National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks, Inc. STRM Release 2010.0

Report Number: CCEVS-VR-VID10426-2011
Version 1.0
April 25, 2011

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

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

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Ken Eggers

Common Criteria Testing Laboratory

Chris Gugel, Lead Evaluator
Booz Allen Hamilton (BAH)
Linthicum, Maryland

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Juniper Networks, Inc. STRM 2010.0. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in March 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2 (Flaw reporting procedures). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

Juniper STRM Release 2010.0, (herein referred to as STRM AKA the TOE), is a distributed software only network security management platform that provides situational awareness and compliance support through the combination of flow-based network knowledge, security event correlation, log management and asset-based vulnerability assessment. STRM collects and processes data including logs from security devices, network devices, applications and databases, network activity data (i.e. flows) from network taps, mirror ports or 3rd party flow sources such as NetFlow, and vulnerability assessment data. The product produces security events by real-time event and flow matching and by comparing the collected data to historical flow-based behavior patterns. The security events are then correlated by the product to produce weighted alerts (i.e. Offenses) which can be viewed in the STRM Console User Interface as well as sent to users or other solutions via email, syslog, or SNMP trap.

The Juniper STRM appliance, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE’s Security Target.

The cryptography used in this product has not been FIPS-certified, nor 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 technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The STRM Release 2010.0 Security Target version 2.0, dated 23 February 2011 identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Juniper appliance by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	Juniper Networks, Inc. STRM Release 2010.0
Sponsor & Developer	Juniper Networks, Inc., Sunnyvale, CA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	XX April 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2 Augmented ALC_FLR.2
Description	The TOE is the STRM appliance, which is a security software product developed by Juniper Networks, Inc. as an Intrusion Detection System.
Disclaimer	The information contained in this Validation Report is not an endorsement of the STRM product by any agency of the U.S. Government, and no warranty of the IDS product is either expressed or implied.
PP	US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7
Evaluation Personnel	Emmanuel Apau Seyithan Ayhan Christopher Gugel Kevin Micciche Derek Scheer John Schroeder Jeremy Sestok Amit Sharma Andrea Wright
Validation Body	NIAP CCEVS

3 Identification

The product being evaluated is Juniper Networks, Inc. STRM Release 2010.0.

4 Security Policy

4.1 Security Audit

The TOE creates syslog audit events for actions taken within STRM, which are populated with reliable timestamps provided by the TOE, event types, identity, outcome, and additional information for each type of audit event. The identity of the user changing the TOE is also reflected in the events. The TOE allows a role with System Administrator privileges to read audit information from the event, with sorting options. All other users are not authorized to view the audit information. Users without these privileges are denied access to the audit events. Audit information can also be displayed as reports.

4.2 Identification and Authentication

The TOE identifies and authenticates users via their usernames and passwords. The TOE requires all users to authenticate through a browser to Apache Tomcat on the STRM Console before performing any administrative functions on the TOE. No actions on the TOE can be performed by a user until he or she is identified and authenticated to the TOE. Once authenticated, all users are assigned a role, which is one of the security attributes maintained by the TOE. The role determines what actions the user is authorized to perform on the TOE. The TOE locks out users for a configurable period of time after a configurable number of failed access attempts. The product provides methods of updating patch and signature (event and vulnerability mappings) information coming from the Juniper servers. In the evaluated configuration, the TOE will not download and apply patch updates without an Administrator action.

4.3 Security Management

All management functions and user operations are performed through the STRM Console User Interface. The TOE has three roles: Administrators, System Administrators, and End Users. Administrators have all privileges, which include the managing of user accounts and configuring system data collection standards/protocols. System Administrators only have the privileges to configure system data collection standards/protocols, basic STRM functionality, and to change their own account passwords. Only Administrators and System Administrators roles can create, modify, and delete rules that modify the behavior of the IDS functionality of the TOE.

End users' roles do not have Admin privileges. End users have the ability to modify their own account passwords and query pre-defined reports. End users may be assigned additional privileges that enable them to perform more operations on the TOE, including Reports, Offense Manager with Customized Rule, Offense Manager, and other privileges as defined by an administrator.

4.4 Protection of the TSF

Administrators of the TOE ensure that all connections between physically separate parts of the TOE (i.e. trusted remote product) are secured using OpenSSH. All data transmitted between TOE subsystems is protected from unauthorized disclosure and modification during transmission. This includes all system data that is passed between TOE subsystems once a scanning session is completed and the data is made. The TOE uses secure hashing to verify the integrity of transmitted data, including detection of any unauthorized modifications of the data.

