Foundry Networks Management Module IV: J-BxGMR4 and J-FxGMR4

Security Target

Version 1.0

PREPARED BY:

COMPUTER SCIENCES CORPORATION
132 NATIONAL BUSINESS PARKWAY
ANNAPOLIS JUNCTION, MD 20701

PREPARED FOR
Foundry Networks, Inc.
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

`

Proprietary and Confidential

Date	Version	Changes Made
August 30, 2002	0.01	Original Draft
March 13, 2003	0.02	Updated for submission to Scheme.
November 17, 2003	1.00	Revision 1.18 – Updated with changes required from evaluation.
December 4, 2003	1.00	Revision 1.19 – Updated with required changes.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

2 The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets Evaluation Assurance Level (EAL) 2.

ST Title:	Foundry Networks Management Module IV: J-BxGMR4 and J-FxGMR4
ST Version:	1.0
Revision:	$Revision: 1.20 $
Publication Date:	$Date: 2004/01/08 09:17:38 $
Authors:	Computer Sciences Corporation, Common Criteria Testing Laboratory
TOE Identification:	Foundry Networks Management Module IV: J-BxGMR4 and J-FxGMR4
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408)
ST Evaluator:	Computer Sciences Corporation (CSC)
Keywords:	Foundry, Foundry Networks, Router, Switch, BigIron, FastIron, Management Module, JetCore, Ironware OS (IOS), Iron shield, ACLs, MAC Port Locking, User Authentication.

1.2 References

4 The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1, CCIMB-99-031 Annotated with interpretations as of 2002-10-25
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1, CCIMB-99-032 Annotated with interpretations as of 2002-10-25
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1, CCIMB-99-033 Annotated with interpretations as of 2002-10-25
[CEM_PART1]	Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, Version 0.6.
[CEM_PART2]	Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, Version 1.0 Annotated with interpretations as of 2002-10-25

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

6 This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

7 The CC allows several operations to be performed on security functional components; *assignment, refinement*, *selection,* and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

a) The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

b) The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

d) *Iterated* functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

e) Plain *italicized text* is used to emphasize text.

1.3.2 Terminology

8 In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

User	Any entity (human user or external IT entity) outside the TOE that interacts with 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[1]) Scope of Control (TSC[2]) 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[3]), perform an operation.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.

9 The following terminology is specific to this ST.

Unauthorized User	An entity that interacts with the TOE Security Function (TSF) in a benign or malicious manner.

As defined in the CC, Part 1, version 2.1:
1 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.
2 TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
3 TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

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.
Port Security Autosave Feature	A method where by the TOE's physical Ethernet ports will learn and save the Media Access Controller (MAC) address of the host Network Interface Card (NIC) and write it in to the startup configuration file.

1.3.3 Acronyms

10 The following acronyms are used in this Security Target:

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
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
EDR	Evaluation Discovery Report
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

ACRONYM	DEFINITION
ST	Security Target
TACACS+	Terminal Access Controller Access Control System (Plus)
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.4 TOE Overview

11 The TOE, the J-BxGMR4 and J-FxGMR4, is a chassis based management module running Foundry Networks' IronWare™ operating system (IOS), Version 07.6.04f (incorporating Foundry Networks' IronShield™ security module), that is used to manage Foundry Networks' Layer 2 and Layer 3 switch chassis. The J-BxGMR4 is for use with the Foundry BigIron 4000, 8000, and 15000 series chassis, and the J-FxGMR4 is for use with the Foundry FastIron 400, 800, and 1500 series chassis.

12 A summary of the Management module security functions can be found in Section 2, TOE Description. A detailed description of the management module security functions can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance Claim

13 This ST conforms to CC Part 2 extended, and is CC Part 3 conformant at the EAL 2 level of assurance.

2 TOE DESCRIPTION

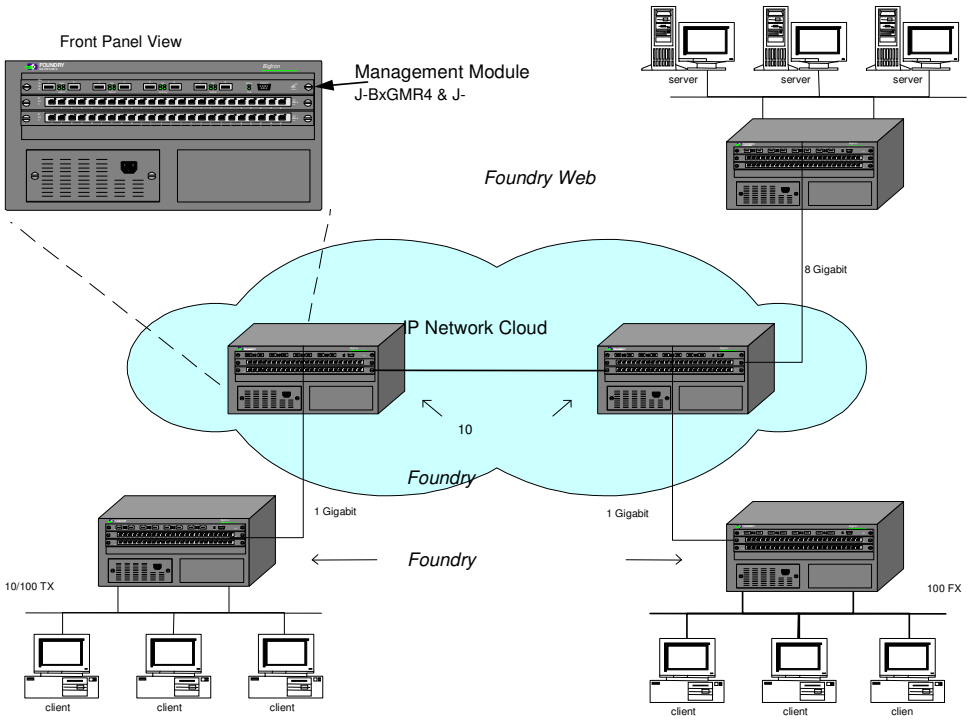
14 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

15 The TOE is a hot-swappable, field replaceable management module in combination with the appropriate Iron Ware software that controls the switching and routing of layer 2/3 frames and packets through Foundry chassis-based switches and routers, and can be employed in a redundant configuration.

Figure 1. J-BxGMR4 Front View (the J-FxGMR4 is visually identical)

Figure 2. Product Application Diagram



Physical Scope and Boundary

16 The TOE is a management module installed within the Foundry Networks' family of chassis-based Layer 2/3 switches. The management module is comprised of the hardware (either the J-BxGMR4 or J-FxGMR4, including a CPU), and Foundry Networks' IronWare 7.6.04f

operating system for MR4s; the difference between the two being that the J-BxGMR4 has twice the on board memory of the J-FxGMR4.

