

**Enterasys Networks, Inc.  
Matrix N, DFE Gold Enterasys  
Networking System v6.01, Matrix N,  
DFE Platinum Enterasys Networking  
System v6.01, Matrix N, DFE Diamond  
Enterasys Networking System v6.01  
and Matrix X Enterasys Networking  
System v1.6.4P4**



## **Security Target**

Evaluation Assurance Level: EAL 3+  
Document Version: 1.5

---

Prepared for:



**Enterasys Networks, Inc.**  
50 Minuteman Road  
Andover, MA 01810  
Phone: (978) 684-1000

<http://www.enterasys.com>

Prepared by:



**Corsec Security, Inc.**  
10340 Democracy Lane, Suite 201  
Fairfax, VA 22030  
Phone: (703) 267-6050

<http://www.corsec.com>

## Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-05-02	Teresa MacArthur	Initial draft.
0.2	2007-06-15	Teresa MacArthur	Title change.
0.3	2007-08-24	Greg Milliken	Addressed verdicts of Observation Report 01, dated July 6, 2007.
0.4	2007-09-13	Greg Milliken	Addressed verdicts of Observation Report 05.
0.5	2007-12-12	Greg Milliken	Addressed verdicts for CB Observation Report 01 and Updated version numbers for version 1.5.5P5 of the X.
0.6	2008-01-23	Amy Nicewick	Updated assurance measures (addressed Observation Report 02).
0.7	2008-02-21	Amy Nicewick	Addressed verdict 1 of Observation Report 07 and added Diamond series to Matrix N reference.
0.8	2008-04-09	Amy Nicewick	Addressed "Unresolved Issues" dated 2008-03-24.
0.9	2008-04-24	Greg Milliken	Updated FMT_MTD table to include SuperUser and Read-Write admin ability to modify audit records. Clarified FAU_GEN.1.1 to show that SNMP failed authentication events aren't logged on the Matrix X.
1.0	2008/05/20	Amy Nicewick	Updated per CB OR #2.
1.1	2008-07-07	Greg Milliken Amy Nicewick	Updated version numbers and added more detail to the TSS description of the audit function for the Matrix X. Modified FMT_MTD.1 table.
1.2	2008-08-14	Greg Milliken	Updates for Unresolved Issues #3 and updated VxWorks and Linux version numbers.
1.3	2008-08-21	Greg Milliken	Updated version numbers in table 14 for Matrix X docs.
1.4	2008-08-26	Greg Milliken	Changes to FMT_MTD.1, FMT_MOF.1(c) and FAU_SAR.1.
1.5	2008-08-29	Greg Milliken	Changes to FMT_MTD.1.

# Table of Contents

---

<b>REVISION HISTORY .....</b>	<b>2</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>TABLE OF FIGURES .....</b>	<b>4</b>
<b>TABLE OF TABLES .....</b>	<b>4</b>
<b>1 SECURITY TARGET INTRODUCTION .....</b>	<b>6</b>
1.1 PURPOSE.....	6
1.2 SECURITY TARGET, TOE AND CC IDENTIFICATION AND CONFORMANCE .....	6
1.3 CONVENTIONS, ACRONYMS, AND TERMINOLOGY .....	7
1.3.1 Conventions .....	7
1.3.2 Acronyms .....	7
1.3.3 Terminology.....	7
<b>2 TOE DESCRIPTION .....</b>	<b>8</b>
2.1 PRODUCT TYPE.....	8
2.2 PRODUCT DESCRIPTION .....	8
2.2.1 Matrix X and Matrix N Switch Routers.....	9
2.2.2 Application of Policy .....	10
2.3 TOE BOUNDARIES AND SCOPE.....	13
2.3.1 Physical Boundary.....	13
2.3.2 Logical Boundary .....	14
2.3.3 Excluded Features and Functionality.....	14
<b>3 SECURITY ENVIRONMENT .....</b>	<b>16</b>
3.1 ASSUMPTIONS .....	16
3.2 THREATS TO SECURITY.....	17
3.3 ORGANIZATIONAL SECURITY POLICIES .....	17
<b>4 SECURITY OBJECTIVES .....</b>	<b>19</b>
4.1 SECURITY OBJECTIVES FOR THE TOE.....	19
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	19
4.2.1 IT Security Objectives .....	19
4.2.2 Non-IT Security Objectives .....	20
<b>5 SECURITY REQUIREMENTS .....</b>	<b>22</b>
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS .....	22
5.1.1 Class FAU: Security Audit.....	24
5.1.2 Class FDP: User Data Protection.....	26
5.1.3 Class FIA: Identification and Authentication .....	27
5.1.4 Class FMT: Security Management .....	28
5.1.5 Class FPT: Protection of the TSF.....	31
5.2 SECURITY FUNCTIONAL REQUIREMENTS ON THE IT ENVIRONMENT .....	32
5.2.1 Class FPT: Protection of the TOE Environment .....	32
5.3 ASSURANCE REQUIREMENTS.....	33
<b>6 TOE SUMMARY SPECIFICATION.....</b>	<b>34</b>
6.1 TOE SECURITY FUNCTIONS.....	34
6.1.1 Security Audit.....	35
6.1.2 User Data Protection.....	36
6.1.3 Identification and Authentication .....	36
6.1.4 Security Management .....	37
6.1.5 Protection of the TSF.....	38
6.2 TOE SECURITY ASSURANCE MEASURES .....	38

6.2.1	<i>ACM_CAP.3, ACM_SCP.1: Configuration Management Document</i> .....	40
6.2.2	<i>ADO_DEL.1: Delivery and Operation Document</i> .....	40
6.2.3	<i>ADO_IGS.1: Installation Guidance</i> .....	40
6.2.4	<i>ADV_FSP.1, ADV_HLD.2, ADV_RCR.1: Development Documentation</i> .....	40
6.2.5	<i>AGD_ADM.1, AGD_USR.1: Guidance Documents</i> .....	41
6.2.6	<i>ALC_DVS.1, ALC_FLR.1: Life Cycle Support</i> .....	41
6.2.7	<i>ATE_COV.2, ATE_DPT.1, ATE_FUN.1: Testing</i> .....	41
6.2.8	<i>AVA_MSU.1, AVA_SOF.1, AVA_VLA.1: Vulnerability Assessment</i> .....	41
<b>7</b>	<b>PROTECTION PROFILE CLAIMS</b> .....	<b>42</b>
7.1	PROTECTION PROFILE REFERENCE.....	42
<b>8</b>	<b>RATIONALE</b> .....	<b>43</b>
8.1	SECURITY OBJECTIVES RATIONALE.....	43
8.1.1	<i>Security Objectives Rationale Relating to Threats</i> .....	43
8.1.2	<i>Security Objectives Rationale Relating to Assumptions</i> .....	44
8.2	SECURITY FUNCTIONAL REQUIREMENTS RATIONALE.....	46
8.2.1	<i>Rationale for Security Functional Requirements of the TOE Objectives</i> .....	46
8.2.2	<i>Rationale for Security Functional Requirements of the IT Environment</i> .....	50
8.2.3	<i>Rationale for Refinements of Security Functional Requirements</i> .....	51
8.3	SECURITY ASSURANCE REQUIREMENTS RATIONALE.....	51
8.4	DEPENDENCY RATIONALE.....	52
8.5	TOE SUMMARY SPECIFICATION RATIONALE.....	53
8.5.1	<i>TOE Summary Specification Rationale for the Security Functional Requirements</i> .....	53
8.5.2	<i>TOE Summary Specification Rationale for the Security Assurance Requirements</i> .....	54
8.6	STRENGTH OF FUNCTION.....	57
<b>9</b>	<b>ACRONYMS</b> .....	<b>58</b>

## Table of Figures

FIGURE 1 – TYPICAL TOE DEPLOYMENT SCENARIO.....	8
FIGURE 2 - MATRIX N-SERIES DFE COMPARISON.....	10
FIGURE 3 – FORWARDING PROCESS FLOW CHART.....	12
FIGURE 4 - PHYSICAL TOE BOUNDARY.....	13

