Skybox Security
Skybox Security Suite
Security Target

Version 1.0
20 August 2018

Prepared for:

Corporate Headquarters:
2077 Gateway Place, Suite 200
San Jose, CA 95110

Prepared By:

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

The TOE is Skybox Security Suite 9.0.201, a Security Operations, Analytics and Reporting (SOAR) solution providing attack surface visualization and a suite of security analytics solutions for vulnerability, threat and security policy management. The Skybox Security Suite provides capabilities for monitoring firewall/device policy compliance, optimizing firewall rules, and managing modifications to firewall rule sets. Analysis capabilities include threat and vulnerability analysis, access path analysis, and firewall rules/configuration checks.

The ST contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Skybox Security Skybox Security Suite Security Target

ST Version – Version 1.0

ST Date – 20 August 2018

TOE Identification – Skybox Security Suite 9.0.201

TOE Developer – Skybox Security

Evaluation Sponsor – Skybox Security

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017.
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_FLR.1).

1.3 Conventions

The following conventions are used in this document:

- Security Functional Requirements—Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration; assignment; selection; and refinement.
    - Iteration—allows a component to be used more than once with varying operations. In this ST, iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
    - Assignment—allows the specification of an identified parameter. Assignments are indicated using bold text and are enclosed by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection—allows the specification of one or more elements from a list. Selections are indicated using bold italics and are enclosed by brackets (e.g., [***selection***]).
    - Refinement—allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
    - Extended Requirements are allowed to create requirements should the Common Criteria not offer suitable requirements to meet the ST needs. To ensure these requirements are explicitly identified, the ending "_EXT" is appended to the newly created short name and the component.
- Other sections of the ST—other sections of the ST use bolding and/or different fonts (such as `Courier`) to highlight text of special interest, such as captions, commands, or filenames specific to the TOE.
- The requirements are copied verbatim, except for some changes to required identifiers to match the iteration convention of this document, from CC Part 2 and only operations performed in this security target are identified.

1.4 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this ST:

CC	Common Criteria
CMOS	Complementary Metal-Oxide Semiconductor
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IOE	Indicators of Exposure
IPS	Intrusion Prevention System
IT	Information Technology
J2EE	Java 2 Platform Enterprise Edition
LDAP	Lightweight Directory Access Protocol
MySQL	My Structured Query Language
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Operations, Analytics and Reporting
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network
XML	eXtensible Markup Language

2. TOE Description

2.1 Overview

The TOE is Skybox™ Security Suite 9.0.201, a Security Operations, Analytics and Reporting Solution providing attack surface visualization and a suite of security analytics solutions for vulnerability, threat and security policy management.

Skybox™ Security provides security professionals with a suite of solutions for security operations, analytics and reporting. Skybox integrates over a hundred networking and security technology organizations, and merges the data into a dynamic network model of an organization's attack surface, giving comprehensive visibility of public, private and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in the environment and correlate them with exploits in the wild. This makes the accurate prioritization and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put an organization at risk. Skybox supports both FIPS and non-FIPS modes, and either is allowed in the evaluated configuration.

2.2 Architecture

The Skybox Security Suite comprises three main components:

- Skybox Server—the core component of the product, providing most of the functionality to support network data collection, modelling, analysis and compliance monitoring. It is built on J2EE and incorporates a MySQL database and InetSoft reporting engine. InetSoft's software is based on open standards technology that incorporates XML, SOAP, Java language, and JavaScript.
- Skybox Manager—the client component of Skybox, which provides a graphical user interface (GUI) to manage and use the capabilities of the Skybox Security Suite. Each of the Skybox components has its own client. Four components (Firewall Assurance, Network Assurance, Vulnerability Control, and Threat Manager) use a thick client implemented in Java Swing, while Change Manager and Horizon use a browser-based web client.
- Skybox Collector—the Collector is similar to the Server component, without the MySQL database. Multiple Collectors can be installed throughout the network to support network data collection and discovery.

The following figure shows an example deployment of the TOE in its operational environment. A Skybox configuration can consist solely of the three components co-located on a single platform, or can contain any number of additional Skybox Servers, Skybox Collectors and Skybox Managers. Communications between distributed TOE components are protected using TLS.

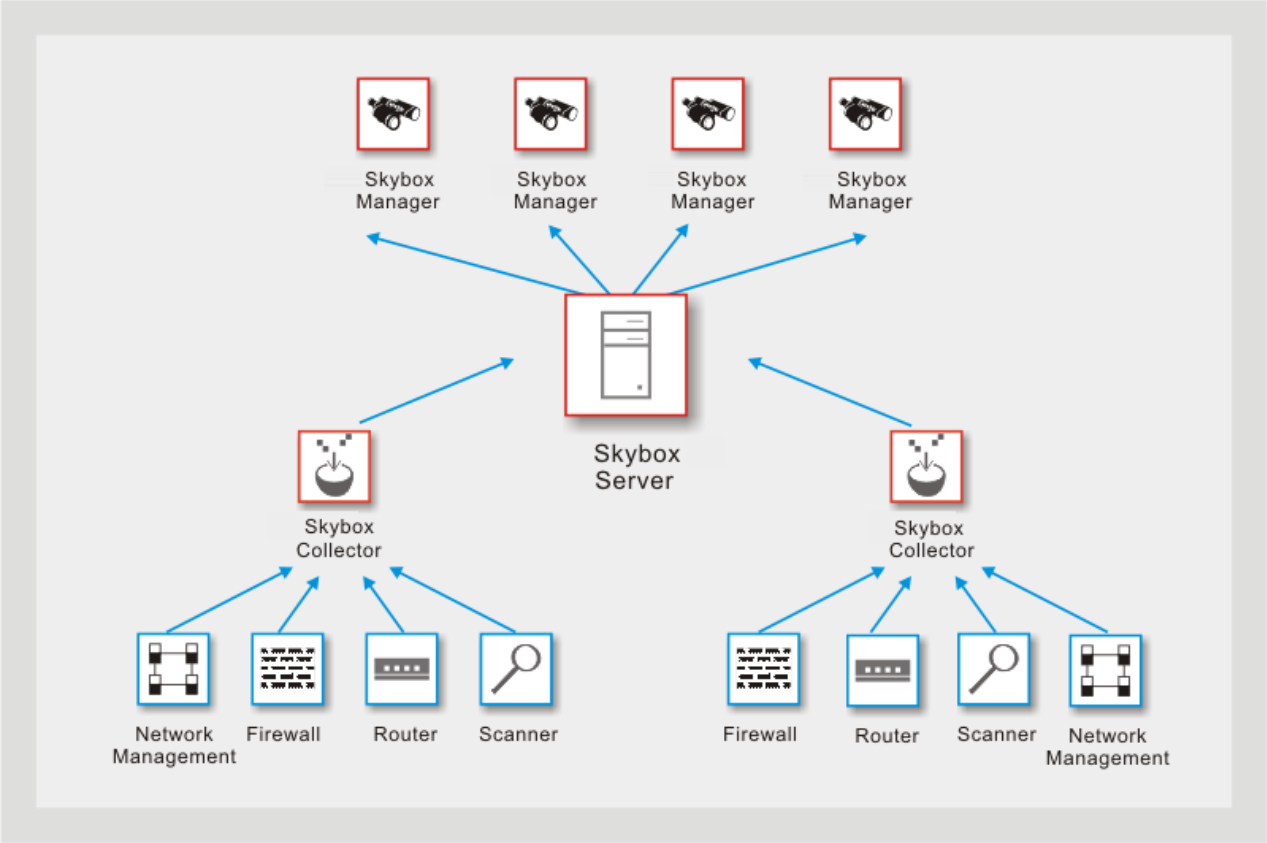

Figure 1: Example TOE Deployment

The Skybox Security Suite provides the following functionality:

- Network data collection and discovery—Skybox Security Suite collects information about all the elements comprising the network: security control devices such as firewalls, IPS, and VPNs; network infrastructure devices such as routers, switches and load balancers; and network assets such as servers and workstations.
- Modelling—Skybox Security Suite uses the information gathered through the data collection and discovery process to create a normalized model of the network that supports attack surface visualization.
- Analysis—Skybox Security Suite uses the network model to perform and support a range of analyses, including: firewall rule and configuration checks; access path analysis; and firewall rule optimization.
- Compliance monitoring—Skybox Security Suite is able to perform audits of the network and monitor the compliance of the network and its elements to various published standards, including: PCI; FISMA; and NIST.

