NetScreen Appliances Security Target

Revision E

November 27, 2002

Prepared for:

NetScreen Technologies, Incorporated
350 Oakmead Parkway
Sunnyvale, California 94085

Prepared By:

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

Restricted Rights Legend

USE, DUPLICATION, OR DISCLOSURE IS SUBJECT TO THE RESTRICTIONS AS SET FORTH IN SUBPARAGRAPH [C][1][II] OF THE RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE OF DFARS 252.227-7013 (OR AT FAR 52.227 [C][1]).

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, encryption, and services requested. In support of the information flow security functions ensure that security relevant activity is audited, ensure that its own functions are protected from potential attacks, and provide 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

ST Version – Revision E

ST Date – November 27, 2002

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: `4.0.0r7.0`
    - Hardware version: 3010
- NetScreen 5XT (Part number: NS-5XT-00*, NS-5XT-10*, where * = 1, 3, 5, 7, or 9)
    - Firmware version: `4.0.0r7.0`
    - Hardware version: 3010
- NetScreen 25 (Part number: NS-025-00*, where * = 1, 3, 5, or 7)
    - Firmware version: `4.0.0r7.0`
    - Hardware version: 4010
- NetScreen 50 (Part number: NS-050-00*, where * = 1, 3, 5, or 7)
    - Firmware version: `4.0.0r7.0`
    - Hardware version: 4010
- NetScreen 100 (Part number: NS-100-001)

  - Firmware version: `4.0.0r7.0`
  - Hardware version: 3110
- NetScreen 204 (Part number: NS-204-00*, where * = 1, 3, 5, or 7)
  - Firmware version: `4.0.0r7.0`
  - Hardware version: 0110
- NetScreen 208 (Part number: NS-208-00*, where * = 1, 3, 5, or 7)
  - Firmware version: `4.0.0r7.0`
  - 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: `4.0.0r7.0`
  - Hardware version: 4110
- NetScreen 5200 (Part number: NS-5200-P00*-S00, NS-5200-P01*-S00, NS-5200-P01*-S01, NS-5200-P01*-S02, where * = A or D)
  - Firmware version: `4.0.0r7.0`
  - Hardware version: 3010

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.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
  - Evaluation Assurance Level 2 (EAL2).

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

- U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

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 only to authorized administrators; and while the operational NetScreen appliance components are protected from theft and tampering by means of encryption techniques and FIPS 140-1 tamper resistance standards, it is expected that they 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 network to which they are connected. The assurance requirements, EAL2, and the minimum strength of function, SOF-basic, were chosen to be consistent with those environments.

1.4 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: assignment, selection, and refinement.
  - 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 operation will be not be highlighted[1]. Rather, 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.

2. TOE Description

NetScreen appliances are integrated security network devices designed and manufactured by NetScreen Technologies, Incorporated, 350 Oakmead Parkway, Suite 500, Sunnyvale, CA 94085 U.S.A, herein called simply NetScreen.

NetScreen's line of appliances combines firewall, virtual private networking (VPN), and traffic management functions. Installing and managing appliances is accomplished using a built-in Web User Interface (WebUI), command line interface (CLI), or NetScreen's central management solutions. However, the Target of Evaluation (TOE) supports only administration via a command line interface (per TOE installation settings).

The TOE includes the NetScreen appliances that run ScreenOS `4.0.0r7.0`, a proprietary operating system. The NetScreen appliances that meet the definition of the TOE include the models: 5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200. Each identified model consists of hardware, firmware, 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, virtual private networking, and traffic management features.

2.2 Product Description

Each NetScreen appliance consists of physical interfaces that are network connections over specific physical ports, a custom operating system ScreenOS, and custom hardware to facilitate communications information flow through the

[1] Note that while highlighting (e.g., character formats) has not been copied, all of the characters have been copied. Hence, brackets that might serve to identify certain types of operations have been copied where present in the PP.

appliance. NetScreen-5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200 all share a very similar hardware architecture and packet flow. All utilize the GigaScreen ASIC for encryption and 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. Module variations are provided for additional throughput, capacity, and redundancy. Compile-time options control the scalability of the resources available to the specific model (e.g. buffer sizes, number of ports). Although the hardware architecture is similar across platforms, each platform has a unique combination of hardware components that support the specific performance and feature requirements for that platform. These customized hardware components include items such as memory type and size, CPU, GigaScreen ASIC type, and traffic and management interfaces.