4.5 Cryptographic Support

Remote users establish a session with the TOE using a web-based HTTPS session. This secured path is used for user authentication, management and operations of the TOE by authorized users. The TOE generates cryptographic keys to support the use of OpenSSH during communication with remote users and between TOE subsystems.

4.6 Intrusion Detection System

The TOE is an Intrusion Detection System which collects various sets of information from the targeted resources, including but not limited to start-up, shutdown, and network traffic. The collected traffic is distributed into groups by the TOE for analysis and reporting purposes. Users are able to view this data based on their role. The TOE analyzes this data to establish whether a correlation exists with behavior and events. Each analytical result records the date/time of the result, the type of result, the identity of the data source, and the overall analysis of the result. After the analysis has occurred and the TOE determines that an intrusion has been detected, the system sends an alarm to the configured user.

All system data is stored by the TOE and is protected from unauthorized deletion and modification. Once the storage capacity is reached, the TOE ensures that the most recent data is maintained. The TOE overwrites the oldest stored data and sends an alarm to the configured user when this occurs.

5 Threats and Assumptions

5.1 Threats to Security

Table 1 summarizes the threats that the evaluated product addresses.

Table 1 – Threats

An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
Unauthorized attempts to access TOE data or security functions may go undetected.
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
Improper security configuration settings may exist in the IT System the TOE monitors.
Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
Vulnerabilities may exist in the IT System the TOE monitors.
The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
The TOE may fail to recognize vulnerabilities or inappropriate activity based on system data received from each data source.
The TOE may fail to identify vulnerabilities or inappropriate activity based on association of system data received from all data sources.
Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
Inadvertent activity and access may occur on an IT System the TOE monitors.
Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

5.2 Intended Usage Assumptions

Table 2 – Intended Usage Assumptions

The TOE has access to all the IT System data it needs to perform its functions.
The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
The TOE is appropriately scalable to the IT System the TOE monitors.

5.3 Personnel Assumptions

Table 3– Personnel Assumptions

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
The TOE can only be accessed by authorized users.

5.4 Physical Assumptions

Table 4 – Physical Assumptions

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the Juniper Networks, Inc. STRM Release 2010.0 product that is comprised of the following:

- STRM Console
- Managed Host - Events
- Managed Host - Flows

6.1 System Requirements

The following components are required on the appliances for the TOE:

500 Platform

Console	Managed Host – Events	Managed Host - Flows
Intel Core2Duo CPU e4300 1.8GHz Single LGA 775 CPU	Intel Core2Duo CPU e4300 1.8GHz Single LGA 775 CPU	Intel Core2Duo CPU e4300 1.8GHz Single LGA 775 CPU
8 GB RAM	8 GB RAM	2 GB RAM
200 MB installation	200 MB installation	200 MB installation
2x500GB RAID 1	2x500GB RAID 1	2x500GB RAID 1
4x 10/100/1000 network interfaces	2x 10/100/1000 network interfaces	1x 10/100/1000 network interfaces

2500 Platform

Console	Managed Host – Events	Managed Host - Flows
Single LGA 775 CPU - Intel	Single LGA 775 CPU - Intel	Single LGA 775 CPU - Intel

Core2 Quad Q9400 2.66GHz 6MB L2 Cache	Core2 Quad Q9400 2.66GHz 6MB L2 Cache	Core2 Quad Q9400 2.66GHz 6MB L2 Cache
8 GB RAM	8 GB RAM	2 GB RAM
200 MB installation	200 MB installation	50 MB installation
1.5 TB data storage (RAID recommended)	1.5 TB data storage (RAID recommended)	No storage required
4x 10/100/1000 network interfaces	2x 10/100/1000 network interfaces	1x 10/100/1000 network interfaces

5000 Platform

Console	Managed Host - Events	Managed Host - Flows
2.13Ghz low power ATCA SKU CPUs, 4 core/2	2.13Ghz low power ATCA SKU CPUs, 4 core/2	2.13Ghz low power ATCA SKU CPUs, 4 core/2
12 GB RAM	12 GB RAM	2 GB RAM
200 MB installation	200 MB installation	50 MB installation
1.5 TB data storage (RAID recommended)	1.5 TB data storage (RAID recommended)	No storage required
4x 10/100/1000 network interfaces	2x 10/100/1000 network interfaces	1x 10/100/1000 network interfaces

6.2 Cryptographic Assurance

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards as part of this evaluation. The vendor has asserted that all cryptography used by the product has been tested.

