National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks, Inc.

Juniper Networks Secure Access 5000 Family 5.1R2

Report Number: **CCEVS-VR-05-0132**
Dated: **December 16, 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

Common Criteria Testing Laboratory

Science Applications International Corporation
7125 Gateway Drive
Columbia, MD 21046

Evaluation Team

Cynthia Reese
Dawn Campbell

Table of Contents

1 Executive Summary

The purpose of this Validation Report (VR) is to document the results of the EAL2 evaluation of `Juniper Networks Secure Access Family 5.1R2` (hereafter `Secure Access`), a product of Juniper Networks, Inc., Sunnyvale, CA.

This Validation Report is not an endorsement of `Secure Access` by any agency of the United States Government, and no warranty of the product is either expressed or implied.

Evaluation of `Secure Access` at EAL2, 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 TOE, which consists of one or more of the following appliances, is identified as the Juniper Networks Secure Access Family, Release 5.1R2.

- Juniper Networks SA 2000, Release 5.1R2
- Juniper Networks NetScreen-SA 3000 FIPS, Release 5.1R2
- Juniper Networks SA 4000, Release 5.1R2
- Juniper Networks NetScreen-SA 5000 FIPS, Release 5.1R2
- Juniper Networks SA 6000, Release 5.1R2

The `Secure Access` appliances are designed and manufactured by Juniper Networks, Inc. The TOE is completely self-contained, housing the software and hardware necessary to perform all functions. The differences between appliance models have no affect on the security functions claimed in the Security Target [STSA1.1]. Model variations are associated with differences in throughput and redundancy.

`Secure Access` acts as a secure application-layer gateway intermediating requests between remote computers and internal corporate resources. All requests from remote computers to a `Secure Access` appliance, and from a `Secure Access` appliance to remote computers, are encrypted as per the Triple Data Encryption Standard (TDES), with cryptographic key sizes 168 binary digits in length. Each request is subject to administratively-defined access control and authorization policies before the request is forwarded to an internal resource.

`Secure Access` supports the roles User, User Admin, Administrator, and Read-Only Administrator. All users are required to be identified and authenticated before any information flows are permitted. Users gain authenticated access to authorized resources via an extranet session hosted by the appliance, and can access Web-based enterprise applications, Java applications, file shares and terminal hosts from any Internet-connected Web browser.

Secure Access generates audit records for security events. The Administrator and Read-Only Administrator are the only roles with access to the audit trail.

Secure Access provides an information flow security policy. The security policy limits traffic (e.g., URLs and resource types, such as file servers) to specific user roles.

Secure Access provides a wide range of security management functions. Administrators can configure the TOE and manage users, the information flow policy, and audit.

Secure Access protects itself by providing well-defined network interfaces for user access, and requiring all users to be identified and authenticated before any information flows are permitted. Additionally, only trusted software runs on the TOE, assuring that the TOE maintains a domain for its own execution.

The TOE includes security functions implemented at the TOE interfaces, as follows:

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

A Strength of Function claim of SOF-medium is made for Secure Access.

The cryptography used in this product has not been FIPS certified, not has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The Secure Access TOE was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004 [CCV2.2], and the *Common Methodology for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004 [CEMV2.2]. 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 Secure Access is contained within the document *Juniper Networks Secure Access Family 5.1R2 Security Target,* Version 1.0, 12/16/2005 [STSA1.1].

The project, which also involved evaluation of the associated Security Target, was completed on December 16, 2005.

1.1 Interpretations

There are no interpretations incorporated into the evaluation.