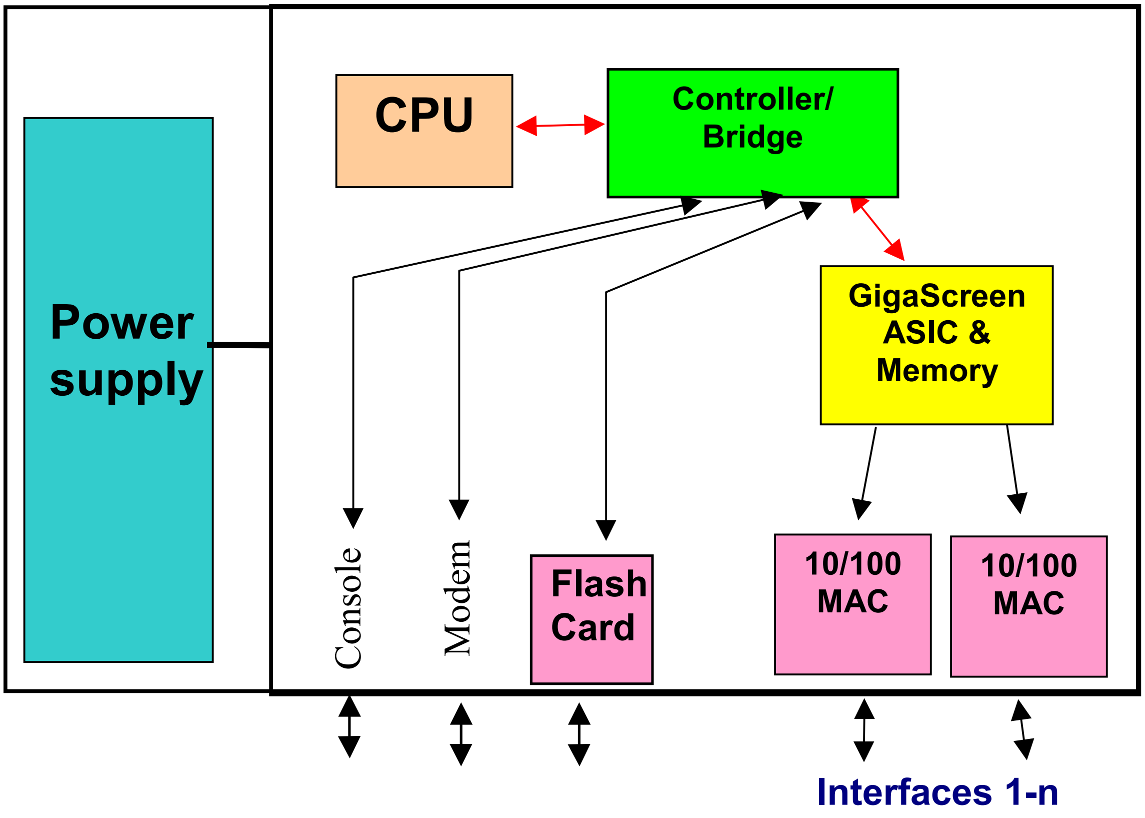
Each identified model runs with the same version of ScreenOS. The source code base for all platforms is identical, however, the code must be compiled and built into different object code for each platform because of the hardware differences described above. The following table identifies the differences in many NetScreen appliance models to underscore that the differences have no affect on the security functions claimed in this Security Target. Although larger appliances support a greater number of security policies, every device can establish the same security policy.

