Security Target

McAfee Network Data Loss Prevention 9.2

Document Version 1.1

March 8, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Network Data Loss Prevention 9.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Network Data Loss Prevention 9.2
ST Revision	1.1
ST Publication Date	March 8, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Network Data Loss Prevention 9.2
TOE Type	Data Loss Prevention

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1 (ISO/IEC 15408)
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
I&A	Identification & Authentication
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
MLOS	McAfee Linux Operating System
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
SF	Security Function
SFP	Security Function Policy

[1] Derived from the IDSPP

TERM	DEFINITION
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength Of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

The McAfee Network Data Loss Prevention solution protects enterprises from the risk associated with unauthorized transfer of data from within or outside the organization. Data loss is defined as confidential or private information leaving the enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols.

Network Data Loss Prevention 9.2 is comprised of the components described in the sections below.

1.6.1 McAfee Network DLP Discover

McAfee Network DLP Discover searches systems based on LAN segment, IP address range, network group, and many other defined criteria. Schedule scans to run at intervals that fit your workflow and automatically fingerprint the results to support the most accurate data protection.

1.6.2 McAfee Network DLP Monitor

McAfee Network DLP Monitor enables you to find, track, and protect sensitive information from any application or location, in any format, over any protocol or port, over time.

1.6.3 McAfee Network DLP Prevent

McAfee Network DLP Prevent helps you enforce safe data handling policies for information leaving the boundaries of your network. It integrates with most commercial Internet gateway security technologies for email, web, IM, and other network applications.

1.6.4 McAfee Network DLP Manager

McAfee Network DLP Manager provides centralized control over the McAfee DLP solution.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE is Network Data Loss Prevention 9.2 and includes the functionality defined in the component listings above. The TOE is a distributed software TOE and includes one Network DLP Manager component and at least one instance of each of the following:

- DLP Discover
- DLP Prevent
- DLP Monitor

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

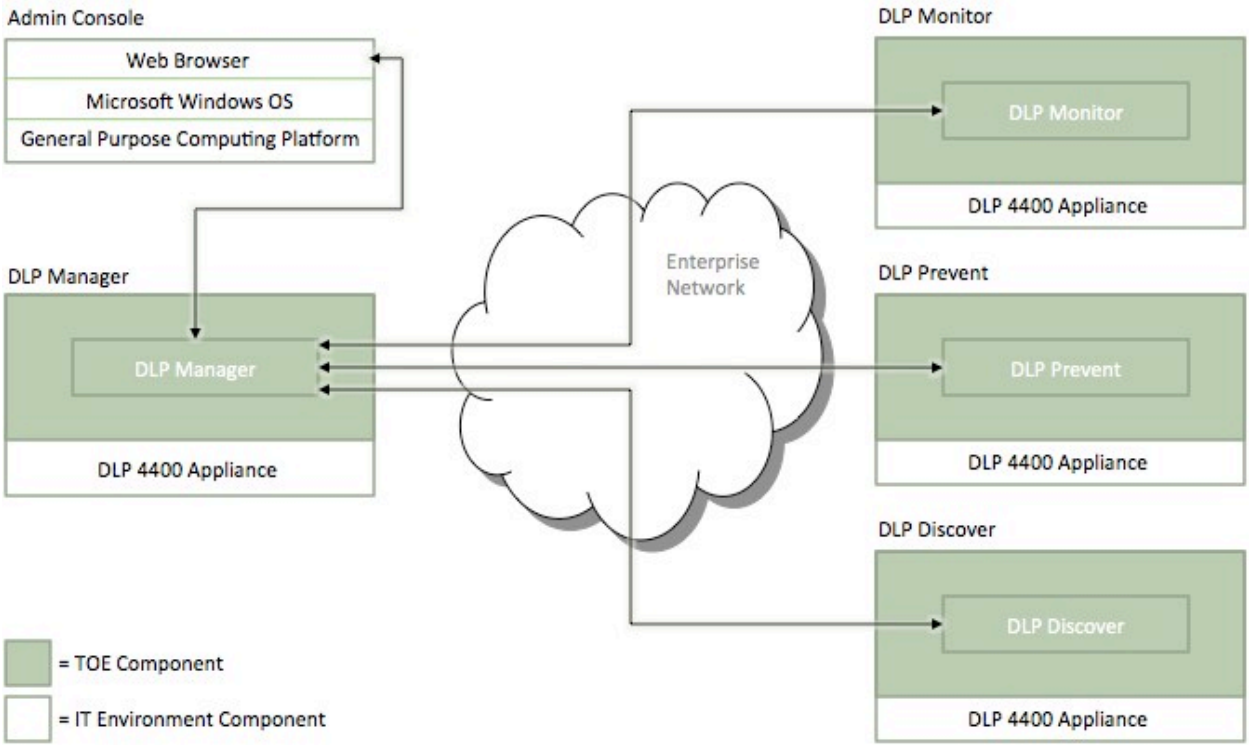

Figure 1 – TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	NDLP Manager Version 9.2 Build 1827 NDLP Discover Version 9.2 Build 1648 NDLP Prevent Version 9.2 Build 1264 NDLP Monitor Version 9.2 Build 1419
IT Environment	• DLP 4400 Appliance • MLOS Version 2.6.27 Build 19 • VMWare ESX/ESXi 4.1 Update 1 and later

Table 3 – Evaluated Configuration for the TOE

The TOE consists of a set of software applications running on McAfee appliances or workstations running VMWare. The appliance hardware, Linux-based operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary. The SSL session which protects information between TOE components is provided by the IT Environment.

1.7.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Policy Enforcement	The TOE enforces policies on managed systems and audits end-user action against those policies. The TOE ensures end users aren't allowed to transmit sensitive data over an internal or external network as specified by an administrator through a data loss prevention policy. Reports based upon security events / user actions may be retrieved via the GUI interface.
Identification and Authentication	The TOE requires administrative users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records.

Table 4 – Logical Boundary Descriptions

1.7.2.1 TOE Guidance

The following guidance documentation is provided as part of the TOE:

- *Operational User Guidance and Preparative Procedures Supplement: McAfee Network Data Loss Prevention 9.2*
- *Product Guide: McAfee Total Protection for Data Loss Prevention 9.2 Software*
- *Release Notes: McAfee Total Protection for Data Loss Prevention 9.2.0 Software*
- *Quick Start Guide: McAfee Total Protection for DLP Version 9.2.0*
- *Installation Guide McAfee Data Loss Prevention 9.2 Virtual Appliance*

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The system(s) on which TOE components execute is dedicated to that purpose. All components execute on dedicated systems and do not provide a general-purpose operating system or capabilities therein.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The appliance provides virtual memory and process separation, which helps ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the OS or third party software (operational environment) to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.SENSITIVE_DATA	An unauthorized user may transmit or transfer sensitive data over a network.

Table 5 – Threats Addressed by the TOE

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.

POLICY	DESCRIPTION
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 6 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.INTEGRITY	The TOE must ensure the integrity of all System data.
O.SENSITIVE_DATA	The TOE shall take specified actions upon transmission of sensitive files or data.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTEROP	The TOE is interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE via mechanisms outside the TSC.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE.

OBJECTIVE	DESCRIPTION
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.ACCESS									✓												
A.ASCOPE									✓												
A.DATABASE																	✓				
A.DYNMIC								✓	✓												
A.LOCATE						✓															
A.MANAGE								✓													
A.NOEVIL					✓	✓	✓														
A.PROTCT						✓															
P.ACCACT			✓							✓						✓			✓		
P.ACCESS		✓	✓												✓	✓	✓				
P.INTEGRITY				✓							✓		✓					✓		✓	✓
P.MANAGE	✓	✓	✓		✓		✓	✓								✓					
P.PROTCT						✓								✓						✓	✓
T.COMDIS		✓	✓											✓		✓					
T.COMINT		✓	✓	✓										✓		✓					
T.IMPCON	✓	✓	✓		✓											✓					
T.LOSSOF		✓	✓	✓												✓					

