National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks

JUNIPER NETWORKS IDP 4.0 & NSM 2006.1

Report Number: **CCEVS-VR-06-0043**
Dated: **23 October 2006**
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

Validator

Paul Bicknell
The MITRE Corporation
Bedford. MA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of the JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 2 October 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2 and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 2.2) for conformance to the *Common Criteria for IT Security Evaluation* (Version 2.2) and with the *Intrusion Detection System Protection Profile* Version 1.5. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 product by any agency of the US Government and no warranty of the product is either expressed or implied.

A Validator monitored the activities of the evaluation team, reviewed evaluation-testing documentation, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validator found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the Validator concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The Validator also confirmed the compliance of the ST with a registered Common Criteria Protection Profile. The conclusions of the testing laboratory in the evaluation technical report are also consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

The JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 TOE is composed of multiple components one of which (i.e., the IDP 4.0) is a hardware appliance that includes the operating system and supporting software. The other components (i.e., the NSM 2006.1 consisting of an NSM Server™ and NSM User Interface™) are software only and do not include the underlying operating system or other supporting software. The purpose of the product is to provide network intrusion and detection. The scope of the evaluation covered the IDP 4.0 appliance as well as the software portions of the NSM Server and NSM User Interface. All other, related, parts of the product were considered as being located in the IT Environment. The components of the TOE communicate via encrypted channels, however, analysis of the encryption was also not included as part of the evaluation.

1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.2, Revision 256, January 2004, which incorporated all applicable interpretations at the time the evaluation started.

1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

Table 1: Threats to the TOE

T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The Security Target also identified the following threats for the IT System the TOE monitors:

Table 2: Threats to IT System monitored by the TOE

T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC	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.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

1.3 Use of Cryptography

The TOE utilizes cryptography to protect TSF data in transmission between distributed parts of the TOE. However, that cryptography was not analyzed or tested to conform to any cryptographic standards during the evaluation.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 3 provides information needed to completely identify the 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, etc.

Table 3: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Intrusion Detection & Prevention system (IDP) 4.0 & Netscreen-Security Manager (NSM) 2006.1
Protection Profile	IDSSPP Version 1.5
ST:	*JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 Security Target,* Version 1.0, October 31, 2006.
Evaluation Technical Report	*Evaluation Technical Report For JUNIPER NETWORKS IDP 4.0 & NSM 2006.1,* Version 1.5, October 10, 2006
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004
Conformance Result	CC Part 2 conformant, CC Part 3 conformant

Item	Identifier
Interpretations Applied	No International Interpretations were applicable and no additional NIAP Interpretations were applied
Sponsor	Juniper Networks
Developer	Juniper Networks
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Paul Bicknell, The MITRE Corporation

3 Security Policy

The following Organizational Security Policies are required by the TOE:

Table 4: Organizational Security Policies

P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.DETECT	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 or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Assumptions

The following secure usage assumptions about the intended environment of the TOE are identified in the Security Target:

Table 5: Intended Usage Assumptions

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

	changes in the IT System the TOE monitors.

Table 6: Personnel Assumptions

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

Table 7: Physical Assumptions

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

4.1 Clarification of Scope

The TOE consists distributed components that exchange information across encrypted links. Verifying that encryption capability was not included in the evaluation. Threats to those communication channels were, likewise, not considered during the evaluation.

Two of the TOE components (i.e., NSM 2006.1 consisting of an NSM Server™ and NSM User Interface™) constitute software-only portions of the TOE. These components consist of TOE software hosted by underlying operating systems and other environmental software. That underlying software was not analyzed during the evaluation and threats to these underlying systems were not considered. This omission is legitimized by the Errata Sheets contained in IDSSPP Version 1.5.

5 Architectural Information

The JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 provides an intrusion detection and prevention device capable of using different detection methods to accurately detect suspicious network traffic (e.g., traffic designed to probe a system) and/or malicious network traffic (e.g., traffic designed to harm a system). IDP is also capable of dropping attacks to prevent damage to a network.

The IDP has the ability to operate in-line as an active gateway or as a passive sniffer. When deployed as an active gateway, IDP uses a policy to control what action to take when an attack is detected (e.g., dropping any identified malicious packets). When deployed as a passive sniffer, IDP can only detect and log attacks.

IDP 4.0 consists of a Sensor or group of Sensors that detect, and optionally prevent, attacks on networks connected to the IDP appliance. NSM 2006.1 consists of an NSM Server™ and NSM User Interface™ (NSM UI) which allows an administrator access to the system

data collected by the Sensor(s). This architecture is used to scale the system into three tiers, as well as to separate management functions from system operation.

5.1 Physical Boundaries

The physical boundaries of the TOE include the Sensor, NSM Server, and NSM UI software components that together comprise IDP 4.0 & NSM 2006.1. All other hardware and software components that are required to support the correct operation of the TOE are outside of the TOE boundaries. This includes the underlying operating systems for both the Sensor and NSM Server and also the network connections between TOE components.