Appliance	Max Throughput	Max Sessions	Max # VPN tunnels	Max # Policies	Max # Virtual Systems	High Availability
NetScreen-5200	4G FW & 2G VPN	1,000,000	25,000	40,000	500	Yes
NetScreen-500	750M FW & 250M VPN	250,000	10,000	20,000	25	Yes
NetScreen-208	550M FW & 200M VPN	128,000	1,000	4,000	NA	Yes
NetScreen-204	400M FW & 200M VPN	128,000	1,000	4,000	NA	Yes
NetScreen-100	200M FW & 185M VPN	128,000	1,000	4,000	NA	Yes
NetScreen-50	170M FW &50M VPN	8,000	100	1,000	NA	Yes
NetScreen-25	100M FW; 20M VPN	4,000	25	500	NA	No
NetScreen-5XT	70M FW & 20M VPN	2,000	10	100	NA	No
NetScreen-5XP	10M FW & VPN	2,000	10	100	NA	No

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 flash memory.

The main components of a NetScreen appliance are the processor, ASIC, memory, interfaces, and surrounding chassis and components. The differences between NetScreen appliances are the types of processor(s), traffic interfaces, management interfaces, number of power supplies, type of ASIC, and redundancy to ensure high availability.



2.2.2 NetScreen ScreenOS

NetScreen ScreenOS provides the Universal Security Gateway Architecture (USGA), an architecture that offers great flexibility in designing the layout of network security. On NetScreen appliances with multiple interfaces, ScreenOS provides multiple security zones, can create specific information flow policies between zones, and control the type and direction of traffic flow between zones by establishing and enforcing information flow policies

One or more interfaces can be bound to each zone and enable a unique set of management and firewall attack screening options on a per-interface basis. Essentially, USGA provides for the creation of a number of zones required by a network, assign a number of interfaces for each zone, and design each zone interface to enforce a specific pre-defined security policy.

ScreenOS runs entirely in firmware and does not support hard drives or a programming environment.

2.3 Product Features

Each NetScreen appliance offers the following security functions:

- Audit: audit data is stored in event logs, self logs, and traffic logs. Audit messages can be collected to record security relevant events.
- 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 who are identified at a locally connected console through an internal authentication database. Administrative login is only supported through the locally connected console. Passwords are used to authenticate through a local authentication database. The only authentication mechanism supported by the TOE is the use of 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.
- 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 monitor, 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 ten models: 5XP, 5XT, 25, 50, 100, 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 are no assumptions for the correct operation of the platform except for the administrative console, which must be a VT-100 terminal or any device that can emulate a VT-100 terminal. The VT-100 terminal/emulator 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 terminal/emulator.

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

Traffic from one network node in a zone will only be forwarded to a node in another zone if the connection requests and the traffic satisfy the information flow policies configured in the NetScreen appliance. If data is received by an appliance that does not conform to those policies, it will be discarded and an audit record will be sent to the Self 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 system-level events as system events, traffic events, and self events. System events are recorded in “Event Log,” traffic events in “Traffic Log,” and traffic whose destination is the NetScreen appliance itself the “Self Log.” System events include appliance state changes and changes to a network configuration or a security policy by an administrator. Traffic events typically are samples of traffic flow for performance tuning, however traffic events will also show what is connected to the NetScreen appliances.

NetScreen appliances also can simultaneously send audit records to flash memory and a remote syslog as a backup device to the audit log and this backup is controlled by a NetScreen administrator. 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.[2] 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, as well as Zones of Addresses),
- 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

[2] 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.

- VSYS Administrator
- VSYS Read-only Administrator

Each administrator must log on using the console locally connected to the NetScreen appliance. Both 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/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. Locally connected VT-100 terminals or a workstation providing VT-100 terminal emulation may be used to enter administrative commands. Both the VT-100 and the workstation used to enter administrative commands are in the environment and not part of the TOE. The TOE does not support any remote administration functions.

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 physically connected to the network 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 VT-100 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 and secure usage assumptions 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 commercial and government 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 may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

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

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.

[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.

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.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

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]

[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.

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 from users on a connected network to users on another connected network, 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.

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.

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.

A.PHYSEC The TOE is physically secure.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered to be low.

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.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.PUBLIC The TOE does not host public data.