1.2 Threats to Security

The Security Target [STSA1.1] identifies the following threats that the evaluated product addresses:

Threat	Description
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 modify the behavior of TSF data without being detected.
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.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
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.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.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 replay valid identification and authentication data obtained while monitoring the TOE's network interface to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

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 SA 2000, SA 4000, and SA 6000, all release 5.1R2, and Juniper Networks NetScreen-SA 3000 FIPS and NetScreen-SA 5000 FIPS, both release 5.1R2.
Security Target	*Juniper Networks Secure Access Family 5.1R2 Security Target,* Version 1.0, 12/16/2005 [STSA1.1]
CC Identification	*Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004. [CCV2.2]
CEM Identification	*Common Methodology for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004. [CEMV2.2]

Item	Identifier
Interpretations	There are no applicable interpretations.
Evaluation Technical Report	Provided by the SAIC Evaluation Team, December 2005.
Conformance Result	Security Target, [STSA1.1]: [CCV2.2] conformant; TOE (Juniper Networks SA 2000, SA 4000, and SA 6000, all release 5.1R2, and Juniper Networks NetScreen-SA 3000 FIPS and NetScreen-SA 5000 FIPS, both release 5.1R2), [CCV2.2] Part 2 and Part 3 conformant.
Sponsor	Juniper Networks, Inc., Sunnyvale, CA
Developer	Juniper Networks, Inc., Sunnyvale, CA
Evaluators	Cynthia Reese and Dawn Campbell, Science Applications International Corporation (SAIC), Columbia, MD
Validator	Timothy J. Bergendahl, The MITRE Corporation, Bedford, MA

Table 1. Evaluation identifiers.

3 Security Policy

The security policy for the `Secure Access` TOE is as follows.

- Security audit
- Cryptographic support
- User data protection
- Identification and Authentication
- Security Management
- Protection of the TSF

Security audit functionality provides the capability to create audit records for selected events; an understandable audit trail; and prevention of audit data loss.

Cryptographic support is enforced by assuring that all requests from remote computers to a `Secure Access` appliance, and from a `Secure Access` appliance to remote computers, are encrypted as per the Triple Data Encryption Standard (TDES), with cryptographic key sizes 168 binary digits in length.

User data protection is enforced by enforcing the AUTHENTICATED USER SFP on users, traffic sent through the TOE from a user on the external network to a resource on the internal network.

Identification and Authentication is enforced by requiring each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

Security Management is enforced by providing the roles User, User Admin, Administrator, and Read-Only Administrator, and being able to associate each user with one of these roles; by providing TSF-controlled management functions such as start-up and shutdown, time/date modification, and create, delete, modify, and view information flow security policy rules; and the ability to associate TSF-controlled management functions with an authorized administrator.

Protection of the TSF is enforced by the TOE by maintaining a security domain for its own execution that protects it from interference and tampering by untrusted subjects; by assuring that TSP enforcement functions are successfully invoked before each function within the TSC is allowed to proceed; and by providing reliable time stamps.

4 Assumptions

The Security Target [STSA1.1] identifies the assumptions about the environment of the TOE.

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.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.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSEC	The TOE is physically secure.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

Table 2. Assumptions.

5 Architectural Information

5.1 Architectural description

An image of the SA 6000 appliance is shown in *Figure 1*. Release 5.1R2 of this appliance is one of the evaluated products identified in *Table 1*.

Figure 1. SA 6000

The following description of the Secure Access architecture is based on the description presented in the documents (a) *Final Evaluation Technical Report for the Juniper Networks Secure Access Family 5.1R2*, Part 1 (Non-Proprietary), Version 0.1, 12/9/05 and (2) the ST [STSA1.1].

5.1.1 Secure Access Components

Secure Access contains four major components as follows:

- Content Intermediation Engine
- Protocol Connectors
- Secure Content Server
- System Data Store and Load Balancing System

The components are depicted in *Figure 2*, with descriptions provided in subsections 5.1.1.1 through 5.1.4.

