NetScreen Appliances Security Target: EAL4 Augmented

Version 1.1

October 27, 2003

P/N - 093-0896-000

Prepared for:
NetScreen Technologies, Incorporated
805 11th Avenue, Building 3
Sunnyvale, California 94089

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1 Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The NetScreen Appliances Target of Evaluation (TOE) primarily supports the definition of and enforces information flow policies among network nodes. The NetScreen appliance provides for stateful inspection of every packet that traverses the network. The appliance provides central management to manage the network security policy. All information flow from one network node to another passes through a NetScreen appliance. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the NetScreen appliances ensures that security relevant activity is audited, that its own functions are protected from potential attacks, and provides the security tools to manage all of the security functions.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, TOE and CC Identification

ST Title - NetScreen Appliances Security Target: EAL4 Augmented

ST Version - Version 1.1

ST Date – October 27, 2003

TOE Identification - The NetScreen appliances TOE consists of one or more of the following components:

- NetScreen 5XP (Part number: NS-5XP-00*, NS-5XP-10*, where * = 1, 3, 5, 7, or 9)
  - Firmware version: 4.0.2r7.0
  - Hardware version: 3010
- NetScreen 5XT (Part number: NS-5XT-00*, NS-5XT-10*, where * = 1, 3, 5, 7, or 9)
  - Firmware version: 4.0.2r7.0
  - Hardware version: 3010
- NetScreen 25 (Part number: NS-025-00*, where * = 1, 3, 5, or 7)
  - Firmware version: 4.0.2r7.0
  - Hardware version: 4010
- NetScreen 50 (Part number: NS-050-00*, where * = 1, 3, 5, or 7)
  - Firmware version: 4.0.2r7.0
  - Hardware version: 4010

- NetScreen 204 (Part number: NS-204-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 4.0.2r7.0
    - Hardware version: 0110
- NetScreen 208 (Part number: NS-208-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 4.0.2r7.0
    - Hardware version: 0110
- NetScreen 500 (Part number: NS-500-SK1, NS-500ES-GB1-**, NS-500ES-GB2-**, NS-500SP-GB1-**, NS-500SP-GB2-**, NS-500ES-FE1-**, NS-500ES-FE2-**, where ** = AC or DC)
    - Firmware version: 4.0.2r7.0
    - Hardware version: 4110
- NetScreen 5200 (Part number: NS-5200-P01*-S00, NS-5200-P01*-S01, NS-5200-P01*-S02, where * = A or D)
    - Firmware version: 4.0.2r7.0
    - Hardware version: 3110

CC Identification - Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Augmented
    - Evaluation Assurance Level 4 (EAL4) augmented with AVA_VLA.3

This TOE is conformant to the following Protection Profiles (PP):

- U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000.
- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

NetScreen has elected to pursue a more rigorous assurance evaluation. The product meets all the U.S. Department of Defense Traffic-Filter Firewall Protection Profile Functional and Assurance Requirements, additionally the TOE conforms to all the Assurance Requirements for an EAL4 product. The resulting assurance level is therefore, EAL4 augmented with AVA_VLA.3.

1.3 Strength of Environment

NetScreen appliances provide a level of protection that is appropriate for IT environments that require that information flows be controlled and restricted among network nodes where the NetScreen appliances components can be appropriately protected from physical attacks. Essentially, the NetScreen appliances management console must be controlled to restrict access to only authorized administrators. It is expected

that the NetScreen Appliances will be protected to the extent necessary to ensure they remain connected to the networks they protect. Essentially, this means that the NetScreen appliance components need to be protected to the degree appropriate to protect the networks to which they are connected. The assurance requirements, EAL4 augmented with AVA_VLA.3, and the minimum strength of function, SOF-medium, were chosen to be consistent with those environments.

1.4 Conventions, Terminology, and Acronyms

1.4.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- Security Functional Requirements - Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FMT_MSA.1(1) and FMT_MSA.1(2) indicate that the ST includes two iterations of the FMT_MSA.1 requirement, 1 and 2.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- If an operation was completed in a related Protection Profile or Interpretation, the corresponding PP or Interpretation should be consulted to determine what operations might have already been performed.

Other sections of the ST use bolding and italics to highlight text of special interest, such as captions.

1.4.2 Terminology and Acronyms

See Terminology and Acronyms section.

2 TOE Description

NetScreen appliances are integrated security network devices designed and manufactured by NetScreen Technologies, Incorporated, 805 11th Avenue, Sunnyvale, CA 94089 U.S.A, herein called simply NetScreen.

NetScreen's line of appliances combines firewall, virtual private networking (VPN), and traffic management functions. All NetScreen appliances have hardware accelerated IPSec encryption and very low latency, allowing them to fit into any network. Installing and managing appliances is accomplished using a command line interface (CLI). Even though the NetScreen appliances include IPSec encryption and VPN capabilities, they are outside the scope of the TOE.

The TOE includes the NetScreen appliances that run ScreenOS 4.0.2r7.0, a custom operating system. The NetScreen appliances that meet the definition of TOE include the models: 5XP, 5XT, 25, 50, 204, 208, 500, and 5200. Each identified model consists of hardware and ScreenOS that runs in firmware.

NetScreen appliances use a technique known as "stateful inspection" rather than an "application proxy," as stateful inspection offers the combination of security and performance. Stateful inspection firewalls examine each packet, and track application-layer information for each connection, by setting up a state table that spans multiple packets. This is used to determine whether incoming packets are legitimate. It eliminates the requirement to establish a TCP session with the firewall itself to access a service on the other side of the firewall (i.e. proxy the service).

2.1 Product Type

NetScreen products are integrated security network appliances that operate as the central security hub in a network configuration. The NetScreen appliances control traffic flow through the network. The NetScreen appliances integrate stateful packet inspection firewall and traffic management features.

2.2 Product Description

NetScreen-5XP, 5XT, 25, 50, 204, 208, 500, and 5200 all share a very similar hardware architecture and packet flow. All utilize custom ASICs for policy lookup acceleration, while a CPU is used as the main processor. All run ScreenOS with common core features across all products. All NetScreen appliances perform the same security functions and export the same types of interfaces. A sample of the differences between these products is listed below.

- The NetScreen-5XP, 5XT, 25, 50, 204, 208, and NetScreen-500 use a version of the GigaScreen ASIC that accelerates policy look-ups.
- The NetScreen-204, 208, and 500 utilize dual-port memory for faster processing and faster packet flow.
- The NetScreen-5200 is different than the rest of the products. It utilizes one or more GigaScreen-II ASICs, which provide a lot more functionality than the GigaScreen ASIC. The GigaScreen-II ASIC is capable of providing most of the functionality, and uses the CPU as a co-processor for handling management traffic and first packet inspections (policy lookups). So the GigaScreen-II ASIC can process an incoming packet, perform a session lookup, NAT, TCP/IP sequence checking, and can then send the packet back out of the device without the CPU every seeing it. The only time the CPU is used is for first packet inspection, management traffic, and packet fragment reassembly for inspection.

2.2.1 Hardware

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 memory because of the large storage capabilities.

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.

2.2.2 NetScreen ScreenOS

NetScreen ScreenOS firmware powers the entire system. At its core is a custom-designed, real time operating system built from the outset to deliver a very high level of security and performance. ScreenOS provides an integrated, easy-to-use platform for its many functions, including:

- Stateful inspection firewall
- Traffic management

ScreenOS does not support a programming environment.

2.3 Product Features

Each NetScreen appliance offers the following security functions:

- Audit: Audit data is stored in memory and is separated into three types of logs; 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. Both audit events and traffic messages can be further defined depending on the severity of the message and/or event.
- Information Flow Policy: Traffic flow from one network node to another network node is controlled by an unauthenticated security flow policy. This policy controls the flow of network traffic based solely upon the administratively configured rule set and information within network traffic and about the port upon which it arrives.
- Identification & Authentication: NetScreen appliances provide an authentication mechanism for administrative users through an internal authentication database. Administrative login is only supported through the locally connected console. The only authentication mechanisms supported by the TOE is passwords.
- Security Management: Every NetScreen appliance provides a command line administrative interface. To execute the CLI, an administrator must use a locally connected VT-100 terminal or workstation providing VT-100 terminal emulation to manage a NetScreen appliance through a direct serial connection. The authorized administrator must be successfully identified and authenticated before they are permitted to perform any security functions on the TOE.
- TOE Protection: Each NetScreen appliance is a hardware device that protects itself largely by offering only a minimal logical interface to the network and attached Nodes. ScreenOS is a special purpose OS that provides no general purpose programming capability. All network traffic from one network zone to another passes through the TOE; however, no protocol services are provided for user communication with the NetScreen appliance itself.

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The physical boundary of the NetScreen appliances is the physical appliance. The console, which is part of the TOE environment, provides the visual I/O for the administrative interface.