2.1.1 Logical Scope and Boundary

17 The TOE logical boundary consists of the functionality inherent to the management module which provides the following security features:

- User Data protection: TSF_UDP_REMOTE, TSF_UDP_MAC, TSF_UDP_PRIV, TSF_UDP_FLOW;
- Identification and Authentication: TSF_FIA_USERS, TSF_FIA_AUTH;
- Security Management: TSF_FMT; and
- Auditing: TSF_FAU.

18 **User Data Protection (TSF_UDP_REMOTE)** – The Foundry Networks J-BxGMR4 and F-xGMR4 management modules have the capability to specify an access control security functional policy in order to restrict management functions from remote sources (NETWORK_MGMT SFP), including Telnet, the Web management interface, and SNMP. The following methods for restricting remote access are supported:

- Using ACLs to restrict Telnet, Web management interface, or SNMP access
- Allowing remote access only from specific IP addresses
- Allowing remote access only to clients connected to a specific VLAN.
- Disabling the Telnet, Web, or SNMP server if no remote access is required.

19 Access decisions for ACLs are based on entries in the device's configured Access Control List(s) (ACL). Access control parameters include entries specifying the allowed or disallowed source host or network IP address.

20 **User Data Protection (TSF_UDP_MAC)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the capability to specify an access control security functional policy (MAC_PORT_LOCK SFP) in order to lock port-level access to the device through determining if the MAC address of the connecting host and the hardware port through which the connection request is made is in the device's startup configuration file; only the authorized administrator specified MAC address or MAC address that was initially learned using the port security autosave feature will be allowed to connect through the port. Autosave allows the switch to dynamically learn MAC addresses which are connected to ports configured for autosave and write them in to the configuration file. There after only the initially learned address is allowed to connect to the port.

21 **User Data Protection (TSF_UDP_PRIV)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the capability to specify an access control security functional policy in order to limit user access to specific levels of the command line interface (CLI) (PRIVILEGE_LEVEL SFP).

22 **User Data Protection (TSF_UDP_FLOW)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 Management Modules have the ability for the Authorized Administrators to specify the information flow control security functional policy [INFOFLOW SFP] 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.

23 **Identification and Authentication (TSF_FIA_USERS)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules allow the assigning of user names and passwords to control access to the management functions of the device. Additionally, a user definition can contain the management privilege level assigned to that user.

24 **Identification and Authentication (TSF_FIA_AUTH)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules allow the Authorized Administrator 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 defined.

25 **Security Management (TSF_FMT)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules include a number of functions to manage security policy and its implementation. Policy management and implementation are controlled through the use of various ACLs, and several security role definitions/privileges.

26 **Auditing (TSF_FAU)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the ability to generate syslog-based audit log entries for each defined ACL entry. The audit information provided in the audit log includes the information provided in Appendix A.

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage Assumptions

27 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

28 The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/Key Operator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment Assumptions

29 The environmental assumptions delineated in Table 1 are required to ensure the security of the TOE:

Table 1: Environmental Assumptions

Assumption	Description
A.INSTALL	The TOE hardware and software have 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.EXTERNAL_I&A	External Identification and Authentication mechanisms function correctly and accurately.
A.NO_EVIL_ADM	An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.
A.PROCEDURE	Procedures exist for granting Authorized Administrator(s) access to the TSF.
A.PHYSICAL_PROTECT	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.

3.2 Threats

3.2.1 Threats Addressed by the TOE

30 Table 2 identifies the threats to the TOE. The threats to the TOE are considered to be users with public knowledge of how the TOE operates and possess the skills and resources to alter TOE configuration settings/parameters. The threat agents do not have physical access to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 2: Threats Addressed by the TOE

Threat	Description
T.ALTER_CONFIG	An unauthorized user may attempt to access the TOE through an external interface in order to alter the TOE configuration to circumvent the configured policy so they can access networks/resources they for which they are not authorized.

3.2.2 Threats Addressed by the IT Environment

31 There are no threats against which specific protection within the IT Environment is required.

3.3 Organizational Security Policies

32 Table 3 identifies the organizational security policies that are determined to be relevant for the TOE.

Table 3: Organizational security policies

Policy	Description
P.LOCAL_ACCOUNTS	The system will have local accounts, and passwords; the passwords will be encrypted.
P.PRIVILEDGE_LEVELS	The system must have the ability to limit Authorized Administrator(s) management privilege level(s).
P.REMOTE_ACCESS	Management access methods, other than the Serial access to the CLI, will be secured via AAA security methods. Though there may be external methods, there will be a local method. If an external I&A mechanism is utilized, the System will enforce the decision of that mechanism.
P.SYS_CLOCK	The time and date will be set on the Management module's onboard system clock.
P.SYSLOG	The Management module's syslog capability will be enabled and have the local message buffer configured to retain 100 messages.

4 SECURITY OBJECTIVES

33 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

34 This section identifies and describes the security objectives of the TOE.

35 The TOE accomplishes the security objectives defined in Table 4.

Table 4: Security Objectives for the TOE

Objectives	Description
O.ADMIN_USERS	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.SYSLOG_AUDIT	The TOE must provide a syslog auditing capability.
O.DATA_FLOW_CONFIG	The TOE must provide the ability for the Authorized Administrator(s) to create and maintain network traffic flow control configuration in accordance with site-specific policy.
O.PRIVILEGE_LEVELS	The TOE must accommodate separate privilege levels for Authorized Administrators to limit their access to the TOE security mechanisms and configuration.
O.REMOTE_ACCESS	The TOE must provide access methods, for other than serial port access to the CLI, of which one will be local, that will be secured via AAA security methods. Also, must provide the Authorized Administrator(s) configurable ACL(s) to specify the allowed remote management access connections.

4.2 Security Objectives for the Environment

36 Table 5 identifies and specifies the security objectives for the IT Environment.

Table 5: Security Objective for the Environment

Objective	Description
OE.INSTALL	Those responsible for the TOE must ensure that the TOE hardware and software are delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.OPTIONAL_I&A	The TOE environment shall provide, per site specific policy, the specified number, and type, of correct and accurately functioning Identification and Authentication mechanisms that are compatible with, and for external use by, the TOE.
OE.PHYSICAL	Those responsible for the TOE will locate it within facilities providing controlled access to prevent unauthorized physical access.

5 IT SECURITY REQUIREMENTS

37 This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

38 The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

39 These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements

40 The TOE satisfies the SFRs delineated in Table 6. The rest of this section contains a description of each component and any related dependencies.