5.1.1.1 Content Intermediation Engine

The Content Intermediation Engine is the core of Secure Access. It consists of:

- **Parsers** - Event-driven components that process resource data streams and decompose them into "chunks" that are manipulated by associated transformers

- **Transformers** - Components that receive the "chunks." The transformers have the opportunity to modify each chunk in the data stream before writing it out to the Request Handler

- **Connectors** - Components that use protocol adapters to retrieve resource and application data streams, such as documents on file servers, HTML pages on the intranet servers, or messages from an MS Exchange server

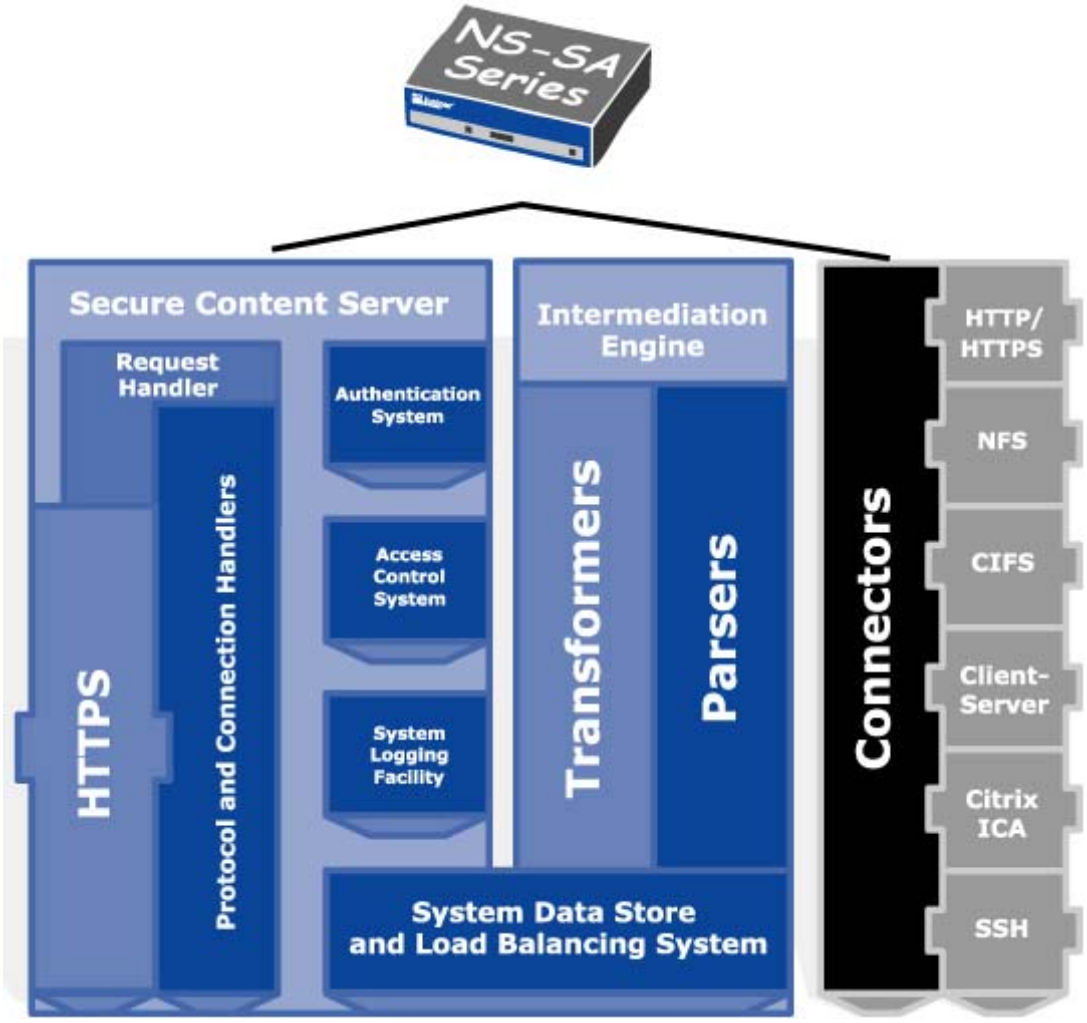

Figure 2. TOE Architecture

Web requests provide the clearest example of the Content Intermediation Engine at work, but generally speaking, support for most content types and application protocols uses a similar approach:

- The file sharing application for remote access to Windows shares and NFS volumes uses a backend connector, and the directory and file meta-data is transformed into a Web view of the volume.
- The client-server application and messaging application support uses backend connectors to communicate with mail servers, messaging servers, and other servers. These messages are transformed into the secure Web protocols before they are written out to the Request Handler.
- The support for Web resources uses a Connector to read HTML and other content streams from an internal HTTP server in addition to a Parser and a Transformer.