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

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

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

A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.[5]

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

[5] 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 Section 7, *Protection Profile Claims*). 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) 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.1.1)
	Subset residual information protection (FDP_RIP.1)
Identification and authentication (FIA)	Authentication failure handling (FIA_AFL.1) 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)
	Timing of authentication (FIA_UAU.1)
	Single-use authentication mechanisms (FIA_UAU.4) do not apply since the TOE does not support remote administration where replay of authentication data might be relevant. As a result, it has been omitted from this section (including removal of component FIA_UAU.4 as well as removal of FMT_MOF.1 references 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) *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.*
	Static attribute initialization (FMT_MSA.3)
	Specification of Management Functions (FMT_SMF.1)[6]
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Non-bypassability of the TSP (FPT_RVM.1)
	Reliable time stamps (FPT_STM.1)
	TSF domain separation (FPT_SEP.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 relevant auditable events for the minimal or basic level of audit specified in **the Table below**; and
c) [the event in **the Table below** listed at the "extended" level].

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	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	basic	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	basic	All use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	Basic	All decisions on requests for information flow.	The presumed address of the source and destination subject.
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation

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

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, subjects identities, 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 four **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 a valid address on the other connected network.]

5.1.2.2.3 FDP_IFF.1.3

The TSF shall enforce the [none].

5.1.2.2.4 FDP_IFF.1.4

The TSF shall provide the following [none].

5.1.2.2.5 FDP_IFF.1.5

The TSF shall explicitly authorize an information flow based on the following rules: [none].

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:

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

5.1.3.2 Timing of authentication (FIA_UAU.1)[7]

5.1.3.2.1 FIA_UAU.1.1

The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator ~~**or authorized external IT entity**~~ accessing the TOE to be performed before the authorized administrator ~~**or authorized external IT entity**~~ is authenticated.

5.1.3.2.2 FIA_UAU.1.2

The TSF shall require each authorized administrator ~~**or authorized external IT entity**~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator ~~**or authorized IT entity**~~.

[7] The TOE does not provide any support for remote administration. As such, the TOE does not provide any support for these features

5.1.3.3 User identification before any action (FIA_UID.2)

5.1.3.3.1 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 (FMT_MOF.1)[8]

5.1.4.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to perform the functions:

a) [{start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

~~**d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);**~~

~~**e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);**~~

~~**f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);**~~

~~**g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);**~~

h) modify and set the time and date;

i) archive, create, delete, empty, and review the audit trail;

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;

k) recover to the state following the last backup;

~~**l) additionally, if the TSF supports remote administration from either an internal or external network:**~~

- ~~**enable and disable remote administration from internal and external networks;**~~
- ~~**restrict addresses from which remote administration can be performed;**~~

m) [**and no other functions**]].

[8] The TOE does not provide any support for remote administration. As such, the TOE does not provide any support for these features

to [an authorized administrator].

5.1.4.2 Static attribute initialization (FMT_MSA.3)

5.1.4.2.1 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.

5.1.4.2.2 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.

5.1.4.3 Specification of Management Functions (FMT_SMF.1)

5.1.4.3.1 FMT_SMF.1.1

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

5.1.4.4 Security roles (FMT_SMR.1)

5.1.4.4.1 FMT_SMR.1.1

The TSF shall maintain the role [authorized administrator].

5.1.4.4.2 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 Requirements Dependencies

The dependencies of the TOE security functional requirements are met through the functionality of the TOE.

The table below maps the TOE functional requirements to the corresponding requirements they are dependent on. The table demonstrates that all TOE functional security requirement dependencies are met within the ST except where noted in Section 8.3Requirement Dependency Rationale.

Dependency

Requirement	CC Identifier	FMT_SMF.1[9]
	FMT_MOF.1	X

Table 2 SFR mapping to SFR dependency

5.3 Security Functional Requirements for the IT Environment

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

5.4 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components as specified in Part 3 of the Common Criteria. The SARs have been changed, when necessary, to conform to National and International Interpretations.

Assurance Class	Assurance Components
Configuration Management (ACM)	Configuration items (ACM_CAP.2)
Delivery and Operation (ADO)	Delivery procedures (ADO_DEL.1)
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	Informal functional specification (ADV_FSP.1)
	Descriptive high-level design (ADV_HLD.1)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance Documents (AGD)	Administrator guidance (AGD_ADM.1)
	User Guidance (AGD_USR.1)
Tests (ATE)	Evidence of coverage (ATE_COV.1)

[9] This dependency requirement has been added to conform to Interpretation RI#65.

