Rapid7™

Nexpose™ Vulnerability Management and Penetration Testing System V.5.1

Security Target

Version 1.7
May 11, 2012

Prepared for:

Rapid7 LLC

545 Boylston Street, Suite 400
Boston, MA 02116

Prepared By:

Ward Rosenberry
Rosenberry Associates Inc.

30 Newfield Street
North Chelmsford, MA 01863

Revision History

Version	Modification Date	Modifier	Details
1.0	May 3, 2010	Gauthaman Ravindran	Initial Draft
1.1	June 22, 2010	Gauthaman Ravindran	Added EAL rationale section; fixed typographical and consistency errors.
1.2	July 5, 2010	Gauthaman Ravindran	Clarified wording in 6.1.2.1; clarified version number in Table 1
1.3	August 19, 2010	Gauthaman Ravindran	Changed version number of TOE from 4.8 to 5.0; information added concerning Cloud Edition.
1.4	December 27, 2011	Ward Rosenberry	Added SFRs for Multi-Tenancy functionality.
1.5	April 2, 2012	Ward Rosenberry	Formatting changes, corrections, updates, and editorial corrections.
1.6	May 3, 2012	Ward Rosenberry	Clarifications.
1.7	May 11, 2012	Ward Rosenberry	Minor edits.

Table of Contents

1 Security Target Introduction

This section identifies the Security Target (ST), the Target of Evaluation (TOE), and also provides an overview and a description of the TOE.

TABLE 1 ST AND TOE IDENTIFICATION

ST Title	Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1 Security Target
ST Version	1.7
ST Date	May 11, 2012
TOE Identification	Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1.0, with one of the following build numbers: - Linux 32: 2220601069 - Linux 64: 839270008 - Windows 32: 1220461598 - Windows 64: 3456844061
Common Criteria Identification	Common Criteria Version 3.1 r3 Part 2 and Part 3 conformant plus applicable interpretations
Assurance Level	Evaluation Assurance Level (EAL) 3+
Keywords	Vulnerability Assessment, Configuration Compliance, Penetration Testing, Database Security, Web Application Security
Author	Ward Rosenberry, Rosenberry Associates, Inc.

1.1 Security Target Reference

This Security Target is called:
Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1 Security Target

1.2 Target of Evaluation Reference

The Target of Evaluation is called: **Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V.5.1.0**, hereafter referred to as Nexpose™. Rapid7 is the developer of the TOE.

1.3 Target of Evaluation Overview

1.3.1 General Overview

Nexpose™ is a vulnerability scanner and vulnerability management tool that also supports policy compliance checking, web application scanning, and penetration testing.

Nexpose™ consists of a Nexpose™ Security Console (NSC) and one or more Nexpose™ Scan Engines (NSE). A single server can host Nexpose, since a local NSE is installed with the NSC. However, it is recommended that an additional NSE be installed on its own dedicated server and paired with the NSC. The NSC and NSE can run on hardware with the following specifications:

1.3.2 Table 2 Recommended Hardware for NSC and NSE

Processor	2GHz or faster
RAM	2GB (32-bit operating systems), 8 GB RAM (64-bit operating systems)
Disk Space	80+GB for NSC with local NSE, 10+GB for NSE only
NIC Card	100Mbps (32-bit operating systems), 1 Gbps (64-bit operating systems)

The TOE is officially supported on Windows Server 2003 SP2 (32-bit and 64-bit), Windows XP SP3 (32-bit), Ubuntu 8.04 (32-bit and 64-bit), and Red Hat Enterprise Linux 5.4 (64-bit), although it can run on other versions of Linux. As an alternative, the NSC and NSE can be run on dedicated hardware appliances available from Rapid7™. These appliances run Ubuntu 8.04 (64-bit).

Nexpose™ scans a specified list or range of IP addresses and collects information about any devices that it finds. Scans are configured via scan templates, which specify exactly how the scan is to be conducted. Scan templates are used to optimize scanning behavior for a particular audit. Some common uses include limiting the types of services that are scanned, searching for specific vulnerabilities, and adjusting network bandwidth usage. A scan template can be chosen from a list of preconfigured templates, or an administrator can create a custom scan template that best meets the needs of the organization.

Scans can be scheduled, or run manually. Scans can also be configured to send alerts when a scan starts, finishes, fails, or when a particular vulnerability is detected during the scan. The alerts can be sent via SMTP, SNMP, or written to the system log.

Nexpose™ is capable of identifying the operating system, installed software, services, and files and directories on a particular device. Nexpose™ can detect vulnerabilities in hosts, databases, and web applications (such as SQL injection or cross-site scripting), and can also detect policy violations based on policy files. Nexpose™ can use user-supplied credentials to log into hosts to acquire more detailed information.

Every vulnerability that Nexpose™ discovers in the scanning process appears in the Nexpose™ vulnerability database. This extensive, full-text, searchable database also stores information onpatches, downloadable fixes, and reference content about security weaknesses. An additional, optional feature is the Metasploit™ module, which provides a link to the Metasploit™ database, where specific information about working exploits for the vulnerability is kept. Nexpose™ keeps the database current through a subscription service that maintains and updates vulnerability definitions, policy checks, exploit information, and links. Nexpose™ contacts this service for new information every six hours.

Individual users can be assigned roles that grant or limit access to various Nexpose™ functions. In addition, administrators can assign assets (IP-enabled devices) to an asset group. Users can be given access to particular asset groups, from which they can view vulnerabilities and scan data for the members of the group, and can be assigned tickets for remediating vulnerabilities.