Table 6: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
User Data Protection (TSF_UDP_REMOTE, TSF_UDP_MAC, TSF_UDP_PRIV, TSF_UDP_FLOW)	
FDP_ACC.1 (1-3)	Access Control Policy
FDP_ACF.1 (1-3)	Security Attribute-based Access Control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
Identification and Authentication (TSF_FIA_USERS, TSF_FIA_AUTH)	
FIA_ATD.1	User Attribute Definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
Security Management Roles (TSF_FMT)	
FMT_MOF.1 (1-2)	Management of security functions behavior
FMT_MSA.1 (1-2)	Management of Security Attributes
FMT_MTD.1 (1-4)	Management of TSF data

Functional Component ID	Functional Component Name
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles

5.1.1 Class FDP: User Data Protection

41 FDP_ACC.1 (1) Subset Access Control

Hierarchical to: No other components

FDP_ACC.1.1 (1) The TSF shall enforce the [NETWORK_MGMT SFP] on [management access requests to the TOE originating over network connections].

Dependencies: FDP_ACF.1 Security attribute-based access control

42 FDP_ACC.1 (2) Subset Access Control

Hierarchical to: No other components

FDP_ACC.1.1 (2) The TSF shall enforce the [MAC_PORT_LOCK SFP] on [Authorized Administrator-specified MAC address to physical port mappings or MACs initially learned through the port security autosave feature].

Dependencies: FDP_ACF.1 Security attribute-based access control

43 FDP_ACC.1 (3) Subset Access Control

Hierarchical to: No other components

FDP_ACC.1.1 (3) The TSF shall enforce the [PRIVILEGE_LEVEL SFP] on [Authorized Administrator issued commands].

Dependencies: FDP_ACF.1 Security attribute-based access control

44 FDP_ACF.1 (1) Security Attribute-based Access Control

Hierarchical to: No other components

FDP_ACF.1.1 (1) The TSF shall enforce the [NETWORK_MGMT SFP] to objects based on [determining if the connecting host is allowed to connect as reported in the management module's ACL for remote management as defined in the configuration file].

FDP_ACF.1.2 (1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the IP address of the originating host is in the Management module's ACL for remote management as defined in the configuration file].

FDP_ACF.1.3 (1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [if VLAN-based access control is configured - the connecting host, as determined by its IP address, is in a VLAN specified in the management module's configuration file].

FDP_ACF.1.4 (1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

45 FDP_ACF.1 (2) Security Attribute-based Access Control

Hierarchical to: No other components

FDP_ACF.1.1 (2) The TSF shall enforce the [MAC_PORT_LOCK SFP] to objects based on [determining if the connecting host is allowed to connect to a port as specified in the management module's configuration file.].

FDP_ACF.1.2 (2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) The MAC address of the connecting host is identified in the Management module's configuration file;

b) The hardware port on which the connection is made has port security enabled in the Management module's configuration file].

FDP_ACF.1.3 (2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4 (2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

46 FDP_ACF.1 (3) Security Attribute-based Access Control

Hierarchical to: No other components

FDP_ACF.1.1 (3) The TSF shall enforce the [PRIVILEGE_LEVEL SFP] to objects based on [the ability to differentiate between allowed and denied operations given one or more privilege levels].

FDP_ACF.1.2 (3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) Read/write access to the system including global system parameters if the privilege level is *Super User*, or

b) Read/write access to specified ports but not global system parameters if the privilege level is *Port Configuration*, or

c) Read access to the Privileged EXEC and CONFIG mode of the command line interface if the privilege level is *Read Only*].

FDP_ACF.1.3 (3) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4 (3) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

47 FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other components

FDP_IFC.1.1 The TSF shall enforce the [INFOFLOW SFP] on

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

b) information: network traffic sent through the TOE from one subject to another

c) operation: pass network traffic].

Dependencies: FDP_IFF.1 Simple Security Attributes

48 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [INFOFLOW SFP] based on the following types of subjects and information security attributes: [

a) If Standard ACLs are configured – subjects: source IP address, information: none;

b) If Extended ACLs are configured – subjects: source IP address, source host name, destination IP address, destination host name, source TCP or UDP port, destination TCP or UDP port.]

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 IP protocol 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 [implicit deny when no ACL match is found].
FDP_IFF.1.4	The TSF shall provide the following [none].
FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: [none].
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes in the Management module's ACL list].
Dependencies:	FDP_IFC.1 Subset Information Flow Control FMT_MSA.3 Static attribute initialization

5.1.2 Class FIA: Identification and Authentication

49 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual **human** users: [user name, authentication data, privilege level].
Dependencies:	No dependencies

50 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1
FIA_UID.2.1	The TSF shall require each **human** user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies

51 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1

FIA_UAU.2.1	The TSF shall require each **human** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

5.1.3 Class FMT: Security Management

52 FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to:	No other components
FMT_MOF.1.1 (1)	The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions [a) authentication method list(s), b) Port Locking, c) VLAN ACL, d) Standard and Extended ACLs] to [the Authorized Administrator(s) with *Super User* level privilege].
Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security Roles

53 FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to:	No other components
FMT_MOF.1.1 (2)	The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions [Port Locking] to [the Authorized Administrator(s) with *Port Configuration* level privileges].
Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security Roles

54 FMT_MSA.1 (1) Management of Security Attributes

Hierarchical to:	No other components
FMT_MSA.1.1 (1)	The TSF shall enforce the [PRIVILEGE_LEVEL SFP] to restrict the ability to *query, modify, delete* the security attributes [user name, password, privilege level] to [Authorized Administrators with Super User privilege].

	Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

55	FMT_MSA.1 (2)	Management of Security Attributes
	Hierarchical to:	No other components
	FMT_MSA.1.1 (2)	The TSF shall enforce the [PRIVILEGE_LEVEL SFP] to restrict the ability to *query, modify, delete,* [*create*] the security attributes [additional access to a privilege level on a command basis] to [Authorized Administrators with Super User privilege].
	Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

56	FMT_MTD.1 (1)	Management of TSF data
	Hierarchical to:	No other components
	FMT_MTD.1.1 (1)	The TSF shall restrict the ability to [*manage*] the [remote management ACL(s)] to [the Authorized Administrator(s) with *Super User* privilege].
	Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security roles

57	FMT_MTD.1 (2)	Management of TSF data
	Hierarchical to:	No other components
	FMT_MTD.1.1 (2)	The TSF shall restrict the ability to [*manage*] the [audit trail] to [the Authorized Administrator(s) with *Super User* privilege].
	Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security roles

58	FMT_MTD.1 (3)	Management of TSF data
	Hierarchical to:	No other components

	FMT_MTD.1.1 (3)	The TSF shall restrict the ability to [*manage*] the [local user accounts] to [the Authorized Administrator(s) with *Super User* privilege].
	Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security roles

