Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Target

Version 1.0
07/10/2008

Prepared for:
Foundry Networks, Inc.

4980 Great America Parkway
Santa Clara, CA 95054

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers provided by Foundry Networks, Inc.. Each switch and router includes a hardware appliance running a version of Foundry Networks' proprietary IronWare Operating System (IOS) and the software-based IronShield Security Module. Each switch and router appliance is designed to manage the flow of network information.

A summary of the IronShield Switch and Router security functions can be found in Section 2, TOE Description and a detailed description of the IronShield Switch security functions can be found in Section 6, TOE Summary Specification.

The Security Target contains the following additional sections:

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

1.1 Security Target, TOE and CC Identification

ST Title – Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Target

ST Version – Version 1.0

ST Date – 07/10/08

TOE Identification –BigIron (RX family with IronWare OS version 2.5.00b), NetIron (XMR family with IronWare OS version 3.8.00a; MLX family with IronWare OS version 3.8.00a;), and FastIron (SuperX series with IronWare OS version 4.1.00; GS/LS Family with IronWare OS version 4.2.00a; EdgeX family with IronWare OS version 4.1.00; and EdgeSwitch family with IronWare OS version 4.0.00a). *See section 2 for the specific models for each family.*

TOE Developer – Foundry Networks

Evaluation Sponsor – Foundry Networks

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

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 2.3, August 2005.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.

- Part 3 Conformant
- Assurance Level: EAL 2 augmented with ALC_FLR.1
- Strength of Function Claim: SOF-basic

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- 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_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.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***]). Note that there is the possibility of an assignment within a selection. In that case the operation would be identified as follows: [***[selected-assignment]***].
  - 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 …").
  - Extension: allows the creation of an explicit requirement not defined in the CC. Explicit CC extensions are indicated using the suffix '_EX' in the symbol representing the requirement.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Unauthorized User	An entity that interacts with the TOE Security Function (TSF) in a benign or malicious manner.
Authorized Administrator	A role with which a human user is associated to administer both the functionality and security parameters of the TOE and the IT Environment. Such users are trusted not to compromise the security policy enforced by the TOE.
Human user	Any person who interacts with the TOE.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and 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.

Authentication data	Information used to verify the claimed identity of a user.
Object	An entity within the TOE Security Function (TSF) Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.
Subject	An entity within the TSC that causes operations to be performed.
Authorized User	A user who may, in accordance with the TOE Security Policy (TSP), perform an operation.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.

1.3.3 Acronyms

ACL	Access Control List
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CLI	Command Line Interface
EAL	Evaluation Assurance Level
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FSP	Functional Specification
HLD	High Level Design
IOS	IronWare™ operating system
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
MOF	Management of Functions
MTD	Management of TSF Data
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TACACS	Terminal Access Controller Access Control System
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

2. TOE Description

The Target of Evaluation (TOE) is Foundry Networks IronShield Switches and Routers which consists of the following product families and their associated models:

- BigIron
  - RX family with IronWare OS version 2.5.00b
    - BI-RX-4-AC (4 slot device)
    - BI-RX-8-AC (8 slot device)
    - BI-RX-16-AC (16 slot device)
    - BI-RX-32-AC (32 slot device)
- NetIron
  - XMR family with IronWare OS version 3.8.00a
    - NI-XMR-4-AC (4 slot device)
    - NI-XMR-8-AC (8 slot device)
    - NI-XMR-16-AC (16 slot device)
    - NI-XMR-32-AC (32 slot device)
  - MLX family with IronWare OS version 3.8.00a
    - NI-MLX-4-AC (4 slot device)
    - NI-MLX-8-AC (8 slot device)
    - NI-MLX-16-AC (16 slot device)
    - NI-MLX-32-AC (32 slot device)
- FastIron
  - SuperX series with IronWare OS version 4.1.00
    - FI-SX1-AC – (8 slot device with single management)
    - FI-SX800-AC – (8 slot device with redundant management)
    - FI-SX1600-AC – (16 slot device with redundant management)
  - GS/LS Family with IronWare OS version 4.2.00a
    - FLS624 (24 port stackable)
    - FLS648 (48 port stackable)
    - FGS624P (24 port stackable)
    - FGS624P-POE (24 port stackable with Power over Ethernet)
    - FGS624XGP (24 port stackable with integrated 10 Gig Interface)
    - FGS624XGP-POE (24 port stackable with integrated 10 Gig Interface with Power over Ethernet)
    - FGS648P (48 port stackable)
    - FGS648P-POE (48 port stackable with Power over Ethernet)
  - Edge X family with IronWare OS version 4.1.00
    - FESX424 (24 port stackable)
    - FESX424-PREM (24 port stackable with full L3 support)
    - FESX424+1XG (24 port stackable with one port 10 Gig Interface)

- FESX424+1XG-PREM (24 port stackable with one port 10 Gig Interface with full L3 support)
- FESX424+2XG (24 port stackable with two port 10 Gig Interface)
- FESX424+2XG-PREM (24 port stackable with two port 10 Gig Interface with full L3 support)
- FESX448 (48 port stackable)
- FESX448-PREM (48 port stackable with full L3 support)
- FESX448+1XG (48 port stackable with one port 10 Gig Interface)
- FESX448+1XG-PREM (48 port stackable with one port 10 Gig Interface with full L3 support)
- FESX448+2XG (48 port stackable with two port 10 Gig Interface)
- FESX448+2XG-PREM (48 port stackable with two port 10 Gig Interface with full L3 support)
- FESX424HF (24 port stackable (100FX/1000X))
- FESX424HF-PREM (24 port stackable (100FX/1000X) with full L3 support)
- FESX424HF+1XG (24 port stackable (100FX/1000X) with one 10 Gig Interface)
- FESX424HF+1XG-PREM (24 port stackable (100FX/1000X) with one 10 Gig Interface with full L3 support)
- FESX424HF+2XG (24 port stackable (100FX/1000X) with two 10 Gig Interface)
- FESX424HF+2XG-PREM (24 port stackable (100FX/1000X) with two 10 Gig Interface with full L3 support)
- FESX424-POE (24 port stackable with Power over Ethernet)
- FESX424-POE+1XG (24 port stackable with one port 10 Gig Interface and Power over Ethernet)
- FESX424-POE+2XG (24 port stackable with two port 10 Gig Interface and Power over Ethernet)
- FESX624 (24 port stackable with hardware based IPv6 support)
- FESX624-PREM (24 port stackable with hardware based IPv6 support and full L3 support)
- FESX624+2XG (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces)
- FESX624+2XG-PREM (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
- FESX648 (48 port stackable with hardware based IPv6 support)
- FESX648-PREM (48 port stackable with hardware based IPv6 support and full L3 support)
- FESX648+2XG (48 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces)
- FESX648+2XG-PREM (48 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
- FESX624HF (24 port stackable with hardware based IPv6 support (100FX/1000X))