5.1.1.2 Protocol Connectors component

Each supported content type has an associated protocol connector. These connectors communicate with the content parsers and with the native content servers. For example, the file share connector communicates with MS Windows file servers through the CIFS protocol over TCP and with UNIX file server through NFS over UDP. In order to enforce native access controls, an additional component connects to the MS NT Domain Controller or UNIX NIS server. Currently Juniper supports connectors for:

- CIFS
- Citrix ICA
- HTTP/HTTPS
- IMAP
- Lotus Notes
- MS MAPI
- NFS
- POP
- SMTP
- Socket-dependent Java applets
- SSH
- Telnet
- URL-dependent Java applets

5.1.1.3 Secure Content Server component

The Secure Content Server provides the core of the security features offered by SA, and consists of the following components:

- Access Control System
- Authentication System
- Protocol and Connection Handlers
- Request Handler
- System Logging Facility
- Web Server

The Access Control System provides access control enforcement on requests to resources protected by the TOE. The Access Control System determines if an authenticated user will be allowed or denied access to a requested resource. When an authenticated user makes a request to the backend resources available to the role associated with the authenticated user, the appliance evaluates the corresponding resource policies. A resource policy is a set of resource names (such as URLs and hostnames) to which you grant or deny access or other resource-specific actions, such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of access features and resources (such as bookmarks and applications), whether or not a user can access a specific resource is controlled by

resource policies. These policies may even specify conditions that, if met, either deny or grant user access to a server share or file.

The Authentication System provides identification and authentication capabilities for authenticating both administrators and users. The Authentication System performs authentication using authentication realms. However, separate authentication databases are used for administrator and user accounts. An authentication realm is a grouping of authentication resources, including:

- An authentication server, which verifies that the user is who he claims to be. An Instant Virtual Extranet (IVE) appliance forwards credentials that a user submits on a sign-in page to an authentication server.
- An authentication policy, which specifies realm security requirements that need to be met before an IVE appliance submits a user's credentials to an authentication server for verification.
- A directory server, which is an LDAP server that provides user and group information to an IVE appliance that the appliance uses to map users to one or more user roles.
- Role mapping rules, which are conditions a user must meet in order for an IVE appliance to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

The Protocol and Connection Handlers provide the necessary protocol negotiations to the end user for the specific protocol being used.

The Request Handler runs within the `Secure Access` appliance. The Request Handler works with the system software and other components to ensure that content can be projected to authorized users in a secure fashion:

- `Secure Access` uses “cookie trapping.” All Web cookies are maintained on the server, and a single session token is transmitted to the Web browser. This feature ensures that no cookie-based session information, stored credentials, or application meta-data leaves the corporate network.
- The `Secure Access` session token expires when the session becomes idle or the user signs out.
- HTTP headers with all sensitive content contain the Cache-Control directive “no-cache,” which prevents them from being stored on the client machine in standard browsers.
- All form fields intermediated by the device includes the autocomplete=”off” attribute to prevent values from being stored on the client machine.

The System Logging Facility provides logging capabilities for recording the access decisions resulting from resource requests initiated by authenticated users. The System Logging Facility also provides logging capabilities for recording the access decisions resulting from the actions performed by authenticated administrators.

The Web Server provides an interface to users for using the TOE to access resources protected by the TOE, and provides an interface to administrators for managing the TOE and its security functions. The Web Server also provides the HTTP protocol that is used for both the user and administrator interfaces to receive/transmit and encrypt/decrypt data to or from the TOE.

