UNISYS
imagine it. done.

UNISYS Stealth Solution For Networks Security Target

Document Version
Version: 2.7
2011-03-15

Prepared For:

InfoGard Laboratories, Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, Ca 93401

Prepared By:
Gordon McIntosh

Notices:

Table of Contents

Tables

Figures

1 Security Target (ST) Introduction

The structure of this document is defined by CC v3.1r3 Part 1 Annex A.2, “Mandatory contents of an ST”:

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, Protection Profile (PP) and package claims, as well as rationale for these conformance claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	UNISYS Stealth Solution for Networks Security Target
ST Version Number:	Version 2.7
ST Author(s):	Gordon D McIntosh, Mike McAlister
ST Publication Date:	2011-03-15

Keywords: Secure Communications

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation.

TOE Developer	Unisys 2476 Swedesford Road Malvern, PA, 19355-1456
TOE Name:	Unisys Stealth Solution for Networks
TOE Version:	1.4.482

1.3 Target of Evaluation Overview

The TOE, the Unisys Stealth Solution for Networks, is made up of three computer system types, working together in a networked environment. These systems are the Configuration (management) workstation, the Gateway Appliance, and the Client Workstations.

As shown in Figure 1 - TOE Network Topology and Communications Paths, the configuration workstation and the client workstations sit "behind" the gateway on a private network termed the "Parsed Network." All communications within the parsed network is encapsulated in a secure communications protocol termed the Stealth Tunneling Protocol (STP), ensuring that communication is limited to computer systems enabled with STP. All communications to the external network, termed the "Non-parsed Network" must pass through the Gateway Appliance subject to the Gateway Protocol which limits information flow based on pre-established rules. The non-parsed network is the network "in front of" the gateway; communications on the non-parsed network does not use the STP.

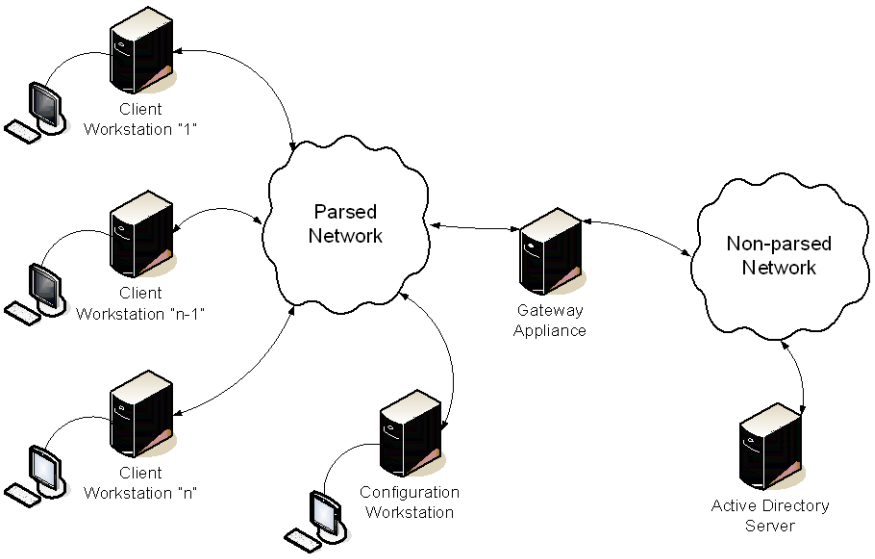

Figure 1 - TOE Network Topology and Communications Paths

1.3.1 TOE Product Type

The TOE is classified as a Multiple Domain Solution product type.

1.3.2 TOE Usage

The intended usage of the TOE is to provide secure communications on a new or existing network (intranet) through the addition of the Unisys Stealth Solution for Networks product; allowing multiple communities of interest (COIs) exchanging information to share the same IT infrastructure, securely and transparently. A COI is a group of users who need to share data among themselves, but cannot permit anyone not in their COI to share their data. Each COI is isolated from all other COIs; and information flow is restricted to users in the same COI.

The TOE provides a gateway to external networks, allowing controlled information flows between devices on the internal secured network and the external network based on pre-established information flow control rules. The gateway hides all devices on the internal secure network from the external network.

The TOE operates at the top of Link Layer (L2) of the OSI network protocol stack, and is transparent to protocols and applications at or above the Network Layer (L3); therefore, no changes are required to the those protocols and applications.

