VMware

NSX v6.3 for vSphere

Security Target

MARCH 2017

Document prepared by

Aeson STRATEGY
IT RISK & SECURITY

vmware

Document History

Version	Date	Author	Description
0.1	29 Jan 2016	A Boulton	Initial draft ST.
0.2	03 Feb 2016	A Boulton	Incorporate discussion/comments
1.0	14 Mar 2016	A Boulton	Evaluation Draft. Some crypto specifications pending FIPS 140 validation.
1.1	14 Mar 2016	A Boulton	Internal review before submission.
1.2	28 Mar 2016	A Boulton	Address ASE OR 1, include NSX Controller, Update Crypto.
1.3	12 Apr 2016	A Boulton	Address ASE OR 1.2
1.4	18 Apr 2016	A Boulton	Address ASE OR 1.3
1.5	20 April 2016	A Boulton	Address ASE OR 1.3 and 1.4
1.6	03 May 2016	M. Mulligan	Crypto module and SFR changes
1.7	17 May 2016	A Boulton	Address Certifier OR
1.8	14 June 2016	A Boulton	Updated TOE version to 6.2.4 to address minor bug fixes and name of TOE for release.
1.9	08 July 2016	A Boulton	Added Edge SSL VPN, change to crypto.
2.0	25 August 2016	A Boulton	Version change (no functional change).
2.1	03 November 2016	A Boulton	Removal of IPSec VPN component, inclusion of NSX Manager Appliance GUI.
2.2	02 December 2016	A Boulton	Resolution of ASE_ADV_AGD_ATE_OR1, changes to remove certificate-based client VPN authentication, changes for SSH vulnerability.
2.3	05 December 2016	A Boulton	Removal of FIA_UAU.5 to reflect certificate-based authentication for VPN being removed from scope, and associated changes.
2.4	27 March 2017	A Boulton	Updates for FIPS
2.5	30 March 2017	M McKay	Removed review comments and corrected FIPS info

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/

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Overview

1 NSX is a software-only network virtualization platform that programmatically provisions and manages virtual networks through software.

2 The TOE is the VMware NSX v6.3 for vSphere, and will hereafter be referred to as the TOE or NSX throughout this document. The TOE is a software-only security solution for VMware virtualized environments that provides firewall and data protection security services.

3 NSX creates a network topology from a library of logical networking elements and services such as logical switches, routers, firewalls, load balancers, VPN, and workload security. NSX deploys virtual networks over existing networks and on supported hypervisors, allowing legacy VLANs and physical hosts to be mapped into virtual networks.

4 NSX provides protection to virtualized networks from network- based attacks, protecting data in transit between datacenters and preventing misuse of network services and protected information contained within the network. NSX includes virtual appliances and services essential for protecting virtual machines from attacks within/from the virtual and the physical environments.

5 NSX can be configured through a number of interfaces including vSphere Web Client, NSX Manager Appliance GUI, a command line interface (CLI), and REST API.

6 NSX 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.

7 NSX 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 - a user- installable or OEM-embedded virtualization layer that runs directly on industry standard x86 64bit-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server.

8 This Security Target (ST) defines the NSX v6.3 for vSphere Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

9 For a precise statement of the scope of incorporated security features, refer to section 2.3.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	VMware NSX v6.3 for vSphere
Security Target	VMware NSX v6.3 for vSphere Security Target, v2.5
FIPS 140-2 Status	Includes four FIPS 140-2 cryptographic modules: • Level 1, OpenSSL v1.0.2h FIPS Object Module v2.0.9, CMVP Certificate 2839 • Level 1, BouncyCastle FIPS 1.0, CMVP Certificate 2866 • Level 1, Linux Kernel Crypto Ubuntu v12.04, CAVP: AES: #4133, TDES: #2258, SHA: #3402, HMAC: #2705 • Level 1, NSS cryptographic module v3.23, CAVP SHA-1: SHS Cert # 3418

1.3 Conformance Claims

10 This ST supports the following conformance claims:

a) CC version 3.1 Release 4

b) CC Part 2 extended

c) CC Part 3 conformant

d) Evaluation Assurance Level (EAL) 2+ augmented (ALC_FLR.1)

1.4 Terminology

Table 2: Terminology

Term	Definition
ACE	Access Control Entries
ACL	Access Control List

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
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.
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
DFW	NSX Distributed Firewall
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
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
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.
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Languages

SSL	Secure Sockets Layer
ST	Security Target
Target Network	The domain of network and managed devices to be analyzed by the TOE.
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
USVM	Universal Security Virtual Machine
VDC	Virtual Datacenters
vDS	Distributed Switch
VLAN	Virual Local Area Network
vNIC	Virtual Network Interface Card
VM	Virtual Machine
VPN	Virtual Private Network

2 TOE Description

2.1 Type

11 The TOE is a software-only security solution for VMware virtualized environments that provide firewall and data protection security services.

2.2 Usage

12 The TOE consists of the following components:

a) **NSX Manager.** The NSX Manager is the centralized network management component of NSX, and is installed as a virtual appliance on an ESXi host in the vCenter Server environment. It provides an aggregated system view. One or more NSX Manager maps to a single vCenter Server environment and multiple NSX Edge, and Guest Introspection instances.