Nexpose™ has an optional “Cloud Edition” configuration, which is a licensed option. The Cloud Edition allows the creation of segregated silos that act as virtual NSCs. Superusers have the ability to create silos, and provision users with the authorization to access one or more silos. Users may only log into one silo at a time, and only have access to the data available with the silo to which they are logged in. Within a silo, silo administrators have no access to administrative functions such as diagnostics or maintenance. These functions are assigned to super-users who have access to all silos.

Nexpose™ is administered through the NSC via a GUI that is accessible via a standard HTTPS-enabled browser. Users can log into Nexpose™ with a username and password combination.

1.3.3 Nexpose™ Security Console

The Nexpose™ Security Console (NSC) is the central management tool for Nexpose™ and as such, has a number of functions:

Central Data Repository: The NSC serves as a central data repository for the NSE. In this role, the NSC actively initiates connections to NSEs. Scan data collected by the NSEs is aggregated and stored in the NSC.

User Interface: The NSC serves as the Nexpose™ interface to the end-user, accessible via an HTTPS-enabled web browser. Users can access network profile and scan data, and administrators can configure all scan engines and specify the network assets to be assigned to those engines.

Updates: The NSC retrieves update information from an update server every six hours. These updates contain new additions to the vulnerability database, new policy checks, and bug fixes. In addition, the NSC retrieves new vulnerability checks. The NSC distributes these checks to the associated NSEs. The update server is not considered part of the TOE; the interface between the TOE and the update server is an external interface.

Logs: The NSC collects and logs all details of the core system that are not related to active scans. The NSC logs include:

- First time configuration
- Nexpose™ start up and shutdown
- Updates
- Scheduled events (such as scans)
- Reporting
- Site configuration
- System diagnostics
- Scan integration
- User sessions (logins and logouts)

The NSC log files are not directly available to the user. For support and troubleshooting purposes, logs are transmitted to Rapid7 Support via HTTP. However, Rapid7 Support is not considered part of the TOE; the interface between the TOE and Rapid7 Support is an external interface.

Authentication: In order to access the Nexpose™ interface, users must log into the NSC. The NSC controls access via a username/password authentication method. The NSC also supports external authentication methods such as LDAP, Active Directory, and Kerberos. However, these external authentication methods are not considered part of the TOE, and will not be evaluated.

Authorization: Nexpose™ stores all user and role definitions, and enforces the role-based access controls. The functions that are presented to a given user are dependent on the user's role. Any functions or data that are restricted from a user's role will not be visible.

1.3.4 Nexpose™ Scan Engine

The Nexpose™ Scan Engine (NSE) is configured to profile a section, or sections, of network space specified in blocks of IP addresses. As such, several steps are involved in this process. The NSE performs the following functions:

Host Discovery: While scanning the targeted network, the NSE discovers which IP addresses in its assigned range have live devices attached to them. In other words, it detects all the IP enabled devices that are linked to the targeted network.

Application Detection: Besides discovering IP enabled devices, the NSE performs application, service, and protocol detection on the open ports it found while performing port scans.

Operating System Classification: After performing application/service/protocol detection, the NSE categorizes the IP enabled devices found on the network by operating system.

Vulnerability and Exposure Assessment: After gathering enough information about the IP enabled devices on the network and the network itself, the NSE performs a quantification of the vulnerabilities and exposures found on detected target hosts. This process includes dynamic scanning of web applications and discovery of database instances, tightly coupled with specific vulnerability and exposure detection.

Reports Findings to the NSC: While performing a scan of the targeted network, the NSE reports its vulnerability findings to the NSC. The reported information is transmitted to the NSC and stored in the NSC. This process is known as scan integration.

1.4 Target of Evaluation Description

1.4.1 Physical Scope

The physical scope of the TOE is the Nexpose™ Security Console (NSC) and the Nexpose™ Scan Engine (NSE), along with the following guidance documentation: Nexpose 5.1 Software Installation and Quick-start Guide, Nexpose 5.1 Administrator's Guide, Nexpose 5.1 User's Guide, and NeXpose Common Criteria Guidance Documentation. The TOE is a software-only TOE.

There are twelve configurations of the TOE under evaluation:

TABLE 3 TOE CONFIGURATIONS UNDER EVALUATION

Configuration	Hardware	OS	Edition
1	Generic (see Table 2)	Windows Server 2003 SP2 32-bit	Standard
2	Generic (see Table 2)	Windows Server 2003 SP2 64-bit	Standard
3	Generic (see Table 2)	Ubuntu 8.04 32-bit	Standard
4	Generic (see Table 2)	Ubuntu 8.04 64-bit	Standard
5	Generic (see Table 2)	Red Hat Enterprise Linux 5.4 64-bit	Standard
6	Generic (see Table 2)	Windows XP SP3 32-bit	Standard
7	Generic (see Table 2)	Windows Server 2003 SP2 32-bit	Cloud
8	Generic (see Table 2)	Windows Server 2003 SP2 64-bit	Cloud
9	Generic (see Table 2)	Ubuntu 8.04 32-bit	Cloud
10	Generic (see Table 2)	Ubuntu 8.04 64-bit	Cloud
11	Generic (see Table 2)	Red Hat Enterprise Linux 5.4 64-bit	Cloud
12	Generic (see Table 2)	Windows XP SP3 32-bit	Cloud

Each configuration of the TOE subject to evaluation consists of a single Nexpose™ Security Console and one or more associated Nexpose™ Scan Engines. The hardware on which the TOE is installed, and the operating system on which the TOE runs are considered part of the operating environment, and are not subject to evaluation.