## Table of Tables

TABLE 1 - ST, TOE, AND CC IDENTIFICATION AND CONFORMANCE.....	6
TABLE 2 - ASSUMPTIONS.....	16
TABLE 3 - THREATS.....	17
TABLE 4 – ORGANIZATIONAL SECURITY POLICIES.....	18
TABLE 5 – TOE SECURITY OBJECTIVES.....	19
TABLE 6 – SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT.....	20
TABLE 7 – NON-IT SECURITY OBJECTIVES.....	20
TABLE 8 - TOE SECURITY FUNCTIONAL REQUIREMENTS.....	22
TABLE 9 - MANAGEMENT OF TSF DATA.....	29
TABLE 10 – SECURITY FUNCTIONAL REQUIREMENTS FOR THE ENVIRONMENT.....	32
TABLE 11 – ASSURANCE REQUIREMENTS.....	33
TABLE 12 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS.....	34
TABLE 13 – AUDIT RECORD CONTENTS.....	36

---

TABLE 14 - ASSURANCE MEASURES MAPPING TO TOE SECURITY ASSURANCE REQUIREMENTS (SARs).....	38
TABLE 15 – SECURITY OBJECTIVES RATIONALE RELATING TO THREATS.....	43
TABLE 16 – SECURITY OBJECTIVES RATIONALE RELATING TO ASSUMPTIONS.....	44
TABLE 17 – SECURITY OBJECTIVES RATIONALE RELATING TO POLICIES .....	45
TABLE 18 – SFR RATIONALE RELATED TO TOE OBJECTIVES .....	46
TABLE 19 – SFR RATIONALE RELATED TO OBJECTIVES OF THE TOE ENVIRONMENT.....	50
TABLE 20 - FUNCTIONAL REQUIREMENTS DEPENDENCIES .....	52
TABLE 21 - MAPPING OF SECURITY FUNCTIONAL REQUIREMENTS TO TOE SECURITY FUNCTIONS .....	54
TABLE 22 - ACRONYMS .....	58

# 1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4, and will hereafter be referred to as the TOE throughout this document. The TOE is the software supporting a product line of switch and router hybrid devices capable of applying access control filtering to routed traffic.

## 1.1 Purpose

This ST provides mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications that relate to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

## 1.2 Security Target, TOE and CC Identification and Conformance

**Table 1 - ST, TOE, and CC Identification and Conformance**

<b>ST Title</b>	Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 Security Target
<b>ST Version</b>	Version 1.5
<b>Author</b>	Corsec Security, Inc. Teresa MacArthur and Amy Nicewick
<b>TOE Identification</b>	Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4

<b>Common Criteria Identification and Conformance</b>	Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 augmented; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted Common Methodology for Information Technology Security Evaluation (CEM) as of 6/18/2007 were reviewed, and no interpretations apply to the claims made in this ST.
<b>PP Identification</b>	None
<b>Evaluation Assurance Level (EAL)</b>	EAL 3 Augmented with ALC_FLR.1
<b>Keywords</b>	Switch, Router, Access Control List

## 1.3 Conventions, Acronyms, and Terminology

### 1.3.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the ST reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSP Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU\_GEN.1(a) Audit Data Generation would be the first iteration and FAU\_GEN.1(b) Audit Data Generation would be the second iteration.

### 1.3.2 Acronyms

The acronyms and terms used within this ST are described in Section 9 – “Acronyms.”

### 1.3.3 Terminology

Throughout this document, the term “user” refers to administrative users. These are the only users that interact directly with the TOE.

## 2 TOE Description

The TOE description provides an overview of the TOE. This section describes the general capabilities and security functionality of the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type, describing the product, and defining the specific evaluated configuration.

### 2.1 Product Type

The Enterasys Matrix X and Matrix N devices fall into a category of equipment known as “switch routers”. These devices offer both layer 3 routing capabilities and higher speed layer 2 switching capabilities. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 offer embedded security features that provide the ability to limit the applications on the network, and restrict the use of specified applications to certain users.

Figure 1 below shows a typical deployment configuration of the TOE:

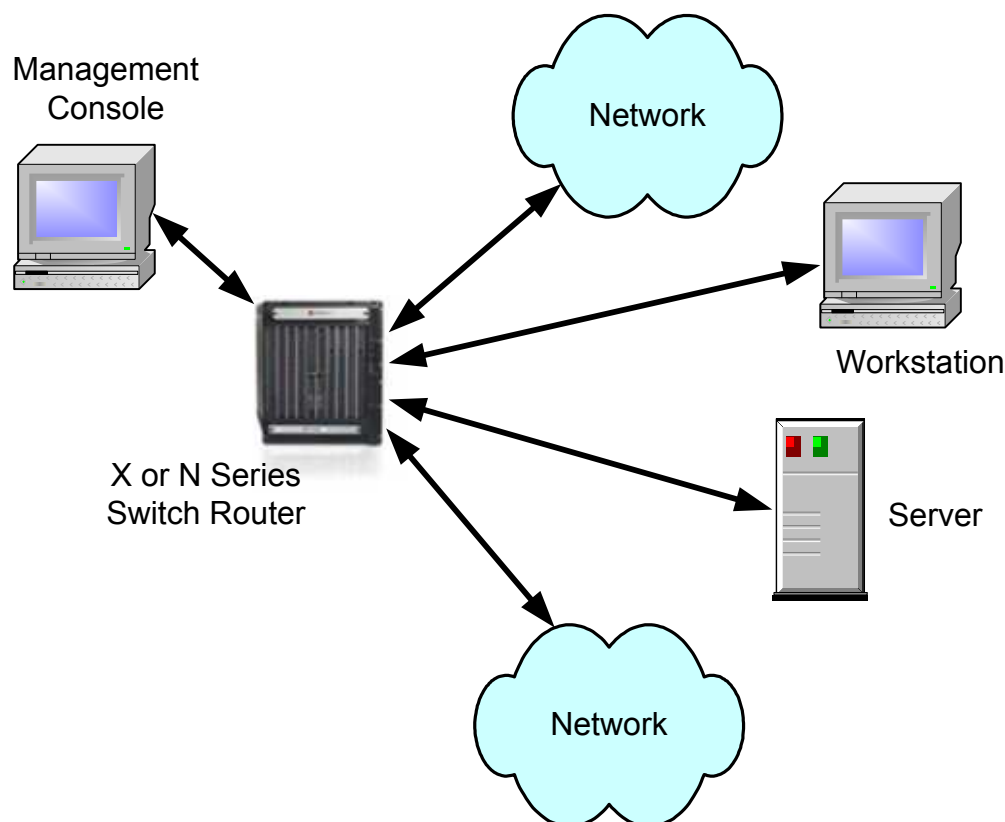


Figure 1 – Typical TOE Deployment Scenario

### 2.2 Product Description

The Enterasys Matrix X and Matrix N product families consist of the software supporting a suite of switch and router hybrids offering a range of functionality and throughput. The TOE is the Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4. These products perform the same central function: packet forwarding at layer 2 and layer 3.



## 2.2.1 Matrix X and Matrix N Switch Routers




The Matrix X product family consists of the following units. Note that each unit uses identical firmware and software and offers a similar user experience.

- The 4-slot Matrix X4 chassis is designed for small/medium enterprise backbones and includes 4 input/output (I/O) slots, redundant power, cooling, switch fabrics and control modules.
- The 8-slot Matrix X8 chassis is designed for medium/large enterprise requirements and includes 8 I/O slots, redundant power, cooling, switch fabrics and control modules.
- The 16-slot Matrix X16 chassis is designed for large enterprise requirements and includes 16 I/O slots, redundant power, cooling, switch fabrics and control modules.

The Matrix N product family includes several chassis, as well. Each chassis can support either of the two software versions provided for the Matrix N family. These two software versions are marketed as three options: Distributed Forwarding Engine (DFE) Gold, DFE Platinum, and DFE Diamond. The Platinum and Diamond versions run the same software image; they vary only in licensed options. Both DFE firmware versions (Gold and Platinum/Diamond) are built from the same source code and offer the same security functionality; however, the DFE Gold software does not support all of the switching and routing features of the Platinum/Diamond version. Both DFEs are supported in any of the 4 chassis types and are designed to ensure a high Quality of Service for critical applications. The specific functionality for each appliance is enforced primarily through the runtime software image installed on each platform, and minor hardware changes to support scale and capacity objectives for each. The following figure outlines the differences between the Gold, Diamond and Platinum series appliances:

## Matrix™ N-Series DFE Comparison



		GOLD	PLATINUM	DIAMOND
 <p><b>Diamond (7R Series)</b></p>  <p><b>Platinum (7 Series)</b></p>  <p><b>Gold (4 Series)</b></p>	Interface Types	Edge	Edge, Dist and Core	Distribution and Core
	Performance (Module/System Maximum)	6.5/45.5 Mpps	13.5/94.5 Mpps	13.5/94.5 Mpps
	High Availability	1+1 (optional)	Optimized N:6	Optimized N:6
	Policy-based, Flow Switching	Yes	Yes	Yes (Double Platinum Capacity)
	Advanced QoS/Rate Limiting/Mirroring Features	No	Yes	Yes
	Authentication/Policy Services	Single User/ Per Port	Multi-User/ Per Port	Multi-User/ Per Port
	Basic and Advanced (optional) Routing	Basic	Advanced (via license)	Advanced
	Legacy Matrix E7 chassis support	Yes	Yes	Yes
	1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> Gen Modules Interoperability	No	Yes	Yes

©2007 Enterasys Networks, Inc. All rights reserved.

