VMware® vCloud Networking and Security 5.5.0a

Security Target

Evaluation Assurance Level: EAL4+

DOCUMENT VERSION: 2.0

vmware®

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
United States of America

Phone: +1 (650) 475-5000
http://www.vmware.com

VMware Security Advisories, Certifications and Guides
http://www.vmware.com/security/

Prepared for VMware by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America
Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

1 INTRODUCTION 6
1.1 PURPOSE 6
1.2 SECURITY TARGET AND TOE REFERENCES 6
1.3 PRODUCT OVERVIEW 7
1.3.1 Product Components 7
1.4 TOE OVERVIEW 9
1.4.1 TOE Environment 10
1.5 TOE DESCRIPTION 10
1.5.1 Physical Scope 10
1.5.2 Logical Scope 13
1.5.3 Product Physical/Logical Features and Functionality not included in the TOE 15

2 CONFORMANCE CLAIMS 16

3 SECURITY PROBLEM 17
3.1 THREATS TO SECURITY 17
3.2 ORGANIZATIONAL SECURITY POLICIES 18
3.3 ASSUMPTIONS 18

4 SECURITY OBJECTIVES 19
4.1 SECURITY OBJECTIVES FOR THE TOE 19
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 19
4.2.1 IT Security Objectives 19
4.2.2 Non-IT Security Objectives 20

5 EXTENDED COMPONENTS 21
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS 21
5.1.2 Class DSM: Data Security Management 24
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS 26

6 SECURITY REQUIREMENTS 27
6.1 CONVENTIONS 27
6.2 SECURITY FUNCTIONAL REQUIREMENTS 27
6.2.1 Class FAU: Security Audit 29
6.2.2 Class FCS: Cryptographic Support 31
6.2.3 Class FDP: User Data Protection 42
6.2.4 Class FIA: Identification and Authentication 47
6.2.5 Class FMT: Security Management 48
6.2.6 Class FPT: Protection of the TSF 51
6.2.7 Class FTP: Trusted Path/Channels 52
6.2.8 Class DSM: Data Security Management 53
6.3 SECURITY ASSURANCE REQUIREMENTS 54

7 TOE SUMMARY SPECIFICATION 55
7.1 TOE SECURITY FUNCTIONS 55
7.1.1 Security Audit 56
7.1.2 Cryptographic Support 57
7.1.3 User Data Protection 58
7.1.4 Identification and Authentication 60
7.1.5 Security Management 60
7.1.6 Protection of the TSF 61
7.1.7 Trusted Path/Channels 61
7.1.8 Data Security Management 62

8 RATIONALE 63
8.1 CONFORMANCE CLAIMS RATIONALE 63
8.2 SECURITY OBJECTIVES RATIONALE 63
8.2.1 Security Objectives Rationale Relating to Threats 63
8.2.2 Security Objectives Rationale Relating to Assumptions 64
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS 65
8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS 65
8.5 SECURITY REQUIREMENTS RATIONALE 65
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 65
8.5.2 Security Assurance Requirements Rationale 71
8.5.3 Dependency Rationale 71

9 ACRONYMS AND TERMS 74
9.1 TERMINOLOGY 74
9.2 ACRONYMS 74

Table of Figures

FIGURE 1 SAMPLE DEPLOYMENT 10
FIGURE 2 TOE BOUNDARY AND EVALUATED CONFIGURATION 11
FIGURE 3 EXTENDED: HTTPS FAMILY DECOMPOSITION 22
FIGURE 4 EXTENDED: TLS FAMILY DECOMPOSITION 23
FIGURE 5 CLASS DSM: DATA SECURITY MANAGEMENT FUNCTION CLASS DECOMPOSITION 24
FIGURE 6 SYSTEM FLOW DATA COLLECTION FAMILY DECOMPOSITION 25
FIGURE 7 ANALYSIS FAMILY DECOMPOSITION 26

List of Tables

TABLE 1 ST AND TOE REFERENCES 6
TABLE 2 TOE MINIMUM REQUIREMENTS 12
TABLE 3 GUIDANCE DOCUMENTATION 12
TABLE 4 CC AND PP CONFORMANCE 16
TABLE 5 THREATS 17
TABLE 6 ASSUMPTIONS 18
TABLE 7 SECURITY OBJECTIVES FOR THE TOE 19
TABLE 8 IT SECURITY OBJECTIVES 19
TABLE 9 NON-IT SECURITY OBJECTIVES 20
TABLE 10 EXTENDED TOE SECURITY FUNCTIONAL REQUIREMENTS 21
TABLE 11 TOE SECURITY FUNCTIONAL REQUIREMENTS 27
TABLE 12 AUDITABLE EVENTS 29
TABLE 13 VMWARE CRYPTOGRAPHIC MODULE FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 32
TABLE 14 EDGE VMTOOLS CAVP VALIDATED ALGORITHM IMPLEMENTATIONS 34
TABLE 15 VMWARE NSS CRYPTOGRAPHIC MODULE FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 35
TABLE 16 VMWARE KERNEL CRYPTOGRAPHIC MODULE FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 37
TABLE 17 ENDPOINT MUX CAVP VALIDATED ALGORITHM IMPLEMENTATIONS 38
TABLE 18 ENDPOINT VSM CAVP VALIDATED ALGORITHM IMPLEMENTATIONS 39
TABLE 19 VMWARE JAVA JCE (JAVA CRYPTOGRAPHIC EXTENSION) CRYPTOGRAPHIC MODULE FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 40
TABLE 20 MANAGEMENT OF SECURITY ATTRIBUTES 48
TABLE 21 EAL4 ASSURANCE REQUIREMENTS 54
TABLE 22 MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS 55
TABLE 23 AUDIT LOG FILTERS 57
TABLE 24 SYSTEM EVENT FILTERS 57
TABLE 25 AUTHORIZED ADMINISTRATOR ROLES 60

TABLE 26 THREATS: OBJECTIVES MAPPING 63
TABLE 27 ASSUMPTIONS: OBJECTIVES MAPPING 64
TABLE 28 OBJECTIVES: SFRS MAPPING 65
TABLE 29 FUNCTIONAL REQUIREMENTS DEPENDENCIES 71
TABLE 30 TERMS 74
TABLE 31 ACRONYMS 74

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the organization of the ST. The TOE is the VMware vCloud Networking and Security, and will hereafter be referred to as the TOE or vCNS throughout this document. The TOE is a software-only suite of security virtual appliances. vCNS includes virtual appliances and services essential for protecting virtual machines as well as physical machines. The TOE includes a hypervisor-based firewall that protects applications running on the virtual machines from network-based attacks. In addition, the TOE provides a dedicated secure virtual appliance to provide anti-virus and malware scans of the virtual machines (VM). The TOE also provides visibility into sensitive data stored within an organization's virtualized and cloud environments.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, 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.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	VMware, Inc. vCloud Networking and Security 5.5.0a Security Target
ST Version	Version 1.9
ST Author	Corsec Security, Inc.
ST Publication Date	3/20/2014
TOE Reference	VMware vCloud Networking and Security 5.5.0a

ST Title	VMware, Inc. vCloud Networking and Security 5.5.0a Security Target
FIPS[1] 140-2 Status	Level 1, Validated cryptographic modules: - VMware Cryptographic Module; Certificate No. [xxx][2] - VMware NSS Cryptographic Module; Certificate No. [xxx][3] - VMware Java JCE (Java Cryptographic Extension) Module; Certificate No. [xxx][4] - VMware Kernel Cryptographic Module; Certificate No. [xxx][5]

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

vCNS is a network virtualization and security product for protecting virtualized datacenters from network-based attacks, protecting data in transit between datacenters and preventing misuse of network services and protected information contained within the network. vCNS includes virtual appliances and services essential for protecting virtual machines from attacks within/from the virtual and the physical environments. vCNS can be configured through a web-based user interface, a vSphere Client plug-in, vCenter Server snap-in, a command line interface (CLI), and REST[6] API[7].

vCNS is comprised of a suite of networking and security virtual appliances built for VMware vSphere integration. VMware vCenter Server provides centralized management of VMware's ESXi. VMware ESXi and vCenter Server 3.5, 4.0, 4.1, and 5.0 have been Common Criteria evaluated. ESXi is a user-installable or OEM[8]-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server.

vCNS can be integrated with VMware vCloud director and VMware Horizon View. VMware vCloud Director abstracts and pools the resources managed by vCNS. The pooled resources can then be used in the provisioning of virtual datacenters that provide software-defined services. VMware Horizon View can be used to simplify and automate the management of an organization's virtual machine infrastructure. From one central location, Horizon View can securely deliver 'desktop as a service' to end users on any device or software applications such as vCNS, granting users maximum mobility and flexibility

1.3.1 Product Components

In order to provide a secure virtual environment, vCNS is comprised of four components: vShield Manager, vShield App, vShield Edge, and vShield Endpoint and Data Security. Each of these components will also be referred to as the Manager, App, Edge, and Endpoint and Data Security respectively throughout this document. The following paragraphs provide a brief description of the product components.

1.3.1.1 vShield Manager (VSM)

The vShield Manager is the centralized network management component of vShield, and is installed as a virtual appliance on an ESXi host in the vSphere environment. A vShield Manager can run on a different

[1] Federal Information Processing Standard
[2] To lab: This will be updated when the FIPS certificate is issued.
[3] To lab: This will be updated when the FIPS certificate is issued.
[4] To lab: This will be updated when the FIPS certificate is issued.
[5] To lab: This will be updated when the FIPS certificate is issued.
[6] Representational State Transfer
[7] Application Programming Interface
[8] Original Equipment Manufacturer

ESXi host from the ESXi host that is running the vShield components such as the App, Edge, and Endpoint and Data Security.

The vShield Manager Component is accessed in five different ways. These below interfaces will be generally referred to as the vShield Manager throughout this ST.

- vShield Manager User Interface - This interface is a snap-in for vCenter Server.
- vSphere Manager Client plug-in User Interface - This is a plug-in that installs in the vSphere Client Interface and is displayed as a tab in the interface.
- vShield Manager Web Graphical User Interface (GUI) - This interface is accessed via a web browser.

Additionally vShield Manager can also be accessed over CLI, and REST APIs. CLI can be accessed over console port, or can be configured to access via SSH. REST APIs are accessed over TLS.

