National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

NetScreen Technologies, Incorporated
NetScreen Appliances

Report Number: CCEVS-VR-02-0027
Version 1.0
Dated: 30 November 2002

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

Jean Hung
Yi-Fang Koh
The MITRE Corporation
Bedford, Massachusetts

Janine Pedersen
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of NetScreen Appliances. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Science Applications International Corporation (SAIC) and was completed on 30 November 2002. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2, resulting in a "pass" in accordance with CC Part 1 paragraph 175. The Target of Evaluation (TOE) also conforms to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

The NetScreen Appliances under evaluation are integrated security network devices designed and manufactured by NetScreen Technologies, Incorporated. NetScreen's line of appliances combines firewall, virtual private networking (VPN), and traffic management functions. Installing and managing appliances is accomplished using a command line interface (CLI).

The Target of Evaluation (TOE) includes the NetScreen appliances that run ScreenOS 4.0.0r7.0, a proprietary operating system. The NetScreen appliances that meet the definition of the TOE includes models: 5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200. Each identified model consists of hardware, firmware, and ScreenOS that runs in firmware.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, reviewed the individual work units and successive versions of the ETR. The validation team 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 validation team concludes that SAIC's findings are accurate, the conclusions justified, and the conformance results correct.

Disclaimers: The information contained in this Validation Report is not an endorsement of NetScreen Appliances by any agency of the U.S. Government and no warranty of NetScreen Appliances is either expressed or implied.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 EAL 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 desire 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 1 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	NetScreen Appliances includes models: 5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200
Protection Profile	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April, 1999
Security Target	NetScreen Appliances, Security Target Revision E, November 27, 2002
Evaluation Technical Report	Evaluation Technical Report for NetScreen Appliances, November, 2002
Conformance Result	Part 2 conformant, Part 3 conformant, and EAL 2
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable National and International Interpretations effective on May 22, 2002
Version of CEM	CEM Version 1.0 [5], [6] and all applicable National and International Interpretations effective on May 22, 2002
Sponsor	NetScreen Technologies, Incorporated
Developer	NetScreen Technologies, Incorporated
Evaluators	Science Applications International Corporation Ms. Cynthia Reese Mr. Neal Haley
Validators	Mrs. Jean Hung (The MITRE Corporation) Mrs. Yi-Fang Koh (The MITRE Corporation) Mrs. Janine Pedersen (NSA)

3 SECURITY POLICY

NetScreen's Networking subsystem provides the packet flow sequence to ensure that only packets that are expressly allowed to traverse the NetScreen appliances are allowed to do so. If a matching policy is found, then the packet is processed according to the policy. If a matching policy is not found, then the traffic is denied.

The Networking subsystem provides the functionality required to process packets based on specific criteria, including:

- Presumed source address: the presumed source IP address of the arriving packet
- Presumed destination address: the presumed destination IP address of the arriving packet
- Transport layer protocol: TCP or UDP protocols. Other protocols are not allowed through a NetScreen device
- Arrival interface: the arrival interface is identified by the source zone
- Service: the service, or port, is identified by the incoming packet

The Networking subsystem uses the above information to identify the incoming packet and uses the information to process the packet, thus enforcing an Information Flow policy upon all packets attempting to traverse the NetScreen appliances. The policy is configurable by the administrator and is based on the specified criteria.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage:

- 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.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

4.2 Physical Assumptions

The evaluation made the following environmental assumptions:

- A VT-100 terminal or any device that can emulate a VT-100 terminal is required for use as a locally connected console. The VT-100 terminal/emulator is part of the IT environment and it expected to correctly display what is sent to it from the TOE.
- The management console (VT-100 terminal/emulator) access will be restricted to authorized administrators.
- The TOE is physically secure.
- Information cannot flow among the internal and external networks unless it passes through the TOE.

4.3 Logical Assumptions

The evaluation made the following logical assumptions:

- There is no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- The TOE does not host public data.
- Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

4.4 Clarification of Scope

NetScreen appliances provide for a level of protection that is appropriate for IT environments that require strict control over the information flow across a network. NetScreen appliances are not designed to withstand physical attacks directed at disabling or bypassing its security features; however, it is designed to withstand logical attacks originating from its attached network performed by an attacker possessing a low attack potential.

All TOE security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats in light of specific assumptions. The ST did not list any organizational security policies.

5 ARCHITECTURAL INFORMATION

This section provides a high level description of the TOE and its subsystems as described in the NetScreen design documentation.