The NetScreen appliance attaches to a physical network that has been separated into zones through port interfaces.

NetScreen appliances come in eight models: 5XP, 5XT, 25, 50, 204, 208, 500, and 5200. Each model differs in the performance capability, however all provide the same security functionality. Each 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.

All hardware on which each NetScreen appliance operates is part of the TOE. Each 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 part of the TOE environment and it expected to correctly display what is sent to it from ScreenOS.

The physical boundary for the TOE is the physical port connections on the outside of the appliance's cabinet. One such port is the management port for the administrative console.

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 forward 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.

2.4.2 Logical Boundaries

The logical boundaries of the NetScreen appliances include 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.

2.4.2.1 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).

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.

2.4.2.2 Audit

NetScreen appliances categorize 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 broken into the following categories. 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. NetScreen appliances also 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.

2.4.2.3 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 which other 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:

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

2.4.2.4 Identification & Authentication

There are five administrative roles supported by a NetScreen appliance, though for the purposes of this Security Target they are treated collectively as a single “authorized administrator” role.

- Root administrator
- Read/Write Administrator
- Read-only Administrator
- VSYS Administrator and VSYS Read-only Administrator[2]

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.

2.4.2.5 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

[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.
[2] The VSYS Administrator roles are outside the scope of the TOE.

administrative commands. The console used to enter administrative commands is in the environment and not part of the TOE. 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.

2.4.2.6 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 NetScreen appliances 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.

3 Security Environment

The TOE security environment consists of the threats to security, secure usage assumptions, organizational security policies as they relate to NetScreen appliances.

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. NetScreen appliances are suitable for use in both Department of Defense and commercial environments.

3.1 Threats to Security

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.REPLAY An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.

T.ASPOOF An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.

T.MEDIAT An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

T.OLDINF Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE. [3]

T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

T.MODEXP A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.

T.TUSAGE The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

[3] Remote administration is optional in the associated Protection Profile. The TOE only supports a locally connected console within the physical protection of the TOE.

3.2 Secure Usage Assumptions

3.2.1 Personnel Assumptions

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

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

3.2.2 Physical Assumptions

A.CONSOLE 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.

A.LOCATE The management console (VT-100 terminal/emulator) access will be restricted to authorized administrators.

A.PHYSEC The TOE is physically secure.

A.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

3.2.3 Logical Assumptions

A.GENPUR There is no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

A.PUBLIC The TOE does not host public data.

A.NOREMO Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

A.REMACC Authorized administrator may access the TOE remotely from the internal and external networks. [4]

3.3 Organizational Security Policies

P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at minimum, with FIPS 140-1 (level 1). [5]

[4] While the associated Protection Profile assumes that administrators may access the TOE remotely, the Protection Profile also explicitly allows this capability to be optional. Hence, while remote administrator access could be allowed, the TOE does not provide any support for this feature.

[5] This Organizational Security Policy is not applicable for EAL2 and EAL4, as Remote Administration is outside the scope of the TOE. Remote administration is optional in the associated Protection Profile. The TOE only supports a locally connected console within the physical protection of the TOE. As such, this policy is included here only for a complete mapping to the Protection Profile.

4 Security Objectives

This section defines the security objectives of NetScreen appliances and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 IT Security Objectives

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

O.MEDIAT The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial startup of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network. [6]

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

O.EAL The TOE must be tested and shown to be resistant to attackers possessing moderate attack potential.

4.2 Security Objectives for the Environment

All of the assumptions, above, are considered to be security objectives for the environment. The following are the non-IT security objectives, which are to be satisfied without imposing technical requirements on the TOE. That is, they will be satisfied largely through application of procedural or administrative measures.

[6] Remote administration is optional in the associated Protection Profile. The TOE only supports a locally connected console within the physical protection of the TOE. As such, this objective is included here only for a complete mapping to the Protection Profile since the TOE does not provide any support for this feature.

O.PHYSEC	The TOE is physically secure.
O.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered to be moderate.
O.GENPUR	There is no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
O.PUBLIC	The TOE does not host public data.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
O.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
O.NOREMO	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
O.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks. [7]
O.GUIDAN	The TOE must be delivered, installed, administered, and operated a manner that maintains security.
O.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
O.CONSOLE	A VT-100 terminal or workstation that can emulate a VT-100 terminal is required for use as a locally connected console. The console is part of the IT environment and it expected to correctly display what is sent to it from the TOE.
O.LOCATE	The management console (VT-100 terminal/emulator) access will be restricted to authorized administrators.

[7] While the associated Protection Profile indicates that remote administration is an objective of the non-IT security environment of the TOE, the Protection Profile explicitly allows this capability to be optional. As such, this objective is included here only for a complete mapping to the Protection Profile since the TOE does not provide any support for these features.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria (indirectly via the Protection Profile (PP) identified in Protection Profile Claims section,). Every SFR included in the PP is addressed in this Security Target. Each SFR, except as noted below, was copied from the PP. Each SFR was changed in this ST to complete operations left incomplete by the PP or to make necessary refinements so that the intent of each SFR remains as specified in the PP. Each SFR was also changed, when necessary, to conform to National and International Interpretations.

Security Functional Class	Security Functional Components
Security Audit (FAU)	Audit data generation (FAU_GEN.1) *Note references to requirements related to remote administration, which is not supported by the TOE, have been removed from this requirement when copying it from the PP.*
	Audit review (FAU_SAR.1)
	Selectable audit review (FAU_SAR.3)
	Protected audit trail storage (FAU_STG.1)
	Prevention of audit data loss (FAU_STG.4)
Cryptographic support (FCS)	Cryptographic operation (FCS_COP.1) *Note this requirement does not apply since the TOE does not support remote administration. As a result, it has been omitted from this section (including entire removal of class FCS as well as removal of FAU_GEN.1 reference to this component.)*
User Data Protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
	Subset residual information protection (FDP_RIP.1)
Identification and authentication (FIA)	Authentication failure handling (FIA_AFL.1) *Note this requirement does not apply since the TOE does not support an interface where a non-administrator can attempt to authenticate itself to the TOE (e.g., for remote administration). As a result, it has been omitted from this section (including removal of family FIA_AFL as well as removal of FAU_GEN.1 and FMT_MOF.1 references to this component).*
	User attribute definition (FIA_ATD.1)
	Multiple authentication mechanisms (FIA_UAU.5) *Note this requirement does not apply since the TOE does not support remote administration from either an internal or external network. As a result, it has been omitted from this section (including removal of component FIA_UAU.5 as well as removal of FMT_MOF.1 references to this component).*
	Timing of authentication (FIA_UAU.1) *Note this requirement has been added since FIA_UAU.5 was removed and it is implied the authorized administrator must be successfully authenticated before allowing any other TSF-mediated actions. The appropriate changes have been included in FAU_GEN.1 and FMT_MOF.1 in reference to this component.*
	User identification before any action (FIA_UID.2)

Security Functional Class	Security Functional Components
Security management (FMT)	Management of security functions behavior (FMT_MOF.1(1)) *Note restrictions related to remote administration, which is not supported by the TOE, have been removed from this requirement when copying it from the PP.*
	Management of security functions behavior (FMT_MOF.1(2))
	Management of security attributes (FMT_MSA.1(1))
	Management of security attributes (FMT_MSA.1(2))
	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (FMT_MTD.1(1))
	Management of TSF data (FMT_MTD.1(2))
	Management of limits of TSF data (FMT_MTD.2) *Note this requirement does not apply since the TOE does not support an interface where a non-administrator can attempt to authenticate itself to the TOE (e.g., for remote administration). As a result, it has been omitted from this section (including removal of FAU_GEN.1 and FMT_MOF.1 references to this component).*
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1) [8]
Protection of the TSF (FPT)	Non-bypassability of the TSP (FPT_RVM.1)
	TSF domain separation (FPT_SEP.1)
	Reliable time stamps (FPT_STM.1)

Table 1 Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

5.1.1.1.1 FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions,
b) All auditable events for *not specified* level of audit; and
c) [the events in **the Table below**].

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	All decisions on requests for information flow.	The presumed address of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation

[8] This requirement has been added to conform to Interpretation RI#65

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation

5.1.1.1.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject**s** identi**ties**, outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three **of the Table in FAU_GEN.1.1**].

5.1.1.2 Audit review (FAU_SAR.1)

5.1.1.2.1 FAU_SAR.1.1

The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

5.1.1.2.2 FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 Selectable audit review (FAU_SAR.3)

5.1.1.3.1 FAU_SAR.3.1

The TSF shall provide the ability to perform *searches and sorting* of audit data based on:

a) [presumed subject address;
b) ranges of dates;
c) ranges of times;
d) ranges of addresses].

5.1.1.4 Protected audit trail storage (FAU_STG.1)

5.1.1.4.1 FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorized deletion.

5.1.1.4.2 FAU_STG.1.2

The TSF shall be able to *prevent* modifications to the audit records.