The NSX Manager Component can be accessed via a number of different interfaces:

- NSX Manager Appliance GUI - Provides way to configure NSX Manager appliance through web based UI, principally for installation procedures.
- vSphere Web Client - Provides way to configure NSX Manager appliance through web based UI, principally for administration of installed appliance.
- Command Lind Interface (CLI) – Admin user only over SSH.
- REST APIs - accessed over TLS via browser.

b) **NSX Distributed Firewall.** NSX Distributed Firewall (DFW) is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. It allows the creation of access control policies based on VMware vCenter objects like datacenters and clusters, virtual machine names and tags, network constructs such as IP/VLAN/VXLAN addresses, as well as user group identity from Active Directory. NSX kernel level firewall complements NSX Edge stateful firewall capabilities.

c) **NSX Controller.** NSX Controller is an advanced distributed state management system that controls virtual networks and overlays secure transport tunnels. NSX Controller is the central control point for all logical switches within a network and maintains information of all virtual machines, hosts, logical switches, and VXLANs. The NSX Manager creates self-signed certificates for the nodes of Controller clusters and installs those certificates over a secure TLS channel over HTTPS. Controller nodes can then communicate with each other over HTTPS using those NSX Manger-signed certificates.

d) **NSX Edge.** NSX Edge provides network edge security and gateway services to isolate a virtualized network. You can install an NSX Edge either as a logical (distributed) router or as a services gateway. The NSX Edge gateway connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, dynamic routing, and Load Balancing. Common deployments of NSX Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the NSX Edge creates virtual boundaries for each tenant. Security features for Edge Services include a stateful Firewall, L2 VPN, and SSL VPN-Plus.

NSX Edge can be managed through the vSphere Web Client. Provisioning and configuration is also supported through REST APIs. NSX 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 NSX Edge.

e) **Guest Introspection.** Guest introspection 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. Guest Introspection, through the Universal Security Virtual Machine (USVM), is able to provide 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 Guest Introspection only provides a framework, no anti-virus SFRs are being claimed for this component.

13 A simple representation of NSX component architecture is depicted in Figure 1, broken down in Management, Control and Data planes. For completeness of operational context, features outside of the TOE have been included in Figure 1.

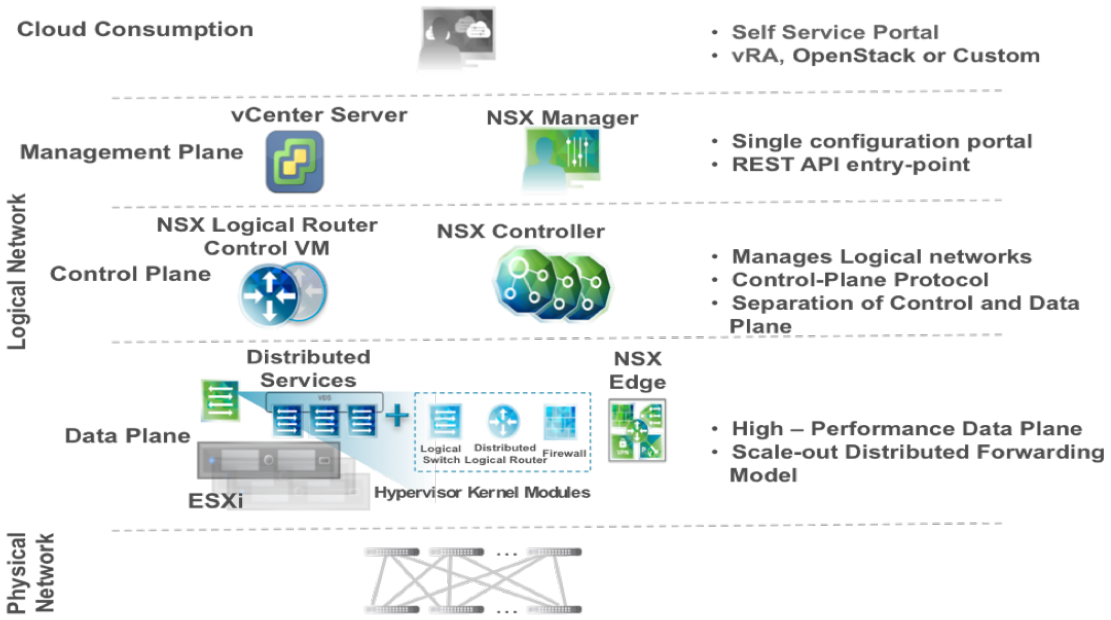


Figure 1: NSX Component Architecture

2.4 Security Functions

14 The TOE provides the following security functions:

a) **Security Audit.** The TOE generates audit records for security relevant events related to NSX operation (system events), and actions of the authorized administrators within the NSX Manager and back-end users with the audit user role from the VSphere Web Client or CLI (audit logs), or the System Administrator role through NSX Manager Appliance GUI. The TOE provides an authorized administrator access to view the audit logs created as a result of administrator actions through the NSX 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.

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

- VSphere Web Client and NSX Manager Appliance GUI connecting to the NSX Manager is secured by HTTPS.
- The connection of the NSX Manager Client plug-in User Interface and NSX Manager User Interface to the NSX Manager is secured via TLS.
- NSX Edge supports three VPN capabilities, two of which are in scope:
  i. SSL-VPN Plus for remote users accessing servers and applications in private networks over a web interface.
  ii. L2 VPN allows networks to retain protected network connectivity across geographical boundaries.
- CLI sessions are secured via SSH
- REST API communications are protected via TLS.

c) **User Data Protection.** For NSX, user data refers to network traffic traversing the NSX Edge Firewall and NSX Distributed Firewall. 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.

d) **Identification and Authentication.** The TOE provides functionality that requires administrators to verify their claimed identity. The Identification and Authentication TSF 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.

e) **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.

f) **Protection of the TSF.** The TOE implements HTTPS 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, leveraging their cryptographic capabilities to prevent replay attacks. The management communication channels between the TOE and a remote entity are distinct from other communication channels and