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

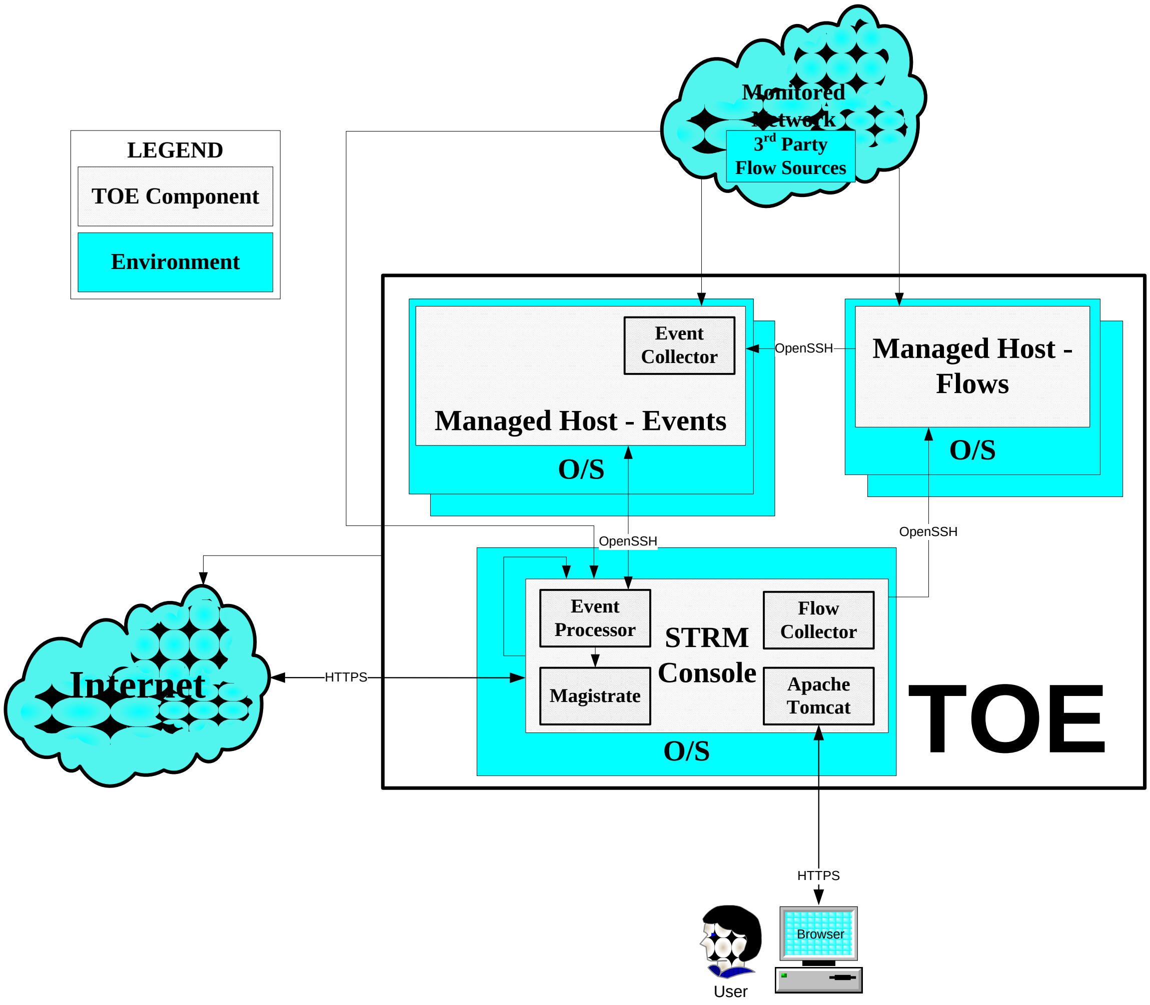

Figure 1 – TOE Boundary for Juniper Networks, Inc. STRM Release 2010.0

7.1 TOE Components

7.1.1 STRM Console

The STRM Console provides the interface for STRM and is accessed from a standard web browser via https. STRM supports the following web browsers:

- Internet Explorer 7.0 and higher
- Mozilla Firefox 3.6 and higher

The STRM Console provides global visibility into real time views, reports, offenses, and in-depth investigation of flows and events.

The Magistrate module of the STRM Console provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense. If no custom rules exist, the

Magistrate uses the default rules to process the event. An offense is an event that has been processed through STRM using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. Magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility. Once processed, Magistrate also produces a list for each attacker, which provides administrators with a list of attackers for each event.

The STRM Console contains the following two processes internally, and their functionality remains the same. The following subsystems act the same when they are external to the console, and provide additional processing power and throughput to augment the scope of the STRM deployment.

7.1.2 Managed Host - Events

This Managed Host collects security events from various types of security devices in the network. This Managed Host includes the Event Collector which gathers events from local, remote, and device sources. The Event Collector also bundles all virtually identical events to conserve system usage. The Event Processor correlates security events and logs. Logs that match correlation rules are forwarded to the STRM Console for additional analysis and possible correlation to an offense.

