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPU	Central Processing Unit
DIP	Dynamic IP
DRP	Dynamic Routing Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol

IPsec	IP Security
IT	Information Technology
MIP	Mapped IP
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SAIC	Science Applications International Corporation
SDRAM	Synchronous Dynamic Random Access Memory
SNMP	Simple Network Message Protocol
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFFPP	Traffic-Filter Firewall Protection Profile *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, April 1999.
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Datagram Protocol
VPN	Virtual Private Network
VR	Validation Report