7

Figure 2 - Matrix N-Series DFE Comparison

There is considerable variation in hardware configuration even within a single member of the Matrix N product family. The Matrix N product family consists of the following units.

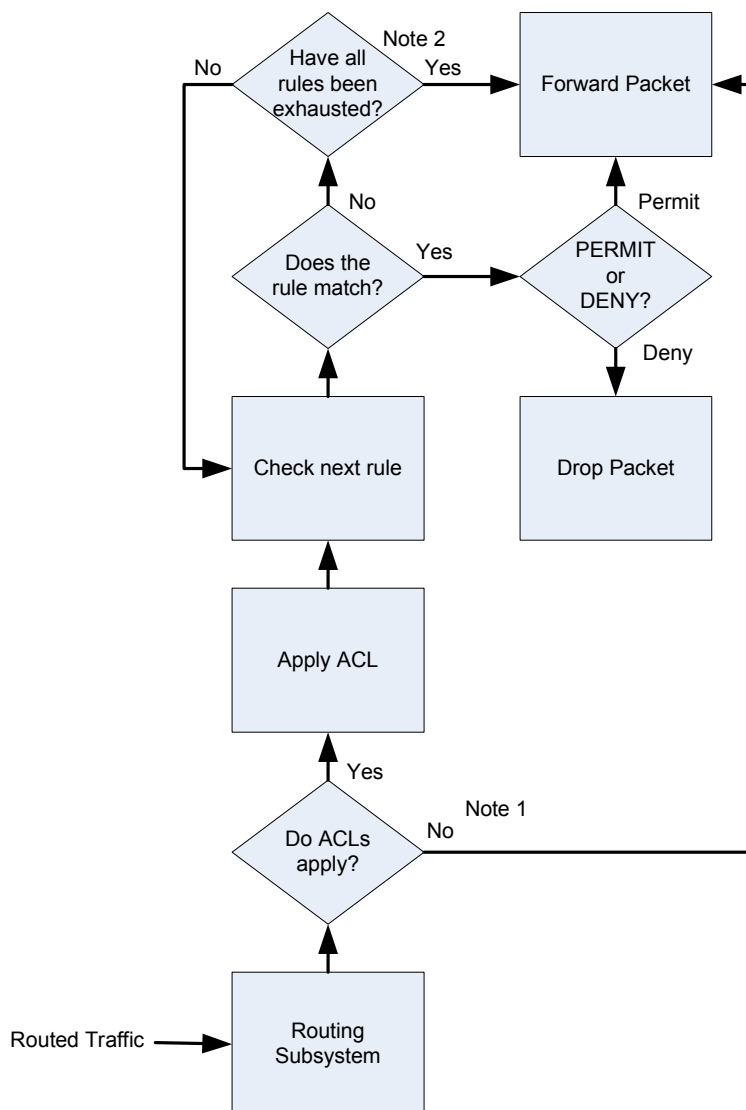
- The Matrix N1 is a single-slot chassis for flexible deployment in all environments.
- The Matrix N3 is a three-slot chassis for small to medium-size networks.
- The Matrix N5 is a modular five-slot chassis with an integrated Power-over-Ethernet (POE) power shelf.
- The Matrix N7 is a modular seven slot chassis for high-density environments.
- The Matrix N-Standalone provides a single blade.

### 2.2.2 Application of Policy

The Enterasys Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 architecture supports the action of either switching a packet or routing a packet. The Matrix X and Matrix N Switch Routers have fully distributed switch management and route processing capabilities, where each module is individually driven and managed by on-board processors. Routing and switching

functionality is provided by a combination of software running on microprocessors and Application Specific Integrated Circuits (ASICs) hardware. Each module maintains its own switching, routing, and network management information. The Matrix X and Matrix N Switch Router backplane is a point-to-point matrix design with fully meshed links between modules to provide scalability and performance. In this architecture, layer 3 Access Control Lists (ACLs) are applied to packets being routed by the device. These packets are referred to as “routed traffic” in this document. Figure 3 shows the application of policy in the TOE.

A packet is considered to be routed traffic if the Media Access Control (MAC) Destination Address (DA) is the same as the MAC DA of the Matrix X or Matrix N device. Otherwise, it is considered non-routed traffic. ACLs are applied by the Routing Subsystem.



**Figure 3 – Forwarding Process Flow Chart<sup>12</sup>**

### 2.2.2.1 Routing Access Control

ACLs are applied to logical, Layer 3 capable interfaces. No more than one ACL may be applied to each ingress or egress interface; however, each ACL may contain up to 999 rules. For the purposes of this evaluation, only the ACL applied to the inbound interface is being considered.

The Routing Subsystem receives the incoming packet, determines which ACL applies to the applicable logical Layer 3 interface, and applies the ACL. As indicated in Footnote 1, there will always be ACLs for all inbound

<sup>1</sup> In the evaluated version, ACLs will always apply.

<sup>2</sup> In the evaluated version, a “DENY All” rule is included as the final rule in the ACL. This causes any packet that has not matched a PERMIT rule to be dropped.

interfaces in the evaluated configuration of the TOE. Rules in an ACL are order dependent. An incoming packet is checked against each rule in the ACL until a rule is matched. At that point, the packet is either forwarded (if the matching rule is a PERMIT rule) or dropped (if the matching rule is a DENY rule). In the CC evaluated version an implicit “DENY All” rule is included at the end of every ACL. Therefore, as indicated in Footnote 2, in the evaluated configuration a packet will not be forwarded simply because none of the rules matched.

### 2.2.2.2 Switching Policy

Non-routed traffic may be dropped, or may be switched in the Switching Subsystem. Although policy may also be applied before the packet is switched, no claims are made with respect to this functionality.

## 2.3 TOE Boundaries and Scope

This section will detail the physical and logical components of the Matrix X and Matrix N Switch Router to be included in the evaluation.

### 2.3.1 Physical Boundary

Figure 4 illustrates the physical scope and the physical boundary of the overall solution and shows how the TOE fits together with the components that constitute the TOE Environment.

The TOE is the Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 software. These software images run on the Matrix X and Matrix N hardware devices listed in Section 2.2.1 above. The TOE may be installed on a network wherever routing and switching services are required. This may be at the edge of the internal network, as part of a backbone, or as part of a data center. The TOE is supported in the TOE environment by the Operating System (OS) and Matrix X and Matrix N Switch Router hardware. The OS for the Matrix X is an embedded Linux system; the OS for the Matrix N is VxWorks v5.5.1. The version of the imbedded Linux is Monta Vista Linux v3.1 with Linux kernel v2.4.20. The TOE Environment also includes a Management Console for managing the TOE.