This functionality is provided by the following components that together comprise the Skybox Security Suite:

- Skybox Horizon
- Skybox Vulnerability Control
- Skybox Threat Manager
- Skybox Firewall Assurance
- Skybox Network Assurance
- Skybox Change Manager.

2.2.1 Skybox Horizon

Skybox Horizon combines security analytics with data integration and visualization technologies to provide visibility of the network attack surface.

Information is collected about all the elements comprising the network: security control devices such as firewalls, IPS, and VPNs; network infrastructure devices such as routers, switches and load balancers; and network assets such as servers and workstations. Skybox Horizon correlates all of this information into model mappings that show exposed vulnerabilities and their exploit status based on real–time threat intelligence provided by Skybox™ Research Lab and other vendors.

Skybox Horizon maps show geographical sites and assets within an attack surface, and the paths between them. The map provides a view of Indicators of exposure (IOEs) severity at each site. IOEs describe security weaknesses specific to an organization's network that could be exploited by an attacker. IOEs are determined by analyzing multiple factors or events as opposed to observing one in isolation. For example, an unexpected firewall rule change is an event, but an unexpected firewall rule change that opens a network path to a critical asset is an IOE. Attack risks tend to cluster around common exposure factors, which can be grouped into five of the most prevalent IOEs.

The geographical map display options include views of specific sites or panoramic attack surface visibility. A Panoramic view displays a map of servers, endpoints, hybrid networks and security and networking devices, as well as the routing between them.

Skybox™ Horizon identifies and categorizes vulnerabilities and threats. The solution tracks progress toward security goals; compares past and current risk levels; and provides management capabilities for ongoing gradual risk reduction of potential threats.

2.2.2 Skybox Vulnerability Control

Skybox™ Vulnerability Control supports vulnerability management by providing visibility of the network attack surface, network topology, security controls, and asset information. Skybox categorizes vulnerabilities' severity, further prioritizing them with the addition of threat and vulnerability intelligence and correlating data such as CVSS scores, availability of an exploit and active campaigns in the wild.

Vulnerability Control provides tools for Skybox users to:

- Find vulnerability exposures and exploitable attack vectors in their attack surface
- Prioritize vulnerabilities based on threats and the risk they pose to their network
- Find vulnerabilities on network devices and "un-scannable" systems without waiting for a scan
- Target imminent threats for immediate response and systematically reduce potential threats with context-aware remediation options.

The Skybox Vulnerability Dictionary provided by Skybox™ Research Lab is used in conjunction with analysis functions to determine vulnerabilities and threats to a network. The Skybox Vulnerability Dictionary contains consolidated information about Vulnerability Definitions for more than 1000 products that are used in enterprise network environments including servers and desktop operating systems, business and desktop applications, databases, runtime frameworks, networking hardware and software, and security software.

2.2.3 Skybox Threat Manager

Skybox™ Threat Manager consolidates threat intelligence sources and analyzes and prioritizes advisories in the context of the users attack surface. This component collects and normalizes real–time threat intelligence — from both security data sources and from website sources. Threat Manager receives analyst-validated threat intelligence from the Skybox™ Research Lab.

Threat Manager automatically analyzes the potential impact of a threat and provides remediation guidance. Threat Manager provides Skybox users with the tools to:

- make on–demand impact assessments
- Prioritize threats and remediation by combining intelligence of their attack surface and exploits in the wild
- Consolidate threat intelligence into one common view

• Optimize threat remediation tasks with built–in workflows and automated status tracking

2.2.4 Skybox Firewall Assurance

Skybox™ Firewall Assurance provides automation of firewall management tasks across different firewall vendors and complex rulesets. Firewall Assurance verifies that firewalls are clean, optimized, effective, and monitors policy compliance. Firewall Assurance analytics extend beyond firewall rule checks to find hidden risk factors by analyzing possible traffic between network zones, flagging unauthorized changes and finding vulnerabilities on firewalls.

Firewall Assurance provides Skybox users with the tools to:

- Analyze virtual and cloud-based firewalls to better control east-west or north-south traffic
- Detect security and compliance problems using out–of–the–box or customized policies
- Track changes for continuous firewall monitoring
- Clean up, optimize and recertify firewall rules
- Normalize firewall rule sets for a consistent view across multiple vendors

2.2.5 Skybox Network Assurance

Skybox™ Network Assurance provides visibility across physical, virtual and cloud networks. This component uncovers potential attack vectors, provides troubleshooting for root causes of network outages and allows a user to check the correct implementation of security zone policies and security tags.

Network Assurance provides tools for Skybox users to:

- Visualize and interact with a model of their hybrid network and security controls
- Keep security zones and device configurations in continuous compliance
- Troubleshoot network connectivity to ensure business continuity
- Plan network changes and check for security risks with “what-if” analysis.

2.2.6 Skybox Change Manager

Skybox™ Change Manager automates change management workflows. The solution provides modeling capabilities to assess change impact prior to implementation to avoid introducing new risks.

Change Manager provides tools for Skybox users to:

- Automate firewall change management workflows
- Validate proposed firewall changes by checking for policy violations, security gaps and new vulnerabilities
- Ensure changes are made as intended and don’t introduce new risk
- Customize and simplify workflows to reduce change management time
- Establish end-to-end rule life cycle management for secure infrastructure and optimized firewalls.

2.3 Physical Boundaries

2.3.1 Physical TOE Components

The Skybox platform includes all Skybox products, so there is a single installer for all of them. Licenses determine which products are available.

The platform uses a 3-tiered architecture with data collectors, a centralized server, and a user interface (the Manager). The solution also offers an API for developers to integrate Skybox data into other applications. The API is not included in the evaluation. Skybox can be easily scaled to suit the complexity and the size of any infrastructure. The Collector and Manager can be installed together with the Server and on the same platform; or on separate platforms.

Multiple Collectors and Managers can be installed across the network as needed. The Server and Collector components must run on a 64-bit operating system. Each TOE hardware appliance instance is a hardened CentOS system running Skybox Security Suite 9.0.201.

The Skybox Manager is a java client software component provided in the following form:

- `SkyboxManager-<version#>-<build#>.exe` file, the installer file for Manager.

The Skybox Collector is provided in the following form factors:

- `SkyboxInstaller-<version#>-<build#>.exe` file, the installer file for Windows containing Collector software
- Skybox 7000 or 8000 appliance with Skybox Collector 9.0.201 installed
- Skybox Virtual Appliance (ISO installed in a VMWare environment).

The Server component is provisioned in the following form factors:

- `SkyboxInstaller-<version#>-<build#>.exe (installer file for Windows)`
- `SkyboxInstaller-<version#>-<build#>.bin (installer file for Linux)`
- Skybox 7000 or 8000 appliance with Skybox Security Suite 9.0.201 installed
- Skybox Virtual Appliance (ISO installed in a VMWare environment). The software version is Skybox Security Suite 9.0.201.

2.3.2 Operational Environment Components

Skybox Server can be installed on a server-class machine. The size and complexity of the network might require a powerful server with a multiprocessor and a large amount of memory. For very large deployments, more than one Skybox Server may be necessary (each running on a separate server). The Collector may be installed with the Server on the same platform, or on a separate platform and additional Collectors may be required in the network. The Skybox Manager is a Java client application installed on a Windows machine and that connects to the Skybox Server. In a software installation, the Manager may be installed with Server or on a separate machine. Multiple Managers can be installed on a single computer; this is useful when connecting to Servers of different versions. The Server must run on a 64-bit operating system.

The Skybox Server and the Skybox Collectors can also be installed as Skybox Virtual Appliances (ISO installed in a VMWare environment). The TOE supports ESX 5.5.x and ESX 6.0.x. The minimal requirements necessary for creating a Skybox Virtual Appliance on VMware are the same as the Server hardware requirements listed below. The recommended requirements in the table apply to large deployments of more than 250 firewalls.

The operating systems supported for the Skybox Server and the Skybox Collectors software installations are:

- Windows 7
- Windows 10
- Windows Server 2012
- Red Hat Enterprise Linux 7
- CentOS 7

Server hardware requirements are listed in the following table.

Hardware	Minimum Requirement	Recommended Requirement
CPU	8 cores	16 cores
RAM	32 GB	128 GB
Available Disk Space	500 GB	1 TB

The hardware requirements for standalone Collectors are listed in the following table.

Hardware	Minimum Requirement	Recommended Requirement
CPU	4 cores	8 cores
RAM	16 GB	32 GB
Available Disk Space	100 GB	500 GB

When installing Skybox Server on Linux or Skybox Collector on Linux, the following additional software packages are required:

- glibc 64bit (for Skybox Appliance)
- pam.i686 (for Skybox Appliance)
- numa (for MYSQL)
- wget (for HTTP file retrieval).