Using the vShield Manager User Interface, vSphere Manager Client plug-in, CLI or REST APIs administrators can install, configure, and maintain vShield components. The vShield Manager leverages the VMware Infrastructure SDK[9] to display a copy of the vSphere Client inventory panel, and includes tabs or screens to manage the virtual Hosts and Clusters as well as Networks. The TOE relies on a PostgreSQL[10] database to provide storage of the audit logs. The PostgreSQL database is a part of the vShield Manager.

1.3.1.2 vShield App

The vShield App is a hypervisor-based firewall that protects applications in the virtual datacenter from network-based attacks. vShield App provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones. A security zone is a firewalled virtual subnet that prevents the data from a particular zone (e.g., zone A) from traversing another zone (e.g., zone B). With vShield App, organizations gain visibility and control over network communications between virtual machines. An authorized administrator can create access control policies based on logical constructs such as VMware vCenter containers and vShield security groups, not just physical constructs such as IP[11] addresses.

The Flow Monitoring feature of vShield App displays network activity between virtual machines at the application protocol level. An authorized administrator can use this information to audit network traffic, define and refine firewall policies, and identify botnets.

1.3.1.3 vShield Edge

vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS[12] port group, or on a Cisco Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP[13], VPN[14], NAT[15], and Load Balancing. Common deployments of vShield Edge include placing it in a DMZ[16], on a VPN Extranet, or in multitenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

[9] Software Development Kit
[10] Postgre Structured Query Languages is a Open Source Object-Relational Database Management System
[11] Internet Protocol
[12] Distributed Switch
[13] Dynamic Host Configuration Protocol
[14] Virtual Private Network
[15] Network Address Translation
[16] Demilitarized Zone

vShield Edge can be managed through the vShield Manager Web interface, as well as the vShield Manager plug-in integrated with vCenter Server, which places most vShield Edge features in dedicated tabs as well as context-sensitive menus. vShield provisioning and configuration of all features is also supported through the vShield Manager REST APIs. vShield Edge does not support CLI-based configuration, but within the console to Edge VM in the vSphere Client, there is a command line interface that can be used for troubleshooting vShield Edge.

1.3.1.4 vShield Endpoint and Data Security

vShield Endpoint offloads anti-virus and anti-malware agent processing to a dedicated secure virtual appliance. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update anti-virus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current anti-virus signatures when they come online. vShield Endpoint provides a framework for other third-party anti-virus products to be run on guest virtual machines from the outside, removing the need for anti-virus agents in every virtual machine. Since vShield Endpoint only provides a framework, no anti-virus SFRs are being claimed for this component.

vShield Data Security provides visibility into sensitive data stored within the organization's virtualized and cloud environments. Based on the violations reported, an authorized administrator can ensure that sensitive data is adequately protected and assess compliance with regulations.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a software-only security solution for VMware virtualized environments. It provides firewall, data protection, and anti-virus and anti-malware services.

The TOE includes all of the components and functionality described above in section 1.3.1 and below in section 1.5, except for the features and functionality listed below in section 1.4.1. Table 2 identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

Figure 2 illustrates a sample deployment of the TOE. The previously undefined acronyms that appear in Figure 2 are as follows:

- OS - Operating System

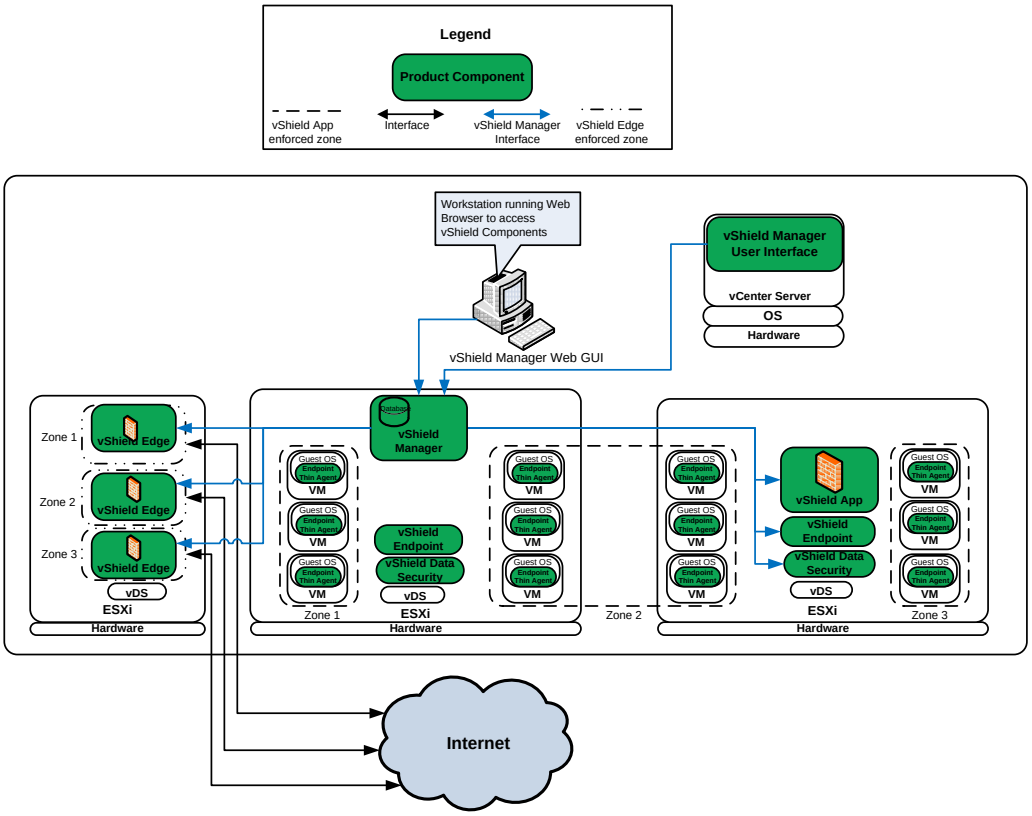

Figure 1 Sample Deployment

1.4.1 TOE Environment

It is assumed that there will be no untrusted users on the TOE components. In addition, the TOE components are intended to be deployed within controlled access facilities which will prevent unauthorized physical access (e.g., badge access, fire control, locks, alarms, etc.).

For management of vShield, a web browser may be used to remotely access the vShield components. This web browser and the computer it runs on are considered to be outside of the TOE Boundary. The computer should have the latest versions of Flash and flash plug-ins downloaded and installed prior to accessing the TOE.

See Table 2 in section 1.5.1 below for a detailed description of the environment relied upon by the TOE components.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The TOE is software-only and the TOE Components are the same as the product components as specified in section 1.3.1.

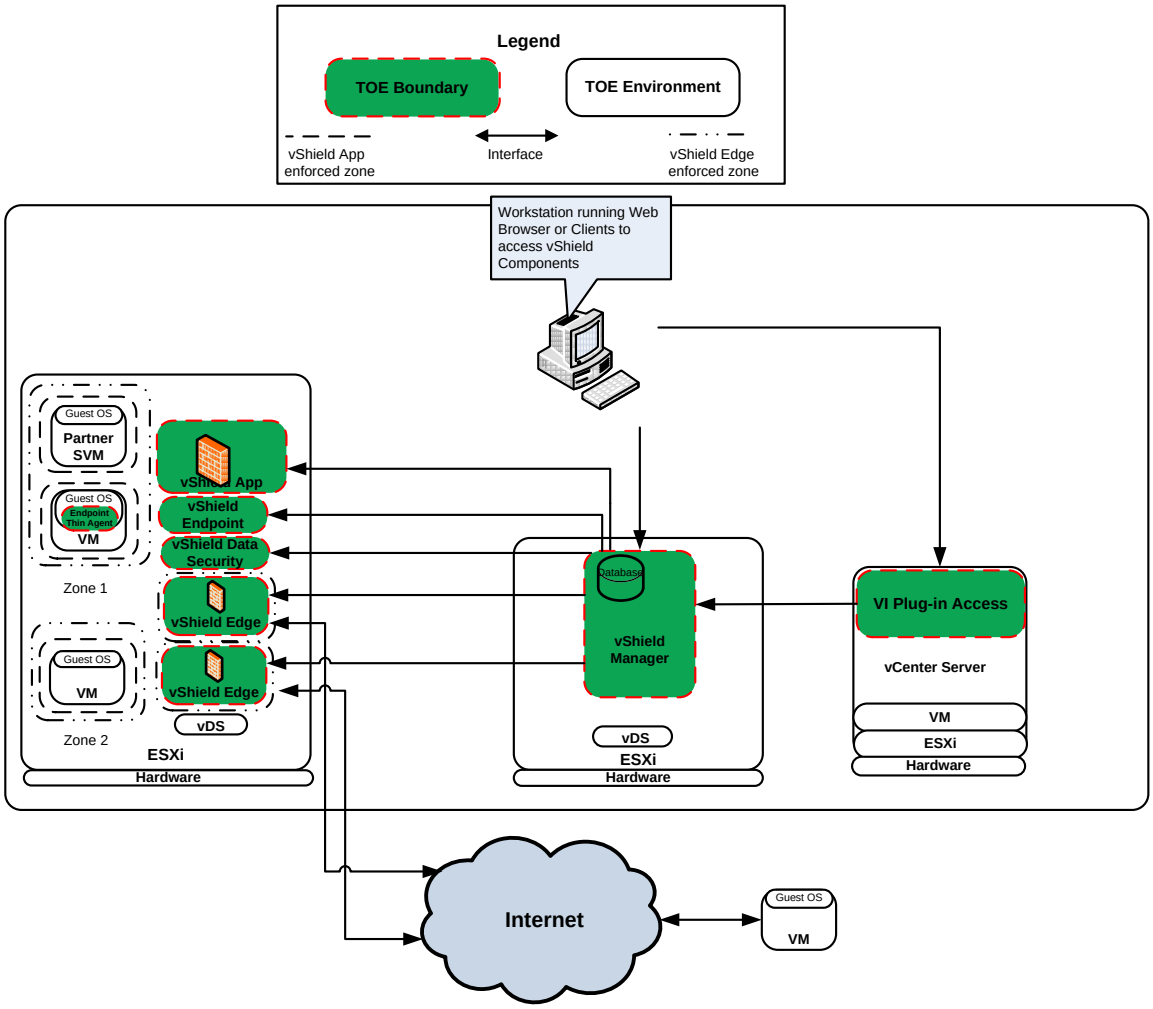

Figure 2 TOE Boundary and Evaluated Configuration

The TOE Boundary includes all the VMware-developed parts of the vCloud Networking and Security product. The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in section 1.4.1 of the ST and Table 2 below.