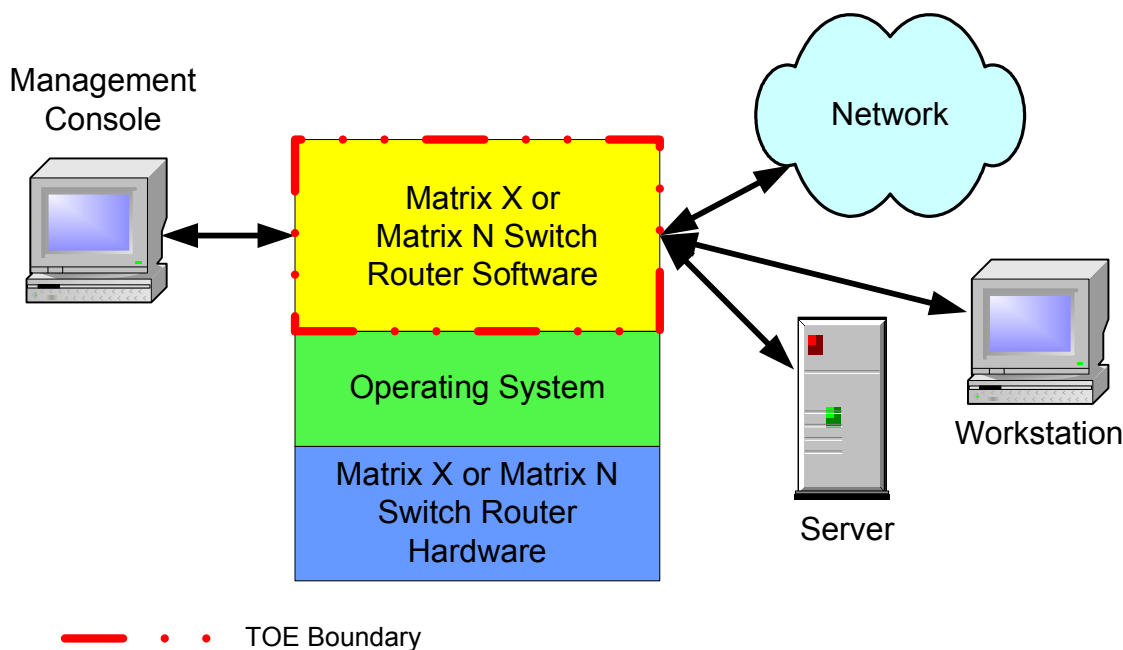


Figure 4 - Physical TOE Boundary

## 2.3.2 Logical Boundary

The security functional requirements implemented by the TOE are grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

### 2.3.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage and viewing of audit records. Audit logs contain user login information and changes to specified ACL rules. Logs are generated and stored within the TOE.

### 2.3.2.2 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting user data. This functionality is provided by the application of ACLs for routed traffic.

### 2.3.2.3 Identification and Authentication

The Identification and Authentication function provides functionality to establish and verify a claimed user identity. This ensures that the user has the appropriate privileges associated with the assigned role. The TOE supports internally enforced username and password based authentication. Password strength rules are also enforced by the TOE.

### 2.3.2.4 Security Management

The Security Management function specifies the management of several aspects of the TOE Security Function (TSF), including security function behaviour and TSF data. The various management roles are also specified here.

### 2.3.2.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features. These features include identification, authentication, and access control mediation. The TOE is separated from other processes by the operating system.

## 2.3.3 Excluded Features and Functionality

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Telnet access to the Command Line Interface (CLI)
- Authentication mechanisms other than local authentication
  - Remote Authentication Dial In User Service (RADIUS)
  - Terminal Access Controller Access-Control System Plus (TACACS+)
  - Request for Comment (RFC) 3580
  - 802.1X authentication
  - Port Web Authentication
  - MAC Authentication
  - Multiple Authentication

- WebView Management
- NetSight Manager
- Simple Network Management Protocol (SNMP) v1/v2 (i.e. SNMP must be used with v3 security features)
- Dynamic Host Configuration Protocol (DHCP)

In addition, all SNMP users must be configured with read-only access in the evaluated configuration of the TOE.

### 3 Security Environment

This section describes the security aspects of the environment where the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects
- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply

#### 3.1 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

**Table 2 - Assumptions**

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the security configuration required to allow the TOE to provide the administrator-intended secure routing and switching functions while connected to the network environment.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.



A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
----------	---

## 3.2 Threats to Security

This section identifies the threats to the Information Technology (IT) assets. Protection from these threats is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE administrative users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data transitioning through the TOE and the entities to which routed traffic is sent. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The applicable threats are shown in Table 3.

**Table 3 - Threats**

Name	Description
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.

## 3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section describes the organizational security policies with which the TOE must comply. Table 4 details the applicable organizational security policies.

**Table 4 – Organizational Security Policies**

Name	Description
P.MANAGE	The TOE may only be managed by authorized users.
P.INTEGRITY	Data collected and produced by the TOE must be protected from modification.
P.TRAFFIC_FLOW	The TOE must route data in accordance with the implemented security policy.

## 4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment to meet the TOE's security needs.

### 4.1 Security Objectives for the TOE

Table 5 shows the specific security objectives for the TOE.

**Table 5 – TOE Security Objectives**

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.
O.TRAFFIC	The TOE must route or switch traffic only as defined by the access control SFP.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.

### 4.2 Security Objectives for the Environment

#### 4.2.1 IT Security Objectives

Table 6 shows the IT security objectives for the TOE environment.

**Table 6 – Security Objectives for the TOE Environment**

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.BYPASS	The TOE environment must ensure that the TSF cannot be bypassed.

#### 4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures. Table 7 shows the non-IT security objectives for the TOE environment.

**Table 7 – Non-IT Security Objectives**

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.TRAFFIC	The TOE environment must be implemented to provide the TOE with a connection that allows legitimate network traffic to reach the TOE while denying malicious network traffic that could exploit TOE vulnerabilities while the TOE is connected.

--	--

## 5 Security Requirements

This section defines the SFRs and SARs met by the TOE, as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

### 5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

**Table 8 - TOE Security Functional Requirements**

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓	✓	
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss		✓	✓	
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_SOS.1	Verification of secrets		✓	✓	
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1(a)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1(b)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1(c)	Management of security functions behaviour	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		

---

FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1(a)	Non-bypassability of the TSP				✓

*Note: S=Selection; A=Assignment; R=Refinement; I=Iteration*

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

## 5.1.1 Class FAU: Security Audit

### FAU\_GEN.1 Audit Data Generation

**Hierarchical to: No other components.**

#### FAU\_GEN.1.1

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events, for the *[not specified]* level of audit;
- c) *[Successful and unsuccessful use of authentication mechanisms, except SNMP access on the Matrix X and successful use of SNMP authentication mechanisms on the Matrix N are not logged;*

*The reaching of the threshold for the unsuccessful authentication attempts and the actions taken;*

*Modification to the group of users that are associated with a role; and*

*Changes to the time.]*

#### FAU\_GEN.1.2

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

- a) Date and time of the event, type of event, subject identity (**except for startup and shutdown**), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *[no other audit relevant information]*.

**Dependencies:** FPT\_STM.1 Reliable time stamps

### FAU\_SAR.1 Audit review

**Hierarchical to: No other components.**

#### FAU\_SAR.1.1

The TSF shall provide *[Super-Users, Read-Write Users and Read-Only Users]* with the capability to read *[all audit information stored in the audit buffer]* 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.

**Dependencies:** FAU\_GEN.1 Audit data generation



## **FAU\_STG.1 Protected audit trail storage**

**Hierarchical to: No other components.**

### **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 audit records in the audit trail.

**Dependencies: FAU\_GEN.1 Audit data generation**

## **FAU\_STG.4 Prevention of audit data loss**

**Hierarchical to: FAU\_STG.3**

### **FAU\_STG.4.1**

The TSF shall [*overwrite the oldest instance of stored audit records*] if the audit trail is full.

**Dependencies: FAU\_STG.1 Protected audit trail storage**

## 5.1.2 Class FDP: User Data Protection

### FDP\_ACC.1 Subset access control

**Hierarchical to: No other components.**

#### FDP\_ACC.1.1

The TSF shall enforce the [*access control SFP*] on [*routed traffic*].

**Dependencies: FDP\_ACF.1 Security attribute based access control**

### FDP\_ACF.1 Security attribute based access control

**Hierarchical to: No other components.**

#### FDP\_ACF.1.1

The TSF shall enforce the [*access control SFP*] to objects based on the following:

[*SUBJECT (packet) attributes:*

- 1) *source Internet Protocol (IP) address,*
- 2) *destination IP address,*
- 3) *protocol,*
- 4) *Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) source port number, and*
- 5) *TCP/UDP destination port number; and*

[*OBJECT (network resource) attributes:*

- 1) *IP address, and*
- 2) *Port number.]*

#### FDP\_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*PERMIT and DENY rules contained in the Access Control List*].

#### FDP\_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no other rules*].

#### FDP\_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*no other rules*].

**Dependencies:** FDP\_ACC.1 Subset access control  
FMT\_MSA.3 Static attribute initialization

### 5.1.3 Class FIA: Identification and Authentication

#### **FIA\_AFL.1 Authentication failure handling**

**Hierarchical to:** No other components.

##### **FIA\_AFL.1.1**

The TSF shall detect when [*an administrator configurable positive integer within [1 to 10]*] unsuccessful authentication attempts occur related to [*remote login to the Command Line Interface*].