NetScreen appliances provide two subsystems to support the security functionality of the TOE, the Administrative subsystem and the Networking subsystem. Together the subsystems provide the following security functionality:

- Audit Generation, Review, and Protection
- Information Flow Policy Enforcement
- Identification and Authentication
- Management of Security Functions
- Protection of TOE Security Functions

5.1 TOE Subsystems

The following subsections describe the subsystems support of the above security functionality.

5.1.1 Administrative Subsystem

The Administrative subsystem includes the console port and the Command Line Interface (CLI). The CLI is accessible through the console port on each NetScreen appliance and is used to manage a NetScreen appliance. The CLI also provides the audit functionality. The TOE enforces the identification and authentication at the console before allowing use of the CLI.

The Syslog interface is an interface to an external Syslog server. This interface is used to transmit audit log information to a Syslog server for longer-term data storage than is possible on the internal flash memory on each NetScreen appliance.

The Administrative subsystem generates audit records corresponding to administrator actions, and identification and authentication. The Administrative subsystem provides interfaces that allow the administrator to review the audit records, including the ability to search and sort upon the audit records. Additionally, the Administrative subsystem provides the ability to protect the audit records and limit the loss of records due to audit storage exhaustion by providing an ability to archive audit data and to stop traffic from traversing the network.

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

Security Management is provided through the administrator interface. This interface allows an administrator (when properly identified and authenticated) to configure the NetScreen appliances. Therefore, the security management functions are only available to administrators.

The security functions of the TOE are protected by the administrative interface being a separate interface that is not connected to the network and, therefore, is not susceptible to many of the general threats on the network such as sniffing packets or attempts to log into a public administrative interface. The administrative commands are limited to the console port, in the evaluation configuration, and the console port does not pass network traffic. Additionally, the TOE includes a system clock that can only be set and modified by the administrator, providing reliable timestamps for audit information.

5.1.2 Networking Subsystem

The Networking Subsystem processes packets as they arrive at a physical interface, providing the packet flow sequence through the device. The traffic flow is audited by the Networking Subsystem and sent to the administrative subsystem for collection and presentation to the administrator.

The Networking subsystem has a packet buffer for temporary storage of packet information. All of the temporary storage is accounted for in that the size of the temporary storage relative to every packet is known, thereby ensuring that the TOE does not reuse any previous packet information. Additionally, in the evaluated configuration the security functions of the TOE are protected by the administrative interface being a separate interface that is not connected to the network and therefore, not susceptible to any of the general threats on the network such as sniffing packets or attempts to log into a public administrative interface.

6 DOCUMENTATION

This section provides a complete listing of the documentation which was issued by the developer (and sponsor).

Design documentation:

1) NetScreen Functional Specification for Common Criteria", Document Number 093-0628-000, Revision F
2) NetScreen High Level Design Document for Common Criteria", Document Number 093-0629-000, Revision E.
3) NetScreen Correspondence Matrix for Common Criteria, Revision F, 093-0654-000

Guidance documentation:

Command Line Interface (CLI) Document Set:

1) NetScreen CLI Reference Guide, Volume 1, P/N 093-0549-000, Rev D
2) NetScreen CLI Reference Guide, Volume 2, P/N 093-0550-000, Rev D
3) NetScreen CLI Reference Guide, Volume 3, P/N 093-0551-000, Rev D
4) NetScreen CLI Reference Guide, Volume 4, P/N 093-0552-000, Rev D

Concepts and Examples Document Set:

1) NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 2, P/N 093-0520-000, Rev E
2) NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 3, P/N 093-0521-000, Rev E

Audit Record Description Document:

1) NetScreen Message Log Reference Guide, P/N 093-0590-000, Rev E

Installation Guides:

1) NetScreen-5XT Installer’s Guide, P/N 093-0581-000, Rev D
2) NetScreen-5XP Installer’s Guide, P/N 093-0580-000, Rev D
3) NetScreen-25 Installer’s Guide, P/N 093-0579-000, Rev D
4) NetScreen-50 Installer’s Guide, P/N 093-0578-000, Rev D
5) NetScreen-100 Installer’s Guide, P/N 093-0577-000, Rev D
6) NetScreen-200 Series Installer’s Guide, P/N 093-0576-000, Rev D
7) NetScreen-500 Installer’s Guide, P/N 093-0575-000, Rev D
8) NetScreen-5000 Series Installer’s Guide, P/N 093-0573-000, Rev D

Configuration Management documentation:

1) NetScreen Configuration Management for Common Criteria 093-0630-000A, Revision F
2) Engineering Change Request and Engineering Change Control Procedure 093-0173-000, Rev A
3) Creating, Labeling and Tracking Serial Numbers and MAC Addresses 093-0229-000, Rev A