59 FMT_MTD.1 (4) Management of TSF data

	Hierarchical to:	No other components
	FMT_MTD.1.1 (4)	The TSF shall restrict the ability to [*manage*]the [privilege level passwords] to [the Authorized Administrator(s) with *Super User* privilege].
	Dependencies:	FMT_SMF.1 Specifications of Management Functions FMT_SMR.1 Security roles

60 FMT_SMF.1 Specification of Management Functions

	Hierarchical to:	No other components
	FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [a) Manage the NETWORK_MGMT SFP, b) Manage the MAC_PORT_LOCK SFP, c) Manage the PRIVILEGE_LEVEL SFP, d) Manage the INFOFLOW SFP e) Manage individual human user security attributes f) Manage security management roles g) Manage the audit trail].
	Dependencies:	No Dependencies

61 FMT_SMR.1 Security Roles

	Hierarchical to:	No other components
	FMT_SMR.1.1	The TSF shall maintain the roles [a) Authorized Administrator with Super User (privilege level 0);

b) Authorized Administrator with Port Configuration (privilege level 4); and

c) Authorized Administrator with Read Only (privilege level 5)].

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

Dependencies: FIA_UID.1 Timing of identification

5.2 TOE Security Assurance Requirements

62 Table 7 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL 2. The SARs are not iterated or refined from Part 3.

Table 7: EAL 2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration Items	None
ADO_DEL.1	Delivery Procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	High-level design	ADV_FSP.1 ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1 ATE_FUN.1
ATE_FUN.1	Functional testing	None.
ATE_IND.2	Independent testing - sample	ADV_FSP.1 AGD_USR.1 ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1 ADV_HLD.1 AGD_USR.1

5.3 Security Requirements for the IT Environment

63 There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

64 This ST contains the explicitly stated SFRs without reference to the CC as enumerated in Table 8 below.

Table 8: Explicitly Stated Security Functional Requirements

Functional Component ID	Functional Component Name
Identification and Authentication (TSF_FIA_AUTH)	
FNC_NEW.1	Authentication-Method Lists
Auditing (TSF_FAU)	
FNC_NEW.2	Syslog generation

65 FNC_NEW.1 Authentication Method Lists

Hierarchical to: No other components

FNC_NEW.1.1 The TSF shall provide a mechanism to allow Authorized Administrator(s) to specify, according to site policy, the order (up to seven entries) by which one or more authentication methods are consulted.

FNC_NEW.1.2 The TSF Authentication Method list will process authentication methods based on the following rules:

a) If the first authentication method is successful, access is granted and processing stops.

b) If the access is rejected, by the first authentication method, access denied and list processing stops.

c) If an error occurs with an authentication method, the next method on the list is tried.

d) If the user, and or password, is not known to an authentication method, this is not an error, and the user is denied access and processing stops.

e) The process will continue until an authentication method is passed or the end of the method list is reached.

f) If the Super User level password is not rejected after all the access methods in the list have been tried, access is granted.

Dependencies: No dependencies

66 FNC_NEW.2 Syslog generation

Hierarchical to: No other components

FNC_NEW.2.1 The TSF shall provide a syslog facility.

FNC_NEW.2.2 The TSF syslog facility shall buffer up to 100 messages locally on a FIFO rotational basis.

FNC_NEW.2.3 The TSF syslog facility shall write syslog messages to separate local buffers based on the following:

a) The Static Buffer shall contain: logs of power failures, fan failures, and temperature warning or shutdown messages

b) The Dynamic Buffer shall contain: logs of all other message types.

FNC_NEW.2.4 The TSF syslog facility shall record within each audit record at least the following information:

a) date and time of the event,

b) the type of event,

c) the outcome of the event,

d) the severity of the event

Dependencies: No dependencies

5.5 SFRs With SOF Declarations

67 FIA_UAU.2: The authentication mechanism has a password space of case-sensitive alpha or numeric characters and a minimum password size of 8. The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

6 TOE SUMMARY SPECIFICATION

68 This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

69 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

70 APPLICATION NOTE: The TOE cannot make any claim to the veracity of the data provided in a data packet, especially with respect to source and destination addresses. Therefore, all following discussions with respect to source and destination host addresses are based on the presumption that the addresses contained in the data packet are correct.

6.1.1 User Data Protection

71 (TSF_UDP_REMOTE) The Foundry Networks Management Module IV has the capability to restrict management functions from remote sources, including Telnet, the Web management interface, and SNMP. The following methods for restricting remote access are supported:

- Using ACLs to restrict Telnet, Web management interface, or SNMP access
- Allowing remote access only from specific IP addresses
- Allowing remote access only to clients connected to a specific VLAN.

72 Remote access decisions are based on entries in the device's Access Control List (ACL). Access control parameters include entries specifying the allowed connecting host IP address and/or the connecting host is in an allowed virtual LAN (VLAN).

73 **Functional Requirements Satisfied:** FDP_ACC.1(1), FDP_ACF.1(1), FIA_UID.2, FMT_MOF.1(1), FMT_MTD.1(1)

74 (TSF_UDP_MAC) Foundry Networks Chassis based Management Modules have the capability to control user access to the device through determining if the MAC address of the connecting host and the hardware port through which the connection request is made is in the device's configuration file.

75 **Functional Requirements Satisfied:** FDP_ACC.1(2), FDP_ACF.1(2), FIA_UID.2, FMT_MTD.1(1)

76 (TSF_UDP_PRIV) The Foundry Networks Management Module IV has three management privilege levels:

- Super User Level (privilege level 0): Allows complete read-and-write access to the system. This is generally for system administrators and is the only management privilege level that allows the configuration of passwords.

- Port Configuration level: Allows read-and-write access for specific ports but not for global (system-wide) parameters.

- Read Only level: Allows access to the Privileged EXEC mode and CONFIG mode of the CLI but only with read access.

77 In the evaluated configuration, the Authorized Administrator assigns a privilege level to each user account defined. Additionally, the Authorized Administrator can assign a password to each management privilege level. When user accounts are defined (as in the evaluated configuration) and privilege level passwords are assigned to the privilege level, the device will validate a management access request/attempt using one or both methods (local user account or privilege level password), depending on the order specified in the authentication-method lists (see Section TSF_FIA_AUTH).

78 Additionally, the Authorized Administrator(s) have the capability to limit the access to specific levels of the command line interface (CLI) based on assigning privilege levels to the CLI level that contains the command.