        - FESX624HF-PREM (24 port stackable with hardware based IPv6 support and full L3 support (100FX/1000X))
        - FESX624HF+2XG (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces (100FX/1000X))
        - FESX624HF+2XG-PREM (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
    - Edge Switch family with IronWare OS version 4.0.00a)
        - FES2402 (24 port stackable)
        - FES2402-PREM (24 port stackable with full L3 support)
        - FES4802 (48 port stackable)
        - FES4802-PREM (48 port stackable with full L3 support)
        - FES9604 (96 port stackable)
        - FES9604-PREM (96 port stackable with full L3 support)
        - FES12GCF (12 port stackable)
        - FES12GCF-PREM (12 port stackable with full L3 support)
        - FES2402-POE (24 port stackable with Power over Ethernet)
        - FES2402-POE-PREM (24 port stackable with full L3 support and Power over Ethernet)
        - FES4802-POE (48 port stackable with Power over Ethernet)
        - FES4802-POE-PREM (48 port stackable with full L3 support and Power over Ethernet)

2.1 TOE Overview

The TOE is composed of a hardware appliance with embedded software installed on the management processor of all routers and switches. The hardware appliance is either a switch or a router and its software is a version of Foundry Networks' proprietary IronWare Operating System (IOS) and the software-based IronShield Security Module. The Foundry IOS controls the switching and routing of layer 2-3 and layer 4-7 network frames and packets through Foundry switch and router appliances.

All switches and routers are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI)[1]. However, the product should be configured in accordance with the evaluated configuration prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH.

The TOE consists of the following product families of switches and routers:

- FastIron (Layer 2-3 Switches)
- NetIron (IPv4/IPv6 and Multiprotocol Label Switching (MPLS)Routers)
- BigIron (Layer 3 Switches)

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations

[1] Note that while the product can be configured to be accessible via a Web Management Interface, this interface is disabled in the evaluated configuration since it is accessible only via insecure HTTP.

- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

The basic operation of the switches and routers is as follows:

1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.

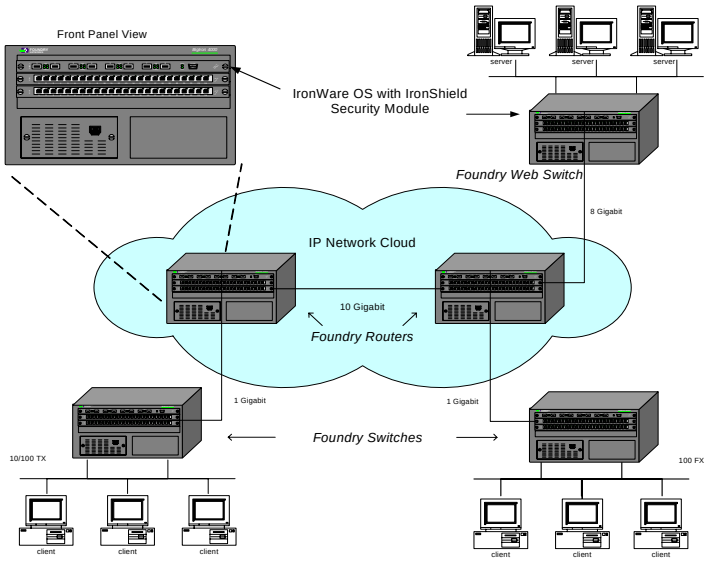

Figure 1: TOE Overview

2.2 TOE Architecture

The basic architecture of each IronShield Switch or Router begins with a hardware appliance with physical network connections. Within the hardware appliance the Foundry Networks proprietary operation system, IronWare Operating System, is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). Within IOS, the IronShield Security Module executes to enforce applicable security policies on network information flowing through the hardware appliance.

2.2.1 Physical Boundaries

Each Ironshield Switch or Router from one of the Ironshield product families (BigIron, NetIron, and FastIron) is a hardware appliance that runs a version of Foundry Networks' IronWare Operating System (IOS) and the software-based IronShield Security Module.

In addition, each IronShield Switch or Router has physical network connections to its environment to facilitate routing and switching of network traffic and can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to a syslog server in the environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can also be configured to use an external authentication service such as a RADIUS or TACACS/TACACS+ using an external server in the environment. In either case, the network traffic coming into or going out of the TOE at those physical interfaces is subject to the security policies which represent logical interfaces as summarized below in Section 2.2.2. .

2.2.2 Logical Boundaries

The TOE logical boundary consists of the security functionality of IronShield Switch or Router summarized below.

Note that the following features, normally available within the product, are excluded or are limited in the evaluated TOE:

1. SNMP is assumed to be **disabled** in the evaluated configuration.
2. Web Management Access is assumed to be **disabled** in the evaluated configuration.
3. Telnet access is assumed to be used only for local, wired connections (i.e., it is assumed to be **disabled** for remote/network access to the TOE).
4. *Strict Password Enforcement* is assumed to be **enabled** in the evaluated configuration.