Standalone installations of Skybox Manager are supported on the following operating systems:

- Windows 7
- Windows 10 (64bit only)
- Windows Server 2012.

The following browsers are supported for the Manager and for connecting to the Skybox Horizon or Skybox Change Manager. If no version is specified, no specific version is required:

- Microsoft Internet Explorer 9 or higher

  Note: Microsoft Edge is not supported
- Google Chrome
- Mozilla Firefox
- Safari (for Skybox Horizon only).

The hardware requirements for the Manager are listed in the following table.

Hardware	Minimum Requirement	Recommended Requirement
CPU	Intel i3 or equivalent	Intel i5 or equivalent
RAM	2 GB	4 GB
Available Disk Space	1 GB	2 GB

The following components are also supported in the operational environment of the TOE, but are not required for the evaluated configuration:

- LDAP and RADIUS servers to support user authentication
- External syslog server for the TOE to send audit logs to
- SMTP Server to support e-mail notifications.

2.4 Logical Boundaries

This section summarizes the security functions provided by the TOE.

2.4.1 Audit

The TOE generates and stores audit records of user management and operational events, including: login; logout; server up/down; password changes; and all user-management operations. Each audit log includes the following information: date and time of the event; type of event; subject identity; and the outcome of the event.

The TOE stores generated audit records locally on the Skybox Server and can be configured to export logs to an external syslog server. The TOE provides read-only access to the audit files for administrative users. The TOE will overwrite the local audit data starting with the oldest data when the log rotation limit is reached.

2.4.2 Identification & Authentication

The TOE requires all users to be successfully identified and authenticated before allowing them to perform any other activities. The TOE can authenticate users directly, based on user password, and can be configured to use an external LDAP or RADIUS authentication server. Passwords managed by the TOE must meet the requirements of the TOE password policy, as follows:

- Passwords must have a minimum length of 8 characters
- Passwords must contain at least 1 upper case letter
- Passwords must contain at least 1 lower case letter
- Passwords must contain at least 1 digit
- Passwords must contain at least 1 non-alphanumeric symbol
- Passwords cannot contain username
- Passwords may not contain 5 or more characters from the previous password if they are in the same positions as they were in the previous password.

The TOE uses roles associated with individual users to give users permission to perform specific actions within the system.

The TOE will lock a user out of their account for a period of 30 seconds following three consecutive failed authentication attempts.

2.4.3 Security Management

The TOE provides several user roles that grant permissions to perform actions in specific parts of the product, as follows:

- Admin—can manage all aspects of the system. There are additional admin roles, which have management permission for a limited part of the system: Admin – Users; Admin – Operational; Admin – Vulnerability Control; and Admin – Assurance.
- User—can run various security analyses. There are also more limited User sub-roles, as follows:
    - User – Vulnerability Control—User role that is limited to the Skybox Vulnerability Control and Threat Manager modules.
    - User – Assurance—User role that is limited to the Skybox Firewall Assurance and Skybox Network Assurance modules
- Read-only User—can view the data and edit tickets that are assigned to their user or group. There are also more limited Read-only User sub-roles, as follows:
    - Read-only User – Vulnerability Control—Read-only User role that is limited to the Skybox Vulnerability Control and Threat Manager modules
    - Read-only User – Assurance—Read-only User role that is limited to the Skybox Firewall Assurance and Skybox Network Assurance modules
- Ticket User—can manage tickets and view (but not generate) reports. This role is for Skybox Vulnerability Control and Skybox Threat Manager. It cannot be used for Skybox Change Manager.
- Web Ticket User—can log in to Change Manager, where they can manage tickets. They cannot log in to the Manager GUI. This role is for Change Manager.

- Web Ticket Requestor—can open tickets (that is, submit change requests) in Change Manager and close tickets that they created. This role is for Change Manager.

The TOE provides capabilities for administrators and users to manage the security functions of the Skybox Security Suite.

2.4.4 Protection of the TSF

Communications between distributed components of the TOE (i.e., between Skybox Managers and the Skybox Server, and between the Server and Skybox Collectors) occur over HTTPS, which provides confidentiality and integrity of transmitted data.

Hardware appliance-based Skybox components maintain time internally and use this internal time as the source for reliable timestamps. Software-based TOE components use the system clock maintained by the underlying operating system as the source for date and time information.

2.4.5 TOE Access

The TOE terminates inactive user sessions after a time period of user inactivity; the default value is 30 minutes. TOE users are also able to initiate termination of their own interactive sessions by logging off.

The TOE displays an advisory warning message regarding unauthorized use before establishing a user session.

2.4.6 Trusted Path/Channels

The TOE provides a trusted channel to communicate securely with LDAP external authentication. The trusted channel is implemented using TLS.

The TOE provides a trusted path for TOE users to communicate with the TOE. The trusted path is implemented using HTTPS for access from the remote users Change Manager and Horizon web UIs to the Skybox Server. Users initiate the trusted path by establishing an HTTPS connection (using a supported web browser). The trusted path is used for initial authentication and all subsequent user interactions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

2.4.7 Network Monitoring

The TOE collects information about all the elements comprising the network. The Collector component receives the data and forwards it to the Server where it is stored, normalized and analyzed. The Server uses the information gathered through the data collection and retrieval process to create a normalized model of the network and perform a range of analyses. The Server also performs audits of the network and monitors the compliance of the network and its elements to various published standards, including: PCI; FISMA; and NIST. The Manager component provides a graphical user interface (GUI) via the Manager's console to manage and use the capabilities of the TOE. The TOE also provides a Web UI accessible through a compatible browser that provides limited access to the TOE.

2.5 Capabilities Provided by the Operational Environment

The TOE relies on the operational environment for the following components and capabilities:

- The underlying operating system of each TOE software component is relied on to protect the component and its configuration from unauthorized access.
- The underlying operating system of each TOE software component is relied on to provide a reliable date and time stamp for use by the TOE.

2.6 TOE Documentation

This section identifies the guidance documentation included in the TOE. A minor non-security relevant change was made to 9.0.200 changing the version to 9.0.201. However the 9.0.200 guidance documents remain valid for the 9.0.201 TOE version. The documentation comprises:

- Skybox Installation and Administration Guide 9.0.200 Revision: 11, 2018

- Skybox Reference Guide 9.0.200 Revision: 11, 2018
- Skybox Virtual Appliance VMware Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Appliance 7000 Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Appliance 8000 Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Change Manager User's Guide 9.0.200 Revision: 11, 2018
- Skybox Horizon User's Guide 9.0.200 Revision: 11, 2018
- Skybox Change Manager Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Change Manager Help 9.0.200 Revision: 11, 2018
- Skybox Threat Manager Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Threat Manager User's Guide 9.0.200 Revision: 11, 2018
- Skybox Firewall Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Firewall Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control Getting Started Guide 9.0.200 Revision: 11, 2018.

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, and assumptions about the intended operational environment of the TOE.

3.1 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE.

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PLATFORM	The underlying operating system of each TOE software component will protect the component and its configuration from unauthorized access.
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment.

T.BRUTE_FORCE	An unauthorized user may gain access to the TOE through repeated password-guessing attempts.
T.INAPPROPRIATE_USE	Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.
T.INTEGRITY_COMPROMISE	An unauthorized user may attempt to modify or destroy audit data, thus removing evidence of unauthorized or malicious activity.
T.NETWORK_COMPROMISE	An unauthorized user may monitor the enterprise network in an attempt to obtain sensitive data, such as passwords, or to modify transmitted data.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNATTENDED_SESSION	An unauthorized user gains access to the TOE via an unattended authorized user session.
T.UNAUTHORIZED_ACCESS	An unauthorized user may gain access to the TOE security functions and data.
T.UNAUTHORIZED_ACTIVITY	Authorized users perform unauthorized actions on the TOE.
T.UNDETECTED_THREATS	Vulnerabilities, threats, and non-compliance rules generated by or existing in devices in the network system indicative of misuse or unauthorized or malicious user activity go undetected.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.AUDIT	The TOE shall be able to generate audit records of security-relevant events.
O.I_AND_A	The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.
O.FNM_COLLECT	The TOE shall provide capabilities to collect network device data from the network.
O.FNM_ANALYSIS	The TOE shall provide analysis functions necessary to detect vulnerabilities, threats, and non-compliance in the network or on the network devices.
O.LOGON_BANNER	The TOE shall be able to display an advisory warning message to potential users pertaining to appropriate use of the TOE.
O.PASSWORD_CONTROLS	The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.
O.PROTECTED_COMMS	The TOE shall protect communications between its distributed components and between itself and external entities.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized users having appropriate roles.
O.SESSION_TERMINATION	The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.
O.STORAGE	The TOE shall protect stored audit records from unauthorized modification or deletion.
O.THROTTLE	The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE.