1.3.3 TOE Major Security Features Summary

- Audit services
  - Allow audit administrators to detect, review, and analyze potential security violations.
- Cryptographic services
  - Provides the underlying mechanisms to protect TSF code, TSF data, and user data as it is transmitted within the TOE
- User data protection
  - Provides access control, information flow control, secure user data transmission, and residual data protection mechanisms
- Identification and Authentication
  - Requires non-privileged users to be identified and authenticated before allowing access to information stored on the system, relying on AD as described Section 1.3.4.
- Security Management
  - Provides administrative users the ability to manage the security features provided by the TOE
- Protection of the TSF
  - Provides accurate time reference, and protection of TSF data as it is transmit within the TOE.

1.3.4 TOE IT environment hardware/software/firmware requirement summary

The TOE IT operational environment is to provide support for TOE security functions as follows:

- Active Directory (AD) Server used for authentication, located outside the gateway on the external network: Any version of Microsoft Windows Server at or later than Windows 2003 Server SP2

1.4 Target of Evaluation Description

This section describes the TOE physical and logical boundaries; the physical boundaries describe the TOE hardware, software and the related guidance documentation; the logical boundary describes what logical security features are included in the TOE.

The TOE is comprised of components ordered from Unisys and components specified by Unisys but provided by the customer. The Unisys components are ordered as Part Number “Stealth Solution for Network 1.4.2,” which consists of hardware and software components that are integrated into the customer’s new or existing network, i.e., those components provided by the customer. It should be noted that this part number contains the TOE Version:1.4.482

As a condition of sale, the TOE must be installed and configured by Unisys Field Engineering personnel to ensure the correct deployment of the TOE into the target network.

1.4.1 Target of Evaluation Physical Boundaries

1.4.1.1 TOE Software

The TOE software consists of the components developed by Unisys and components developed by third party software developers, these components are listed separately in Table 1 – Unisys Software and Table 2- Third Party Software Components.

Table 1 – Unisys Software

Description	Version	Developer
Stealth Gateway Software Note: This software is pre-installed at the factory.	1.4.482	Unisys 2476 Swedesford Road Malvern, PA, 19355-1456 http://www.unisys.com/

Stealth Configuration Workstation Software Note: This software is delivered on CD-ROM.	1.4.482	Unisys 2476 Swedesford Road Malvern, PA, 19355-1456 http://www.unisys.com/
Stealth Client Workstation Software Note: This software is generated during installation by the configuration workstation, then installed on the client workstations.	1.4.482	Unisys 2476 Swedesford Road Malvern, PA, 19355-1456 http://www.unisys.com/

Table 2- Third Party Software Components

Description	Version	Developer
Gateway Appliance OS Software Microsoft Windows XP embedded Operating System Notes: This software is pre-installed at the factory. This OS has been previously evaluated, NIAP Evaluation ID 10184 with the following features removed: o Internet Information Services This OS includes the following features not in the previous NIAP Evaluation ID 10184[1] o Microsoft Enhanced RSA Cryptographic Module o Version 5.1.2600.5507 o FIPS Cert #989	5.1 SP3[2]	Microsoft Corporation http://www.microsoft.com
Client Workstation OS Software Microsoft Windows XP Professional Operating System Notes: This OS must be provided by the customer and installed on the Client Workstation prior to installation of the TOE Stealth Client Workstation Software component . Includes the following features not in previous NIAP Evaluation ID 10184[3] o Internet Explorer 8 browser o Hotfixes identified in the configuration guidance o Microsoft Enhanced RSA Cryptographic Module o Version 5.1.2600.5507 o FIPS Cert #989	5.1 SP3[4]	Microsoft Corporation http://www.microsoft.com

[1] Evaluation 10184 applies to SP2 only; the evaluated configuration includes everything that changed from SP2 to SP3.
[2] SP2 with patches to SP3
[3] Evaluation 10184 applies to SP2 only; the evaluated configuration includes everything that changed from SP2 to SP3.
[4] SP2 with patches to SP3

