National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

NetScreen Technologies, Incorporated
NetScreen Appliance Model 5200

Report Number: CCEVS-VR-03-0042

Dated: 30 October 2003

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
The MITRE Corporation
Bedford, Massachusetts

Janine Pedersen
National Security Agency
Ft. Meade, Maryland

Technical Oversight Panel

James Donndelinger
The Aerospace Corporation
Columbia, Maryland

Alton Lewis
National Security Agency
Ft. Meade, Maryland

Bradford O’Neill
The MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

DATED: 30 OCTOBER 2003 .... **III**
1 EXECUTIVE SUMMARY **6**
2 IDENTIFICATION **7**
3 SECURITY POLICY **8**
4 ASSUMPTIONS AND CLARIFICATION OF SCOPE **8**
4.1 USAGE ASSUMPTIONS 8
4.2 PHYSICAL ASSUMPTIONS 9
4.3 LOGICAL ASSUMPTIONS 9
4.4 CLARIFICATION OF SCOPE 9
5 ARCHITECTURAL INFORMATION **9**
5.1 TOE SUBSYSTEMS 10
5.1.1 Administrative Subsystem *10*
5.1.2 Networking Subsystem *10*
6 DOCUMENTATION **11**
7 PRODUCT TESTING **13**
7.1 DEVELOPER TESTING 13
7.2 EVALUATOR TESTING 14
8 EVALUATED CONFIGURATION **15**
8.1 Physical Boundaries *15*
8.2 Logical Boundaries *15*
9 RESULTS OF THE EVALUATION **18**
9.1 EVALUATION OF THE NETSCREEN SECURITY TARGETS (ST) (ASE) 18
9.2 EVALUATION OF THE CM CAPABILITIES (ACM) 18
9.3 EVALUATION OF THE DELIVERY AND OPERATION DOCUMENTS (ADO) 18
9.4 EVALUATION OF THE DEVELOPMENT (ADV) 18
9.5 EVALUATION OF THE GUIDANCE DOCUMENTS (AGD) 19
9.6 EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC) 19
9.7 EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE) 19
9.8 VULNERABILITY ASSESSMENT ACTIVITY (AVA) 19
9.9 SUMMARY OF EVALUATION RESULTS 19
10 VALIDATOR COMMENTS **19**
11 SECURITY TARGET **20**
12 GLOSSARY **20**
13 BIBLIOGRAPHY **22**

LIST OF TABLES

Table 1: Evaluation Identifiers 7

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of EAL4 Augmented NetScreen Appliance, model 5200 (hereafter referred to as the Netscreen Appliance). It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed jointly by Science Applications International Corporation (SAIC) and elements of the National Security Agency (NSA) and was completed in October 2003. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by both SAIC and NSA and submitted to the validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 Augmented to meet the requirements of Evaluation Assurance Level (EAL) 4 augmented with AVA_VLA.3, resulting in a "pass" in accordance with CC Part 1 paragraph 175. The Target of Evaluation (TOE) also conforms to the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000 and the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.
.

The NetScreen Appliance is an 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. NetScreen appliances have hardware accelerated IPSec encryption and low latency, allowing them to fit into any network. Installing and managing appliances is accomplished using a command line interface (CLI). However, some of the features and capabilities that are part of the NetScreen appliance were not evaluated and administrators are prohibited from configuring such functionality in the evaluated configuration per the administrative guidance. These features are:

- Virtual Private Networking (VPN),
- External Administrator Authentication (use of an external authentication server (e.g. Radius server)),
- Remote Management of the device,
- NTP (use of an external server to synchronize the time),
- The Malicious-URL screen commands (used to block specific URLs),
- Active-Active mode of NSRP (supports redundancy between traffic),
- Schedule specific policies (used to restrict a traffic flow policy to a specific time range), and
- Timer (used to automatically execute management functions).