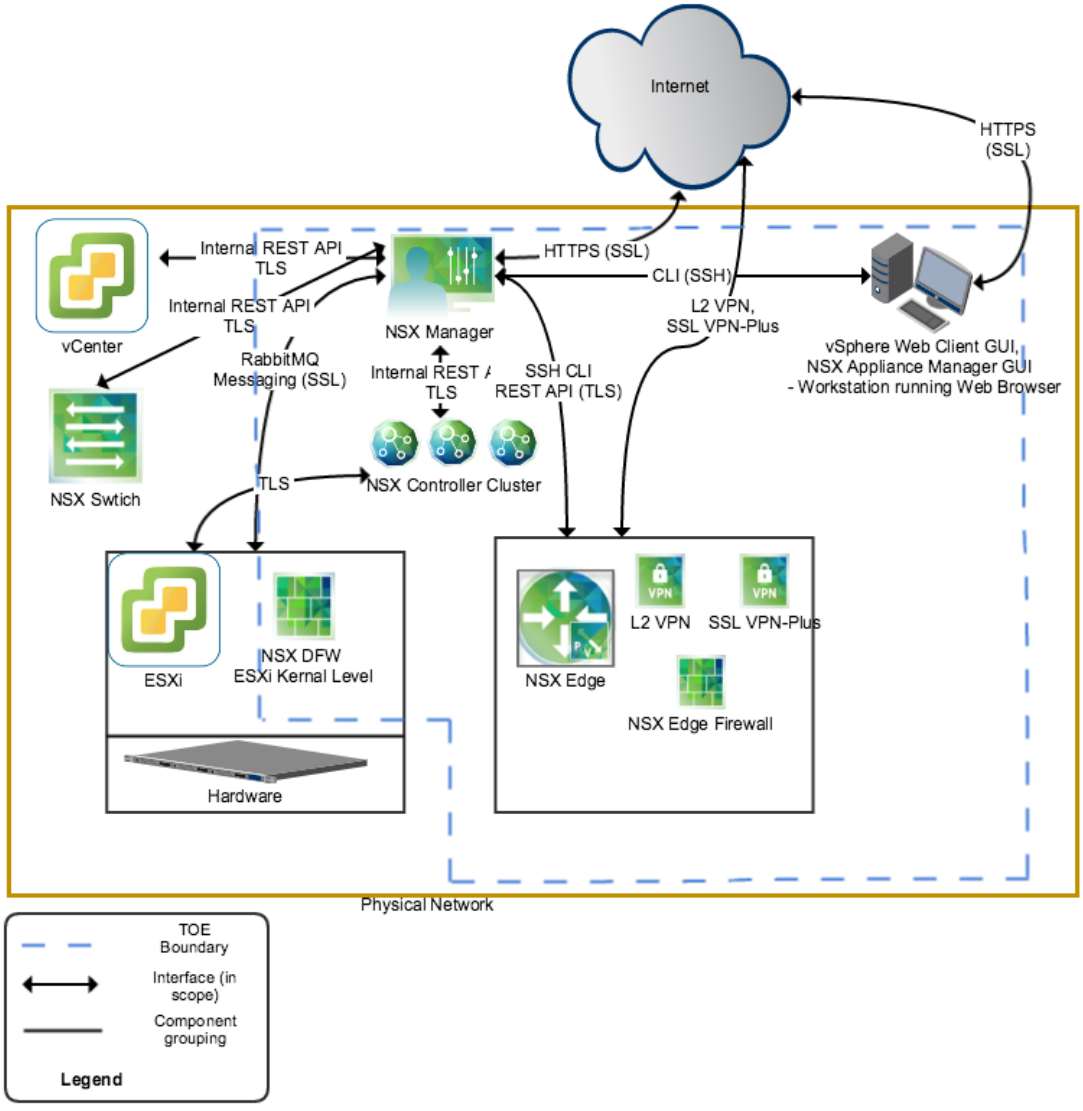
provide assured identification of both endpoints. This ensures the session between the remote browser and NSX Manager is secure. The TOE also provides a reliable timestamp for its own use.

g) **Trusted Path/Channels.** The communications between the TOE components and the remote NSX Manager is secured via a trusted path using TLS, or SSH. SSL VPN-Plus (Edge SSL VPN) allows remote users to connect securely to private networks behind an NSX Edge gateway using an OpenSSL VPN with TLS. In addition, L2 VPN provides a TLS tunnel connecting separate networks at different physical locations.

2.5 Physical Scope

15 The TOE is software-only and the TOE Components are the same as the product components as specified in section 2.2 of this document, Figure 2, and 3 below. The TOE Boundary includes all the VMware-developed parts of the NSX product.

Figure 2: TOE Scope



16 The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in Section 2.4.2 of the ST and Table 3 below.

Table 3: TOE and Environment Requirements

Component	Requirement	TOE	TOE Environment
NSX 6.3, Build 4559345	Software-only	✓	
NSX Manager	Hardware: • Memory – 12GB • Disk Space – 60 GB • vCPU - 4		✓
NSX Controller	Hardware: • Memory: 4 GB • Disk Space: 20 GB • vCPU - 4		✓
NSX Edge (Compact)	Hardware: • Memory – 512 MB • Disk Space – 512 MB • vCPU - 1		✓
Guest Introspection	Hardware: • Memory – 1 GB • Disk Space – 4 GB • vCPU - 2		✓
TOE Environment Supporting Software	Software: • VMware vCenter Server 6.0u2 • VMware ESXi 6.0u2 or later • VMware Tools		✓
TOE Environment GUI Web Browsers	Software: • Microsoft Internet Explorer 11 • Mozilla Firefox 45		✓

	• Safari 9 • Chrome 48		

2.5.1 Guidance Documents

17 The TOE includes the following guidance documents:

a) NSX Installation Guide NSX for vSphere 6.2

b) NSX Administration Guide NSX for vSphere 6.2

c) NSX API Guide 6.0.4 for vSphere

d) NSX Command Line Interface Reference NSX 6.2 for vSphere

e) VMware NSX for vSphere Hardening Guide version 1.6

f) NSX 6.2.x Troubleshooting Guide for vSphere 6.2

g) Self-Service Download Maintenance Tool Quick Reference Guide Version 1.8

h) NSX for vSphere 6.3.0 Release Notes

2.5.2 Non-TOE Components

18 The TOE operates with the following components in the environment:

a) **Anti-virus and anti-malware services.** These are provisioned by third parties.

b) **Audit Server.** The TOE can utilize a Syslog server to store audit records.

c) **Web Browser.** The remote administrator can use a web browser to access the vSphere Web Client and NSX Manager Appliance interfaces.

d) **Domain credential authorization.**

e) **All physical installation media.**

f) **Top-of-Rack physical switch integration.**

2.6 Logical Scope

19 The logical scope of the TOE comprises the TOE usage described in Section 2.2 and the security functions defined in section 2.3.