##### **FIA\_AFL.1.2**

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*lock the Read-Write User and Read-Only User out until re-enabled by a Super-User, and lock the Super-User out for a configurable period of time between 1 and 60 minutes*].

**Dependencies:** FIA\_UAU.1 Timing of authentication

#### **FIA\_SOS.1 Verification of secrets**

**Hierarchical to:** No other components.

##### **FIA\_SOS.1.1**

The TSF shall provide a mechanism to verify that ~~secrets meet~~ **passwords must be** [*at least 8 characters in length*].

**Dependencies:** No dependencies

#### **FIA\_UAU.2 User authentication before any action**

**Hierarchical to:** FIA\_UAU.1

##### **FIA\_UAU.2.1**

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

**Dependencies:** FIA\_UID.1 Timing of identification

#### **FIA\_UID.2 User identification before any action**

**Hierarchical to:** FIA\_UID.1

##### **FIA\_UID.2.1**

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

**Dependencies:** No dependencies

## 5.1.4 Class FMT: Security Management

### FMT\_MOF.1(a) Management of security functions behaviour

**Hierarchical to:** No other components.

#### FMT\_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*routing functionality, policy configuration and auditing configuration*] to [*Super-Users and Read-Write Users*].

**Dependencies:** FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

### FMT\_MOF.1(b) Management of security functions behaviour

**Hierarchical to:** No other components.

#### FMT\_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*of administering CLI user accounts*] to [*Super-Users*].

**Dependencies:** FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

### FMT\_MOF.1(c) Management of security functions behaviour

**Hierarchical to:** No other components.

#### FMT\_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*of administering the SNMP system*] to [*Super-Users and Read-Write Users (Read-Write for Matrix N only)*].

**Dependencies:** FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

### FMT\_MTD.1 Management of TSF data

**Hierarchical to:** No other components.

#### FMT\_MTD.1.1

The TSF shall restrict the ability to [See Table 9 below] the [list of TSF data – See Table 9 below] to [the authorised identified roles – See Table 9 below].

**Table 9 - Management of TSF Data**

Roles \ TSF Data	Super-User	Read-Write User	Read-Only User
Routing Configuration Data	Query Modify	Query Modify	Query
Routing Policy Data	Query Modify	Query Modify	Query
Auditing Parameters	Query Modify	Query Modify	Query
Audit Data	Query Modify Delete	Query Modify Delete (Matrix N only)	Query
User Account Data	Query Modify	Query (minimal information)	Query (minimal information)
Passwords	Modify	Modify (own password only)	Modify (own password only) (Matrix N only)
SNMP Configuration Data	Query Modify	Query  Modify (Matrix N only)	Query

**Dependencies:** FMT\_SMR.1 Security roles  
FMT\_SMF.1 Specification of Management Functions

### **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: [TSF data management and security function management].

**Dependencies:** No Dependencies

### **FMT\_SMR.1 Security roles**

**Hierarchical to:** No other components.

**FMT\_SMR.1.1**

The TSF shall maintain the roles [*Read-Only User, Read-Write User, and Super-User*].

**FMT\_SMR.1.2**

The TSF shall be able to associate users with roles.

**Dependencies: FIA\_UID.1 Timing of identification**

## 5.1.5 Class FPT: Protection of the TSF

### **FPT\_RVM.1(a) Non-bypassability of the TSP**

**Hierarchical to: No other components.**

#### **FPT\_RVM.1.1**

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC<sup>3</sup> is allowed to proceed.

**Dependencies: No dependencies**

---

<sup>3</sup> TSF Scope of Control

## 5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated SFRs for the IT Environment of the TOE presented in this section have been drawn from Part 2 of CC Version 2.3 and are hence conformant to CC Version 2.3 Part 2. Table 10 shows the SFRs for the environment.

**Table 10 – Security Functional Requirements for the Environment**

<i>Name</i>	<i>Description</i>	<i>S</i>	<i>A</i>	<i>R</i>	<i>I</i>
<i>FPT_SEP.1</i>	<i>TSF domain separation</i>			✓	
<i>FPT_STM.1</i>	<i>Reliable time stamps</i>			✓	
<i>FPT_RVM.1(b)</i>	<i>Non-bypassability of the TSP</i>			✓	✓

*Note: S=Selection; A=Assignment; R=Refinement; I=Iteration*

Section 5.2.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations, please refer to Section 1.3.1.

### 5.2.1 Class FPT: Protection of the TOE Environment

#### **FPT\_RVM.1(b) Non-bypassability of the TSP**

**Hierarchical to: No other components.**

##### **FPT\_RVM.1.1**

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

Dependencies: No dependencies

#### **FPT\_SEP.1 TSF domain separation**

**Hierarchical to: No other components.**

##### **FPT\_SEP.1.1**

The ~~TSF~~ **TOE Environment** shall maintain a security domain for ~~its own~~ the TOE's execution that protects it from interference and tampering by untrusted subjects.

##### **FPT\_SEP.1.2**

The ~~TSF~~ **TOE Environment** shall enforce separation between the security domains of subjects in the TSC.

**Dependencies: No dependencies**



## FPT\_STM.1 Reliable time stamps

**Hierarchical to: No other components.**

### FPT\_STM.1.1

The ~~TSF~~ **TOE Environment** shall be able to provide reliable time stamps for ~~its own~~ **the TOE's** use.

**Dependencies: No dependencies**

## 5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL 3 augmented with ALC\_FLR.1. Table 11 summarizes the requirements.

**Table 11 – Assurance Requirements**

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC : Life Cycle Support	ALC_FLR.1 Basic flaw remediation
	ALC_DVS.1 Identification of Security Measures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

## 6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

### 6.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 12 shows the mapping of each TSF to its SFRs.

**Table 12 – Mapping of TOE Security Functions to Security Functional Requirements**

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Security Management	FMT_MOF.1(a)	Management of security functions behaviour
	FMT_MOF.1(b)	Management of security functions behaviour
	FMT_MOF.1(c)	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data

	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Protection of TOE Security Functions	FPT_RVM.1(a)	Non-bypassability of the TSP

### 6.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. In order to provide evidence of security-relevant events, the TOE records administrative user access to the TOE, including unsuccessful attempts and user lockout. Modification of users and roles, and changes to the time are also logged. All audit records contain the date, time, event type, subject identity (except for startup and shutdown), and the outcome of the event.

All of the logs are stored locally within the device. TOE users must authenticate in order to gain access to read the audit records. TOE users may add information to the audit logs to aid in debugging; however, they may not alter

audit records. Only authorized users may delete audit records. TOE users in any of the roles may view the audit logs.

On the Matrix N, there are two log files per blade. Each log file can be up to 256 kilobytes.

On the Matrix X, there is one main log file that named syslog.log. After a log file becomes full, it is compressed and archived with the name syslog.log.1.gz. There can be up to 50 compressed log files, named syslog.log.[1-50].gz. After the last archived log file becomes full, the last ten compressed log files are deleted to make space for additional logs.

When the audit becomes full, the TOE ensures that the oldest audit file is overwritten.

The TOE audit records contain the information shown in Table 13.

**Table 13 – Audit Record Contents**

Field	Content
Date	The date is shown in the format mmm dd.
Time	Time is displayed as hh:mm:ss.
Application (Type of Event)	This is the internal function or module that generated the entry.
Severity	This is the severity of the event.
Subject	If applicable, the subject identity is displayed.
Outcome	This is a description of the event.

**TOE Security Functional Requirements Satisfied:** FAU\_GEN.1, FAU\_SAR.1, FAU\_STG.1 and FAU\_STG.4.

### 6.1.2 User Data Protection

The Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 architecture supports the action of either switching a packet or routing a packet. User Data Protection is provided by the application of ACLs for routed data. If the MAC DA indicated in the packet is the same as the MAC DA of the Matrix X or Matrix N Switch Router, it is routed data and is subject to the application of ACLs. All other data is non-routed traffic, and may be sent to the Switching Subsystem for processing, or may be discarded.

ACLs are applied to logical, Layer 3 capable interfaces. The rules in an ACL allow the packet to be forwarded or dropped based on source and destination IP address, source and destination port number and protocol. An incoming packet is checked against each rule in the ACL until a rule is matched. At that point, the packet is either forwarded (if the matching rule is a PERMIT rule), or dropped (if the matching rule is a DENY rule). In the CC evaluated version, an implicit “DENY all” rule is included at the end of every ACL to ensure that packets not specifically permitted, are denied.

This functionality enforces the access control SFP on packets passing through the TOE.