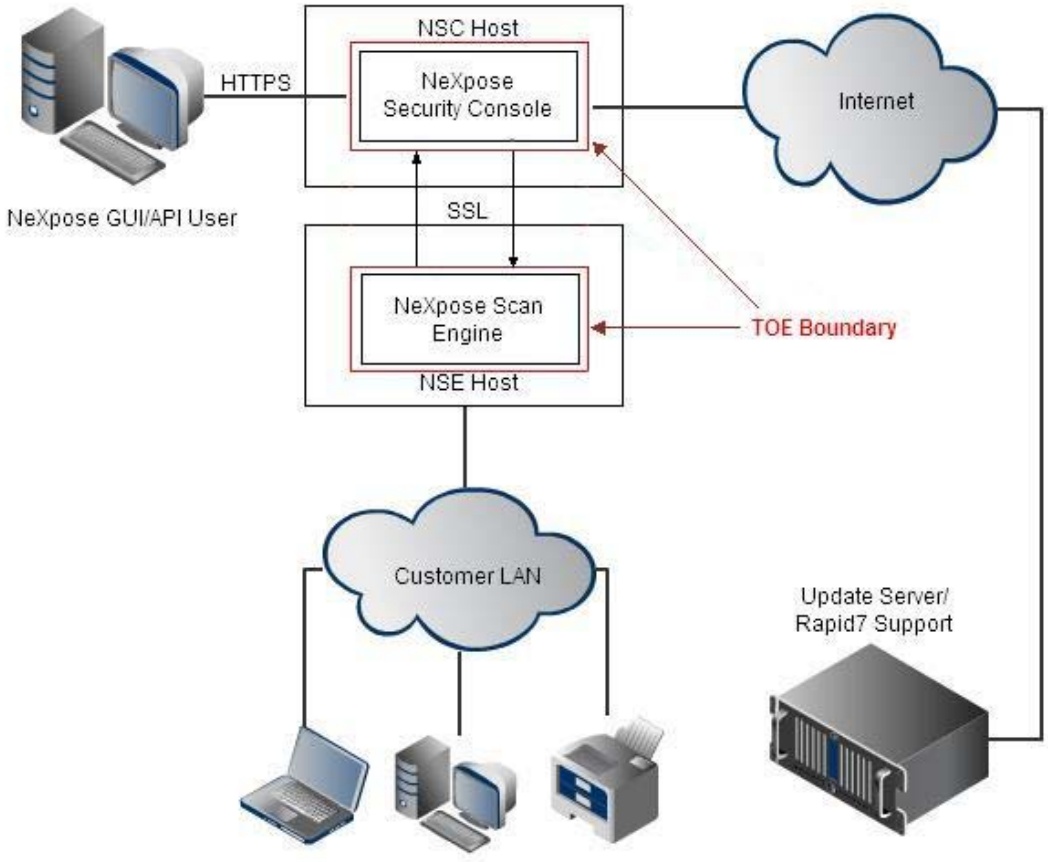

FIGURE 1 TOE BOUNDARY

A list of components and entities that are outside the TOE boundary is included in Table 4. Note that the NSC GUI via Browser is not part of the TOE boundary; however, the NSC GUI itself is part of the TOE boundary and resides in the NSC software.

TABLE 4 LIST OF COMPONENTS NOT INCLUDED IN THE TOE

COMPONENTS NOT INCLUDED IN THE TOE
NSC Host
NSE Host
NSC GUI via Browser
Network Connected Devices (on Customer LAN)
Update Server/Rapid7 Support

1.4.2 Logical Boundary

- The logical boundary of the TOE includes the functions of the TOE listed below:
- Identification and Authentication
- User Data Protection
- Security Management and Role Enforcement
- Audit
- TOE Access

1.4.2.1 Identification and Authentication

TOE users must identify themselves and be authenticated in order to gain access to services provided by the TOE. The NSC provides a Graphical User Interface that requires authentication to access. The NSC GUI addresses password guessing attacks by disabling a user's account after four failed attempts to authenticate.

1.4.2.2 User Data Protection

For the Cloud Edition, a data access security policy prevents users from accessing data in silos to which they are not authorized.

1.4.2.3 Security Management and Role Enforcement

The administrator and restricted users are provided with a graphic user interface (GUI) to perform configuration and troubleshooting tasks. Restricted users can be granted privileges in the NSC based on granular controls. Further, restricted users can be given variable access to scan data—users only have access to the scan data and asset information granted by administrative users.

1.4.2.4 Audit

Audit data of the TOE, in the form of log files, is recorded by the NSC. The TOE disallows access to the logs from the GUI, thereby preserving the integrity of audit data from TOE users.

1.4.2.5 TOE Access

Session activity is monitored by the TOE. Sessions that have not shown activity in a configurable amount of time are automatically terminated. As such, user activities are disabled and the user needs to log back in for another session.

1.4.2.6 Logical Functionality Not Included in TOE

SSL connections between the NSC and NSE are excluded from the TOE.