This Managed Host also collects, analyzes and stores data from the Flow Managed Host(s). The Event Processor performs correlation and analysis on the system data (flow data) in order to classify the network activity based on additional characteristics besides applications, such as geography, threatening traffic or other user definable classifications. Additionally, it serves to remove duplicate flows and create aggregate flows.

7.1.3 Managed Host - Flows

This Managed Host collects data from devices and various live and recorded feeds, such as network taps, span/mirror ports (i.e. packet data) as well as 3rd party flow sources such as JFlow, NetFlow, Packeteer flow records etc. This Managed Host contains the Flow Collector process. The Flow Collector then groups related individual packets into a flow. A flow starts when the Flow Collector detects the first packet with a unique source IP address, destination IP address, source port, and destination port as well as other specific protocol options, which may determine the start of a communication. Each additional packet is evaluated and counts of bytes and packets are added to the statistical counters in the flow record. In addition, Flow performs layer 7 application analysis on packet data to associate an application id to the flow. This allows STRM to provide more granular policy monitoring through being able to monitor unsecure or out of policy applications running in an organization. At the end of an interval, a status record of the flow is sent to the Event Collector and statistical counters for the flow are reset. A flow ends when no activity for the flow is seen within the configured period of time. Flow reporting generates records of all the active or expired flows during a specified period of time. STRM defines these flows as a communication session between two pairs of unique IP address/ports that use the same protocol or application.

8 Documentation and Delivery

The NIAP-certified Juniper STRM product is acquired via normal sales channels, and physical delivery of the TOE is coordinated with the end customer by Juniper Networks, Inc. STRM Release 2010.0 (to include STRM Console, Managed Host – Events, and Managed Host – Flows). The product is provided to normal customers as an appliance accompanied by a documentation CD with the following set of documents/books.

- STRM Users Guide r2010.0
- STRM Administration Guide r2010.0
- Managing Vulnerability Assessment Release 2010.0
- STRM Application Configuration Guide r2010.0
- Configuring DSMs Release 2009.2 and Release 2010.0
- Log Sources User Guide Release 2009.2 and Release 2010.0
- NSM Plug-In User Guide Release 2010.0
- STRM RELEASE NOTES RELEASE 2010.0
- STRM Installation Guide Release 2010.0
- UPGRADING TO STRM RELEASE 2010.0
- TECHNICAL NOTE OPEN PORTS USED BY STRM
- TECHNICAL NOTE CONFIGURING iSCSI
- STRM LOG MANAGER RELEASE NOTES RELEASE 2010.0
- STRM Log Manager Installation Guide Release 2010.0
- UPGRADING TO STRM LOG MANAGER RELEASE 2010.0
- Adaptive Log Exporter Users Guide Release 2010.0
- AQL Flow and Event Query CLI Guide Release 2010.0
- TECHNICAL NOTE GENERATING PUBLIC KEYS
- TECHNICAL NOTE INSTALLING AND CONFIGURING ALE USING A CLI
- STRM Log Manager Administration Guide Release 2010.0
- STRM Log Manager Users Guide Release 2010.0

Additionally, the vendor provides documentation on their support website, http://www.juniper.net/techpubs/en_US/strm2010.0/information-products/pathway-pages/strm-series/index.html. Included within this documentation is the 'Evaluated Configuration for Juniper Networks, Inc. STRM 2010.0' which should be referenced to place the product within the CC evaluated configuration.

The following documents were included within the scope of the evaluation:

- STRM Administration Guide r2010.0
- STRM Users Guide r2010.0
- Evaluated Configuration for Juniper Networks, Inc. STRM 2010.0

9 IT Product Testing

9.1 Functional Testing

9.1.1 Functional Test Methodology

The test team's test approach was to test the security mechanisms of STRM by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface was described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

EAL2 requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

9.1.2 Functional Results

During the course of the evaluation, the Booz Allen evaluation team reviewed the vendor’s functional testing and determined that all *security relevant* TOE external interfaces were tested and all of the claimed functionality was tested by the vendor. The evaluation team then created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing developed by the evaluators. The evaluators test suite emphasized on the product’s primary functionality and additional regression testing. Based upon the results of the vendor and evaluator testing; it has been determined that the product functionally operates as described.