3 Security Problem Definition

3.1 Threats

20 Table 4 identifies the threats addressed by the TOE.

Table 4: Threats

Identifier	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.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
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.

3.3 Organizational Security Policies

21 There are no Organizational Security Policies (OSPs) defined for this ST.

3.4 Assumptions

22 Table 5 identifies the assumptions related to the TOE's environment.

Table 5: Assumptions

Identifier	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 an external networks unless it passes through the TOE.

4 Security Objectives

4.1 Objectives for the Operational Environment

23 Table 6 identifies the objectives for the operational environment.

Table 6: Operational environment objectives

Identifier	Description
OE.GUIDAN	The TOE must 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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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 Objectives for the TOE

24 Table 7 identifies the security objectives for the TOE.

Table 7: Security objectives

Identifier	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_COMMUNICATI ONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.

Identifier	Description
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.

5 Security Requirements

5.1 Conventions

25 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with *italicized text*.

b) **Refinement.** Indicated with **bold text** and ~~strikethroughs~~.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with *italicized and underlined text*.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

26 Explicitly stated SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs.

5.2 Extended Components Definition

27 There are no extended components defined for the TOE.

5.4 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title
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
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_IFC.1(4)	Subset information flow control
FDP_IFC.1(5)	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
FDP_IFF.1(4)	Simple security attributes
FDP_IFF.1(5)	Simple security attributes
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User identification before any action

Requirement	Title
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

5.4.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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 9*].

Table 9: Audit 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) FDP_IFF.1 (4) FDP_IFF.1 (5)	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, 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 9*].

FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

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

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*an Enterprise Administrator, NSX Administrator, System Administrator, Security Administrator, Auditor*] with the capability to read *["system events" as defined in Table 9*] 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.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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)

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

5.4.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*SP 800-90A R1 Hash_DRBG*] and specified cryptographic key sizes [*listed in the 'Key Size (bits)' column of Table 10*] that meet the following: [*standards listed in the 'Standards' column of Table 10*].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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.4.1 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*].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 10*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 10*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 10 or message digest sizes*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 10*].

Table 10: VMware Cryptographic Module FIPS-Approved Algorithm Implementations

Operation	Algorithm	Key Size (bits)	Message Digest Size (bits)	Standards and Certificate #
Symmetric encryption and decryption	AES operating in ECB, CBC, OFB, CFB-1, CFB-8, CFB-128, GCM	128, 192, 256	N/A	CAVP (cert #4133) FIPS PUB 197, "Advanced

				Encryption Standard (AES)" NIST SP800-38A
	AES operating in ECB, CBC, OFB, CFB8, CFB128, CTR, CCM, GCM, KW, KWP,	128, 192, 256	N/A	CAVP (cert #4153)
	AES operating in ECB, CBC, OFB, CFB 1, CFB 8, CFB 128, CTR, XTS; CCM; GCM	128, 192, 256	N/A	CAVP (cert #4137)
Cryptographic Signature Services	RSA PKCS #1 v1.5, PSS signature generation and signature verification	2048, 3072, 4096	N/A	SP 800-90A CAVP (cert #2261) FIPS PUB 186-2, "Digital Signature Standard" , FIPS PUB 186-4, "Digital Signature Standard"
	RSA PKCS #1 v1.5, PSS signature generation and signature verification	2048, 3072, 4096	N/A	SP 800-90A CAVP (cert #2251) FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard" , FIPS PUB 186-4, "Digital Signature Standard"
Asymmetric key generation	RSA (ANSI X9.31) key pair generation	2048, 3072, 4096	N/A	NIST 800-133, SP 800-131A, FIPS 186-4 CAVP (cert #2261) FIPS PUB 186-3, "Digital Signature Standard", FIPS

				PUB 186-2, “Digital Signature Standard”
	RSA (ANSI X9.31) key pair generation	2048, 3072, 4096	N/A	NIST 800-133, SP 800-131A, FIPS 186-4 CAVP (cert #2251) 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 #3402) FIPS Pub 180-3, “Secure Hash Standard.”
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #3418) FIPS Pub 180-3, “Secure Hash Standard.”
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	160, 224, 256, 384, 512	CAVP (cert #3407) 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 #2705) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, “Secure Hash Standard”
	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 #2788) FIPS Pub 198-1, "The Keyed-Hash Message

				Authentication Code, and FIPS Pub 180-3, “Secure Hash Standard”
	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 #2710) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, “Secure Hash Standard”
	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 #2721) FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, “Secure Hash Standard”
Random number generation	Hash DRBG, HMAC DRBG, CTR DRBG	256	256	SP800-90A R1 Hash CAVP (cert #1261)
	Hash DRBG, HMAC DRBG, no reseed CTR DRBG	256	256	SP800-90A R1 Hash CAVP (cert #1254)

5.4.3 Class FDP: User Data Protection

FDP_IFC.1 (1) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (1) The TSF shall enforce the [*Edge 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].*

FDP_IFC.1 (2) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (2) The TSF shall enforce the [*Edge Firewall 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].*

FDP_IFC.1 (3) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (3) The TSF shall enforce the [L2 *SSL VPN SFP*] on[

a) *subjects:*

- *a human user*
- *a virtual machine*
- *source subject: Web interface or network on which information is sent;*
- *destination subject: Servers and applications under the TOE scope of control;*

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

c) *operations:*

- *encrypt, decrypt, or*
- *pass or reject information].*

FDP_IFC.1 (4) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (4) The TSF shall enforce the [*DFW UNAUTHENTICATED SFP*] on[

a) subjects: : unauthenticated VMware vCenter objects 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].

FDP_IFC.1 (5) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (5) The TSF shall enforce the [*Edge SSL 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].*

FDP_IFF.1 Simple security attribute

Hierarchical to: No other components.

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

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;*
- *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*

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., RFC47). This shall be accomplished through a protocol filtering proxy for FTP traffic.]

