Juniper Networks Security Appliances

Security Target:

EAL4

Revision L

December 19, 2005

P/N - 093-0896-000

Prepared for:
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, California 94089-1206
http://www.juniper.net

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046
http://www.saic.com/

and

EnPointe Technologies Inc.
8310 N. Capital of Texas Highway, Ste 305
Austin, TX 78731
http://www.enpointe.com

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

LIST OF FIGURES

1.0 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 security appliances Target of Evaluation (TOE) primarily supports the definition of and enforces information flow policies among network nodes. The security 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 security appliance. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the security appliances ensures that security relevant activity is audited, that its own functions are protected from potential attacks, and provides the security tools to manage all of the security functions.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)
- Terminology and Acronyms (Section 9)

1.1 Security Target, TOE and CC Identification

ST Title – Juniper Networks Security Appliances Security Target: EAL4

ST Revision - L

ST Date – December 19, 2005

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

- Juniper Networks NetScreen-5GT (Part number: NS-5GT-00*, NS-5GT-10*, NS-5GT-20*, where * = 1, 3, 5, 7, 8
    - Firmware version: 5.0.0r9.r
    - Hardware version: 1010
- Juniper Networks NetScreen-5XT (Part number: NS-5XT-00*, NS-5XT-10*, where * = 1, 3, 5, 7, or 9)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 1010
- Juniper Networks NetScreen-25 (Part number: NS-025-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 4010
- Juniper Networks NetScreen-50 (Part number: NS-050-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 4010

EAL4

- Juniper Networks NetScreen-204 (Part number: NS-204-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 0110
- Juniper Networks NetScreen-208 (Part number: NS-208-00*, where * = 1, 3, 5, or 7)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 0110
- Juniper Networks 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: 5.0.0r9.o
    - Hardware version: 4110
- Juniper Networks NetScreen ISG 1000 (Part number: NS-ISG-1000, NS-ISG-1000-DC, NS-ISG-1000B, NS-ISG-1000B-DC)
    - Firmware version: 5.0.0r9.y
    - Hardware version: 3010
- Juniper Networks NetScreen ISG 2000 (Part number: NS-ISG-2000, NS-ISG-2000-DC, NS-ISG-2000B, NS-ISG-2000B-DC)
    - Firmware version: 5.0.0r9.y
    - Hardware version: 3010
- Juniper Networks NetScreen 5200 (Part number: NS-5200, NS-5200-DC)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 3010
- Juniper Networks NetScreen 5400 (Part number: NS-5400 NS-5400-DC)
    - Firmware version: 5.0.0r9.o
    - Hardware version: 3010

CC Identification - Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 14508, including applicable International Interpretations.

EAL4

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

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

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

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

Juniper has elected to pursue a more rigorous assurance evaluation. The product meets all the Traffic-Filter Firewall Protection Profile Functional and Assurance Requirements, additionally the TOE conforms to all the Assurance Requirements for an EAL4 product.

1.3 Strength of Environment

The security 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 security appliances components can be appropriately protected from physical attacks. Essentially, the security appliances management console must be controlled to restrict access to only authorized administrators. It is expected that the security appliances will be protected to the extent necessary to ensure they remain connected to the networks they protect. Essentially, this means that the security appliance components need to be protected to the degree appropriate to protect the networks to which they are connected. The assurance requirements, EAL4, and the minimum strength of function, SOF-medium, were chosen to be consistent with those environments.

1.4 Conventions, Terminology, and Acronyms

1.4.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST, with the exception of FDP_IFC.1a(EXP), FDP_IFC.1b(EXP), FDP_IFC.1c(EXP), FDP_IFF.1a(EXP), FDP_IFF.1b(EXP) and FDP_IFF.1c(EXP) are reproduced relative to the requirements defined in CC v2.1.
- Security Functional Requirements - Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_IFF.1a(EXP) and FDP_IFF.1b(EXP) indicate that the ST includes two iterations of the FDP_IFF.1 requirement, a and b.
    - 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 …").

- This ST includes explicitly stated requirements. Each requirement that is explicitly stated is identified by the letters EXP in parenthesis (EXP).
- If an operation was completed in a related Protection Profile or Interpretation, the corresponding PP or Interpretation should be consulted to determine what operations might have already been performed.

Other sections of the ST use bolding and italics, without brackets, to highlight text of special interest, such as captions.

1.4.2 Terminology and Acronyms

See Terminology and Acronyms section.

2.0 TOE Description

Juniper Networks security appliances, hereafter referred to as security appliances, are integrated security network devices designed and manufactured by Juniper Networks, 194 North Mathilda Avenue, Sunnyvale, California 94089-1206 U.S.A, herein called simply Juniper.

Juniper's line of security appliances combines firewall, virtual private networking (VPN), and traffic management functions. All security appliances have hardware accelerated IPSec encryption and very low latency, allowing them to fit into any network. Installing and managing appliances is accomplished using a command line interface (CLI).

The TOE includes the security appliances that run ScreenOS 5.0.0r9, a custom operating system. The security appliances that meet the definition of TOE include the models: 5GT, 5XT, 25, 50, 204, 208, 500, ISG 1000, ISG 2000, 5200, and 5400. Each identified model consists of hardware and ScreenOS that runs in firmware.

The security 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).

To perform routing functions ScreenOS relies on a virtual router (VR) component, which functions as a router and has its own interfaces and its own routing table. In ScreenOS, a security appliance supports two predefined virtual routers, trust-vr and untrust-vr. This allows the security appliance to maintain two separate routing tables and to conceal the routing information in one virtual router from the other. For example, the untrust-vr is typically used for communication with untrusted parties and does not contain any routing information for the protected zones. Routing information for the protected zones is maintained by the trust-vr. Thus, no internal network information can be gleaned by the surreptitious extraction of routes from the untrust-vr. There are no limitations on the number of virtual routers to be used in the evaluated configuration.

2.1 Product Type

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

2.2 Product Description

Juniper Networks NetScreen-5GT, 5XT, 25, 50, 204, 208, 500, ISG 1000, ISG 2000, 5200, and 5400 all share a very similar hardware architecture and packet flow. All utilize custom ASICs for policy lookup acceleration, while a CPU is used as the main processor. All run ScreenOS with common core features across all products. All security appliances perform the same security functions and export the same types of interfaces. A sample of the differences between these products is listed below.

- The Juniper Networks NetScreen-5GT, 5XT, 25, 50, 204, 208, and 500 use a version of the GigaScreen ASIC that accelerates policy look-ups.
- The Juniper Networks NetScreen-204, 208, and 500 utilize dual-port memory for faster processing and faster packet flow.
- The Juniper Networks NetScreen-ISG1000 & ISG2000 utilizes a Cavium Nitrox Lite ASIC, which serves requests from 100 Mbps up to 1 Gbps of data.
- The Juniper Networks NetScreen-5200 and 5400 are different than the rest of the products. They utilizes one or more GigaScreen-II ASICs, which provide a lot more functionality than the GigaScreen ASIC. The GigaScreen-II ASIC is capable of providing most of the functionality, and uses the CPU as a co-processor for handling management traffic and first packet inspections (policy lookups). So the GigaScreen-II ASIC can process an incoming packet, perform a session lookup, NAT, TCP/IP sequence checking, and can then send the packet back out of the device without the CPU every seeing it. The only time the CPU is used is for first packet inspection, management traffic, and packet fragment reassembly for inspection.

2.2.1 Hardware

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

The main components of a security appliance are the processor, ASIC, memory, interfaces, and surrounding chassis and components. The differences between security 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 ScreenOS

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

- Stateful inspection firewall
- Traffic management
- Site-to-Site VPN using manual key authentication

ScreenOS does not support a programming environment.

2.2.3 Policies

Security appliances enforce information flow control decisions by defining policies which permit, deny, or tunnel information flows in accordance with the rules defined in each policy. All policies on a security appliance include the following attributes:

- Direction – The direction of traffic between two security zones (from a source zone to a destination zone)
- Source address – The address from which traffic initiates
- Destination address – The address to which traffic is sent
- Service – The type of traffic transmitted
- Action – The action that the security appliance performs when it receives traffic meeting the first four criteria: permit, deny, nat, or tunnel

Security appliances provide three different types of policies which support the information flow control decisions enforced by the TOE. This includes Interzone Policies, Intrazone Policies, and Global Policies. The SFRs, FDP_IFF.1a(EXP).3, FDP_IFF.1b(EXP).3, and FDP_IFF.1c(EXP).3 specify the manner in which each of these three types of policies are invoked when determining the appropriate decision to make on an information flow (Global policy lookup is not supported by the TOE in Authenticated Transparent Mode). The following sections describe differences between each of these three types of policies.

2.2.3.1 Interzone policies

Interzone policies provide traffic control between security zones. You can set interzone policies to permit, deny, or tunnel traffic from one zone to another. Using stateful inspection techniques, the TOE maintains a table of active TCP sessions and active UDP “pseudo” sessions so that it can allow replies to service requests.

2.2.3.2 Intrazone Policies

Intrazone policies provide traffic control between interfaces bound to the same security zone. The source and destination addresses are in the same security zone, but reached via different interfaces on the TOE. Like interzone policies, intrazone policies control traffic flowing unidirectionally. To allow traffic initiated at either end of a data path, you must create two policies—one policy for each direction.

Intrazone policies do not support VPN tunnels or source network address translation (NAT-src) when it is set at the interface level (**set interface** *interface* **nat**). However, intrazone policies do support policy-based NAT-src and NAT-dst. They also support destination address translation when the policy references a mapped IP (MIP) as the destination address. A mapped IP address is a direct one-to-one mapping of traffic destined for one IP address to another IP address.

2.2.3.3 Global Policies

Unlike interzone and intrazone policies, global policies do not reference specific source and destination zones. Global policies reference user-defined Global zone addresses or the predefined Global zone address “any”. These addresses can span multiple security zones. For example, if you want to provide access to or from multiple zones, you can create a global policy with the Global zone address “any”, which encompasses all addresses in all zones.

2.2.3.3.1 Order of Invocation

When the TOE initiates a policy lookup, it first checks to see if the security zones are the same or different. If the zones are different, the TOE performs a policy lookup in the interzone policy set list. If the zones match, the TOE performs a policy lookup in the intrazone policy set. If a policy is not found within either the interzone or intrazone set lists, the TOE performs a policy lookup in the global policy set list.

2.2.4 Services

Security appliances enforce policies based on a service. A service specifies the protocol (TCP or UDP), the port number, the service group, the timeout and the flag associated to a specific service and maps the service to a defined name.

EAL4

2.3 Product Features

Each security appliance offers the following security functions:

- Audit: Audit data is stored in memory and is separated into three types of logs; events, traffic logs, and self logs. Events are system-level notifications and alarms which are generated by the system to indicate events such as configuration changes, network attacks detected, or administrators logging in our out of the device. Traffic logs are directly driven by policies that allow traffic to go through the device. Both audit events and traffic messages can be further defined depending on the severity of the message and/or event.
- Information Flow Policy: Traffic flow from one network node to another network node is controlled by an information 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. If an authenticated information flow policy is enforced (i.e. FDP_IFC.1a or FDP_IFC.1c), then the information flow policy additionally utilizes cryptographic support for the authentication and protection of the information flows associated with the information flow policy.
- Identification & Authentication: The security appliances provide an authentication mechanism for administrative users through an internal authentication database. Administrative login is only supported through the locally connected console. The only authentication mechanisms supported by the TOE is passwords.
- Security Management: Every security 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 security appliance through a direct serial connection. The authorized administrator must be successfully identified and authenticated before they are permitted to perform any security functions on the TOE.
- TOE Protection: Each security 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 or between two networks within the same network zone passes through the TOE; however, no protocol services are provided for user communication with the security appliance itself. The TOE also preserves its configuration for a trusted recovery in the event that the configuration has been modified and not saved or if the security appliance has been ungracefully shutdown. The TOE additionally protects the session table by enforcing destination-based session limits and applying procedures to limit the lifetime of sessions when the session table reaches the defined watermark.

2.4 TOE Configurations

The TOE supports a variety of configurations. The TOE provides three possible ways to configure a network interface. A network interface may be configured to operate in Transparent Mode, NAT Mode, or Route Mode. In addition, the TOE also supports Site-To-Site VPNs using a pre-shared key for authentication. These various configurations are further described below.

2.4.1 Interface Modes

The TOE supports three types of interface modes. These interface modes include a Transparent Mode, NAT Mode, and Route Mode each of which determine how packets are routed and filtered by the TOE. Each instance of the TOE can include one, a combination of, or all three interface modes. However, each individual network interface may only be configured with one interface mode and may not share a combination of or all three interface modes with one physical network interface. Each interface mode consistently satisfies all of the TOE security functional requirement claims identified in this ST. These three interface modes are further described below.

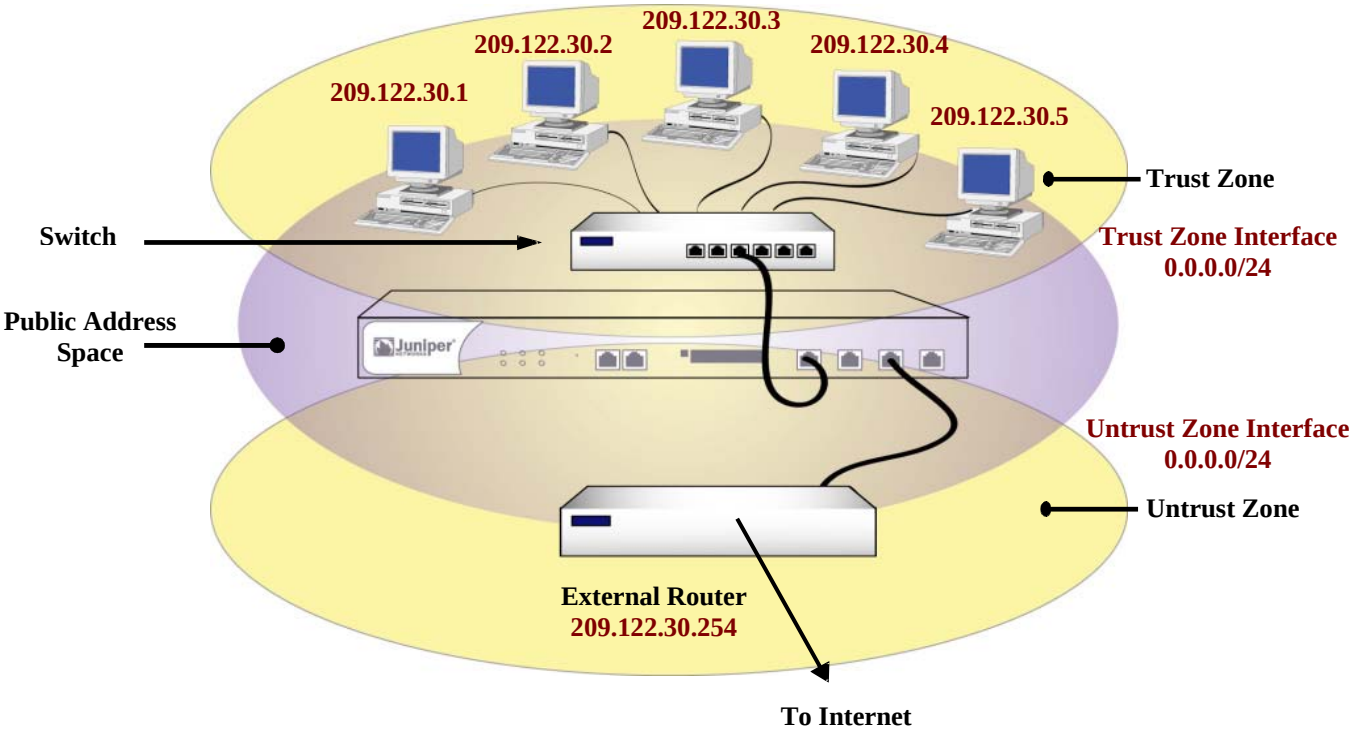
2.4.1.1 Transparent Mode

When the TOE is configured in Transparent Mode, the TOE filters packets traversing the firewall without modifying any of the source or destination information in the IP packet header. All interfaces behave as though they are part of the same network, with the TOE acting much like a Layer 2 switch or bridge. In Transparent mode, the IP addresses of interfaces are set at 0.0.0.0, making the presence of the TOE invisible, or "transparent," to users.