Table 2 below indicates which elements of the product are included in the TOE Boundary as well as the TOE minimum requirements.

Table 2 TOE Minimum Requirements

Requirement	TOE	TOE Environment
vCloud Networking and Security 5.5.0a	✓	
vShield Manager Hardware Requirements: • Memory – 8 GB allocated, 3 GB reserved • Disk Space – 60 GB • vCPU – 2		✓
vShield App Hardware Requirements: • Memory – 1 GB allocated, 1 GB reserved • Disk Space – 5 GB per vShield App per ESX host • vCPU – 2		✓
vShield Edge Compact Hardware Requirements: • Memory – 256 MB, Large and Quad Large: 1 GB, X-Large: 8GB • Disk Space – 300 MB, Large, Quad Large, and X-Large: 448 MB • vCPU – 1, Large: 2, Quad Large and X-Large: 4		✓
vShield Endpoint and Data Security Hardware Requirements: • Memory – 512 MB • Disk Space – 6GB per ESX host • vCPU – 1		✓
Required Supporting TOE Environment Software: • VMware vCenter Server 5.1 or later • VMware ESXi 5.0 or later for each server • VMware Tools		✓
Required TOE Environment Web Browsers for the vShield Manager Web GUI: • Microsoft Internet Explorer Internet Explorer 6.x and later • Mozilla Firefox 1.x and later • Safari 1.x or 2.x and later		✓

1.5.1.1 Guidance Documentation

Table 3 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

Table 3 Guidance Documentation

Document Name	Description
vShield Installation and Upgrade Guide vShield Manager 5.5, vShield Edge 5.5, vShield Endpoint 5.5	Includes steps for the basic initialization and setup of the TOE.
vShield Administration Guide vShield Manager 5.5, vShield App 5.5, vShield Edge 5.5, vShield Endpoint 5.5	Contains detailed steps for how to properly configure and maintain the TOE.

Document Name	Description
vShield API Programming Guide vShield 5.5, vShield App 5.5, vShield Edge 5.5, vShield Endpoint 5.5	Describes how to install, configure, monitor, and maintain the TOE system by using REST API requests. The information includes step-by-step configuration instructions and examples.
Command Line Interface Reference vShield Manager 5.1, vShield App 5.1, vShield Edge 5.1, vShield Endpoint 5.1	Contains detailed steps for how to properly configure and maintain the TOE using the CLI.
VMware vCNS v5.50a Guidance Supplement v0.4	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

1.5.2.1 Security Audit

The TOE generates audit records for security relevant actions of the authorized administrators within the vShield Manager and back-end users with the audit user role from the Web GUI or CLI. The TOE provides an authorized administrator access to view the audit logs created as a result of administrator actions through the vShield Manager. In case of audit trail saturation the TSF does rollover of the logs. For backup purposes, the audit event logs can be sent to an external Syslog Server.

1.5.2.2 Cryptographic Support

The Cryptographic Support of the TSF function provides cryptographic functions to secure sessions as follows:

- vShield Manager Web GUI connecting to the vShield Manager is secured by HTTPS.
- The connection of the vShield Manager Client plug-in User Interface and vShield Manager User Interface to the vShield Manager is secured via TLS[17].
- IPSec[18] VPN capabilities to provide authentication and encryption of information being passed through the VPN tunnel between two Edge components.
- CLI sessions are secured via SSH, and REST API communications are protected via TLS.

1.5.2.3 User Data Protection

For vShield, user data refers to network traffic traversing the Edge and App firewalls. The Information Control functionality of the TOE is defined in the User Data Protection SFRs and allows authorized administrators to set up rules between interfaces of the TOE. These rules control whether a packet is transferred from one interface to another and/or transferred encrypted based upon:

- User identities (source and/or destination)
- Presumed address of source subject
- Presumed address of destination subject
- Service used
- Transport layer protocol
- Security-relevant service command

[17] Transport Layer Security
[18] Internet Protocol Security

- Network interface on which the connection request occurs and is to depart
- Information gleaned from prior packets

For vShield Edge packets will be dropped unless a specific rule or policy in an access control list (ACL) has been set up to allow the packet to pass. For vShield App packets are passed by default. The order of Access Control Entries (ACEs) in an ACL is important. When the TOE decides whether to forward or drop a packet, the TOE tests the packet against the ACE in the order in which the entries are listed. Starting at the beginning of the ACEs, once a match is found no more ACEs are checked. For example, if the ACE at the beginning of the ACL explicitly permits all traffic, no further ACEs are checked. Interface ACLs are applied first before IPSec negotiations occur in the evaluated configuration.

In providing the Information Flow Control functionality, vShield Edge has the ability to translate network addresses contained within a packet. This functionality is called Network Address Translation. Depending upon vShield Edge's configuration, the address can be translated into a permanently defined static address, an address selected from a range, or a single address with a unique port number (Port Address Translation). Also, Network Address Translation can be disabled, so that addresses are not changed when passing through the TOE.

The TOE rejects FTP[19] command requests that do not conform to generally accepted, published protocol definitions.

The IPSec VPN Function includes IPSec and Internet Security Association and Key Management Protocol (ISAKMP) functionality to support VPNs. A secure connection between two IPSec peers is called a tunnel. The TOE implements ISAKMP and IPSec tunneling standards to build and manage VPN tunnels. ISAKMP and IPSec accomplish the following:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users
- Encrypt and decrypt data
- Manage data transfer across the tunnel.

The TOE implements IPSec in a VLAN[20]-to-VLAN configuration between two Edge IPSec security gateways. In IPSec VLAN-to-VLAN connections, the TOE can function as initiator or responder. Initiators propose Security Associations (SAs); responders accept, reject, or make counter-proposals, all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The TOE IPSec implementation contains a number of functional components that comprise the IPSec VPN function. In IPSec terminology, a peer is a remote-access client or another secure gateway. For the purposes of the evaluated configuration, a peer will be considered another Edge operating as an IPSEC VPN.

1.5.2.4 Identification and Authentication

The TOE provides functionality that requires administrators to verify their claimed identity. The Identification and Authentication TSF[21] ensures that only legitimate administrators can gain access to the configuration settings and management settings of the TOE. Administrators must log in with a valid user name and password before the TOE will permit the administrators to manage the TOE.

[19] File Transfer Protocol
[20] Virtual Local Area Network
[21] TOE Security Functionality

1.5.2.5 Security Management

The TOE provides a set of commands for administrators to manage the security functions, configuration, and other features of the TOE components. The Security Management function specifies user roles with defined access for the management of the TOE components.

1.5.2.6 Protection of the TSF

The TOE implements HTTPS[22] for protection of the data being sent from the Management Console to a remote TOE component. HTTPS (TLS) connections are used to protect all communication between the TOE and remote management interfaces. CLI sessions are secured via SSH, and REST API communications are protected via TLS. HTTPS and SSH protect data transfer and leverages cryptographic capabilities to prevent replay attacks. The management communication channels between the TOE and a remote entity are distinct from other communication channels and provide assured identification of both endpoints. This ensures the session between the remote browser and vShield Manager is secure. The TOE also provides a reliable timestamp for its own use.

1.5.2.7 Trusted Path/Channels

The communications between the TOE components and the remote vShield Manager is secured via a trusted path using TLS, or SSH. In addition, the session between the Edge and remote IT external entity is secured using an IPSEC VPN.

1.5.2.8 Data Security Management

The vShield Data Security provides the collection of system data and the analysis of the system data collected. It provides an authorized administrator with the capability to scan for data violations.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

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

- TLS VPN
- Anti-virus and anti-malware services
- Domain credential authorization
- Physical installation media

[22] Hypertext Transfer Protocol Secure

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[23] as of 2/1/2012 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ Augmented with Flaw Remediation ALC_FLR.2

[23] Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which 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:

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

3.1 Threats to Security

This section identifies the threats to the IT[24] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three 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 or parameters and no physical access to the TOE.
- TOE 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 or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.) An administrator is considered to be a TOE user.
- TOE failure: The threat of the TOE failing in its operations or exhausting its resources which leads to a failure of TOE operations.
- External IT Entities: External IT entities that are being used by malicious attackers to adversely affect the security of the TOE.

All are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[25] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable to the TOE:

Table 5 Threats

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms and a loss of user data while traversing the TOE.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to sensitive user data on a virtual machine.
T.MEDIAT	An attacker may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.UNAUTHORIZED_ACCESS	An attacker, process, or external IT entity may misrepresent itself as the TOE, or may gain unauthorized access to TOE to obtain TOE data, identification and authentication data, or executable code.
T.UNDETECTED_ACTIONS	An attacker or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected

[24] IT – Information Technology
[25] TSF – TOE Security Functionality

Name	Description
	and thus their effects cannot be effectively mitigated.
T.UNTRUSTPATH	An attacker may intercept traffic and cause TSF data to be inappropriately accessed (viewed, modified, or deleted) during transfer with a peer or trusted external IT entity.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 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 6 Assumptions

Name	Description
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.SCAN	The TOE must be able to collect information from the targeted virtual machines and analyze the data for violations.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators via TLS, SSH, or IPsec.
O.TRUSTEDPATH	The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 IT Security Objectives

Name	Description
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security and meets the TOE minimum

Name	Description
	requirements.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

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 9 Non-IT Security Objectives

Name	Description
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE.

Table 10 Extended TOE Security Functional Requirements

Name	Description
FCS_HTTPS_EXT.1	Extended: HTTPS
FCS_TLS_EXT.1	Extended: TLS
DSM_SDC_EXT.1	Extended: System data collection
DSM_ANL_EXT.1	Extended: Analysis

5.1.1 Class FCS: Cryptographic Support

Families in this class address the requirements for functions to implement cryptographic functionality as defined in CC Part 2.

5.1.1.1 Family FCS_HTTPS_EXT: Extended: HTTPS

Family Behaviour

Components in this family address the requirements for protecting communications using HTTPS. This is a new family defined for the FCS Class.

Component Leveling

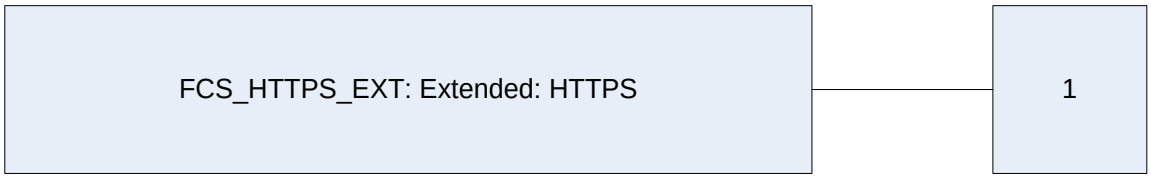

Figure 3 Extended: HTTPS family decomposition

FCS_HTTPS_EXT.1 Extended: HTTPS requires that HTTPS be implemented.