79 **Functional Requirements Satisfied:** FDP_ACC.1(3), FDP_ACF.1(3), FMT_MSA.1(2), FMT_MTD.1(4), FMT_SMR.1

80 (TSF_UDP_FLOW) The Foundry Networks Management Module IV has the ability to control the flow of 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 by the Authorized Administrator(s), "Standard" and "Extended."

81 "Standard" ACLs permit or deny packets based on source IP address only.

82 "Extended" ACLs filter based on:

- IP protocol (TCP, UDP, etc.)

- Source IP address or host name,

- Destination IP address or host name,

- Source TCP or UDP port for TCP/IP traffic,

- Destination TCP or UDP port for TCP/IP traffic.

83 The ordering of the rules in an ACL is important because the first match is executed without consideration of subsequent rules in the list.

84 **Functional Requirements Satisfied:** FDP_IFC.1, FDP_IFF.1, FIA_UID.2

6.1.2 Identification and Authentication

85 (TSF_FIA_USERS) Foundry Networks Chassis Based Management Modules allow the assigning of user names and passwords to control access to the management functions of the device. The Authorized Administrator(s) can define up to 16 local user accounts on the device. These User accounts regulate who can access the management functions in the CLI using the following methods: telnet access, Web management access, and SNMP access.

86 For each local user account, the Authorized Administrator specifies the user name, password, and privilege level (see Section TSF_UDP_PRIV). Additionally, when local user accounts are configured, the Authorized Administrator(s) must configure an authentication-method list (see below).

87 **Functional Requirements Satisfied:** FIA_ATD.1, FIA_UID.2, FIA_UAU.2, FMT_MTD.1(3), FMT_SMR.1

88 (TSF_FIA_AUTH) Foundry Networks Chassis Based Management Modules allow the Authorized Administrator to configure Authentication-Method lists. These lists are used when one or more authentication methods are implemented, and they are used to specify the order in which the authentication methods are employed.

89 In an authentication–method list for a particular access method, up to seven authentication methods can be specified. If the first authentication method is successful, the software grants access and stops the authentication process. If the access is rejected by the first authentication method, the software denies access and stops checking.

90 However if there is a failure in an authentication method (e.g., if the authentication method is unreachable, this is a failure; if the user name and/or password is not known to the method, this is not a failure), the software tries the next method on the list, and so on. The software will continue this process until either the authentication method is passed or the software reaches the end of the method list.

91 **Functional Requirements Satisfied:** FMT_MOF.1(1), FIA_UAU.2, FMT_MTD.1(4), FNC_NEW.1

6.1.3 Security Management

92 (TSF_FMT) The Foundry Management Module IV includes a number of functions to manage security policy and its implementation. Policy management and implementation are controlled through the use of various ACLs, and several security role definitions/privileges.

93 The device supports the use of Authorized Administrator-developed remote management ACLs, configuration files, user account definitions (including privilege levels), data flow ACLs , and authentication-method lists.

94 **Functional Requirements Satisfied:** FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FNC_NEW.1, FNC_NEW.2, FMT_SMF.1

6.1.4 Auditing

95 (TSF_FAU) The Foundry Management Module IV has the ability to generate syslog-based audit log entries for each defined ACL entry. The audit information provided in the audit log includes the information provided in Appendix A.

96 The TOE is also capable of connecting to up to six external (IT Environment) syslogd servers. This capability allows for the external storage of syslog messages. When the TOE is connected to a syslogd server, it writes the syslog messages to the system log/buffer and the syslogd server.

97 **Functional Requirements Satisfied:** FMT_MTD.1(2), FNC_NEW.2

6.2 Assurance Measures

98 The TOE satisfies CC EAL 2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Foundry to satisfy the CC EAL 2 assurance requirements.

Table 9: Security Assurance Requirements

Assurance Component	How requirement will be met
ACM_CAP.2	The requirement for configuration items will be met by the submission of evidence in accordance with the developer action elements for the component as specified in [CC_PART3].
ADO_DEL.1	The developer will provide evidence in accordance with the developer action elements for the component as specified in [CC_PART3].
ADO_IGS.1	Factory Installation: The developer will perform IGS; this procedure meets the intent of the IGS requirement. Customer Installation: The developer will provide evidence in accordance with the developer action elements for the component as specified in [CC_PART3].
ADV_FSP.1	The vendor provided an informal function specification.
ADV_HLD.1	The vendor provided a high-level design.
ADV_RCR.1	The informal correspondence demonstration is provided in the design documentation. ST to FSP in the FSP, FSP to HLD in the HLD.
AGD_ADM.1	The vendor submitted an Administrator manual and release notes.
AGD_USR.1	The vendor submitted a release note.

Assurance Component	How requirement will be met
ATE_COV.1	The developer will provide a coverage analysis in accordance with the developer action elements for the component as specified in [CC_PART3].
ATE_FUN.1	The developer provided functional test evidence.
ATE_IND.2	The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.
AVA_SOF.1	The developer will provide evidence in accordance with the developer action elements for the component as specified in [CC_PART3].
AVA_VLA.1	The developer will provide evidence in accordance with the developer action elements for the component as specified in [CC_PART3].

7 PROTECTION PROFILE (PP) CLAIMS

99 The TOE does not claim conformance to a PP.

8 RATIONALE

100 This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- security objectives to threats encountered
- environmental objectives to assumptions met
- SFRs to objectives met

Assurance Level A justification is provided for selecting an EAL 2 level of assurance for this ST.

SOF A rationale is provided for the SOF level chosen for this ST.

Dependencies A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

101 This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

Table 10: Security Objectives Rationale (TOE and Environment)

Objective	Threat Organizational Security Policy Assumption	Rational
O.ADMIN_USERS	T.ALTER_CONFIG P.LOCAL_ACCOUNTS P.PRIVILEDGE_LEVELS	O.ADMIN_USERS helps to counter the threat T.ALTER_CONFIG by associating accounts and passwords with the administrative functionality. It also supports P.LOCAL_ACCOUNTS and

Objective	Threat Organizational Security Policy Assumption	Rational
		P.PRIVILEGE_LEVELS.
O.SYSLOG_AUDIT	T.ALTER_CONFIG P.SYS_CLOCK P.SYSLOG	O.SYSLOG_AUDIT supports P.SYS_CLOCK and P.SYSLOG and helps to counter T.ALTER_CONFIG by providing a means for Authorized Administrators to monitor both ACL decisions made on the device and TOE system status. This information can be used to indicate/identify any possible attempts to access/modify the security policy configured on the device.
O.DATA_FLOW_CONFIG	T.ALTER_CONFIG P.REMOTE_ACCESS	O.DATA_FLOW_CONFIG helps to counter the threat T.ALTER_CONFIG by allowing the Authorized Administrator(s) to specify the type, data, and destination of externally visible connections to the device.
O.PRIVILEGE_LEVELS	T.ALTER_CONFIG P.PRIVILEGE_LEVELS	O.PRIVILEGE_LEVELS supports the OSP P.PRIVILEGE_LEVELS and helps to counter the threat T.ALTER_CONFIG by having multiple levels of access to the commands used to configure/maintain the device.
O.REMOTE_ACCESS	T.ALTER_CONFIG P.LOCAL_ACCOUNTS P.PRIVILEGE_LEVELS P.REMOTE_ACCESS	O.REMOTE_ACCESS helps to counter the threat T.ALTER_CONFIG by requiring that the TOE must provide access methods, for other than serial port access to the CLI, of which one will be local, that will be secured via AAA security methods.