Assurance Class	Assurance Components
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

Table 3 EAL2 Assurance Components

5.4.1 Configuration Management (ACM)

5.4.1.1 Configuration Items (ACM_CAP.2)

5.4.1.1.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

5.4.1.1.2 ACM_CAP.2.2D

~~**The developer shall use a CM system.**~~[10]

5.4.1.1.3 ACM_CAP.2.3D

The developer shall provide CM documentation.

5.4.1.1.4 ACM_CAP.2.1C

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

5.4.1.1.5 ACM_CAP.2.2C

The TOE shall be labeled with its reference.

5.4.1.1.6 ACM_CAP.2.3C

The CM documentation shall include a configuration list.

5.4.1.1.7 International Interpretation RI #3

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

5.4.1.1.8 ACM_CAP.2.4C

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

5.4.1.1.9 ACM_CAP.2.5C

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

5.4.1.1.10 ACM_CAP.2.6C

The ~~**CM system**~~ **configuration**[11] list shall uniquely identify all configuration items.

[10] This element has been stricken to conform to U.S. National Interpretation I-412.
[11] This change has been made to conform to U.S. National Interpretation I-412.

5.4.1.1.11 ACM_CAP.2.1E

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

5.4.2 Delivery and Operation (ADO)

5.4.2.1 Delivery Procedures (ADO_DEL.1)

5.4.2.1.1 ADO_DEL.1.1D

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

5.4.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

5.4.2.1.3 ADO_DEL.1.1C

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

5.4.2.1.4 ADO_DEL.1.1E

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

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

5.4.2.2.1 ADO_IGS.1.1D

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

5.4.2.2.2 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.[12]

5.4.2.2.3 ADO_IGS.1.1E

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

5.4.2.2.4 ADO_IGS.1.2E

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

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

5.4.3 Development (ADV)

5.4.3.1 Fully defined external interfaces (ADV_FSP.1)

5.4.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.4.3.1.2 ADV_FSP.1.1C

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

5.4.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.4.3.1.4 ADV_FSP.1.3C

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

5.4.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

5.4.3.1.6 ADV_FSP.1.1E

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

5.4.3.1.7 ADV_FSP.1.2E

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

5.4.3.2 Security enforcing high-level design (ADV_HLD.1)

5.4.3.2.1 ADV_HLD.1.1D

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

5.4.3.2.2 ADV_HLD.1.1C

The presentation of the high level design shall be informal.

5.4.3.2.3 ADV_HLD.1.2C

The high level design shall be internally consistent.

5.4.3.2.4 ADV_HLD.1.3C

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

5.4.3.2.5 ADV_HLD.1.4C

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

5.4.3.2.6 ADV_HLD.1.5C

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.

5.4.3.2.7 ADV_HLD.1.6C

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

5.4.3.2.8 ADV_HLD.1.7C

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

5.4.3.2.9 ADV_HLD.1.1E

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

5.4.3.2.10 ADV_HLD.1.2E

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

5.4.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.4.3.3.1 ADV_RCR.1.1D

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

5.4.3.3.2 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.

5.4.3.3.3 ADV_RCR.1.1E

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

5.4.4 Guidance Documents (AGD)

5.4.4.1 Administrator Guidance (AGD_ADM.1)

5.4.4.1.1 AGD_ADM.1.1D

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

5.4.4.1.2 AGD_ADM.1.1C

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

5.4.4.1.3 AGD_ADM.1.2C

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

5.4.4.1.4 AGD_ADM.1.3C

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

5.4.4.1.5 AGD_ADM.1.4C

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

5.4.4.1.6 AGD_ADM.1.5C

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

5.4.4.1.7 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.

5.4.4.1.8 AGD_ADM.1.7C

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

5.4.4.1.9 AGD_ADM.1.8C

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

5.4.4.1.10 AGD_ADM.1.1E

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

5.4.4.2 User Guidance (AGD_USR.1)

5.4.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.4.4.2.2 AGD_USR.1.1C

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

5.4.4.2.3 AGD_USR.1.2C

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

5.4.4.2.4 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.

5.4.4.2.5 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.