5.1.1.5 Prevention of audit data loss (FAU_STG.4)

5.1.1.5.1 FAU_STG.4.1

The TSF shall *prevent auditable events, except those taken by the authorized **administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

5.1.2 User Data Protection (FDP)

5.1.2.1 Subset information flow control (FDP_IFC.1)

5.1.2.1.1 FDP_IFC.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) operation: pass information].

5.1.2.2 Simple security attributes (FDP_IFF.1)

5.1.2.2.1 FDP_IFF.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] based on at least the following types of subject and information security attributes:

a) [subject security attributes:
   - presumed address;
   - [**and no additional attributes**];
b) information security attributes:
   - presumed address of source subject;
   - presumed address of destination subject;
   - transport layer protocol;
   - TOE interface on which traffic arrives and departs;
   - service; and
   - [**no additional attributes**]].

5.1.2.2.2 FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
   - the presumed address of the source subject, in the information, translates to an internal network address; and
   - the presumed address of the destination subject, in the information, translates to an address on the other connected network.
b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
   - the presumed address of the source subject, in the information, translates to an external network address; and
   - the presumed address of the destination subject, in the information, translates to an address on the other connected network].

5.1.2.2.3 FDP_IFF.1.3

The TSF shall enforce the **following information flow control rules:** [~~none~~ **no additional information control SFP rules**]. [9]

5.1.2.2.4 FDP_IFF.1.4

The TSF shall provide the following [~~none~~ **no additional SFP capabilities**]. [10]

5.1.2.2.5 FDP_IFF.1.5

The TSF shall explicitly authorize an information flow based on the following rules: [~~none~~ **no explicit authorization rules**]. [11]

5.1.2.2.6 FDP_IFF.1.6

The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network].

5.1.2.3 Subset residual information protection (FDP_RIP.1)

5.1.2.3.1 FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource* to the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

5.1.3 Identification and Authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

5.1.3.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

a) [identity;
b) association of a human user with the authorized administrator role;
c) [**and no additional attributes**]].

[9] This change has been made to conform to U.S. Interpretation I-0407.
[10] This change has been made to conform to U.S. Interpretation I-0407.
[11] This change has been made to conform to U.S. Interpretation I-0407.

5.1.3.2 Timing of authentication (FIA_UAU.1)

5.1.3.2.1 FIA_UAU.1.1

The TSF shall allow [**identification as stated in FIA_UID.2**] on behalf of the user to be performed before the user is authenticated.

5.1.3.2.2 FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.4 User identification before any action (FIA_UID.2)

5.1.3.4.1 FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user**.**

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behavior (1) (FMT_MOF.1(1)) [12]

5.1.4.1.1 FMT_MOF.1.1 (1)

The TSF shall restrict the ability to *enable*, *disable* the functions:

a) [operation of the TOE;
b) ~~single-use authentication function described in FIA_UAU.5~~] to [an authorized administrator].

5.1.4.2 Management of security functions behavior (2) (FMT_MOF.1(2)) [13]

5.1.4.2.1 FMT_MOF.1.1(2)

The TSF shall restrict the ability to *enable, disable, determine and modify the behaviour of* the functions:

a) [audit trail management;
b) backup and restore for TSF data, information flow rules, and audit trail data; and
c) ~~communication of authorized external IT entities with the TOE~~] to [an authorized administrator].

5.1.4.3 Management of security attributes (1) (FMT_MSA.1(1))

5.1.4.3.1 FMT_MSA.1.1 (1)

The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule and add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1) [14]] to [the authorized administrator].

---

[12] The TOE does not provide any support for remote administration. As such, the TOE does not provide any support for these features.
[13] The TOE does not provide any support for remote administration. As such, the TOE does not provide any support for these features.
[14] The reference is a typographically error that was copied from the PP. The requirement has not been refined. The reference should read FDP_IFF.1.1.

5.1.4.4 Management of security attributes (2) (FMT_MSA.1(2))

5.1.4.4.1 FMT_MSA.1.1 (2)

The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the authorized administrator].

5.1.4.5 Static attribute initialization (FMT_MSA.3)

5.1.4.5.1 FMT_MSA.3.1

The TSF shall enforce the [UNAUTHENTICATED SFP] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

5.1.4.5.2 FMT_MSA.3.2

The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.6 Management of TSF data (1) (FMT_MTD.1(1))

5.1.4.6.1 FMT_MTD.1.1(1)

The TSF shall restrict the ability to *query*, *modify*, *delete*, [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

5.1.4.7 Management of TSF data (2) (FMT_MTD.1(2))

5.1.4.7.1 FMT_MTD.1.1(2)

The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

5.1.4.8 Specification of Management Functions (FMT_SMF.1)

5.1.4.8.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [**create, delete, modify, and view information flows rules that permit or deny information flows**].

5.1.4.9 Security roles (FMT_SMR.1)

5.1.4.9.1 FMT_SMR.1.1

The TSF shall maintain the role [authorized administrator].

5.1.4.9.2 FMT_SMR.1.2

The TSF shall be able to associate **human** users with **the authorized administrator** role.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1)

5.1.5.1.1 FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 TSF domain separation (FPT_SEP.1)

5.1.5.2.1 FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.1.5.2.2 FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 Reliable time stamps (FPT_STM.1)

5.1.5.3.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.2 Security Functional Requirements for the IT Environment

There are no security functional requirements (SFRs) assigned to the IT environment rather than the TOE itself.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria. Note that the EAL 4 requirements that exceed EAL 2 augmented with AVA_VLA.3, by the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments are indicated in italics in the following table. No operations are applied to the assurance components. The SARs have been changed, when necessary, to conform to National and International Interpretations.

Assurance Class	**Assurance Components**
Configuration Management (ACM)	*ACM_AUT.1 Partial CM automation*
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and Operation (ADO)	*ADO_DEL.2 Detection of modification*
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	*ADV_FSP.2 Fully defined external interfaces*
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration

	ADV_SPM.1 Informal TOE security policy model
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	*ALC_DVS.1 Identification of security measures*
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests (ATE)	*ATE_COV.2 Analysis of Coverage*
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	*AVA_MSU.2 Validation of analysis*
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.3 Moderately resistant

Table 2 EAL4 augmented Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Partial CM automation (ACM_AUT.1)

5.3.1.1.1 ACM_AUT.1.1D

The developer shall use a CM system.

5.3.1.1.2 ACM_AUT.1.2D

The developer shall provide a CM plan.

5.3.1.1.3 ACM_AUT.1.1C

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

5.3.1.1.4 ACM_AUT.1.2C

The CM system shall provide an automated means to support the generation of the TOE.

5.3.1.1.5 ACM_AUT.1.3C

The CM plan shall describe the automated tools used in the CM system.

5.3.1.1.6 ACM_AUT.1.4C

The CM plan shall describe how the automated tools are used in the CM system.

5.3.1.1.7 ACM_AUT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Generation support and acceptance procedures (ACM_CAP.4)

5.3.1.2.1 ACM_CAP.4.1D

The developer shall provide a reference for the TOE.

5.3.1.2.2 ACM_CAP.4.2D

The developer shall use a CM system.

5.3.1.2.3 ACM_CAP.4.3D

The developer shall provide CM documentation.

5.3.1.2.4 ACM_CAP.4.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.2.5 ACM_CAP.4.2C

The TOE shall be labelled with its reference.

5.3.1.2.6 ACM_CAP.4.3C

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

5.3.1.2.7 International Interpretation RI #3

The configuration list shall uniquely identify all configuration items that comprise the TOE. [15]

5.3.1.2.8 ACM_CAP.4.4C

The configuration list shall describe the configuration items that comprise the TOE.

5.3.1.2.9 ACM_CAP.4.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

5.3.1.2.10 ACM_CAP.4.6C

The CM system shall uniquely identify all configuration items.

5.3.1.2.11 ACM_CAP.4.7C

The CM plan shall describe how the CM system is used.

5.3.1.2.12 ACM_CAP.4.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

5.3.1.2.13 ACM_CAP.4.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

5.3.1.2.14 ACM_CAP.4.10C

The CM system shall provide measures such that only authorised changes are made to the configuration items.

5.3.1.2.15 ACM_CAP.4.11C

The CM system shall support the generation of the TOE.

5.3.1.2.16 ACM_CAP.4.12C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

[15] This new assurance element has been added to conform to Interpretation RI#3

5.3.1.2.17 ACM_CAP.4.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.3 Problem tracking CM coverage (ACM_SCP.2)

5.3.1.3.1 ACM_SCP.2.1D

The developer shall provide **a list of configuration items for the TOE.** ~~CM documentation~~. [16]

5.3.1.3.2 ACM_SCP.2.1C

~~The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws~~. **The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.** [17]

~~5.3.1.3.3 ACM_SCP.2.2C~~

~~The CM documentation shall describe how configuration items are tracked by the CM system.~~ [18]

5.3.1.3.4 ACM_SCP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Detection of modification (ADO_DEL.2)

5.3.2.1.1 ADO_DEL.2.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.2.2D

The developer shall use the delivery procedures.