The FDP_IFC.1a(EXP), and FDP_IFF.1a(EXP) security functional requirements specify the requirements for protecting information flows on a security appliance when it is configured in transparent mode.

Only Authenticated Transparent mode is supported by the TOE. Non-Authenticated Transparent mode is not supported by the TOE and should not be used.

Figure 2.1: Transparent Mode



2.4.1.2 NAT Mode

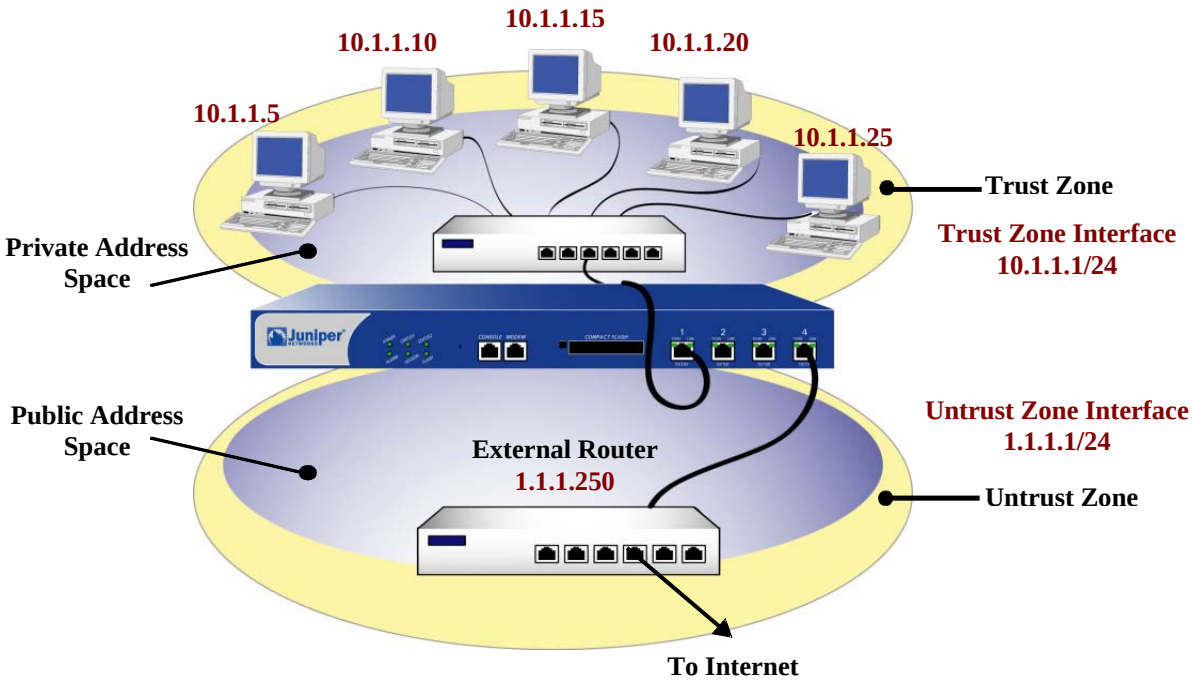
When an ingress interface is in Network Address Translation (NAT) mode, the security appliance, acting like a Layer 3 switch (or router), translates two components in the header of an outgoing IP packet destined for the Untrust zone: its source IP address and source port number. The security appliance replaces the source IP address of the originating host with the IP address of the Untrust zone interface. Also, it replaces the source port number with another random port number generated by the security appliance.

When the reply packet arrives at the security appliance, the device translates two components in the IP header of the incoming packet: the destination address and port number, which are translated back to the original numbers.

The security appliance then forwards the packet to its destination. NAT adds a level of security not provided in Transparent mode: The addresses of hosts sending traffic through an ingress interface in NAT mode (such as a Trust zone interface) are never exposed to hosts in the egress zone (such as the Untrust zone) unless the two zones are in the same virtual routing domain and the security appliance is advertising routes to peers through a dynamic routing protocol (DRP). Even then, the Trust zone addresses are only reachable if you have a policy permitting inbound traffic to them. (If you want to keep the Trust zone addresses hidden while using a DRP, then put the Untrust zone in the untrust-vr and the Trust zone in the trust-vr, and do not export routes for internal addresses in the trust-vr to the untrust-vr.) If the security appliance uses static routing and just one virtual router, the internal addresses remain hidden when traffic is outbound, due to interface-based NAT. The policies you configure control inbound traffic. If you use only mapped IP (MIP) and virtual IP (VIP) addresses as the destinations in your inbound policies, the internal addresses still remain hidden.

The FDP_IFC.1b(EXP), FDP_IFF.1b(EXP), FDP_IFC.1c(EXP), FDP_IFF.1c(EXP), and security functional requirements specify the requirements for protecting information flows on a security appliance when it is configured in NAT mode.

Figure 2.2: NAT Mode



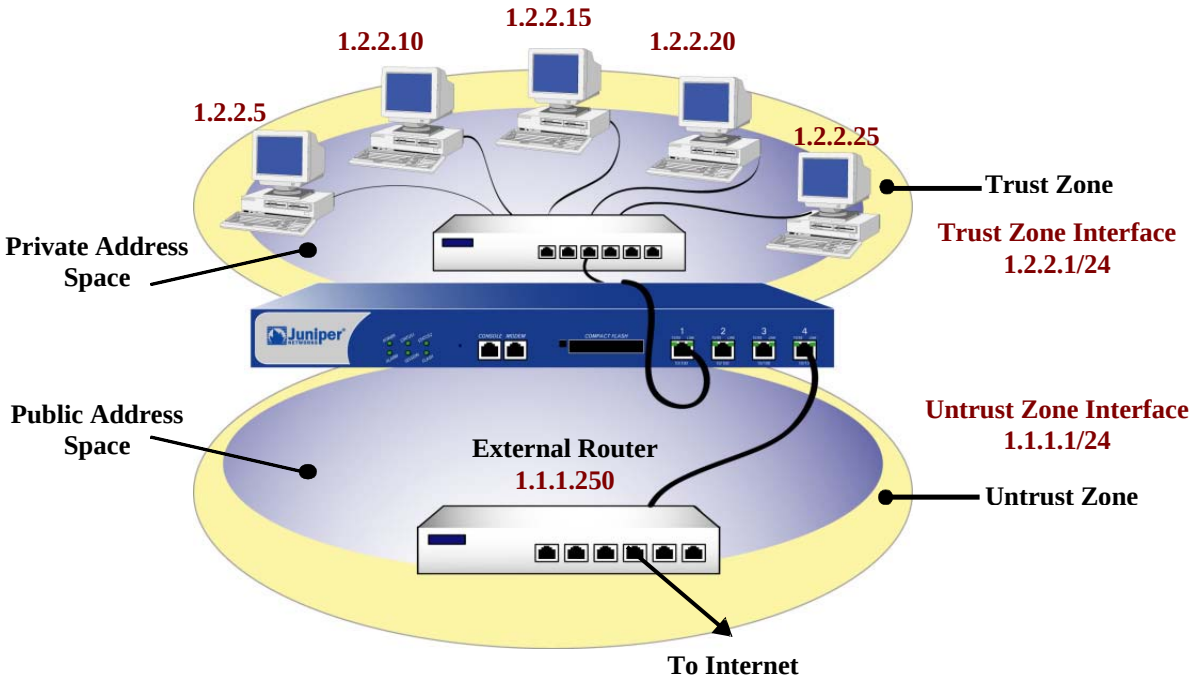
2.4.1.3 Route Mode

When an interface is in Route mode, the security appliance routes traffic between different zones without performing source NAT (NAT-src); that is, the source address and port number in the IP packet header remain unchanged as it traverses the security appliance. Unlike NAT-src, you do not need to establish mapped IP (MIP) and virtual IP (VIP) addresses to allow inbound traffic to reach hosts when the destination zone interface is in Route mode. Unlike Transparent mode, the interfaces in each zone are on different subnets.

In NAT Mode, Network Address Translation is applied to all traffic arriving at the untrust interface. By default, no address translation is provided in Route mode. However, selective network address translation is possible in Route mode using policy definitions. You can determine which traffic to route and on which traffic to perform NAT-src by creating policies that enable NAT-src for specified source addresses on either incoming or outgoing traffic. For network traffic, NAT can use the IP address or addresses of the destination zone interface from a Dynamic IP (DIP) pool, which is in the same subnet as the destination zone interface. For VPN traffic, NAT can use a tunnel interface IP address or an address from its associated DIP pool.

The FDP_IFC.1b(EXP), FDP_IFF.1b(EXP), FDP_IFC.1c(EXP) and FDP_IFF.1c(EXP) security functional requirements specify the requirements for protecting information flows on a security appliance when it is configured in route mode.

Figure 2.3: Route Mode



2.4.2 VPN

Site-To-Site VPNs allow an organization to securely connect to a remotely connected network. The TOE supports and defines security claims (FDP_IFC.1a(EXP) and FDP_IFF.1a(EXP) for Transparent Mode) and (FDP_IFC.1c(EXP) and FDP_IFF.1c(EXP) for Route Mode and NAT Mode) for utilizing Site-To-Site VPN connections using pre-shared key (PSK) authentication. In order to meet these security functional requirement claims, the TOE must have the appropriate VPN tunnels and permit filters allowing such connectivity and have the appropriate pre-shared key authentication credentials configured. The product supports various methods for VPN connectivity (i.e. Dialup VPN, L2TP VPN, Site-To-Site VPN), authentication (i.e. Manual Key, AutoKey), IPSEC Modes (i.e. Transport, Tunnel), and cryptographic algorithms (i.e. MD5, SHA-1, HMAC, DES, 3DES, AES). However, the evaluated configuration of the TOE requires that VPN connections are only configured as Site-To-Site VPNs using Manual Key authentication, also known as Pre-Shared Key authentication, using the IPSEC Tunnel Mode, and either of the following algorithms; MD5, SHA-1, HMAC, DES, 3DES, AES.

While the TOE defines security claims for Site-To-Site VPN connections, an organization is not bound to having VPN configured to meet the evaluated configuration of the TOE. If an organization does not wish to implement the Site-To-Site VPN functionality, then they may exclude it from their configuration of the TOE by ensuring that no VPN tunnels, permit filters, and pre-shared key credentials are established for such connectivity. However in doing so, the organization will not be able to implement the security functionality of the TOE that satisfies the three (3) different Security Function Policies (SFP) which include the AUTHENTICATED TRANSPARENT MODE SFP, UNAUTHENTICATED ROUTE MODE SFP, and AUTHENTICATED ROUTE MODE SFP.
The AUTHENTICATED TRANSPARENT MODE SFP applies to traffic to or from a network interface configured in Transparent Mode that is using a VPN tunnel.
The UNAUTHENTICATED ROUTE MODE SFP applies to traffic to or from a network interface configured in Route Mode or NAT Mode that is not using a VPN tunnel.
The AUTHENTICATED ROUTE MODE SFP applies to traffic to or from a network interface configured in Route Mode or NAT Mode that is using a VPN tunnel

2.4.2.1 Policy-Based VPN

Policy-Based VPNs define VPN tunnels through a “tunnel” policy action. A “tunnel” policy action always permits traffic to flow for traffic matching the related routes and services of the VPN tunnel policy.

2.4.2.2 Route-Based VPN

Route-Based VPNs define VPN tunnels using the routing table. For each VPN tunnel, a route is identified to where the VPN tunnel is invoked. Policies can be used in conjunction with the Route-Based VPN to explicitly permit or deny VPN tunnel access based on specified attributes, whereas the Policy-Based VPN only allows the capability to permit specific traffic to a VPN tunnel. Route-Based VPN’s are not supported in Transparent mode and only Policy-Based VPN’s can be used.

2.5 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.5.1 Physical Boundaries

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

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

Security appliances come in eight models: 5XT, 25, 50, 204, 208, 500, and 5200. Each model differs in the performance capability, however all provide the same security functionality. Each appliance enforces a security policy for all connection request and traffic flow between any two network zones. There are no direct connections between nodes in two separate zones except through the security appliance.

All hardware on which each security appliance operates is part of the TOE. Each security appliance has a custom operating system that is part of the TOE. The operating system, ScreenOS runs completely in firmware. There is one assumption pertaining to the correct operation of the TOE and that is for the administrative console, which must be a VT-100 terminal or any device that can emulate a VT-100 terminal. The console is part of the TOE environment and it expected to correctly display what is sent to it from ScreenOS.

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

The physical boundaries of the security 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 security appliance, and from the security appliance to the receiving node in another network zone if the security policy allows the information flow.

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

2.5.2 Logical Boundaries

The logical boundaries of the security appliances include the interfaces to communicate between the network nodes in one zone with network nodes in other zones. Security policies are applied to interzone and intrazone information flows.

2.5.2.1 Zone

A zone is a logical abstraction on which a security 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).

2.5.2.1.1 Security Zone

A security zone is a segment of network space to which security measures are applied. Multiple security zones can be configured on a single security appliance by 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 also be established to bring finer granularity to a network security design, without deploying multiple security appliances to do so.

Each security appliance is also configured with a Global Zone. A Global Zone is a security zone without a security zone interface. The Global zone serves as a storage area for mapped IP (MIP) and virtual IP (VIP) addresses. The predefined Global zone address “Any” applies to all MIPs, VIPs, and other user-defined addresses set in the Global zone. Because traffic going to these addresses is mapped to other addresses, the Global zone does not require an interface for traffic to flow through it.

2.5.2.1.1.1 Security Zone Interface

A security zone interface is an interface in which information can be sent to and from a security zone. Security zones support five types of security zone interfaces, which include physical interfaces, subinterfaces, aggregate interfaces, redundant interfaces, and virtual security interfaces. However, the evaluated configuration of the TOE may only utilize the physical interfaces, aggregate interfaces, and redundant interfaces.

2.5.2.1.1.1.1. Physical Interface

Each physical network port on the security appliance represents a physical interface, and the name of the interface is predefined. The name of a physical interface is composed of the media type, slot number (for some security appliances), and port number, for example, ethernet3/2 or ethernet2. A physical interface can bind to any security zone where it acts as a doorway through which traffic enters and exits the zone. Without a physical interface, no traffic can access the zone or leave it.

2.5.2.1.1.1.2. Aggregate Interface

The Juniper Networks NetScreen-5000 series supports aggregate interfaces. An aggregate interface is the accumulation of two or more physical interfaces, each of which shares the traffic load directed to the IP address of the aggregate interface equally among them. By using an aggregate interface, the amount of bandwidth available to a single IP address can be increased. Also, if one member of an aggregate interface fails, the other member or members can continue processing traffic, although with less bandwidth than previously available.

2.5.2.1.1.1.3. Redundant Interface

A redundant interface consists of binding two physical interfaces together to create one redundant interface, which you can then bind to a security zone. One of the two physical interfaces acts as the primary interface and handles all the traffic directed to the redundant interface. The other physical interface acts as the secondary interface and stands by in case the active interface experiences a failure. If that occurs, traffic to the redundant interface fails over to the secondary interface, which becomes the new primary interface. The

use of redundant interfaces provides a first line of redundancy before escalating a failover to the device level.

2.5.2.1.2 Tunnel Zone

A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is conceptually affiliated with a security zone in a “child-parent” relationship. The security zone acting as the “parent”, provides the firewall protection to the encapsulated traffic. The tunnel zone provides packet encapsulation/decapsulation, and by supporting tunnel interfaces with IP addresses and netmasks that can host mapped IP (MIP) addresses and dynamic IP (DIP) pools, can also provide policy-based NAT services. The security appliance uses the routing information for the carrier zone to direct traffic to the tunnel endpoint. The default tunnel zone is Untrust-Tun, and it is associated with the Untrust zone. Other tunnel zones can be created and bound to other security zones, with a maximum of one tunnel zone per carrier zone per virtual system. Virtual systems, however, are outside the scope of the evaluated configuration.

2.5.2.1.2.1 Tunnel Interfaces

A tunnel interface acts as a doorway to a VPN tunnel. Traffic enters and exits a VPN tunnel via a tunnel interface.
When you bind a tunnel interface to a VPN tunnel, you can reference that tunnel interface in a route to a specific destination and then reference that destination in one or more policies. With this approach, you can finely control the flow of traffic through the tunnel. It also provides dynamic routing support for VPN traffic. When there is no tunnel interface bound to a VPN tunnel, you must specify the tunnel in the policy itself and choose **tunnel** as the action.