5.4.4.2.6 AGD_USR.1.5C

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

5.4.4.2.7 AGD_USR.1.6C

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

5.4.4.2.8 AGD_USR.1.1E

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

5.4.5 Security Testing (ATE)

5.4.5.1 Analysis of coverage (ATE_COV.1)

5.4.5.1.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

5.4.5.1.2 ATE_COV.1.1C

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

5.4.5.1.3 ATE_COV.1.1E

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

5.4.5.2 Functional testing (ATE_FUN.1)

5.4.5.2.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.4.5.2.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.4.5.2.3 ATE_FUN.1.1C

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

5.4.5.2.4 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.

5.4.5.2.5 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.

5.4.5.2.6 ATE_FUN.1.4C

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

5.4.5.2.7 ATE_FUN.1.5C

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

5.4.5.2.8 ATE_FUN.1.1E

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

5.4.5.3 Independent testing – sample (ATE_IND.2)

5.4.5.3.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.4.5.3.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.4.5.3.3 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.

5.4.5.3.4 ATE_IND.2.1E

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

5.4.5.3.5 ATE_IND.2.2E

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

5.4.5.3.6 ATE_IND.2.3E

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

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

5.4.5.4.1 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.

5.4.5.4.2 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.

5.4.5.4.3 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.

5.4.5.4.4 AVA_SOF.1.1E

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

5.4.5.4.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.4.5.5 Developer analysis (AVA_VLA.1)

5.4.5.5.1 AVA_VLA.1.1D

The developer shall perform a vulnerability analysis.[13] ~~and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~

5.4.5.5.2 AVA_VLA.1.2D

The developer shall provide vulnerability analysis documentation.[14] ~~document the disposition of obvious vulnerabilities.~~

5.4.5.5.3 AVA_VLA.1.1C

~~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 obvious ways in which a user can violate the TSP.[15]

5.4.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[16]

5.4.5.5.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.[17]

5.4.5.5.6 AVA_VLA.1.1E

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

[13] This change has been made to conform to Interpretation RI#51
[14] This change has been made to conform to Interpretation RI#51
[15] This change has been made to conform to Interpretation RI#51
[16] This change has been made to conform to Interpretation RI#51
[17] This change has been made to conform to Interpretation RI#51

5.4.5.5.7 AVA_VLA.1.2E

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

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 default values; 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 system-level events as system events, traffic events, and self events. System events are recorded in “Event Log,” traffic events in “Traffic Log,” and traffic whose destination is the NetScreen appliance itself the “Self Log.” System events include appliance state changes and changes to a network configuration or a security policy by an administrator. Traffic events typically are samples of traffic flow for performance tuning, however traffic events will also show what is connected to the NetScreen appliances.

The information contained in the three types of logs include the date and time of event, the type of event, the subject identify, and the outcome (success or failure) of the event. The logs contain the following auditable events:

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

b) All auditable events for the level of audit as specified in table listed in FAU_GEN.1.1;

c) Starting and Stopping a NetScreen appliance,

d) Administrator commands,

e) User I&A success and failures,

f) 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 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 policy” 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

A series of over 70 "get" commands provided by the CLI provide the appropriate administrator the tools to review the logs and search by specific attributes of each audited event. The audit security function addresses this requirement.

FAU_STG.1 Protected Audit Trail Storage

The only external interface into the flash storage is through the administrative CLI. Only specific administrators have access to the logs and those administrator(s) are restricted to a specific console. The only means to access the audit logs are via the console that is limited to administrative use only. The audit function addresses this requirement.

FAU_STG.4 Prevention of Audit Data Loss

NetScreen appliances provide flash storage that holds 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. Flash 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 the flash 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 is not part of the TOE.

The technique of overwriting the oldest audit records once the flash 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 the flash 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. By overwriting the oldest audit information with the latest audit information to a very high-speed flash memory the flash memory can never lose audit information in that no audit records can ever be "dropped" or not written.

The danger of losing audit information is that audit records in the flash memory may be overwritten before that record is actually written to the backup syslog. Through the use of a FIFO technique of writing to the flash memory, the rate of audited events and bursts of audited data can be accommodated. Additionally, the NetScreen appliances can be configured to notify the administrator when the logs have reached a specified percentage.