FDP_IFF.1 (2) Simple security attribute

Hierarchical to: No other components.

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

FDP_IFF.1.1 (2) The TSF shall enforce the [*Edge Firewall 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) *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]

FDP_IFF.1 (3) Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1 (3) The TSF shall enforce the [*L2 SSL 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 rule set 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(4) 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 subject does not have a valid SSL certificate;*

FDP_IFF.1 (4) Simple security attribute

Hierarchical to: No other components.

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

FDP_IFF.1.1 (4) The TSF shall enforce the [*DFW 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;*
- *layer 2, 3 or 4 protocol;*
- *TOE interface on which traffic arrives and departs;*
- *service;*
- *information gleaned from prior packets; and*
- *none].*

FDP_IFF.1.2 (4) 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 MAC or 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 (4) The TSF shall enforce the [*none*].

FDP_IFF.1.4 (4) *The TSF shall* explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 (4) 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]

FDP_IFF.1 (5) Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1 (5) The TSF shall enforce the [*Edge SSL 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 (5) 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(5) is to be applied to that information flow*].

FDP_IFF.1.3 (5) The TSF shall enforce the [*none*]

FDP_IFF.1.4 (5) The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 (5) 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].

5.4.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: None

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].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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.

5.4.5 Class FMT: Security Management

FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 (1) The TSF shall restrict the ability to [disable, enable] the functions [firewall operation of the TOE].

FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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, NSX Administrator, System Administrator]

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control

FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*see information flow control SFP(s) as described in Table 11*] to restrict the ability to [*operations described in Table 11*] the security attributes [*see security attributes in Table 11*] to [*authorized identified roles in Table 11*].

Table 11: Security Attribute Management

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
Edge Firewall 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
L2 SSL 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
DFW UNAUTHENTICATED SFP	Delete attributes from a rule, modify attributes in a rule, add attributes to a rule	Listed in FDP_IFF1.1 (4)	Enterprise Administrator, Security Administrator
Edge SSL VPN SFP	Delete attributes from a rule, modify attributes in a rule, add attributes to a rule	Listed in FDP_IFF1.1 (5)	Enterprise Administrator, Security Administrator

FMT_MSA.3 (1) Static attribute initialization

Hierarchical to: No other components.

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

FMT_MSA.3.1 (1) The TSF shall enforce the [*Edge UNAUTHENTICATED SFP, L2 VPN SFP, and Edge SSL VPN SFP*] 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.

FMT_MSA.3 (2) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 (2)	The TSF shall enforce the [*Edge Firewall UNAUTHENTICATED SFP and DFW 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.

FMT_MTD.1 (1) Management of TSF Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
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, NSX Administrator, System Administrator*].

FMT_MTD.1 (2) Management of TSF Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
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, System Administrator, Security Administrator*].

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	None.

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, disable, determine and modify the behavior of the functionality to backup and restore TSF data, information flow rules, and audit trail data;*

c) *Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE;*

d) *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), (3), (4), and (5);*

e) *Delete and create attributes/ rules defined in FDP_IFF.1 (1), (2), (3), (4), and (5);*

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Enterprise Administrator, NSX Administrator, System Administrator, Security Administrator, and Auditor*]

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

5.4.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: None.

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

FPT_RPL.1 Replay Detection

Hierarchical to: No other components.

Dependencies: None.

FPT_RPL.1.1	The TSF shall detect replay for the following entities: [*network packets terminated at the SSL VPN network interface of the TOE*].
FPT_RPL.1.2	The TSF shall perform: [*reject the data*] when replay is detected.

FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	None.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps **for its own use**.

5.4.7 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	None.
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 [*SSL VPN sessions between Edge and external IT entities*].

FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
Dependencies:	None.
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*].

5.6 Assurance Requirements

28 The TOE security assurance requirements are summarized in Table 12, commensurate with EAL2+ (ALC_FLR.1).

Table 12: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.1	Basic Flaw Remediation
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Security Audit

29 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 NSX operation. They are recorded as audit records to detail various operational events of the TOE, such as a NSX Application reboot or a break in communication between a NSX Application and the NSX 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 NSX users.

30 NSX Edge, DFW, Guest Introspection, and NSX MANAGER 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 NSX Manager 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)

31 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.

32 NSX Manager audit logs and system events stored in the NSX Manager can be sorted into a small set of fields through the GUI. NSX Manager audit logs and system events can also be sorted based on the criteria as shown in Table 13 and Table 14 below respectively.

Table 13: Audit Log Filters

Option	Action
Module	Select the NSX 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 14: System Event Filters

Option	Action
Module	Select the NSX 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

33 As authorized administrators manage and configure the TOE, their actions are tracked and recorded as audit records. The resulting audit records can be examined to determine which security relevant actions took place and who (i.e., which user) is responsible for those actions. 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.

34 Logs stored in the NSX Manager are viewable by users with the following roles over the VSphere Web Client, NSX Appliance Manager GUI, and/or CLI: Enterprise Administrator, NSX Administrator, System Administrator, Security Administrator, and Auditor. Only authorized administrators with the appropriate role and permissions can review the audit logs.

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

Related SFRs:	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4

6.2 Cryptographic Support

36 The TOE implements four FIPS 140-2 cryptographic modules. These modules support SSH, TLS, HTTPS, encryption, decryption, key generation and key destruction and are provided by OpenSSL v1.0.2h FIPS Object Module v2.0.9, BouncyCastle FIPS 1.0, Linux Kernel Crypto Ubuntu v12.04, and NSS cryptographic module v3.23. All modules have CAVP of CMVP certificates. For a complete list of the cryptographic algorithms, modes, and key sizes, please see Table 10 above.

37 The TOE has five main components that utilize various instances of the crypto modules as indicated below:

- **NSX Manager:** OpenSSL, BouncyCastle
- **NSX Distributed Firewall:** OpenSSL, BouncyCastle
- **NSX Controller:** OpenSSL, BouncyCastle, Linux Kernel Crypto

- **NSX Edge:** OpenSSL, NSS
- **Guest Introspection:** OpenSSL

38 The TOE provides L2 (SSL) 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.

39 The TOE also provides HTTPS communications between NSX Manager and NSX Controller clusters, establishing SSL encrypted communications using certificates generated by NSX Manager.