The following security-related features of the product can be freely used but have not been subject to specific evaluation claims. This means that the product has been evaluated with these features enabled and while these features do not interfere with any claims made in this Security Target, it was not determined whether these features operate correctly. Note that this is true of all the non-security rel;ated features of the product as well.

1. There are no specific claims regarding the MAC Authentication feature which serves to limit access to a network based on a host MAC address.
2. There are no specific claims regarding the 802.1x Authentication feature which serves to limit access to a network based on user 802.1x compatible credentials.
3. There are no specific claims regarding the BGP (Border Gateway Protocol) Guard feature which protects the network routing topology by limiting the number of router hops that a BGP session can traverse.

2.2.2.1 Security audit

The TOE has the ability to generate syslog-based audit log entries for attempts to log into the TOE, management of user accounts and passwords, and management of access control rules. The resulting logs are protected within the TOE and are accessible by authorized TOE users. The logs can also be made available outside the TOE by configuring specific external syslogd servers to receive a copy of the audit records.

2.2.2.2 User data protection

The TOE has the ability for the Authorized Administrators to specify the information flow control security functional policy used to control the flow of user data across the ports of the device. ACLs are used by Foundry to control forwarding of network data at specified ports on network equipment. There are two types of ACLs that can be configured, standard and extended. Standard ACLs permit or deny packets based on source IP address only. Extended ACLs take more factors into consideration including IP protocol information.

2.2.2.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes...

The TOE also provides the Authorized Administrator with the ability to configure Authentication Method lists. These lists are used to specify the order in which the authentication methods are employed whenever there are one or more authentication methods available. Authentication methods include external authentication using such mechanisms as RADIUS and TACACS/TACACS+ provided by an external server in the IT environment of the TOE.

2.2.2.4 Security management

The TOE includes a number of command-line functions to manage its security policies. These functions can be accessed using the Command Line Interface (CLI) (via a directly connected terminal or a remote SSH session). The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

2.2.2.5 Protection of the TSF

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE. Note that the TOE implements its own clock to provide time for its audit records.

The TOE includes the ability to communicate with syslog, TACACS/TACACS+, and RADIUS servers in its environment to access their corresponding services. The TOE is designed to interact with each of those servers in accordance with their respective protocols, including security capabilities where applicable.

2.2.2.6 Trusted path/channels

The TOE provides and requires use of a version of secure shell (SSH version 2) for remote administration of the TOE. This ensures that a secure communication path between the TOE and remote users is provided in order to protect communicated data from modification or disclosure. If the negotiation of an SSH session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

2.3 TOE Documentation

Foundry has a number of administration and configuration guides for the TOE. These documents and others are enumerated in section 6.2.

3. Security Environment

The following subsections describe the threats countered by the TOE and assumptions about the environment of the TOE. Note that the threat statements are objective in nature and do not attempt to qualify subjective aspects, such as resources that might be available to an attacker. The intention is that the TOE mitigates those threats to a degree commensurate with the claimed assurance target, EAL 2 augmented with ALC_FLR.1.

3.1 Threats

T.ACCESS	An attacker may attempt to access the TOE through an external interface in order to alter the TOE configuration or otherwise circumvent the TOE policies so they can access networks/resources for which they are not authorized.
T.AUDIT	Attempts by external entities to violate TOE security policies may not be detected.
T.REMOTE	Through the interception of network traffic, an attacker may attempt to obtain or modify TOE management/administrator secrets and configuration data that is either a parameter of TOE administrative commands, or part of a TOE administrative session, in order to gain access to TOE management functions and/or configuration data for the purpose of circumventing and/or altering TOE security policy.

3.2 Assumptions

A.EAUTH	External authentication services will be available via RADIUS or TACACS/TACACS+.
A.FLOW	The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE.
A.GOODADM	An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.
A.INSTALL	The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.MANAGE	There will be one or more competent Authorized Administrator(s) assigned to manage the TOE and the security functions it performs.
A.PHYSICAL	The TOE will be appropriately located within facilities providing controlled access to prevent unauthorized physical access and to ensure that the TOE controls the applicable information flows.

4. Security Objectives

The following subsections describe objectives for the TOE and its environment that are consistent with the environment described in the previous section.

4.1 Security Objectives for the TOE

O.ADMIN The TOE must provide functions to enable Authorized Administrators to effectively manage and maintain the TOE and its security functions in accordance with site-specific policy, ensuring that only they can access administrative functionality.

O.AUDIT The TOE must provide the capability to audit security-relevant events.

O.AUTH The TOE must ensure that users are appropriately identified and authenticated in order to access protected security functions.

O.INFOFLOW The TOE must provide the ability for the Authorized Administrator(s) to create and maintain network traffic flow control configuration that will be enforced by the TOE.

O.PROTECT The TOE must protect itself from attempts to tamper with or bypass the security policies implemented by the TOE.

O.REMOTE The TOE must provide a mechanism to protect remote administration sessions from inappropriate disclosure and modification.

4.2 Security Objectives for the Environment

OE.EAUTH A RADIUS or TACACS/TACACS+ server must be available for external authentication services when the TOE is configured to use these mechanisms for authentication.

OE.FLOW The network infrastructure in which the TOE is placed must be installed, administered and operated in a manner that ensures all information to be controlled flows through the TOE.

OE.GOODADM Authorized Administrators must not be careless, willfully negligent, nor hostile, and must follow and abide by the instructions provided by the Administrator documentation.

OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.MANAGE One or more competent Authorized Administrator(s) must be assigned to manage the TOE and the security functions it performs.

OE.PHYSICAL Those responsible for the TOE will locate it within facilities providing controlled access to prevent unauthorized physical access and to ensure that it controls the applicable information flows.