5.1.1.4 System Data Store component

All data stored on the device is encrypted using AES, however, the protection of the AES encryption is outside of the scope of the TOE. Only the `Secure Access` system software can read the encrypted data store. Further, users and administrators cannot replace arbitrary executable files, and they do not have system-level accounts, so potential attackers cannot employ privilege-elevation attacks against the appliance.

5.1.2 `Secure Access` Subsystems

The `Secure Access` design documentation describes the following subsystems:

- Auditing Management Subsystem – manages the audit log (provides access to the audit logs and configures the audit functionality).
- System Management Subsystem – offers the system management capabilities such as performing archiving of the Events log, User Access log, and Admin Access log, restarting, rebooting, and shutting down the server, session encryption management, enable/disable external IT entities from communicating to the TOE, and time & date management.
- User Management Subsystem – offers the user management capabilities such as managing users, roles, user password restrictions, sessions, and enforcing authentication.
- Policy Enforcement Subsystem - offers the capabilities for managing and enforcing resource policies. TSF Protection Subsystem
- TSF Protection Subsystem - offers the capabilities for protecting TOE security functions from residual information, protecting TOE security functions from being bypassed, providing a domain of separation, and providing TSF-initiated session termination.

The subsystems support the following security functions of the TOE, as described in the Security Target [STSA1.1]

- Security Audit
- Cryptographic Support
- User Data Protection

- Identification and Authentication
- Security Management
- Protection of the TSF

5.2 TOE Boundaries

5.2.1 Physical Boundaries

The TOE physical boundary is the appliance itself. The TOE is completely self-contained, housing the software and hardware necessary to perform all functions. The TOE has two logical interfaces: end user and admin interface. The admin interface to the TOE includes both a terminal console and a Web-Based administrative interface. The end user interfaces to the TOE using a Web-Based user interface.

The TOE includes a proprietary web server developed by Juniper which is part of the Secure Content Server and provides the main interface for both users and administrators of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE.

The TOE also utilizes a Linux operating system that is based on the Red Hat Linux 7.3 distribution and includes the 2.4 kernel. The operating system is relied upon for all access to the physical hardware devices connected to the TOE and for providing reliable time stamping.

The TOE boundaries are depicted in the *Figure 1*. The TOE components are identified with a gray background. The TOE components consist of the Secure Content Server, Web Server, Intermediation Engine, Protocol Connectors, an internal and external Network Interface Card (NIC), Hard Disk, Memory, Central Processing Unit (CPU), System Data Store, Operating System, and Real Time Clock (RTC). The non-TOE components are identified with a white background. These non-TOE components consist of clients and protected resources. Clients exist outside the TOE and connect to the TOE through the external NIC, which is open to the Internet for allowing this connectivity. Protected resources consist of file, web, and email resources, which are added to the TOE by administrators in an operational environment. These protected resources are located within the System Data Store, which is accessible from the internal NIC. Such resources are considered outside the scope of the TOE.