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

41 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.

42 The L2 VPN connection is an SSL tunnel using OpenSSL with FIPS Object Module v2.0.10, connecting separate networks in each location. The connected networks offer connectivity to the same address space (e.g., IP subnet). This is the characteristic that makes this a L2 VPN service.

43 Similarly the SSL VPN is an SSL tunnel using OpenSSL with FIPS Object Module v2.0.10, allowing remote users to connect private networks behind a NSX Edge gateway to securely access servers and applications in private networks.

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

45 All cryptographic operations are performed by a FIPS 140-2 validated algorithms and/or cryptographic modules.

Related SFRs: FCS_CKM.1, FCS_CKM.4, FCS_COP.1

6.3 User Data Protection

46 For NSX, user data refers to network traffic traversing the Edge and NSX Distributed firewalls. NSX Edge protects access to user data in four ways: by restricting external access to TOE networks using its Layer 3 and 4 firewall functionality, by enabling secure access to user data by external entities through SSL VPN-Plus and L2 SSL VPN connections, and through NSX Distributed Firewall (DFW) operating at Layers 2-4.

47 **SSL VPN-Plus**. NSX Edge supports an SSL VPN termed SSL VPN-Plus that allows remote users to connect securely to private networks behind a NSX Edge gateway. This uses OpenSSL to create a tunnel between the remote user and the required network resources. The SSL VPN network access configuration requires users to install the SSL VPN-Plus client and that user being added to the local database before being granted access to SSL VPN services. The SSL VPN gateway requires

port 443 to be accessible from external networks and the SSL VPN client requires the NSX Edge gateway IP and port 443 to be reachable from client system.

48 **L2 VPN.** This uses OpenSSL to create a secure tunnel between network nodes. The local networks or connection points can be of any nature, such as VLAN or VXLAN, and need not be the same type at each side of the connection. The L2 VPN is a point-to-point service that can be established between two locations such that the NSX Edge deployed in one datacenter site takes the role of the L2 VPN server while the NSX Edge at the second site is the L2 VPN client initiating the connection to the server. Certificates are self-generated at each NSX Edge.

49 **NSX Edge Firewall.** This protects access to user data by functioning as an application-aware Layer 4 firewall capable of extremely granular access control. Edge Firewall enforces the Edge Firewall UNAUTHENTICATED SFP and operates at the vNIC48 level, capable of leveraging access control policy based on portgroups. Additionally, Edge Firewall 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 running any operating system across any type of hardware and storage supported by vSphere, and includes audit events.

50 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 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
- Port groups on which the connection request occurs
- composition of packets for FTP, Oracle TNS43, DCE44/RPC45, and ONC46 RPC

51 The Edge Firewall Component performs 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.

52 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.

53 **NSX Distributed Firewall (DFW)**. DFW works similarly to Edge Firewall, however operates at Layers 2-4 to offer stateful firewall functionality to all workloads of the NSX environment.

54 A DFW instance is created per VM vNIC and runs in the kernel space where it is activated as soon as the host preparation process is completed. If a VM does not require DFW service, it can be added in the exclusion list functionality. By default, NSX Manager, NSX Controllers, and Edge services gateways are automatically excluded from DFW function.

55 The DFW system architecture is based on 3 distinct entities, each with a clearly defined role:

- **vCenter Server:** vCenter Server is the management plane of the solution. DFW policy rules are created in the vSphere Web client. Any vCenter container can be used in the source/destination field of the policy rule.
- **NSX Manager:** NSX manager is the control plane of the solution. It receives rules from the vCenter Server and stores them in its central database. NSX manager then pushes DFW rules down to all ESXi hosts that have been prepared for enforcement over a RabbitMQ message broker. NSX EDGE manager can also receive DFW rules directly from REST API calls in deployments where a cloud management system is used.
- **ESXi Host:** ESXi host is the data plane of the solution. DFW rules are received from the NSX manager and translated into kernel space for real- time execution. VM network traffic is inspected and enforced per ESXi host.

56 The DFW instance on an ESXi host contains 2 separate tables. The rule table is used to store all policy rules, while the connection tracker table caches flow entries for rules with permit actions. A specific flow is identified by the 5-tuple information consisting source IP address, destination IP address, protocols, L4 source port, and L4 destination port fields. By default, DFW does not perform a lookup on L4 source port, but it can be configured to do so by defining a specific policy rule.

57 DFW rules are enforced as follows:

- Rules are processed in top-to-bottom ordering.
- Each packet is checked against the top rule in the rule table before moving down the subsequent rules in the table.
- The first rule in the table that matches the traffic parameters is enforced. No subsequent rules can be enforced as the search is then terminated for that packet.

Related SFRs:	FDP_IFC.1 (1), FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFC.1(4), FDP_IFF.1(1), FDP_IFF.1(2), FDP_IFF.1(3), FDP_IFF.1(4), FDP_IFC.1(5), FDP_IFF.1(5)

58 Edge facilitates SSL VPN communication with SSL VPN-Plus client installations. The TOE compares plaintext traffic received from the VPN or destined to the 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.

59 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

60 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 NSX Manager.

61 The TOE will take the following actions based on the SSL VPN policy:

- Verify remote user credentials at Edge database at SSL VPN connection request
- Permit OpenSSL VPN tunnel establishment upon credential verification
- Pass packets without modification

Related SFRs: FDP_IFC.1 (3), FDP_IFF.1 (3). FDP_IFC.1(6), FDP.1 (6)

6.4 Identification and Authentication

62 NSX maintains security attributes that are used in the operation of the TOE. NSX maintains the following user security attributes: user identity, association of a human user with the authorized administrator role, and password or other authentication credential. NSX 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 NSX Manager, a user's 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 uses to authenticate to the TOE is securely maintained by vCenter.