Management: FCS_HTTPS_EXT.1

a) There are no management activities foreseen.

Audit: FCS_ HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FCS_HTTPS_EXT.1 Extended: HTTPS
Hierarchical to: No other components.
FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC[26] 2818.
FCS_HTTPS_EXT.1.2
The TSF shall implement the HTTPS protocol using TLS as specified in FCS_TLS_EXT.1.
Dependencies: FCS_TLS_EXT.1 Extended: TLS

[26] Request For Comment

5.1.1.2 Family FCS_TLS_EXT: Extended: TLS

Family Behaviour

Components in this family address the requirements for protecting communications using TLS. This is a new family defined for the FCS Class.

Component Leveling

Figure 4 Extended: TLS family decomposition

FCS_TLS_EXT.1 Extended: TLS requires that TLS be implemented.

Management: FCS_TLS_EXT.1

a) There are no management activities foreseen.

Audit: FCS_ TLS _EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FCS_TLS_EXT.1 Extended: TLS

Hierarchical to: No other components.

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
[selection:
None
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Dependencies: No dependencies

5.1.2 Class DSM: Data Security Management

Data Security Management functions involve the collection of system data and the analysis of this system data. The DSM: Data Security Management function class was modeled after the CC FAU: Security audit class. The extended family and related components for DSM_SDC_EXT: System data collection was modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family DSM_ANL_EXT: Analysis was modeled after the family FAU_SAA: Potential violation analysis.

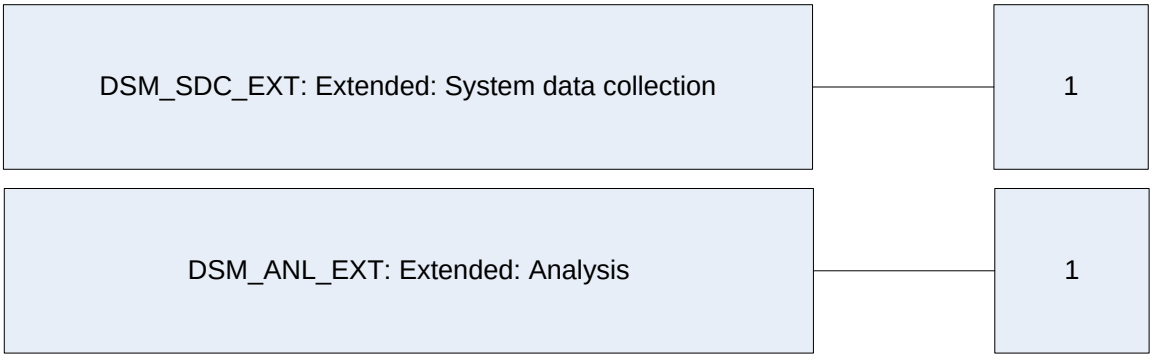

Figure 5 Class DSM: Data Security Management Function Class Decomposition

5.1.2.1 System data collection (DSM_SDC_EXT)

Family Behaviour

This family defines the requirements for the collecting of system data that take place under TSF control. This family identifies the level of system data collection, enumerates the types of data that shall be collected by the TSF, and identifies the minimum set of related information that should be provided within various system data event record types.

Component Leveling

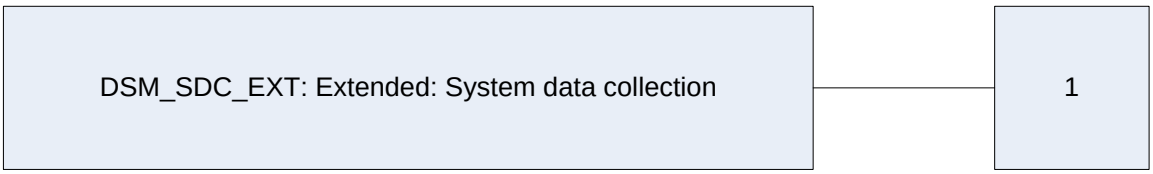

Figure 6 System flow data collection family decomposition

DSM_SDC_EXT.1 System data collection, defines the level of system data events, and specifies the list of data that shall be recorded in each record.

Management: DSM_SDC_EXT.1

a) There are no management activities foreseen.

Audit: DSM_SDC_EXT.1

b) There are no auditable events foreseen.

DSM_SDC_EXT.1 System data collection
Hierarchical to: No other components.
DSM_SDC_EXT.1.1
The TSF shall be able to collect the following information from the targeted virtual machine(s): [assignment: *description of data collected*.]

DSM_SDC_EXT.1.2
At a minimum, the TSF shall collect and record the following information:
- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Dependencies: FPT_STM.1 Reliable time stamps

5.1.2.2 Analysis (DSM_ANL_EXT)

Family Behaviour

This family defines the analysis the TOE performs on the collected system data. This family enumerates the types of analysis that is performed on the collected System data.

Component Leveling

Figure 7 Analysis family decomposition

DSM_ANL_EXT.1 analysis specifies the list of analyses the TOE will perform on the collected System data.

Management: DSM_ANL_EXT.1

1) Maintenance of the analysis functions by (adding, modifying, deletion) of policies from the set of policies.

Audit: DSM_ANL_EXT.1

2) Minimal: Enabling and disabling of any of the analysis mechanisms.

DSM_ANL_EXT.1 Analysis
Hierarchical to: No other components.
DSM_ANL.1_EXT.1

The TSF shall perform the following analysis function(s) on all System data collected:

- [*assignment: analytical functions*.]

Dependencies: DSM_SDC_EXT.1

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target 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 Part 2 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 text within brackets]. In keeping with these conventions, in the event an assignment is within a selection, it will be depicted as *italicized, underlined* text.
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement. In keeping with these conventions, in the event a refinement is within an assignment, it will be depicted as ***bold italicized*** text, and when a refinement is within a selection, it will be depicted in **bold underlined** text.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.
- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association			✓	
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓	✓	
FCS_CKM.1	Cryptographic key generation		✓	✓	
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		✓
FCS_HTTPS_EXT.1	Explicit: HTTPS				

Name	Description	S	A	R	I
FCS_TLS_EXT.1	Extended: TLS	✓			
FDP_IFC.1(1)	Subset information flow control		✓		✓
FDP_IFC.1(2)	Subset information flow control		✓		✓
FDP_IFC.1(3)	Subset information flow control		✓		✓
FDP_IFF.1(1)	Simple security attributes		✓	✓	✓
FDP_IFF.1(2)	Simple security attributes		✓	✓	✓
FDP_IFF.1(3)	Simple security attributes		✓	✓	✓
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected Authentication Feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1(1)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1(2)	Management of security functions behaviour	✓	✓		✓
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3(1)	Static attribute initialisation	✓	✓		
FMT_MSA.3(2)	Static attribute initialisation	✓	✓		
FMT_MTD.1(1)	Management of TSF data	✓	✓		
FMT_MTD.1(2)	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓		✓	✓
FPT_RPL.1	Replay Detection		✓		
FPT_STM.1	Reliable time stamps			✓	
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		
DSM_SDC_EXT.1	System data collection		✓		
DSM_ANL_EXT.1	Analysis		✓		

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

6.2.1 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; and

c) [*system and information flow events and the specifically defined auditable events as listed in the 'Auditable Events' column of Table 12]*.

Table 12 Auditable Events

Functional Component	Event Type	Auditable Events	Additional Audit Record Content
FMT_SMR.1	System Event	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FDP_IFF.1 (1) FDP_IFF.1 (2) FDP_IFF.1 (3)	Information Flow Event	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	System Event	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1 (1)	System Event	Firewall operation of the TOE	The identity of the authorized administrator performing the operation.
FMT_MOF.1(2)	System Event	Backup and restore operations for TSF data, information flow rule, and audit trail data; Maintenance of the analysis functions	The identity of the authorized administrator performing the operation.

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 (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, [*information specified in column three of Table 12*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

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

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1
The TSF shall provide [*an Enterprise Administrator, vShield Administrator, Security Administrator, Auditor, CLI Administrator*] with the capability to read ["*system events" as defined in Table 12*] 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_SAR.2 Restricted audit review
Hierarchical to: No other components.
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.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
FAU_SAR.3.1
The TSF shall provide the ability to apply [*sorting of system events over the GUI*] of audit data based on [
a) *module (for audit logs and system events)*
b) *user name (for audit logs only)*
c) *operation (for audit logs only)*
d) *resource (for audit logs only)*
e) *time (for audit logs and system events)*
f) *severity (for system events only)*
g) *event source (for system events only)*
h) *code (for system events only)*
i) *object name (for system events only)*
].
Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
FAU_STG.1.1
The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2
The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
FAU_STG.4.1
The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.
Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ANSI[27] X9.31 A.2.4; SP 800-90A Hash_DRBG*] and specified cryptographic key sizes [*listed in the 'Key Size (bits)' column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19*] that meet the following: [*standards listed in the 'Standards' column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19*].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 Level 1*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19* or message digest sizes] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 13, Table 14, Table 15, Table 16, Table 17, Table 18, and Table 19*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

[27] American National Standards Institute

Table 13 VMware Cryptographic Module FIPS-Approved Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES[28] ECB[29], CBC[30], CFB-1[31], CFB-8, CFB-64, OFB[32]	112, 168	N/A[33]	CAVP[34] (cert # 1620) FIPS 46-3
	AES operating in ECB, CBC, OFB, CFB-1, CFB-8, CFB-128	128, 192, 256	N/A	CAVP (cert #2701) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA[35] (ANSI X9.31, PKCS #1 v1.5, PSS) signature generation and signature verification	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1399) FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
	Digital Signature Algorithm (DSA) signature generation and signature verification	1024	N/A	CAVP (cert #822) Case: Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
Asymmetric key generation	RSA (ANSI X9.31) key pair generation	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1399) FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"

[28] DES Data Encryption Standard
[29] ECB Electronic Codebook
[30] CBC Cipher-block Chaining
[31] CFB Cipher Feedback
[32] OFB Output Feedback
[33] N/A Not Applicable
[34] CAVP Cryptographic Algorithm Validation Program
[35] RSA Rivest, Shamir, and Adleman