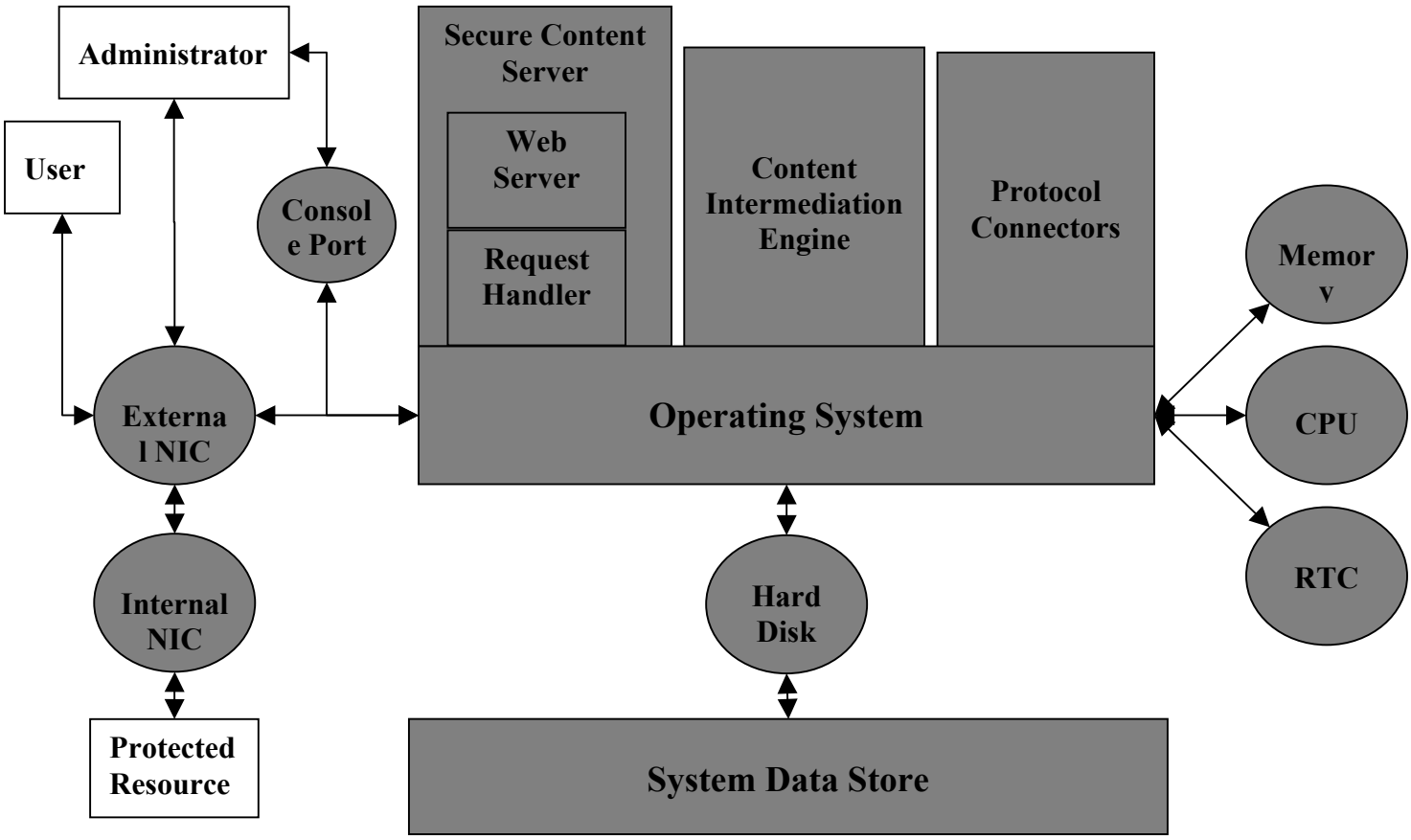

Figure 1. TOE Physical Boundaries.

5.2.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include Security Audit, Cryptography Support, User Data Protection, Identification and Authentication for the administrative functions, the management of the security configurations and the self-protection of the TOE itself.

Security Audit
`Secure Access` generates audit records for security events. The administrator and read-only administrator are the only roles with access to the audit trail and have the ability to view the audit trail.

Cryptographic support
`Secure Access` supports secure communications between users and the TOE. This encrypted traffic prevents modification and disclosure of user information.

User data protection
Secure Access provides an information flow security policy. The security policy limits traffic to URLs and resource types, such as file servers, to specific user roles.

Identification and Authentication
All users are required to perform identification and authentication before any information flows are permitted. Additionally, administrators must be authenticated before performing any administrative functions.

Security Management
Secure Access provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.

Protection of the TSF
Secure Access protects itself by providing well-defined network interfaces for user access and requiring all users to perform identification and authentication before any information flows are permitted. Additionally, no untrusted software runs on the TOE which ensures the TOE maintains a domain for its own execution.

5.3 Documentation

The following documentation supported the evaluation of the TOE.