2 Conformance Claims

The TOE is Common Criteria Version 3.1 r3 Part 2 and Part 3 conformant plus applicable interpretations, and conformance to Evaluation Assurance Level 3+ is claimed, augmented with ALC_FLR.2. No conformance claim is made regarding Protection Profiles.

3 Security Problem Definition

This section describes the threats identified for the TOE, and describes any assumptions about the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed.

3.1 Threats to Security

The following are threats identified for the TOE. Unsophisticated attacker expertise for all the threats is assumed.

TABLE 5 LIST OF THREATS FOR THE TOE

Threat	Description
T.ACCESS	An unauthorized user may attempt to gain access to data collected and produced by the TOE.
T.BRUTE	An unauthorized user may attempt to gain access to the TOE by repeatedly trying to guess authentication data.
T.DELETE	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.ELEVATE	An unauthorized or restricted user may attempt to access TOE administrative functions.
T.INTERCPT	An attacker or unauthorized user may attempt to intercept data being passed between TOE components.
T.MODIFY	An attacker or unauthorized user may attempt to modify data collected or produced by the TOE.

3.2 Secure Usage Assumptions

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

TABLE 6 LIST OF ASSUMPTIONS REGARDING SECURITY ENVIRONMENT AND INTENDED USAGE FOR THE TOE

Assumption	Description
A.ATTACK	Attackers are assumed to have a low level of expertise, resources and motivation.
A.CLIENT	The SSL- connection between the user's browser and the TOE, and the SSL-connection between the NSC and the NSE are assumed to be secure.
A.CONNECT	The components of the TOE are assumed to be connected to the target network at all times.
A.ENV	The TOE is assumed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.
A.INSTALL	The TOE hardware and software are delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.INTROP	The TOE is assumed to be interoperable with the IT System that it monitors.
A.NOEVIL	Those responsible for the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PHYSICAL	The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities, preventing unauthorized physical access and modification by potentially hostile outsiders.
A.PRIVIL	Users of the TOE are assumed to posses the necessary privileges to access information managed by the TOE.
A.REMOTE	The update server and Support site with which the TOE communicates are assumed to be under the same management control and operated under the same security policy constraints as the TOE.
A.TRUSTED	The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the requirements of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The TOE satisfies the following objectives.

TABLE 7 LIST OF SECURITY OBJECTIVES FOR THE TOE

Objective	Description
O.ACCESS	The TOE must allow authorized users to access only the TOE functions and data for which they have privileges .
O.ADMIN	The TOE will provide facilities to enable an authorized administrator to effectively manage the TOE, and will ensure that only authorized administrators are able to access such functionality.
O.AUDITS	The TOE must provide an audit trail of TOE events in the form of log files.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the TOE Environment

The TOE's operating environment must satisfy the following objectives.

TABLE 8 LIST OF SECURITY OBJECTIVES FOR THE TOE'S OPERATING ENVIRONMENT

Objective	Description
OE.ATTACK	Those responsible for the TOE are proactive in preventing attacks.
OE.CONNECT	Those responsible for the TOE must ensure that all components of the TOE remain connected to the target network at all times.
OE.CREDENT	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.ENV	Those responsible for the TOE must ensure that the TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with documented delivery and installation/setup procedures.
OE.INTROP	Those responsible for the TOE must ensure that the TOE is interoperable with the IT System it monitors.
OE.NOEVIL	Those responsible for the TOE are non-hostile and follow all administrator guidance.
OE.PERSON	Those responsible for the TOE shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.PRIVIL	Those responsible for the TOE possess the necessary privileges to access information managed by the TOE.
OE.REMOTE	The Software Repository and other servers with which the TOE communicates are under the same management control and operate under the same security policy constraints as the TOE.
OE.SSL	The environment will protect data from disclosure between TOE components.
OE.TIME	The environment will provide a reliable time service for the TOE.
OE.TRAIN	Those responsible for the TOE must be trained to establish and maintain sound security policies and practices.
OE.TRUSTED	Those responsible for the TOE must ensure that the users of the network from which the TOE will be administered are trusted.

4.3 Security Objectives Rationale

This section describes associates the security objectives of the TOE and the TOE environment with security threats and assumptions, and provides justifications for those associations.

TABLE 9 THREATS AND ASSUMPTIONS VS. OBJECTIVES

	Security Objective for the TOE					Security Objective for the Environment													
	O.ACCESS	O.ADMIN	O.AUDITS	O.IDAUTH	O.PROTECT	OE.ATTACK	OE.CONNECT	OE.CREDENT	OE.ENV	OE.INSTALL	OE.INTEROP	OE.NOEVIL	OE.PERSON	OE.PHYSICAL	OE.PRIVIL	OE.REMOTE	OE.SSL	OE.TIME	OE.TRAIN	OE.TRUSTED
A.ATTACK						X														
A.CLIENT									X		X						X			
A.CONNECT							X													
A.ENV									X											
A.INSTALL										X										
A.INTEROP											X									
A.NOEVIL								X				X							X	
A.PHYSICAL														X						
A.PRIVIL															X					
A.REMOTE																X				
A.TRUSTED												X	X						X	X
T.ACCESS	X		X	X	X													X		
T.BRUTE				X	X															
T.DELETE	X	X		X	X															
T.ELEVATE	X	X		X																
T.INTERCPT					X												X			X
T.MODIFY	X	X		X	X															

A.ATTACK Attackers are assumed to have a low level of expertise, resources and motivation. The OE.ATTACK objective ensures that proactive measures in preventing attacks are taken.