5.3.2.1.3 ADO_DEL.2.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.2.2C

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

5.3.2.1.5 ADO_DEL.2.3C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

---

[16] This change has been made to conform to International Interpretation RI#4
[17] This change has been made to conform to International Interpretation RI#4
[18] This change has been made to conform to International Interpretation RI#4

5.3.2.1.6 ADO_DEL.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.3.2.2.2 ADO_IGS.1.1C

~~The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.~~ **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.** [19]

5.1.1.5.2 5.3.2.2.3 ADO_IGS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Fully defined external interfaces (ADV_FSP.2)

5.3.3.1.1 ADV_FSP.2.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.2.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.2.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.2.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

5.3.3.1.5 ADV_FSP.2.4C

The functional specification shall completely represent the TSF.

5.3.3.1.6 ADV_FSP.2.5C

The functional specification shall include rationale that the TSF is completely represented.

[19] This change has been made to conform to International Interpretation RI#51

5.3.3.1.7 ADV_FSP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.1.8 ADV_FSP.2.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

5.3.3.2.1 ADV_HLD.2.1D

The developer shall provide the high-level design of the TSF.

5.3.3.2.2 ADV_HLD.2.1C

The presentation of the high-level design shall be informal.

5.3.3.2.3 ADV_HLD.2.2C

The high-level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.2.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.2.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.2.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.2.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.2.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.2.10 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

5.3.3.2.11 ADV_HLD.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2.12 ADV_HLD.2.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

5.3.3.3.1 ADV_IMP.1.1D

The developer shall provide the implementation representation for a selected subset of the TSF.

5.3.3.3.2 ADV_IMP.1.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

5.3.3.3.3 ADV_IMP.1.2C

The implementation representation shall be internally consistent.

5.3.3.3.4 ADV_IMP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3.5 ADV_IMP.1.2E

The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.4 Descriptive low-level design (ADV_LLD.1)

5.3.3.4.1 ADV_LLD.1.1D

The developer shall provide the low-level design of the TSF.

5.3.3.4.2 ADV_LLD.1.1C

The presentation of the low-level design shall be informal.

5.3.3.4.3 ADV_LLD.1.2C

The low-level design shall be internally consistent.

5.3.3.4.4 ADV_LLD.1.3C

The low-level design shall describe the TSF in terms of modules.

5.3.3.4.5 ADV_LLD.1.4C

The low-level design shall describe the purpose of each module.

5.3.3.4.6 ADV_LLD.1.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

5.3.3.4.7 ADV_LLD.1.6C

The low-level design shall describe how each TSP-enforcing function is provided.

5.3.3.4.8 ADV_LLD.1.7C

The low-level design shall identify all interfaces to the modules of the TSF.

5.3.3.4.9 ADV_LLD.1.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

5.3.3.4.10 ADV_LLD.1.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.4.11 ADV_LLD.1.10C

The low-level design shall describe the separation of the TOE into TSP enforcing and other modules.

5.3.3.4.12 ADV_LLD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4.13 ADV_LLD.1.2E

The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.5 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.5.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.3.3.5.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.5.3 ADV_RCR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.6 Informal TOE security policy model (ADV_SPM.1)

5.3.3.6.1 ADV_SPM.1.1D

The developer shall provide a TSP model.

5.3.3.6.2 ADV_SPM.1.2D

The developer shall demonstrate correspondence between the functional specification and the TSP model.

5.3.3.6.3 ADV_SPM.1.1C

The TSP model shall be informal.

5.3.3.6.4 ADV_SPM.1.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

5.3.3.6.5 ADV_SPM.1.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

5.3.3.6.6 ADV_SPM.1.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.3.3.6.7 ADV_SPM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documents supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life Cycle Support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

5.3.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

5.3.5.1.2 ALC_DVS.1.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

5.3.5.1.3 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.3.5.1.4 ALC_DVS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.1.5 ALC_DVS.1.2E

The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Developer defined life-cycle model (ALC_LCD.1)

5.3.5.2.1 ALC_LCD.1.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

5.3.5.2.2 ALC_LCD.1.2D

The developer shall provide life-cycle definition documentation.

5.3.5.2.3 ALC_LCD.1.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

5.3.5.2.4 ALC_LCD.1.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

5.3.5.2.5 ALC_LCD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Well-defined development tools (ALC_TAT.1)

5.3.5.3.1 ALC_TAT.1.1D

The developer shall identify the development tools being used for the TOE.

5.3.5.3.2 ALC_TAT.1.2D

The developer shall document the selected implementation-dependent options of the development tools.

5.1.1.5.3 5.3.5.3.3 ALC_TAT.1.1C

All development tools used for implementation shall be well-defined.

5.3.5.3.4 ALC_TAT.1.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

5.3.5.3.5 ALC_TAT.1.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.3.5.3.6 ALC_TAT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Security Testing (ATE)

5.3.6.1 Analysis of Coverage (ATE_COV.2)

5.3.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

5.3.6.1.2 ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.6.1.3 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.3.6.1.4 ATE_COV.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

5.3.6.2.1 ATE_DPT.1.1D

The developer shall provide the analysis of the depth of testing.

5.3.6.2.2 ATE_DPT.1.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.3.6.2.3 ATE_DPT.1.2E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

5.3.6.3.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.6.3.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.6.3.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.6.3.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.6.3.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.6.3.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.6.3.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.6.3.8 ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

5.3.6.4.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.6.4.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.6.4.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.3.6.4.4 ATE_IND.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.6.4.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

5.3.7.1 Validation of analysis (AVA_MSU.2)

5.3.7.1.1 AVA_MSU.2.1D

The developer shall provide guidance documentation.

5.3.7.1.2 AVA_MSU.2.2D

The developer shall document an analysis of the guidance documentation.

5.3.7.1.3 AVA_MSU.2.1C

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

5.3.7.1.4 AVA_MSU.2.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

5.1.1.5.4 5.3.7.1.5 AVA_MSU.2.3C

The guidance documentation shall list all assumptions about the intended environment.

5.3.7.1.6 AVA_MSU.2.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.3.7.1.7 AVA_MSU.2.5C

The analysis documentation shall demonstrate that the guidance documentation is complete.

5.3.7.1.8 AVA_MSU.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.7.1.9 AVA_MSU.2.2E

The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

5.3.7.1.10 AVA_MSU.2.3E

The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.1.11 AVA_MSU.2.4E

The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.7.2.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.7.2.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.7.2.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.7.2.4 AVA_SOF.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Moderately resistant (AVA_VLA.3)

5.3.7.3.1 AVA_VLA.3.1D

The developer shall perform **a vulnerability analysis** ~~and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP~~. [20]

5.3.7.3.2 AVA_VLA.3.2D

The developer shall provide **vulnerability analysis documentation** ~~document the disposition of identified vulnerabilities~~. [21]

5.3.7.3.3 AVA_VLA.3.1C

~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE~~. **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.** [22]

[20] This change has been made to conform to International Interpretation RI#51.
[21] This change has been made to conform to International Interpretation RI#51.
[22] This change has been made to conform to International Interpretation RI#51.

5.3.7.3.4 AVA_VLA.3.2C

~~The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.~~ **The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.** [23]

5.3.7.3.5 AVA_VLA.3.3C

~~The evidence shall show that the search for vulnerabilities is systematic.~~ **The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.** [24]

5.3.7.3.6 AVA_VLA.3.4C

The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks. [25]

5.3.7.3.7 AVA_VLA.3.5C

The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic. [26]

5.3.7.3.8 AVA_VLA.3.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.7.3.9 AVA_VLA.3.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

5.3.7.3.10 AVA_VLA.3.3E

The evaluator shall perform an independent vulnerability analysis.

5.3.7.3.11 AVA_VLA.3.4E

The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

5.3.7.3.12 AVA_VLA.3.5E

The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

[23] This change has been made to conform to International Interpretation RI#51.
[24] This change has been made to conform to International Interpretation RI#51.
[25] This change has been made to conform to International Interpretation RI#51.
[26] This change has been made to conform to International Interpretation RI#51.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation

Auditing is the action of recording log messages. Messages correspond to log entries and provide a rich audit mechanism. Audit messages provide the current values of the information as specified in the table listed in FAU_GEN.1.1; yet offer an authorized administrator the ability to create audit messages with the ability to audit on every value for which a security decision is taken.

NetScreen appliances categorize 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 broken into the following categories. 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.

NetScreen appliances also 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.