Outbound traffic enters the tunnel zone via the tunnel interface, is encapsulated, and exits via the security zone interface. Inbound traffic enters via the security zone interface, is decapsulated in the tunnel zone, and exits via the tunnel interface.

2.5.2.1.3 Function Zone

The function zone is a zone that performs a specific function. Functional zones support five types of zones, which include null zones, MGT zones, HA zones, self zones, and VLAN zones. However, the evaluated configuration of the TOE may only utilize the null zones and self zones. Each zone exists for a single purpose, as explained below.

2.5.2.1.3.1 Null Zone

This zone serves as temporary storage for any interfaces that are not bound to any other zone.

2.5.2.1.3.2 Self Zone

This zone hosts the interface for remote management connections. When you connect to the security appliance via HTTP, SCS, or Telnet, you connect to the Self zone. Remote management is not supported in the evaluated configuration of the TOE and therefore, also excludes Self Zones.

2.5.2.2 Loopback Interfaces

A loopback interface is a virtual interface that can be used either as a redundancy feature for binding a logical interface to more than one physical network interface, or as a management feature for providing an interface that can be dedicated to provide specific hosts the capability to manage the TOE. Since the evaluated configuration of the TOE restricts the use of remote management, loopback interfaces cannot be used to provide remote management of the TOE. However, loopback interfaces can be used to provide redundancy between to physical network interfaces which can assist in the enforcement of the information flow policies defined.

2.5.2.3 Audit

Security appliances categorize auditing information into three categories, events, traffic logs, and self logs. Events are system-level notifications and alarms which are generated by the system to indicate events such as configuration changes, network attacks detected, or administrators logging in our out of the device. Traffic logs are directly driven by policies that allow traffic to go through the device. When logging and

counting are enabled for a policy, all traffic will be logged to the traffic log. Self logs store information on traffic that is dropped and traffic that is sent to the device. For example, if you disable some management options on an interface—such as WebUI, SNMP, and ping—and HTTP, SNMP, or ICMP traffic is sent to that interface, entries appear in the self log for each dropped packet.

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

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

2.5.2.4 Information Flow Protection

By default, a security appliance denies all traffic in all directions. [1] Through the creation of information flow policies, traffic flow across an interface can be controlled by defining the kinds of traffic permitted to pass from one security zone to another. In addition, the NAT and Route mode configurations also control traffic across an interface by defining the kinds of traffic permitted to pass between hosts within the same security zone.

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 or within the same zone. Once a connection is established, 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),
- Service[2] (port or groups of ports, such as port 80 for HTTP, or service name such as FTP, or service data type such as ftp-get), and
- Network Interface (i.e. from zone and to zone, direction).

Additionally, if a security appliance attempts to connect to another security appliance using Site-to-Site VPN, the security appliance establishing the connection must supply a manual key consistent with the manual key configured on the destination security appliance before access is granted to establish the VPN tunnel. Once a VPN tunnel is successfully established, the information flow policy is enforced.

While the information flow policies stated in FDP_IFC.1a, FDP_IFC.1b, and FDP_IFC.1c are indicated to be optional, at least one of the three information flow policies identified must be enforced to remain within the evaluated configuration and compliant to the TFFPP requirements.

2.5.2.5 Identification & Authentication

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

- Root administrator
- Read/Write Administrator

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

[2] A service also specifies the protocol (TCP or UDP) used for the specific type of service defined.

EAL4

- Read-only Administrator
- VSYS Administrator
- VSYS Read-only Administrator[3]

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

2.5.2.6 Security Management

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

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

2.5.2.7 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 security appliances will remain attached to the physical connections made by an administrator so that an appliance cannot be bypassed. Each security appliance is completely self-contained in that the hardware and firmware developed by Juniper provide all the services necessary to implement the TOE. There are no external interfaces into the TOE other than the well-defined physical ports. There is no general purpose computing capabilities that might offer an opportunity for a user to bypass or otherwise corrupt the TOE.

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

Logically, each security 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 security 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.

Additionally, the TOE protects its session table by enforcing destination-based session limits and watermarks for limiting the time a session may live when the session table reaches the specified watermark. The TOE also provides a trusted recovery function for cases when the configuration is modified or the system is ungracefully shutdown.

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

3.0 Security Environment

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

Security appliances provide for a level of protection that is appropriate for IT environments that require strict control over the information flow across a network. Security 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. Security appliances are suitable for use in both Department of Defense and commercial environments.

3.1 Threats to Security

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person 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. 4
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.
T. PROTECTION	The data transmitted from the TOE to a peer TOE via encryption may be accessed by an unauthorized person.

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

3.2 Secure Usage Assumptions

3.2.1 Personnel Assumptions

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

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

3.2.2 Physical Assumptions

A.CONSOLE A VT-100 terminal or any device that can emulate a VT-100 terminal is required for use as a locally connected console. The VT-100 terminal/emulator is part of the IT environment and it expected to correctly display what is sent to it from the TOE.

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

A.PHYSEC The TOE is physically secure.

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

3.2.3 Logical Assumptions

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

A.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. [5]

[5] 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.

4.0 Security Objectives

This section defines the security objectives of security 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. [6]
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.PROTECTION	The TOE shall be able to protect the confidentiality of data transmitted to a peer TOE via encryption. Upon receipt of data from a peer TOE, the TOE must be able to decrypt the data.

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

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.

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

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

5.0 IT Security Requirements

5.1 TOE Security Functional Requirements

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

Table 5.1: Security Functional Components

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)
Cryptography (FCS)	Cryptographic operation (FCS_COP.1a) Cryptographic operation (FCS_COP.1b) Cryptographic operation (FCS_COP.1c)
User Data Protection (FDP)	Subset information flow control (FDP_IFC.1a(EXP)) Simple security attributes (FDP_IFF.1a(EXP)) *Note these iterations of information flow control specify a policy similar to the UNAUTHENTICATED SFP in the PPs yet tailored to differentiate the filtering capabilities for authenticated information flows (i.e. VPN) using a network interface configured in Transparent Mode.*
	Subset information flow control (FDP_IFC.1b(EXP)) Simple security attributes (FDP_IFF.1b(EXP)) *Note these iterations satisfy the information flow control policy identified within the PPs for the UNAUTHENTICATED SFP, yet they are also tailored to differentiate the filtering capabilities for a network interface configured in Route Mode or NAT Mode.*
	Subset information flow control (FDP_IFC.1c(EXP)) Simple security attributes (FDP_IFF.1c(EXP)) *Note these iterations of information flow control specify a policy similar to the UNAUTHENTICATED SFP in the PPs yet tailored to differentiate the filtering capabilities for authenticated information flows (i.e. VPN) using a network interface configured in Route Mode or NAT Mode.*
	Subset residual information protection (FDP_RIP.1)

EAL4

Security Functional Class	Security Functional Components
Identification and Authentication (FIA)	~~Authentication failure handling (FIA_AFL.1)~~ *Note this requirement does not apply since the TOE does not support an interface where a non-administrator can attempt to authenticate itself to the TOE (e.g., for remote administration). As a result, it has been omitted from this section (including removal of family FIA_AFL as well as removal of FAU_GEN.1 and FMT_MOF.1 references to this component).*
	User attribute definition (FIA_ATD.1)
	Verification of secrets (FIA_SOS.1) *Note this requirement has been added to require passwords generated by administrator to be at least 8 characters in length.*
	~~Single-use authentication mechanisms (FIA_UAU.4)~~ *Note this requirement does not apply since the TOE does not support remote administration from either an internal or external network. As a result, it has been omitted from this section (including removal of component FIA_UAU.4 as well as removal of FMT_MOF.1 references to this component).*
	Timing of authentication (FIA_UAU.1)
	User identification before any action (FIA_UID.2)
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) *Note this requirement has been added to conform to International Interpretation I-065.*
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Manual recovery (FPT_RCV.1(EXP)) *Note this requirement has been added to include the capability for the TOE to recover to a known state.*
	Non-bypassability of the TSP (FPT_RVM.1)
	TSF domain separation (FPT_SEP.1)
	Reliable time stamps (FPT_STM.1)
	Inter-TSF confidentiality during transmission (FPT_ITC.1a) *Note these iterations of information flow control specify a policy similar to the UNAUTHENTICATED SFP in the PPs yet tailored to differentiate the filtering capabilities for authenticated information flows (i.e. VPN) using a network interface configured in Transparent Mode.*
	Inter-TSF confidentiality during transmission (FPT_ITC.1b) *Note these iterations of information flow control specify a policy similar to the UNAUTHENTICATED SFP in the PPs yet tailored to differentiate the filtering capabilities for authenticated information flows (i.e. VPN) using a network interface configured in Route Mode or NAT Mode*

EAL4

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[8]

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 [***not specified***] level of audit; and
c) [**the events in Table 5.2**].

Table 5.2: Audit Events & Audit Event Details

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the authorized administrator** role	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	All decisions on requests for information flow.	The presumed address of the source and destination subject **and the action taken (i.e. permit, deny, tunnel)**.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation

5.1.1.1.2 FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity, outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in column three of Table 5.2**].

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

[8] This change has been made to conform to International Interpretation #202

EAL4

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 Cryptography (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1a)

5.1.2.1.1 FCS_COP.1a.1

The TSF shall perform [**encryption and decryption of site-to-site VPN sessions**] in accordance with a specified cryptographic algorithms: [**Data Encryption Standard (DES) or Triple DES (3DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 81 [4], or Advanced Encryption Standard (AES) as specified in FIPS 197**] and cryptographic key sizes [**that are 64 binary digits in length for DES, 196 binary digits in length for 3DES, or 128, 192, or 256 binary digits in length for AES**] that meet the following: [**FIPS PUB 46-3 and FIPS PUB 81 [4] for DES or 3DES, or FIPS 197 for AES**].

5.1.2.2 Cryptographic operation (FCS_COP.1b)

5.1.2.2.1 FCS_COP.1b.1

The TSF shall perform [**IPSEC Authentication of site-to-site VPN sessions**] in accordance with a specified cryptographic algorithm [**HMAC-MD5-96**] and cryptographic key sizes **[16 byte in length]** that meet the following: [**RFC 2403**].

5.1.2.3 Cryptographic operation (FCS_COP.1c)

5.1.2.3.1 FCS_COP.1c.1

The TSF shall perform [**IPSEC Authentication of site-to-site VPN sessions**] in accordance with a specified cryptographic algorithm [**HMAC-SHA-1-96**] and cryptographic key sizes **[20 bytes in length**] that meet the following: [**RFC 2404**].

EAL4

5.1.3 User Data Protection (FDP)[9]

5.1.3.1 Subset information flow control (FDP_IFC.1a(EXP))

5.1.3.1.1 FDP_IFC.1a(EXP).1

The TSF shall **be able to** enforce the [**AUTHENTICATED TRANSPARENT MODE SFP**] on:

a) [**subjects: external IT entities that have authenticated to the TOE's Route-Based or Policy-Based Site-To-Site IPSEC VPN using a pre-shared secret key to 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 using VPN in tunnel mode**].

5.1.3.2 Subset information flow control (FDP_IFC.1b(EXP))

5.1.3.2.1 FDP_IFC.1b(EXP).1

The TSF shall **be able to** enforce the [**UNAUTHENTICATED ROUTE MODE 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].

5.1.3.3 Subset information flow control (FDP_IFC.1c(EXP))

5.1.3.3.1 FDP_IFC.1c(EXP).1

The TSF shall **be able to** enforce the [**AUTHENTICATED ROUTE MODE SFP**] on:

a) [**subjects: external IT entities that have authenticated to the TOE's Route-Based or Policy-Based Site-To-Site IPSEC VPN using a pre-shared secret key to 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 using VPN in tunnel mode].

5.1.3.4 Simple security attributes (FDP_IFF.1a(EXP))

5.1.3.4.1 FDP_IFF.1a(EXP).1

The TSF shall **be able to** enforce the [**AUTHENTICATED TRANSPARENT MODE SFP**] based on at least the following types of subject and information security attributes:

a) [**subject security attributes:**
- **presumed address;**
- **pre-shared secret key;**
- [**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**]].

5.1.3.4.2 FDP_IFF.1a(EXP).2

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

a) [**Subjects initiating the VPN tunnel on an internal network can cause information to flow through the TOE to another connected network if:**

[9] Although the FDP_IFC.1* and FDP_IFF.1* requirements are optional, at least one of the three FDP_IFC.1* and FDP_IFF.1* requirements must be enforced to comply with the evaluated configuration of the TOE.

- **the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;**
- **all the information security attribute values are unambiguously permitted by the VPN 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 initiating the VPN tunnel on the external network can cause information to flow through the TOE to another connected network if:**

- **the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;**
- **all the information security attribute values are unambiguously permitted by the VPN 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.**]

5.1.3.4.3 FDP_IFF.1a(EXP).3

The TSF shall **be able to** enforce the [**following additional information flow control SFP rules:**

1) The TSF shall check to see if the source and destination zones are the same or different.

- **If the source and destination zones are different, the TSF shall perform a policy lookup in the interzone policy set list,**

2) If the TSF performs the interzone policy lookup and does not find a match, the TSF shall apply the default deny policy to the packet,

5.1.3.4.4 FDP_IFF.1a(EXP).4

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

5.1.3.4.5 FDP_IFF.1a(EXP).5

The TSF shall **be able to** explicitly authorize an information flow based on the following rules: [**no explicit authorization rules**].10

5.1.3.4.6 FDP_IFF.1a(EXP).6

The TSF shall **be able to** 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.**]

5.1.3.5 Simple security attributes (FDP_IFF.1b(EXP))

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

EAL4

5.1.3.5.1 FDP_IFF.1b(EXP).1

The TSF shall **be able to** enforce the [**UNAUTHENTICATED ROUTE MODE 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**]].

5.1.3.5.2 FDP_IFF.1b(EXP).2

The TSF shall **be able to** 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.**]

5.1.3.5.3 FDP_IFF.1b(EXP).3

The TSF shall **be able to** enforce the [**following additional information flow control SFP rules:**

1) The TSF shall check to see if the source and destination zones are the same or different.
- **If the source and destination zones are different, the TSF shall perform a policy lookup in the interzone policy set list,**
  or
- **If the source and destination zones are the same, the TSF shall perform a policy lookup in the intrazone policy set list.**

5.1.3.5.4 FDP_IFF.1b(EXP).4

The TSF shall **be able to** provide the following [**additional SFP capabilities:**

a) The TSF shall provide the capability to perform policy-based address translation on the presumed address of the source subject, in the information, if a policy with one of the following policy-based translation options is invoked by the information:
- **NAT-Src from a DIP Pool with PAT**
- **NAT-Src from a DIP Pool without PAT**
- **NAT-Src from a DIP Pool with Address Shifting**
- **NAT-Src from the Egress Interface IP Address**

EAL4

b) The TSF shall provide the capability to perform policy-based address translation on the presumed address of the destination subject, in the information, if a policy with one of the following policy-based translation options is invoked by the information:
- **NAT-Dst to a Single IP Address with Port Mapping**
- **NAT-Dst to a Single IP Address without Port Mapping**
- **NAT-Dst from an IP Address Range to a Single IP Address**
- **NAT-Dst between IP Address Ranges**

c) The TSF shall provide the capability to block or reassemble fragmented packets on a per zone basis].

5.1.3.5.5 FDP_IFF.1b(EXP).5

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

5.1.3.5.6 FDP_IFF.1b(EXP).6

The TSF shall **be able to** 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.**]

5.1.3.6 Simple security attributes (FDP_IFF.1c(EXP))

5.1.3.6.1 FDP_IFF.1c(EXP).1

The TSF shall **be able to** enforce the [**AUTHENTICATED ROUTE MODE SFP**] based on at least the following types of subject and information security attributes:

a) [**subject security attributes:**
- **presumed address;**
- **pre-shared secret key;**
- [**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**]].