Delivery and Operation documentation:

1) Delivery of the Product to Buyer, 093-0648-000, Rev C
2) The "Properly Identifying the NetScreen Device for a CC EAL 2 Compliance" section in the below documents:
   NetScreen-5XT Installer's Guide, P/N 093-0581-000, Rev C
   NetScreen-5XP Installer's Guide, P/N 093-0580-000, Rev C
   NetScreen-25 Installer's Guide, P/N 093-0579-000, Rev C
   NetScreen-50 Installer's Guide, P/N 093-0578-000, Rev C
   NetScreen-100 Installer's Guide, P/N 093-0577-000, Rev C
   NetScreen-200 Series Installer's Guide, P/N 093-0576-000, Rev C
   NetScreen-500 Installer's Guide, P/N 093-0575-000, Rev C
   NetScreen-5000 Series Installer's Guide, P/N 093-0573-000, Rev C

Test documentation:

1) NetScreen Correspondence Matrix for Common Criteria, P/N 093-0654-000, Revision F.
2) NetScreen Test Cases for Common Criteria, P/N 093-0736-000, Revision F

Vulnerability Assessment documentation:

1) NetScreen Vulnerability Analysis for Common Criteria", Document Number 093-0595-000, Revision C.

Security Target:

1) NetScreen Appliances Security Target, Revision E, November 27, 2002.

7 IT PRODUCT TESTING

7.1 Developer Testing

Testing Approach:

The developer extracted from a test database (Test Technologies database) a set of test cases that reflect the TSF requirements (those requirements included in the Security Target (ST)). The test cases selected are included in the test evidence, specifically, the Test Cases document.

Each test case selected and included in the Test Cases document consisted of:

Test Procedure Description - TSF Code (a specific requirement element), Test Doc #, Test Doc. Name, Test Case No.

Test Procedures – For each Test Procedure Description, a test procedure is provided that includes the following information:

- Test procedure Steps: these are the steps that must be taken to stimulate the functionality being tested;
- Verification Steps: these are the steps that must be taken to confirm the actual result;
- Expected Results: these are the results expected based on the stimuli described in the test procedure steps and the verification steps; and
- Actual Results: these are snapshots of the results received when the test case is run.

Test Configuration:

The Introduction of the Test Cases document includes a description of test beds, each of which identifies a configuration of a NetScreen appliance(s). The test bed identifies the number of NetScreen appliances included in the configuration, the amount of PCs and if they are on the Trusted or Untrusted side of the NetScreen appliance, the syslog server if included in the configuration, the NTP server if included, the TFTP server if included, and the models included in each test bed.

Depth:

The amount of testing performed as it relates to the required functionality is described in the rationale for ATE_COV.1. Note that complete test coverage of the TSF is not required. The evaluation team considered the required functionality that was not tested in the developer test suite when formulating their team independent tests.

Test Results:

The test suite is primarily a manual test suite. The expected and actual test results for each test case is included in the Test Cases document. In addition to what can be observed by viewing the stream of traffic flow through the firewall, test results are also confirmed in audit records.

7.2 Evaluator Testing

The evaluators performed testing on a sample set of the vendor test suite. The selection of vendor tests to be included in the sample set was based on the following:

- Coverage of security functions
- Coverage of subsystems
- Size (20% of vendor test suite)

Each vendor test in the sample set was run successfully (i.e., the actual results matched the expected results). The evaluators then used the same configuration used in the vendor test subset to perform team tests. The evaluation team used the same test tools (such as the packet sniffers) documented and used for the vendor test subset, as well as their own packet sniffer.

All team tests performed succeeded (actual results matched the expected results). The penetration tests did not reveal any vulnerability that can be exploited in the evaluated configuration.

The results of the evaluation team tests and the evaluation penetration tests demonstrated the NetScreen Appliances product behaved as claimed in the Security Target. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

8 EVALUATED CONFIGURATION

The hardware is manufactured to NetScreen's specifications by sub-contracted manufacturing facilities. NetScreen's custom OS, ScreenOS, runs in firmware. The NetScreen appliances provide no extended permanent storage like disk drives and no abstractions like files. Audit information is stored in flash memory.

The main components of a NetScreen appliance are the processor, ASIC, memory, interfaces, and surrounding chassis and components. The differences between NetScreen appliances are the types of

processor(s), traffic interfaces, management interfaces, number of power supplies, type of ASIC, and redundancy to ensure high availability.