9.2 Vulnerability Testing

9.2.1 Vulnerability Test Methodology

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:
  - Web (HTTPS)
  - Managed Host (SSH)
  - Log/Flow Data
- Port Scanning
  Remote access to the TOE was limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

  Backdoors
  CGI abuses
  Denial of Service
  Finger abuses
  Firewalls
  FTP
  Gain a shell remotely
  Gain root remotely
  General
  Miscellaneous
  Netware
  NIS
  Port scanners
  Remote file access
  RPC
  Settings
  SMTP Problems
  SNMP
  Untested
  Useless services
- TCP Malformed Packet Flooding
  This test attempted to shutdown TOE resources by flooding the network with large amounts of malformed tcp packets.
- Unauthenticated Access / Directory Traversal Attack
  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).
- SQL Injection / Cross Site Scripting Attack / Cross Site Request Forgery
  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.

- Web Server Vulnerability Scanner (Nikto)
  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

  File Upload.
  Interesting File / Seen in logs.
  Misconfiguration / Default File.
  Information Disclosure.
  Injection (XSS/Script/HTML).
  Remote File Retrieval
  Denial of Service.
  Command Execution / Remote Shell.
  SQL Injection.
  Authentication Bypass.
  Software Identification
  Remote source inclusion.

- Vulnerability Scanner (Retina)
  This test used the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
  The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

  Accounts
  Anti-Virus
  Backdoors
  CGI Scripts
  Database Issues
  DoS
  IP Services
  Registry
  Remote Access
  RPC Services
  Service Control
  Spyware
  Web Services
  CVE Issues
  SecurityFocus BID Issues

- Syslog Spoofing
  In this test, the attacker attempts to spoof syslog messages from one of the log sources configured in Juniper.

9.2.2 Vulnerability Results

During the vulnerability testing, there were several issues discovered that could affect the security posture of a deployed system. These issues have been broken up into the following categories:

9.2.2.1 Mitigated by Guidance

Webmin

It was discovered during the evaluation that the TOE web UI linked to a different listener on port 10000 that was running a modified version of webmin. This can be used to change passwords, configure interface roles, configure firewall access, and configure system time. The interface itself appears to be fairly well locked down. It requires valid user authentication before allowing any actions. However, it uses a different certificate and private key from the standard web interface and these files are not updated when the product HTTPS cert/private key are changed. It uses the certificate and private key that come with the open source version of webmin. An attacker could download these values and use them to decrypt traffic to and from the webmin interface thereby revealing user passwords. Guidance has been included that instructs the end user to synchronize the certificate and private key of the webmin interface with that of the rest of the web UI.

Legacy Apache Virtual Host Listener

The evaluators discovered an additional apache virtual host listening on port 4333 of the STRM Console. This listener only served a single html page that contained an error condition. It, however, also supported the unsafe http method TRACE. This listener was included to support legacy applications and is not needed in the Common Criteria version. Guidance has been included that instructs the end user how to shut off this listener in the evaluated configuration.

9.2.2.2 Informational Notes

Log Message Spoofing and Interception

Log messages are collected by the product using syslog. The syslog protocol can be transmitted over TCP or UDP and is unencrypted on the network. This means that any syslog message could potentially be sniffed by an untrusted party and leak information. In addition, syslog messages have no authentication of either the client or the server. Therefore messages can be forged that appear to come from a valid source and contain false information. A product administrator should be aware of these facts and should not rely on the confidentiality or integrity of log data.

Use of Valid Certificates

All implementations of SSL/TLS in use by the product should be configured using valid certificates signed by a trusted certificate authority. The use of self-signed certificates could expose users to Man-In-the-Middle attacks resulting in credential theft.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the Juniper Networks, Inc. STRM Release 2010.0 TOE meets the security requirements contained in the Security Target.

The criteria against which the STRM TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the Juniper STRM, Inc. STRM Release 2010.0 TOE is EAL2 augmented with ALC_FLR.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed on 30 March 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

11 Validator Comments/Recommendations

11.1 IDS Event Message Spoofing and Interception

Syslog messages can be spoofed or intercepted, since they are not protected by the TOE. This affects messages that arrive at the Event Collector from sources communicating via the monitored network, these sources are third party IDS event message.

As stated in Section 9.2.2.3, "This means that any syslog message could potentially be sniffed by an untrusted party and leak information. In addition, syslog messages have no authentication of either the client or the server. Therefore messages can be forged that appear to come from a valid source and contain false information. A product administrator should be aware of these facts and should not rely on the confidentiality or integrity of log data." That is, third party IDS event messages may be forged, causing false IDS information to be sent to the TOE Event Collector, compromising the integrity of the TOE's IDS databases.

The following response to this issue is provided as part of "Evaluated Configuration for Juniper Networks, Inc. STRM 2010.0":

> "Because of the inherent insecurity of the UDP and syslog protocols, responsibility to protect the confidentiality and integrity of the transmitted messages falls to the network environment in which the product is deployed.
>
> The TOE should be deployed only in trusted network environments where there is reasonable assurance about the identity of all connected machines and corresponding users. In addition, there should be reasonable assurance that all connected machines and corresponding users are non-malicious in nature.
>
> The network environment should contain appropriate network security systems such as firewalls, IDS/IPS systems, or Network Access Control devices in order to maintain the security of the TOE in its intended operational environment."