5. IT Security Requirements

This section defines the security functional requirements satisfied by the TOE and security assurance requirements levying against the TOE in an evaluation. With a couple exceptions the requirements have been drawn from the common criteria.

Note that FIA_UAU.1 is the only security functional requirement that is subject to the SOF claim of SOF-basic.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by IronShield (BigIron, NetIron, and FastIron) Switches and Routers.

Requirement Class	Requirement Component
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FDP: User data protection	FDP_IFC.2: Complete information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps
FTP: Trusted path/channels	FTP_TRP.1: Trusted path

Table 1 CC TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**TOE users**] with the capability to read [**all information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.2 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.1.2 User data protection (FDP)

5.1.2.1 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the [**Information Flow Policy**] on [

a) subjects: external IT entities that send information through the TOE and

b) information: network traffic sent through the TOE from one subject to another] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Information Flow Policy**] based on the following types of subject and information security attributes: [**subject attributes: source IP address, source TCP or UDP port; information attributes: source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port and TOE attributes: Access Control Lists (ACLs)**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) If Standard ACLs are configured - the source IP address is in the Management module's ACL list, as specified in the configuration file, with a permit statement.

b) If Extended ACLs are configured:

1) The source and destination IP address are defined in the Management module's ACL list, as specified in the configuration file, with a permit statement; and/or

2) The source and destination TCP or UDP port information is/are defined in the Management module's ACL list, as specified in the configuration file, with a permit statement].

FDP_IFF.1.3 The TSF shall enforce the [**following: no additional information control rules**].

FDP_IFF.1.4 The TSF shall provide the following [**: no additional capabilities**].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [**no explicit authorisation rules**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**no explicit denial rules**].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user name, authentication data, and role**].

5.1.3.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**information to flow in accordance with the Information Flow Policy**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**information to flow in accordance with the Information Flow Policy**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Information Flow Policy**] to restrict the ability to [***query, modify***] the security attributes [**ACLs**] to [**Authorized Administrator with Super User privilege**].

5.1.4.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Information Flow Policy**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Authorized Administrator with Super User privilege**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query, modify***] the [**audit trail configuration, user and administrator attributes, authentication method list**] to [**the Authorized Administrator with Super User privilege**].

5.1.4.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**manage (in accordance with the other SFRs):**

- **the audit trail**
- **the information flow policy ACLs;**
- **user and administrator accounts and associated attributes;**
- **the security management roles**].

5.1.4.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**TOE User and Authorized Administrator with Super User privilege**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

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

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 TSF domain separation (FPT_SEP.1)

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.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.3 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Trusted path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***[remote administration of the TOE]***].

5.2 Explicitly Stated TOE Security Functional Requirements

The following table describes the explicitly stated SFRs that are satisfied by the security functionality of Foundry Networks IronShield Switches and Routers.

Requirement Class	Requirement Component
FAU: Security audit	FAU_LOG_EX.1: Syslog generation
FIA: Identification and authentication	FIA_MTH_EX.1: Authentication Method Lists

Table 2 Explicitly Stated TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Syslog generation (FAU_LOG_EX.1)

FAU_LOG_EX.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) the success and failure login of the user, regardless of the authentication mechanism;
b) changing a user's password;
c) adding and deleting user accounts; and,
d) modification, addition and deletion of ACLs.

FAU_LOG_EX.1.2 The TSF shall record within each audit record at least the following information: date and time of the event, type of event, subject identity, and the outcome of the event.

5.2.2 Identification and authentication (FIA)

5.2.2.1 Authentication Method Lists (FIA_MTH_EX.1)

FIA_MTH_EX.1.1 The TSF shall provide a mechanism to allow Authorized Administrator(s) to specify the order by which one or more authentication methods will be tried by the switch or router device.

FIA_MTH_EX.1.2 The TSF Authentication Method list will process authentication methods based on the following rules:
a) If the authentication method is available, access is granted if the authentication information is correct, otherwise, access is denied and the processing stops;
b) If an error occurs (because the authentication method is unavailable) with an authentication method, processing continues with the next method;
c) If all authentication methods are exhausted without success or failure (i.e., they all have errors) access is denied unless the user has Administrator with Super User privilege and successfully logs on using their Super User password.

5.3 IT Environment Security Functional Requirements

The following table describes the SFRs that are satisfied by the IT environment of Foundry Networks IronShield Switches and Routers.

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_UAU.5: Multiple Authentication Mechanisms

Table 3 IT Environment Security Functional Components

5.3.1 Identification and authentication (FIA)

5.3.1.1 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The **IT environment** ~~TSF~~ shall provide **[external server (RADIUS or TACACS/TACACS+) mechanisms]** to support user authentication.

FIA_UAU.5.2 The **IT environment** ~~TSF~~ shall authenticate any user's claimed identity according to the **[authentication mechanism specified by an authorized administrator].**

5.4 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_FLR.1: Basic flaw remediation
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4 EAL 2 augmented with ALC_FLR.1 Assurance Components

5.4.1 Configuration management (ACM)

5.4.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 Delivery and operation (ADO)

5.4.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.3 Development (ADV)

5.4.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

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.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4 Guidance documents (AGD)

5.4.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
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.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
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.
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 behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5 Life cycle support (ALC)

5.4.5.1 Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.1.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.1.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6 Tests (ATE)

5.4.6.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

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.

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.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

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.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.7 Vulnerability assessment (AVA)

5.4.7.1 Strength of TOE security function evaluation (AVA_SOF.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.

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.

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.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.4.7.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE is designed to produce syslog conformant messages in a number of circumstances including warnings about the device itself (such as temperature, power failures, etc.) as well as security relevant events (the success and failure login of the user, regardless of the authentication mechanism; changing a user's password; adding and deleting user accounts; and, modification, addition and deletion of ACLs). In each case the audit record includes the time and date, identification of the responsible subject, the type of event, the outcome of the event, and other information depending on the event type.