The Target of Evaluation (TOE) includes the NetScreen 5200 that runs ScreenOS 4.0.2r7, a proprietary operating system with its VPN functionality disabled. The NetScreen appliance that meets the definition of the TOE is model 5200 and 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 EAL4 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 Appliance model 5200 with VPN disabled
Protection Profiles	U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000 and U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.
Security Target	NetScreen Appliances, Security Target: EAL4 Augmented Version 1.1, October 27, 2003
Evaluation Technical Report	Evaluation Technical Report for the NetScreen Appliances Product EAL4, Version 0.5, October 28, 2003
Conformance Result	Part 2 conformant, Part 3 Augmented conformant, and EAL4 augmented with AVA_VLA.3

Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable National and International Interpretations effective on November 20, 2002
Version of CEM	CEM Version 1.0 [5], [6] and all applicable National and International Interpretations effective on November 20, 2002
Sponsor	NetScreen Technologies, Incorporated
Developer	NetScreen Technologies, Incorporated
Evaluators	Science Applications International Corporation Ms. Cynthia Reese Ms. Tammy Compton Ms. Marie Eve Pierre Ms. Shukrat Abbass
Validators	Ms. Jean Hung (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 not part of the TOE, but rather is part of the IT environment and is 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 are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or 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

The NetScreen appliance provides for a level of protection that is appropriate for IT environments that require strict control over the information flow across a network. The NetScreen appliance is 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.

The NetScreen appliance provides 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 used to manage a Netscreen appliance and is accessible through its console port. 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 the 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

Following is a list of the evaluation evidence, each of which was issued by the developer

Design documentation

1) NetScreen Functional Specification for Common Criteria, P/N 093-0755-000, Revision I.
2) NetScreen High Level Design Document for Common Criteria, P/N 093-0756-000, Revision H.
3) NetScreeen Low Level Design Document for Common Criteria, P/N 093-0757-000, Revision I
4) NetScreen Correspondence Matrix for Common Criteria, 093-0758-000, Revision I
5) NetScreen Audit Loss Mitigation, 093-0853-000, Revision B
6) NetScreen Common Criteria EAL4 Security Policy Model, P/N 093-0759-000, Revision B

Guidance documentation

Command Line Interface (CLI) Document Set:

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

NetScreen New Features Guide, P/N 093-0845-000, Revision C

Concepts and Examples Document Set:

1) NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 2, P/N 093-0520-000, Revision E
2) NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 3, P/N 093-0521-000, Revision E-CC2

Audit Record Description Document:

1) NetScreen Message Log Reference Guide, P/N 093-0590-000, Revision F-CC3

Installation Guides:

1) NetScreen-5XT Installer’s Guide, P/N 093-0581-000, Revision F-CC10

2) NetScreen-5XP Installer’s Guide, P/N 093-0580-000, Revision F-CC10
3) NetScreen-25 Installer’s Guide, P/N 093-0579-000, Revision F-CC10
4) Netscreen-50 Installer’s Guide, P/N 093-0578-000, Revision F-CC10
5) Netscreen-200 Series Installer’s Guide, P/N 093-0576-000, Revision F-CC10
6) NetScreen-500 Installer’s Guide, P/N 093-0575-000, Revision F-CC10
7) NetScreen-5000 Series Installer’s Guide, P/N 093-0573-000, Revision G-CC1

Release Notes:

1) NetScreen Release Notes ScreenOS 4.0.2r7, P/N 093-1043-000, Revision A

Configuration Management

1) NetScreen Configuration Management for Common Criteria, P/N 093-0839-000, Revision K
2) NetScreen Engineering Change Request and Engineering Change Control Procedure, P/N 093-0173-000, Revision A
3) NetScreen Creating, Labeling and Tracking Serial Numbers and MAC Addresses, P/N 093-0229-000, Revision A
4) NetScreen Part Number and Product ID Process, P/N 093-0264-000, Revision A
5) NetScreen SKU Release Procedure, P/N 093-0325-000, Revision A