The information contained in the logs include:

a) The date and time of event,

b) The type of event,

c) The subject identity,

d) The outcome (success or failure) of the event, and

e) The presumed address of the source and destination subject as they pertain to decisions based on request for information flow,

The logs contain the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit and the events listed in the table in FAU_GEN.1.1 to include the additional audit record content as specified;

c) Administrator commands,

d) User I&A success and failures, and

e) Attempted Traffic (connection and packet filter) Information Flow Policy violations as well as successes

FAU_SAR.1 Audit Review

NetScreen appliances provide a Command Line Interface (CLI) for administrators to review the logs that records audited events using the CLI "get" commands. The logs display the date, time, level, and description for each event.

The CLI provides the an authorized administrator the ability to use "set" commands to configure a NetScreen appliance, "get" commands to display system configuration parameters and data, and "clear" commands to remove data collected in various tables, memory, and buffers. The "set" commands are used to set auditable events. The "get log" command displays all records in the log.

Messages are reported by type and severity. For every log message within a message type, the message is documented, as well as the meaning of the message, and the appropriate action that an administrator needs to take. There are dozens of specific message types. "Authentication" is but one type. Authentication message types relate to user authentication. Within this message there are four levels of severity: 1 - alert, 2 - warning, 3 - information, and 4 - notification.

FAU_SAR.3 Selectable Audit Review

The "get log" command provided by the CLI provides the appropriate administrator the tools to review the audit logs and search by specific attributes of each audited event. A few of the attributes available within the get log command are:

a) src-ip which displays traffic log entries for a specific source IP address or range of source IP addresses and
b) start time and end-time which displays event log entries that occurred at or after the time specified - day/month/year hour:minute:second.

Additionally, the 'get log sort-by' command provides the appropriate administrator the ability to sort the audit logs by specific attributes of each audited event. Those attributes are:

a) presumed subject address;
b) ranges of dates;
c) ranges of times;
d) ranges of addresses

FAU_STG.1 Protected Audit Trail Storage

Only authorized administrators have access to the audit logs and memory where the audit logs are stored. Authorized administrators must be identified and authenticated before they can gain access to the CLI and memory. The only external interface to access memory is through the administrative CLI. The 'get' command only allows the administrator to view the contents of memory, the audit logs, and to save the audit logs to an external file such as syslog. The available commands do not permit any user, including an authorized administrator to modify the audit logs or permit restoration of the audit logs.

FAU_STG.4 Prevention of Audit Data Loss

NetScreen appliances provide memory to hold a fixed maximum number of audit records and then once the storage limit is reached, the audit mechanism 'wraps' or acts as a first-in-first-out (FIFO) stack, when overwriting the oldest audit information in the storage device with the new audit information. Memory is used because of the very high traffic flow speeds supported by a NetScreen appliance. Storing audit records on a disk or other permanent storage media simply is too slow to capture audited events and audit data would be lost using a slower audit recording device. NetScreen appliances do follow every write to an audit log with an asynchronous write to a backup syslog device. This way memory acts as a high-speed

FIFO buffer device to store megabytes of audit information, so that all writes to the backup device will be serviced without audit data loss. The syslog backup device is not part of the TOE.

The technique of overwriting the oldest audit records once memory no longer has space for audit information limits the audit records that can be lost. All audit information is written at a speed that is directly proportional to audited activity. Audited activity on a protected network is rarely continuous over time, but occurs in bursts, average traffic flow, and lulls where traffic that causes audited events are low. The worst case for audit loss would occur if memory wrote an audit record in the last available location, and a burst of audited events occurred before they could be written to the backup syslog device. By overwriting the oldest audit information with the latest audit information to a very high-speed memory, the memory can never lose audit information in that no audit records can ever be "dropped" or not written. Additionally, the NetScreen appliances can be configured to notify the administrator when the logs capacity has reached a specified percentage.

There is an internal field that identifies when an audit record has been written to the syslog device. If this field indicates that the record has not been written to the syslog device, and the record is about to be overwritten, then an alarm will be created and all traffic will stop until all of the existing audit records are written to the syslog device. Once all existing audit records are written to the syslog device, network traffic will be allow to resume. During this stoppage of network traffic, device administration is allowed to continue, allowing an authenticated administer to make configuration changes if necessary to prevent further problems with audit loss, such as changing an information flow policy. This feature ensures that no auditable events, expect those taken by the authorized administrator will occur.

6.1.2 Information Flow

FDP_IFC.1 Subset Information Flow Control

The TSF enforces the UNAUTHENTICATED SFP on all IT entities that send and receive information through the TOE to one another. This includes information sent and received over the following protocols: ICMP, HTTP, TCP, IP, NetBIOS, and UDP, from a sending node identified to the TOE to a receiving node identified to the TOE.

NetScreen appliances act as stateful inspection firewalls that examine each packet and track application-layer information for each connection by setting up a state table that spans multiple packets. This is used to determine whether incoming packets are legitimate. It eliminates the requirement to establish a TCP session with the firewall itself to access a service on the other side of the firewall (i.e. proxy the service).

FDP_IFF.1 Simple Security Attributes

The UNAUTHENTICATED SFP by default enforces the use of an "access policy" that is established by an administrator to filter on certain objects and to take an appropriate action depending upon the contents of a packet, or a default policy is available. Each access policy contains at least the following elements:

- Addresses and/or Address Zones (source and destination)
- Service (A service is considered a protocol assigned to a port)
- Interface (i.e., physical network port)
- Transport Layer (protocol)

The access policy can be configured to control information flow based on all combinations of these elements. Access policies only apply to TCP and UDP transport layer protocols.

By default, a NetScreen appliance denies all traffic in all directions, except the NetScreen-5XP and 5XT, which will allow traffic from the trusted network to the untrusted network by default. NetScreen appliances are designed to prevent inappropriate information flows since all information flow from one zone to another must pass through the NetScreen appliance.

FDP_RIP.1 Subset Residual Information Flow

There are only two resources made available to information flowing through a NetScreen appliance. One is the temporary storage of packet information when access is requested and when information is being routed. The second type of information is key material.

To secure all connection attempts, NetScreen appliances use a dynamic packet filtering method known as stateful inspection. Using this method, a NetScreen appliance notes various components in a TCP packet header. State information recognized by the device includes: source and destination IP addresses, source and destination port numbers, packet sequence numbers, and packet length. The NetScreen appliance maintains the state of each TCP session traversing the firewall. This means that NetScreen appliances keep track of packet length and packet attributes such that each packet must be complete and correct for information to flow from source to destination. The NetScreen appliance interprets every byte in a complete information stream from the first packet to the last. All temporary storage is accounted for in that the size of a temporary storage relative to every packet is known. Therefore, no residual information from packets not associated with a specific information stream can traverse through a NetScreen appliance.

Key material resources are distributed and managed using the NetScreen appliances IPSec capabilities. All temporary storage associated with key material is handled in the same manner since it is encapsulated within packets. Therefore, no residual information from packets not associated with a specific information stream can traverse through a NetScreen appliance.

6.1.3 Identification and Authentication

FIA_ATD.1 User attribute Definition

The TSF maintains an identity and password for each administrator authorized to manage the security configuration of the TOE. Since all users are administrators and there is a single administrator role, the association between each user and their role is implicit.

FIA_UAU.1 Timing of Authentication

NetScreen appliances require administrative personnel to perform authentication before they may access any of the TOE functions or data. Once their identity has been provided, the administrator must enter the correct password in order to be successfully authenticated.

FIA_UID.2 User Identification Before any Action

The first and only interface presented to an administrator when attempting to login is a command line requesting user identification and password. There is no other interface to the TOE presented.

6.1.4 Security Management

FMT_MOF.1 Management of Security Functions Behavior (1 & 2)

The UNAUTHENTICATED SFP is configured through a locally connected console. The authorized administrator must be successfully identified and authenticated before they can access any security management functions.

Authorized administrators may add, remove, and change values within the security policy.

Because only authorized administrators can access the security management functions, the TSF restricts the ability to enable and/or disable the operation of the TOE such as TOE start-up and shut down to an authorized administrator

Additionally, the TSF restricts the ability to enable, disable, determine, and modify the behavior of the following functions to an authorized administrator:

a) audit trail management; and
b) backup and restore for TSF data, backup and restore of information flow rules, and backup of audit trail data.

The available commands do not permit any user, including an authorized administrator to modify the audit logs or permit restoration of the audit logs.

FMT_MSA.1 Management of Security Attributes (1 & 2)

The UNAUTHENTICATED SFP is configured through a locally connected console. The authorized administrator must be successfully identified and authenticated before they can access any security management functions. Authorized administrators may add, remove, and change values within the security policy.

Since only authorized administrators can access the security attributes associated with the information flow policies, the TSF restricts the ability to delete attributes from a rule, modify attributes in a rule, and add attributes to a rule to an authorized administrator. Additionally, the TSF restricts the ability to delete and create the security attributes for the information flow control SFP.