The audit records are stored in a log that is protected so that only an authorized TOE user can read (for which tools are provided) or otherwise access them. The log stores up to 50 entries after which the audit entries will be overwritten. The administrator (with Super User privilege) can (and should) choose to configure an external syslogd server where the TOE will send a copy of the audit records if so desired. However, that capability extends beyond the scope of evaluation.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_LOG_EX.1: The TOE generates the applicable audit records with the required content.
- FAU_SAR.1: The TOE provides the TOE users with tools that can be used to review all of the audit data.
- FAU_STG.1: The TOE protects the audit data from everyone except the authorized TOE users.

6.1.2 User data protection

The TOE has the ability to control the flow of all network data across the external interfaces (i.e., network ports) of the appliance. Access Control Lists are used by the TOE to control forwarding of network data at specified ports on network equipment. There are two types of ACLs that can be configured by the Authorized Administrator with Super User privilege, 'Standard' and 'Extended.'

- 'Standard' ACLs permit or deny packets based on source IP address only. Essentially, the TOE supports the specification of source addresses that are allowed to send information through the TOE.
- 'Extended' ACLs filter based on: Source IP address; Destination IP address; Source TCP or UDP port for TCP/IP traffic; and, Destination TCP or UDP port for TCP/IP traffic. In this case the rules are much more flexible since the TOE allows essentially any combination of source and destination addresses as well as source and destination ports to specify which information flows will be allowed.

In each case, the ordering of the rules in an ACL is important because the first match is executed without consideration of subsequent rules that might be in the list.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.2: The TOE enforces an information flow policy on all network traffic flowing among its external interfaces.
- FDP_IFF.1: The TOE enforces a specific set of rules that define how information is allowed to flow among external subjects.

6.1.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE. The TOE authenticates users against their user name, password and privilege level. However, the information is allowed to flow through the TOE without identification or authentication so long as it conforms to the information flow policy rules.

The Authorized Administrator with Super User privilege is able to define local user accounts and to assign passwords and privilege levels to the accounts. Each user account has a user name, password, and a privilege level associated with it. The default privilege level accounts predate the notion of users and there is one such account associated with each privilege level and each has its own password. It is up to the Authorized Administrator with Super User privilege to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level.

While the Authorized Administrator with Super User privilege can create or otherwise modify accounts freely, other users cannot change their own (or any other) security attributes. Note that the TOE supports a strict password enforcement configuration where the minimum password length is set to 8 characters and the value cannot be reset to a lower value. Also, the TOE can also be configured to lock accounts after a pre-configured number of failed logon attempts. These functions are also restricted to the Authorized Administrator with Super User privilege.

Alternative authentication mechanisms can also be configured by an Authorized Administrator using an Authentication Method List. This allows some flexibility in setting up authentication mechanisms when desired. The available mechanisms include the Local Password for the Super User Privilege level, Local User Accounts configured on the device as well as the external mechanisms Terminal Access Controller Access Control System (TACACS/TACACS+) and Remote Authentication Dial In User Service (RADIUS.) The use of the TACACS/TACACS+ and RADIUS mechanisms requires a RADIUS or TACACS/TACACS+ server in the IT environment of the TOE.

The Authentication Method List is ordered so that it will be processed from first to last. In each case, the user authentication will succeed, fail, or result in an error. Only in the case of an error (e.g., an external server is unavailable) will processing proceed to the next authentication method in the list. If a given authentication method succeeds, the user will be logged in and will be able to perform functions according to their privilege level. If a given authentication mechanism fails, the user will be denied a login session. If the point is reached where every authentication method on the list fails, only an authorized administrator with Super User privilege whose Super User password is not rejected will succeed in logging in to the system.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE associates user names, passwords, and privileges with each user account.
- FIA_MTH_EX.1: The TOE provides the Authorized Administrator with Super User privilege with the ability to configure an order authentication method list.
- FIA_UAU.1: The TOE requires users to be authenticated, except for information flows subject to the information flow policy.
- FIA_UAU.5: The TOE provides external mechanisms which are used to authenticate any user's claimed identity.
- FIA_UID.1: The TOE requires users to be authenticated, except for information flows subject to the information flow policy.

6.1.4 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Super User (with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as users or TOE users). The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on those privilege levels. In this manner, the TOE is able to ensure that only the Authorized Administrator with Super User privilege can access audit configuration data, information flow policy ACLs, user and administrator security attributes, and authentication method lists.

As indicated above only an Authorized Administrator with Super User privilege can modify the information flow policy ACLs and only they can change the default permissions associated with that policy which are initially permissive in nature (i.e., the TOE does not restrict information flows by default).

The TOE offers command line functions which are accessible via the CLI. The CLI is a text based interface which can be accessed from a directly connected terminal or via a remote terminal using SSH. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: The TOE restricts the ability to manage the information flow ACLs to the Authorized Administrator with Super User privilege.
- FMT_MSA.3: The TOE initially provides permissive default values for the information flow policy and restricts the ability to change the defaults to the Authorized Administrator with Super User privilege.
- FMT_MTD.1: The TOE restricts the ability to manage (query/modify) the TOE configuration data associated with each of the security functions to the Authorized Administrator with Super User privilege, with the exception of passwords.
- FMT_SMF.1: The TOE provides a complete set of command line functions for the effective management of the TOE security functions.
- FMT_SMR.1: The TOE realizes the single security role Authorized Administrator with Super User privilege as any user with Super User privilege.

6.1.5 Protection of the TSF

The TOE is a stand-alone appliance that is designed to offer limited and controlled functions at its interfaces. In particular, these interfaces are designed so that functions are not offered that can be used to tamper with or bypass the TOE security policy enforcing mechanisms. Users must authenticate at these interfaces before any administrative functions can be performed on the system, whether those functions are related to the management of user accounts or the configuration of traffic flows. Additionally, all administration and configuration operations are performed within the physical boundary of the TOE.