Life-Cycle Documentation

NetScreen Common Criteria EAL4 Life Cycle Model, P/N 093-0841-000, Revision C

NetScreen Common Criteria EAL4 Security Measures P/N 093-0852-000, Revision B

Delivery and Operation documentation

1) Delivery of the Product to Buyer, P/N 093-0840-000, Revision B
2) The “Properly Identifying the NetScreen Device for a CC EAL4 Compliance” section in the below documents:
   NetScreen-5XT Installer’s Guide, P/N 093-0581-000, Revision F-CC10
   NetScreen-5XP Installer’s Guide, P/N 093-0580-000, Revision F-CC10
   NetScreen-25 Installer’s Guide, P/N 093-0579-000, Revision F-CC10
   NetScreen-50 Installer’s Guide, P/N 093-0578-000, Revision F-CC10
   NetScreen-200 Series Installer’s Guide, P/N 093-0576-000, Revision F-CC10
   NetScreen-500 Installer’s Guide, P/N 093-0575-000, Revision F-CC10
   NetScreen-5000 Series Installer’s Guide, P/N 093-0573-000, Revision G-CC1

Test documentation

1) NetScreen Correspondence Matrix for Common Criteria, P/N 093-0758-000, Revision I
2) Test Cases for Common Criteria, P/N 093-0830-000, Revision P
3) NetScreen Functional Specification for Common Criteria, P/N 093-0755-000, Revision I
4) NetScreen Low Level Design Document for Common Criteria, P/N 093-0757-000, Revision J

Vulnerability Assessment documentation

1) NetScreen Vulnerability Assessment Plan and Report for Common Criteria, P/N 093-0842-000, Revision J
2) NetScreen Vulnerability Discovery and Resolution Process, P/N 093-0833-000, Revision C

3) NetScreen Misuse Document for Common Criteria, P/N 093-0897-000, Revision B

Security Target

1) NetScreen Appliances Security Target EAL4, P/N 093-0895-000, Version 1.0 dated April 23, 2003.
2) NetScreen Appliances Security Target EAL4 Augmented, P/N 093-093-0896-000, Version 1.1 dated October 27, 2003.

7 PRODUCT TESTING

7.1 Developer Testing

Testing Approach:

The developer testing approach as stated in the Introduction section of the Test Cases document is that 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 consists of:

Test Procedure Description - TSF Code (a specific requirement element), Test Doc #, Test Doc. Name,

Test Case Number.Test Procedures – For each Test Procedure Description, a test procedure is provided that includes the following types of steps:

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.

Actual Results: these are snapshots of the results received when the test case is run.

Test documentation including test plans, test procedures, a description of the test configuration, test coverage documentation, expected test results, and actual test results were provided to both the CCTL and NSA for review. Both evaluation teams reviewed the developer's tests and test results to ensure that the developer's testing and test results were appropriate for the evaluated configuration.

Test Configuration:

The Introduction of the Test Cases document includes a description of several test beds, each of which identifies a configuration of a NetScreen appliance(s). The test bed identifies the amount of NetScreen appliances included in the configuration, the amount of PCs and if they are on the Trust or Untrust 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/Coverage:

The amount of testing performed as it relates to the required functionality is described in the rationale for ATE_COV work units.

The depth of testing performed as it relates to the High Level design is described in the rationale for the ATE_DPT work units.

Test Results:

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 through the firewall via the "get dbuf stream" interface, test results are sometimes confirmed in audit records and sniffers.

7.2 Evaluator Testing

The evaluation team based the selection of which vendor tests to include in the sample set on the following criteria:

- Size
- Coverage of security functions
- Coverage of subsystems
- Coverage of models (at least 20% of the vendor test suite)

The 5200 model has more of its packet flow functionality implemented in hardware than the other models. This model difference is appropriately addressed in the sample because tests related to information flow were run on the 5200 model.

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.

Evaluation team testing at NSA, heretofore referred to as "the NSA evaluation team," was completed in October 2003. Using the results of the VLA.2 evaluation by the SAIC evaluation team, the NSA evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration
2. Vulnerability Testing (AVA_VLA.3)

Tools employed by the NSA evaluation team for independent testing included the same category of tools employed by the SAIC evaluation team, as well as in-house developed tools, which assisted in determining that the TOE was resistant to penetration attacks performed by attackers possessing a moderate attack potential. Numerous In-house tools were developed to stress network protocols. The team developed packet generators, (TCP, UDP, ICMP), denial of service (DoS) tools, and small programs, shells and Perl scripts designed for a specific purpose.