5.1.3.6.2 FDP_IFF.1c(EXP).2

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

a) [**Subjects initiating the VPN tunnel on an internal network can cause information to flow through the TOE to another connected network if:**
- **the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;**
- **all the information security attribute values are unambiguously permitted by the VPN policy rules, where such rules may be composed from all possible combinations of the**

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

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 initiating the VPN tunnel on the external network can cause information to flow through the TOE to another connected network if:**

- **the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;**
- **all the information security attribute values are unambiguously permitted by the VPN 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.**]

5.1.3.6.3 FDP_IFF.1c(EXP).3

The TSF shall **be able to** enforce the [**following additional information flow control SFP rules:**

1) The TSF shall check to see if the source and destination zones are the same or different.

- **If the source and destination zones are different, the TSF shall perform a policy lookup in the interzone policy set list,**
  or
- **If the source and destination zones are the same, the TSF shall perform a policy lookup in the intrazone policy set list.**

2) If the TSF performs the interzone or intrazone policy lookup and does not find a match, the TSF shall check the global policy set list for a match.

- **If the TSF performs the interzone and global policy lookups and does not find a match, the TSF shall apply the default deny policy to the packet,**
  or
- **If the TSF performs the intrazone and global policy lookups and does not find a match, the TSF shall apply the intrazone blocking setting for that zone to the packet**].

5.1.3.6.4 FDP_IFF.1c(EXP).4

The TSF shall **be able to** provide the following [**additional SFP capabilities:**

a) The TSF shall provide the capability to perform policy-based address translation on the presumed address of the source subject, in the information, if a policy with one of the following policy-based translation options is invoked by the information:

- **NAT-Src from a DIP Pool with PAT**
- **NAT-Src from a DIP Pool without PAT**
- **NAT-Src from a DIP Pool with Address Shifting**
- **NAT-Src from the Egress Interface IP Address**

b) The TSF shall provide the capability to perform policy-based address translation on the presumed address of the destination subject, in the information, if a policy with one of the following policy-based translation options is invoked by the information:

- **NAT-Dst to a Single IP Address with Port Mapping**
- **NAT-Dst to a Single IP Address without Port Mapping**
- **NAT-Dst from an IP Address Range to a Single IP Address**
- **NAT-Dst between IP Address Ranges**

c) The TSF shall provide the capability to block or reassemble fragmented packets on a per zone basis].

5.1.3.6.5 FDP_IFF.1c(EXP).5

EAL4

The TSF shall **be able to** explicitly authorize an information flow based on the following rules: [**no explicit authorization rules**].12

5.1.3.6.6 FDP_IFF.1c(EXP).6

The TSF shall **be able to** 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.]

5.1.3.7 Subset residual information protection (FDP_RIP.1)

5.1.3.7.1 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].

5.1.4 Identification and Authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1)

5.1.4.1.1 FIA_ATD.1.1

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

a) [identity;
b) association of a human user with the authorized administrator role;
c) [**and authentication data**]].

5.1.4.2 Verification of secrets (FIA_SOS.1)

5.1.4.2.1 FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [**a minimum length of 8 characters**].

5.1.4.3 Timing of authentication (FIA_UAU.1)

5.1.4.3.1 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.

5.1.4.3.2 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.

5.1.4.4 User identification before any action (FIA_UID.2)

5.1.4.4.1 FIA_UID.2.1

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

EAL4

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

5.1.5 Security management (FMT)

5.1.5.1 Management of security functions behavior (FMT_MOF.1) 13

5.1.5.1.1 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) other security-relevant administrative functions {**create, delete, and modify VPN tunnels**

n) **Enable/Disable SCREEN firewall protections**;

o) **Manage TOE interfaces**;

p) **Recovery of the TOE to a secure state**;

to [an authorized administrator].

5.1.5.2 Static attribute initialization (FMT_MSA.3)

5.1.5.2.1 FMT_MSA.3.1

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

5.1.5.2.2 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.

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

EAL4

5.1.5.3 Specification of Management Functions (FMT_SMF.1)

5.1.5.3.1 FMT_SMF.1.1[14]

The TSF shall be capable of performing the following security management functions: [

a) Startup and shutdown;

b) Create, delete, modify, and view information flows rules that permit or deny information flows;

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

d) Create, delete, modify and view VPN tunnels;

e) Enable/Disable SCREEN firewall protections;

f) Manage TOE interfaces;

g) Modify and set the time and date;

h) Archive, create, delete, empty, and review the audit trail;

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

j) Recovery of the TOE to a secure state;

5.1.5.4 Security roles (FMT_SMR.1)

5.1.5.4.1 FMT_SMR.1.1

The TSF shall maintain the role [authorized administrator].

5.1.5.4.2 FMT_SMR.1.2

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

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Manual recovery (FPT_RCV.1(EXP))

5.1.6.1.1 FPT_RCV.1(EXP).1

After a modified configuration results in a failure or insecure state of the TOE, the TSF shall provide the capability for an administrator to enter a maintenance mode where the ability to return to a secure state is provided.

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

5.1.6.2.1 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.

5.1.6.3 TSF domain separation (FPT_SEP.1)

5.1.6.3.1 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.

5.1.6.3.2 FPT_SEP.1.2

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

5.1.6.4 Reliable time stamps (FPT_STM.1)

[14] This requirement was added to conform to International Interpretation I-065

EAL4

5.1.6.4.1 FPT_STM.1.1

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

5.1.6.5 Inter-TSF trusted Channel during transmission (FPT_ITC.1a)

5.1.6.5.1 FPT_ITC.1a.1

The TSF shall be able to enforce the **[AUTHENTICATED TRANSPARENT MODE SFP]** to protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Application Note: The encryption used to protect the communication channel from disclosure is the symmetric algorithm specified in FCS_COP.1a.

5.1.6.6 Inter-TSF trusted Channel during transmission (FPT_ITC.1b)

5.1.6.6.1 FPT_ITC.1b.1

The TSF shall be able to enforce the **[AUTHENTICATED ROUTE MODE SFP]** to protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Application Note: The encryption used to protect the communication channel from disclosure is the symmetric algorithm specified in FCS_COP.1a.

EAL4

Security Functional Requirements for the IT Environment

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

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria. Note that the EAL 4 requirements that exceed EAL 2, by the TFFPP are indicated in bold in the following table. No operations are applied to the assurance components. The SARs have been changed, when necessary, to conform to National and International Interpretations.

Table 5.3 EAL4 Assurance Components

Assurance Class	**Assurance Components**
Configuration Management (ACM)	**ACM_AUT.1 Partial CM automation**
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and Operation (ADO)	**ADO_DEL.2 Detection of modification**
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	**ADV_FSP.2 Fully defined external interfaces**
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	**ALC_DVS.1 Identification of security measures**
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests (ATE)	**ATE_COV.2 Analysis of Coverage**
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	**AVA_MSU.2 Validation of analysis**
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent Vulnerability Analysis

EAL4

5.2.1 Configuration Management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

5.2.1.1.1 ACM_AUT.1.1D

The developer shall use a CM system.

5.2.1.1.2 ACM_AUT.1.2D

The developer shall provide a CM plan.

5.2.1.1.3 ACM_AUT.1.1C

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

5.2.1.1.4 ACM_AUT.1.2C

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

5.2.1.1.5 ACM_AUT.1.3C

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

5.2.1.1.6 ACM_AUT.1.4C

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

5.2.1.1.7 ACM_AUT.1.1E

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

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

5.2.1.2.1 ACM_CAP.4.1D

The developer shall provide a reference for the TOE.

5.2.1.2.2 ACM_CAP.4.2D

The developer shall use a CM system.

5.2.1.2.3 ACM_CAP.4.3D

The developer shall provide CM documentation.

5.2.1.2.4 ACM_CAP.4.1C

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

5.2.1.2.5 ACM_CAP.4.2C

The TOE shall be labeled with its reference.

5.2.1.2.6 ACM_CAP.4.3C

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

5.2.1.2.7 International Interpretation RI #3

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

5.2.1.2.8 ACM_CAP.4.4C

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

5.2.1.2.9 ACM_CAP.4.5C

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

5.2.1.2.10 ACM_CAP.4.6C

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

EAL4

The CM system shall uniquely identify all configuration items.

5.2.1.2.11 ACM_CAP.4.7C

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

5.2.1.2.12 ACM_CAP.4.8C

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

5.2.1.2.13 ACM_CAP.4.9C

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

5.2.1.2.14 ACM_CAP.4.10C

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

5.2.1.2.15 ACM_CAP.4.11C

The CM system shall support the generation of the TOE.

5.2.1.2.16 ACM_CAP.4.12C

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

5.2.1.2.17 ACM_CAP.4.1E

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

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

5.2.1.3.1 ACM_SCP.2.1D

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

5.2.1.3.2 ACM_SCP.2.1C

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

5.2.1.3.3 ACM_SCP.2.2C

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

5.2.1.3.4 ACM_SCP.2.1E

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

5.2.2 Delivery and Operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

5.2.2.1.1 ADO_DEL.2.1D

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

5.2.2.1.2 ADO_DEL.2.2D

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

EAL4

The developer shall use the delivery procedures.

5.2.2.1.3 ADO_DEL.2.1C

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

5.2.2.1.4 ADO_DEL.2.2C

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

5.2.2.1.5 ADO_DEL.2.3C

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

5.2.2.1.6 ADO_DEL.2.1E

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

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

5.2.2.2.1 ADO_IGS.1.1D

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

5.2.2.2.2 ADO_IGS.1.1C

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

5.2.2.2.3 ADO_IGS.1.1E

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

5.2.2.2.4 ADO_IGS.1.2E

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

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

5.2.3.1.1 ADV_FSP.2.1D

The developer shall provide a functional specification.

5.2.3.1.2 ADV_FSP.2.1C

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

5.2.3.1.3 ADV_FSP.2.2C

The functional specification shall be internally consistent.

5.2.3.1.4 ADV_FSP.2.3C

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

5.2.3.1.5 ADV_FSP.2.4C

The functional specification shall completely represent the TSF.

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

EAL4

5.2.3.1.6 ADV_FSP.2.5C

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

5.2.3.1.7 ADV_FSP.2.1E

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

5.2.3.1.8 ADV_FSP.2.2E

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

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

5.2.3.2.1 ADV_HLD.2.1D

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

5.2.3.2.2 ADV_HLD.2.1C

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

5.2.3.2.3 ADV_HLD.2.2C

The high-level design shall be internally consistent.

5.2.3.2.4 ADV_HLD.2.3C

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

5.2.3.2.5 ADV_HLD.2.4C

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

5.2.3.2.6 ADV_HLD.2.5C

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

5.2.3.2.7 ADV_HLD.2.6C

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

5.2.3.2.8 ADV_HLD.2.7C

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

5.2.3.2.9 ADV_HLD.2.8C

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

5.2.3.2.10 ADV_HLD.2.9C

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

5.2.3.2.11 ADV_HLD.2.1E

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

5.2.3.2.12 ADV_HLD.2.2E

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

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

5.2.3.3.1 ADV_IMP.1.1D

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

EAL4

5.2.3.3.2 ADV_IMP.1.1C

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

5.2.3.3.3 ADV_IMP.1.2C

The implementation representation shall be internally consistent.

5.2.3.3.4 ADV_IMP.1.1E

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

5.2.3.3.5 ADV_IMP.1.2E

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

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

5.2.3.4.1 ADV_LLD.1.1D

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

5.2.3.4.2 ADV_LLD.1.1C

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

5.2.3.4.3 ADV_LLD.1.2C

The low-level design shall be internally consistent.

5.2.3.4.4 ADV_LLD.1.3C

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

5.2.3.4.5 ADV_LLD.1.4C

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

5.2.3.4.6 ADV_LLD.1.5C

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

5.2.3.4.7 ADV_LLD.1.6C

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

5.2.3.4.8 ADV_LLD.1.7C

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

5.2.3.4.9 ADV_LLD.1.8C

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

5.2.3.4.10 ADV_LLD.1.9C

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

5.2.3.4.11 ADV_LLD.1.10C

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

5.2.3.4.12 ADV_LLD.1.1E

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

5.2.3.4.13 ADV_LLD.1.2E

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

EAL4

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

5.2.3.5.1 ADV_RCR.1.1D

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

5.2.3.5.2 ADV_RCR.1.1C

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

5.2.3.5.3 ADV_RCR.1.1E

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

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

5.2.3.6.1 ADV_SPM.1.1D

The developer shall provide a TSP model.

5.2.3.6.2 ADV_SPM.1.2D

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

5.2.3.6.3 ADV_SPM.1.1C

The TSP model shall be informal.

5.2.3.6.4 ADV_SPM.1.2C

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

5.2.3.6.5 ADV_SPM.1.3C

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

5.2.3.6.6 ADV_SPM.1.4C

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

5.2.3.6.7 ADV_SPM.1.1E

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

5.2.4 Guidance Documents (AGD)

5.2.4.1 Administrator Guidance (AGD_ADM.1)

5.2.4.1.1 AGD_ADM.1.1D

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

5.2.4.1.2 AGD_ADM.1.1C

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

5.2.4.1.3 AGD_ADM.1.2C

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

5.2.4.1.4 AGD_ADM.1.3C

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

EAL4

5.2.4.1.5 AGD_ADM.1.4C

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

5.2.4.1.6 AGD_ADM.1.5C

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

5.2.4.1.7 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.

5.2.4.1.8 AGD_ADM.1.7C

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

5.2.4.1.9 AGD_ADM.1.8C

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

5.2.4.1.10 AGD_ADM.1.1E

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

5.2.4.2 User Guidance (AGD_USR.1)

5.2.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.2.4.2.2 AGD_USR.1.1C

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

5.2.4.2.3 AGD_USR.1.2C

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

5.2.4.2.4 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.

5.2.4.2.5 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.

5.2.4.2.6 AGD_USR.1.5C

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

5.2.4.2.7 AGD_USR.1.6C

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

5.2.4.2.8 AGD_USR.1.1E

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

5.2.5 Life Cycle Support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

EAL4

5.2.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

5.2.5.1.2 ALC_DVS.1.1C

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

5.2.5.1.3 ALC_DVS.1.2C

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

5.2.5.1.4 ALC_DVS.1.1E

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

5.2.5.1.5 ALC_DVS.1.2E

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

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

5.2.5.2.1 ALC_LCD.1.1D

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

5.2.5.2.2 ALC_LCD.1.2D

The developer shall provide life-cycle definition documentation.

5.2.5.2.3 ALC_LCD.1.1C

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

5.2.5.2.4 ALC_LCD.1.2C

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

5.2.5.2.5 ALC_LCD.1.1E

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

5.2.5.3 Well-defined development tools (ALC_TAT.1)

5.2.5.3.1 ALC_TAT.1.1D

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

5.2.5.3.2 ALC_TAT.1.2D

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

5.2.5.3.3 ALC_TAT.1.1C

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

5.2.5.3.4 ALC_TAT.1.2C

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

5.2.5.3.5 ALC_TAT.1.3C

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

5.2.5.3.6 ALC_TAT.1.1E

EAL4

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

5.2.6 Security Testing (ATE)

5.2.6.1 Analysis of Coverage (ATE_COV.2)

5.2.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

5.2.6.1.2 ATE_COV.2.1C

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

5.2.6.1.3 ATE_COV.2.2C

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

5.2.6.1.4 ATE_COV.2.1E

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

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

5.2.6.2.1 ATE_DPT.1.1D

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

5.2.6.2.2 ATE_DPT.1.1C

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

5.2.6.2.3 ATE_DPT.1.2E

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

5.2.6.3 Functional testing (ATE_FUN.1)

5.2.6.3.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.2.6.3.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.2.6.3.3 ATE_FUN.1.1C

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

5.2.6.3.4 ATE_FUN.1.2C

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

5.2.6.3.5 ATE_FUN.1.3C

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

5.2.6.3.6 ATE_FUN.1.4C

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

5.2.6.3.7 ATE_FUN.1.5C

EAL4

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

5.2.6.3.8 ATE_FUN.1.1E

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

5.2.6.4 Independent testing - sample (ATE_IND.2)

5.2.6.4.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.2.6.4.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.2.6.4.3 ATE_IND.2.2C

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

5.2.6.4.4 ATE_IND.2.1E

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

5.2.6.4.5 ATE_IND.2.2E

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

5.2.6.4.6 ATE_IND.2.3E

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

5.2.7 Vulnerability Assessment (AVA)

5.2.7.1 Validation of analysis (AVA_MSU.2)

5.2.7.1.1 AVA_MSU.2.1D

The developer shall provide guidance documentation.