**TOE Security Functional Requirements Satisfied:** FDP\_ACC.1, and FDP\_ACF.1.

### 6.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE user requesting a service is identified and authenticated by providing a valid username and password. For each user, the TOE maintains the username,

password, and privilege level. When the TOE user enters a username and password, the user is authenticated by the TOE and allowed to perform functions and view data as appropriate for the privilege level.

The TOE supports internally enforced username and password-based authentication. Password strength rules are enforced at password creation to ensure that passwords are at least eight characters long. The TOE detects unsuccessful authentication attempts made using the CLI with Secure Shell (SSH). After a configurable number of unsuccessful authentication attempts, the TOE will lock out a Read-Write or Read-Only user until re-enabled by a Super-User, and lock out a Super-User for a configurable period of time. TOE administrative functions and data are not available to users prior to identification and authentication.

The TOE also provides username and password-based authentication through the SNMP Interface. Password strength rules are enforced at password creation to ensure that passwords are at least eight characters long. SNMP data are not available to users prior to identification and authentication. For the evaluated configuration of the TOE, all SNMP users must have Read-Only access.

The Strength of Function (SOF)-basic claim applies to the identification and authentication security functions of the CLI and the SNMP Interface. Passwords are case-sensitive and must meet the following requirement:

- Passwords must be greater than or equal to eight characters long.

In addition, the TOE must be configured according to the following requirements:

- Users are locked out after a configurable number of unsuccessful authentication attempts. The number is configurable between 1 and 10.
- Read-Only and Read-Write users must be re-enabled by a Super-User. Super-Users are locked out for a configurable period of time between 1 and 60 minutes.

Furthermore, users in this instance are TOE administrators. Since TOE administrators are assumed to be competent and non-hostile, they shall not choose passwords that can be easily guessed or cracked, such as the user ID, “aaaaaaa”, or “qwertyui”.

**TOE Security Functional Requirements Satisfied:** FIA\_AFL.1, FIA\_SOS.1, FIA\_UAU.2 and FIA\_UID.2.

## 6.1.4 Security Management

The TOE maintains three user roles for managing the Matrix X and Matrix N Switch Router: Super-User, Read-Write User and Read-Only User. Users in the Super-User role may delete audit data (as well as Read-Write users on the Matrix N only). Users in the Super-User and Read-Write User roles may query and modify routing configuration data, policy data, and auditing parameters. Users in the Read-Only User role may view this data. All users may view the audit data stored in the audit buffer.

Only users in the Super-User and the Read-Write User roles are able to manage the behaviour of the security functions. Users in these roles are able to make modifications to ACLs such as:

- Creating, deleting and modifying ACLs and policies
- Applying ACLs and policies to particular interfaces
- Adding, removing, and modifying the rules within the ACLs

Only users in the Super-User role may administer user accounts. Super-Users (and Read-Write Users on the Matrix N only) configure SNMP users through the CLI. All users accessing the TOE through the SNMP Interface must be configured as Read-Only for the evaluated configuration of the TOE.

**TOE Security Functional Requirements Satisfied:** FMT\_MOF.1(a), FMT\_MOF.1(b), FMT\_MOF.1(c), FMT\_MTD.1, FMT\_SMF.1 and FMT\_SMR.1.

### 6.1.5 Protection of the TSF

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. It is not possible to perform any actions on the system without successfully authenticating. Once a user has been authenticated, that user is bound to the appropriate privileges defined by the TOE. For any user to perform a TOE operation, a user in the Super-User role must have granted that user the rights to perform that operation. These privileges are granted on a per operator basis. Since all access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each operator, the TSF maintains separation between users. As an example, if a user in the Read-Only role attempts to edit a policy, the command will result in an error.

**TOE Security Functional Requirements Satisfied:** FPT\_RVM.1(a).

## 6.2 TOE Security Assurance Measures

EAL 3+ was chosen to provide a moderate level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL 3+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

**Table 14 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)**

Assurance Component	Assurance Measure
ACM_CAP.3 ACM_SCP.1	Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 - Configuration Management Plan: Capabilities, Scope
ADO_DEL.1	Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 - Secure Delivery

Assurance Component	Assurance Measure
ADO_IGS.1	<p>Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, and Matrix N, DFE Diamond Enterasys Networking System v6.01 - Common Criteria Administrative Guide Supplement</p> <p>Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Common Criteria Administrative Guide Supplement</p> <p>Enterasys Matrix N1 7C111 Single-Slot Chassis Hardware Installation Guide (P/N 9034137-03)</p> <p>Enterasys Matrix N3 7C103 Chassis Hardware Installation Guide (P/N 9033824-05)</p> <p>Enterasys Matrix N5 POE (7C105-P) Chassis Hardware Installation Guide (P/N 9033943-03)</p> <p>Enterasys Matrix N7 7C107 Chassis Hardware Installation Guide (P/N 9033851-05)</p> <p>Enterasys Matrix N Series N-POE Power System Installation Guide (P/N 9033952-05)</p> <p>Enterasys Matrix X Secure Core Router X4-C Chassis Installation Guide (P/N 9034084-02)</p> <p>Enterasys Matrix X X8-C Secure Core Router X8-C Chassis Installation Guide (P/N 9034083-03)</p> <p>Enterasys Matrix X Secure Core Router X16-C Chassis Installation Guide (P/N 9034082-04)</p>
ADV_FSP.1 ADV_HLD.2 ADV_RCR.1	<p>Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 - Development: Functional Specification, High Level Design, Representation Correspondence</p> <p>Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Development: Functional Specification, High Level Design, Representation Correspondence</p>
AGD_ADM.1 AGD_USR.1	<p>Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, and Matrix N, DFE Diamond Enterasys Networking System v6.01 - Common Criteria Administrative Guide Supplement</p> <p>Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Common Criteria Administrative Guide Supplement</p> <p>Enterasys Matrix DFE-Gold Series Configuration Guide Firmware Version 6.01.xx (P/N 9033933-13)</p> <p>Enterasys Matrix DFE-Platinum and Diamond Series Configuration Guide Firmware Version 6.01.xx (P/N 9033800-16)</p> <p>Enterasys Networks, Inc. Enterasys Matrix N Standalone (NSA) Series Configuration Guide Firmware Version 6.01.xx (P/N 9034073-10)</p> <p>Enterasys Matrix X Secure Core Router Command Line Interface Reference Guide Firmware Version 1.6.x (P/N 9034085-06)</p> <p>Enterasys Matrix X Secure Core Router Configuration Guide Firmware Version 1.6.x (P/N 9034086-06)</p>
ALC_DVS.1 ALC_FLR.1	<p>Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, Matrix N, DFE Diamond Enterasys Networking System v6.01 and Matrix X Enterasys Networking System v1.6.4P4 - Life Cycle Support : Development Security, Flaw Remediation</p>

Assurance Component	Assurance Measure
ATE_COV.2 ATE_DPT.1 ATE_FUN.1	Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, and Matrix N, DFE Diamond Enterasys Networking System v6.01 - Testing: Coverage, Depth  Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Testing: Coverage, Depth
AVA_MSU.1 AVA_SOF.1 AVA_VLA.1	Enterasys Networks, Inc. Matrix N, DFE Gold Enterasys Networking System v6.01, Matrix N, DFE Platinum Enterasys Networking System v6.01, and Matrix N, DFE Diamond Enterasys Networking System v6.01 - Vulnerability Assessment  Enterasys Networks, Inc. Matrix X Enterasys Networking System v1.6.4P4 - Vulnerability Assessment

### 6.2.1 ACM\_CAP.3, ACM\_SCP.1: Configuration Management Document

The Configuration Management (CM) document is made up of ACM\_CAP.3, Authorisation controls and ACM\_SCP.1 TOE CM coverage and provides a description of the various tools used to control the configuration items and how they are used internally at Enterasys. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. The list of configuration items includes implementation representation and the evaluation evidence required by the assurance components in the ST. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation includes a Configuration Management Plan, which details the Configuration Management System and how the TOE configuration items are controlled by that system.

### 6.2.2 ADO\_DEL.1: Delivery and Operation Document

The Delivery and Operation document contains ADO\_DEL.1 Delivery procedures and provides a description of the secure delivery procedures implemented by Enterasys to protect against TOE modification during product delivery. The installation documentation provided by Enterasys details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The installation documentation provides guidance to the TOE Users on configuring the TOE and how those TOE configurations affect the TSF.