5.2 Logical Boundaries

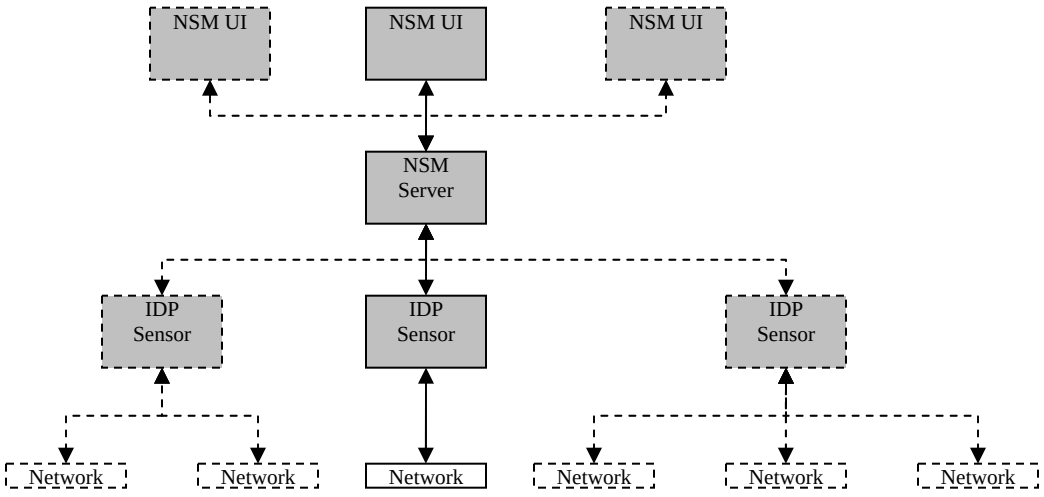

Figure 1 Logical TOE Boundaries

The logical boundaries of the TOE include the following IT Security features for the Sensor, NSM Server, and NSM UI. These IT security features of IDP 4.0 & NSM 2006.1 enable users to effectively implement and maintain the IDP appliance.

- The Sensor monitors the network on which the IDP appliance is installed. The Sensor is a hardware appliance that runs the IDP Sensor software. The Sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rule-bases. If the Sensor is running in-line as an active gateway, it can also take a predefined action against malicious traffic. The Sensor provides both the sensor and analyzer functionalities as defined within the IDSSPP v1.5.

- The NSM Server is software that manages the system resources of the Sensor and the data it collects. The NSM Server centralizes the logging, reporting, data, and Security Policy management for a set of Sensors. All objects, Security Policies, and log records are stored in the underlying filesystem on the NSM Server and are administered using the NSM UI. The NSM Server also includes a utility called Profiler that performs scanning capabilities as defined within the IDSSPP v1.5. The Profiler is a network analysis tool that assists in creating security policies. After being configured, the Profiler automatically learns about the internal network and the elements that comprise it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and data from layer-7 that uniquely identifies hosts, applications, commands, users, and filenames.
- The NSM User Interface (UI) is software that provides a graphical environment for centrally managing IDP. The UI is a java-based software application that can be installed on virtually any platform that supports the Java Runtime Environment (JRE) version 1.4.2. Although the UI supports multiple users, only one user at a time can take control of the NSM Server; this eliminates concerns about synchronization or data loss.

6 Documentation

Following is a list of the product documentation that is supplied to purchasers of the TOE. All documents, other than the configuration guides, are supplied on a CD delivered with the TOE. The two configuration guides can be separately obtained from the vendor. All documents are delivered in .pdf form.

Table 8: Product Documentation

Topic	Document Title
Delivery and Installation	• Juniper Networks IDP 4.0 & NSM 2006.1 Evaluated Configuration Guide, Rev B.2, 8/1/2006 • Intrusion Detection and Prevention Installer's Guide, IDP 50, 200, 600, 1100, Release 4.0, Part Number: 093-1765-000, Rev. B
User Guidance	• Juniper Networks IDP 4.0 & NSM 2006.1, Evaluated Configuration Guide, Rev A, 11/15/2005 • Juniper Networks IDP Concepts & Examples Guide, Release 4.0, P/N 093-1763-000, Revision B • Juniper Networks IDP Installer's Guide, Release 4.0, P/N 093-1765-000, Revision B

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Vender Testing

The vendor ran the documented test procedures before the evaluation team's Independent Testing Activity began. The vendor provided a complete set of test results for analysis. The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the vendor's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset of the tests that the vendor performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed all the security functions. The Evaluation Team used the vendor's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine that those procedures result in a secure configuration. However, the evaluation team did not test any cryptographic mechanism for compliance with any standards.

The Validator confirmed that the selection of vendor tests for re-running by the evaluation team covered all possible modes of operation and a majority of the Security Functional Requirements (SFR), and that each vendor test selected for rerunning corresponded to an SFR. In addition all administrative interfaces were covered as well as all the Intrusion Detection/Prevention subsystem interfaces.

The Validator also confirmed that the independent tests developed by the evaluation team tests covered all of the TOE Security Functions (i.e., Auditing, Identification & Authentication, Security Management, Self Protection, and Intrusion Detection & Prevention).