A.CLIENT The OE.SSL objective ensures that the web browsers that act as the GUI interface to the TOE are capable of providing a secure SSL connection, and the SSL connection between TOE components is likewise secure. The OE.ENV objective ensures that the TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product. The OE.INTROP ensures that the TOE is interoperable with the IT System it monitors.

A.CONNECT The components of the TOE are assumed to be connected to the target network at all times. The OE.CONNECT objective ensures that all components of the TOE remain connected to the target network at all times.

A.ENV The TOE is assumed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product. The OE.ENV objective

ensures that the TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

A.INSTALL The TOE hardware and software are delivered, installed, and setup in accordance with documented delivery and installation/setup procedures. The OE.INSTALL objective ensures that the TOE is delivered, installed managed, and operated in a manner which is consistent with documented delivery and installation/setup procedures.

A.INTROP The TOE is assumed to be interoperable with the IT System it monitors. The OE.INTROP ensures that the TOE is interoperable with the IT System it monitors.

A.NOEVIL Those responsible for the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.CREDENT objective ensures that all access credentials are protected by the users in a manner which is consistent with IT security. The OE.NOEVIL objective ensures that the users of the TOE are non-hostile and follow all administrator guidance. The OE.TRAIN objective ensures that the users of the TOE must be trained to establish and maintain sound security policies and practices.

A.PHYSICAL The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities which will prevent unauthorized physical access and modification by potentially hostile outsiders. The OE.PHYSICAL objective ensures that the TOE is protected from any physical attack.

A.PRIVIL Users of the TOE are assumed to possess the necessary privileges to access information managed by the TOE. The OE.PRIVIL objective ensures that the users of the TOE possess the necessary privileges to access information managed by the TOE.

A.REMOTE The software repository and Support server with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints as the TOE. The **OE.REMOTE** objective ensures that the software repository and Support server with which the TOE communicates are under the same management control and operate under the same security policy constraints as the TOE.

A.TRUSTED The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks. The OE.NOEVIL objective ensures that the users of the TOE are non-hostile and follow all administrator guidance. The OE.PERSON objective ensures that the users of the TOE are carefully selected and trained for proper operation of the TOE. The OE.TRAIN objective ensures that the users of the TOE must be trained to establish and maintain sound security policies and practices. The OE.TRUSTED objective ensures that the users of the network from which the TOE will be administered are trusted.

T.ACCESS An undetected compromise of the TOE may occur as a result of an attacker (whether an insider or an outsider) attempting to perform actions that the individual is not authorized to perform. The O.ACCESS objective builds upon the O.IDAUTH objective by only allowing authorized users to access TOE data. The O.AUDITS objective addresses this threat by ensuring that the TOE provides an audit trail of security-related events. The OE.TIME object builds on the O.AUDITS objective by ensuring that the audit trail has reliable time stamps. The O.PROTECT objective addresses this threat by providing TOE self-protection.

T.BRUTE An unauthorized user may attempt to compromise the integrity of the data collected and produced by brute force attacking the authentication mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.

T.DELETE An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The OE.PROTECT objective addresses this threat by providing TOE self-protection. The O.ADMIN objective counters this threat by providing facilities to enable an authorized administrator to delete or purge data. The O.ACCESS objective builds upon the O.IDAUTH objective by only allowing authorized users to access TOE data.

T.ELEVATE An unauthorized user may attempt to gain access to TOE security functions or data for which they do not have access. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ADMIN objective counters this threat by providing facilities to enable an authorized administrator to delete or purge data. The O.ACCESS objective builds upon the O.IDAUTH objective by only allowing authorized users to access TOE data.

T.INTERCPT An attacker or unauthorized user my attempt to intercept data being passed between TOE components. The O.PROTECT objective addresses this threat by providing TOE self-protection. The OE.SSL objective ensures that data being passed between TOE components is protected. The OE.TRUSTED objective ensures that the users of the network from which the TOE will be administered are trusted.

T.MODIFY The integrity of information may be compromised due to unauthorized modification of the TOE data by an attacker. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection. The O.ADMIN objective counters this threat by providing facilities to enable an authorized administrator to modify data. The O.ACCESS objective builds upon the O.IDAUTH objective by only allowing authorized users to access TOE data.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented with the following conventions:

The CC allows for several operations to be performed on security requirements; *assignment*, *refinement*, *selection* and *iteration*. All of these operations is/are used within this ST. These operations are presented in the same manner in which they appear in Part 2 and 3 of the CC with the following exceptions:

A. Changes based upon Interpretations are identified using ***red bolded italicized text***
B. Completed assignment statements are identified using [*italicized text within brackets*]
C. Completed selection statements are identified using *underlined italicized text*
D. Refinements are identified using bold text. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement
E. Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1 (b) Audit Data Generation would be the second iteration.

5.1 TOE Security Functional Requirements

The following table provides a summary of the security functional requirements implemented by the TOE.