### 6.2.3 ADO\_IGS.1: Installation Guidance

The installation guidance documents provide the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

### 6.2.4 ADV\_FSP.1, ADV\_HLD.2, ADV\_RCR.1: Development Documentation

The Enterasys design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Informal Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The Security Enforcing High-level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. It describes the purpose and method of use of all interfaces to the subsystems of the TSF, and provides details of effects, exceptions and error messages, as appropriate. The High-level Design identifies the basic structure of the TSF, the major elements, provides a listing of all interfaces, and describes the purpose and method of use for each interface.



- The Informal Correspondence Demonstration shows the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the high-level design.

### **6.2.5 AGD\_ADM.1, AGD\_USR.1: Guidance Documents**

The AGD\_ADM.1 Administrator Guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The AGD\_USR.1 User Guidance documentation directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised. There is no user guidance supplied for the evaluated TOE, as all guidance is intended for the Administrator.

### **6.2.6 ALC\_DVS.1, ALC\_FLR.1: Life Cycle Support**

The Life Cycle Support documentation is made up of the ALC\_DVS.1 Identification of Security Measures and ALC\_FLR.1 Basic flaw remediation. The ALC\_DVS.1 document describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. It provides evidence that these security measures are followed during the development and maintenance of the TOE. The Basic flaw remediation document includes procedures addressed to TOE developers, and the established procedures for accepting and acting upon all reports of security flaws and requests for corrections of those flaws are provided. The documentation also describes the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

### **6.2.7 ATE\_COV.2, ATE\_DPT.1, ATE\_FUN.1: Testing**

There are a number of components that make up the Test documentation. The ATE\_COV.2 Analysis of coverage demonstrates that testing is performed against the functional specification, and that the tests identified in the test documentation are complete. The Analysis of coverage demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement ATE\_FUN.1 Functional testing. ATE\_DPT.1 Testing: high level design demonstrates that the identified tests are sufficient to demonstrate that the TSF operates in accordance with the high-level design.

### **6.2.8 AVA\_MSU.1, AVA\_SOF.1, AVA\_VLA.1: Vulnerability Assessment**

AVA\_MSU.1 Examination of guidance investigates whether the TOE can be configured or used in a manner that is insecure, but that would appear to be secure to a TOE administrator or user. The guidance documentation is provided to demonstrate that the TOE can be configured and used securely using only the supplied guidance documentation.

The AVA\_SOF.1 Strength of TOE security function evaluation demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE. The analysis shows how the TOE meets or exceeds the minimum SOF requirements for each mechanism.

The AVA\_VLA.1 Developer vulnerability analysis is provided to demonstrate ways in which an entity could violate the TOE Security Policy (TSP). Additionally, this document provides a list of identified vulnerabilities and evidence of how the TOE is resistant to obvious attacks.

## 7 Protection Profile Claims

This section provides the identification and justification for any PP conformance claims.

### 7.1 Protection Profile Reference

There are no PP claims for this security target.

## 8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, threats, and organizational security policies. In particular it shows that the security requirements are suitable to meet the security objectives, which are in turn shown to be suitable to cover all aspects of the TOE security environment.

### 8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ST. The tables in Section 8.1 demonstrate the mapping between the assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

#### 8.1.1 Security Objectives Rationale Relating to Threats

**Table 15 – Security Objectives Rationale Relating to Threats**

Threats	Objectives	Rationale
<p>T.MASQUERADE</p> <p>A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.</p>	<p>O.AUTHENTICATE</p> <p>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.</p>	<p>By ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE mitigates this threat.</p>
<p>T.TAMPERING</p> <p>A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.</p>	<p>O.AUDIT</p> <p>The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.</p>	<p>The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.</p>
	<p>O.ADMIN</p> <p>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.</p>	<p>O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.</p>
	<p>O.PROTECT</p> <p>The TOE must ensure the integrity of audit and system data by protecting</p>	<p>O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized</p>

	<p>itself from unauthorized modifications and access to its functions and data.</p>	<p>modification.</p>
	<p>OE.PROTECT</p> <p>The TOE environment must protect itself and the TOE from external interference or tampering.</p>	<p>OE.PROTECT ensures that the TOE is protected from external interference or tampering.</p>
	<p>OE.BYPASS</p> <p>The TOE environment must ensure that the TSF cannot be bypassed.</p>	<p>The objective OE.BYPASS ensures that the TSF cannot be bypassed.</p>
<p>T.UNAUTH</p> <p>A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.</p>	<p>O.AUDIT</p> <p>The TOE must record events of security relevance at the “not specified level” of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.</p>	<p>The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.</p>
	<p>O.ADMIN</p> <p>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.</p>	<p>The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.</p>
	<p>O.AUTHENTICATE</p> <p>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.</p>	<p>The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.</p>

### 8.1.2 Security Objectives Rationale Relating to Assumptions

Table 16 – Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.INSTALL	OE.PLATFORM	OE.PLATFORM ensures that the TOE

The TOE is installed on the appropriate, dedicated hardware and operating system.	The TOE hardware and OS must support all required TOE functions. OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	hardware and OS supports the TOE functions. Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.NETCON The TOE environment provides the security configuration required to allow the TOE to provide the administrator-intended secure routing and switching functions while connected to the network environment.	OE.TRAFFIC The TOE environment must be implemented to provide the TOE with a connection that allows legitimate network traffic to reach the TOE while denying malicious network traffic that could exploit TOE vulnerabilities while the TOE is connected.	OE.TRAFFIC satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

Table 17 – Security Objectives Rationale Relating to Policies

Policies	Objectives	Rationale
P.MANAGE The TOE may only be managed by authorized users.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the	O.ADMIN ensures that the TOE provides the necessary tools to support the P.MANAGE policy.

	appropriate privileges and only those TOE users, may exercise such control.	
	<p>O.AUTHENTICATE</p> <p>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.</p>	<p>O.AUTHENTICATE ensures that only authorized users are granted access to the tools required to manage the TOE.</p>
<p>P.INTEGRITY</p> <p>Data collected and produced by the TOE must be protected from modification.</p>	<p>O.PROTECT</p> <p>The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.</p>	<p>O.PROTECT ensures that the TOE protects audit and system data to meet this policy.</p>
<p>P.TRAFFIC_FLOW</p> <p>The TOE must route data in accordance with the implemented security policy.</p>	<p>O.AUDIT</p> <p>The TOE must record events of security relevance at the “not specified level” of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.</p>	<p>The O.AUDIT objective ensures that security relevant events related to changes in the routing configuration are maintained, and may be reviewed by privileged users. This ensures that data is routed in accordance with policy.</p>
	<p>O.TRAFFIC</p> <p>The TOE must route or switch traffic only as defined by the access control SFP.</p>	<p>O.TRAFFIC ensures that traffic is routed only as dictated by the access control SFP, meeting the P.TRAFFIC_FLOW policy.</p>

## 8.2 Security Functional Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

### 8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

**Table 18 – SFR Rationale Related to TOE Objectives**

Objective	Requirements Addressing the Objective	Rationale
<p>O.AUDIT</p> <p>The TOE must record events of security relevance at the “not</p>	<p>FAU_GEN.1</p> <p>Audit Data Generation</p>	<p>The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details</p>

<p>specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.</p>		about the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data.
<p>O.TRAFFIC</p> <p>The TOE must route or switch traffic only as defined by the access control SFP.</p>	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that access control is applied to all packets before they are passed to the internal network.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces access control based on the implemented policy.
<p>O.ADMIN</p> <p>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.</p>	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that security attributes, including authentication failure thresholds, may only be changed by authorized users.
	FMT_MOF.1(a) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MOF.1(b) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MOF.1(c) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the

	Management of TSF data	user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUTHENTICATE  The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_AFL.1 Authentication failure handling	In order to ensure that users are properly authenticated prior to access, the TOE enforces a lockout after a configurable number of unsuccessful authentication attempts. The requirement for authentication failure handling meets the objective by mitigating the risk of a brute force attack on a username and password.
	FIA_SOS.1 Verification of secrets	The process that identifies and authenticates users also enforces a minimum password length of eight characters. This requirement meets the objective by mitigating the risk of a brute force attack on a username and password.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1(a) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MOF.1(b) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users



		may manage the security behaviour of the TOE.
	FMT_MOF.1(c ) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FPT_RVM.1(a) Non-bypassability of the TSP	The requirement meets the objective by ensuring that authentication functions succeed before users are able to access TSF management functions and data.
O.PROTECT  The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that no one may delete or alter information in the audit logs.
	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that the TOE protects itself by enforcing a lockout after a configurable number of unsuccessful authentication attempts.
	FIA_SOS.1 Verification of secrets	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized access by enforcing a minimum password length of eight characters.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.