Configuration Workstation OS Software Microsoft Windows XP Professional Operating System Notes: This OS must be provided by the customer and installed on the Configuration Workstation prior to installation of the TOE Stealth Configuration Workstation Software component. Includes the following features not in previous NIAP Evaluation ID 10184[5] ○ Internet Explorer 8 browser ○ Hotfixes identified in the configuration guidance ○ Microsoft Enhanced RSA Cryptographic Module ○ Version 5.1.2600.5507 ○ FIPS Cert #989	5.1 SP3[6]	Microsoft Corporation http://www.microsoft.com
SecureParser® Cryptographic Module • FIPS 140-2 Level 2 Certified, cert #1430 Notes: This software is pre-installed at the factory on the Gateway appliance. This software is installed on the Configuration workstation as part of the Configuration workstation installation This software is installed on the Client Workstation as part of the Client Workstation installation	4.7	Security First Corp. 22362 Gilberto #130 Rancho Santa Margarita, CA 92688 http://www.securityfirstcorp.com/
Apache Tomcat servlet container Notes: This software is pre-installed at the factory on the Gateway appliance.	6.0.18	The Apache Software Foundation http://www.apache.org/
Java Virtual Machine Notes: This software is pre-installed at the factory on the Gateway appliance. This software is installed on the Configuration workstation as part of the Configuration workstation installation	5.0 Update 11	Oracle Corp. http://www.java.com/
.NET Framework 2.0[7] Notes: This software is pre-installed at the factory on the Gateway appliance.	SP1	Microsoft Corporation http://www.microsoft.com
Chilkat Zip 2 Secure EXE [8] Notes: This software is installed on the Configuration workstation as part of the Configuration workstation installation	12.1	Chilkat Software Inc. 1719 E Forest Ave. Wheaton, IL 60187 http://www.chilkatsoft.com

[5] Evaluation 10184 applies to SP2 only; the evaluated configuration includes everything that changed from SP2 to SP3.
[6] SP2 with patches to SP3
[7] .NET is installed in accordance with [6] Section 4.4, “Initial Configuration of Configuration Machine”
[8] Chilkat is installed in accordance with [6] Section 4.5, “Install Stealth Files on Configuration Machine”

1.4.1.2 TOE Hardware

The TOE is made up of three computer system types, working together in a networked environment; in the evaluated configuration it consists of one Gateway appliance, two or more Client Workstation(s), and one Configuration (management) workstation. The configuration workstation and the client workstations sit "behind" the gateway; all communications to or from the client and configuration workstations are encapsulated within a secure communications protocol ensuring that successful communication is limited to only other Stealth-enabled computer systems.

The Gateway appliance is delivered with all necessary firmware and software pre-installed. The Client Workstations are customer provided and may be part of the customer's existing network or components for a new network; the Configuration workstation is customer provided. The Client Workstations and Configuration workstation hardware must be installed with the operating system specified in Table 2, and meet the requirements specified in the Microsoft Windows Security Target section 1.1, under evaluation VID 10184 http://www.niap-ccevs.org/st/vid10184/ with the following restrictions:

- Hardware must support 32-bit OS
- No 64-bit only hardware configurations are supported

The evaluated configuration consists of the following components, however, the number of client workstations allowed in the evaluated configuration is restricted only by the number of Stealth licenses purchased.

- One Gateway appliance, Unisys provided
  - Dell OEM CR100 Server 1U form factor, rack mountable Server
  - Single Intel® Core™ 2 Duo E4300 Processor running at 1.8Ghz, 800 MHz FSB, 2 MB cache.
  - 2 GB RAM.
  - 250 GB SATA hard drive
- Two Client Workstations, customer provided
  - General purpose workstation: must meet hardware requirements specified above
  - Must be configured as specified in TOE guidance (See Section 1.4.1.3)
- One Configuration Workstation, customer provided
  - General purpose workstation: must meet hardware requirements specified above
  - Must be configured as specified in TOE guidance (See Section 1.4.1.3)

1.4.1.3 TOE Guidance Documentation

The TOE guidance documentation delivered is listed in Section 9, "References," within Table 33 - TOE Guidance Documentation.

1.4.2 Target of Evaluation Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE. These security functions were summarized in Section 1.3.3 above and further described in the following subsections. A more detailed description of the implementation of these security functions is provided in Section 7, "TOE Summary Specification."

1.4.2.1 Audit services

The TOE provides audit services that allow audit administrators to detect and analyze security relevant events. The audit trail contains invaluable information that can be used to

- Review security-critical events
- Discover attempts to bypass security mechanisms
- Track usage of privileges by users

The TOE has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated (if known), and other event specific data. Tools are provided so the audit administrator(s) can review audit logs, which are stored and protected in the TOE file system.

1.4.2.2 Cryptographic services

The TOE provides cryptographic mechanisms to protect TSF code and data, including mechanisms to encrypt, decrypt, hash, digitally sign data, and perform cryptographic key agreement.

1.4.2.3 User data protection

The TOE protects user data by enforcing the access control, information flow control and, residual information protection. The TOE uses access control methods to allow or deny access to objects, such as files and directory entries; it uses information flow control methods to control the flow of network traffic and protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

1.4.2.4 Identification and Authentication

The TOE configuration workstation performs local identification and authentication using Windows XP OS mechanisms. It requires each user to be identified and authenticated (using a username and password) prior to performing any functions, maintaining a local database of accounts including their identities, authentication information, group associations, and privilege and logon rights associations.
The TOE client workstation uses Windows XP OS Active Directory mechanism to identify and authenticate users (using a username and password) prior to performing any functions.
The TOE Gateway appliance is “headless” and does not support direct logon; Windows XP OS is configured to allow clients to establish connections to the appliance for audit and security management functions prior to identification and authentication. These connections are then subject to identification and authentication by the server-side programs using username and passwords.
The TOE includes a set of functions that allows management of identification and authentication functions, including the ability to define minimum password length.