In addition, the TOE includes a hardware clock that is used to provide reliable time information for the audit records it generates. The TOE can be configured to periodically synchronize its clock with a timer server, but the TOE can only ensure its own reliability and not that of an external time mechanism.

Note that the TOE can be configured to interact with servers in the IT environment (i.e., syslog, RADIUS, TACACS/TACACS+). The TOE is designed to communicate correctly with those servers in accordance with their respective protocols. As such, while it does not detract from the security available in the IT environment it also does not enhance the security or any limitations thereto resulting from the use of such servers. It is left to the TOE users to decide whether the use of such servers and any security mechanisms available in or surrounding those servers is appropriate for their environment.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: The TOE is designed to ensure its policies are always enforced.
- FPT_SEP.1: The TOE is designed to prevent tampering attempts.
- FPT_STM.1: The TOE implements its own internal clock mechanism.

6.1.6 Trusted path/channels

The TOE implements SSH which is required to be used for remote administration. When an administrator attempts to connect to the TOE, the TOE attempts to negotiate a SSH session. If the session cannot be negotiated, the

connection is dropped. Furthermore, even when a session can be negotiated, the TOE then checks to ensure the user is authorized for remote administration and if not the session is dropped.

The TOE includes an implementation of version 2 of SSH with the AES, DES, 3DES, RC4, and Blowfish algorithms for encryption and with MD5 or SHA-1 for MAC. When a client attempts to connect using SSH, the TOE and the client will negotiate the most secure algorithms available at each end to protect that session.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1: The TOE requires the successful establishment of a SSH session for remote administration.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Foundry Networks ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Foundry Networks performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, delivery and operation, vulnerability assessment and the CM documentation.

These activities are documented in:

- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers Configuration Management Plan (CMP)*
- *Common Criteria Configuration Item List*
- *Foundry Networks Production and Manufacturing Process*
- *Common Criteria Software Release and Quality Assurance Process*

The Configuration management assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Foundry Networks provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Foundry Networks's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Foundry Networks also provides documentation that describes the steps necessary to install IronShield (BigIron, NetIron, and FastIron) Switches and Routers in accordance with the evaluated configuration.

These activities are documented in:

- *Foundry Product Order and Delivery Process, version 1.1, 04/26/2006*
- *Foundry BigIron RX Series Installation Guide, March 2008*
- *Foundry BigIron RX Series Configuration Guide, June 2008*
- *Foundry Switch and Router Installation and Basic Configuration Guide, December 2007*
- *Foundry FastIron Compact Switch Hardware Installation Guide, December 2007*
- *Foundry FastIron Configuration Guide, June 25 2008*
- *Foundry FastIron GS Compact Layer 2 Switch POE and POE-Upgradeable Hardware Installation Guide, December 2007*
- *Foundry FastIron LS Layer 2 Compact Switch Hardware Installation Guide, December 2007*
- *Foundry FastIron X Series Chassis Hardware Installation Guide, November 2007*
- *Foundry FastIron Compact Switch Hardware Installation Guide, December 2007*
- *Foundry NetIron MLX Series Installation and Basic Configuration Guide, December 2007*
- *Foundry NetIron XMR Series Installation and Basic Configuration Guide, December 2007*
- *Foundry NetIron XMR/MLX Configuration Guide, April 2008*

The Delivery and operation assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Foundry Networks has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE (including details of security effects, exceptions and error messages), its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- *Foundry Switch and Router Command Line Interface Reference*
- *Foundry Security Guide*
- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers Security Module Architecture*
- *BigIron RX Architecture (white paper)*
- *FastIron SuperX Architecture (white paper)*
- *FES High Level Architecture*
- *Next Generation Terabit System Architecture, The High Performance Revolution for 10 Gigabit Networks*
- *ServerIron 450/850, GT-E Architecture Technical Brief*
- *NetIron XMR Series Router Architecture*
- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers High-level Design/Functional Specification Correspondence*
- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers High-level Design/Functional Specification Correspondence*
- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers Interface Correspondence*

The Development assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Foundry Networks provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- *Foundry Switch and Router Command Line Interface Reference, December 2007*

- *Foundry Security Guide, December 2007*

The Guidance documents assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Foundry Networks has procedures that define the process for accepting and acting upon user reports of security flaws. These procedures describe the acceptance criteria for security flaws and how all security flaws and the status of fixes for each security flaw are tracked.

These activities are documented in:

- *Foundry Networks IronShield (ServerIron, BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers Flaw Remediation*

The Life cycle support assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- ALC_FLR.1

6.2.6 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- *Foundry Networks Incorporate Common Criteria testing Test Plan,*
- *Foundry Networks, Incorporated Common Criteria (CC) Testing Test Results*

The Tests assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

Foundry Networks has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

Foundry Networks performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

The vulnerability analysis activities are documented in:

- *Foundry Networks IronShield Family of Switches and Routers Vulnerability Analysis Report*

As for strength of functions, the only applicable mechanism is authentication using passwords configured in the TOE. In the evaluated configuration strict password enforcement is required which imposes as a minimum: a

minimum password length of 8; a useable password alphabet of 94 characters; and a restriction requiring at least 2 each upper case alphabetic characters, lower case alphabetic characters, numbers, and special characters. As such, there are at least 26^2 * 26^2 * 10^2 * 32^2 = 46,794,342,400 possible passwords. Assuming on average an attacker would have to guess half the passwords in order to successfully log in, within a month the attacker would be required to make 46,794,342,400/2/30/24/60/60[2] = ~9026 attempts per second. Even to successfully log in within a year the attacker would be required to make 9026*30/365 = ~742 attempts per second. Even assuming an automated capability it is not possible for the device to answer thousands of authentication attempts to its management interfaces in a second. Furthermore, while no specific settings are required, the TOE can be configured to lock accounts upon a pre-determined number of failed logon attempts this would serve to make it essentially impossible to guess a password. Given this, the TOE seems to readily fulfill the expectations of SOF-basic.