TABLE 10 FUNCTIONAL REQUIREMENTS FOR THE TOE MAPPED TO ST OPERATIONS

Functional Component	Description
FAU_GEN.1	Audit Data Generation
FAU_STG.1	Protected Audit Trail Storage
FDP_ACC.1	Access Control Policy
FDP_ACF.1	Access Control Functions
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UAU.2	User Authentication Before Any Action
FIA_UID.2	User Identification Before Any Action
FMT_MOF.1	Management of Security Functions Behavior
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FTA_SSL.3	TSF-Initiated Termination

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) [*User authentication*].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [FAU_GEN.1: Startup and shutdown of the audit functions, FIA_UAU.2:All use of the authentication mechanism)]

5.1.1.2 FAU_STG.1 Protected Audit Trail Storage

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

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

5.1.2 User Data Protection

5.1.2.1 FDP_ACC.1 Access Control Policy

FDP_ACC.1.1 The TSF shall enforce the *Data Access Security Policy* on *authorized users, asset and vulnerability data, viewing*.

5.1.2.2 FDP_ACF.1 Access Control Functions

FDP_ACF.1.1 The TSF shall enforce the *Data Access Security Policy* to objects based on the following:

a) *Subjects: Authorised users*
b) *Objects: asset and vulnerability data in a specific silo*
c) *Subject Security Attributes: Silo Access*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Authorised user is allowed to view asset and vulnerability data in a specific silo if they have Silo Access.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the *no further rules*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *no further rules*.

5.1.3 Identification and Authentication

5.1.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [*4*] unsuccessful authentication attempts occur related to [*user attempting to authenticate to the NSC GUI*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [*disable/ lock the user's account, until the Administrator enables it manually*].

5.1.3.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*see Table 11*]

TABLE 11 USER SECURITY ATTRIBUTES

User Info	Specification
Username	This field is required for user creation.
Full Name	This field is required for user creation.
Password	If not specified user will be prompted to input a new password at next logon
E-mail Address	If not specified, this field is left blank
Role	If not specified, the default role is "User"
Site Access	Defaults to Custom List of Sites
Asset Group Access	Defaults to Custom List of Asset Groups
Superuser	This field is required for user creation [Cloud Edition only]
Default Silo	If not specified, this field is left blank [Cloud Edition only]
Silo	This field is required for user creation [Cloud Edition only]

5.1.3.3 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.

5.1.3.4 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.

5.1.4 Security Management

5.1.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behavior of* the functions of [*user creation and management, NSC management and configuration, NSE management and configuration, diagnostics, and maintenance*] to [*the administrator*].

5.1.4.2 FMT_MTD .1 Management of TSF Data

FMT_MTD.1.1(a) The TSF shall restrict the ability to *modify* the [*TSF data associated with user creation and management, NSC management and configuration, NSE management and configuration, diagnostics, and maintenance*] to [*the administrator*].

FMT_MTD.1.1(b) The TSF shall restrict the ability to *query* the [*TSF data associated with diagnostics and maintenance*] to [*the administrator*].

5.1.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [*user creation and management, NSC management and configuration, NSE management and configuration, diagnostics, and maintenance*].

5.1.4.4 FMT_SMR .1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*administrator, restricted user*].

Note: By default, the TSF maintains an administrator role and four restricted user roles (called Security Manager, Site Administrator, System Administrator, and User). However, a user can receive a custom role that includes any functionality that belongs to any of the restricted roles, but cannot receive administrator functionality unless given the administrator role. Hence, there are effectively two roles—administrator and restricted user.

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

5.1.5 TOE Access

5.1.5.1 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TOE shall terminate an interactive session after a [*configurable time interval of user inactivity with 1 minute being the minimum, and 7 days being the maximum*].

5.2 Security Requirements Rationale

This section maps the security functional requirements to the security objectives of the TOE.

TABLE 12 MAPPING OF FUNCTIONAL REQUIREMENTS TO OBJECTIVES

	O.ACCESS	O.ADMIN	O.AUDITS	O.IDAUTH	O.PROTECT
FAU_GEN.1			X		
FAU_STG.1	X			X	X
FDP_ACC.1	X				
FDP_ACF.1	X				
FIA_AFL.1				X	
FIA_ATD.1				X	
FIA_UAU.2	X			X	
FIA_UID.2	X			X	
FMT_MOF.1	X	X		X	X
FMT_MTD.1	X	X		X	X
FMT_SMF.1	X	X		X	
FMT_SMR.1				X	
FTA_SSL.3					X

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

O.ACCESS The TOE must allow authorized users to access only the TOE functions and data for which they have privileges. The TOE meets this objective by enforcing the following security requirements:

- TOE is required to protect the audit data from deletion [FAU_STG.1].
- Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2].
- The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1].
- Only authorized administrators of the System may query and modify all other TOE data [FMT_MTD.1]
- The TOE is required to be capable of performing the defined security management functions of the TOE [FMT_SMF.1].

O.ADMIN The TOE will provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and will ensure that only authorized administrators are able to access such functionality. The TOE meets this objective by enforcing the following security requirements:

- The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1].
- Only authorized administrators of the System may query and modify all other TOE data [FMT_MTD.1].
- The TOE is required to be capable of performing the defined security management functions of the TOE [FMT_SMF.1].

O.AUDITS The TOE must provide an audit trail of security-related events, with accurate dates and times. The TOE meets this objective by enforcing the following security requirements:

- Security relevant events must be defined and auditable for the TOE [FAU_GEN.1].