Guidance documentation • Juniper Networks Secure Access family 5.1R2 Evaluated Configuration Guide, Version 0.7.1, 2/17/2006 • NetScreen Secure Access, NetScreen Secure Access FIPS, NetScreen Secure Meeting Administration, release 5.0, Part Number 500B051605
Delivery and Operation documentation • Juniper Networks Secure Access family 5.1R2 Delivery Procedures, VERSION 0.3 DRAFT, REVISION 40, February 17, 2006
Design documentation • Secure Access family 5.1R2 Functional Specification, VERSION 0.4 DRAFT, REVISION 137, February 17, 2006 • Secure Access family 5.1R2, High-Level Design, VERSION 0.2 DRAFT, REVISION 6, February 17, 2006 • Juniper Networks Secure Access family 5.1R2 Correspondence Analysis, VERSION Rev C Draft, REVISION 46, February 17, 2006
Configuration Management documentation • Juniper Networks NetScreen-SA 4.1.1R1 Configuration Management System, VERSION 0.1 DRAFT, REVISION 38, February 17, 2006

Test documentation • Juniper Networks Secure Access family 5.1R2Test Plan, Procedures, and Results VERSION 0.3.1 DRAFT, REVISION 91, February 17, 2006
Vulnerability Assessment documentation • NetScreen Secure Access 5.1 Vulnerability Analysis VERSION 0.1 DRAFT, REVISION 3, February 17, 2006
Security Target • Juniper Networks Secure Access family 5.1R2 Security Target, Version 1.1, 2/2/2006

Table 3. Documentation.

6 IT Product Testing

Testing of the `Juniper Networks Secure Access Family 5.1R2` TOE took place at Juniper Networks, Inc., Sunnyvale, CA, during October 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 EAL2.

The testing and vulnerability related detail that is described in the CEM guidance beyond the CEM work unit information is provided in the ETR Part II and is considered proprietary. This detail is described within the CEM guidance for the testing and vulnerability assessment work units.

The cryptography used in this product has not been FIPS certified, not has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7 Evaluated Configuration

The evaluated configuration of `Secure Access` is one or more of the following appliances:

- Juniper Networks SA 2000, Release 5.1R2

- Juniper Networks NetScreen-SA 3000 FIPS, Release 5.1R2
- Juniper Networks SA 4000, Release 5.1R2
- Juniper Networks NetScreen-SA 5000 FIPS, Release 5.1R2
- Juniper Networks SA 6000, Release 5.1R2

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 [STSA1.1] is *Common Criteria* V2.2 conformant, and (b) the TOE is *Common Criteria* V2.2 Part 2 and Part 3 conformant, and recommended that an EAL2 certificate rating be issued for `Juniper Networks Secure Access Family 5.1R2`.

9 Validator Comments/Recommendations

The Validator offers the following comment.

- The Validator did not attend testing for this product, but did carefully review all of the documentation provided by Juniper Networks, Inc., in support of the evaluation. The quality of that documentation was excellent.

- Secure communication involving the secure sockets layer (SSL) was not included in this evaluation.

- The cryptography used in this product has not been FIPS certified, not has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

10 Annex

10.1 Annex A: Bibliography

10.1.1 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)

10.1.2 Common Criteria/CCEVS Documents

[CEMV2.2] *Common Criteria for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004, CCIMB-2004-01-004.

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Part 1 (CCIMB-2004-01-001); Part 2 (CCIMB-2004-01-002); and Part 3 (CCIMB-2004-01-003).

[CEMV2.2] *Common Criteria for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004, CCIMB-2004-01-004.

[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.

11 Security Target

[STSA1.1] *Juniper Networks Secure Access Family 5.1R2 Security Target*, Version 1.1, 2/2/2006.

12 Glossary

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.2, January 2004.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HTTP	HyperText Transport Protocol
IT	Information Technology
IVE	Instant Virtual Extranet
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
RTC	Real Time Clock
SAIC	Science Applications International Corporation
SFP	Security Functional Policy
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VR	Validation Report