Related SFRs: FIA_ATD.1

63 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.

64 Administrators accessing the NSX vSphere Web Client or NSX Manager Appliance GUI must authenticate to the NSX Manager VM. No management functionality is available to administrators prior to identifying to and authenticating with the vSphere Web Client or NSX Manager Appliance GUI. Administrators accessing NSX management functionality via the NSX Manager Appliance GUI authenticate with vCenter against an external authentication server, normally an Active Directory domain controller, which resides outside of the TOE. 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. NSX Edge provides password based identification and

authentication mechanisms for SSL VPN-Plus session establishment. The TOE stores administrator passwords that are encrypted with AES256 and are kept in the PostgreSQL database, in order to request vCenter services.

Related SFRs:	FIA_UAU.2, FIA_UID.2

65 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.

Related SFRs:	FIA_UAU.7

6.5 Security Management

66 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 15.

Table 15: Authorized Administrator Roles

Option	Action
Enterprise Administrator	NSX operations and security.
NSX Administrator	NSX operations only: for example, install virtual appliances, configure port groups.
System Administrator	Created at installation, available only at the NSX Manager Appliance GUI, used for installation procedures.
Security Administrator	NSX security only: for example, create port groups, create reports for NSX modules.
Auditor	Read only.

67 The TOE provides authorized administrators with two GUIs to the NSX Manager to manage the security functions and TSF data of the TOE. Within the NSX 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.

Related SFRs:	FMT_MOF.1 (1), FMT_MOF.1(2), FMT_MSA.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_SMF.1, FMT_SMR.1

68 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, Edge Firewall 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).

Related SFRs:	FMT_MSA.3 (1), FMT_MSA.3(2)

6.6 Protection of the TSF

69 The TOE provides protection mechanisms for its security functions. The Protection of the TSF function ensures the TSF data transmitted between various TOE components NSX Manager, NSX Edge, NSX DFW, Guest Introspection, and vSphere Web Client and NSX Manager Appliance GUI is secured. TSF data transmitted between vSphere Web Client or NSX Manager Appliance GUI and NSX Manager is secured via TLS. TSF data transmitted between NSX Manager and NSX Edge is secured via TLS. TSF data transmitted between NSX Manager and Edge Firewall is secured via SSH. TSF data transmitted between NSX Manager and Guest Introspection 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.

Related SFRs:	FPT_ITT.1, FPT_RPL.1

70 NSX provides a source of date and time information for the NSX components that is used in audit timestamps. This centralised source of time ensures that the TOE provides a reliable timestamp for all auditing. In addition, NSX can connect to a Network Time Protocol (NTP) Server that will provide time updates. NSX 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 NSX Manager by an authorized administrator that has successfully been identified and authenticated to the TOE.

Related SFRs:	FPT_STM.1

6.7 Trusted Path/Channels

71 NSX 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 NSX 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, NSX Edge is able to secure the session between Edge and an external IT entity with a SSL VPN. The TOE implements TLS for protection of remote web access to the management of the TOE via the NSX Manager. The TOE generates its own certificate, which is then shared among the distributed components.

72 The TOE uses FIPS validated cryptographic algorithms to implement the above cryptographic functions.

Related SFRs: FTP_ITC.1, FTP_TRP.1

7 Rationale

7.1 Security Objectives Rationale

73 This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target, providing a mapping between the threats, policies, and assumptions to the security objectives.

74 Table 16 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 16: Security Objectives Coverage

	T.ADMIN_ERROR	T.MEDIAT	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	T.UNTRUSTPATH	A.NOEVIL	A.PHYSICAL	A.REMACC	A.SINGEN
O.TOE_ADMINISTRATION	X		X						
O.MEDIAT		X							
O.PROTECTED_COMMUNICATIONS			X						
O.SYSTEM_MONITORING				X					
O.TRUSTEDPATH					X				
OE.GUIDAN						X			
OE.REMACC								X	
OE.SINGEN									X
OE.NOEVIL						X			
OE.PHYSICAL							X		

75 The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

Table 17: Security Objectives Rationale

Element	Justification
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** 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** 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.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** counters this threat by providing protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
	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** 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** 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.
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	**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.

Element	Justification
	OE.NOEVIL satisfies the assumption that 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.	**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** 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** Satisfies the assumption that information cannot flow among the internal and external networks unless it passes through the TOE.

7.3 Security Requirements Rationale

7.3.1 SAR Rationale

76 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.1 to provide assurance that any identified security flaws will be addressed.

7.3.2 SFR Rationale

Table 18: Security Requirements Mapping

	O.MEDIAT	O.PROTECTED_COMMUNICATIONS	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TRUSTEDPATH
FAU_GEN.1			X		
FAU_GEN.2			X		
FAU_SAR.1			X		
FAU_SAR.2			X		
FAU_SAR.3			X		
FAU_STG.1			X		
FAU_STG.4			X		
FCS_CKM.1		X		X	
FCS_CKM.4		X			
FCS_COP.1		X		X	
FDP_IFC.1(1)	X				
FDP_IFC.1(2)	X				
FDP_IFC.1(3)					X

	O.MEDIAT	O.PROTECTED_COMMUNICATIONS	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TRUSTEDPATH
FDP_IFC.1(4)	X				
FDP_IFC.1(5)	X				
FDP_IFF.1(1)	X				
FDP_IFF.1(2)	X				
FDP_IFF.1(3)	X				
FDP_IFF.1(4)	X				
FDP_IFF.1(5)	X				
FIA_ATD.1				X	
FIA_UAU.2				X	
FIA_UAU.7				X	
FIA_UID.2				X	
FMT_MOF.1(1)				X	
FMT_MOF.1(2)				X	
FMT_MSA.1				X	
FMT_MSA.3(1)				X	
FMT_MSA.3(2)				X	
FMT_MTD.1(2)				X	

	O.MEDIAT	O.PROTECTED_COMMUNICATIONS	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TRUSTEDPATH
FMT_MTD.1(1)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FTP_ITC.1		X		X	
FPT_ITT.1		X			
FPT_RPL.1		X			
FPT_STM.1			X		
FTP_TRP.1		X			