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE meets this objective by enforcing the following security requirements:

- The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1].
- The TOE is required to disable a user account subsequent to four consecutive failed login attempts [FIA_AFL.1].
- Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1].
- Users authorized to access the TOE pass an identification and authentication process [FIA_UID.2, FIA_UAU.2].
- The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1].
- Only authorized administrators of the System may query and modify all other TOE data [FMT_MTD.1].
- The TOE is required to be capable of performing the defined security management functions of the TOE [FMT_SMF.1].
- The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE meets this objective by enforcing the following security requirements:

- The TOE is required to protect the audit data from deletion [FAU_STG.1].
- The TOE is required to provide the ability to restrict managing the behavior of modules and functions of the TOE to authorized users of the TOE [FMT_MOF.1].
- Only authorized administrators of the System may query and modify all other TOE data [FMT_MTD.1].
- The TOE is required to logout interactive sessions after remaining inactive for a configurable amount of time which is by default 10 minutes [FTA_SSL.3].

5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 13 lists each requirement from to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

TABLE 13 FUNCTIONAL REQUIREMENTS DEPENDENCIES

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	Yes*
FAU_STG.1	FAU_GEN.1	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FIA_AFL.1	FIA_UAU.1	Yes **
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	Yes ***
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_SMF.1	None	N/A

FMT_SMR.1	FIA_UID.1	Yes ***
FTA_SSL.3	None	N/A

***** Although FPT_STM.1 is not included, the TOE environment security object OE.TIME fulfills this dependency.
****** By including FIA_UAU.2 which is hierarchical to FIA_UAU.1, the dependency of FIA_UAU.1 is satisfied.
******* By including FIA_UID.2 which is hierarchical to FIA_UID.1, the dependency of FIA_UID.1 is satisfied.

5.4 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC 3.1r3 Part 3 and are EAL3 augmented with ALC_FLR.2. Table 14 – Assurance Requirements summarizes the requirements.

TABLE 14 ASSURANCE REQUIREMENTS

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis

5.5 EAL Rationale

EAL3+ was chosen to provide a moderate to high level of independently assured security that is consistent with good practices. The chosen assurance level is appropriate for the threats defined for the environment. Although the TOE might monitor a hostile environment, it is expected that the TOE be placed in a non-hostile position and be protected by other products designed to address threats that correspond to the intended environment.

6 TOE Summary Specification

This section provides a high-level definition of the IT Security Functions provided by the TOE to meet the SFRs specified in this ST.

6.1 TOE Security Functions

6.1.1 Security Audit (FAU)

The TOE has two types of security audit data logs: an audit record of login activities, and the NSC log. These logs are not directly accessible to users of the TOE. No user at any level is able to modify the logs.

The TOE audits login activity and the start up and shutdown of audit functions. No users of the TOE have access to stop the collection of audit logs. The start up and shut down of audit functions corresponds to when the NSC and NSE are powered on and off. The start up and shut down of the NSC are logged in the NSC Log.

While the NSC and NSE logs indicate state changes, the access log indicates user access changes (e.g., updates to the system via NSC GUI). All attempts to authenticate to the TOE via NSC GUI are logged. The audit records generated by the TOE also include a timestamp, the event being logged, the subsystem triggering the log, and the outcome of the event. By default all audit records result from successful operations and unsuccessful operations are ceased and not audited with the exception of login failures.

The provided explanation meets the following functional requirement: FAU_GEN.1.

6.1.1.1 Security Audit Event Storage

Rapid7™ does not provide a mechanism for any TOE User to delete the audit logs directly. Audit logs cannot be modified by any level of user of the TOE. The audit logs are backed up in the hard drive as text files when they reach a certain size, which is 1048576 bytes by default, at which point a new log file is started. The administrator can specify how many log files should be retained before the oldest files are deleted. The default is 10 files.

The provided explanation meets the following functional requirement: FAU_STG.1.

6.1.2 User Data Protection (FDP)

Nexpose multi-tenant functionality enables Nexpose to provide unified vulnerability management as a service to multiple, segregated entities that are known as tenants. Examples include the following:

- the organization's own internal corporate divisions, such as accounting, marketing, and sales
- external, unrelated customer-organizations

Multi-tenant deployments use a silo mechanism to constrain users to the data they are authorized to view. Each silo defines a discrete Nexpose system providing complete Nexpose functionality for separate tenants. A global administrator having the superuser permission is authorized to create and delete silos.

The database schema defines separate database structures for containing the user attributes, log files, and vulnerability and asset data of each silo. Silo profiles specify the functionality available within a silo and the Data Access Security Policy prevents users from accessing data in silos to which they are not logged in.

Each silo's scan data, log data, and silo-specific user attribute data is completely segregated frfom that of other silos and therefore is not accessible within any other silo.

6.1.2.1 Access Control Policy

The Data Access Security Policy uses the *Silo Access* user security attribute to associate users with zero or more silos to which they are authorized access.

An authenticating user may authenticate to any named silo that corresponds to a Silo Access name included in the user's Silo Access attribute list.

6.1.2.2 Access Control Functions

The TOE supports Silo Access using the *Silo Access* user security attribute that binds a user to one or more silos. A user must be logged in to a specific silo to access data within the silo. The Data Access Security Policy defines the rule *Authorised user is allowed to view asset and vulnerability data in a specific silo if they have Silo Access.*

When a user authenticates to a silo, the Data Access Security Policy is applied to users to regulate user access to the silo data and to prevent access to data in other silos. Other user security attributes Site Access and Asset Group Access may restrict users from seeing some data within a silo but these restrictions are separate from, and orthogonal to the Silo Access attribute.