The results of the evaluation team tests and the evaluation penetration tests demonstrated the NetScreen Appliance behaved as claimed in the Security Target. The testing found that the product was implemented as described in the functional specification.

8 EVALUATED CONFIGURATION

This section documents the configuration of the IT product during the evaluation. The administrator and installation guides provide the necessary details for the correct configuration of the IT product in its evaluated configuration.

It is important for potential users to realize that if the evaluated configuration differs from the intended operational use, the differences must be factored into the final risk assessment.

The NetScreen product is an integrated security network appliance that operates as the central security hub in a network configuration. The NetScreen appliance controls traffic flow through the network and integrates stateful packet inspection firewall and traffic management features.

The TOE includes both physical and logical boundaries.

8.1 Physical Boundaries

The physical boundary of the NetScreen appliance is the physical appliance. All hardware on which the NetScreen appliance operates is part of the TOE. The NetScreen appliance has a custom operating system that is part of the TOE. The operating system, ScreenOS, runs completely in firmware. There is one assumption pertaining to the correct operation of the TOE and that is for the administrative console, which must be a VT-100 terminal or any device that can emulate a VT-100 terminal. The console is not part of the TOE. Rather, it is included in the environment and is expected to correctly display what is sent to it from ScreenOS.

The appliance enforces a security policy for all connection request and traffic flow between any two network zones. There are no direct connections between nodes in two separate zones except through the NetScreen appliance.

The NetScreen appliance attaches to a physical network that has been separated into zones through port interfaces. The physical boundaries of the NetScreen appliance include the interfaces to communicate between an appliance and a network node assigned to a network zone. All network communication flow goes from the sender network node in one zone, through the NetScreen appliance, and from the NetScreen appliance to the receiving node in another network zone if the security policy allows the information flow.

Traffic from one network node in a zone will only be forwarded to a node in another zone if the connection requests and the traffic satisfy the information flow policies configured in the NetScreen appliance. If data is received by an appliance that does not conform to those policies, it will be discarded and an audit record will be sent to the traffic log.

8.2 Logical Boundaries

The logical boundaries of the NetScreen appliance includes the interfaces to communicate between the network nodes in one zone with network nodes in other zones. Security policies are applied to inter-zone information flow.

8.2.1 Zones

A zone is a logical abstraction on which a NetScreen appliance provides services that are typically configurable by the administrator. A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or logical entity that performs a specific function (a function zone). Note that although the TOE includes a VPN (encryption) capability, this functionality was not evaluated and administrators are prevented from configuring such functionality in the evaluated configuration per the administrative guidance.

On a single NetScreen appliance, multiple security zones can be configured, sectioning the network into segments to which various security policies may be applied to satisfy the needs of each segment. At a minimum, two security zones must be identified, basically to protect one area of the network from the other. Many security zones can be identified to bring finer granularity to the network security design.

8.2.2 Audit

The NetScreen appliance categorizes auditing information into three categories: events, traffic logs, and self logs. Events are system-level notifications and alarms which are generated by the system to indicate events such as configuration changes, network attacks detected, or administrators logging in our out of the device. Traffic logs are directly driven by policies that allow traffic to go through the device. When logging and counting are enabled for a policy, all traffic will be logged to the traffic log. Self logs store information on traffic that is dropped and traffic that is sent to the device.

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

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

8.2.3 Information Flow Protection

By default, a NetScreen appliance denies all traffic in all directions. [1] Through the creation of information flow policies, traffic flow across an interface can be controlled by defining the kinds of traffic permitted to pass from one security zone to another.

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

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

- Addresses (source and destination),
- Transport Layer (i.e., protocol),
- Service (port or groups of ports, such as port 80 for HTTP), and
- Network Interface.