1.4.2.5 Security Management

The management of the security critical parameters of the TOE is performed by the authorized administrators. The administrative tasks are separated by roles using commands that require specific privileges for system and audit management; they require users to possess appropriate privileges to execute them. Security parameters that require authorization are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users that are not authorized administrators.

1.4.2.6 Protection of the TSF

While in operation, the TOE depends on the hardware Memory Management Unit (MMU) to provide hardware enforced domain separation for all components addressed by the CPU, e.g., memory and other hardware addressable by the CPU. This provides protection for system firmware residing on the hardware, components such as disk controllers, network interfaces, display devices, as well as system memory. Hardware protection of system memory affords domain separation of the underlying memory resident objects such as kernel code and data, and user processes and data. Additionally, this enables the kernel memory and process management components ensure user processes cannot access kernel storage or storage belonging to other processes.

The TOE depends on the CPU to support two types of hardware components: those directly accessible to user processes (a subset of the CPU registers and memory); and those accessible by kernel (all CPU registers, memory and hardware) that the kernel protects from direct access by user programs.

A user process may execute unprivileged instructions, read or write processor user registers, and read and write to memory and within the bounds defined by the kernel for that user process. Memory accesses are mediated by the MMU, unprivileged instructions and user register usage are not mediated by the kernel. All other types of access to hardware resources by user processes can only be performed by requests (in the form of system calls) to the kernel.

Non-kernel TSF software and data are protected by access control and process isolation mechanisms. In the evaluated configuration, discretionary access control mechanisms prevent non-privileged users from

accessing the files and directories containing TSF configuration data. Other access control mechanisms grant only an authorized administrator the privilege necessary to access programs that access TSF configuration data.

The process isolation mechanism is applied to memory resident programs and data such that non-privileged processes cannot access other process space unless specifically granted access.

The TOE and underlying hardware and firmware are required to be physically protected from unauthorized access.

The TOE provides utilities that allow an administrative user to check the correct operation of the underlying hardware and cryptographic modules.

The combination of the hardware memory protection, memory and process management components, access control mechanisms, and process isolation mechanisms, provide sufficient protections such that the TSF cannot be bypassed, corrupted, or otherwise compromised.

1.5 Roles, User Data, and TSF Data

The TOE supports the following roles:

1. Security administrator:
    a. Privileged system administration except for audit functions
2. Audit administrator
3. Non-privileged user role
    a. Users authorized by the DAC policy to modify the value of object security attributes,
    b. Users authorized to modify their own authentication data, and
    c. Users that create objects

The security and audit administrators may be referred to as authorized administrators as these roles are associated with tasks that require specific authorizations.

User data is any data created by and for the user, which does not affect the operation of the TSF.

TSF data includes the following:

- System configuration information
- Security attributes belonging to individual users
    - unique identifier;
    - group memberships;
    - authentication data;
    - security-relevant roles
- Object security attributes
- Audit data

1.6 Common Criteria Specific Configuration Requirements

- Each user is only allowed to be a member of one COI.
- Only the Security Administrator is allowed logical access to the one (and only) Configuration Workstation.
- Only one Stealth Gateway is allowed per network (which also excludes Appliance Teaming).
- Internet access is not allowed as a network resource.
- Only the Security Administrator has administrative access on the TOE computers.

1.7 Notation, formatting, and conventions

The notation, formatting, and conventions used in this security target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification. Those notes specific to the Stealth portion of the TOE are marked “Stealth Application Note.”

The notation conventions that refer to iterations, assignments, selections, and refinements made in this security target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3.

The notation used in other documents included by reference within this document to indicate iterations, assignments, selections, and refinements of SARs and SFRs is not carried forward into this document.

The CC permits four component operations: assignment, iteration, refinement, and selection to be performed on requirement components. These operations are defined in Common Criteria, Part 1; paragraph 6.4.1.3.2, “Permitted operations on components” as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

Iterations made by the ST author are indicated by a letter following the requirement number, e.g., FIA_UAU.1.1(a); the iterated requirement titles are similarly indicated, e.g., FIA_UAU.1(a).

Assignments made by the ST author are identified with ***bold italics;*** selections are identified with **bold text.**

Refinements made by the ST author are identified with "**Refinement:**" right after the short name; the refined text indicated by underlined text; any refinement that performs a deletion in text is noted in the endnotes sections indicated.