There is an internal field that identifies when an audit record has been written to the syslog server. If this field indicates that the record has not been written to the syslog server, 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 server. Once all existing audit records are written to the syslog server, 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 (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.

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.

Packets sent to the NetScreen appliance are held in a temporary storage of packet information. Invalid packets are dropped and do not traverse through the NetScreen appliance. Valid packets are processed and possibly routed according to the access control policies of the NetScreen appliance. Information copied from the temporary storage to form routed packets is limited to the information contained in the packet received. Therefore, only information associated with that packet traverses through the 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

The UNAUTHENTICATED SFP is configured through the locally connected console, to which only administrators have physical and logical (via username and password) access. Through the console, administrators add, remove, and change values within the security policy.

Because only authorized administrators can access the security management functions via the console, the TSF restricts the ability to perform the following functions to an authorized administrator:

a. start-up and shutdown;
b. create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c. create, delete, modify, and view administrator attribute values defined in FIA_ATD.1;
d. modify and set the time and date;
e. archive, create, delete, empty, and review the audit trail;
f. backup of administrator attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
g. recover to the state following the last backup.

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. The information flow function addresses this requirement.

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. But, 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 administrator 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 physically connected to the network so that an appliance cannot be bypassed. Further, cryptographic techniques and FIPS level 2 tamper techniques are used to protect against or serve to identify tampering and theft of a NetScreen appliance. 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 subinterface), 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 proprietary operating system that runs in hardware, remains memory resident, and supports only one process, itself. 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 EAL2 assurance requirements:

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

6.2.1 Configuration Management

The configuration management measures applied by NetScreen ensure that configuration items are uniquely identified and the TOE is uniquely labeled. 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

The Configuration Management assurance measure satisfies the ACM_CAP.2 assurance requirements

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-100 Installers Guide
    - NS-200 Series Installers Guide

  - NS-25 Installers Guide
  - NS-50 Installers Guide
  - NS-500 Installers Guide
  - NS-5000 Series Installers Guide
  - NS-5XP Installers Guide
  - NS-5XT 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-100 Installers Guide
  - NS-200 Series Installers Guide
  - NS-25 Installers Guide
  - NS-50 Installers Guide
  - NS-500 Installers Guide
  - NS-5000 Series Installers Guide
  - NS-5XP Installers Guide
  - NS-5XT Installers Guide
- NetScreen Message Log Reference Guide
- NetScreen Concepts and Examples ScreenOS Reference Guide
- NetScreen Command Line Interface Reference Guide

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

- ADO_DEL.1;
- 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 Correspondence Matrix

The Design Documentation security assurance measure satisfies the following security assurance requirements:

- ADV_FSP.1: The NetScreen Functional Specification, including its references, describes the external interfaces to the TOE.

- ADV_HLD.1: The NetScreen High Level Design, and its references, decomposes the TOE into subsystems.
- ADV_RCR.1: The NetScreen Correspondence Matrix document:
    - 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.

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

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1: The test case descriptions in the NetScreen Test Cases for the Common Criteria document and the mapping provided in the NetScreen Correspondence Matrix document describe the test cases for each of the security-relevant interfaces of the TOE and indicate which test cases are used to test which interfaces.
- ATE_FUN.1: The NetScreen Test Cases for the Common Criteria document 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 were made available for independent testing.

6.2.5 Vulnerability Assessment

All of the SOF claims are based on password space calculations and is documented in Section 8.6 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_SOF.1; and,
- AVA_VLA.1.

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.

This Security Target includes all of the assumptions and threats statements described in the PP, verbatim. There are no organizational security policies described in the PP or this ST. 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 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 this feature is not supported by the TOE, 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.4 – this requirement is intended to prevent the reuse of authentication information for remote administration authentication attempts.

Removal of these three 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	*Refinement* – changed table references to the table in the ST.
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	*Refinement* – removed inapplicable references to an “authorized external IT entity”.

Note that the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments indicates that a number of security functional requirements have specific strength of function metrics. Of those requirements, FIA_UAU.4 is a FIPS 140 issue, outside the scope of the evaluation. The second, FIA_UAU.1, is addressed in section 8.6 where at least minimum compliance with the 1 in 1,000,000 probability, suggested in the PP, for a successful guess can be seen to be satisfied. The PP requires a minimum level of SOF-basic.