OE.PERSONNEL	Those responsible for the TOE must ensure that personnel working as authorized administrators have been carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PLATFORM	The underlying operating system of each TOE software component will protect the component and its configuration from unauthorized access.
OE.TIME	The underlying operating system of each TOE software component provides a reliable time source for use by the TOE.

5. IT Security Requirements

5.1 Extended Components Definition

5.1.1 Network Monitoring (FNM)

This ST defines a new functional class for use within this ST: Network Monitoring (FNM). The ST author determined none of the existing CC Part 2 functional classes, families or components specifies requirements for a capability to retrieve and collect network device data.

5.1.1.1 Network Monitoring Device Data Collection (FNM_DDC_EXT)

This family defines data retrieval options and data collection for device data from a network.

Management: FNM_DDC_EXT.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control Device Data Retrieval.

Management: FNM_DDC_EXT.2

The following actions could be considered for the management functions in FMT:

a) configuration of the functions that control Device Data Collection.

Audit: FNM_DDC_EXT.1, FNM_DDC_EXT.2

There are no auditable events foreseen.

FNM_DDC_EXT.1– Network device data retrieval method

Hierarchical to: No other components.

Dependencies: None

FNM_DDC_EXT.1.1 The TSF shall be able to retrieve data from a network device using the following methods: [**assignment:** ***non-empty list of retrieval method***].

FNM_DDC_EXT.2– Network device data collection

Hierarchical to: No other components.

Dependencies: FNM_DDC_EXT.1: Network device data retrieval method

FNM_DDC_EXT.2.1 The TSF shall be able to collect [**assignment: non-empty list of data to be collected**] from the network devices.

5.1.1.2 Network Analysis (FNM_ANL_EXT)

This family defines the analysis functions performed on the collected network device data.

Management: FNM_ANL_EXT.1

The following actions could be considered for the management functions in FMT:

There are no management activities foreseen.

Audit: FNM_ANL_EXT.1

There are no auditable events foreseen.

FNM_ANL_EXT.1 – Network analysis

Hierarchical to: No other components.

Dependencies: FNM_DDC_EXT.2

FNM_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on Network data collected from network devices: [**assignment: analysis functions performed on the data**].

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 4, and from the extended components defined in Section 5.1 above.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of security function behaviour
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_STM.1: Reliable time stamps
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination
	FTA_SSL.4: User-initiated termination
	FTA_TAB.1: Default TOE access banners
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted path
FNM: Network Monitoring	FNM_DDC_EXT.1: Network device data retrieval method
	FNM_DDC_EXT.2: Network device data collection
	FNM_ANL_EXT.1: Network analysis

Table 1: TOE Security Functional Components

5.2.1 Security Audit (FAU)

FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit; and

c) [**the following auditable events:**

- **User login**
- **User logout**
- **Server up/down**
- **Password changes**
- **All user-management operations**
- **User actions that change the model]**.

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, [**none**].

FAU_GEN.2 – User Identity Association

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

FAU_SAR.1 – Audit review

FAU_SAR.1.1 The TSF shall provide [**Admin, Admin – Users, Admin – Operational, Admin – Vulnerability Control**] with the capability to read [**all audit information except the server up/down events**] 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.

Application Note: The Server up/down events are viewable through the TSF's host OS interface**.**

FAU_SAR.2 – Restricted audit review

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

FAU_STG.1 – Protected audit trail storage

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

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

5.2.2 Identification and Authentication (FIA)

FIA_AFL.1 – Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***3***] unsuccessful authentication attempts occur related to [**user login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**disable the user account for 30 seconds**].

FIA_ATD.1 – User attribute definition

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

- **User Identity**
- **Password**
- **Role**].

FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following constraints for all user accounts:**

- **Minimum length of 8 characters**
- **At least 1 upper case letter**
- **At least 1 lower case letter**
- **At least 1 digit**
- **At least 1 non-alphanumeric symbol**
- **Cannot contain username**
- **May not contain 5 or more characters from the previous password if they are in the same positions as they were in the previous password**].

FIA_UAU.2 – User authentication before any action

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.5 – Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [**a local password mechanism and allow for remote authentication via LDAP or RADIUS**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **Locally defined users are authenticated using the password associated with the user's account**
- **Users defined in the external LDAP or RADIUS server are authenticated using the password associated with the externally managed account**].

FIA_UID.2 – User identification before any action

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.

5.2.3 Security Management (FMT)

FMT_MOF.1 – Management of security function behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of, modify the behavior of***] the functions [**user authentication methods**] to [**Admin, Admin-Operational, Admin – Vulnerability Control, Admin – Assurance].**

.

FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***query, modify, delete, [create]***] the [**TOE users]** to [**Admin, Admin-users, Admin – Vulnerability Control**[1]**, Admin – Assurance**[2]].

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**Live network model]** to [**Admin, Admin-Operational, Admin – Vulnerability Control, Admin – Assurance**].

[1] User management for this admin is restricted to creation of Vulnerability Control roles.
[2] User management for this admin is restricted to creation of Assurance roles.

FMT_MTD.1.1(3) The TSF shall restrict the ability to [***query***] the [**audit logs]** to [**Admin, Admin-Operational, Admin – Vulnerability Control, Admin – Assurance**].

FMT_SMF.1 – Specification of Management Functions

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

- **Manage users,**
- **View audit logs,**
- **Configure user authentication methods,**
- **Manage live network model**].

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- **Admin**
- **Admin – Users**
- **Admin – Operational**
- **Admin – Vulnerability Control**
- **Admin – Assurance**

].

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

5.2.4 Protection of the TSF (FPT)

FPT_ITT.1 – Basic internal TSF data transfer protection

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

FPT_STM.1 – Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.5 TOE Access (FTA)

FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**time period of user inactivity**].

FTA_SSL.4 – User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 – Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

5.2.6 Trusted Path/Channels (FTP)

FTP_ITC.1 –Inter-TSF trusted channel

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***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**LDAP external user authentication**].

FTP_TRP.1 –Trusted path

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***].

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 [***initial user authentication, [all subsequent user interactions]***].

5.2.7 Network Monitoring (FNM)

FNM_DSC_EXT.1 – Network device data retrieval method

FNM_DSC_EXT.1.1 The TSF shall be able to retrieve data from a network device using the following methods: [**online collection, offline file import, script**].

FNM_DSC_EXT.2: Network device data collection

FNM_DSC_EXT.2.1 The TSF shall be able to collect [

- **Host names;**
- **Device type;**
- **IP addresses and subnet masks;**
- **Network interfaces;**
- **Status;**
- **Access rules;**
- **Routing rules;**
- **Hit counts;**
- **Change events; and**
- **Configuration files or vulnerability scan data**]

from the network devices.

FNM_ANL_EXT.1 – Network Analysis

FNM_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on Network data collected from network devices: [

- **Access Analyzer**
- **Network Map**
- **Access Compliance**
- **Rule Compliance**
- **Shadowed and redundant rules analysis**
- **Rule optimization**
- **Change tracking**
- **Path Analysis (in Change Manager)**
- **Vulnerability and Attack Simulation (in Vulnerability Control)**
- **Configuration Compliance**].

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: 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
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims
	ASE_ECD.1: Extended components definition
	ASE_INT.1: ST introduction
	ASE_OBJ.2: Security objectives
	ASE_REQ.2: Derived security requirements
	ASE_SPD.1: Security problem definition
	ASE_TSS.1: TOE summary specification
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 2: TOE Security Assurance Components

5.3.1 Development (ADV)

ADV_ARC.1 – Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 – Security-enforcing functional specification	
ADV_FSP.2.1D	The developer shall provide a functional specification.
ADV_FSP.2.2D	The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.2.1C	The functional specification shall completely represent the TSF.
ADV_FSP.2.2C	The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C	The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C	For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C	For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 – Basic design	
ADV_TDS.1.1D	The developer shall provide the design of the TOE.
ADV_TDS.1.2D	The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C	The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C	The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C	The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.
ADV_TDS.1.5C	The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C	The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.
ADV_TDS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E	The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

AGD_OPE.1 – Operational user guidance	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

ALC_CMC.2 – Use of a CM system

ALC_CMC.2.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D	The developer shall provide the CM documentation.
ALC_CMC.2.3D	The developer shall use a CM system.
ALC_CMC.2.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 – Parts of the TOE CM coverage

ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures	
ALC_DEL.1.1D	The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.
ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_FLR.1 – Basic Flaw Remediation	
ALC_FLR.1.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR. 1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims	
ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
ASE_INT.1.3C	The TOE reference shall identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

ASE_OBJ.2.1D	The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D	The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE summary specification

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.3.5 Tests (ATE)

ATE_COV.1 – Evidence of coverage

ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing – sample

ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis

AVA_VAN.2.1D	The developer shall provide the TOE for testing.
AVA_VAN.2.1C	The TOE shall be suitable for testing.
AVA_VAN.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3E	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section describes the following security functions implemented by the TOE to satisfy the SFRs claimed in Section 5.2:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Network Monitoring.