5.2.7.1.2 AVA_MSU.2.2D

The developer shall document an analysis of the guidance documentation.

5.2.7.1.3 AVA_MSU.2.1C

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

5.2.7.1.4 AVA_MSU.2.2C

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

5.2.7.1.5 AVA_MSU.2.3C

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

5.2.7.1.6 AVA_MSU.2.4C

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

5.2.7.1.7 AVA_MSU.2.5C

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

5.2.7.1.8 AVA_MSU.2.1E

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

EAL4

5.2.7.1.9 AVA_MSU.2.2E

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

5.2.7.1.10 AVA_MSU.2.3E

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

5.2.7.1.11 AVA_MSU.2.4E

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

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

5.2.7.2.1 AVA_SOF.1.1D

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

5.2.7.2.2 AVA_SOF.1.1C

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

5.2.7.2.3 AVA_SOF.1.2C

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

5.2.7.2.4 AVA_SOF.1.1E

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

5.2.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.2.7.3 Independent vulnerability analysis (AVA_VLA.2)

5.2.7.3.1 AVA_VLA.2.1D

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

The developer shall perform a vulnerability analysis. [20]

5.2.7.3.2 AVA_VLA.2.2D

~~The developer shall document the disposition of identified vulnerabilities.~~

The developer shall provide vulnerability analysis documentation. [21]

5.2.7.3.3 AVA_VLA.2.1C

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

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP. [22]

5.2.7.3.4 AVA_VLA.2.2C

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

EAL4

~~The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.~~

The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities. [23]

5.2.7.3.5 AVA_VLA.2.3C

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

5.2.7.3.6 AVA_VLA.2.4C

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

5.2.7.3.7 AVA_VLA.2.1E

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

5.2.7.3.8 AVA_VLA.2.2E

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

5.2.7.3.9 AVA_VLA.2.3E

The evaluator shall perform an independent vulnerability analysis.

5.2.7.3.10 AVA_VLA.2.4E

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

5.2.7.3.11 AVA_VLA.2.5E

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

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

6.0 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

Audit data generation (FAU_GEN.1)

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

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

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

Security appliances also can simultaneously send audit records to SDRAM and a remote syslog as a backup device to the audit log and an administrator controls this backup. The platform and storage device that control the syslog are not part of the TOE.

The information contained in the logs include:

a) The date and time of event,

b) The type of event,

c) The subject identity,

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

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

The logs contain the following auditable events:

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

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

c) Administrator commands,

d) User I&A success and failures, and

e) Attempted Traffic (connection and packet filter) Information Flow Policy violations as well as successes and the policy decision taken for each information flow (i.e. permit, deny, tunnel).

EAL4

Audit review (FAU_SAR.1)

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

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

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

Selectable audit review (FAU_SAR.3)

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

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

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

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

Protected audit trail storage (FAU_STG.1)

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

Prevention of audit data loss (FAU_STG.4)

Security appliances provide memory to hold a fixed maximum number of audit records and then once the storage limit is reached, the audit mechanism ‘wraps’ or acts as a first-in-first-out (FIFO) stack, when overwriting the oldest audit information in the storage device with the new audit information. Memory is used because of the very high traffic flow speeds supported by a security 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. Security appliances do follow every write to an audit log with an asynchronous write to a backup syslog device. This way memory acts as a high-speed FIFO buffer device to store megabytes of audit information, so that all writes to the backup device will be serviced without audit data loss. The syslog backup device is not part of the TOE.

The technique of overwriting the oldest audit records once memory no longer has space for audit information limits the audit records that can be lost. All audit information is written at a speed that is directly proportional to audited activity. Audited activity on a protected network is rarely continuous over

time, but occurs in bursts, average traffic flow, and lulls where traffic that causes audited events are low. The worst case for audit loss would occur if memory wrote an audit record in the last available location, and a burst of audited events occurred before they could be written to the backup syslog device. By overwriting the oldest audit information with the latest audit information to a very high-speed memory, the memory can never lose audit information in that no audit records can ever be "dropped" or not written. Additionally, the security appliances can be configured to notify the administrator when the logs capacity has reached a specified percentage.

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

6.1.2 Information Flow

The TOE implements three (3) different Security Function Policies (SFP) which include the AUTHENTICATED TRANSPARENT MODE SFP, UNAUTHENTICATED ROUTE MODE SFP, and AUTHENTICATED ROUTE MODE SFP.
The AUTHENTICATED TRANSPARENT MODE SFP applies to traffic to or from a network interface configured in Transparent Mode that is using a VPN tunnel.
The UNAUTHENTICATED ROUTE MODE SFP applies to traffic to or from a network interface configured in Route Mode or NAT Mode that is not using a VPN tunnel.
The AUTHENTICATED ROUTE MODE SFP applies to traffic to or from a network interface configured in Route Mode or NAT Mode that is using a VPN tunnel.
The differences in these three (3) types of SFPs are further described below.

Security 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).

EAL4

Simple security attribute (FDP_IFC.1a(EXP))

The TSF enforces the AUTHENTICATED TRANSPARENT MODE SFP on all IT entities that send and receive information through the TOE to one another using the Route-Based or Policy-Based Site-To-Site IPSEC VPN with pre-shared secret key authentication. 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.

The TOE uses only manual preshared keys for both authentication and encryption. The generation of these keys is outside the scope of the TOE. The manual pre-share key is delivered out of band using a mechanism beyond the scope of the TOE. The key values are included in the configuration information for the VPN channel. These values are stored locally in the SA tables. The encryption manual key is used to encrypt outgoing information in the VPN channel. A corresponding preshare key must be available in the receiving device otherwise the information will not be decrypted. Similarly, an authentication key is used for the authentication header generation when using HMAC. If a corresponding key is not available at the receiving device then the information will not be authenticated. In the case where the information cannot be decrypted or authenticated at the receiving end a VPN channel will not be established. Furthermore, the cryptographic methods used for the transmission and reception points for the VPN tunnel must match. These are also defined in the VPN configuration and stored in the SA table. If access is granted, information flow requests are still subject to other defined security policies and screen options and this may include those that are also subject to the AUTHENTICATED TRANSPARENT MODE SFP.

Multiple VPN tunnels can be configured in the TOE. For each VPN configuration, the parameters are stored in the SA table. The VPN attributes table size is dynamic and grows with each new VPN that is defined. The VPN attributes table stores the VPN relevant configuration data pertaining to the VPN name, cryptographic algorithms configured, tunnel interface binding, local and remote Security Parameters Index (SPI) , Encapsulating Security Payload (ESP) & Authentication Header (AH) Key[26], Key Exchange Proposals, and the VPN lifetime.

The security 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).

Simple security attributes (FDP_IFF.1a(EXP))

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

- Addresses and/or Address Zones (source and destination)
- Transport Layer (protocol)
- Interface (i.e., physical network port)
- Tunnel interface on which the traffic arrives and departs
- Service (A service is considered a protocol assigned to a port or as data specific to a service such as FTP-GET)

The service can be filtered using the Application Layer Gateway27 (ALG) software component of the TOE. ALG intercepts and analyzes specified traffic, allocates resources, and enforces dynamic policies defined to permit or deny traffic passing trough the TOE. Through support of the ALG, the TOE provides the capability to filter DNS, RSH, FTP, HTTP, and H.323 services, as well as, granular HTTP component

[26] The ESP and AH key is what the pre-shared secret key consists of.
[27] The RSH ALG filtering is not supported when used with port address translation.

blocking. HTTP component blocking allows the administrator to selectively choose which HTTP components[28] (e.g. ActiveX controls, Java applets, .exe files, .zip files) that are to be blocked by the TOE.

The addresses and/or address groups may be used to map a network or a group of networks to a security zone. This allows the administrator to configure a policy that applies to a specific network or to a group of networks, rather than having to write multiple policies to perform a similar task for a group of networks.

The access policy can be configured to control information flow based on all combinations of these elements. Access policies only apply to TCP and UDP transport layer protocols. Access policies may be configured to permit, deny, or tunnel information matching the policy. The AUTHENTICATED TRANSPARENT MODE SFP supports all three of these actions. However, the tunnel action is required for an external IT entity to successfully invoke the tunnel interface and establish a VPN connection. The TOE also supports establishing multiple tunnels to a single tunnel interface.

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

The security appliances also support multiple policies based on zones. When performing a policy lookup on an information flow received by the TOE, the TOE applies the following rules to determine which type of zone policy shall apply to the information flow:

Any time an information flow request is received by the TOE, the TOE performs a policy lookup to determine how the requesting information flow should be treated.

If the information flow request initiating a VPN tunnel arrives on an internal network, the information flow may be permitted to traverse through the TOE to another connected network if:

- the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;
- 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.

If the information flow request initiating a VPN tunnel arrives on the external network, the information flow may be permitted to traverse through the TOE to another connected network if:

- the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;
- 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.

The TOE first checks to see if the source and destination zones are the same or different.

- If the source and destination zones are different, then the TOE performs a policy lookup in the interzone policy set list, or

[28] It is noted that only .zip and .exe files are supported in the evaluated configuration of the TOE. While Java and ActiveX components are not restricted from the evaluated configuration, their functionality is not included within the TSF claims made by the TOE.

- If no interzone policy is defined to permit the requested information flow, then the information flow is dropped by the default deny policy.

In addition to the set of policy checks an information flow request is subjected to, the TOE also checks information flow requests against IP spoofing, broadcasted packets and loopback packets.

An information flow request is detected as IP spoofing if the request arrives on an external TOE interface and the presumed address of the source subject is an external IT entity on an internal network, or if the request arrives on an internal TOE interface and the presumed address of the source subject is an external IT entity on the external network.

An information flow request is detected as a broadcast packet if the request 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.

An information flow request is detected as a loopback packet if the request 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.

Subset information flow control (FDP_IFC.1b(EXP))

The TSF enforces the UNAUTHENTICATED ROUTE MODE 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.

Security 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).

Simple security attributes (FDP_IFF.1b(EXP))

The UNAUTHENTICATED ROUTE MODE 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 to apply a default policy that is available. Each access policy contains at least the following elements:

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

The service can be filtered using the Application Layer Gateway[29] (ALG) software component of the TOE. ALG intercepts and analyzes specified traffic, allocates resources, and enforces dynamic policies defined to permit or deny traffic passing trough the TOE. Through support of the ALG, the TOE provides the capability to filter DNS, RSH, FTP, HTTP, and H.323 services, as well as, granular HTTP component blocking. HTTP component blocking allows the administrator to selectively choose which HTTP components[30] (e.g. ActiveX controls, Java applets, .exe files, .zip files) that are to be blocked by the TOE.

The addresses and/or address groups may be used to map a network or a group of networks to a security zone. This allows the administrator to configure a policy that applies to a specific network or to a group of networks, rather than having to write multiple policies to perform a similar task for a group of networks.

[29] The RSH ALG filtering is not supported when used with port address translation.

[30] It is noted that only .zip and .exe files are supported in the evaluated configuration of the TOE. While Java and ActiveX components are not restricted from the evaluated configuration, their functionality is not included within the TSF claims made by the TOE.

EAL4

The access policy can be configured to control information flow based on all combinations of these elements. Access policies only apply to TCP and UDP transport layer protocols. Access policies may be configured to permit, deny, or tunnel information matching the policy. However, the UNAUTHENTICATED ROUTE MODE SFP only supports the actions to permit or deny.

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

In addition to the actions identified, a policy may also be configured to perform Policy-Based Address Translation on information matching such a policy and may also be configured to block or reassemble fragmented packets pertaining to HTTP or FTP services

Policy-Based Address Translation may be performed on either the presumed source address of the information or on the presumed destination address of the information.

Policy-Based Address Translation that is applied to the presumed source address of the information may be configured to perform any of the following types of address translation:

- NAT-Src from a DIP Pool with PAT
- NAT-Src from a DIP Pool without PAT
- NAT-Src from a DIP Pool with Address Shifting
- NAT-Src from the Egress Interface IP Address

Policy-Based Address Translation that is applied to the presumed destination address of the information may be configured to perform any of the following types of address translation:

- NAT-Dst to a Single IP Address with Port Mapping
- NAT-Dst to a Single IP Address without Port Mapping
- NAT-Dst from an IP Address Range to a Single IP Address
- NAT-Dst between IP Address Ranges

The security appliances also supports multiple policies based on zones. When performing a policy lookup on an information flow received by the TOE, the TOE applies the following rules to determine which type of zone policy shall apply to the information flow:

Any time an information flow request is received by the TOE, the TOE performs a policy lookup to determine how the requesting information flow should be treated.

If the information flow request arrives on an internal network, the information flow may be permitted to traverse 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.

If the information flow request arrives on the external network, the information flow may be permitted to traverse 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.

The TOE first checks to see if the source and destination zones are the same or different.

- If the source and destination zones are different, then the TOE performs a policy lookup in the interzone policy set list, or
- If the source and destination zones are the same, then the TOE performs a policy lookup in the intrazone policy set list.

If the TOE performs the interzone or intrazone policy lookup and does not find a match, then the TOE checks the global policy set list for a match.

- If the TOE performs the interzone and global policy lookups and does not find a match, then the TOE applies the default deny policy to the packet.

In addition to the set of policy checks an information flow request is subjected to, the TOE also checks information flow requests against IP spoofing, broadcasted packets and loopback packets.

An information flow request is detected as IP spoofing if the request arrives on an external TOE interface and the presumed address of the source subject is an external IT entity on an internal network, or if the request arrives on an internal TOE interface and the presumed address of the source subject is an external IT entity on the external network.

An information flow request is detected as a broadcast packet if the request 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.

An information flow request is detected as a loopback packet if the request 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.

Subset information flow control (FDP_IFC.1c(EXP))

The TSF enforces the AUTHENTICATED ROUTE MODE SFP on all IT entities that send and receive information through the TOE to one another using the Route-Based or Policy-Based Site-To-Site IPSEC VPN with pre-shared secret key authentication. 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.

The TOE uses only manual preshared keys for both authentication and encryption. The generation of these keys is outside the scope of the TOE. The manual pre-share key is delivered out of band using a mechanism beyond the scope of the TOE. The key values are included in the configuration information for the VPN channel. These values are stored locally in the SA tables. The encryption manual key is used to encrypt outgoing information in the VPN channel. A corresponding preshare key must be available in the receiving device otherwise the information will not be decrypted. Similarly, an authentication key is used for the authentication header generation when using HMAC. If a corresponding key is not available at the receiving device then the information will not be authenticated. In the case where the information cannot be decrypted or authenticated at the receiving end a VPN channel will not be established. Furthermore, the cryptographic methods used for the transmission and reception points for the VPN tunnel must match. These are also defined in the VPN configuration and stored in the SA table. If access is granted, information flow requests are still subject to other defined security policies and screen options and this may include those that are also subject to the AUTHENTICATED ROUTE MODE SFP.

Multiple VPN tunnels can be configured in the TOE. For each VPN configuration, the parameters are stored in the SA table. The VPN attributes table size is dynamic and grows with each new VPN that is defined. The VPN attributes table stores the VPN relevant configuration data pertaining to the VPN name, cryptographic algorithms configured, tunnel interface binding, local and remote Security Parameters Index

(SPI) , Encapsulating Security Payload (ESP) & Authentication Header (AH) Key[31], Key Exchange Proposals, and the VPN lifetime.

Security 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).

Simple security attributes (FDP_IFF.1c(EXP))

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

- Addresses and/or Address Zones (source and destination)
- Transport Layer (protocol)
- Interface (i.e., physical network port)
- Tunnel interface on which the traffic arrives and departs
- Service (A service is considered a protocol assigned to a port or as data specific to a service such as FTP-GET)

The service data can be filtered using the Application Layer Gateway32 (ALG) software component of the TOE. ALG intercepts and analyzes specified traffic, allocates resources, and enforces dynamic policies defined to permit or deny traffic passing trough the TOE. Through support of the ALG, the TOE provides the capability to filter DNS, RSH, FTP, HTTP, and H.323 services, as well as, granular HTTP component blocking. HTTP component blocking additionally allows the administrator to selectively choose which HTTP components[33] (e.g. ActiveX controls, Java applets, .exe files, .zip files) that are to be blocked by the TOE.