Note that the network environment identified in this discussion is the monitored network, which is used to transmit third party IDS event messages to the TOE Event Collector.

11.2 Secure Installation and Configuration Documentation

The "Evaluated Configuration for Juniper Networks, Inc. STRM 2010.0" defines the recommendations and secure usage directions for the TOE as derived from testing.

11.3 Network events collection excluded from the evaluated configuration

After evaluation design analysis and testing was complete the vendor introduced a number of additional event types that could be collected and analyzed by the TOE. These events were primarily directed at Microsoft Windows activities. Since these events were not reviewed during the evaluation they are not considered as being contained in the TOE's evaluated configuration. They should, therefore, not be used when the TOE is running in the evaluated configuration. These events are covered in Section 2.3.3 in the Security Target.

12 Security Target

The security target for this product's evaluation is Juniper Networks, Inc. STRM Release 2010.0 Security Target, Version 2.0, 23 February 2011.

13 List of Acronyms

Acronym	Definition
ARP	Address Resolution Protocol
ASN	Autonomous System Number
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CIDR	Classless Inter-Domain Routing
DSM	Device Support Module
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
JDBC	Java Database Connectivity
LAN	Local Area Network
LEA	Log Export API
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
ODBC	Open Database Connectivity
OSI	Open System Interconnection
P2P	Peer to Peer
PP	Protection Profile
SCP	Secure Copy
SID	STRM Identifier
SIM	Security Information Management
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
ST	Security Target
STRM	Security Threat Response Manager
TCP	Transmission Control Protocol
TNC	Trusted Network Computing
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
VoIP	Voice over Internet Protocol

14 Terminology

Terminology	Definition
Administrator	A user that has all of the Admin extended privileges enabled for their account via roles.
Alert	A message sent or event generated in response to a monitored condition. For example, an alert informs a user if a policy has been breached or the network is under attack.
Analyzer	See Intrusion Detection System Analyzer
Analyzer Data	IDS data collected by the Analyzer functions
Analyzer Functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Asset	Information or resources (servers and hosts) to be protected by the countermeasures of a TOE.
Asset Profile	Displays the services running on each asset gathered from vulnerability assessment solutions and or network activity (flow) data. The profile data is used for correlation purposes to reduce false positives.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of log events and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Data	In an IT System, a chronological log of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized. All audit data is captured in audit events. The term audit event is synonymous with audit record.
Audit Record	See Audit data.
Authentication	To establish the validity of a claimed user or object.
Authorized Administrator	A subset of authorized users that manage an IDS component
Authorized User	A user that is allowed to perform IDS functions and access data
Availability	Assuring information and communications services will be ready for use when expected.
Behavior	Indicates the normal manner in which the system or network functions or operates.
Category	Contains the name, magnitude, local target count, events, and last event of a specific offense.
Checkpoint LEA	Product that extracts IT data logs from Checkpoint firewalls.
Cisco SDEE	Cisco Security Device Event Exchange is an application-level communications protocol that is used to exchange IPS messages between IPS clients and IPS servers.
Classless Inter-Domain Routing	CIDR is an addressing scheme for the Internet, which allocates and specifies Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.
Client	The host that originates communication.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Console	See STRM Console.
Content Capture	Flow Collectors capture a configurable amount of payload and store the data