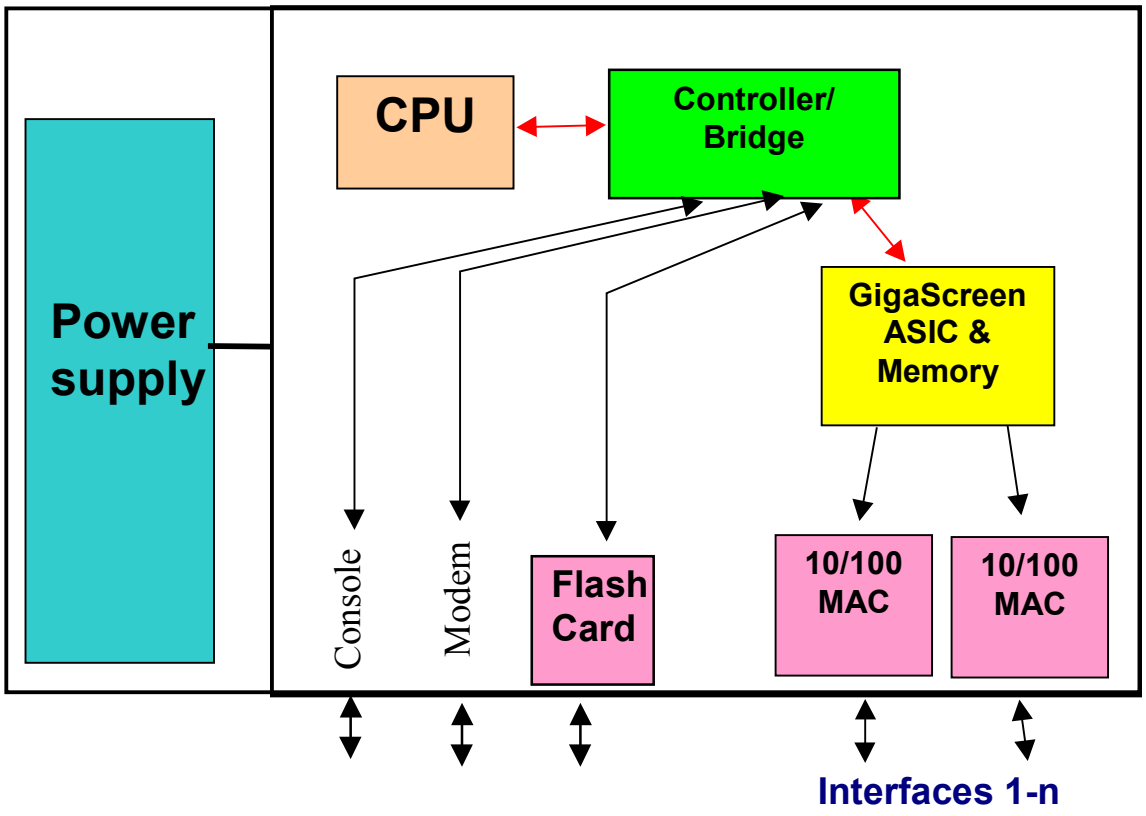

Figure 1: Main components of a NetScreen Appliance

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.1 [1], [2], [3] ,[4] and CEM version 1.0 [5], [6] and all applicable National and International Interpretations in effect on May 22, 2002. The evaluation determined the product to be Part 2 conformant, and to meet the Part 3 EAL 2 requirements. The details of the evaluation are recorded in the Evaluation Technical Report [8] which is controlled by SAIC.

9.1 Evaluation of the NetScreen Appliances Security Target (ST) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the NetScreen product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user and administrator guidance.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

9.8 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy (or veracity) of the claims in the ST.

10 VALIDATOR COMMENTS

The NetScreen Appliances TOE satisfies the NetScreen Appliances Security Target, Revision E, when configured according to the Installation Guides listed in Section 8 and the NetScreen Appliances ST is a CC compliant ST.

11 SECURITY TARGET

The Security Target, "NetScreen Appliances Security Target, Revision E, November 27, 2002", is included here by reference.

12 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
MAC	Mandatory Access Control
MRA	Mutual Recognition Arrangement
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol

TOE	Target of Evaluation
TSFI	TSF Interface
UDP	User Datagram Protocol
VPN	Virtual Private Networking

13 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Evaluation Technical Report for the NetScreen Appliances Product, Version 0.3, November 12, 2002.

[9] NetScreen Technologies, Inc. NetScreen Appliances Security Target Revision E, November 27, 2002.