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2268) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC[36] SHA[37]-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1682) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"
Random number generation	ANSI[38] X9.31 PRNG[39] Appendix A.2.4	N/A	N/A	CAVP (cert #1255) ANSI X9.31, "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms"

[36] HMAC Keyed-Hash Message Authentication Code
[37] SHA Secure Hash Algorithm
[38] ANSI American National Standards Institute
[39] PRNG Pseudo-Random Number Generator

Table 14 Edge VMtools CAVP Validated Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES CBC	168	N/A	CAVP (cert #1660) FIPS 46-3
	AES ECB, CBC, OFB, CFB128 mode	128, 192, 256	N/A	CAVP (cert #2771) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA (PKCS#1 v1.5) signature generation	2048, 3072	N/A	CAVP (cert #1447) FIPS PUB 186-4, "Digital Signature Standard"
Cryptographic signature services	RSA (PKCS#1 v1.5) signature verification	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1447) FIPS PUB 186-2, "Digital Signature Standard"
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2328) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1733) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"

Table 15 VMware NSS Cryptographic Module FIPS-Approved Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES in ECB, CBC	168	N/A	CAVP (cert # 1619) FIPS 46-3
	Hardware-accelerated AES in ECB, CBC	128, 192, 256	N/A	CAVP (cert #2700) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA (ANSI X9.31, PKCS #1 v1.5, PSS) signature generation and signature verification	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1398) FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
	DSA signature generation and signature verification	1024	N/A	CAVP (cert #821) Case: Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
Asymmetric key generation	RSA (ANSI X9.31) key pair generation	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1398) FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
	DSA key pair generation	1024	N/A	CAVP (cert #821) Case: Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2267) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1681) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"
Random number generation	SP 800-90A Hash-based DRBG	256	256	CAVP (cert #443) NIST SP 800-90A, 'Recommendation for Random Number Generation Using Deterministic Random Bit Generators"

Table 16 VMware Kernel Cryptographic Module FIPS-Approved Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES in ECB, CBC, CTR	168	N/A	CAVP (cert # 1635) FIPS 46-3
	Hardware-accelerated AES in ECB, CBC, CTR, Hardware accelerated XTS-AES	128, 192, 256 128, 256	N/A	CAVP (cert #2718) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic hashing services	SHA-1, SHA-224, SHA-256	N/A	160, 224, 256	CAVP (cert #2283) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256	160, 224, 256	160, 224, 256	CAVP (cert #1697) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"
Random number generation	ANSI X9.31 PRNG Appendix A.2.4 using AES-128	N/A	N/A	CAVP (cert #1259) ANSI X9.31, "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms"

Table 17 Endpoint MUX CAVP Validated Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES CBC	168	N/A	CAVP (cert #1661, 1662) FIPS 46-3
	AES ECB, CBC, OFB, CFB128 mode	128, 192, 256	N/A	CAVP (cert #2772, 2773) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA (PKCS#1 v1.5) signature generation	2048, 3072	N/A	CAVP (cert #1448, 1449) FIPS PUB 186-4, "Digital Signature Standard"
Cryptographic signature services	RSA (PKCS#1 v1.5) signature verification	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1448, 1449) FIPS PUB 186-2, "Digital Signature Standard"
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2329, 2330) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1734, 1735) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"

Table 18 Endpoint VSM CAVP Validated Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES CBC	168	N/A	CAVP (cert #1663) FIPS 46-3
	AES ECB, CBC, OFB, CFB128 mode	128, 192, 256	N/A	CAVP (cert #2774) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA (PKCS#1 v1.5) signature generation	2048, 3072	N/A	CAVP (cert #1450) FIPS PUB 186-4, "Digital Signature Standard"
Cryptographic signature services	RSA (PKCS#1 v1.5) signature verification	1024, 1536, 2048, 3072, 4096	N/A	CAVP (cert #1450) FIPS PUB 186-2, "Digital Signature Standard"
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2331) FIPS Pub 180-3, "Secure Hash Standard."
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1736) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"

Table 19 VMware Java JCE (Java Cryptographic Extension) Cryptographic Module FIPS-Approved Algorithm Implementations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES in ECB, CBC, CFB-8, CFB-64, CMAC	168	N/A	CAVP (cert # 1623) FIPS 46-3
	AES in ECB, CBC, CFB, OFB, CMAC	128, 192, 256	N/A	CAVP (cert #2704) FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A
Cryptographic signature services	RSA (PKCS #1 v1.5, PSS) key pair generation	2048, 3072	N/A	CAVP (cert #1402) FIPS PUB 186-3, "Digital Signature Standard"
	DSA signature generation and signature verification	1024, 2048, 3072	N/A	CAVP (cert #825) Case: Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
Asymmetric key generation	RSA (PKCS #1 v1.5) key pair generation	2048, 3072	N/A	CAVP (cert #1402) FIPS PUB 186-3, "Digital Signature Standard"
	DSA key pair generation	1024, 2048, 3072	N/A	CAVP (cert #825) Case: Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"
Cryptographic hashing services	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #2271) FIPS Pub 180-3, "Secure Hash Standard."

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Message Digest Size	Standards (Certificate #)
Keyed-Hash message authentication	HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 224, 256, 384, 512	160, 224, 256, 384, 512	CAVP (cert #1685) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"
Random number generation	SP 800-90A Hash-based DRBG	256	512	CAVP (cert #446) NIST SP 800-90A, 'Recommendation for Random Number Generation Using Deterministic Random Bit Generators"

FCS_HTTPS_EXT.1 Extended: HTTPS
Hierarchical to: No other components.
FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2
The TSF shall implement the HTTPS using TLS as specified in FCS_TLS_EXT.1.
Dependencies: FCS_TLS_EXT.1 Extended: TLS

FCS_TLS_EXT.1 Extended: TLS
Hierarchical to: No other components.
FCS_TLS_EXT.1.1
The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246)] supporting the following ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
[None].
Dependencies: No dependencies.

6.2.3 Class FDP: User Data Protection

FDP_IFC.1 (1) Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 (1)
The TSF shall enforce the [*Edge UNAUTHENTICATED SFP*[46]] on [
a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) *operation: pass or reject information*].
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1 (2) Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 (2)
The TSF shall enforce the [*App UNAUTHENTICATED SFP*] on [
a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) *operation: pass or reject information*].
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1 (3) Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 (3)
The TSF shall enforce the [*Edge IPSEC VPN SFP*] on [
a) subjects:
- *a human user*
- *source subject: TOE interface on which information is sent;*
- *destination subject: TOE interface to which information is destined.;*

b) information: traffic sent through the TOE from one subject to another;
c) operations:
- *encrypt, decrypt, or*
- *pass or reject information*].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 (1) Simple security attributes
Hierarchical to: No other components.
FDP_IFF.1.1 (1)
The TSF shall enforce the [*Edge UNAUTHENTICATED SFP*] based on **at least** the following types of subject and information security attributes: [
a) *subject security attributes:*
- *presumed address;*
- *none;*

b) information security attributes:
- *presumed address of source subject;*
- *presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs;*
- *service;*

[46] Security Function Policy

- *composition of packets for the protocol FTP;*
- *information gleaned from prior packets; and*
- *none]*.

FDP_IFF.1.2 (1)

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

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*
- *the presumed address of the source subject, in the information, translates to an internal network address;*
- *the presumed address of the destination subject, in the information, translates to an address on the other connected network or context;*
- *the packets for protocol FTP conform to its protocol specifications; and*
- *a matched state of connection is recognized from information gleaned from prior packets flowing on the connection*

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*
- *the presumed address of the source subject, in the information, translates to an external network address;*
- *the presumed address of the destination subject, in the information, translates to an address on the other connected network or context;*
- *the packets for protocol FTP conform to its protocol specifications; and*
- *a matched state of connection is recognized from information gleaned from prior packets flowing on the connection*].

FDP_IFF.1.3 (1)

The TSF shall enforce the [*none*].

FDP_IFF.1.4 (1)

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 (1)

The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;*

c) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;*

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;*

e) *For the FTP protocol, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC[47]). This shall be accomplished through a protocol filtering proxy for FTP traffic.*]

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1 (2) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 (2)

The TSF shall enforce the [*App UNAUTHENTICATED SFP*] based on **at least** the following types of subject and information security attributes: [

a) *subject security attributes:*
- *presumed address;*
- *none;*

b) information security attributes:
- *presumed address of source subject;*
- *presumed address of destination subject;*
- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs*
- *service;*
- *information gleaned from prior packets; and*
- *none.].*

FDP_IFF.1.2 (2)

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

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:
- *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*
- *the presumed address of the source subject, in the information, translates to an internal network address;*
- *the presumed address of the destination subject, in the information, translates to an address on the other connected network or context; and*
- *a matched state of connection is recognized from information gleaned from prior packets flowing on the connection;*

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
- *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*
- *the presumed address of the source subject, in the information, translates to an external network address;*
- *the presumed address of the destination subject, in the information, translates to an address on the other connected network or context; and*
- *a matched state of connection is recognized from information gleaned from prior packets flowing on the connection].*

FDP_IFF.1.3 (2)

The TSF shall enforce the [*none*].

FDP_IFF.1.4 (2)

[47] Request For Comment

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 (2)

The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;*

c) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;*

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network]*

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1 (3) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 (3)

The TSF shall enforce the [*Edge IPSec VPN SFP*] based on the following types of subject and information security attributes: [

a) *subject security attributes:*
- *user identity;*
- *user group;*
- *presumed address;*

b) information security attributes:
- *presumed address of source subject;*
- *presumed address of destination subject*].

FDP_IFF.1.2 (3)

The TSF shall permit an information flow between a **source subject and a destination subject** via a controlled operation if the following rules hold: [

a) the user identity is part of the VPN users group;

b) the information security attributes match the attributes in a VPN policy rule (contained in the VPN ruleset defined by the Security Administrator) according to the following algorithm [access control policies are followed first, then the VPN flow decision is made]; and

c) the selected information flow policy rule specifies that the information flow is to be permitted, and what specific operation from FDP_IFC.1(3) is to be applied to that information flow].

FDP_IFF.1.3 (3)

The TSF shall enforce the [*none*].

FDP_IFF.1.4 (3)

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 (3)

The TSF shall explicitly deny an information flow based on the following rules: [

a) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;

b) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;

c) The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier;

d) *The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject*].