The Vulnerability assessment assurance measure satisfies the following EAL 2 augmented with ALC_FLR.1 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

[2] possible passwords / 2 for average attempts / 30 days in a month / 24 hours in a day / 60 minutes in an hour / 60 seconds in a minute

7. Protection Profile Claims

This security target does not claim conformance with any protection profile. Note that while there are protection profiles for Firewalls, at the time this Security Target was developed there were no validated protection profiles for routers or switches.

8. Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of usage assumptions and threats by the security objectives.

	T.ACCESS	T.AUDIT	T.REMOTE	A.EAUTH	A.FLOW	A.GOODADM	A.INSTALL	A.MANAGE	A.PHYSICAL
O.ADMIN	X								
O.AUDIT		X							
O.AUTH	X								
O.INFOFLOW	X								
O.PROTECT	X								
O.REMOTE			X						
O.EAUTH				X					
OE.FLOW					X				
OE.GOODADM						X			
OE.INSTALL							X		
OE.MANAGE								X	
OE.PHYSICAL									X

Table 5 Environment to Objective Correspondence

8.1.1.1 T.ACCESS

An attacker may attempt to access the TOE through an external interface in order to alter the TOE configuration or otherwise circumvent the TOE policies so they can access networks/resources for which they are not authorized.

This Threat is satisfied by ensuring that:

- O.ADMIN: This objective helps counter this threat by ensuring that administrators have the functions they need and those functions are protected.
- O.AUTH: This objective helps counter this threat by ensuring that users are identified and authenticated appropriately in order to access protected TOE functions.
- O.INFOFLOW: This objective helps counter this threat by ensuring administrators can configure the information flow policies and those policies are enforced.
- O.PROTECT: This objective helps counter this threat by ensuring that the TOE protects itself from tampering and bypass of security policies.

8.1.1.2 T.AUDIT

Attempts by external entities to violate TOE security policies may not be detected.

This Threat is satisfied by ensuring that:

- O.AUDIT: This objective counters this threat by ensuring that the TOE will provide the ability to audit security-relevant events.

8.1.1.3 T.REMOTE

Through the interception of network traffic, an attacker may attempt to obtain or modify TOE management/administrator secrets and configuration data that is either a parameter of TOE administrative commands, or part of a TOE administrative session, in order to gain access to TOE management functions and/or configuration data for the purpose of circumventing and/or altering TOE security policy.

This Threat is satisfied by ensuring that:

- O.REMOTE: This objective counters this threat by ensuring that remote administration sessions are protected from disclosure or modification.

8.1.1.4 A.EAUTH

External authentication services will be available via RADIUS and TACACS/TACACS+.

This Assumption is satisfied by ensuring that:

- OE.EAUTH: This objective directly corresponds with this assumption.

8.1.1.5 A.FLOW

The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE.

This Assumption is satisfied by ensuring that:

- OE.FLOW: This objective directly corresponds with this assumption.

8.1.1.6 A.GOODADM

An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.

This Assumption is satisfied by ensuring that:

- OE.GOODADM: This objective directly corresponds with the assumption.

8.1.1.7 A.INSTALL

The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: This objective directly corresponds with the assumption.

8.1.1.8 A.MANAGE

There will be one or more competent Authorized Administrator(s) assigned to manage the TOE and the security functions it performs.

This Assumption is satisfied by ensuring that:

- OE.MANAGE: This objective directly corresponds with the assumption.

8.1.1.9 A.PHYSICAL

The TOE will be appropriately located within facilities providing controlled access to prevent unauthorized physical access and to ensure that the TOE controls the applicable information flows.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: This objective directly corresponds with the assumption.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 6** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ADMIN	O.AUDIT	O.AUTH	O.INFOFLOW	O.PROTECT	O.REMOTE	OE.AUTH
FAU_LOG_EX.1		X					
FAU_SAR.1		X					
FAU_STG.1		X					
FDP_IFC.2				X			
FDP_IFF.1				X			
FIA_ATD.1			X				
FIA_MTH_EX.1			X				
FIA_UAU.1			X				
FIA_UAU.5							X
FIA_UID.1			X				
FMT_MSA.1	X			X			
FMT_MSA.3	X			X			
FMT_MTD.1	X	X	X				
FMT_SMF.1	X		X				
FMT_SMR.1	X						
FPT_RVM.1					X		

	O.ADMIN	O.AUDIT	O.AUTH	O.INFOFLOW	O.PROTECT	O.REMOTE	OE.AUTH
FPT_SEP.1					X		
FPT_STM.1		X					
FTP_TRP.1						X	X

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.ADMIN

The TOE must provide functions to enable Authorized Administrators to effectively manage and maintain the TOE and its security functions in accordance with site-specific policy, ensuring that only they can access administrative functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1: This requirement helps address this objective by enforcing the Information Flow Policy to restrict the ability to query and modify the ACLs to an authorized administrator with Super User privilege.
- FMT_MSA.3: This requirement helps address this objective by allowing an authorized administrator with Super User privilege to specify alternative initial values ot override the default values when an object or information is created.
- FMT_MTD.1: This requirement helps address this objective by restricting the ability to query and modify the audit trail configuration, administrator and user attributes and the authentication method list to an authorized administrator with Super User privilege.
- FMT_SMF.1: This requirement helps address this objective by ensuring that the authorized administrator has the functions necessary for effective management of the TOE security functions.
- FMT_SMR.1: This requirement helps address this objective by ensuring that the TOE implements an appropriate user and authorized administrator role.

8.2.1.2 O.AUDIT

The TOE must provide the capability to audit security-relevant events.