6.1 Security Audit

The TOE generates audit records of user management and operational events, including: login; logout; server up/down; password changes; and all user-management operations. Each audit log includes the following information: date and time of the event; type of event; subject identity; and the outcome of the event. The manner in which the TOE is able to provide a reliable time stamp for audit records is described in Section 6.4 below.

Skybox Security Suite stores generated audit records locally on the Skybox Server and can be configured to export logs to an external syslog server.

The TOE provides an Activity log and an Audit log. The Activity log displays application and user events and the Audit log displays user management and login/logout events.

User actions that change the model are logged in the Activity log. Actions logged include:

- Changes to and creation or deletion of assets, networks, network interfaces, tickets, security metrics, and notifications
- Vulnerability Dictionary updates and alert service feeds
- Online updates of Skybox

The Audit log includes all audit events for user management actions, login/logout, and password changes, as well as messages about the creation of new tasks, and the modification or deletion of existing tasks.

Additionally the TOE includes an Event Logging function and Log Files which provides other log information including system events (e.g. starting and stopping the Server events). These logs are accessible through the host system rather than TOE interfaces. The TOE can be configured to export logs to an external syslog server using the Event Logging functions.

Note that the audit functions automatically start at system start-up and shut down only at system shutdown—there is no capability to otherwise shut down or start up the Activity log and Audit log. As such, the requirement to audit start-up and shutdown of the audit function is satisfied vacuously because there is no startup or shutdown of the audit function to be audited. Event Logging can be enabled and disabled and these actions are audited.

The TOE provides users in the Admin, Admin-Operations, Admin-Vulnerability Control, and Admin-Assurance roles the ability to view all locally stored audit logs. The Activity logs and the Audit logs can be viewed from the System folder of the Admin tree. The system events (e.g. starting and stopping the Server events) are viewable from the file: <Skybox home>\server\log\debug\tasks.log.

The audit events generated by the TOE are stored in a MySQL database that is included with the Skybox Server. The TOE does not provide any interface or mechanism to modify or delete the audit records stored in the database. The TOE specifies maximum storage allocation for its log files and will overwrite the oldest stored audit records when the log files reach their maximum size.

The Security Audit security function satisfies the following security functional requirements:

- FAU_GEN.1—audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.
- FAU_GEN.2—the TOE associates each auditable event resulting from actions of identified users with the identity of the user that caused the event.
- FAU_SAR.1—the TOE provides authorized users with the capability to read audit information from the audit records. The audit records are displayed in a manner suitable for the authorized user to interpret the information.
- FAU_SAR.2—the TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access.
- FAU_STG.1—the TOE protects stored audit records from unauthorized modification and deletion.
- FAU_STG.4—the TOE overwrites the oldest stored audit records if the audit trail is full.

6.2 Identification and Authentication

The TOE maintains accounts of its authorized users. A user account includes the following attributes associated with the user: user identity; password; and role. The TOE uses roles associated with individual users to give users permission to perform specific actions within the system.

The TOE requires all users to be successfully identified and authenticated before allowing them to perform any other activities. The TOE can authenticate users directly in Skybox, based on user password, and can be configured to use an external LDAP or RADIUS authentication server. Authentication occurs as follows:

- Local password-based authentication—as part of the login process, the user supplies a login name and password. The password must match the password associated with the user account.
- External authentication using LDAP—the user supplies a login name and password. The login name is mapped to the DN for that user (stored in the local database) and the DN and user password are used to authenticate to the LDAP server.
- External authentication using RADIUS—the user is authenticated by a (RADIUS) password matching the submitted user name.

Skybox Security Suite detects when an administrator-configurable positive integer of unsuccessful authentication attempts occur related to user authentication. When the defined number of unsuccessful authentication attempts has been met, the TOE locks the user account for the specified time period. The default lockout time is 30 seconds following three consecutive failed authentication attempts.

Passwords managed by Skybox Security Suite must meet the requirements of the Skybox password policy, as follows:

- Passwords must have a minimum length of 8 characters
- Passwords must contain at least 1 upper case letter
- Passwords must contain at least 1 lower case letter
- Passwords must contain at least 1 digit
- Passwords must contain at least 1 non-alphanumeric symbol
- Passwords cannot contain username
- Passwords may not contain 5 or more characters from the previous password if they are in the same positions as they were in the previous password

When the TOE is configured for local password-based authentication, users are able to change their own passwords.

To login to the TOE, the user provides the login name and associated authentication data. If either the login name or the authentication data is incorrect, the login request fails and no user or administrator functions are made available.

As a result of a successful login, the interactive session is established and the user or administrator functions appropriate to the user's assigned roles are made available.

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1—the TOE is able to detect when an administrator-configurable positive integer of unsuccessful authentication attempts occur related to user authentication. When the defined number of unsuccessful authentication attempts has been met, the TOE locks the user account for a specified time period as configured by authorized administrator.
- FIA_ATD.1—the TOE maintains the following security attributes associated with each user: user identity; password; role.
- FIA_SOS.1—the TOE enforces a password policy that ensures all secrets (i.e., passwords) associated with user accounts meet policy requirements.
- FIA_UAU.2—the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5—the TOE supports multiple authentication mechanisms: local password; LDAP; and RADIUS.
- FIA_UID.2—the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3 Security Management

Skybox Security Suite provides several user roles that grant permissions to perform actions in specific parts of the product, as follows:

- Admin—can manage all aspects of the system. There are additional admin roles, which have management permission for a limited part of the system: Admin – Users; Admin – Operational; Admin – Vulnerability Control; and Admin – Assurance.
- User—can run various security analyses. There are also more limited User sub-roles, as follows:
    - User – Vulnerability Control—User role that is limited to the Skybox Vulnerability Control and Threat Manager modules.
    - User – Assurance—User role that is limited to the Skybox Firewall Assurance and Skybox Network Assurance modules
- Read-only User—can view the data and edit tickets that are assigned to their user or group. There are also more limited Read-only User sub-roles, as follows:
    - Read-only User – Vulnerability Control—Read-only User role that is limited to the Skybox Vulnerability Control and Threat Manager modules
    - Read-only User – Assurance—Read-only User role that is limited to the Skybox Firewall Assurance and Skybox Network Assurance modules
- Ticket User—can manage tickets and view (but not generate) reports. This role is for Skybox Vulnerability Control and Skybox Threat Manager. It cannot be used for Skybox Change Manager.
- Web Ticket User—can log in to Change Manager, where they can manage tickets. They cannot log in to the Manager GUI. This role is for Change Manager.
- Web Ticket Requestor—can open tickets (that is, submit change requests) in Change Manager and close tickets that they created. This role is for Change Manager.

The TOE provides capabilities for the following administrators to manage the security functions of the Skybox Security Suite: Admin, Admin – Users, Admin – Operational, Admin – Vulnerability Control, and Admin – Assurance. The administration functions are accessed from the Skybox Manager GUI and include: user management

(users, user groups and user roles), viewing audit records, configuration of authentication methods, and managing the network model.
Administrators configure the TOE to collect device data using automated data collection tasks. The TOE correlates this device data into the Live Model that represents the current state of the network. Devices that can be configured for collection include: security control devices such as firewalls, IPS, and VPNs; network infrastructure devices such as routers, switches and load balancers; and network assets such as servers and workstations. In addition, administrators can configure the TOE to automatically check for updates to the Vulnerability Dictionary to keep the model up-to-date.

Administrative users can also manage all entities that can be managed by the corresponding user-type role. For example, Admin – Assurance users can manage all entities that can be managed by User – Assurance users. Table 3 identifies all user and administrator roles and their respective permissions; and includes roles and capabilities not related to SFRs being claimed for the TOE.