The addresses and/or address groups may be used to map a network or a group of networks to a security zone. This allows the administrator to configure a policy that applies to a specific network or to a group of networks, rather than having to write multiple policies to perform a similar task for a group of networks.

The access policy can be configured to control information flow based on all combinations of these elements. Access policies only apply to TCP and UDP transport layer protocols. Access policies may be configured to permit, deny, or tunnel information matching the policy. The AUTHENTICATED ROUTE MODE SFP supports all three of these actions. However, the tunnel action is required for an external IT entity to successfully invoke the tunnel interface and establish a VPN connection. The TOE also supports establishing multiple tunnels to a single tunnel interface.

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

In addition to the actions identified, a policy may also be configured to perform Policy-Based Address Translation on information matching such a policy and may also be configured to block or reassemble fragmented packets on a per-zone basis.

Policy-Based Address Translation may be performed on either the presumed source address of the information or on the presumed destination address of the information.

[31] The ESP and AH key is what the pre-shared secret key consists of.
[32] The RSH ALG filtering is not supported when used with port address translation.
[33] It is noted that only .zip and .exe files are supported in the evaluated configuration of the TOE. While Java and ActiveX components are not restricted from the evaluated configuration, their functionality is not included within the TSF claims made by the TOE.

EAL4

Policy-Based Address Translation that is applied to the presumed source address of the information may be configured to perform any of the following types of address translation:

- NAT-Src from a DIP Pool with PAT
- NAT-Src from a DIP Pool without PAT
- NAT-Src from a DIP Pool with Address Shifting
- NAT-Src from the Egress Interface IP Address

Policy-Based Address Translation that is applied to the presumed destination address of the information may be configured to perform any of the following types of address translation:

- NAT-Dst to a Single IP Address with Port Mapping
- NAT-Dst to a Single IP Address without Port Mapping
- NAT-Dst from an IP Address Range to a Single IP Address
- NAT-Dst between IP Address Ranges

The security appliances also supports multiple policies based on zones. When performing a policy lookup on an information flow received by the TOE, the TOE applies the following rules to determine which type of zone policy shall apply to the information flow:

Any time an information flow request is received by the TOE, the TOE performs a policy lookup to determine how the requesting information flow should be treated.

If the information flow request initiating a VPN tunnel arrives on an internal network, the information flow may be permitted to traverse through the TOE to another connected network if:

- the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;
- 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.

If the information flow request initiating a VPN tunnel arrives on the external network, the information flow may be permitted to traverse through the TOE to another connected network if:

- the external IT entity initiating the information flow has successfully authenticated to the TOE using the pre-shared secret key associated with the VPN connection;
- 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.

The TOE first checks to see if the source and destination zones are the same or different.

- If the source and destination zones are different, then the TOE performs a policy lookup in the interzone policy set list, or
- If the source and destination zones are the same, then the TOE performs a policy lookup in the intrazone policy set list.

EAL4

If the TOE performs the interzone or intrazone policy lookup and does not find a match, then the TOE checks the global policy set list for a match.

- If the TOE performs the interzone and global policy lookups and does not find a match, then the TOE applies the default deny policy to the packet.

In addition to the set of policy checks an information flow request is subjected to, the TOE also checks information flow requests against IP spoofing, broadcasted packets and loopback packets.

An information flow request is detected as IP spoofing if the request arrives on an external TOE interface and the presumed address of the source subject is an external IT entity on an internal network, or if the request arrives on an internal TOE interface and the presumed address of the source subject is an external IT entity on the external network.

An information flow request is detected as a broadcast packet if the request 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.

An information flow request is detected as a loopback packet if the request 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.

Subset residual information protection (FDP_RIP.1)

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

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

Key material resources are distributed and managed using the security 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 security appliance.

Error! Reference source not found.

To support the FDP_IFC.1a, FDP_IFF.1a FDP_IFC.1c and FDP_IFF.1c information flow requirements, the TOE provides encryption/decryption capabilities for VPN sessions. The TOE performs encryption/decryption using IPSEC. The TOE supports performing encryption and decryption using 64-bit DES, 196-bit 3DES, or 128-bit, 192-bit, or 256-bit AES. The DES and 3DES encryption/decryption capabilities conform to FIPS PUB 81 [4] and the AES encryption/decryption capabilities conform to FIPS 197. The TOE supports secure hashing using MD5 Message-Digest Algorithm as specified in IETF RFC1321, or Secure Hash Standard (SHA) as specified in FIPS 180-2 or HMAC specified in IETF RFC2104

When data arrives at a tunnel interface and the policies defined permit the information flow and the pre-shared key supplied matches the pre-shared key configured for the destined tunnel, then the TOE performs decryption of the session and processes the information flow. When data departs through a tunnel interface and the policies defined permit the information flow and the pre-shared key supplied matches the pre-

shared key configured for the destined tunnel, then the TOE performs encryption of the session and processes the information flow.

6.1.3 Identification and Authentication

User attribute definition (FIA_ATD.1)

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.

Verification of secrets (FIA_SOS.1)

The TSF requires administrators of the TOE to maintain a password of at least eight (8) characters in length, by default. The TSF also provides the capability for an administrator to configure password requirements to require a minimum length of up to thirty one (31) characters. However, the evaluated configuration of the TOE requires passwords to be at least a minimum of eight (8) characters. Therefore password length values may be set to more than eight (8) characters in length, but should not be set to less than eight (8) characters in length. In order to successfully change the minimum password length, the password of the administrator performing the change must first meet the minimum password requirements that are to be enforced before the requested change succeeds.

Timing of authentication (FIA_UAU.1)

Security 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.

User identification before any action (FIA_UID.2)

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

Management of security functions behavior (FMT_MOF.1)

The UNAUTHENTICATED TRANSPARENT MODE SFP, AUTHENTICATED TRANSPARENT MODE SFP, UNAUTHENTICATED ROUTE MODE SFP, and AUTHENTICATED ROUTE MODE SFP are configured through a locally connected console. The authorized administrator must be successfully identified and authenticated before they can access any security management functions.

The following security management functions are restricted to the authorized administrator:

- start-up and shutdown;
- create, delete, modify, and view information flow security policy rules that permit or deny information flows;
- create, delete, modify, and view user attribute values defined in FIA_ATD.1;
- create, delete, and modify VPN tunnels.
- modify and set the time and date;
- archive, create, delete, empty, and review the audit trail;
- backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
- recover to the state following the last backup;
- Enable/Disable SCREEN firewall protections;
- Manage TOE interfaces;
- Recovery of the TOE to a secure state.

EAL4

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

Static attribute initialization (FMT_MSA.3)

By default, a security appliance denies all traffic in all directions, except the Juniper Networks NetScreen-5GT, and 5XT, which will allow traffic from the trusted network to the untrusted network by default. The administrator is instructed in the administrative guidance[34] to change the policy for the 5GT, 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.

Specification of Management Functions (FMT_SMF.1)

Security appliances provide the security management function for the following management capabilities:

- Startup and shutdown;
- Create, delete, modify, and view information flows rules that permit or deny information flows;
- Create, delete, modify, and view user attribute values defined in FIA_ATD.1;
- Create, delete, modify and view VPN tunnels;
- Enable/Disable SCREEN firewall protections;
- Manage TOE interfaces;
- Modify and set the time and date;
- Archive, create, delete, empty, and review the audit trail;
- Backup and recovery of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
- Recovery of the TOE to a secure state.

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

Security roles (FMT_SMR.1)

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

6.1.5 Protection of the TSF

Manual recovery (FPT_RCV.1(EXP))

Security appliances provide the capability to recover the configuration of an appliance to a Last-Known-Good configuration. Therefore in the event that an appliance has been reconfigured to an inoperable or vulnerable state, the appliance can be quickly recovered to its Last-Known-Good configuration. In the case where the TOE is within an inoperable state, an administrator can enter into a maintenance mode to recover to the Last-Known-Good configuration from within the console. This functionality, however, requires that an administrator has established a recovery point as a Last-Known-Good configuration.

Non-bypassability of the TSP (FPT_RVM.1)

[34] For instructions on configuring 5GT, or 5XT security appliances to provide restrictive default information flow policies, see the appendix within the User Guide of the respective security appliance.

EAL4

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

TSF domain separation (FPT_SEP.1)

Protection of the TOE from physical tampering is ensured by its environment. It is assumed that security appliances will remain attached to the physical connections made by an administrator so that an appliance cannot be bypassed. Each security appliance is completely self-contained. The hardware and firmware provided by security appliances provide all the services necessary to implement the TOE. There are no external interfaces into the TOE other than the physical ports provided. No general purpose operating system, disk storage, or programming interface is provided.

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

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

Logically, each security appliance is protected by the integrity of the protocol interpreters supporting the external interface. As long as network packets remain objects to be operated on by ScreenOS, the TSF is protected. ScreenOS is a custom operating system that runs in hardware, remains memory resident, and supports only trusted processes. A security 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 security 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.

Reliable time stamps (FPT_STM.1)

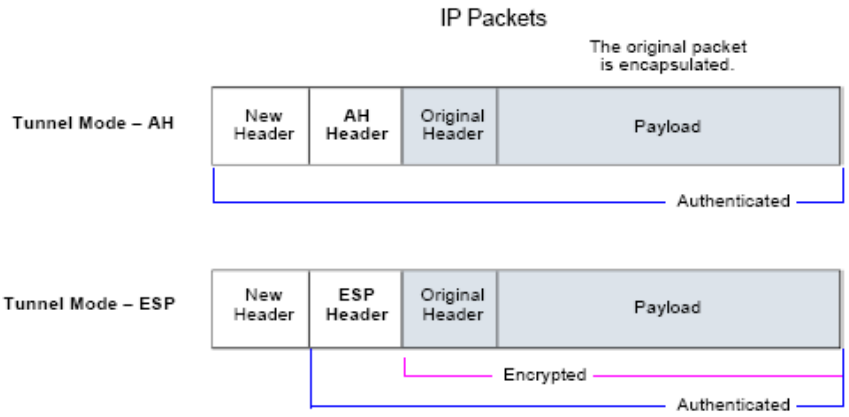
Security appliance hardware provides a reliable clock, and the ScreenOS uses this clock to provide reliable time stamps. Both are part of the TSF.

Inter-TSF confidentiality during transmission (FPT_ITC.1a and FPT_ITC.1b)

IPSEC Tunnel

The entire original IP packet—payload and header—is encapsulated within another IP payload and a new header appended to it. The entire original packet can be encrypted, authenticated, or both. With AH, the AH and new headers are also authenticated. With ESP, the ESP header can also be authenticated. In a site-to-site VPN, the source and destination addresses used in the new header are the IP addresses of the outgoing interface (in NAT or Route mode) or the VLAN1 IP address (in Transparent mode); the source and destination addresses of the encapsulated packets are the addresses of the ultimate endpoints of the connection.

EAL4



Authentication Header

The Authentication Header (AH) protocol provides a means to verify the authenticity/integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated via a hash-based message authentication code (HMAC) using a secret key and either MD5 or SHA-1 hash functions.

Message Digest version 5 (MD5)—An algorithm that produces a 128-bit hash (also called a digital signature or message digest) from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity.
Secure Hash Algorithm-1 (SHA-1)—An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the NetScreen ASIC, the performance cost is negligible.

ESP

The Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption), and source authentication and content integrity (authentication). ESP in tunnel mode encapsulates the entire IP packet (header and payload), and then appends a new IP header to the now encrypted packet. This new IP header contains the destination address needed to route the protected data through the network. With ESP, you can encrypt and authenticate, encrypt only, or authenticate only. For encryption, you can choose either of the following encryption algorithms:

Data Encryption Standard (DES)—A cryptographic block algorithm with a 56-bit key.
Triple DES (3DES)—A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Advanced Encryption Standard (AES)—An emerging encryption standard which, when adopted by Internet infrastructures worldwide, will offer greater interoperability with other network security devices. NetScreen supports AES with 128-, 192-, and 256-bit keys. For authentication, you can use either MD5 or SHA-1 algorithms.

For either the encryption or authentication algorithm you can select **NULL**; however, you cannot select **NULL** for both simultaneously.

With Manual Keys, administrators at both ends of a tunnel configure all the security parameters. This is a viable technique for small, static networks where the distribution, maintenance, and tracking of keys are not difficult. However, safely distributing Manual Key configurations across great distances poses security issues. Aside from passing the keys face-to-face, you cannot be completely sure that the keys have not been

compromised while in transit. Also, whenever you want to change the key, you are faced with the same security issues as when you initially distributed it.

The following is an example of the CLI command to define the VPN parameters. In this example, two passwords are given one, for the authentication (SHA-1) and one for the encryption (3DES).

The VPN parameters are defined in the set vpn command. In the case of manual key, the body of the command has three options, regarding the IPSEC tunnel.

```
set vpn tunn_str manual spi_num1 spi_num2 gateway ip_addr [
outgoing-interface interface ] { ah { md5 | sha-1 } { key key_str |
password pswd_str } | esp {
aes128 | aes192 | aes256 | des | 3des
{ key key_str | password pswd_str } |
null
}
[ auth { md5 | sha-1 }
{ key key_str | password pswd_str }
]
}
```

The "ah" parameter configures the use of the Authentication Header (per RFC 2402). And supports the following parameters:

Parameter	Algorithm	RFC
md5	MD5	2402
sha1	SHA-1	2402

If the ah parameter is omitted, then no application header is generated.

The "esp" parameter configures the use of the Encapsulating Security Protocol header (per RFC 2406) and supports the following
sub-parameters:

Parameter	Algorithm	RFC
des	DES	1829
3des	Triple-DES	1851
aes128	AES (128 bit key)	3602
aes192	AES (192 bit key)	3602
aes256	AES (256 bit key)	3602
null	None	2410
auth		
md5	MD5	2406
sha1	SHA-1	2406

A null value in any of the fields will disable the function.

For more information regarding the establishment and configuration of VPN please refer to the Netscreen Concept and Examples ScreenOS Reference Guide Chapter 5 VPNs
P/N 093-138-000

EAL4

The following devices have received FIPS 140-2 certification

Product	FIPS Product Certification	FIPS Algorithm Certification
NetScreen-5400	Certificate No. 605	AES (Cert. #11); Triple-DES (Certs. #118 and #133); DES (transitional phase only - valid until May 19, 2007; Certs. #174 and #184); SHS (Certs. #103 and #119); RSA (Cert. #24); HMAC (Cert. #52); DSA (Cert. #132); RNG (Cert. #33)
NetScreen-5200	Certificate No. 603	AES (Cert. #11); Triple-DES (Certs. #118 and #133); DES (transitional phase only - valid until May 19, 2007; Certs. #174 and #184); DSA (Cert. #132); SHS (Certs. #103 and #119); RSA (Cert. #24); HMAC (Cert. #52); RNG (Cert. #33)
ISG 2000	Conformance Claimed, no Certificate	DES (Cert. #323) TDES (Cert. #352) AES (Cert. #269) SHA (Cert. #349
NetScreen-500	Certificate No. 604	AES (Cert. #244); Triple-DES (Cert. #50); DES (transitional phase only - valid until May 19, 2007; Cert. #115); DSA (Cert. #134); SHS (Cert. #47); RSA (Cert. #23); HMAC (Cert. #54); RNG (Cert. #32)
NetScreen-208	Certificate No. 607	AES (Cert. #11); Triple-DES (Cert. 118); DES (transitional phase only - valid until May 19, 2007; Cert. #174); DSA (Cert. #132); SHS (Cert. 103); RSA (Cert. #24); HMAC (Cert. #52); RNG (Cert. #33)
NetScreen-204	Certificate No. 607	AES (Cert. #11); Triple-DES (Cert. 118); DES (transitional phase only - valid until May 19, 2007; Cert. #174); DSA (Cert. #132); SHS (Cert. 103); RSA (Cert. #24); HMAC (Cert. #52); RNG (Cert. #33)
NetScreen-5GT	**Certificate No. 629**	AES - CBC mode (Cert. #239) . Triple-DES - TCBC mode (Cert. #329) . DES - CBC mode (transitional phase only - valid until May 19, 2007, Cert. #307, for legacy systems only) . DSA (Cert. #125) . SHS (Cert. #286) . RSA Sign/Verify (Cert. #59) . HMAC SHA-1 (Cert. #16) . RNG (Cert. #58)
NetScreen-5XT	Certificate No. 606	AES (Cert. #11); Triple-DES (Cert. #118); DES (transitional phase only - valid until May 19, 2007; Cert. #174); DSA (Cert. #132); SHS (Cert. #103); RSA (Cert. #24); HMAC (Cert. #52); RNG (Cert. #33)