FMT_MSA.3 Static Attribute Initialization

By default, a NetScreen appliance denies all traffic in all directions, except the NetScreen-5XP and 5XT, which will allow traffic from the trusted network to the untrusted network by default. The administrator is instructed in the administrative guidance to change the policy for the 5XP and 5XT to be the same as the other models.

The administrator has the ability to configure the policy to reflect the needs of the organization.

FMT_MTD.1 Management of TSF Data (1)

Authorized administrators must be successfully identified and authenticated before gaining access to the TOE's security functions. Only authorized administrators can access the security management functions. Therefore, the TSF restricts the ability to query, modify, delete, and assign user attributes as defined in FIA_ATD.1 to the authorized administrator.

FMT_MTD.1 Management of TSF Data (2)

The data and time is set accordingly during installation. Once the TOE is operational, only a successfully identified and authenticated authorized administrator has access to time and date security function. The TSF restricts the ability to set the time and date to the authorized administrator.

FMT_SMF.1 Specification of Management Functions

NetScreen appliances provide the security management function of creating, deleting, modifying, and viewing the information flow security policy rules that permit or deny information flows.

The TOE provides this function and the TSF restricts this security management function to the authorized administrator as depicted in SFR FMT_MOF.1.

FMT_SMR.1 Security Roles

NetScreen appliances provide several levels of administrative user. For the purposes of this Security Target all of the available roles are treated collectively as the "authorized administrator." This role is assumed automatically by any authorized administrator that successfully logging into the console since no other user roles are supported by the TOE.

6.1.5 Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

All network traffic is assumed to be routed through the NetScreen appliance. Once network traffic is received on one of the NetScreen appliance network ports, it is always subject to the UNAUTHENTICATED SFP rules. This ensures non-bypassability of the TSP.

FPT_SEP.1 TSF Domain Separation

Protection of the TOE from physical tampering is ensured by its environment. It is assumed that NetScreen appliances 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. The hardware and firmware provided by NetScreen appliances provide all the services necessary to implement the TOE. There are no

external interfaces into the TOE other than the physical ports provided. No general purpose operating system, disk storage, or programming interface is provided.

The TOE protects its management functions by isolating them through authentication. Any interface that is controlled by a security zone can have two IP addresses. One is a physical port interface IP address (or a logical sub-interface), which connects to a network. The other is a second logical IP address for receiving administrative traffic.

Administrators are instructed to change the default password. If an administrator forgets their password, the NetScreen appliance has to be reset to the factory settings and connection configurations and Access Policy profiles are lost.

Logically, each NetScreen appliance is protected by the integrity of the protocol interpreters supporting the external interface. As long as network packets remain objects to be operated on by ScreenOS, the TSF is protected. ScreenOS is a custom operating system that runs in hardware, remains memory resident, and supports only trusted processes. A NetScreen appliance provides no file abstractions or permanent storage for "executables" to remain for further execution. ScreenOS has been designed to control the protocols that it recognizes at its external interface.

Each identification and authentication interface of the NetScreen appliance that provides access to TSF internal objects is password protected, physically protected, and only can be manipulated by a person acting in an administrative role.

FPT_STM.1 Reliable time stamps
NetScreen appliance hardware provides a reliable clock, and the NetScreen OS uses this clock to provide reliable time stamps. Both are part of the TSF.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL4 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The CM documentation describes the processes and procedure that are followed and automated tools that are utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE. The configuration management measures applied by NetScreen ensure that configuration items are uniquely identified. NetScreen ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. NetScreen performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation. These activities are documented in:

- Creating, Labeling, & Tracking S/N & MAC Addresses
- NetScreen Configuration Management for Common Criteria
- Engineering Change Request and Engineering Change Control Procedure

6.2.1.2 Life Cycle Support

NetScreen ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. NetScreen includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. NetScreen achieves this through the use of a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results. NetScreen has procedures for accepting and addressing identified operational flaws as well as security flaws, including tracking of all identified flaws, describing, correcting, and taking other remedial actions such as producing guidance related to such flaws. These procedures are documented in:

- NetScreen Life-Cycle Plan

The Process Assurance measures satisfy the following assurance requirements:

- ACM_AUT.1
- ACM_CAP.4,
- ACM_SCP.2,
- ALC_DVS.1,
- ALC_LCD.1, and
- ALC_TAT.1.

6.2.2 Delivery and Guidance

NetScreen provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. NetScreen's delivery procedures describe the procedures to be used for the secure installation, generation, and start-up of the TOE. These procedures are documented in:

- NetScreen Installer's Guides
    - NS-25 Installers Guide
    - NS-50 Installers Guide
    - NS-200 Series Installers Guide
    - NS-500 Installers Guide
    - NS-5000 Series Installers Guide
    - NS-5XP Installers Guide
    - NS-5XT Installers Guide
    - Appendix to Installers guide
- Delivery of Product to Buyer Document

NetScreen provides administrator guidance on how to utilize the TOE security functions and warnings to authorized administrators about actions that can compromise the security of the TOE. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install NetScreen appliances in accordance with the evaluated configuration. The administrator and user guidance is documented in:

- NetScreen Installer's Guides
    - NS-25 Installers Guide
    - NS-50 Installers Guide

  - NS-200 Series Installers Guide
  - NS-500 Installers Guide
  - NS-5000 Series Installers Guide
  - NS-5XP Installers Guide
  - NS-5XT Installers Guide
  - Appendix to Installers guide
- NetScreen Message Log Reference Guide
- NetScreen Concepts and Examples ScreenOS Reference Guide
- NetScreen Command Line Interface Reference Guide
- NetScreen Release Notes

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.2;
- ADO_IGS.1;
- AGD_ADM.1; and,
- AGD_USR.1.

6.2.3 Development

NetScreen provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems. The design documentation consists of the following documents and various references from these documents:

- NetScreen Functional Specification
- NetScreen High Level Design
- NetScreen Low Level Design
- NetScreen Correspondence Matrix
- NetScreen Security Policy Model For Common Criteria
- ADV_FSP.2: The NetScreen Functional Specification, including its references, describes the external interfaces to the TOE
- ADV_HLD.2: The NetScreen High Level Design, and its references, decomposes the TOE into subsystems
- ADV_LLD.1: The NetScreen Low-level Design Specification satisfies the requirement to decompose each subsystem into modules and fully describes each module.
- ADV_IMP.1: A subset of the source code and hardware diagrams used to generate the TOE satisfies this requirement.
- ADV_RCR.1: The way that this correspondence is evident within the design documentation is:
  - ST-TSS to FSP: The NetScreen Correspondence Matrix document identifies the interfaces that provide the security functions in the ST.
  - FSP to HLD: The NetScreen Correspondence Matrix document describes how the various security behavior of the external interfaces described in the FSP are further refined.

- HLD to LLD: The NetScreen Correspondence Matrix document, describes how the various security behavior of the external interfaces described in the NetScreen High-level Design Specification are further refined.
- LLD to IMP: The NetScreen Low-level Design Specification also serves to correspond modules with their specific implementations.

- ADV_SPM.1: The NetScreen Security Policy Model models the entities and rules related to the policies for identification and authentication, audit, and all of the information flow policies. Additionally, correspondence with the NetScreen Functional Specification is described.

6.2.4 Tests

NetScreen provides test documentation that describes how each of the TOE security functions is tested, as well as the actual results of applying the tests. The test documentation consist of the following documents:

- NetScreen Correspondence Matrix
- NetScreen Test Cases for the Common Criteria
- NetScreen Appliances Test Plan

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2: The test case descriptions (in the NetScreen Appliances Functional Specification) describe the test cases for each of the security-relevant interfaces of the TOE. The descriptions indicate which tests are used to satisfy the test cases identified for each interface.
- ATE_DPT.1: The test case descriptions (in the NetScreen High-level Design Specification) include more detailed test case descriptions that demonstrate that all of the corresponding interfaces are appropriately exercised
- ATE_FUN.1: The NetScreen Appliances Test Plan describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
- ATE_IND.2: The TOE and test documentation will be available for independent testing.

6.2.5 Vulnerability Assessment

6.2.5.1 Evaluation of Misuse

The guide and NetScreen Installer's Guides, and Appendix to Installers guide describe the operation of NetScreen and how to maintain a secure state. These guides also describe all operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. These guides are documented in:

- NetScreen Installer's Guides

The misuse analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

- The NetScreen Misuse Analysis

6.2.5.2 Strength of TOE Security Functions and Vulnerability Analysis

All of the SOF claims are based on password space calculations and is documented in Strength of Function (SOF) Rationale section in this ST. A separate SOF analysis is not applicable.

NetScreen performs systematic vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:

- NetScreen Vulnerability Analysis.