Note that the TOE maintains a user role of 'Recipient' for external users to receive tickets, alerts, and reports. Users assigned to this role are not TOE users since they cannot login or access any other Skybox features other than items sent to them.

Role	**Description**	**Permissions**
Admin	**Admins** have permissions for all actions, including those that regular users do not.	**Administration functions** User management (users, user groups and user roles) Triggers Read system logs Configuration of user authentication methods (Tools>Options>Server Options) Model building (Model instances (Live, What if, Forensics) and collection tasks) **Vulnerability Control and Threat Manager related entities** Business Impact Types Regulations Threat Alert Ticket Policies Vulnerability Occurrence Ticket Policies **Firewall Assurance and Network Assurance related entities** Rule Review Policies Rule Recertification Policies **Operational Console** Collection tasks Other tasks Collectors **Reports and analysis** Reports – public and private Ticket analysis – public and private Vulnerability Control/Threat Manager analysis – public and private Firewall Assurance/Network Assurance analysis Model analysis **Skybox Horizon (Admin is the only role with access to Horizon).** **Admin users can also manage all entities that can be**

		managed by users .
Admin – Users	Same as **Admin** but functionality is limited to user administration only.	User management
Admin – Operational	Same as **Admin** but functionality is limited to everything except user administration and Skybox Horizon.	**Administration functions** (all except user administration) • Triggers • Read system logs • Configuration of user authentication methods (Tools>Options>Server Options) • Model building (Model instances (Live, What if, Forensics) and collection tasks) Vulnerability Control and Threat Manager related entities Firewall Assurance and Network Assurance related entities Operational Console Reports and analysis
Admin – Vulnerability Control	Same as **Admin** but Skybox access is limited to Vulnerability Control and Threat Manager.	**Administration (**User management restricted to creation of Vulnerability Control roles): Admin – Vulnerability Control, User – Vulnerability Control, Read-only User – Vulnerability Control, Recipient. • Triggers • Read system logs • Configuration of user authentication methods (Tools>Options>Server Options) • Model building (Model instances (Live, What if, Forensics) and collection tasks Vulnerability Control and Threat Manager related entities Operational Console Reports and analysis (except as related to Firewall Assurance/Network Assurance analysis) Admin users can also manage all entities that can be managed by the corresponding user-type role. For example, Admin – Assure users can manage all entities that can be managed by User – Assure users such as tickets and network maps.
Admin – Assurance	Same as **Admin** but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.	**Administration (**User management restricted to creation of Assurance roles): Admin – Assurance, User – Assurance, Read-only User – Assurance, Recipient: • Triggers • Read system logs • Configuration of user authentication methods (Tools>Options>Server Options) • Model building (Model instances (Live, What if, Forensics) and collection tasks Firewall Assurance, Change Manager, and Network

		Assurance Operational Console Reports and analysis (except as related to Vulnerability Control/Threat Manager analysis) Admin users can also manage all entities that can be managed by the corresponding user-type role. For example, Admin – Assure users can manage all entities that can be managed by User – Assure users such as tickets and network maps.
User	**Users** have permissions for all actions except administration tasks (for example, user management and model building). Users can access all Skybox products.	Vulnerability Control and Threat Manager related entities Firewall Assurance and Network Assurance related entities Operational Console (Read-only access to Collectors and Collection tasks) Reports and analysis (Read-only access to Public ticket analysis, Vulnerability Control/Threat Manager public analysis, and Model analysis)
User – Vulnerability Control	Same as **User** but Skybox access is limited to Vulnerability Control and Threat Manager.	Vulnerability Control and Threat Manager related entities Operational Console Reports and analysis
User – Assurance	Same as User but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.	Firewall Assurance and Network Assurance related entities Operational Console Reports and analysis
Read-only User	Read-only Users can view the model but they cannot make changes to it. They have permissions for all activities required for managing tickets, including using and creating private analyses for displaying tickets.	All activities required for managing tickets, including using and creating private analyses for displaying tickets and can view all user tasks in: Vulnerability Control, Threat Manager, Firewall Assurance, Change Manager, Network Assurance.
Read-only User – Vulnerability Control	Same as Read-only User but Skybox access is limited to Vulnerability Control and Threat Manager.	All activities required for managing tickets, including using and creating private analyses for displaying tickets and can view all user tasks in: Vulnerability Control and Threat Manager read-only user activities.
Read-only User – Assurance	Same as Read-only User but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.	All activities required for managing tickets, including using and creating private analyses for displaying tickets and can view all user tasks in: Firewall Assurance, Change Manager, and Network Assurance read-only user activities

Ticket User	Ticket Users can manage tickets and view (but not generate) reports. This role is for Vulnerability Control and Threat Manager. It cannot be used for Change Manager.	View reports and manage tickets in Vulnerability Control and Threat Manager
Web Ticket User	Web Ticket Users can log in to Change Manager, where they can manage tickets. They cannot log in to the Manager GUI. This role is for Change Manager.	Manage tickets in Change Manager
Web Ticket Requestor	Web Ticket Requestors can create tickets (that is, submit change requests) in Change Manager and close tickets that they created. This role is for Change Manager.	Create and close tickets in Change Manager
Recipient	Recipients can receive tickets, alerts, and reports. They cannot log in to Skybox or access any other Skybox features.	Receive tickets, alerts, and reports.

Table 3: Role – Permissions

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1—the TOE is able to restrict the management of aspects of the TSF to users assigned specific roles.
- FMT_MTD.1(*)—the TOE is able to restrict the management of TSF data to users assigned specific roles.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—the TOE defines security management roles based on the privileges assigned to user groups.

6.4 Protection of the TSF

Skybox Security Suite uses HTTPS to protect communications between the Skybox Server and Skybox Manager clients and between the Skybox Server and Skybox Collectors. HTTPS protects the transmitted TSF data from disclosure, and modification.

When the TOE is an appliance-based component, the TOE maintains time internally using a CMOS clock and this internal time is used as the source for reliable timestamps used by those components (e.g., for the date-time stamp recorded in audit events or for calculating interactive user session inactivity).

Software-based TOE components use the system clock maintained by the underlying operating system as the source for date and time information.

The Protection of the TSF security function satisfies the following security functional requirements:

- FPT_ITT.1—the TOE uses HTTPS to protect TSF data from disclosure and modification when it is transmitted between distributed parts of the TOE.
- FPT_STM.1—the TOE is able to provide reliable time stamps, based on its own internal clock (for hardware appliance-based components) or a time source in its operational environment.

6.5 TOE Access

The TOE can be configured to terminate an interactive user session after a specified time interval of user inactivity. The timeout value for an inactive session is configurable through the TSF's host OS interface in terms of minutes. By default, a user account is logged out after 30 minutes of inactivity.

The TOE allows user-initiated termination of the user's own interactive session by explicitly logging off.

Skybox Security Suite displays an advisory warning regarding unauthorized use that is configurable through the TSF's host OS interface. The message is displayed prior to a user login at the GUI and Web UI.

The TOE Access security function satisfies the following security functional requirements:

- FTA_SSL.3—the TOE terminates an interactive session after a time interval of user inactivity.
- FTA_SSL.4—the TOE allows user-initiated termination of the user's own interactive session.
- FTA_TAB.1—the TOE displays an advisory warning message regarding unauthorized use of the TOE.

6.6 Trusted Path/Channels

The TOE provides a trusted channel to communicate securely with external authentication servers. The trusted channel is implemented using TLS for LDAP.

The Skybox Server component uses the trusted channel for communication with external authentication servers. The use of TLS ensures all communication over the trusted channel is protected from disclosure and modification.

The TOE provides a trusted path for users of the TOE to communicate with the TOE. The trusted path is implemented using HTTPS for access from Skybox Horizon and Skybox Change Manager web GUIs to the Skybox Server. Users initiate the trusted path by establishing an HTTPS connection (using a supported web browser) to the Skybox Horizon or Skybox Change Manager components located on the Skybox Server as appropriate. The trusted path is used for initial authentication and all subsequent user actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

The Trusted Path/Channels security function satisfies the following security functional requirements:

- FTP_ITC.1—the TOE provides a trusted channel for the TOE to communicate with LDAP external authentication servers.
- FTP_TRP.1—the TOE provides a trusted path for users to communicate with the TOE, using HTTPS to access the Skybox Horizon and Skybox Change Manager GUIs as appropriate.

6.7 Network Monitoring

6.7.1 Device Data Retrieval Method

The TOE retrieves data from a network device using the following techniques: online collection; offline file import; and script. The TOE is configured with the devices on the network, and configured to collect the device data using one or more of the data retrieval methods.