8.2.4 Identification & Authentication

There are five administrative roles supported by a NetScreen appliance. Three of these administrative roles are included as part of the evaluated configuration. All the administrative roles are treated collectively as a single “authorized administrator” role for the purpose of this report. The three administrative roles included as part of the evaluated configuration are:

- Root administrator,
- Read/Write Administrator, and
- Read-only Administrator.

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

8.2.5 Security Management

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

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

8.2.6 TOE Self Protection

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

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

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

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 November 20, 2002. The evaluation determined the product to be Part 2 conformant, and to meet the Part 3 EAL4 Augmented with AVA_VLA.3 requirements. The details of the evaluation are recorded in the Evaluation Technical Report [8] which is controlled by SAIC.

The handling of derived sessions was verified with a code analysis rather than testing. The code analysis examined the protocols that dynamically allocate ports. This analysis is documented in the Low Level Design (LLD) documentation.

9.1 Evaluation of the NetScreen Security Targets (ST) (ASE)

The evaluation team applied each 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 4 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 adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 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, a high-level design document, a low-level design document, and a security policy model. 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.

Additionally, the evaluation team ensured that the security policy model document describes the security policy rules that were found to be consistent with the design documentation.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

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

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. 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. The handling of derived sessions was verified with a code analysis rather than testing. The code analysis examined the protocols that dynamically allocate ports. This analysis is documented in the Low Level Design (LLD) documentation.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 and VLA.3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 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 tests also demonstrates the accuracy (or veracity) of the claims in the ST.

10 VALIDATOR COMMENTS

The NetScreen Appliance TOE satisfies the NetScreen Appliances Security Target: EAL4 Augmented, Version 1.1 dated October 27, 2003, when configured according to the Installation Guides listed in Section 8.

The vendor design documentation identified 3 categories of functionality in the product. Functions outside of the TOE, functions within the TOE that are security relevant, and functions within the TOE that are not security relevant. Only the security relevant functionality within the TOE was addressed by the vendor's test evidence (evidence used to meet the ATE_FUN work units). Of the two remaining categories, only the functionality outside of the TOE has been identified in the installation guide. Therefore, the functionality within the TOE that is not security relevant (and therefore not verified via testing) is not explicitly identified in the user documentation.

The product's Installation Guide lists the commands that are outside of the TOE. The features supported by these commands are not needed to satisfy the Traffic Filter Firewall Protection Profile for Medium Robustness Environments requirements or the Traffic Filter Firewall Protection Profile for Low-Risk Environments and the vendor did not present evidence in their test documentation that these functions were verified. The NetScreen appliance features that were not evaluated and administrators are prohibited from configuring such functionality in the evaluated configuration per the administrative guidance are:

- Virtual Private Networking (VPN)
- External Administrator Authentication (use of an external authentication server (e.g. Radius server))
- Remote Management of the device
- NTP (use of an external server to synchronize the time)
- The Malicious-URL screen commands (used to block specific URLs)
- Active-Active mode of NSRP (supports redundancy between traffic)
- Schedule specific policies (used to restrict a traffic flow policy to a specific time range)
- Timer (used to automatically execute management functions)

Options of the policy functionality are listed in the category of within the TOE and not security relevant. An example within this category is the option that invokes user authentication on traffic filtering rules (e.g., the auth option and the user, group, and group-expression commands). The vendor has asserted that this functionality is not required to meet the PP requirements because it only serves to further restrict which packets are eligible for forwarding. Additionally, the evaluation team considered this not security relevant functionality in the development of their independent team tests. The vendor claims and the evaluation confirmed that the PP requirements are satisfied by the required source, destination, and service components of rules.

11 SECURITY TARGET

The Security Target, "NetScreen Appliances Security Target EAL4 Augmented, P/N 093-0896-000, Version 1.1", 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
IT	Information Technology
MAC	Mandatory Access Control
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
TSF	TOE Security Functions
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 EAL4, Version 0.5, October 28, 2003.

[9] NetScreen Technologies, Inc. NetScreen Appliances Security Target EAL4 Augmented, P/N 093-0896-000, Version 1.1 dated October 27, 2003.