The following products have FIPS compatible components by virtue that they are identical to cryptographic modules used by certified products

Product	FIPS Product Certification	FIPS Algorithm Attestation
ISG 1000	Conformance Claimed, no Certificate	cryptographically identical to the ISG-2000
NetScreen-50	Conformance Claimed, no Certificate	cryptographically identical to the Netscreen - 204
NetScreen-25	Conformance Claimed, no Certificate	cryptographically identical to the Netscreen - 204

EAL4

6.2 TOE Security Assurance Measures

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

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

6.2.1 Configuration Management

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

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

6.2.2 Life Cycle Support

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

- Juniper Life-Cycle Plan

The Process Assurance measures satisfy the following assurance requirements:

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

6.2.3 Delivery and Guidance

Juniper 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. Juniper'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:

Reference Guide

Juniper Networks NetScreen CLI Reference Guide, Version 5.0.0 Command Descriptions, P/N 093-1352-000, Rev A

Concepts and Examples Document Set:

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 2: Fundamentals Screen OS 5.0.0 P/N 093-1345-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 3: Administration, P/N 093-1346-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 4: Attack Detection and Defense Mechanisms, P/N 093-1347-000, Revision A

NetScreen Concepts and Examples ScreenOS Reference Guide, Volume 5: VPNs, P/N 093-1348-000, Revision A

Audit Record Description Document:

NetScreen Message Log Reference Guide, ScreenOS Version 5.0.0, P/N 093-1353-000, Revision A

User's Guides:

NetScreen-5XT User's Guide, Version 5.0, P/N 093-1323-000, Revision A

NetScreen-25 User's Guide, Version 5.0, P/N 093-1245-000, Revision A

NetScreen-50 User's Guide, Version 5.0, P/N 093-1249-000, Revision A

NetScreen-200 Series User's Guide, Version 5.0, P/N 093-1253-000, Revision A

NetScreen-500 User's Guide, Version 5.0, P/N 093-0973-000, Revision A

NetScreen-5000 User's Guide, Version 5.0, P/N 093-1216-000, Revision A

NetScreen-5GT User's Guide, Version 5.0, P/N 093-1239-000, Revision B

NetScreen-ISG 1000 User's Guide, Version 5.0, P/N 093-1511-000, Revision B

NetScreen-ISG 2000 User's Guide, Version 5.0, P/N 093-1220-000, Revision C

Release Notes:

NetScreen Release Notes ScreenOS 5.0.0r9, P/N 093-1459-000, Revision A

Configuration Guidance

Juniper 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 Security appliances in accordance with the evaluated configuration. The administrator and user guidance is documented in:

Juniper Networks Configuration for Common Crtieria, EAL4, Document Number 093-1737-000, Revision D, 11/23/2005

EAL4

Delivery and Operation documentation

Juniper Networks Common Criteria EAL4 Delivery of the Product to Buyer, Document Number 093-1557-000, Revision C• •

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

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

6.2.4 Development

Juniper 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:

- Juniper Networks Security Appliances Functional Specification
- Juniper Networks Security Appliances High Level Design
- Juniper Networks Security Appliances Low Level Design
- Juniper Networks Security Appliances Correspondence Matrix
- Juniper Networks Security Appliances Security Policy Model For Common Criteria
- ADV_FSP.2: The Juniper Networks Security Appliances Functional Specification, including its references, describes the external interfaces to the TOE
- ADV_HLD.2: The Juniper Networks Security Appliances High Level Design, and its references, decomposes the TOE into subsystems
- ADV_LLD.1: The Juniper Networks Security Appliances Low-level Design Specification satisfies the requirement to decompose each subsystem into modules and fully describes each module.
- ADV_IMP.1: A subset of the source code and hardware diagrams used to generate the TOE satisfies this requirement.
- ADV_RCR.1: The way that this correspondence is evident within the design documentation is:
    - ST-TSS to FSP: The Juniper Networks Security Appliances Correspondence Matrix document identifies the interfaces that provide the security functions in the ST.
    - FSP to HLD: The Juniper Networks Security Appliances Correspondence Matrix document describes how the various security behavior of the external interfaces described in the FSP are further refined.
    - HLD to LLD: The Juniper Networks Security Appliances Correspondence Matrix document, describes how the various security behavior of the external interfaces described in the Juniper Networks Security Appliances High-level Design Specification are further refined.
    - LLD to IMP: The Juniper Networks Security Appliances Low-level Design Specification also serves to correspond modules with their specific implementations.
- ADV_SPM.1: The Juniper Networks Security Appliances Security Policy Model models the entities and rules related to the policies for identification and authentication, audit, and all of the information flow policies. Additionally, correspondence with the Juniper Networks Security Appliances Functional Specification is described.

EAL4

6.2.5 Tests

Juniper 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:

- Juniper Networks Security Appliances Correspondence Matrix
- Juniper Networks Security Appliance Test Cases for the Common Criteria
- Juniper Networks Security Appliances Test Plan

The Tests assurance measure satisfies the following assurance requirements:

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

6.2.6 Vulnerability Assessment

6.2.6.1 Evaluation of Misuse

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

- Juniper Networks Security Appliance User's Guides

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

- The Juniper Networks Security Appliances Misuse Analysis

6.2.6.2 Strength of TOE Security Functions and Vulnerability Analysis

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

Juniper 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:

- Juniper Networks Security Appliances Vulnerability Analysis.

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

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

7.0 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. The rationale in this section and Section 8 demonstrates conformance to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. Juniper has elected to pursue a more vigorous assurance level as depicted in Conformance Claims section.

7.1 PP Reference

This ST complies with all security requirements, security objectives, and security environment statements for the defined TOE and its environment as they are stated within U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

7.1.1 IT Security Requirement Statements

The following IT security requirement statements are stated within this ST using the permitted operations specified within the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999:

IT Security Assurance Requirements

- ACM_CAP.4 Generation support and acceptance procedures (Exceeds ACM_CAP.2)
- ADO_DEL.2 Detection of modification (Exceeds ADO_DEL.1)
- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.2 Fully defined external interfaces (Exceeds ADV_FSP.1)
- ADV_HLD.2 Security enforcing high-level design (Exceeds ADV_HLD.1)
- ADV_RCR.1 Informal correspondence demonstration
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance
- ATE_COV.2 Analysis of Coverage (Exceeds ATE_COV.1)
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing - sample
- AVA_SOF.1 Strength of TOE security function evaluation
- AVA_VLA.2 Independent Vulnerability Analysis (Exceeds AVA_VLA.1)

EAL4

IT Security Functional Requirements

- Audit data generation (FAU_GEN.1)
- 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 operation (FCS_COP.1a)
- Cryptographic operation (FCS_COP.1b)
- Cryptographic operation (FCS_COP.1c)
- Subset information flow control (FDP_IFC.1a(EXP))
- Subset information flow control (FDP_IFC.1b(EXP))
- Subset information flow control (FDP_IFC.1c(EXP))
- Simple security attributes (FDP_IFF.1a(EXP))
- Simple security attributes (FDP_IFF.1b(EXP))
- Simple security attributes (FDP_IFF.1c(EXP))
- Subset residual information protection (FDP_RIP.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- User identification before any action (FIA_UID.2)
- Management of security functions behavior (FMT_MOF.1)
- Static attribute initialization (FMT_MSA.3)
- Security roles (FMT_SMR.1)
- Non-bypassability of the TSP (FPT_RVM.1)
- TSF domain separation (FPT_SEP.1)
- Reliable time stamps (FPT_STM.1)
- Inter-TSF confidentiality during transmission (FPT_ITC.1a)
- Inter-TSF confidentiality during transmission (FPT_ITC.1b)

7.2 PP Tailoring

This section identifies the security requirements, security objectives, or security environment statements that are tailored from their original specification in the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

Note that the TFFPP indicates that security functional requirements have specific strength of function metrics. Of those requirements, FIA_UAU.4 requires a FIPS PUB 140-1 compliant mechanism for single-use authentication, which is outside the scope of the evaluation. However, FIA_UAU.1 does address the password authentication mechanism portion of the requirement. This is addressed in Strength of Function (SOF) Rationale. Additionally, the PP requires a minimum overall level of SOF-basic. However, this ST is claiming SOF-medium to conform better to the EAL 4 requirements.

This Security Target includes all of the assumption and threat statements described in the PP, verbatim. Note that the assumption A.REMACC is included in this ST, even though it is unnecessary since it allows but does not demand that remote administration can be supported.

7.2.1 Modified PP Items

The following table identifies items that were modified from the original specification within the PP.

Table 7.1: Modifications from PP

Requirement Component	Rationale for Modification
FAU_GEN.1	*Assignment* – The assignment started in the PP was completed with no additional attributes, however the assignment was refined to properly identify the referenced table.
FAU_GEN.1.1	*Refinement* – Changed the audit level claim to "not specified" to comply with International Interpretation #202.
	Refinement – Column three of Table 5.2 within the row labeled "FDP_IFF.1" was refined from its original state in the PP to include the additional capability of the TOE to record the action taken by each information flow decision.
FAU_GEN.1.1(c)	*Refinement* – The statement 'listed at the "extend" level' was removed from the assignment operation.
FAU_GEN.1.2(a)	*Refinement* – 'subject identities' was changed to 'subject identity'.
FCS_COP.1a, FCS_COP.1b AND FCS_COP.1c	*Refinement* – This requirement was refined to include the additional cryptographic algorithms 3DES and AES.
FDP_IFC.1* & FDP_IFF.1*	*Iteration* – These requirements were iterated to allow for three (3) types of information flow control policies being the following: AUTHENTICATED TRANSPARENT MODE SFP (FDP_IFC.1a(EXP) and FDP_IFF.1a(EXP)); UNAUTHENTICATED ROUTE MODE SFP (FDP_IFC.1b(EXP) and FDP_IFF.1b(EXP)); and AUTHENTICATED ROUTE MODE SFP (FDP_IFC.1c(EXP) and FDP_IFF.1c(EXP)).
FDP_IFC.1* & FDP_IFF.1*	*Refinement* – These requirements were refined from the original specification in the TFFPP from stating "The TSF shall…" to "The TSF shall **be able to**…". This refinement is necessary to allow the option of selecting a configuration (i.e. authenticated transparent mode, unauthenticated NAT/Route mode, or authenticated NAT/Route mode). Each of the listed configurations conforms to the TFFPP requirements. However in accordance with the footnote indicated in section 5.1.3, at least one of the identified configurations must be enforced to remain within the evaluated configuration and compliant with the TFFPP requirements.

EAL4

Requirement Component	Rationale for Modification
FDP_IFC.1a(EXP).1 & FDP_IFC.1c(EXP).1	*Refinement* – This requirement was refined from the original specification in the TFFPP. This requirement was refined to identify cases where authenticated information flows are established.
FDP_IFF.1a(EXP).1 FDP_IFF.1b(EXP).1 FDP_IFF.1c(EXP).1	*Assignment* – Completed one of the assignments stated in the PP with no additional attributes and completed the second assignment with "and service data".
FDP_IFF.1a(EXP).3 FDP_IFF.1b(EXP).3 FDP_IFF.1c(EXP).3	*Refinement* – This requirement was refined from the original specification in the TFFPP. The TFFPP completes the assignment in this requirement with "none". However, the "none" has been replaced with text that specifies additional information flow control rules enforced by the TOE for the order in which policies are checked in relation to zones.
FDP_IFF.1b(EXP).4 FDP_IFF.1c(EXP).4	*Refinement* – This requirement was refined from the original specification in the TFFPP. The TFFPP completes the assignment in this requirement with "none". However, the "none" has been replaced with text that specifies additional information flow control capabilities for address translation and fragment reassembly and blocking of information matching the policy rules to perform such action.
FIA_ATD.1	*Assignment* – Completed the assignment started in the PP with no additional attributes.
FMT_MOF.1 d) e) g) l)	This requirement excludes items d, e, g, & l since remote management is excluded from the TOE.
FMT_MSA.3	*Refinement* – This requirement was refined from the original specification in the TFFPP. The TFFPP completes the assignment in this requirement with "UNAUTHENTICATED SFP". However, the "UNAUTHENTICATED SFP" has been replaced with "AUTHENTICATED TRANSPARENT MODE SFP, UNAUTHENTICATED ROUTE MODE SFP, and AUTHENTICATED ROUTE MODE SFP" to support the additional information flow control policies defined within this ST.
EAL4	The PP requires only EAL 2. However, to satisfy the assurance requirements of environment requiring more assurance that the security functions are enforced, this Security Target has adopted the EAL 4 security assurance requirements and also increased the minimum SOF level from SOF-basic to SOF-medium.

7.2.1.1 Interpretations

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

Interpretation	Component	Rationale for Modification
I-202	FAU_GEN.1.1	Changed the audit level claim to "not specified" to comply with International Interpretation I-202.
I-0407	FDP_IFF.1a(EXP).4, FDP_IFF.1a(EXP).5, FDP_IFF.1b(EXP).4, FDP_IFF.1b(EXP).5, and FDP_IFF.1c(EXP).4, FDP_IFF.1c(EXP).5	These requirements were modified to reflect the proper selection per U.S. National Interpretation I-0407. There is no impact on the requirements.
RI #3	ACM_CAP.2	A new element was added to this component per International Interpretation.
I-0412	ACM_CAP.2.2D	This element was changed 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.

EAL4

Interpretation	Component	Rationale for Modification
RI #51	ADO_IGS.*.1C	this element was changed per International Interpretation RI #51
	AVA_VLA.*.1D and AVA_VLA.*.1D	these element were changed per International Interpretation RI #51
	AVA_VLA.2.1C through AVA_VLA.2.4C	these elements were changed and/or added per International Interpretation RI #51

7.2.2 Removed PP Items

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

Component	Rationale for Removal
FIA_AFL.1	This requirement is optional within the PP and is intended to detect attempts by untrusted users to gain unauthorized access by repeated logon attempts. Only remote administration would support the ability for such an attempt and since the TOE does not support this feature, this requirement is not applicable. Note that it cannot be applied to the local administrator logon interface since the result would be to lock the authorized administrator out which would prevent them from re-enabling their own access.
FIA_UAU.4	This requirement is requirement is optional within the PP and is intended to prevent the reuse of authentication information for remote administration authentication attempts by the use of single-use authentication mechanisms. However since the TOE does not support remote authentication, this requirement has been removed.

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

7.2.3 Added Items

The following items were added into this ST that were not included within the PP

Component	Rationale for Addition
A.CONSOLE	This assumption and corresponding security objective have been added to support the notion that non-remote administration is actually performed using a device connected to a local serial port.
A.LOCATE	This assumption and corresponding security objective have been added to support the access restriction of the management console to authorized administrators.
T. PROTECTION	This threat was added and the corresponding security objective O.PROTECTION have been added to support the notion that data transmitted from the TOE to a peer TOE via encryption may be accessed by an unauthorized person
FMT_SMF.1	This requirement was added in this Security Target to satisfy a dependency added to FMT_MOF.1 by International Interpretation I-065. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
FPT_RCV.1(EXP)	This requirement was added in this Security Target to define the capability for security appliances to recover to a last known good state in cases were a configuration is applied that results in an inoperable TOE.

EAL4

Component	Rationale for Addition
FIA_SOS.1	This requirement was added in this Security Target to define the capability for security appliances to require a minimum length of 8 characters for passwords generated by administrators of the TOE.
FPT_ITC. 1a and FPT_ITC.1b	This requirement was added to this Security Target to define the capability for security appliances to ensure Inter-TSF confidentiality during transmission.

8.0 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 TFFPP, is directly applicable to the Security Target. As such, references to the corresponding sections are provided rather than recreating or repeating that rationale.

8.1 Security Objectives Rationale

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

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

8.2 Security Functional Requirements Rationale

Except as noted below, the security functional requirements rationale is presented in Sections 6.3 of the TFFPP.

Even though requirements (i.e. 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.