	in the flow logs. A user can view this data using the View Flows function.
Credibility	The credibility of this offense, as determined by the credibility rating from source devices. For example, credibility is increased when multiple sources report the same event.
Custom Rules Engine	Determines the custom rules to apply to an event in determining if an offense has occurred.
Custom Rule Partial Matched	Event indicating that part of a custom defined rule was observed.
Deployment Editor	The deployment editor allows administrators to manage the individual subsystems of a STRM deployment. Once the Flow, Event, and System Views are configured, administrators can access and configure the individual subsystems of each managed host. Note: The Deployment Editor requires Java Runtime Environment.
Device Support Module	Allows integration of the TOE with external devices in a network. Through the user interface, users configure Log Sources to use the appropriate DSMs to enable the collection and parsing of events which are processed through the QIDmap for the intended log source and Normalized. Using the event mapping tool, an administrator can map a normalized or raw event to another event description and category if they so wish. Event mapping also allows the user to map unknown log source events to be displayed, categorized and correlated appropriately.
End Time	Specifies the last event or offense as reported by STRM.
End User	Someone who belongs to a non-administrative role. The privileges assigned to this role are defined by the administrator.
Event	Record from a device that describes an action on a network or host. The events in the evaluated configuration include the following: SOAP, Syslog (TCP), Syslog (UDP), JDBC/ODBC, SNMP, NSM, Lea, Cisco SDEE, and Log file protocol.
Event Collector	Component of the Event Processor. Collects security events and log messages from various types of security devices in a network. The Event Collector gathers events or logs from local, remote, and device sources. The Event Collector then normalizes the logs and events and sends the information to the Event Processor.
Event Processor	Processes events/log messages collected from its Event Collector. The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the logs in real time for association to offenses. The Event processor also provides distributed storage of event and log data.
Extended Privilege	A privilege that requires another privilege to be given before it can be given.
External IT Product	In the evaluated configuration, the External IT product is the Internet that the TOE connects to in order to receive patch and/or IDS definition updates on event and vulnerability mappings through the auto-update service provided by Juniper.
FTP	A protocol that allows file transfers via TCP.
Flow	Communication session between two devices. Describes how traffic is communicated, what was communicated (if content capture option has been selected), and includes such details as when, who, how much, protocols, priorities, options, etc. Flow data refers to: Specific properties of a flow including: IP addresses, ports, protocol, bytes, packets, flags, direction, and application ID. Flow logs refer to: Record of flows that enables the system to understand the context of a particular transmission over the network.

	Flow data is a type of IDS data.
Flow Sources	Source of flows that the Flow Collector receives. Using the deployment editor, one can add internal and external flow sources from the System or Flow Views in the deployment editor.
Flow Type View	Allows one to view network activity according to flow types. This depends on the ratio of incoming activity to outgoing activity.
Geographic Region	A geographic location which networks can be associated with.
High Level Category	Category that classifies the type of offense. Some examples of High Level Categories are Access, DOS, and Malware.
Identity	Specifies the IP address of the attacker.
IDS Data	Synonymous with System data.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Internet Protocol	IP is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.
Interval	The default time period in the system. Affects the update intervals of the graphs and how much time each flow log file contains.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer	The component of an IDS that accepts IDS data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Component	A Sensor, Scanner, or Analyzer.
Intrusion Detection System Scanner	The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
Intrusion Detection System Sensor	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
Is CRE Event	Describes an event that is generated by an offense or event rule.
JDBC	Java API that allows database access through SQL statements.
JFlow	A proprietary accounting technology used by Juniper® Networks that allows users to collect IP traffic flow statistics. J-Flow enables users to export data to a UDP ort on a J-Flow collector.
Juniper NSM	The Juniper Networks NSM console passively collects asset information from the network through deployed Juniper IDP sensors. STRM connects to the Profiler database stored on the NSM server to retrieve these records.
Layer 7	A layer of the OSI model that supports application and end-user processes. This layer provides application services for file transfers, e-mail, and other network software services.
Logic Unit	Sentry component that includes specific algorithms used to test objects.
Log Source	An external IT product that forwards formulated logs to the TOE for processing.
Magistrate	Component of the Console. The Magistrate provides views, reports, alerts,

	and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense.
Magnitude	Specifies the relative importance of the offense and is a weighted value calculated from the Relevance, Severity, and Credibility. The magnitude bar in the Offenses interface and Dashboard provides a visual representation of all correlated variables of the offense, attacker, target, or network. The magnitude of an offense is determined by several tests that performed on an offense every time it has been scheduled for re-evaluation, usually because events have been added or the minimum time for scheduling has occurred.
Managed host	A managed host is a system in a deployment that has STRM software installed.
NAT	Used to translate an IP and Port after passing a NAT enabled device. Pre NAT source and destination IP and port are translated to post NAT source and destination IP and port.
NetFlow	A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. A user can configure STRM to accept Network Data Exports (NDE's) and thus become a NetFlow collector. The TOE understands NDE’s for version 1, 5, 7, and 9.
Network	Two or more machines interconnected for communications.
ODBC	Allows database access regardless of which Database Management System is employed.
Offense	Includes multiple events from one host. An offense is an incident that has been processed through STRM using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packeteer	Packeteer is a 3rd party data source that collects, aggregates, and stores network performance data. Once an external flow source is configured for Packeteer, one can send flow information from a Packeteer device to STRM.
Payload	Within an event, this specifies the payload of the event that the log describes.
Permission	See privilege
Privilege	Privileges are bundled into roles and applied to Users. Users can be assigned these to access different parts and functions of the TOE. The following are the main privileges associated with STRM: Admin, Offenses, Log Activity, Assets, Resolution, Network Activity, and Reports.
Protocol	A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It may still require an authorization exchange with a policy module or external policy server prior to admission.
Flow Collector	Collects IDS data from devices and various live or recorded data feeds, such as network taps, span/mirror ports, NetFlow, and STRM flow logs.
SCP	SCP is a method of file transfer that employs SSH for encryption and authentication.
STRM Console	Web interface for STRM. STRM is accessed from a standard web browser (Internet Explorer 7.0 or Mozilla Firefox 3.0). When accessing the system, a prompt appears for a user name and password, which must be configured in advance by the STRM administrator.
STRM Identifier	SID is a mapping of a single event of an external device to a Juniper unique identifier.
Relevance	Relevance determines the impact on a network of an event, category, or offense. For example, if a certain port is open, the relevance is high.
Remote Network	A network that a device in question is not located in. Can also be used to