The supported device types are firewall, router, load balancer, proxy, network device, wireless device, IPS, and switch. Specific supported devices are identified on the Skybox website:
https://www.skyboxsecurity.com/sites/default/files/Skybox_Supported_Devices.pdf

Offline file import (for supported devices): Obtains the data from files written by the device. The files might be stored in a repository or they might be stored elsewhere. The data files are imported to Skybox using an offline file import task.

Online collection (for supported devices): Obtains the data directly from the device or the device management system. An administrator creates a task in Skybox, which instructs the Skybox Collector to retrieve the necessary data from the device. This data is then added to the model.

Skybox can also be configured to collect data from unsupported devices by scripts created by Skybox professional services. Note that all data collection methods require creation of a data collection task which instructs the Skybox Collector to periodically and automatically retrieve the data from the device using the specified retrieval method.

6.7.2 Network Device Data Collection

The TOE collects device data from the following types of network devices: firewall; router; load balancer; proxy; network device; wireless device; IPS; Switch. The collected data includes Host names, Device type, IP addresses

and subnet masks, Network interfaces, Status, Access rules, Routing rules, and Configuration files or vulnerability scan data. A data collection task is created by an administrator which instructs the Skybox Collector to periodically and automatically retrieve the data from the device using the specified retrieval method. The TOE uses the collected data to analyze the network.

6.7.3 Network Analysis

The TOE uses the host names, device type, IP addresses and subnet masks, network interfaces, status, access rules, routing rules, hit counts, change events, and configuration files or vulnerability scan data to analyze the network. The analysis performed on this data includes:

- Access Analyzer: Simulation tool that analyses access in the network, taking into account access rules, routing rules, and network topology. It works by answering specific queries about access in your organization's network (for example, "Is network X available from network Y over HTTP?")
- Network Map: Analyzes and shows the topology of the entire model or specific parts.
- Access Compliance: Ensures compliance with your organization's Access Policy.
- Rule Compliance: Compares the existing access rules of a firewall to a list of syntactic Rule Checks that consist of basic standards for access rules.
- Shadowed and redundant rules analysis: Shadowing and redundancy is based on a logical analysis of the firewall's ACL to find access rules that can never be reached and other access rules that you can delete without changing the behaviour of the firewall.
- Rule optimization: Finds redundant, hidden and obsolete rules for cleanup and optimization.
- Change tracking: Validates proposed firewall changes by checking for policy violations, security gaps and new vulnerabilities; and ensures changes are made as intended and that the changes don't introduce new risk.
- Path Analysis (in Change Manager): analyzes end-to-end network connectivity & assesses compliance.
- Vulnerability and Attack Simulation (in Vulnerability Control): Detects vulnerability occurrences based on version and patch information (imported from patch management and asset management systems) and adds them to the model.
- Configuration Compliance: Configuration Compliance is analysed by comparing a firewall's configuration data with a Configuration Policy—the predefined policy included with the device or a customized policy created by your organization. The analysis shows where the configuration data does not comply with the policy.
- The Skybox Vulnerability Dictionary is also used to determine vulnerabilities and threats to a network. Skybox uses the Vulnerability Dictionary to normalize vulnerability occurrences found by scanners, adding all the relevant information—including description, cross-references from various sources, and external URLs—to the model.

The Skybox Vulnerability Dictionary supports more than 68,000 vulnerabilities collected from leading public and private security data sources, and built as a superset of vulnerabilities. As a state-of-the-art vulnerability database, it is CVE compliant and implements CVSS v2 and v3 standards.

The Vulnerability Dictionary is continuously updated by the Skybox Research Lab. It models all new Vulnerability Definitions as they are released and updates existing Vulnerability Definitions throughout their life cycle. Administrators can configure the Vulnerability Dictionary for automatic updates to keep the security model up-to-date.

The Network Monitoring security function satisfies the following security functional requirements:

- FNM_DSC_EXT.1—the TOE retrieves data from a network device using specified methods.
- FNM_DSC_EXT.2—the TOE collects information from network devices.
- FNM_ANL_EXT.1—the TOE performs analysis functions on Network data collected from network devices.

7. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

	T.BRUTE_FORCE	T.INAPPROPRIATE_USE	T.INTEGRITY_COMPROMISE	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T.UNATTENDED_SESSION	T. UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	T.UNDETECTED_THREATS	A. MANAGE	A.PLATFORM	A. PROTECT
O.AUDIT					X							
O.I_AND_A							X					
O.FNM_COLLECT									X			
O.FNM_ANALYSIS									X			
O.LOGON_BANNER		X										
O.PASSWORD_CONTROLS	X											
O.PROTECTED_COMMS				X								
O.SECURITY_MANAGEMENT								X				
O.SESSION_TERMINATION						X						
O.STORAGE			X									
O.THROTTLE	X											
OE.PERSONNEL										X		
OE.PHYSICAL												X
OE.PLATFORM											X	
OE.TIME					X							

Table 4: Security Problem Definition to Security Objective Correspondence

T.BRUTE_FORCE

An unauthorized user may gain access to the TOE through repeated password-guessing attempts.

This threat is countered by the following security objectives:

- O.PASSWORD_CONTROLS—addresses this threat by providing a mechanism, configurable by an administrator, which encourages users to choose difficult-to-guess passwords.
- O.THROTTLE—addresses this threat by providing a mechanism, configurable by an administrator, to lock a user account after a specified number of consecutive failed authentication attempts has been met.

T.INAPPROPRIATE_USE

Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.

This threat is countered by the following security objective:

- O.LOGON_BANNER—addresses this threat by displaying an advisory warning message to potential users pertaining to appropriate use of the TOE.

T.INTEGRITY_COMPROMISE

An unauthorized person may attempt to modify or destroy audit data, thus removing evidence of unauthorized or malicious activity.

This threat is countered by the following security objective:

- O.STORAGE—addresses this threat by ensuring the TOE is able to protect stored audit records from unauthorized modification and deletion.

T.NETWORK_COMPROMISE

An unauthorized user may monitor the enterprise network in an attempt to obtain sensitive data, such as passwords, or to modify transmitted data.

This threat is countered by the following security objective:

- O.PROTECTED_COMMS—addresses this threat by ensuring the TOE is able to protect communications between its distributed components and between itself and external entities.

T.NO_ACCOUNTABILITY

Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by ensuring the TOE is able to generate audit records of security relevant events.
- OE.TIME—supports O.AUDIT by ensuring the operational environment is able to provide the TOE software components with a reliable time source that can be used to generate time stamps for inclusion within generated audit records.

T.UNATTENDED_SESSION

An unauthorized user gains access to the TOE via an unattended authorized user session.

This threat is countered by the following security objectives:

- O.SESSION_TERMINATION—addresses this threat by providing users with a mechanism to terminate their interactive sessions with the TOE, and by ensuring sessions that have been inactive for a period of time will be terminated by the TOE.

T.UNAUTHORIZED_ACCESS

An unauthorized user may gain access to the TOE Security functions and data.

This threat is countered by the following security objective:

- O.I_AND_A—addresses this threat by ensuring all users of the TOE are identified and authenticated prior to gaining further access to the TOE and its services.

T.UNAUTHORIZED_ACTIVITY

Authorized users perform unauthorized actions on the TOE.

This threat is countered by the following security objective:

- O.SECURITY_MANAGEMENT—addresses this threat by providing a mechanism that requires authorized users to have appropriate roles in order to perform actions on the TOE.

T.UNDETECTED_THREATS

Vulnerabilities, threats, and non-compliance rules generated by or existing in devices in the network system indicative of misuse or unauthorized or malicious user activity go undetected.

This threat is countered by the following security objectives:

- O.FNM_COLLECT—addresses this threat by providing capabilities to collect network device data that the TOE will apply analysis functions on in order to identify vulnerabilities, threats, and non-compliance.
- O.FNM_ANALYSIS—supports O.FNM_COLLECT in addressing this threat by ensuring the TOE provides the analysis functions necessary to detect vulnerabilities, threats, and non-compliance in the network or on the network devices.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are properly trained in operating the TOE.

A.PLATFORM

The underlying operating system of each TOE software component will protect the component and its configuration from unauthorized access.

This assumption is satisfied by the following security objective:

- OE.PLATFORM—this objective satisfies the assumption by ensuring the operating system underlying each TOE software component protects the component and its configuration from unauthorized access.