Objective	Threat Organizational Security Policy Assumption	Rational
		Also, must provide the Authorized Administrator(s) configurable ACL(s) to specify the allowed remote management access connections.
OE.INSTALL	A.INSTALL A.MANAGE A.NO_EVIL_ADM A.PROCEDURE	OE.INSTALL is met by A.INSTALL, A.MANAGE, A.NO_EVIL_ADM, and A.PROCEDURE. These environmental assumptions specify the need for the TOE hardware and software to be delivered, installed, and setup in accordance with documented delivery and installation/setup procedures. Additionally, they call for one or more competent Authorized Administrator(s), that are not willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation, assigned to manage the TOE and the security functions it performs.
OE.OPTIONAL_I&A	T.ALTER_CONFIG A.EXTERNAL_I&A P.REMOTE_ACCESS	OE.OPTIONAL_I&A helps to counter the TOE threat T.ALTER_CONFIG by allowing for external I&A mechanisms (based on site specific policy). Additionally it supports the OSP P.REMOTE_ACCESS, As such, A.EXTERNAL_I&A helps to meet this objective by specifying that any external I&A mechanisms function correctly and

Objective	Threat Organizational Security Policy Assumption	Rational
		accurately.
OE.PHYSICAL	A.PHYSICAL_PROTECT	OE.PHYSICAL is met by the A.PHYSICAL_PROTECT environmental assumption. This assumption acknowledges the need for the TOE to be located within facilities providing controlled access to prevent unauthorized physical access.

8.2 Security Requirements Rationale

102 This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

103 These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Rationale For TOE Security Requirements

104 This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following paragraphs provide the security requirement to security objective mapping and a rationale to justify the mapping.

Table 11: Rationale for TOE Security Requirements

Security Functional Requirement	Rationale
FDP_ACC.1 (1)	Ensures that there is an access control policy covering access requests from external network connections. This SFR traces back to and aids in meeting the following objective(s): O.REMOTE_ACCESS.
FDP_ACC.1 (2)	Ensures that there is an access control policy enforced with respect to MAC addresses and the hardware port on which the access/connection is requested. This SFR traces back to and aids in meeting the following objective(s): O.REMOTE_ACCESS.
FDP_ACC.1 (3)	Ensures that there is an access control policy, set by

Security Functional Requirement	Rationale
	the Authorized Administrator(s) with regard to privilege levels. This SFR traces back to and aids in meeting the following objective(s): O.PRIVILEGE_LEVELS.
FDP_ACF.1 (1)	Ensures access control from external network ports based on determining if the IP address of the connecting host is in the device's ACL. This SFR traces back to and aids in meeting the following objective(s): O.DATA_FLOW_CONFIG.
FDP_ACF.1 (2)	Ensures that the access control policy, MAC_PORT_LOCK_SFP, is enforced based on the connecting host's MAC address. This SFR traces back to and aids in meeting the following objective(s): O.REMOTE_ACCESS.
FDP_ACF.1 (3)	Ensures that the access control policy PRIVILEGE_LEVEL_SFP is based on the privilege level attribute of the object. This SFR traces back to and aids in meeting the following objective(s): O.PRIVILEGE_LEVELS.
FDP_IFC.1	Ensures that there is an information flow control policy. This SFR traces back to and aids in meeting the following objective(s): O.DATA_FLOW_CONFIG.
FDP_IFF.1	Ensures that the INFOFLOW SFP is enforced based on "Standard" ACLs and "Extended" ACLs, and the specified security attributes. This SFR traces back to and aids in meeting the following objective(s): O.DATA_FLOW_CONFIG.
FIA_ATD.1	Ensures that there are specified security attributes maintained by the TOE with respect to individual human users. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.REMOTE_ACCESS.
FIA_UID.2	Ensures that each user is identified before any other TSF-mediated actions are allowed. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.REMOTE_ACCESS.

Security Functional Requirement	Rationale
FIA_UAU.2	Ensures that human users are authenticated before any other TSF-mediated actions occur. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.REMOTE_ACCESS.
FMT_MOF.1 (1)	Ensures that Authorized Administrator(s) can manage the TOE. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.PRIVILEGE_LEVELS.
FMT_MOF.1 (2)	Ensures that Authorized Administrator(s) can manage the TOE. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.PRIVILEGE_LEVELS.
FMT_MSA.1 (1)	Ensures that Authorized Administrator(s) can manage the human user attributes specified in FIA_ATD.1. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.PRIVILEGE_LEVELS.
FMT_MSA.1 (2)	Ensures that Authorized Administrator(s) can manage the NETWORK_MGMT_SFP. This SFR traces back to and aids in meeting the following objective(s): O.REMOTE_ACCESS.
FMT_MTD.1 (1)	Ensures that the Authorized Administrator(s) can manage the remote access ACLs. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.REMOTE_ACCESS.
FMT_MTD.1 (2)	Ensures that the Authorized Administrators can manage the audit trail. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.SYSLOG_AUDIT.
FMT_MTD.1 (3)	Ensures that the Authorized Administrators can manage the local user accounts. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.REMOTE_ACCESS.

Security Functional Requirement	Rationale
FMT_MTD.1 (4)	Ensures that the Authorized Administrators can manage the privilege levels. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS, O.PRIVILEGE_LEVELS.
FMT_SMF.1	Ensures that the management functions to be provided for by the TOE are specified. This SFR traces back to, and aids in meeting the following objective(s): O.ADMIN_USERS, O.PRIVILEGE_LEVELS, O.SYSLOG_AUDIT, O.DATA_FLOW_CONFIG, O.REMOTE_ACCESS
FMT_SMR.1	Ensures that the capabilities of the Authorized Administrator(s) are based on their role (privilege level). This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS.
FNC_NEW.1	Ensures that there may be multiple authentication mechanisms, and that the Authorized Administrator(s) can set the order in which these mechanisms are attempted. This SFR traces back to and aids in meeting the following objective(s): O.ADMIN_USERS.
FNC_NEW.2	Ensures that the TOE will maintain a syslog audit mechanism. This SFR traces back to and aids in meeting the following objective(s): O.SYSLOG_AUDIT.