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 Static attribute initialization

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [
a) identity;
b) association of a human user with the authorized administrator role (as defined in FMT_SMR.1);
c) *password or other authentication credential*].
Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
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_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
FIA_UAU.5.1
The TSF shall provide [*password and certificate based authentication mechanisms*] to support user authentication.
FIA_UAU.5.2
The TSF shall authenticate any user's claimed identity according to the [*following multiple authentication mechanism rules:*
a) *reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;*
b) if configured, certificate-based authentication mechanism shall be used to establish an IPSEC VPN session between Edge Components such that successful authentication must be achieved before allowing any other TSF-mediated actions;
c) *reusable password mechanism shall be used for IPSEC VPN session between Edge Components such that successful authentication must be achieved before allowing any other TSF-mediated actions*
d) *password authentication will be used for SSH sessions]*
Dependencies: No dependencies

FIA_UAU.7 Protected Authentication Feedback
Hierarchical to: No other components.
FIA_UAU.7.1
The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.
Dependencies: FIA_UAU.1

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MOF.1 (1) Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1 (1)

The TSF shall restrict the ability to [disable, enable] the functions [

a) *firewall operation of the TOE;*
b) *multiple use authentication functions described in FIA_UAU.5*] to [*an Enterprise Administrator, vShield Administrator, CLI Administrator*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1 (2) Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1 (2)

The TSF shall restrict the ability to [disable, enable, determine and modify the behavior] the functions [

a) *backup and restore for TSF data, information flow rules, and audit trail data; and*
b) *communication of authorized external IT entities with the TOE*
c) *maintenance of the analysis functions by (adding, modifying, deletion) of policies from the set of policies*] to [*an Enterprise Administrator, vShield Administrator]*

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1

The TSF shall enforce the [*see information flow control SFP(s) as described in Table 20*] to restrict the ability to [*operation as described* in *Table 20*] the security attributes [*see security attributes in Table 20*] to [*authorized identified roles in Table 20*].

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

Table 20 Management of Security Attributes

Information Flow Control SFP	Operation	Security Attributes	Authorized Role
Edge UNAUTHENTICATED SFP	Delete attributes from a rule, modify attributes in a rule, add attributes to a rule	Listed in FDP_IFF1.1 (1)	Enterprise Administrator, Security Administrator
App UNAUTHENTICATED SFP	Delete attributes from a rule, modify attributes in a rule, add attributes to a rule	Listed in FDP_IFF1.1 (2)	Enterprise Administrator, Security Administrator
Edge IPSec VPN SFP	Delete attributes from a rule, modify attributes in a rule, add attributes to a rule	Listed in FDP_IFF1.1 (3)	Enterprise Administrator, Security Administrator

FMT_MSA.3 (1) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 (1)

The TSF shall enforce the [*Edge UNAUTHENTICATED SFP and Edge IPSEC VPN*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (1)

The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3 (2) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 (2)

The TSF shall enforce the [*App UNAUTHENTICATED SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (2)

The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 (1) Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete [*and assign*]**]** the [

- *user attributes defined in FIA_ATD.1.1*
- *maintenance of the group of users with read access right to the audit records*] to the [*Enterprise Administrator, vShield Administrator, CLI Administrator*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1 (2) Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [[*set*]**]** the [*time and date used to form the timestamps in FPT_STM.1.1*] to the [*Enterprise Administrator, Security Administrator*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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 management functions: [

a) Enable or disable the firewall operation of the TOE;
b) Enable or disable the multiple use authentication functions described in FIA_UAU.5;
c) Enable, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data;
d) Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE;
e) Delete attributes from a rule, modify attributes in a rule, add attributes to a rule for all security attributes in FDP_IFF.1 (1), (2), and (3);
f) Delete and create attributes/ rules defined in FDP_IFF.1 (1), (2), and (3);

g) Query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1;

h) *Set the time and date used to form the timestamps in FPT_STM.1.1*.]

Dependencies: No dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Enterprise Administrator, vShield Administrator, Security Administrator, CLI Administrator and Auditor*]

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.
Dependencies: No dependencies

FPT_RPL.1 Replay Detection
Hierarchical to: No other components.
FPT_RPL.1.1
The TSF shall detect replay for the following entities: [*network packets terminated at the IPsec VPN network interfaces of the TOE*].
FPT_RPL.1.2
The TSF shall perform: [*reject the data*] when replay is detected.
Dependencies: No dependencies

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps **for its own use**.
Dependencies: No dependencies

6.2.7 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*IPSEC VPN sessions between Edge and external IT entities*].

Dependencies: No dependencies

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure, [*none*]].

FTP_TRP.1.2

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

FTP_TRP.1.3

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

Dependencies: No dependencies

6.2.8 Class DSM: Data Security Management

DSM_SDC_EXT.1 System data collection
Hierarchical to: No other components
DSM_SDC_EXT.1.1

The TSF shall be able to collect the following information from the targeted virtual machine(s):

- [*Machine name*
- *DNS Name*
- *UUID*
- *IP Addres*
- *OS*
- *Timestamp*
- *Scan Policy that returned a result due to violating file*]

DSM_SDC_EXT.1.2

At a minimum, the TSF shall collect and record the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Dependencies: FPT_STM.1 Reliable time stamps

DSM_ANL_EXT.1 Analysis
Hierarchical to: No other components
DSM_ANL_EXT.1.1

The TSF shall perform the following analysis function(s) on all System data collected:

[

- *comparing collected system data at some point in time with those of another point in time to detect the differences (baseline);*
- *comparing collected system data with a set of standards;*
- *comparing collected system data with a set of policies;*
- *comparing collected system data with a set of exceptions.*]

Dependencies: DSM_ALN_EXT.1

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.2.

Table 21 below summarizes the requirements.

Table 21 EAL4 Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: Basic Design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused Vulnerability analysis

7 TOE Summary Specification

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

7.1 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 22 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	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_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_HTTPS_EXT.1	Explicit: HTTPS
	FCS_TLS_EXT.1	Extended: TLS
User Data Protection	FDP_IFC.1(1)	Subset information flow control
	FDP_IFC.1(2)	Subset information flow control
	FDP_IFC.1(3)	Subset information flow control
	FDP_IFF.1(1)	Simple security attributes
	FDP_IFF.1(2)	Simple security attributes
	FDP_IFF.1(3)	Simple security attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.2	User identification before any action

TOE Security Function	SFR ID	Description
Security Management	FMT_MOF.1(1)	Management of security functions behaviour
	FMT_MOF.1(2)	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation
	FMT_MSA.3(2)	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data
	FMT_MTD.1(2)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RPL.1	Replay Detection
	FPT_STM.1	Reliable time stamps
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Data Security Management	DSM_SDC_EXT.1	System data collection
	DSM_ANL_EXT.1	Analysis

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. The TOE categorizes the audit records into system events and audit logs. System events are events that are related to vCNS operation. They are recorded as audit records to detail various operational event of the TOE, such as a vShield Application reboot or a break in communication between a vShield Application and the vShield Manager. Events might relate to basic operation (Informational) or to a critical error (Critical). The audit logs provide a view into the actions performed by all vCNS users.

Edge, App, Endpoint, and VSM audit events not pertaining to information flow are provided in Syslog format, and are stored in the audit trail in a PostgreSQL database residing in the VSM VM. The system event message logged in the syslog has the following structure:
Syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter '::' (double colons)
Each name/value pair separated by delimiter ';;' (double semi-colons)

The TSF shall record within each audit record for both system events and audit logs at least the following information: Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. The audit records for system events contain the following fields: Event

Time, Severity, Event Source, Code, Event Message, Module, Object Name. The audit fields available for the audit logs tabs are: User Name, Module, Operation, Resource(s), and Time.

VSM audit logs and system events stored in the VSM can be sorted into a small set of fields through the GUI. VSM audit logs and system events can also be sorted based on the criteria as shown in Table 23 and Table 24 below respectively.

Table 23 Audit Log Filters

Option	Action
Module	Select the vShield module on which the action was performed
User Name	Select the login name of a user who performed the action
Operation	Select the type of action performed
Resource	Select the type of resource on which the action was performed
Time	Select the time when the operation was performed

Table 24 System Event Filters

Option	Action
Module	Select the vShield component on which the action was performed
Object Name	Select the object or resource name on which the action was performed
Code	Select the event code
Event Source	Select the object or resource which initiated the event
Severity	Select the severity level of the event
Time	Select the time when the event was occurred

As authorized administrators manage and configure the TOE, their activities are tracked and recorded as audit records. The resulting audit records can be examined to determine which security relevant activities took place and who (i.e., which user) is responsible for those activities. For audit events that result from actions of identified users, the TOE associates the action with the user who initiated the action in the audit records.

Logs stored in the VSM are viewable by users with the following roles over GUI and/or CLI: Enterprise Administrator, vShield Administrator, Security Administrator, CLI Administrator, and Auditor. Only authorized administrators with the appropriate role and permissions can review the audit logs.

In case of audit trail saturation the TSF does rollover of logs.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4

7.1.2 Cryptographic Support

The TOE provides IPSec VPN functionality for secure communications between two or more computers or protected networks over the public internet. This provides user authentication and encryption of information being passed through the VPN tunnel. The TOE uses the Internet Key Exchange (IKE) protocol for exchanging authentication information, and establishing the VPN tunnel. IKE uses either pre-shared secrets or digital certificates to authenticate peer devices. IKE uses a two phase process to secure the VPN tunnel. Phase 1 of IKE is the authentication phase. The nodes or gateways on either end of the tunnel

authenticate with each other, exchange encryption and decryption keys, and establish the secure VPN tunnel. Phase 2 is the negotiation phase. Once authenticated, two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN.

They then negotiate the number of SAs in the tunnel and the lifetimes allowed before requiring renegotiation of the encryption and decryption keys. Encryption methods implemented by the TOE include 3DES, AES-128, and AES-256. The hashing method used to authenticate the key is SHA-1. Keys are generated and destroyed securely. All cryptographic operations are performed by the FIPS 140-2 validated cryptographic modules. The TOE implements CAVP-validated cryptographic algorithms to handle all cryptographic functions for the encryption and the decryption of data.

The TOE protects the confidentiality and integrity of all data as it passes between the remote components of the TOE, or from the TOE to another trusted IT product. The TOE achieves this by using TLS and SSH which performs the encryption and the decryption of data that is being passed.

The TOE implements CAVP-validated cryptographic algorithms to handle all cryptographic functions for the encryption and the decryption of data.