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.2;
- AVA_SOF.1; and,
- AVA_VLA.3.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 and the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, May 1, 2000. Note that the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments PP is a superset of the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. Therefore, the rationale in this section and Section 8 demonstrates conformance to the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, which consequently demonstrates conformance to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. NetScreen has elected to pursue a more vigorous assurance level as depicted in Conformance Claims section.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim. Note that the assumption A.REMACC is included in this ST, even though it is unnecessary since it allows but does not demand that remote administration can be supported. Note also that a single assumption and corresponding security objective, A.CONSOLE, has been added to support the notion that non-remote administration is actually performed using a device connected to a local serial port. Furthermore, A.LOCATE and corresponding objective, was added to support the access restriction of the management console to authorized administrators.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP, except those exclusively related to remote administration. Specifically:

- FCS_COP.1 - this requirement is intended to require that communications related to remote administration must be encrypted.
- FIA_AFL.1 - this requirement is intended to detect attempts by untrusted users to gain unauthorized access by repeated logon attempts. Only remote administration would support the ability for such an attempt and since the TOE does not support this feature, this requirement is not applicable. Note that it cannot be applied to the local administrator logon interface since the result would be to lock the authorized administrator out which would prevent them from re-enabling their own access.
- FIA_UAU.5 - this requirement is intended to prevent the reuse of authentication information for remote administration authentication attempts by the use of multiple authentication mechanisms such as passwords and single-use authentication mechanisms.
- FMT_MTD.2 - this requirement is intended to specify limits for authentication attempts and to specify actions to be taken if those limits are exceeded. Since FIA_AFL has been removed and the fact the TOE does not support remote administration, this requirement is not applicable.

Removal of these four requirement components impacts FAU_GEN.1 and FMT_MOF.1. FAU_GEN.1 has been refined such that it no longer requires auditing of events related to the removed requirements. Similarly, FMT_MOF.1 has been refined such that it no longer requires restricting the ability to manage settings associated with the removed requirements.

Additional requirement modifications are identified below:

Requirement Component	Modification
FAU_GEN.1	*Assignment* -the assignment started in the PP was completed with no additional attributes, however the assignment was refined to properly identify the referenced table.
FDP_IFF.1	*Assignment* - completed the assignment started in the PP with no additional attributes.
FIA_ATD.1	*Assignment* - completed the assignment started in the PP with no additional attributes.
FIA_UAU.1	*Added* - this requirement has been added since FIA_UAU.5 was removed and it is

Requirement Component	Modification
	implied the authorized administrator must be successfully authenticated before allowing any other TSF-mediated.
FMT_SMF.1	*Added* - this requirement was added in this Security Target to satisfy a dependency added to FMT_MOF.1 by International Interpretation RI#65. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
EAL4	*Added* - the PP requires only EAL 2 augmented with AVA_VLA.3. However, to satisfy the assurance requirements of environment requiring more assurance that the security functions are enforced, this Security Target has adopted the EAL 4 security assurance requirements, augmented with AVA_VLA.3 and also increased the minimum SOF level from SOF-basic to SOF-medium.

Note that the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments indicates that security functional requirements have specific strength of function metrics. Of those requirements, FIA_UAU.5 requires a FIPS PUB 140-1 compliant mechanism for single-use authentication, which is outside the scope of the evaluation. However, FIA_UAU.1 has been added to address the password authentication mechanism portion of the requirement. This is addressed in Strength of Function (SOF) Rationale. Additionally, the PP requires a minimum overall level of SOF-basic. However, this ST is claiming SOF-medium to conform better to the EAL 4 augmented with AVA_VLA.3 requirements.

Interpretations

The following changes to the have been made based on National and International Interpretations.

a) Security Functional Requirements

- FDP_IFF.1.3 through FDP_IFF.1-5 - these requirements was modified to reflect the proper selection. There is no impact on the requirement.

b) Security Assurance Requirements

Note: These interpretations have no impact on conformance with the PP since they only serve to clarify three of the assurance claims.

- ACM_CAP.2 - a new element was added to this component per International Interpretation RI #3.
- ACM_CAP.2.2D - this element was deleted to conform to U.S. National Interpretation I-0412.
- ACM_CAP.2.6C - this element was changed to conform to U.S. National Interpretation I-0412
- ADO_IGS.*.1C - this element was changed per International Interpretation RI #51
- AVA_VLA.*.1D and AVA_VLA.*.1D - these element were changed per International Interpretation RI #51
- AVA_VLA.3.1C through AVA_VLA.3.5C - these elements were changed and/or added per International Interpretation RI #51

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

In general, the rationale provided in the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments (DoDTFFPP), is directly applicable to the Security Target. As such, references to the corresponding sections are provided rather than recreating or repeating that rationale.

8.1 Security Objectives Rationale

The security objective rationale is presented in Sections 6.1and 6.2 of the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, (DoDTFFPP).

This ST has two assumptions and corresponding security objectives for the environment that is not included in the DoDTFFPP. A.CONSOLE and A.LOCATE are included in this ST as both an assumption and as the corresponding security objective. Since both statements are the same, the security objective addresses the assumption.

8.2 Security Requirements Rationale

Except as noted below, the security requirements rationale is presented in Sections 6.3 and 6.4 of the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, (DoDTFFPP).

Even though requirements (i.e., FCS_COP.1, FIA_AFL.1, FIA_UAU.5, and FMT_MTD.2), presumably supporting some of the objectives, have been excluded, the objectives are still satisfied since there is no related feature that might allow the objective and related threat to be violated. This effectively means that all references to these requirements should simply be ignored when examining the corresponding rationale in the DoDTFFPP.

All of the assumptions, threats, and security objectives have been reproduced from the DoDTFFPP to this ST, except for FMT_SMF.1. This requirement was included to satisfy a dependency of FMT_MOF.1 introduced in International Interpretation RI#65. FMT_SMF.1 requires that a defined set of security management functions are made available so that an administrator can effectively manage the security configuration of the TOE. This security functional requirement provides direct support for the O.SECFUN security objective.

8.3 Security Assurance Rationale

The NetScreen appliances meet all the U.S. Department of Defense Traffic-Filter Firewall Protection Profile Functional and Assurance Requirements. Additionally, the TOE conforms to all the Assurance Requirements for an EAL4 product. The resulting assurance level is therefore, EAL4 augmented with AVA_VLA.3.

The EAL 4 requirements that exceed EAL 2 augmented with AVA_VLA.3, by the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments are rationalized below:

ACM_AUT.1 Partial CM automation
Automation in the configuration management system can help reduce the risk of human error or negligence.

ACM_CAP.4 Generation support and acceptance procedures
It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that when changes are made, they are appropriate and correctly applied to the resulting TOE.

ACM_SCP.2 Problem tracking configuration management coverage
It is important that tracking of security flaws and problems with the TOE be appropriately tracked. This requirement helps to ensure that when problems are identified, they are appropriate and correctly tracked and applied to the resulting TOE

ADO_DEL.2 Detection of modification
It is important to maintain security during transfer of the TOE to the user. Using tamper-proof seals, digital signatures, and other methods ensures that the components of the TOE have not been tampered with prior to installation. This requirement helps to ensure authenticity of the delivered TOE.

ADV_FSP.2 Fully defined external interfaces
It is important to fully define all external interfaces to the product. This is necessary to correctly develop the product for interaction with other products. This requirement will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_HLD.2 Security enforcing high-level design
It is important to identify the basic structure of the TSF and the major hardware, firmware, and software elements of the product. This requirement will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_IMP.1 Subset of the implementation of the TSF
It is important given the high a level of assurance that additional documentation regarding the implementation of the product is provided. This requirement, through examination of this portion of the implementation subset, ensures the product can be adequately evaluated with regard to the requirements.

ADV_LLD.1 Descriptive low-level design
This high a level of assurance requires that additional documentation regarding the design of the product be provided. This requirement provides the detailed design specification necessary for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_SPM.1 Informal TOE security policy model
It is important to identify the security policies of the TSP. This requirement provides the structured representation of the security policies of the TSP. Additionally, this requirement provides the increased assurance that the functional specification corresponds to the security policies of the TSP and ultimately to the TOE security functional requirements.

ALC_DVS.1 Identification of security measures
It is important to document the procedures that cover the physical, procedural, personnel, and other security measures that are used in the development environment. This requirement identifies the physical security of the development location, controls on the development staff, and other procedural security measures employed to protect the development environment.

ALC_LCD.1 Developer defined life-cycle model

It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that the development and maintenance of the TOE are appropriately controlled.

ALC_TAT.1 Well-defined development tools
It is important that the correct tools and techniques are used in the development of the TOE. This requirement ensures that the tools and techniques used to analyze and implement the TOE are unambiguous.

ATE_COV.2 Analysis of Coverage
It is important to demonstrate that the TSF satisfies the TOE security functional requirements. This requirement ensures the completeness of the functional tests performed by the developer as well as the extent to which the TOE security functions are tested.

ATE_DPT. 1 Testing: high-level design
It is important to demonstrate the level of detail to which the developer tests the TOE. This requirement ensures that the TSF operates in accordance with the high-level design.