	FMT_MOF.1(a) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MOF.1(b) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MOF.1(c) Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
	FPT_RVM.1(a) Non-bypassability of the TSP	The requirement meets the objective by ensuring that the security functions of the TOE must be invoked and succeed before the regular operation of the TOE may continue. The TOE does this by preventing unauthorized users from accessing TOE functions.

## 8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 19 – SFR Rationale Related to Objectives of the TOE Environment

Objective	Requirements Addressing the Objective	Rationale
OE.TIME The TOE environment must provide reliable timestamps to the TOE.	FPT_STM.1 Reliable time stamps	The OS provides timestamps to the TOE. The requirement meets the environmental objective by ensuring that the OS has reliable time through the use of NTP.

<p>OE.PROTECT</p> <p>The TOE environment must protect itself and the TOE from external interference or tampering.</p>	<p>FPT_SEP.1</p> <p>TSF domain separation</p>	<p>The requirement meets the environmental objective by ensuring that the TOE Environment, particularly the Matrix X and Matrix N hardware and associated OS, provide a security domain that protects the TOE from interference and tampering.</p>
<p>OE.PLATFORM</p> <p>The TOE hardware and OS must support all required TOE functions.</p>	<p>FPT_SEP.1</p> <p>TSF domain separation</p>	<p>The requirement meets the environmental objective by ensuring that the TOE Environment supports security domain separation by providing a dedicated environment for the execution of the TOE.</p>
	<p>FPT_STM.1</p> <p>Reliable time stamps</p>	<p>The requirement meets this objective by ensuring that the TOE maintains accurate timestamps obtained from the TOE environment for the TOE's audit records.</p>
<p>OE.BYPASS</p> <p>The TOE environment must ensure that the TSF cannot be bypassed.</p>	<p>FPT_RVM.1(b)</p> <p>Non-bypassability of the TSP</p>	<p>The requirement meets this objective by ensuring that the TSF cannot be bypassed.</p>

### 8.2.3 Rationale for Refinements of Security Functional Requirements

The following refinements of SFRs from CC version 2.3 have been made to clarify the content of the SFRs and to make them easier to read.

In Section 5.1.1, the words “(except for startup and shutdown)” have been added to FAU\_GEN.1.2 to provide a more accurate description of the audit record content. The audit records for startup and shutdown of the TOE do not contain a subject identity.

In Section 5.1.1, the words “instance of” have been added to FAU\_STG.4.1 to provide a more accurate description of how the logs are handled. The audit logs are held in distinct files and the oldest log file is overwritten when the audit trail is full.

In Section 5.1.3, FIA\_SOS.1.1 has been refined for clarity. The words “secrets meet” have been replaced by “passwords must be” to be more specific and for easier reading.

## 8.3 Security Assurance Requirements Rationale

EAL 3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software and hardware engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate for the threats defined for the environment. While the TOE may exist in a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed

to address threats that correspond with the intended environment. At EAL 3+, the TOE will incur a search for obvious flaws to support its introduction into the non-hostile environment.

## 8.4 Dependency Rationale

Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. Where a dependency is not met, the rationale is given.

**Table 20 - Functional Requirements Dependencies**

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	No	FMT_MSA.3 is not required because the security attributes used by the TOE are never given default attributes.
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_SOS.1	No dependencies		
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MOF.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

FMT_MOF.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MOF.1(c)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_RVM.1(a)	No dependencies		

## 8.5 TOE Summary Specification Rationale

### 8.5.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions works to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 21 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

Flaw remediation was included in order to provide assurance to TOE customers that a process is in place to handle flaws in the TOE after the TOE has been released.

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

**Table 21 - Mapping of Security Functional Requirements to TOE Security Functions**

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1	This implements appropriate audit records generation.
	FAU_SAR.1	This implements viewability for the audit records by authorized users.
	FAU_STG.1	This implements protection of the audit records from unauthorized modification.
	FAU_STG.4	This implements protection of the audit records appropriately when the space allocated to the audit records becomes close to exhaustion.
User Data Protection	FDP_ACC.1	This implements application of access control to specified functions.
	FDP_ACF.1	This SFR details the attributes on which the access control must be based.
Identification and Authentication	FIA_AFL.1	This implements the necessity for action to be taken on a configurable number of unsuccessful authentication attempts.
	FIA_SOS.1	This implements the necessity for passwords to be at least eight characters in length.
	FIA_UAU.2	This implements authentication of users before they are allowed access to the TSF.
	FIA_UID.2	This implements identification of users before they are allowed access to the TSF.
Security Management	FMT_MOF.1(a)	This implements the restriction of the ability to modify security functions to authorized users.
	FMT_MOF.1(b)	This implements the restriction of the ability to modify security functions to authorized users.
	FMT_MOF.1(c)	This implements the restriction of the ability to modify security functions to authorized users.
	FMT_MTD.1	This implements the restriction of the ability to modify security data to authorized users.
	FMT_SMF.1	This implements the ability of the TOE to perform specified security management functions.
	FMT_SMR.1	This requirement defines the roles used for access control.
Protection of the TSF	FPT_RVM.1(a)	This requirement ensures that the TSF may not be bypassed.

### 8.5.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL 3+ was chosen to provide a moderate level of independently assured security in the absence of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE may exist in a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs.

### 8.5.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control configuration items and a description of how they are used at Enterasys. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details that the TOE configuration items are effectively maintained under a configuration management system such that only authorized users may make changes to the configuration items.

Corresponding CC Assurance Components:

- Authorization controls
- TOE CM coverage

### 8.5.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Enterasys to protect against TOE modification during product delivery. The installation documentation provided by Enterasys details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The installation documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

### 8.5.2.3 Development

The Enterasys design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The high-level design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the high-level design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Security enforcing high-level design
- Informal Representation Correspondence

### 8.5.2.4 Guidance Documentation

The Enterasys guidance documentation provides administrator guidance on how to securely operate the TOE. The administrator guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use

the TSF privileges and protective functions. The guidance provided directs administrators on how to operate the TOE in a secure manner. Additionally, it explains the security functions and how they are to be used and explains the administrator's role in maintaining the TOE's Security.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance (not applicable)

#### **8.5.2.5 Life Cycle Support**

Life cycle support provides evidence of discipline and control in the processes of refinement of the TOE during its development and maintenance. The Enterasys development security documentation describes the physical, procedural, personnel and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Flaw remediation documentation describes the procedures used to track all reported security flaws in each release of the TOE.

Corresponding CC Assurance Components:

- Identification of security measures
- Basic flaw remediation

#### **8.5.2.6 Tests**

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Depth deals with the level to which the system has been tested. This area describes the testing of the high-level design of the TSF in terms of subsystems. Enterasys Test Plans and Test Procedures detail the overall testing efforts and break down the specific steps taken by a tester.

Corresponding CC Assurance Components:

- Evidence of Coverage and Depth
- Testing: high-level design
- Functional Testing

#### **8.5.2.7 Vulnerability Assessment**

The administrative guidance is examined to ensure that misleading, unreasonable and conflicting guidance is absent from the documentation, and that insecure states should be easy to detect. The developer vulnerability analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The strength of TOE security function evaluation demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Examination of guidance
- Strength of TOE security function evaluation
- Developer vulnerability analysis



## 8.6 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 3+ assurance requirements, this SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense (DoD) low robustness environments processing unclassified information.

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. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security function that has probabilistic or permutational functions is Identification and Authentication. The relevant security functional requirements that have probabilistic or permutational functions are FIA\_UAU.2 and FIA\_SOS.1. These SFRs and security function claim a strength of function rating of SOF-basic. This is consistent with the rating of SOF-basic claimed by the TOE.

## 9 Acronyms

**Table 22 - Acronyms**

Acronym	Definition
ACL	Access Control List
ASIC	Application Specific Integrated Circuits
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CM	Configuration Management
DA	Destination Address
DFE	Distributed Forwarding Engine
DoD	Department of Defense
EAL	Evaluation Assurance Level
IP	Internet Protocol
I/O	Input/Output
IT	Information Technology
MAC	Media Access Control
NTP	Network Time Protocol
OS	Operating System
POE	Power-over-Ethernet
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSC	TSF Scope of Control

Acronym	Definition
TSP	TOE Security Policy
UDP	User Datagram Protocol