Interpretations

The following changes have been made to requirements based on National and International Interpretations. 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.*.1 – this element was changed per International Interpretation RI #51
- AVA_VLA.*.1D - this element was changed per International Interpretation RI #51
- AVA_VLA.1.1C through AVA_VLA.1.3C – 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. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments (TFFPP) is directly applicable to the Security Target. As such, references to the corresponding sections are provided rather than recreating or repeating that rationale. The exception involves the omission of remote administration related requirements. This only affects the rationale for security requirements, as described in that section.

8.1 Security Objectives Rationale

The security objective rationale is presented in sections 6.1and 6.2 of the TFFPP.

This ST has a single assumption and corresponding security objective for the environment that is not included in the TFFPP. A.CONSOLE is 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

The security requirements rationale is presented in sections 6.3 and 6.4 of the TFFPP.

All of the assumptions, threats, and security objectives have been reproduced from the TFFPP to this ST. Even though requirements (i.e., FCS_COP.1, FIA_AFL.1, and FIA_UAU.4), 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 TFFPP.

8.3 Requirement Dependency Rationale

The ST satisfies the requirement dependencies of the Common Criteria, except as noted below. **Table 4 Requirement Dependency Rationale** lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

The dependency requirement of FMT_SMF.1 was included to conform to Interpretation RI#65.

Functional Component	Dependency	Included
Management of security functions behavior (FMT_MOF.1)	FMT_SMF.1	FMT_SMF.1

Table 4 Requirement Dependency Rationale

The rationale for not satisfying all dependencies is presented in section 6.5 of the TFFPP.

Note also that none of the requirements in this ST depend on the requirements that have been omitted (i.e., FCS_COP.1, FIA_AFL.1, and FIA_UAU.4). Hence, removal of these requirements does not affect the rationale presented in the TFFPP, except that the rationale provided for failing to satisfy FCS_COP.1 dependencies is now irrelevant and should be ignored.

8.4 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.

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. Government Traffic-Filter Firewall Protection Profile for Low-Risk 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 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. Government Traffic-Filter Firewall Protection Profile for Low-Risk 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).
- There are a number of U.S. National Interpretations (e.g., I-407, I-429) that serve to change assignments. In each of these cases, the assignment has already been either entirely or partially completed in the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. As a result, this ST only completes those assignments where the PP left them incomplete. In these cases, the final requirements in this ST seem to be compatible with the interpretations.
- There are a number of interpretations, such as those referenced in the previous requirement, that change the names of the associated requirements. This ST only uses the names originally defined in the CC Part 2 and Part 3. These names have no bearing on the actual content of the requirements, but changing of the identifiers might be considered a refinement relative to the associated interpretations.

8.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, 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 Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to fulfill the TOE security requirements. Table 5 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 Section 8.6.

	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.3				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X
FPT_SEP.1					X
FPT_STM.1					X

Table 5 Security Functions vs. Requirements Mapping

8.6 Strength of Function (SOF) Rationale

Strength of function rating of SOF-basic was designated for this TOE to meet 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 this 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.

Authorized users (administrators) of the system choose their own passwords numbers when initially authorized to use the system, and change passwords every 30 days. The system places the following restrictions on the passwords selected by the user:

- The password must be at least eight and no greater than ten characters 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
+ 10 special characters
72 possible values

72^8 = (72*72*72*72*72*72*72*72) = **722,204,136,308,736**

The authentication mechanism is designed with a terminal locking feature. Upon the third failed authentication attempt the terminal is locked for thirty seconds. The failed authentication count is reset after thirty seconds so that an attacker can at best attempt four password entries every minute, or 240 password entries every hour.

On average, an attacker would have to enter (722,204,136,308,736 / 2 =) **361,102,068,154,368** passwords, over (361,102,068,154,368 / 240) **1,504,591,950,643** hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:

(1,504,591,950,643 / 24 / 365 =) **171,757,071** years

In accordance with Table 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-basic.

8.7 PP Claims Rationale

See section 7, Protection Profile Claims.