OBJECTIVE / THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
T.NOHALT		✓	✓													✓					
T.PRIVIL		✓	✓													✓					
T.SENSITIVE_ DATA												✓									

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTEROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the hardware and software.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. The OE.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION and OE.DATABASE objectives counter this threat for mechanisms outside the TSC via IT Environment protections of the system data trail and the database used to hold TOE data. The OE.SD_PROTECTION and O.ACCESS objectives counter this threat for mechanisms inside the TSC via TOE protections of the system data trail and the database used to hold TOE data.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGRITY objective ensures the protection of System data from modification. The O.AUDIT_PROTECT and OE.AUDIT_PROTECT objectives ensure the integrity of audit records in the database generated by the TOE using access mechanisms inside and outside the TSC respectively. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be deleted.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.SENSITVE_DATA	An unauthorized user may transmit or transfer sensitive data from managed systems. The O.SENSITIVE_DATA objective requires the TOE to take specified actions upon the transmission of sensitive files or data.

Table 11 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

This Security Target does not include any extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 12 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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; and

c) *The events identified in the FAU_GEN.1.2.*

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), 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, *the information detailed in the following table*.

Application Note: The auditable events for the (not specified) level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be generated.	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 13 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *Administrators* with the capability to read *all information* from the audit records.

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

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* on

Subjects: External IT entities attempting to transfer or transmit sensitive data

Information: Files and content stored on the managed system or transferred from the managed system

Operations: Encrypt, redirect, quarantine, send email notification, and block.

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* based on the following types of subject and information security attributes:

Subject Security Attributes:

- *IP Address*
- *VLAN ID*
- *Protocol*
- *Device ID*
- *Group ID*

Information security attributes

- *Traffic Classification*
  - *Source IP*
  - *Destination IP*

- *VLAN ID*
- *Protocol*

- *Content Classification*
  - *Office documents*
  - *Multimedia files*
  - *Source code*
  - *Design files*
  - *Encrypted files*

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

A. Monitoring option is enabled for the service and information structure type and:

1. *The attribute is not covered by policy*
2. *The attribute is assigned an action of "send email notification" via policy*

Or

B. DLP monitoring is disabled for the subject and information structure type.

FDP_IFF.1.3 The TSF shall enforce ~~the~~ *no other additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *No explicit authorization rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *No explicit denial rules*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User name;

b) Authentication data;

c) *Permission Sets.*

6.1.3.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

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

6.1.3.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

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

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, clear, *create, export and use* the *TSF data associated with the actions in FMT_SMF.1* to *an Administrator*.

6.1.4.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) User Account management,

b) Audit Log management,

c) Event Log management,

d) Notification management,

e) Device management

f) DLP Policy and Rule management

6.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Administrator and User*.

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

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 14 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied[2]
FIA_ATD.1	No other components	None	n/a
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_UID.1	No other components	None	n/a
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied

Table 15 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

OBJECTIVE / SFR	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDENTIFY	O.INTEGRITY	O.SENSITIVE_DATA
FAU_GEN.1		✓					
FAU_GEN.2		✓					
FAU_SAR.1	✓						
FAU_SAR.2	✓						
FAU_STG.1		✓	✓				
FDP_IFC.1							✓

[2] FMT_MSA.3 does not impact the security required by FDP_IFF.1 for this particular TOE because there are no configurable security attributes

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDENTIFY	O.INTEGRITY	O.SENSITIVE_DATA
FDP_IFF.1							✓
FIA_ATD.1					✓		
FIA_UID.1	✓				✓		
FIA_UAU.1	✓				✓		
FMT_MTD.1	✓			✓		✓	
FMT_SMF.1	✓			✓			
FMT_SMR.1	✓			✓			

Table 16 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification and authentication process [FIA_UAU.1, FIA_UID.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The user associated with the events must be recorded [FAU_GEN.2]. The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators [FAU_STG.1].
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification [FAU_STG.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].