All cryptographic operations are performed by a FIPS 140-2 validated cryptographic module.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_HTTPS_EXT.1, FCS_TLS_EXT.1

7.1.3 User Data Protection

For vShield, user data refers to network traffic traversing the Edge and App firewalls. vShield Edge protects access to user data in two ways: by restricting external access to TOE networks using its Layer 3 and 4 firewall functionality, and by enabling secure access to user data by external entities through IPSEC VPN connections. vShield Edge supports a site-to-site IPSec VPN between a vShield Edge and remote VPN router. The vShield Edge IPSEC VPN supports certificate authentication, pre-shared key mode, IP unicast traffic, and static routing protocol between the vShield Edge and remote VPN routers. Behind each remote VPN router, an authorized administrator can configure multiple subnets to connect to the internal network behind a vShield Edge through IPSec tunnels.

vShield App protects access to user data by functioning as an application-aware Layer 4 firewall capable of extremely granular access control. App enforces the App UNAUTHENTICATED SFP and operates at the vNIC[48] level, capable of leveraging access control policy based on portgroups. Additionally, App can leverage access control policy against specific VMs, identified by name, providing a scalable framework for preserving access control policy even if a VM is vMotioned between hosts, resources pools, or virtual datacenters. VMware VMotion enables the migration of a running VM from one host to the other with zero down time. VMotion is capable of migrating virtual machines between:

- One ESX host and another ESX host
- An ESX host and an ESXi host (and vice versa)

The user data that the TOE is protecting is the information passing through the TOE. This functionality is provided by the application of a stateful packet filtering firewall. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host IP addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets

[48] Virtual Network Interface Card

flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated. The firewall policy enforces rules on subjects that send traffic through the TOE, or receive traffic flowing through the TOE. The rules determine whether traffic should be passed from the sender to the receiver, denied passage, or discarded based on the following security attributes:

- presumed address of source
- presumed address of destination
- transport layer protocol
- service used
- Portgroups on which the connection request occurs
- composition of packets for FTP, Oracle TNS[49], DCE[50]/RPC[51], and ONC[52] RPC

The Edge and App Components perform stateful packet inspection on every packet received. Pattern matching is performed on incoming packets, as a function of the firewall state tables (e.g. flow table), and trigger responses that include:

- Accept - the packet is allowed through;
- Drop – the packet is dropped without notification to the sender.

Packet pattern matching can be configured to have security-relevant side-effects that include updating firewall state tables, and generating log messages. Rules are enforced on a first match basis from the top down. As soon as a match is found, the action associated with the rule is applied.

TOE Security Functional Requirements Satisfied: FDP_IFC.1 (1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2)

Edge facilitates IPSec VPN communication with IPSec enabled IT devices. The TOE compares plaintext traffic received from the IPSec VPN or destined to the IPsec VPN to the configured information flow policies. If the information flow meets a configured information flow policy that allows the traffic, then traffic originated from a VPN tunnel or destined to a VPN tunnel is permitted. If the information flow meets a configured policy that denies traffic, such traffic is not permitted.

The TOE supports the ability to set up VPN rules for the interfaces of the Edge. These rules determine whether or not a packet is sent via an encrypted tunnel to or from the interface based on:

- Presumed address of source
- Presumed address of destination

VPN tunnels will not be established unless a specific policy allowing them has been set up. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied.

These policies are created in the VSM. The TOE will take the following actions based on the VPN policy:

- pass packets without modifying;
- send IPSEC encrypted and authenticated packets to a VPN peer using ESP in tunnel mode as defined in RFC 2406;
- decrypt, verify authentication and pass received packets from a VPN peer in tunnel mode using ESP.

Note: the TOE does not support IPv6 IPSec VPNs. The TOE only supports IPSec VPN via IPv4.

TOE Security Functional Requirements Satisfied: FDP_IFC.1 (3), FDP_IFF.1 (3).

[49] TNS Transparent Network Substrate
[50] DCE Distributed Computing Environment
[51] RPC Remote Procedure Calls
[52] ONC Open Network Computing

7.1.4 Identification and Authentication

vShield maintains security attributes that are used in the operation of the TOE. vShield maintains the following user security attributes: user identity, association of a human user with the authorized administrator role, and password or other authentication credential. vShield maintains the definition of administrators by individual user IDs, and these IDs are associated with a specific user role which control the level of access of the administrator user within the TOE. Within the vShield Manager, a user's role defines the actions the user is allowed to perform on a given resource. The role determines the user's authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. The password an administrator user uses to authenticate to the TOE is securely maintained by the TOE. The administrator passwords are encrypted with AES256 and are stored in the PostgreSQL database.

TOE Security Functional Requirements Satisfied: FIA_ATD.1

The TOE must perform successful identification and authentication of the TOE administrator user before the TSF grants the user access to other TOE security functions. Administrator user authentication is enforced through the use of username-password combination or certificates.

Administrators accessing the vShield Web GUI must authenticate to the VSM VM. No management functionality is available to administrators prior to identifying to and authenticating with the Web GUI. Administrators accessing vShield management functionality via the vCenter snap-in authenticate with vCenter against an external authentication server, normally an Active Directory domain controller, which resides outside of the TOE. Likewise, administrators accessing vShield management functionality via the CLIs of the VSM VM, App VM, or Edge VM are authenticated by vCenter. CLI can be accessed over console port, or can be configured to access via SSH. Password-based authentication will be used for SSH sessions. Access to CLI over console is secured by password authentication. vShield Edge provides password and certificate based identification and authentication mechanisms for IPSEC VPN session establishment..

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UAU.5, FIA_UID.2

Within each TOE interface that accepts identification and authentication information, the password will be obscured while the user types it in so that it is not readable by another individual.

TOE Security Functional Requirements Satisfied: FIA_UAU.7

7.1.5 Security Management

Security management specifies how the TOE manages several aspects of the TSF including TSF data and security functions. The TSF data includes security related configuration data of the TSF and audit data. The management of TSF data and management functions is restricted to authorized administrators of the TOE which are defined by their assigned role as listed in Table 25.

Table 25 Authorized Administrator Roles

Role	Permissions
Enterprise Administrator	vShield operations and security.
vShield Administrator	vShield operations only: for example, install virtual appliances, configure port groups.
Security Administrator	vShield security only: for example, define data security policies, create port groups, create reports for vShield modules.

Role	Permissions
Auditor	Read only.
CLI Administrator	Limited vShield operations: for example viewing system settings and configurations, debugging and trouble shooting

The TOE provides authorized administrators with a GUI console referred to as the vShield Manager to easily manage the security functions and TSF data of the TOE. Within the vShield Manager, a user's role defines the actions the user is allowed to perform on a given resource. The role determines the user's authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows administrative control over specific resources and security functionality, or system-wide control if the right has no restrictions.

TOE Security Functional Requirements Satisfied: FMT_MOF.1 (1), FMT_MOF.1(2), FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

By default, Edge will drop packets unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). By default, App will allow all packets to be passed unless a specific rule has been set up to deny the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to deny traffic).

TOE Security Functional Requirements Satisfied: FMT_MSA.3 (1), FMT_MSA.3(2)

7.1.6 Protection of the TSF

The TOE provides protection mechanisms for its security functions. The Protection of the TSF function ensures the TSF data transmitted between various TOE components VSM, vShield Edge, vShield App, vShield Endpoint and Data Security, and VI Plug-in is secured. TSF data transmitted between VI Plug-in and VSM is secured via TLS. TSF data transmitted between VSM and vShield Edge is secured via TLS. TSF data transmitted between VSM and vShield App is secured via SSH. TSF data transmitted between VSM and vShield Endpoint and Data Security is secured via HTTPS. This protects the data from disclosure by encryption within the TLS, or SSH protocols, and by hashing that verifies the data has not been modified while in transit. This also prevents replay attacks since the TLS sessions use a random nonce.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_RPL.1

vShield provides a source of date and time information for the vShield components that is used in audit timestamps. This centeralized source of time ensures that the TOE provides a reliable timestamp for all auditing. In addition, vShield can connect to a Network Time Protocol (NTP) Server that will provide time updates. vShield uses the timestamp updates from the NTP Server to ensure that its own timestamps remain accurate. The NTP Server is considered outside the TOE boundary. This function can only be managed from within the vShield Manager by an authorized administrator that has successfully been identified and authenticated to the TOE.

TOE Security Functional Requirements Satisfied: FPT_STM.1

7.1.7 Trusted Path/Channels

vShield provides trusted channels for all data from disclosure or modification while in transit between TOE components and between TOE components and authorized IT entities. All communications between the vShield components are secured via TLS or SSH. TLS or SSH is used to provide trusted channels between

separate parts of the TOE, between the TOE and authorized IT entities and to prevent the data from disclosure and modification. In addition, vShield Edge is able to secure the session between Edge and an external IT entity with an IPSEC VPN. The TOE implements TLS for protection of remote web access to the management of the TOE via the vShield Manager. The TOE generates its own certificate which is then shared among the distributed components. The TOE uses FIPS validated cryptographic algorithms to implement the above cryptographic functions.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1

7.1.8 Data Security Management

The Data Security Management provides the collection of system data and the analysis of the system data collected. The collected data is stored in the PostgreSQL database. The vShield Data Security Component scans the VMs and analyzes the collected system data according to configured policies.

To begin using vShield Data Security, an authorized administrator creates a policy that defines the regulations that apply to data security in an organization and specifies the areas of the environment and files to be scanned. When a vShield Data Security scan is started, vShield analyzes the data on the virtual machines in the vSphere inventory and reports the number of violations detected and the files that violated the configured policy.

To define a policy, an authorized administrator must specify the following:

1. Regulations

A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information. An authorized administrator can select the regulations that a company needs to comply. When an authorized administrator runs a scan, vShield Data Security identifies data that violates the regulations in the configured policy and is sensitive for the organization. The Security Administrator will select the regulations the company is targeting and then vShield will identify files that contain information which violates these particular regulations.

2. Exclusion areas

By default, all virtual machines in the targeted data center are subject to sensitive data discovery. A Security Administrator can exclude specific areas of the environment from the data security scan.

3. File filters

The Security Administrator can create filters to limit the data being scanned and exclude file types unlikely to contain sensitive data from the scan. Using file filters a Security Administrator can restrict the files that are monitored based on size, last modified date, or file extensions.

The vShield Endpoint Component facilitates scanning of the VMs and sends the collected information to the dedicated secure VM for the anti-virus and anti-malware processing.
Through the violation reports in the VSM, the Security Administrator or Auditor can view the violations that were discovered by the data security scan.