AVA_MSU.2 Validation of analysis components
It is important to demonstrate that the TOE is configured and operating in a manner that is secure. This requirement ensures that an administrator and/or user of the TOE and with an understanding of the guidance documents would be able to determine if the TOE is configured and operating in a manner that is insecure. .

8.4 Requirement Dependency Rationale

The rationale for not satisfying all dependencies is presented in Section 6.5 of the DoDTFFPP. This Security Target includes a single Security Functional Requirement not included in the DoDTFFPP - FMT_SMF.1. This requirement was included to satisfy a dependency of FMT_MOF.1 introduced in International Interpretation RI#65 and introduces no additional dependencies itself.

8.5 Explicitly Stated Requirements Rationale

All requirements in this ST are reproduced relative to the requirements defined in CC v2.1, using the conventions described in Section 1.4, Conventions.

In the context of CC v2.1 and International Interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements.

In the context of U.S. National interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements. However, it should be noted that some interpreted requirements have been *refined* (in accordance with the CC refinement rules) to its original form defined in CC v2.1.

- *Protected audit trail storage (FAU_STG.1)*: U.S National interpretations I-0422 and I-0423 serve to modify the original requirement by making it clear that the requirement is limited to unauthorized modifications and deletion or modification of audit records in the audit trail. Both of these changes serve to make implications in the CC explicit in the requirement and might also serve to narrow the scope (i.e., it can be argued that if the original requirement is satisfied, the interpretation would necessarily always be satisfied) of the requirements. Given that the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments uses the original version of this requirement from the CC v2.1, it was decided to use that version in this ST as well. Since the version of the requirement in this ST has a broader scope, any TOE meeting the requirement in this ST would meet the interpretations. The requirement stated in this ST is effectively a refinement of the version represented in the interpretations and is not an explicitly stated requirement.
- *Audit data generation (FAU_GEN.1)*: U.S. National Interpretation I-410 serves to modify the original requirement to only require that audit records include user identifies when applicable.

The U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments has already refined this requirement and this ST includes that version of the requirement. The modification suggested by I-410 has not been adopted since the relevant audit records will always have a user identity, even though the identity might not be valid (i.e., the identity typed in will be recorded). Hence, the requirement in this ST is effectively a refinement of the interpretation (i.e., any TOE meeting the requirement in this ST would meet the interpretation).

8.6 TOE Summary Specification Rationale

Each subsection in the TOE Summary Specification section describes a security function of the TOE. Each description is organized by requirement with rationale that indicates how each requirement is satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements. Table 3 Security Functions vs. Requirements Mapping identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

	AUDIT	INFORMATION FLOW	IDENTIFICATION & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF THE TSF
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.3	X				
FAU_STG.1	X				
FAU_STG.4	X				
FDP_IFC.1		X			
FDP_IFF.1		X			
FDP_RIP.1		X			
FIA_ATD.1			X		
FIA_UAU.1			X		
FIA_UID.2			X		
FMT_MOF.1(*)				X	
FMT_MSA.1(*)				X	
FMT_MSA.3				X	
FMT_MTD.1(*)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X
FPT_SEP.1					X
FPT_STM.1					X

Table 3 Security Functions vs. Requirements Mapping

8.7 Strength of Function (SOF) Rationale

Strength of function rating of SOF-medium was designated for this TOE to exceed the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments minimum level. The rationale for the chosen level is based on the low attack potential of the threat agents identified in the ST.

This security target includes a probabilistic or permutational function. The list of relevant security functions and security functional requirements includes:

- Identification and Authentication
    - FIA_UAU.1 - Timing of authentication

      The password used at administrator login from a locally connected console is the only probabilistic or permutational function on which the strength of the authentication mechanism depends.

The system places the following restrictions on the passwords selected by the user:

- The password must be at least eight long;

Furthermore, the user is told to not use consecutive sequences, or easily guessable passwords

The password space is calculated as follows:

Patterns of human usage are important considerations that can influence the approach to searching a password space, and thus affect SOF. Assuming the worst case scenario and the user chooses a number comprising only eight characters, the number of password permutations is:

52 alpha characters (upper and lower)
10 digits
+ 16 special characters (!, @, #, $, %, ^, &, *, (,), +, =, <, >, :, ;)
78 possible values

78^8 = (78*78*78*78*78*78*78*78) = **1,370,114,370,683,136**

The amount of time it takes to manually type a password given that authentication can only occur based upon manual input is 7 seconds. An attacker can at best attempt (60/7= 8.6 password entries every minute, or 514 password entries every hour.

On average, an attacker would have to enter (1,370,114,370,683,136 / 2 =) 685,057,185,341,568 passwords, over (685,057,185,341,568 / 514) 1,332,055,638,164 hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:

(1,332,055,638,164 / 24 / 365 =) 152,061,146 years

In accordance with annex B.3 in the CEM, the elapse time of attack is not practical and thus results in a High strength of function rating, which exceeds SOF-medium.

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.

9. Terminology and Acronyms

The following definitions are used throughout this ST. Reference the U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments, (DoDTFFPP) for additional terms and acronyms.

Address - The network portion of an IP address. Most IP addresses have a network portion and a node portion.

ASIC - Application-Specific Integrated Circuit. A customized microchip, which is designed for a specific application.

Authorized Administrator - A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized external IT entity - Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

CPU - Central Processing Unit. The CPU controls the operation of a computer.

DoDTFFPP - U.S. Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments.

DRAM - Dynamic Random Access Memory. A type of computer memory that is stored in capacitors on a chip. Most computers have DRAM chips, because they provide a lot of memory at a low cost.

External IT entity -- Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

FIPS - The Federal Information Processing Standards Publication (FIPS PUB) series issued by the U.S. National Institute of Standards and Technology as technical guidelines for U.S. Government procurements of information processing system equipment and services.

FIPS 140-1 - The U.S. Government standard for security requirements to be met by a cryptographic module used to protect unclassified information in computer and communication systems. The standard specifies four increasing levels (from 'Level 1' to 'Level 4') of requirements to cover a wide range of potential applications and environments. The requirements address basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference and electromagnetic compatibility (EMI/EMC), and self-testing.

Firmware - Software stored in ROM or PROM; essential programs that remain even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on disk.

Flash Memory - A small printed circuit board that holds large amounts of data in memory. Flash memory is used because it is small and holds its data when the computer is turned off.

HTTP - Hyper Text Transfer Protocol. The protocol most commonly used in the World-Wide Web to transfer information from Web servers to Web browsers.

ICMP - Internet Control Message Protocol. An extension to the Internet Protocol, which is used to communicate between a gateway and a source host, to manage errors and generate control messages.

IPsec - IP Security. An IP security protocol that provides for encapsulation of standard IP packets into Type 51 IP, allowing firewalls to recognize and admit encapsulated, encrypted data.

NAT - Network Address Translation. Allows a number of nodes on a network to access the Internet through a single IP address.

NetBIOS - Network Basic Input/Output System. An application programming interface used in conjunction with other programs to transmit messages between applications running on PCs hooked to a local area network.

Network - A composition of a communications media and components attached to that medium whose responsibility is the transfer of information. Such components may include automated information systems, packet switches, telecommunications controllers, distribution centers, technical management, and control devices. It is a set of devices such as computers, terminals, and printers that are physically connected by a transmission medium so that they can communicate with each other

Node - A concentration point in a network where numerous trunks come together at the same switch.

Packet - A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

PKI - public-key infrastructure. A system of Certificate Authority (CAs) (and, optionally, Registration Authority (RAs) and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.

SDRAM - Synchronous Dynamic Random Access Memory. High-speed DRAM that adds a separate clock signal to the control signals. SDRAM can transfer bursts of non-contiguous data at 100 MBytes/sec, and has an access time of 8-12 nanoseconds. It comes in 64-bit modules: long 168-pin DIMMs

Stateful inspection - Also referred to as *dynamic packet filtering*. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.

Tampering - An unauthorized modification that alters the proper functioning of equipment or system in a manner that degrades the security or functionality it provides

TCP/IP - Transmission Control Protocol/Internetwork Protocol - A communications protocol developed under contract from the U.S. Department of Defense to internetwork dissimilar systems. Transport Control Protocol/Internet Protocol. Generally refers to the Internet Protocol Suite, which includes TCP and IP, as well as several other protocols, used by computers to communicate with each other. TCP/IP is the standard protocol used on the Internet. It can also be used as a communications protocol in the private networks called intranets and in extranets. TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted

over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Tunneling - Use of one data transfer method to carry data for another method.

UDP - User Datagram Protocol. A communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Like TCP (Transmission Control Protocol), UDP is used with IP (the Internet Protocol). Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.

VPN - Virtual Private Network. An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. It includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system.

Zone(s) - 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).