Table 12: TOE SFR mappings to Objectives

	O.ADMIN_USERS	O.SYSLOG_AUDIT	O.DATA_FLOW_CONFIG	O.PRIVILEGE_LEVELS	O.REMOTE_ACCESS
FDP_ACC.1 (1)					X
FDP_ACC.1 (2)					X
FDP_ACC.1 (3)				X	
FDP_ACF.1 (1)			X		
FDP_ACF.1 (2)					X
FDP_ACF.1 (3)				X	
FDP_IFC.1			X		
FDP_IFF.1			X		
FIA_ATD.1	X				X
FIA_UID.2	X				X
FIA_UAU.2	X				X
FIA_MOF.1 (1)	X			X	
FIA_MOF.1 (2)	X			X	
FMT_MSA.1 (1)	X			X	
FMT_MSA.1 (2)					X
FMT_MTD.1 (1)	X				X
FMT_MTD.1 (2)	X	X			
FMT_MTD.1 (3)	X				X
FMT_MTD.1 (4)	X			X	
FMT_SMF.1	X	X	X	X	X
FMT_SMR.1	X				
FNC_NEW.1	X				
FNC_NEW.2		X			

8.3 Rationale For Assurance Level

105 This ST has been developed for Foundry Networks Management Module IV. The TOE environment will be exposed to a low level of risk. As such, the Evaluation Assurance Level 2 is appropriate.

8.4 Rationale For TOE Summary Specification

106 This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

107 The specified TSFs work together to satisfy the TOE SFRs. Table 13 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 13: Mapping of SFRs to Security Functions

SFR	Name	TSF
FDP_ACC.1 (1)	Access control policy	TSF_UDP_REMOTE
FDP_ACC.1 (2)	Access control policy	TSF_UDP_MAC
FDP_ACC.1 (3)	Access control policy	TSF_UDP_PRIV
FDP_ACF.1 (1)	Security attribute-based access control	TSF_UDP_REMOTE
FDP_ACF.1 (2)	Security attribute-based access control	TSF_UDP_MAC
FDP_ACF.1 (3)	Security attribute-based access control	TSF_UDP_PRIV
FDP_IFC.1	Subset information flow control	TSF_UDP_FLOW
FDP_IFF.1	Simple security attributes	TSF_UDP_FLOW
FIA_ATD.1	User attribute definition	TSF_FIA_USERS
FIA_UID.2	User identification before and action	TSF_FIA_USERS TSF_UDP_MAC TSF_UDP_REMOTE TSF_UDP_FLOW
FIA_UAU.2	User authentication before any action	TSF_FIA_USERS TSF_FIA_AUTH
FIA_MOF.1	Management of security functions behavior	TSF_UDP_REMOTE TSF_UDP_FLOW TSF_FIA_AUTH TSF_FAU
FMT_MSA.1 (1)	Management of security attributes	TSF_FIA_FLOW TSF_FMT

SFR	Name	TSF
FMT_MSA.1 (2)	Management of security attributes	TSF_UDP_PRIV TSF_FMT
FMT_MTD.1 (1)	Management of TSF data	TSF_UDP_REMOTE TSF_UDP_MAC TSF_FMT
FMT_MTD.1 (2)	Management of TSF data	TSF_FAU TSF_FMT
FMT_MTD.1 (3)	Management of TSF data	TSF_FIA_USERS TSF_FMT
FMT_MTD.1 (4)	Management of TSF data	TSF_FIA_PRIV TSF_FIA_AUTH TSF_FMT
FMT_SMF.1	Specification of Management Functions	TSF_FMT
FMT_SMR.1	Security Roles	TSF_UDP_PRIV TSF_FIA_USERS TSF_FMT
FNC_NEW.1	Authentication-Method Lists	TSF_FIA_AUTH TSF_FMT
FNC_NEW.2	Syslog generation	TSF_FAU TSF_FMT

8.4.1 TOE Assurance Requirements

108 Section 6.2 of this document identifies the Assurance Measures implemented by Foundry to satisfy the assurance requirements of EAL 2 as delineated in the table in Annex B of the CC, Part 3. Table 14 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 14: Assurance Requirement Compliance Matrix

Assurance Requirement	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Analysis
ACM_CAP.2	**X**					
ADO_DEL.1		**X**				

Assurance Requirement	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Analysis
ADO_IGS.1		**X**				
ADV_FSP.1			**X**			
ADV_HLD.1			**X**			
ADV_RCR.1			**X**			
AGD_ADM.1				**X**		
AGD_USR.1				**X**		
ATE_COV.1					**X**	
ATE_FUN.1					**X**	
ATE_IND.1					**X**	
AVA_SOF.1						**X**
AVA_VLA.1						**X**

8.4.2 TOE SOF Claims

109 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. The claim of SOF-basic ensures that the mechanism is resistant to a low attack potential.

8.5 Rationale For SFR and SAR Dependencies

110 Table 15 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 15: SFR Dependency Status

Functional Component ID	Functional Component Name	Dependency(ies)	Satisfied
FDP_ACC.1 (1-3)	Subset Access	FDP_ACF.1	Yes

Functional Component ID	Functional Component Name	Dependency(ies)	Satisfied
	Contol		
FDP_ACF.1 (1-3)	Security attribute-based access control	FDP_ACC.1 FMT_MSA.3	No – see explanation below
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Yes
FDP_IFF.1	Simple security attributes	FDP_IFC.1 FDP_MSA.3	No – see explanation below
FIA_ATD.1	User attribute definition	None	N/A
FIA_UAU.2	User authentication before any action	FIA_UID.1	Yes – by virtue of the fact that FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UID.2	User identification before any action	None	N/A
FIA_MOF.1	Management of security functions behavior	FMT_SMR.1	Yes
FMT_MSA.1 (1-2)	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	Yes
FMT_MTD.1 (1-4)	Management of TSF data	FMT_SMR.1	Yes
FMT_SMF.1	Specification of Management Functions	None	N/A
FMT_SMR.1	Security Roles	FIA_UID.1	Yes – by virtue of the fact that FIA_UID.2 is hierarchical to FIA_UID.1
FNC_NEW.1	Authentication-Method Lists	None	N/A
FNC_NEW.2	Syslog generation	None	N/A

111 The dependency on FMT_MSA.3, Static attribute initialization, by both FDP_ACF.1 and FDP_IFF.1 are not met because they are not supported in the implementation of this TOE since the primary objects traversing the device, and consequently their attributes, are created dynamically (i.e., Ethernet packets). Additionally, the other data objects contained within the TOE physical and logical boundary (e.g., ACLs, user definitions) are comprised of Authorized Administrator definable attribute values, and are based strictly on site-specific policy and specified in the OSP section of this ST.