TOE Security Functional Requirements Satisfied: DSM_SDC_EXT.1, DSM_ANL_EXT.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3. This ST does not conform to a PP.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 26 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms and a loss of user data while traversing the TOE.	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators via TLS, SSH, or IPsec.	O.TOE_ADMINISTRATION counters this threat by ensuring that only authorized administrators are able to log in and configure the TOE, and the TOE provides protections for logged-in Administrators.
T.MEDIAT An attacker may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.	O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.	O.MEDIAT counters this threat by ensuring that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
T.EXPLOIT An attacker may attempt to gain unauthorized access to sensitive user data on a virtual machine.	O.SCAN The TOE must be able to collect information from the targeted virtual machines and analyze the data for violations.	O.SCAN counters this threat by ensuring that the TOE collects information from the virtual machines and analyzes the collected data.
T.UNAUTHORIZED_ACCESS An attacker, process, or external IT entity may misrepresent itself as the TOE, or may gain unauthorized access to TOE to obtain TOE data, identification and authentication data, or executable code.	O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	O.PROTECTED_COMMUNICATIONS counters this threat by providing protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

Threats	Objectives	Rationale
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators via TLS, SSH, or IPsec.	O.TOE_ADMINISTRATION counters this threat by ensuring that only administrators are able to log in and configure the TOE and providing protections for logged-in administrators.
T.UNDETECTED_ACTIONS An attacker or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.	O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and send those data to an external IT entity.	O.SYSTEM_MONITORING counters this threat by generating audit data.
T.UNTRUSTPATH An attacker may intercept traffic and cause TSF data to be inappropriately accessed (viewed, modified, or deleted) during transfer with a peer or trusted external IT entity.	O.TRUSTEDPATH The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.	O.TRUSTEDPATH counters this threat by ensuring that users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 27 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security and meets the TOE minimum requirements.	OE.GUIDAN satisfies the assumption that the users who manage the TOE are trusted and follow all guidance so that the TOE be delivered, installed, administered, and operated in a manner that maintains security and meets the TOE minimum requirements.
	OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	OE.NOEVIL satisfies the assumption that authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	OE.PHYSICAL satisfies the assumption that the TOE environment provides physical security commensurate with the value of the TOE and the data it contains.
A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.	OE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.	OE.REMACC satisfies the assumption that authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN satisfies the assumption that information can not flow among the internal and external networks unless it passes through the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

The extended requirements are defined in section 5. These SFRs exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 28 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and	FDP_IFC.1(1) Subset information flow control	This requirement meets the objective by ensuring that the TOE identifies the entities involved in the Edge

Objective	Requirements Addressing the Objective	Rationale
external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.		UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa).
	FDP_IFC.1(2) Subset information flow control	This requirement meets the objective by ensuring that the TOE identifies the entities involved in the App UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa).
	FDP_IFF.1(1) Simple security attributes	This requirement meets the objective by ensuring that the TOE identifies the attributes of the users sending and receiving the information in the Edge UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.
	FDP_IFF.1(2) Simple security attributes	This requirement meets the objective by ensuring that the TOE identifies the attributes of the users sending and receiving the information in the App UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.
	FDP_IFF.1(3) Simple security attributes	This requirement meets the objective by ensuring that the TOE ensures that all IPSEC encrypted data received from a peer TOE or trusted external IT entity is properly decrypted and authentication verified.
O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations.

Objective	Requirements Addressing the Objective	Rationale
distributed TOE, and authorized IT entities.	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE can zeroize cryptographic keys.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE can perform encryption and decryption in accordance with the defined algorithms and key sizes.
	FCS_HTTPS_EXT.1 Explicit: HTTPS	The requirement meets the objective by ensuring that the TOE protects remote communications.
	FCS_TLS_EXT.1 Extended: TLS	The requirement meets the objective by ensuring that the TOE protects remote communications.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by ensuring that the TOE protects TSF data from disclosure when transmitted between separate parts of the TOE.
	FPT_RPL.1 Replay Detection	The requirement meets the objective by ensuring that the TOE detects replay of network packets.
	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by ensuring that the TOE provides a trusted path between itself and authorized IT entities from modification or disclosure.
	FTP_TRP.1 Trusted path	The requirement meets the objective by ensuring that the TOE provides a trusted path between itself and authorized IT entities from modification or disclosure.
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and send those data to an external IT entity.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.

Objective	Requirements Addressing the Objective	Rationale
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that only authorized users are able to review logs.
	FAU_SAR.3 Selectable audit review	This requirement meets this objective by providing searches and sorting of the audit data.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit records from unauthorized deletion and prevention of unauthorized modifications.
	FAU_STG.4 Prevention of audit data loss	This requirement meets this objective by taking action in case of audit trail storage exhaustion. This requirement meets this objective by providing protection mechanisms for the audit trail.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the TOE provides reliable timestamps.
O.SCAN The TOE must be able to collect information from the targeted virtual machines and analyze the data for violations.	DSM_SDC_EXT.1 System data collection	The requirement meets the objective by ensuring that the TOE collects information from the virtual machines.
	DSM_ANL_EXT.1 Analysis	The requirement meets the objective by ensuring that the TOE analyzes the virtual machines for violations to the configured policy.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the	FCS_CKM.1 Cryptographic key generation	This requirement meets the objective by providing protections for logged-in administrators via TLS, SSH or Ipsec sessions.

Objective	Requirements Addressing the Objective	Rationale
TOE, and provide protections for logged-in administrators via TLS, SSH, or IPsec.	FCS_COP.1 Cryptographic operation	This requirement meets the objective by providing protections for logged-in administrators via TLS, SSH or Ipsec sessions.
	FCS_HTTPS_EXT.1 Explicit: HTTPS	This requirement meets the objective by providing protections for logged-in administrators via TLS sessions.
	FCS_TLS_EXT.1 Extended: TLS	This requirement meets the objective by providing protections for logged-in administrators via TLS sessions.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by ensuring that the TOE maintains the user's security attributes.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE ensures that a user must be successfully authenticated before being allowed access to the TOE management functions.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that the TOE ensures that a user must be successfully authenticated before being allowed access to TOE management functions.
	FIA_UAU.7 Protected Authentication Feedback	The requirement meets the objective by ensuring that the TOE provides obscured feedback while the user is authenticating.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE ensures that a user must be successfully identified before being allowed access to the TOE management functions.
	FMT_MOF.1(1) Management of security functions behaviour	The requirement meets the objective by ensuring that the TSF restricts the ability of the TOE to start up and shut down operation and multiple authentication function to an authorized administrator.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MOF.1(2) Management of security functions behaviour	The requirement meets the objective by ensuring that the TSF restricts the ability of the TOE to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts which users are allowed to query and modify security attributes.
	FMT_MSA.3(1) Static attribute initialisation	The requirement meets the objective by ensuring that there is a default deny policy for the information flow control security rules.
	FMT_MSA.3(2) Static attribute initialisation	The requirement meets the objective by ensuring that there is a default allow policy for the information flow control security rules.
	FMT_MTD.1(2) Management of TSF data	The requirement meets the objective by ensuring that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator.
	FMT_MTD.1(1) Management of TSF data	The requirement meets the objective by ensuring that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TSF restrict the set of management functions to the authorized administrator.
	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.

Objective	Requirements Addressing the Objective	Rationale
	FTP_ITC.1 Inter-TSF trusted channel	This requirement meets the objective by providing protections for logged-in administrators via Ipsec sessions.
O.TRUSTEDPATH The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.	FDP_IFC.1(3) Subset information flow control	This requirement meets the objective by ensuring that all IPSEC encrypted data received from a peer TOE or trusted external IT entity are properly decrypted and authentication verified.

8.5.2 Security Assurance Requirements Rationale

EAL4, augmented with ALC_FLR.2 was chosen to provide a moderate- to high-level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. At EAL4+, penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 29 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 29 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2 is hierarchical to FIA_UID.1.
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	✓	
FCS_TLS_EXT.1	No dependencies	✓	
FDP_IFC.1(1)	FDP_IFF.1(1)	✓	
FDP_IFC.1(2)	FDP_IFF.1(2)	✓	
FDP_IFC.1(3)	FDP_IFF.1(3)	✓	
FDP_IFF.1(1)	FMT_MSA.3	✓	
	FDP_IFC.1(1)	✓	
FDP_IFF.1(2)	FMT_MSA.3(2)	✓	
	FDP_IFC.1(2)	✓	
FDP_IFF.1(3)	FDP_IFC.1(3)	✓	
	FMT_MSA.3(1)	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2 is hierarchical to FIA_UAU.1.
FIA_UID.2	No dependencies	✓	
FMT_MOF.1(1)	FMT_SMF.1	✓	
FMT_MOF.1(2)	FMT_SMR.1	✓	
FMT_MSA.1	FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MSA.3(2)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MTD.1(2)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(1)	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_ITT.1	No dependencies	✓	
FPT_RPL.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	
DSM_SDC_EXT.1	No dependencies	✓	
DSM_ANL_EXT.1	DSM_SDC_EXT.1	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Terminology

Table 30 Terms

Name	Definition
Authorized Administrator	A user with administrator TOE access that has been successfully identified and authenticated by the TOE.
Botnet	A botnet is a collection of compromised computers connected to the Internet. Termed *bots*, they are used for malicious purposes. When a computer becomes compromised, it becomes a part of a botnet.
Peer	In IPSec terminology, a peer is a remote-access client or another secure gateway.
Security Zone	Security zones within VMware ESXi are logical zones that span all the physical resources of the virtual datacenter, so that distinct levels of trust, privacy and confidentiality can be maintained. These zones are firewalled off from each other to comply with corporate security policies and industry regulations.
Target network	The domain of network and managed devices to be analyzed by the TOE.

9.2 Acronyms

Table 31 Acronyms

Acronym	Definition
ACE	Access Control Entries
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CSP	Critical Security Parameters
CTR	Counter Mode
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone

Acronym	Definition
DNS	Domain Name Server
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EC	Elliptical Curve
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
PostgreSQL	Postgre Structured Query Language
NAT	Network Address Translation
NIST	Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
REST	Representational State Transfer
RFC	Request for Comment
SA	Security Associations
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Languages

Acronym	Definition
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSAP	Transport Service Application Protocol
TSP	TOE Security Policy
UDP	User Datagram Protocol
VDC	Virtual Datacenters
vDS	Distributed Switch
VLAN	Virual Local Area Network
vNIC	Virtual Network Interface Card
VM	Virtual Machine
VPN	Virtual Private Network
VSM	vShield Manager

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com