This TOE Security Objective is satisfied by ensuring that:

- FAU_LOG_EX.1: This requirement helps address this objective by requiring that the appropriate security-relevant events are audited.
- FAU_SAR.1: This requirement helps address this objective by ensuring that TOE users have the ability to review the audit records.
- FAU_STG.1: This requirement helps address this objective by ensuring that audit records are appropriately protected.
- FMT_MTD.1: This requirement helps address this objective by ensuring that audit data is appropriately protected.
- FPT_STM.1: This requirement helps address this objective by ensuring that the TOE has reliable time stamps to associate with audit records.

8.2.1.3 O.AUTH

The TOE must ensure that users are appropriately identified and authenticated in order to access protected security functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: This requirement helps address this objective by ensuring that the necessary security attributes are associated with user accounts.
- FIA_MTH_EX.1: This requirement helps address this objective by allowing an administrator to configure an order list of alternative authentication mechanisms to ensure that users are authenticated in an acceptable manner.
- FIA_UAU.1: This requirement helps address this objective by ensuring that users are authenticated when necessary. Note that authentication is not required in the case of traffic subject to the information flow policy..
- FIA_UID.1: This requirement helps address this objective by ensuring that users are always identified, though traffic subject to the information flow policy does not require identification.
- FMT_MTD.1: This requirement helps address this objective by ensuring that user attributes are appropriately protected.
- FMT_SMF.1: This requirement helps address this objective by ensuring that administrators can effectively manage user and administrator accounts.

8.2.1.4 O.INFOFLOW

The TOE must provide the ability for the Authorized Administrator(s) to create and maintain network traffic flow control configuration that will be enforced by the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: The requirement helps address this objective by ensuring that inter-subject communication is appropriately controlled.
- FDP_IFF.1: The requirement helps address this objective by ensuring that appropriate rules are enforced to control the flow of information among subjects.
- FMT_MSA.1: This requirement helps address this objective by ensuring that information flow policy access control lists are appropriately protected.
- FMT_MSA.3: This requirement helps address this objective by ensuring that the information flow policy has appropriate defaults and that only an authorized administrator can change those defaults.

8.2.1.5 O.PROTECT

The TOE must protect itself from attempts to tamper with or bypass the security policies implemented by the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: This requirement helps address this objective by ensuring that the TOE policies are not bypassable.
- FPT_SEP.1: This requirement helps address this objective by ensuring that the TOE policies are not susceptible to tampering.

8.2.1.6 O.REMOTE

The TOE must provide a mechanism to protect remote administration sessions from inappropriate disclosure and modification.

This TOE Security Objective is satisfied by ensuring that:

- FTP_TRP.1: This requirement addresses this objective by requiring a distinct communication vehicle for remote administration that is protected from disclosure or modification.

8.2.1.7 OE.EAUTH

A RADIUS or TACACS/TACACS+ server must be available for external authentication services when the TOE is configured to use these mechanisms for authentication.

This IT Environment security objective is satisfied by ensuring that:

- FIA_UAU.5: This requirement helps address this objective by providing a RADIUS or TACACS/TACACS+ server to support user authentication and authenticating a user's claimed identity according to whichever mechanism is specified by an authorized administrator.

8.3 Security Assurance Requirements Rationale

This ST has been developed for Foundry Networks' IronShield-based appliances. Each appliance is assumed to be physically protected and the only non-authenticated functions it provides at exposed interfaces are limited in scope. As such, the assurance target, EAL 2 augmented with ALC_FLR.1, is appropriate.

8.4 Strength of Functions Rationale

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats commensurate with the assurance target, EAL 2 augmented with ALC_FLR.1. The SOF-basic claim applies only to the authentication mechanism which is based on user-provided passwords.

8.5 Requirement Dependency Rationale

As can be seen in the table below all of the dependencies defined in the CC are satisfied. Note, however, that FAU_GEN.1 has been effectively replaced with an explicit requirement, FAU_LOG_EX.1 that fulfills the need to generate audit records to be protected and reviewed.

ST Requirement	CC Dependencies	ST Dependencies
FAU_LOG_EX.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_LOG_EX.1
FAU_STG.1	FAU_GEN.1	FAU_LOG_EX.1
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_MTH_EX.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	none	none
FIA_UID.1	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
FTP_TRP.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1

ST Requirement	CC Dependencies	ST Dependencies
ALC_FLR.1	none	none
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

Table 7 Requirement Dependencies

8.6 Explicitly Stated Requirements Rationale

This Security Target defines two explicit requirements.

The first, FAU_LOG_EX.1, is necessary because the CC requirement FAU_GEN.1 requires that start up and shut down of the audit functions must be auditable and offers a selection of an audit level. In this TOE the audit function is somewhat more limited. It is restricted only to Authorized Administrators with Super User privilege, so it is not clear whether auditing the start and stop of the audit function serves and practical purpose. Furthermore, the auditing is limited to the condition of the TOE (e.g., power, heat, etc.) which is not obviously security relevant and to information flow policy violations.

The second, FIA_MTH_EX.1, is necessary to specify the capability to define a ordered list of alternate authentication methods.

In both cases, the requirement specify straight-forward functions, as they exist in the TOE and are subject to evaluation using the entire set of security assurance requirements.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**User data protection**	**Identification and authentication**	**Security management**	**Protection of the TSF**	**Trusted path/channels**
FAU_LOG_EX.1	X					
FAU_SAR.1	X					
FAU_STG.1	X					

	Security audit	User data protection	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels
FDP_IFC.2		X				
FDP_IFF.1		X				
FIA_ATD.1			X			
FIA_MTH_EX.1			X			
FIA_UAU.1			X			
FIA_UAU.5			X			
FIA_UID.1			X			
FMT_MSA.1				X		
FMT_MSA.3				X		
FMT_MTD.1				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_RVM.1					X	
FPT_SEP.1					X	
FPT_STM.1					X	
FTP_TRP.1						X

Table 8 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.