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of open-source information and the vendor's test report documentation and procedures to identify a set of penetration test cases. The Evaluation Team used the vendor's test configuration to successfully perform its penetration tests.

The Validator confirmed that the vulnerability testing conducted by the team appeared adequate.

7.4 Test Configuration

The evaluation team exercised developer and independent tests against the evaluated configuration of the TOE. The evaluation team tested two models of the appliance – the low-end and high-end models. The evaluation team believes this is acceptable since the security functionality among all the models is identical (as supported by the design) and the vendor has tested all models. The evaluation team tested the NSM Server on one variant of Unix since all of the security code on all of the Unix platforms is identical. The only source code differences among the Unix platforms are Kernel services (process handling, signal handling, network IO, disk IO, etc). Additional, the NSM UI was tested on a Windows XP platform. The NSM client relies on Java Runtime Environment (JRE) version 1.4.2 so the underlying platform is irrelevant as it is not directly called.

Test Hardware:

The following hardware was used in the test configurations:

- TOE Hardware
  - IDP50 version 4.0
  - IDP1100F version 4.0
- It Environment Hardware
  - Red Hat Enterprise Linux ES (for NSM Server and SMTP Server) – A commercially available hardware platform was connected to a test LAN.
  - Windows XP professional SP2 machine (for NSM client) – A commercially available hardware platform was connected to a test LAN.
- Test Hardware
  - Router used to establish test network
  - Windows XP profession SP2 machines (for test PCs) - Commercially available hardware platforms were connected to a test LAN

Test Software:

The following software was used in the test configurations:

- TOE Software
  - IDP 4.0
  - NSM Server version 2006.1
  - NSM UI version 2006.1
- It Environment Software
  - Red Hat Enterprise Linux ES
  - Windows XP professional SP2
  - Java Runtime Environment (JRE) version 1.4.2
- Test software
  - Packet Sniffer – Ethereal Network Protocol Analyzer
  - TCPReplay – retransmit network capture files
  - Netdude – capture file modification tool
  - VistaTask – MS Windows-based GUI scripting tool
  - SNOT – arbitrary file generator
  - SNORT Signatures – Intrusion Detection
  - Serial Console on a Windows based PC – Hyper Terminal by Hilgraeve for Microsoft

8 Evaluated Configuration

The evaluated configuration consists of a JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 system composed of the following components:

IDP 4.0

- IDP 50,
- IDP 200,
- IDP 600C,
- IDP 600F,
- IDP 1100C, and
- IDP 1100F

NSM 2006.1

- NSM Server
  - Sun Microsystems Ultra SPARC IIi 500MHz,
  - Solaris 8, Solaris 9, or
  - Red Hat Enterprise Linux ES 4.0 with Update 5 or 4.0 with Update 1, or
  - Red Hat Enterprise Linux AS 3.0 with Update 5 or 4.0 with Update 1
- NSM User Interface
  - 400MHz Pentium® II or equivalent (minimum); 700 MHz Pentium II or equivalent (recommended),
  - Microsoft Windows XP, or
  - Microsoft Windows NT® Workstation/Server 4.0, Service Pack 6a or higher, or
  - Microsoft Windows 2000 Server, Advanced Server, or Professional editions, or
  - Red Hat Enterprise Linux ES 3.0 or 4.0, Red Hat Enterprise Linux A
  - Java Runtime Environment (JRE) version 1.4.2

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.2 and the Common Evaluation Methodology (CEM) Version 2.2. There were no applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Section 4, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> "The evaluation determined the IDP TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements."

Section 5.3, Protection Profile Compliance, further states:

> "The JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 Security Target, Version 1.0, October 31, 2006 is compliant with the Intrusion Detection System System Protection Profile (IDSSPP), Version 1.5, March 9, 2005."

The Validator followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation and its results of pass are complete.

10 Validator Comments/Recommendations

In addition to the information presented in other sections of this document, the Validator has the following comments:

Updated Protection Profile: The Validator notes that well before the completion of this evaluation a newer version of the Intrusion Detection System System Protection Profile, than the one claimed compliance with in this evaluation, was released. The differences between that version and the one used in this evaluation are thought to be quite small and are believed to be mostly to correct some minor textual errors. The Validator feels that the fact that a new version of the PP exists may lead to some confusion regarding the results of this evaluation and for that reason recommends that an effort be made to demonstrate compliance with the newer PP.

Cryptography: 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.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 Security Target,* Version 1.0, October 31, 2006.

The document identifies the security functional requirements (SFRs) necessary to implement Access Control and TOE Self Protection security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) – The portions of the TOE that are relied on for correct enforcement of the TOE security policies.

14 Bibliography

The Validator used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.2 Revision 256, January 2004.
- Intrusion Detection System System Protection Profile, Version 1.5, March 9, 2005
- *JUNIPER NETWORKS IDP 4.0 & NSM 2006.1 Security Target*, Version 1.0, October 31, 2006.
- ETR Part 1 (Non-Proprietary), Version 1.5, October 10, 2006.