All of the security functional and assurance requirements have been reproduced from the TFFPP to this ST, except for FMT_SMF.1, FDP_IFC.1a(EXP), FDP_IFC.1b(EXP), FDP_IFC.1c(EXP), FDP_IFF.1a(EXP), FDP_IFF.1b(EXP), FDP_IFF.1c(EXP), FIA_SOS.1 and FPT_RCV.1(EXP).

FMT_SMF.1 was included to satisfy a dependency of FMT_MOF.1 introduced in International Interpretation RI#65. FMT_SMF.1 requires that a defined set of security management functions are made available so that an administrator can effectively manage the security configuration of the TOE. This security functional requirement provides direct support for the O.SECFUN security objective.

FDP_IFF.1a(EXP) FDP_IFc.1a(EXP) were iterated from FDP_IFF.1 and FDP_IFC.1of the TFFPP to address the specific filtering capabilities provided by the TOE for Site-To-Site VPN connectivity through an interface configured in Transparent Mode. This security functional requirement provides direct support for the O.MEDIATE and O.PROTECTION security objectives.

FDP_IFF.1b(EXP) was iterated from FDP_IFF.1 of the TFFPP to address the specific filtering capabilities provided by the TOE through an interface configured in Route Mode or NAT Mode. This security functional requirement provides direct support for the O.MEDIATE security objective.

FDP_IFF.1c(EXP) FDP_IFC.1c(EXP) were iterated from FDP_IFF.1 and FDP_IFC.1 of the TFFPP to address the specific filtering capabilities provided by the TOE for Site-To-Site VPN connectivity through an interface configured in Route Mode or NAT Mode. This security functional requirement provides direct support for the O.MEDIAT and O.PROTECTION security objectives.

EAL4

FIA_SOS.1 was included to address the additional security functionality provided by the TOE for requiring administrator passwords to meet a defined level of strength properties. This security functional requirement provides direct support for the O.SELFPRO security objective.

FPT_RCV.1(EXP) was included to address the additional security functionality provided by the TOE for configuration rollback. This security functional requirement provides direct support for the O.SECSTA security objective.

FPT_ITC1a, FPT_ITC.1b, FCS_COP.1a, FCS_COP1b and FCS_COP1c were included to address the additional security functionality provided by the TOE for peer to peer data encryption. This security functional requirement provides direct support for the O.PROTECTION security objective.

8.3 Security Assurance Requirements Rationale

The security appliances meet all the TFFPP Assurance Requirements. Additionally, the TOE conforms to all the Assurance Requirements for an EAL4 assurance level.

Except as noted below, the security assurance requirements rationale is presented in Sections 6.4 of the TFFPP.

The EAL 4 requirements that exceed EAL 2, by the TFFPP are rationalized below:

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

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

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

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

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

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

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

ADV_LLD.1 Descriptive low-level design

EAL4

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

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

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

ALC_LCD.1 Developer defined life-cycle model
It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that the development and maintenance of the TOE are appropriately controlled.

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

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

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

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

8.4 Requirement Dependency Rationale

The rationale for not satisfying all dependencies is presented in Section 6.5 of the TFFPP. This Security Target includes the following Security Functional Requirements not included in the TFFPP:

FMT_SMF.1 – This requirement was included to satisfy a dependency of FMT_MOF.1 introduced in International Interpretation RI#65 and introduces no additional dependencies itself.

FIA_SOS.1 – This requirement was included to address restrictions of the password length for administrator accounts and introduces no additional dependencies itself.

FCS_COP.1a, b, c – This requirement was included to address the encryption/decryption of information flows and introduces the following dependencies:

- FCS_CKM.1 – This dependency was excluded from the ST since the TOE does not provide nor require any cryptographic key management capabilities for the claimed encryption/decryption method.

EAL4

- FCS_CKM.4 – This dependency was excluded from the ST since the TOE does not provide nor require any cryptographic key management capabilities for the claimed encryption/decryption method.
- FMT_MSA.2 – This dependency was excluded from the ST since the TOE does not provide nor require any cryptographic key management capabilities for the claimed encryption/decryption method.

In addition, the following requirements were explicitly stated:

FDP_IFC.1*(EXP) and FDP_IFF.1*(EXP) – These requirements were based upon FDP_IFC.1 and FDP_IFF.1 from the TFFPP, yet had to be explicitly stated to apply as a selection. However the dependencies for these requirements, as indicated within the TFFPP, are satisfied.

FPT_RCV.1(EXP) – This requirement was based upon FPT_RCV.1 from CC Part 2, yet had to be explicitly stated to require a manual means of recovery rather than through an automated means of recovery. However no dependencies, as indicated in CC Part 2, are introduced by this requirement.

8.5 Explicitly Stated Requirements Rationale

This ST contains requirements explicitly stated outside of context from, yet derived upon, the requirements defined within CC v2.1. These requirements are identified below along with their rationale explaining why they needed to be explicitly stated:

- *Subset information flow control (FDP_IFC.1a(EXP)), (FDP_IFC.1b(EXP)), (FDP_IFC.1c(EXP))*: These requirements were explicitly stated to allow for the selection of the three available information flow policies rather than requiring the enforcement of information flow control for a specific configuration. However, the ST clearly indicates that at least one of these three information flow policies must be enforced to remain compliant with the evaluated configuration. Therefore the original intent of FDP_IFC.1, to require an information flow policy to be enforced, is still applied.
- *Simple security attributes (FDP_IFF.1a(EXP)), (FDP_IFF.1b(EXP)), (FDP_IFF.1c(EXP))*: These requirements were explicitly stated to allow for the selection of the three available information flow policies rather than requiring the enforcement of information flow control for a specific configuration. However, the ST clearly indicates that at least one of these three information flow policies must be enforced to remain compliant with the evaluated configuration. Additionally, the security attributes defined within each of these requirements remain conformant to those security attributes defined for FDP_IFF.1 within the TFFPP. Therefore the original intent of FDP_IFF.1, to require an information flow policy to be enforced with the predefined set of security attributes, is still applied.
- *Manual recovery (FPT_RCV.1(EXP))*: This requirement was explicitly stated to allow for the manual recovery of the TOE rather than by an automated means, as was originally intended by FPT_RCV.1. However, all other attributes of this requirement conform to those defined for FPT_RCV.1 within CC v2.1.

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

In the context of 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 TFFPP

uses the original version of this requirement from the CC v2.1, it was decided to use that version in this ST as well. Since the version of the requirement in this ST has a broader scope, any TOE meeting the requirement in this ST would meet the interpretations. The requirement stated in this ST is effectively a refinement of the version represented in the interpretations and is not an explicitly stated requirement.

- *Audit data generation (FAU_GEN.1)*: U.S. National Interpretation I-410 serves to modify the original requirement to only require that audit records include user identifies when applicable. The TFFPP has already refined this requirement and this ST includes that version of the requirement. The modification suggested by I-410 has not been adopted since the relevant audit records will always have a user identity, even though the identity might not be valid (i.e., the identity typed in will be recorded). Hence, the requirement in this ST is effectively a refinement of the interpretation (i.e., any TOE meeting the requirement in this ST would meet the interpretation).

8.6 TOE Summary Specification Rationale

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

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

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

EAL4

Table 8.1 Security Functions vs. Requirements Mapping

	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				
FCS_COP.1(*)		X			
FDP_IFC.1(*)		X			
FDP_IFF.1(*)		X			
FDP_RIP.1		X			
FIA_ATD.1			X		
FIA_SOS.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_RCV.1(EXP)					X
FPT_RVM.1					X
FPT_SEP.1					X
FPT_STM.1					X
FPT_ITC.1(*)					X

8.7 Strength of Function (SOF) Rationale

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

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

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

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

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

- The password must be at least eight long;

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

The password space is calculated as follows:

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

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

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

EAL4

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

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

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

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

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.

9.0 Terminology and Acronyms

The following definitions are used throughout this ST. Refer to the TFFPP for additional terms and acronyms.

9.1 CC-Specific Terminology & Acronyms

These terms are drawn from section 2.3 of CC Part 1.

Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Guidance documentation	Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in section 5.2.4 of this ST.
Human user	Any person who interacts with the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Iteration	The use of a component more than once with varying operations.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.
Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Reference monitor	The concept of an abstract machine that enforces TOE access control policies.
Reference validation mechanism	An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security attribute	Characteristics of subjects, users, objects, information, and/or resources that is used for the enforcement of the TSP.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component.

Semiformal	Expressed in a restricted syntax language with defined semantics.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.
Subject	An entity within the TSC that causes operations to be performed.
System	A specific IT installation, with a particular purpose and operational environment.
Target of Evaluation (TOE)	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
Transfers outside TSF control	Communicating data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

9.2 TOE-Specific Terminology & Acronyms

Address	The network portion of an IP address. Most IP addresses have a network portion and a node portion.
Address Shifting	A mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in a different range.
Application-Specific Integrated Circuit (ASIC)	A customized microchip, which is designed for a specific application.
Authorized Administrator	A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.
Authorized external IT entity	Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.
Central Processing Unit (CPU)	The CPU controls the operation of a computer.
Destination Network Address Translation (NAT-dst)	The translation of the original destination IP address in a packet header to a different destination address. ScreenOS supports the translation of one or several original destination IP addresses to a single IP address (“one-to-one” or “many-to-one” relationships). The TOE also supports the translation of one range of IP addresses to another range (a “many-to-many” relationship) using address shifting. When the TOE performs NAT-dst without address shifting it can also map the destination port number to a different predetermined port number. When the TOE performs NAT-dst with address shifting, it cannot also perform port mapping.
Dynamic IP (DIP) Pool	A dynamic IP (DIP) pool is a range of IP addresses from which the security appliance can dynamically or deterministically take addresses to use when performing network address translation on the source IP address (NAT-src) in IP packet headers.
Dynamic Random Access Memory (DRAM)	A type of computer memory that is stored in capacitors on a chip. Most computers have DRAM chips, because they provide a lot of memory at a low cost.
External IT entity --	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Federal Information Processing Standards (FIPS)	The Federal Information Processing Standards Publication (FIPS PUB) series issued by the U.S. National Institute of Standards and Technology as technical guidelines for U.S. Government procurements of information processing system equipment and services.
FIPS 140-1 -	The U.S. Government standard for security requirements to be met by a cryptographic module used to protect unclassified information in computer and communication systems. The standard specifies four increasing levels (from 'Level 1' to 'Level 4') of requirements to cover a wide range of potential applications and environments. The requirements address basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference and electromagnetic compatibility (EMI/EMC), and self-testing.
Firmware -	Software stored in ROM or PROM; essential programs that remain even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on disk.

Flash Memory -	A small printed circuit board that holds large amounts of data in memory. Flash memory is used because it is small and holds its data when the computer is turned off.
Hyper Text Transfer Protocol (HTTP)	The protocol most commonly used in the World-Wide Web to transfer information from Web servers to Web browsers.
Internet Control Message Protocol (ICMP)	An extension to the Internet Protocol, which is used to communicate between a gateway and a source host, to manage errors and generate control messages.
IP Security (IPSEC)	An IP security protocol that provides for encapsulation of standard IP packets into Type 51 IP, allowing firewalls to recognize and admit encapsulated, encrypted data.
Mapped IP Address (MIP)	A MIP is a direct one-to-one mapping of traffic destined for one IP address to another IP address. The TOE forwards incoming traffic destined for a MIP to the host with the address to which the MIP points. Essentially, a MIP is static destination address translation, mapping the destination IP address in an IP packet header to another static IP address. When a MIP host initiates outbound traffic, the TOE translates the source IP address of the host to that of the MIP address. This bidirectional translation symmetry differs from the behavior of source and destination address translation. MIPs allow inbound traffic to reach private addresses in a zone whose interface is in NAT mode. MIPs also provide part of the solution to the problem of overlapping address spaces at two sites connected by a VPN tunnel.
Network Address Translation (NAT)	NAT involves translating the source IP address in a packet header to a different IP address. In the case of a traditional NAT, the translated source IP addresses comes from the IP address of the egress interface. When the security appliance uses the IP address of the egress interface, it translates all original source IP addresses to the address of the egress interface.
NAT Destination (NAT-dst)	NAT-dst involves translating the original destination IP address in a packet header to a different destination address. ScreenOS supports the translation of one or several original destination IP addresses to a single IP address (“one-to-one” or “many-to-one” relationships). The security appliance also supports the translation of one range of IP addresses to another range (a “many-to-many” relationship) using address shifting. When the security appliance performs NAT-dst without address shifting it can also map the destination port number to a different predetermined port number. When the security appliance performs NAT-dst with address shifting, it cannot also perform port mapping.
NAT Source (NAT-src)	NAT-src involves translating the source IP address in a packet header to a different IP address from a dynamic IP (DIP) address pool. When the security appliance draws addresses from a DIP pool, it can do so dynamically or deterministically. When doing the former, it randomly draws an address from the DIP pool and translates the original source IP address to the randomly selected address. When doing the latter, it uses address shifting to translate the source IP address to a predetermined IP address in the range of addresses that constitute the pool.
Network Basic Input/Output System (NetBIOS)	An application programming interface used in conjunction with other programs to transmit messages between applications running on PCs hooked to a local area network.
Network	A composition of a communications media and components attached to that medium whose responsibility is the transfer of information. Such components may include automated information systems, packet switches, telecommunications controllers, distribution centers, technical management, and control devices. It is a set of devices such as computers, terminals, and printers that are physically connected by a transmission medium so that they can communicate with each other.
Node	A concentration point in a network where numerous trunks come together at the same switch.

Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Port Address Translation (PAT)	The translation of the original source port number in a packet to a different, randomly designated port number.
Public-Key Infrastructure (PKI)	A system of Certificate Authority (CAs) (and, optionally, Registration Authority (RAs) and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
Session	A series of interactions between two communication end points that occur during the span of a single connection. Typically, one end point requests a connection with another specified end point and if that end point replies agreeing to the connection, the end points take turns exchanging commands and data ("talking to each other"). The session begins when the connection is established at both ends and terminates when the connection is ended.
Session Table	A resource within the security appliance that maintains a list of active sessions. The session table is utilized to verify if any requesting information flows may already have an established session.
Stateful inspection	Also referred to as *dynamic packet filtering*. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.
Synchronous Dynamic Random Access Memory (SDRAM)	High-speed DRAM that adds a separate clock signal to the control signals. SDRAM can transfer bursts of non-contiguous data at 100 MBytes/sec, and has an access time of 8-12 nanoseconds. It comes in 64-bit modules: long 168-pin DIMMs
Tampering	An unauthorized modification that alters the proper functioning of equipment or system in a manner that degrades the security or functionality it provides.
Transmission Control Protocol/Internetwork Protocol (TCP/IP)	A communications protocol developed under contract from the U.S. Department of Defense to internetwork dissimilar systems. Transport Control Protocol/Internet Protocol. Generally refers to the Internet Protocol Suite, which includes TCP and IP, as well as several other protocols, used by computers to communicate with each other. TCP/IP is the standard protocol used on the Internet. It can also be used as a communications protocol in the private networks called intranets and in extranets. TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.
TFFPP	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments
Tunneling	Use of one data transfer method to carry data for another method.

User Datagram Protocol (UDP)	A communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Like TCP (Transmission Control Protocol), UDP is used with IP (the Internet Protocol). Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.
Virtual IP Address (VIP)	A Virtual IP address (VIP) maps traffic received at one IP address to another address based on the destination port number in the packet header. In other words, the actual destination IP addresses for two VIPs can be the same, yet the TOE uses destination port number to determine where to forward traffic.
Virtual Private Network (VPN)	An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. It includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system.
Virtual Router (VR)	A virtual router (VR) is the component of ScreenOS that performs routing functions. A virtual router functions as a router. It has its own interfaces and its own routing table. By default, a security appliance supports two virtual routers: Untrust-VR and Trust-VR. This allows the security appliance to maintain two separate routing tables and to conceal the routing information in one virtual router from the other. For example, the untrust-vr is typically used for communication with untrusted parties and does not contain any routing information for the protected zones. Routing information for the protected zones is maintained by the trust-vr. Thus, no internal network information can be gleaned by the surreptitious extraction of routes from the untrust-vr.
Virtual System	A virtual system (vsys) is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same security appliance. Each one can be managed by its own virtual system administrator. Virtual systems are outside the scope of the evaluated configuration of the TOE.
Zone(s)	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or logical entity that performs a specific function (a function zone).