A.PROTECT

The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

This assumption is satisfied by the following security objective:

- OE.PHYSICAL—this objective satisfies the assumption by ensuring the TOE is protected from physical attack.

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. Table 5 summarizes the correspondence of functional requirements to TOE security objectives.

	O.AUDIT	O.I_AND_A	O.FNM_COLLECT	O.FNM_ANALYSIS	O.LOGON_BANNER	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_TERMINATION	O.STORAGE	O.THROTTLE
FAU_GEN.1	X										
FAU_SAR.1	X										
FAU_SAR.2	X										
FAU_STG.1										X	
FAU_STG.4										X	
FIA_AFL.1											X
FIA_ATD.1		X									
FIA_SOS.1						X					
FIA_UAU.2		X									
FIA_UAU.5		X									
FIA_UID.2		X									
FMT_MOF.1								X			
FMT_MTD.1								X			
FMT_SMF.1								X			
FMT_SMR.1								X			
FPT_ITT.1							X				
FPT_STM.1	X										
FTA_SSL.3									X		
FTA_SSL.4									X		
FTA_TAB.1					X						
FTP_ITC.1							X				
FTP_TRP.1							X				
FNM_DDC_EXT.1			X								
FNM_DDC_EXT.2			X								
FNM_ANL_EXT.1				X							

Table 5: Objectives to Requirement Correspondence

O.AUDIT

The TOE shall be able to generate audit records of security-relevant events.

The following security functional requirements contribute to satisfying this security objective:

- FAU_GEN.1—the ST includes FAU_GEN.1 to specify the capability to generate audit records of security-relevant events, and to specify the specific events to be audited and the content of generated audit records of those events.
- FAU_SAR.1—the ST includes FAU_SAR.1 to specify which roles are to be able to read data from stored audit records.

- FAU_SAR.2—the ST supports FAU_SAR.1 by including FAU_SAR.2 to specify that the ability to read data from stored audit records is restricted to only the roles specified in FAU_SAR.1.
- FPT_STM.1—the ST supports FAU_GEN.1 by including FPT_STM.1 to specify the capability to provide reliable time stamps, which are applied to generated audit records.

O.I_AND_A

The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.

The following security functional requirements contribute to satisfying this security objective:

- FIA_UID.2, FIA_UAU.2—the ST includes FIA_UID.2 and FIA_UAU.2 to specify that users must be successfully identified and authenticated by the TOE before being able to perform any other TSF-mediated actions.
- FIA_ATD.1—the ST supports FIA_UID.2 and FIA_UAU.2 by including FIA_ATD.1 to ensure user identity and authentication data security attributes are associated with individual users.
- FIA_UAU.5—the ST supports FIA_UAU.2 by including FIA_UAU.5 to specify the authentication mechanisms supported by the TOE and the rules by which the TOE authenticates a user's claimed identity.

O.FNM_ANALYSIS

The TOE shall provide analysis functions necessary to detect vulnerabilities, threats, and non-compliance in the network or on the network devices.

The following security functional requirement contributes to satisfying this security objective:

- FNM_ANL_EXT.1—the ST includes FNM_ANL_EXT.1to specify the analysis functions that can detect vulnerabilities, threats, and non-compliance in the network or on the network devices.

O.FNM_COLLECT

The TOE shall provide capabilities to collect network device data that the TOE will apply to analysis functions on in order to identify vulnerabilities, threats, and non-compliance.

The following security functional requirement contributes to satisfying this security objective:

- FNM_DDC_EXT.2—the ST includes FNM_DDC_EXT.1to specify the capability to collect network device data from devices in the network.
- FNM_DDC_EXT.1— FNM_DDC_EXT.1 supports FNM_DDC_EXT.2by specifying the methods by which the TOE is capable of retrieving the network device data from devices in the network.

O.LOGON_BANNER

The TOE shall be able to display an advisory warning message to potential users pertaining to appropriate use of the TOE.

The following security functional requirement contributes to satisfying this security objective:

- FTA_TAB.1—the ST includes FTA_TAB.1 to specify the capability to display an advisory warning message regarding unauthorized use of the TOE.

O.PASSWORD_CONTROLS

The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.

The following security functional requirement contributes to satisfying this security objective:

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify that passwords must meet minimum construction requirements, in terms of length and character set.

O.PROTECTED_COMMS

The TOE shall protect communications between its distributed components and between itself and external entities.

The following security functional requirements contribute to satisfying this security objective:

- FPT_ITT.1—the ST includes FPT_ITT.1 to specify that TSF data communicated between distributed parts of the TOE will be protected from disclosure and modification.
- FTP_ITC.1—the ST includes FTP_ITC.1 to specify that data will be communicated between the TOE and LDAP external IT entities through a trusted channel that protects the data from disclosure and modification.
- FTP_TRP.1—the ST includes FTP_TRP.1 to specify that data will be communicated between the TOE and remote users through a trusted path that protects the data from disclosure and modification.

O.SECURITY_MANAGEMENT

The TOE shall restrict the ability to perform security management functions on the TOE to authorized users having appropriate roles.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FMT_MTD.1—the ST includes these requirements to specify the security management functions to be provided by the TOE (FMT_SMF.1), to specify security management roles (FMT_SMR.1), and to specify the restrictions on management of security function behavior and TSF data (FMT_MOF.1, FMT_MTD.1).

O.SESSION_TERMINATION

The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.

The following security functional requirements contribute to satisfying this security objective:

- FTA_SSL.3—the ST includes FTA_SSL.3 to specify the capability for the TSF to terminate an interactive user session after a period of inactivity.
- FTA_SSL.4—the ST includes FTA_SSL.4 to specify the capability for users to terminate their own interactive sessions.

O.STORAGE

The TOE shall protect stored audit records and IDS data from unauthorized modification or deletion.

The following security functional requirements contribute to satisfying this security objective:

- FAU_STG.1—the ST includes FAU_STG.1 to specify that stored audit records will be protected from unauthorized modification and deletion.
- FAU_STG.4—the ST includes FAU_STG.4 to specify that the oldest stored audit data will be overwritten when the audit trail is full in order to ensure that new audit records are stored.

O.THROTTLE

The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify the capability to limit the rate at which consecutive failed authentication attempts (which may indicate a password-guessing attack) can be made.

7.3 Security Assurance Requirements Rationale

EAL 2 augmented with ALC_FLR.1 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. ALC_FLR.1 was selected to exceed

EAL2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is intended for use in an environment with good physical access security where it is assumed that attackers will have Basic attack potential. The target assurance level of EAL 2 augmented with ALC_FLR.1 is appropriate for such an environment.

7.4 Requirement Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied by inclusion in the ST of the appropriate dependent SFRs.

Requirement	Dependencies	How Satisfied
FAU_GEN.1	FPT_STM.1	FPT_STM.1 See TimeStamp Note below
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	None	None
FIA_UID.2	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	None	None
FPT_STM.1	None	None
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None
FNM_DDC_EXT.1	None	None
FNM_DDC_EXT.2	FNM_DDC_EXT.1	FNM_DDC_EXT.1
FNM_ANL_EXT.1	FNM_DDC_EXT.2	FNM_DDC_EXT.2

Table 6: Requirement Dependencies

TimeStamp Note: The TOE may consist of software components or hardware appliances (with software). Hardware appliance-based components maintain time internally and use this internal time as the source for reliable timestamps. The software components operate as applications within a process provided by the environment. Thus, in a software-only configuration, the environment is providing resources for components of the TOE. The environmental objective OE.TIME requires that the TOE's software-only environment provide a reliable timestamp which the TOE can use as needed (e.g., within audit records). Therefore, the functionality specified in the dependency of FAU_GEN.1 upon FPT_STM.1 is available to the software components of the TOE from their environment.

7.5 TOE Summary Specification Rationale

Section 6, the TOE Summary Specification, describes how the security functions of the TOE meet the claimed SFRs. The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

	Security Audit	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path/Channels	Network Monitoring
FAU_GEN.1	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_STG.1	X						
FAU_STG.4	X						
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_SOS.1		X					
FIA_UAU.2		X					
FIA_UAU.5		X					
FIA_UID.2		X					
FMT_MOF.1			X				
FMT_MTD.1			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPT_ITT.1				X			
FPT_STM.1				X			
FTA_SSL.3					X		
FTA_SSL.4					X		
FTA_TAB.1					X		
FTP_ITC.1						X	
FTP_TRP.1						X	
FNM_DDC_EXT.1							X
FNM_DDC_EXT.2							X
FNM_ANL_EXT.1							X

Table 7: Security Functions vs. Requirements Mapping