Table 19: Suitability of SFRs

Objectives	SFRs
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.	**FDP_IFC.1(1)** This requirement meets the objective by ensuring that the TOE identifies the entities involved in the Edge UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). **FDP_IFC.1(2)**This requirement meets the objective by ensuring that the TOE identifies the entities involved in the Edge Firewall UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). **FDP_IFC.1(4)**This requirement meets the objective by ensuring that the TOE identifies the entities involved in the DFW UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice

Objectives	SFRs
	versa). **FDP_IFF.1(1)**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)** This requirement meets the objective by ensuring that the TOE identifies the attributes of the users sending and receiving the information in the Edge Firewall 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)** This requirement meets the objective by ensuring that the TOE ensures that all L2 VPN encrypted data received from a peer TOE or trusted external IT entity is properly decrypted and authentication verified. **FDP_IFF.1(4)** This requirement meets the objective by ensuring that the TOE identifies the attributes of the users sending and receiving the information in the DFW 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(5)** This requirement meets the objective by ensuring that the TOE ensures that all SSL encrypted data transmitted between a TOE user and the TSF is properly decrypted and authentication verified.
O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_CKM.1** The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations. **FCS_CKM.4** The requirement meets the objective by ensuring that the TOE can zeroize cryptographic keys. **FCS_COP.1** The requirement meets the objective by ensuring that the TOE can perform encryption and decryption in accordance with the defined algorithms and key sizes. **FPT_ITT.1** 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** The requirement meets the objective by ensuring that the TOE detects replay of network packets. **FTP_ITC.1** The requirement meets the objective by ensuring that the TOE provides a trusted path between itself and authorized IT entities from modification or disclosure.

Objectives	SFRs
	FTP_TRP.1 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** The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event. **FAU_GEN.2** 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** The requirement meets the objective by ensuring that the TOE provides the ability to review logs. **FAU_ SAR.2** 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.3** This requirement meets this objective by providing searches and sorting of the audit data. **FAU_ STG.1** 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** 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** The requirement meets the objective by ensuring that the TOE provides reliable timestamps.
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 or SSH	**FCS_CKM.1** This requirement meets the objective by providing protections for logged-in administrators via TLS or SSH sessions. **FCS_COP.1** This requirement meets the objective by providing protections for logged-in administrators via TLS or SSH sessions. **FIA_ATD.1** The requirement meets the objective by ensuring that the TOE maintains the user's security attributes. **FIA_UAU.2** 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.7** The requirement meets the objective by ensuring that the TOE provides obscured feedback while the user is authenticating.

Objectives	SFRs
	FIA_UID.2 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)** The requirement meets the objective by ensuring that the TSF restricts the ability of the TOE to start up and shut down operation to an authorized administrator. **FMT_MOF.1(2)** 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** 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)** 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)** 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)** 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)** 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** The requirement meets the objective by ensuring that the TSF restrict the set of management functions to the authorized administrator. **FMT_SMR.1** The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
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(5)** This requirement meets the objective by ensuring that all SSL VPN encrypted data received from a peer TOE or trusted external IT entity are properly decrypted and authentication verified.

7.4 TOE Summary Specification Rationale

77 Table 20 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 20: Map of SFRs to TSS Security Functions

SFR	Security Audit	Cryptographic Support	User Data Protection	Identification & Authentication	Security Management	Protection of the TSF	Trusted Path/Channels
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_STG.1	X						
FAU_STG.4	X						
FCS_CKM.1		X					
FCS_CKM.4		X					
FCS_COP.1		X					
FDP_IFC.1(1)			X				
FDP_IFC.1(2)			X				
FDP_IFC.1(3)			X				
FDP_IFC.1(4)			X				
FDP_IFC.1(5)			X				
FDP_IFF.1(1)			X				
FDP_IFF.1(2)			X				
FDP_IFF.1(3)			X				
FDP_IFF.1(4)			X				

SFR	Security Audit	Cryptographic Support	User Data Protection	Identification & Authentication	Security Management	Protection of the TSF	Trusted Path/Channels
FDP_IFF.1(5)			X				
FIA_ATD.1				X			
FIA_UAU.2				X			
FIA_UAU.7				X			
FIA_UID.2				X			
FMT_MOF.1(1)					X		
FMT_MOF.1(2)					X		
FMT_MSA.1					X		
FMT_MSA.3(1)					X		
FMT_MSA.3(2)					X		
FMT_MTD.1(1)					X		
FMT_MTD.1(2)					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_ITT.1						X	
FPT_RPL.1						X	
FPT_STM.1						X	
FTP_ITC.1							X
FTP_TRP.1							X

7.5 Extended Security Functional Requirements Rationale

78 There are no extended Security Functional Requirements.

7.6 Security Functional Requirements Dependencies Rationale

79 All the requirement dependencies of the Common Criteria are satisfied and Table 21 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 21: Functional Requirements Dependencies

Requirement	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FIA_UID.1 FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4 FCS_CKM.1	✓	
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_IFC.1(4)	FDP_IFF.1(4)	✓	

FDP_IFC.1(5)	FDP_IFF.1(5)	✓	
FDP_IFF.1(1)	FMT_MSA.3 FDP_IFC.1(1)	✓	
FDP_IFF.1(2)	FMT_MSA.3 FDP_IFC.1(2)	✓	
FDP_IFF.1(3)	FMT_MSA.3 FDP_IFC.1(3)	✓	
FDP_IFF.1(4)	FMT_MSA.3 FDP_IFC.1(4)	✓	
FDP_IFF.1(5)	FMT_MSA.3 FDP_IFC.1(5)	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.2	No dependencies	✓	
FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	✓	
FMT_MOF.1(2)	FMT_SMF.1 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(1)	FMT_SMF.1 FMT_SMR.1	✓	
FMT_MTD.1(2)	FMT_SMF.1	✓	

	FMT_SMR.1		
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	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	✓	