OBJECTIVE	RATIONALE
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using a identification process of a username/password combination [FIA_UID.1 and FIA_UAU.1].
O.INTEGRITY	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.1].
O.SENSITIVE_DATA	The TOE shall take specified actions upon transmission of sensitive files or data. The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted inappropriately [FDP_IFC.1 and FDP_IFF.1].

Table 17 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Network Data Loss Prevention 9.2
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Network Data Loss Prevention 9.2
ADV_TDS.1: Basic Design	Basic Design: McAfee Network Data Loss Prevention 9.2
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Network Data Loss Prevention 9.2
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Network Data Loss Prevention 9.2
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Network Data Loss Prevention 9.2
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Network Data Loss Prevention 9.2
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Network Data Loss Prevention 9.2
ALC_FLR.2: Flaw Reporting	Flaw Reporting: McAfee Network Data Loss Prevention 9.2
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Network Data Loss Prevention 9.2
ATE_FUN.1: Functional Testing	Security Testing: McAfee Network Data Loss Prevention 9.2

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Network Data Loss Prevention 9.2

Table 18 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

SFR \ TSF	Policy Enforcement	Identification and Authentication	Management	Audit
FAU_GEN.1				✓
FAU_GEN.2				✓
FAU_SAR.1				✓
FAU_SAR.2				✓
FAU_STG.1				✓
FDP_IFC.1	✓			
FDP_IFF.1	✓			
FIA_ATD.1			✓	

SFR \ TSF	Policy Enforcement	Identification and Authentication	Management	Audit
FIA_UID.1		✓		
FIA_UAU.1		✓		
FMT_MTD.1			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	

Table 19 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN.1	**Audit –** User actions area audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FDP_IFC.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted or transferred inappropriately.
FDP_IFF.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted or transferred inappropriately.
FIA_ATD.1	**Management** – User security attributes are associated with the user user account via User Account management.
FIA_UID.1	**Identification and Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.

SFR	SF AND RATIONALE
FIA_UAU.1	**Identification and Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MTD.1	**Management** – The Administrator status and user permissions determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the Administrator status for the user.

Table 20 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Enforcement

There are three main TOE components responsible for enforcing the DLP Information Flow Control SFP:

- Discover
- Monitor
- Prevent

The DLP Discover component discovers sensitive information by crawling entire networks, including laptops, desktops, servers, document repositories, portals, and file-transfer locations, identifying sensitive data as it finds it.

The DLP Monitor component performs real-time scanning and analysis of network traffic based on traffic type or content. Through detailed classification, indexing, and storage of all network traffic the McAfee Network DLP Monitor appliance allows you to quickly leverage historical information to understand what data is sensitive, how it is being used, who is using it, and where it is going. Additionally, the DLP Monitor appliance performs real-time scanning and analysis of network traffic.

Content and network capture filters allow different types of user actions. Content capture filter actions keep certain types of traffic from being recognized by the capture engine. Network capture filter actions ignore specific components of network traffic or store data that is transmitted via certain protocols. Network capture filter actions may ignore or store network data depending on port or protocol used.

The following table provides the standard filters for capturing content during discovery/analysis:

FILTER	DESCRIPTION
Ignore binary	Excludes all binary files
Ignore BMP and GIF images	Excludes images in BMP and GIF formats
Ignore crypto	Excludes encrypted data
Ignore HTTP Gzip responses	Keeps compressed files from being opened more than once (excludes HTTP Gzip responses)
Ignore HTTP headers	Excludes HTTP headers
Ignore P2P	Excludes all peer-to-peer traffic
Ignore small JPG images	Excludes insignificant images (JPG images smaller than 4 MB)
Ignore flow headers	Excludes flow headers

Table 21 – Standard Content Capture Filters

The following table provides the standard filters for capturing network packets during discovery/analysis:

FILTER	DESCRIPTION

FILTER	DESCRIPTION
Ignore RFC 1918	Excludes traffic routed to 10.0.0.0.-10.255.255.255, 172.16.0.0.-172.31.255.255 and 192.168.0.0- 192.168.255.255
Ignore HTTP Responses	Excludes program output sent from a server after receiving and interpreting an HTTP Request
Ignore unknown	Excludes traffic using unknown protocols
Ignore SMB	Excludes Session Message Block and Microsoft Basic Input/Output System (NetBIOS) traffic
Ignore SSH	Excludes secure shell traffic
Ignore POP	Excludes Post Office Protocol 3 traffic
Ignore IMAP	Excludes Internet Message Access Protocol traffic
Ignore HTTPS	Excludes secure Hypertext Transport Protocol Traffic
Ignore LDAP	Excludes Lightweight Directory Access Protocol traffic
Ignore NTLM	Excludes Microsoft New Technology Local Area Network Manager traffic
BASE	Base Configuration filter (opens the system for storage of incoming data)

Table 22 – Standard Network Capture Filters

The DLP Prevent component enforces policies for information leaving the network through email, webmail, instant messaging (IM), wikis, blogs, portals, and social networking sites. This component provides a variety of remediation actions, including encrypting, redirecting, quarantining, and blocking.

7.2 Identification and Authentication

Users must log in to the DLP Manager appliance with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. When the credentials are presented by the user, DLP Manager determines if the user name is defined and enabled. If not, the login process is terminated and the login GUI is redisplayed.

If the authentication attempt is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, the login GUI is redisplayed.

7.3 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the DLP Manager GUI, which is a browser-based management console connecting to the DLP Manager via SSL session provided by the IT Environment. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. User Accounts,
2. Notifications,
3. Devices,

4. DLP Policies and Rules,

Each of these items is described in more detail in the following sections.

7.3.1 User Account Management

Only Administrators may perform user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name
2. Password
3. Permission sets granted to the user

One or more permission sets may be associated with an account. Administrators are granted all permissions.

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to any users who are not administrators (administrators have all permissions to all products and features).

Administrators may create, view, modify and delete permission sets. When a permission set is created or modified, the permissions granted via the permission set may be specified by an administrator.

7.3.2 Notification Management

Notifications of system alerts may be specified in response to events generated by the TOE. Notifications cause email messages to be sent to the configured recipient(s). System alerts are events that are regularly reported to the events database. The database is polled every 2 minutes, and every alert in the database is sent to the dashboard within this interval. A timestamp is reported for each alert. There are three types of system alerts:

1. Critical alerts report the most serious system errors. They are reported instantaneously.
2. Warning alerts report system errors that may affect system performance. They are reported within 30 minutes of their generation.
3. Informational alerts report events that may contain useful system information. They are reported within 30 minutes of their generation.

7.3.3 Device Management

Administrators can manage the devices that comprise the TOE. In addition to initial setup and configuration for use with DLP Manager, the administrator can perform the following types of configuration:

- Adding devices to NDLP

- Backing up NDLP systems
- Changing link speed
- Connecting to syslog servers
- Correcting system time in the interface
- Deregistering devices from NDLP
- Managing disk space
- Resetting system time manually
- Restarting NDLP systems
- Resynchronizing an NDLP device
- Upgrading NDLP Systems
- Viewing NDLP managed devices

7.3.4 DLP Policy and Rule Management

The TOE provides the capability to configure and manage policies and rules regarding the transmission and transfer of sensitive data. Details are included in the Policy Enforcement section.

7.4 Audit

The Audit Log maintains a record of user actions. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section.

Additionally, the TOE provides the following DLP Information Flow Control SFP events: Keywords, Concepts, Content type, Email (Address, subject, CC, BCC), IP address (source ,destination, bidirectional), GeoIP (country, campus), URL, User (name, group, department), File (properties – size, signature, header properties like author etc), Protocol, Port (source, destination, bidirectional), File name/pattern, Repository type, share name, database catalog, database table name, database schema, database column name, signature percent match, and database records matched.