6.1.3 Identification and authentication (FIA)

Access control is implemented via a password authentication method. A typical attacker in the intended environment for the TOE is assumed to have a low level of sophistication, but may have knowledge of vulnerabilities and access to attack methods that are in the public domain.

6.1.3.1 Authentication Failure

An authorized user of the system can authenticate to the TOE via the NSC GUI with a username and password. All the passwords are stored in an obfuscated format.

When a password is entered, it is checked against all valid passwords. In essence, all passwords entered are obfuscated and compared to the previously obfuscated passwords. The User is authenticated if the password entered matches the stored obfuscated password. Otherwise, s/he may retry to login. As a means to mitigate brute force attacks on passwords, users are allowed by default up to four unsuccessful authentication attempts. After four unsuccessful attempts, the account is automatically locked. The system records the time of the fourth unsuccessful attempt and sets a flag in the database to indicate that the account is temporarily locked. Locked accounts must be manually unlocked by the administrator.

To enable or disable a user account, an Administrator with the permission to do so, will click respectively on the following tabs: Administration/Manage users, then select the user account for editing to change the account status.

The provided explanation meets the following functional requirement: FIA_AFL.1.

6.1.3.2 User Attribute Definition

As a good security practice, detailed information about each user of the TOE can be collected when a new account is set up. The database maintains a list of security attributes in the form of individual records that belong to a particular user. These attributes are the user identity, authentication data, and authorizations (roles and access). These attributes can be modified by the administrator from the GUI.

The Username, Full Name, and Password are the only attributes belonging to the user that are required to be provided upon user creation. The provided explanation meets the following functional requirement: FIA_ATD.1.

6.1.3.3 User Authentication and Identification

Authorized users must provide a valid username along with a valid password associated with it for successful authentication. If the username and password are correct, the user is granted the privileges that have been stored in association with that user role. The NSC refers to the user's attributes stored in the database table to grant privileges. The TOE does not provide any services to an unauthenticated user of the NSC GUI, except to request authentication.

In order to start a session with the NSC GUI, the user must open a web browser and initiate a secure session by typing "https://" followed by the IP address of the NSC. The user will not be redirected to "https://" if "http://" is typed. After initiating a secure session, the login page comes up. The user is then prompted to enter a valid username and password before being granted access. User authentication is performed in the database session by making sure that the username and associated password entered exist in the database list of valid usernames and associated passwords. If the user is successfully authenticated; therefore successfully identifies itself, the user is logged into the NSC GUI. Only then are additional functions and types of access made available.

This implies that the TOE does not allow any action to be performed on behalf of the user prior to being successfully authenticated and identified itself. The user is logged into the desired interface only after successfully identifying and authenticating themselves. The TOE ensures that a user can only access the TOE login page before identification. No other functions or types of access are permitted prior to identification and authentication.

The provided explanation meets the following functional requirements: FIA_UAU.2 and FIA_UID.2.

6.1.4 Security Management (FMT)

6.1.4.1 Management of Functions and TSF Data

The TOE allows very granular access permission controls for each user. Access control is implemented via a password authentication method. The administrator specifies Access or No Access rights for each function a TOE user could potentially access. If a user does not have access to the NSC GUI function, the function does not appear in the user's session. The permission-enforcement database of the NSC GUI compares the user access for all incoming requests to the access privileges of the user provided and maintained by the authorization database. For instance, if the user does not have write permission to a function that s/he is trying to modify, the current user's access request is denied.

This applies to the restriction to query or modify the TSF associated with the following functions : user creation and management, NSC management and configuration, NSE management and configuration, diagnostics, and maintenance. It also applies to the restriction to query the TSF associated with: scan data.

The provided explanation meets the following functional requirements: FMT_MOF.1 and FMT_MTD.1

6.1.4.2 System Management Functions

The TOE provides a series of functions that allow the authorized users of the TOE to configure the TOE to perform its services. This includes the following functions: user creation and management, NSC management and configuration, NSE management and configuration, diagnostics, and maintenance.. Access to the TOE and TOE data is controlled by the authentication and access control mechanisms that the TOE provides and implements.

The provided explanation meets the following functional requirement: *FMT_SMF.1*.

6.1.4.3 Role Management

The TOE maintains a list of security attributes in the form of individual records that belong to a particular user; one of these attributes is the user's role. Although there exist a number of default roles with specific

attributes, it is possible to create "custom roles" that combine attributes available to different roles. However, access to administrative functions is granted only to administrators, such that effectively there are only two roles defined on the TOE:

Administrator – Full access to the NSC GUI. This role is able to manage the users of the NSC GUI and to view/modify the configuration of the TOE and the logs.

Restricted user – Access is determined according to the security attributes assigned to the user.

The provided explanation meets the following functional requirement: FMT_SMR.1.

6.1.5 TOE Access (FTA)

By default, a user is automatically logged out of the NSC after 10 minutes of inactivity. Administrators can change that value (minimum value = 60 seconds). When the user is logged out, the last display viewed by the user is cleared making the current contents unreadable. All permissions and accesses that had been granted during the session are removed until the user re-authenticates by logging back into the TOE. When the user is logged out, the GUI clears and overwrites the current display by making the contents unreadable. That is simply achieved by displaying a generic screen and closing the session. As such, any user activity, data access/display device is disabled and the user needs to log back in for another session. In order to re-authenticate, the user must first click on the login tab and enter a valid username and password. Session termination only applies to the NSC GUI.

The provided explanation meets the following functional requirement: FTA_SSL.3.