112 The SAR dependencies identified in the CC have been met by this ST as shown in Table 16.

Table 16: EAL 2 SAR Dependencies

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration Items	None	NA
ADO_DEL.1	Delivery Procedures	None	N/A
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	YES
ADV_FSP.1	Informal functional specification	ADV_RCR.1	YES
ADV_HLD.1	High-level design	ADV_FSP.1 ADV_RCR.1	YES
ADV_RCR.1	Informal correspondence demonstration	None	N/A
AGD_ADM.1	Administrator guidance	ADV_FSP.1	YES
AGD_USR.1	User guidance	ADV_FSP.1	YES
ATE_COV.1	Evidence of coverage	ADV_FSP.1 ATE_FUN.1	YES
ATE_FUN.1	Functional testing	None.	N/A
ATE_IND.2	Independent testing - sample	ADV_FSP.1 AGD_USR.1 ATE_FUN.1	YES
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1	YES

8.6 Rationale for Explicitly Stated Requirements

113 Two explicitly stated requirements are specified in Section 5.4 of this ST: FNC_NEW.1 and FNC_NEW.2.

114 FNC_NEW.1: Authentication method lists – was added to ensure coverage of the fact that the Authorized Administrator(s) could, through this mechanism, specify the ordering regardless of the location (internal or external to the TOE) of human user authentication.

115 FNC_NEW.2: Syslog audit – was added because CC permitted operations on the TSF FAU_GEN.1 could not accurately reflect the implementation of the audit functionality of the TOE.

8.7 Internal Consistency and Mutually Supportive Rationale

116 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Table 13. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 15 and Table 16 and described in Section 8.6.

c) The SARs are appropriate for the assurance level of EAL 2 and are satisfied by the TOE as shown in Table 9. EAL 2 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.

APPENDIX A: SYSLOG ENTRY TYPES

Table 21: Foundry Syslog Message Examples

Message Level	Message	Explanation

Alert	Power supply <num>, <location>, failed	A power supply has failed.
		The <num> is the power supply number.
		The <location> describes where the failed power supply is in the chassis. The location can be one of the following:
		• In 4-slot Chassis devices:
		  • left side power supply
		  • right side power supply
		• In 8-slot Chassis devices:
		  • bottom power supply
		  • middle bottom power supply
		  • middle top power supply
		  • top power supply
		• In Stackable devices:
		  • power supply on right connector
		  • power supply on left connector

Alert	Fan <num>, <location>, failed	A fan has failed.
		The <num> is the power supply number.
		The <location> describes where the failed power supply is in the chassis. The location can be one of the following:
		• In 4-slot Chassis devices:
		  • left side panel, back fan
		  • left side panel, front fan
		  • rear/back panel, left fan
		  • rear/back panel, right fan
		• In 8-slot Chassis devices:
		  • rear/back panel, top fan
		  • rear/back panel, bottom fan

		• top panel, fan • top panel, fan • In Stackable devices: • fan on right connector • fan on left connector
Alert	Management module at slot <slot-num> state changed from <module-state> to <module-state>.	Indicates a state change in a management module. The <slot-num> indicates the chassis slot containing the module. The <module-state> can be one of the following: • active • standby • crashed • coming-up • unknown
Alert	Temperature <degrees> C degrees, warning level <warn-degrees> C degrees, shutdown level <shutdown-degrees> C degrees	Indicates an overtemperature condition on the active module. The <degrees> value indicates the temperature of the module. The <warn-degrees> value is the warning threshold temperature configured for the module. The <shutdown-degrees> value is the shutdown temperature configured for the module.
Alert	<num-modules> modules and 1 power supply, need more power supply!!	Indicates that the Chassis device needs more power supplies to run the modules in the chassis. The <num-modules> parameter indicates the number of modules in the chassis.
Alert	Out of tcp send buffer at <application>	Indicates that the TCP send buffer is exhausted.

		The <application> parameter is the application that caused the buffer overflow.
Alert	Out of TCB memory at <application>	Indicates that TCB memory is exhausted. The <application> parameter shows which application is out of TCB memory.
Warning	Locked address violation at interface e<portnum>, address <mac-address>	Indicates that a port on which you have configured a lock-address filter received a packet that was dropped because the packet's source MAC address did not match an address learned by the port before the lock took effect. The e<portnum> is the port number. The <mac-address> is the MAC address that was denied by the address lock. Assuming that you configured the port to learn only the addresses that have valid access to the port, this message indicates a security violation.
Warning	NTP server <ip-addr> failed to respond	Indicates that a Simple Network Time Protocol (SNTP) server did not respond to the device's query for the current time. The <ip-addr> indicates the IP address of the SNTP server.
Warning	Dup IP <ip-addr> detected, sent from MAC <mac-addr> interface <portnum>	Indicates that the Foundry device received a packet from another device on the network with an IP address that is also configured on the Foundry device. The <ip-addr> is the duplicate IP address. The <mac-addr> is the MAC address of the device with the duplicate IP address. The <portnum> is the Foundry port that received the packet with the duplicate IP address. The address is the packet's source IP address.

Warning	mac filter group denied packets on port <portnum> src macaddr <mac-addr>, <num> packets	Indicates that a Layer 2 MAC filter group configured on a port has denied packets. The <portnum> is the port on which the packets were denied. The <mac-addr> is the source AMC address of the denied packets. The <num> indicates how many packets matching the values above were dropped during the five-minute interval represented by the log entry.
Warning	list <acl-num> denied <ip-proto> <src-ip-addr> (<src-tcp/udp-port>) (Ethernet <portnum> <mac-addr>) -> <dst-ip-addr> (<dst-tcp/udp-port>), <num> packets	Indicates that an Access Control List (ACL) denied (dropped) packets. The <acl-num> indicates the ACL number. Numbers 1 – 99 indicate standard ACLs. Numbers 100 – 199 indicate extended ACLs. The <ip-proto> indicates the IP protocol of the denied packets. The <src-ip-addr> is the source IP address of the denied packets. the <src-TCP/UDP-port> is the source TCP or UDP port, if applicable, of the denied packets. The <portnum> indicates the port number on which the packet was denied. The <mac-addr> indicates the source MAC address of the denied packets. The <dst-ip-addr> indicates the destination IP address of the denied packets. The <dst-tcp/udp-port> indicates the destination TCP or UDP port number, if applicable, of the denied packets. The <num> indicates how many packets matching the values above were dropped during the five-minute interval represented by the log entry.

117