	indicate a destination network.
Remote Trusted IT Product	In the evaluated configuration, a remote trusted IT product is a TOE component that is installed on a separate machine. All TOE components are installed on separate machines in the evaluated configuration.
Remote Service	A function offered by a device other than the device in question.
Reports	A function that creates executive or operational level charting representations of network and security activity.
Resolver	A Resolver executes assigned Resolver Actions.
Resolver Action	A Resolver Action blocks host(s) affecting a network. A Resolver Action can have several Resolvers assigned as primary or reserve Resolvers.
Resolver Type	Specifies the type of Resolver. STRM pushes out resolver actions to the following devices: TCP Reset, ARP Redirect, Cisco, Cisco PIX, NetScreen Firewall, Juniper router, and Checkpoint Firewall Resolver.
Role	A set of privileges specified by an Administrator. Roles are applied to users.
Rule	Collection of conditions and consequent actions. A user can configure rules that allow STRM to capture and respond to specific event and or flow sequences. The rules allow a user to detect specific, specialized events and forward notifications to either the Offense interface or log file, e-mail a user, or resolve the event or offense, if the Resolution option is active.
Scanner	See Intrusion Detection System Scanner
Scanner Data	IDS data collected by the Scanner functions
Scanner Functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
Scanner Schedule	The times that a Scanner will collect information.
Security	A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.
Security Information Management (SIM)	SIM is a general IT system concept that involves a distributed environment of machines that generate output. Within SIM, machines can be configured to send outputs to a centralized system for aggregation purposes. SIM is used in the TOE to refer to the ability for Managed Hosts to send data to the Console for correlation and aggregation.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensor	See Intrusion Detection System Sensor
Sensor Data	IDS data collected by the Sensor functions
Sensor Functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data)
Severity	The severity of an offense. Severity indicates the amount of threat than an attacker poses in relation to how prepared the target is for the attack. This value is directly mapped to the event category that correlates to the offense. For example, a Denial of Service (DoS) attack is always has a severity of 10, which indicates a severe occurrence.
SFlow	A multi-vendor and end-user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously. sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. STRM supports sFlow versions 2, 4, and 5.
Simple Network Management Protocol	SNMP is a network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.
SOAP	An XML based protocol used to allow communication between different applications. SOAP uses HTTP to accomplish this.
Start Time	Specifies the time of the first event or offense as reported by STRM.

Subnet	A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.
Superflows	Multiple flows with the same properties are combined into one flow to increase processing by reducing storage.
Syslog Forwarding	Passing system log messages to another device.
System Administrator	System Administrators can only configure IDS data collection standards/protocols and basic STRM functionality. However, System Administrators cannot edit user accounts, with the exception of changing their own password.
System Data	Network traffic and host profile information that is collected by the TOE.
System Log	This log is used to capture alerts sent by the system when an intrusion is detected.
TOE Security Functions	TSF is a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
Transmission Control Protocol	TCP is a reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.
Transmission Control Protocol Flags	A type of marker that can be added to a packet to alert the system of abnormal activity. Only a few specific combinations of flags are valid and typical, in normal traffic. Abnormal combinations of flags often indicate an attack or an abnormal network condition.
Transmission Control Protocol Resets	For TCP-based applications, STRM can issue a TCP reset to either the client or server in a conversation. This stops the communications between the client and the server.
User	Any user of the TOE with one of the following roles: Administrator, System Administrator, or End User.
User Account	A record of the information about a specific user, including username, password, and role.
User Authentication	See Authentication.
User Data	User data refers to data captured during the following processes by all users of the TOE: identification and authentication and management functions.
User Role	See Role
Username	The name given to a user account.
Violation	Includes a violation of corporate policy.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. Juniper Networks, Inc. STRM Release 2010.0 Security Target, Version 2.0, 23 February 2011
6. Evaluation Technical Report for a Target of Evaluation "Juniper Networks, Inc. STRM Release 2010.0" Evaluation Technical Report v2.0 dated 30 March 2011.