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r3, CC Part 2 extended [8], and CC Part 3 [9].

2.2 Conformance to Protection Profiles

This Security Target does not claim conformance to a protection profile.

2.3 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements package, neither as package-conformant or package-augmented.

This Security Target is Evaluation Assurance Level 4 (EAL 4) augmented.

2.4 Conformance Claims Rationale

This Security Target does not claim conformance to a protection profile, therefore, no rationale is presented.

3 Security Problem Definition

3.1 Threats

The following subsections define the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset.

3.1.1 Threats countered by the TOE

Table 3 - Threats countered by the TOE		
#	Threat	Description
1	T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
2	T.AUDIT_COMPROMISE	A malicious process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker's actions.
3	T.CRYPTO_COMP	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
4	T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE.
5	T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
6	T.OBJECTS_NOT_CLEAN	Users may request access to resources and gain unauthorized access to information because the system may not adequately remove the data from objects between uses by different users, thereby releasing information to the subsequent user.
7	T.SPOOFING	A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain Stealth key material.
8	T.SYSACC	An unauthorized user may gain unauthorized access to the system and act as the administrator or other trusted personnel due to failure of the system to restrict access.
9	T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
10	T.UNAUTH_ACCESS	An unauthorized user may gain access to system data due to failure of the system to restrict access.
11	T.UNAUTH_MODIFICATION	An unauthorized user may cause the modification of the security enforcing functions in the system, and thereby gain unauthorized access to system and user resources due to failure of the system to protect its security enforcing functions
12	T.UNDETECTED_ACTIONS	An unauthorized user may perform unauthorized actions that go undetected because of the failure of the system to record actions.
13	T.UNIDENTIFIED_ACTIONS	Failure of the administrator to identify and act upon unauthorized actions may occur.
14	T.USB_DEVICE	A USB device may unintentionally be plugged into the Gateway appliance resulting in transfer of data to or from the Gateway TOE component.
15	T.USER_CORRUPT	User data may be tampered with by unauthorized users due to failure of the system to enforce the restrictions to data specified by authorized users.

3.1.2 Threats countered by the TOE Operating Environment

Table 4 - Threats countered by the TOE Operating Environment		
#	Threat	Description

Table 4 - Threats countered by the TOE Operating Environment		
#	Threat	Description
1	TE.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
2	TE.SYSACC	An unauthorized user may gain unauthorized access to the system and act as the administrator or other trusted personnel due to failure of the system to restrict access.
3	TE.UNAUTH_ACCESS	An unauthorized user may gain access to system data due to failure of the system to restrict access.

.

3.2 Organizational Security Policies

3.2.1 Organizational Security Policies for the TOE

Table 5 - Organizational Security Policies for the TOE		
#	OSP	Description
1	P.ACCOUNTABILITY	The users of the system shall be held accountable for their actions within the system.
2	P.AUTHORIZATION	The system must have the ability to limit the extent of each user's authorizations.
3	P.AUTHORIZED_USERS	Only those users who have been authorized access to information within the system may access the system.
4	P.NEED_TO_KNOW	The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a "need to know" for that information.
5	P.WARN	The system must have the ability to warn users regarding the unauthorized use of the system.

3.2.2 Organizational Security Policies for the TOE Operational Environment

Table 6 - Organizational Security Policies for the TOE Operating Environment		
#	OSP	Description
1	PE.AUTHORIZED_USERS	Only those users who have been authorized access to information within the system may access the system.

3.3 Assumptions on the TOE Operational Environment

This section describes the assumptions that are made on the operational environment in which the TOE is intended to be used in order to be able to provide security functionality. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following subsections define specific conditions that are assumed to exist in an environment where the TOE is deployed.

3.3.1 Assumptions on Physical Aspects of the Operational Environment:

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

Table 7 - Assumptions on Physical Aspects of the Operational Environment	
Assumption	Description
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification

3.3.2 Assumptions on Personnel Aspects of the Operational Environment

Table 8 - Assumptions on Personnel Aspects of the Operational Environment

Assumption	Description
A.CERT	The Operational Environment provides public/private key pairs for network users and allows export of public keys for use by TOE Administrators in securing Stealth key material for storage and distribution. These certificates are installed as part of the installation process.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.ENDP_INSTALL	Installation of software on the Client Workstations must be accomplished by an authorized administrator possessing the administrative passwords for both the Configuration workstation where the Client Workstation software is generated and the Client Workstation where the software is to be installed
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains; these personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation
A.NOGENPUR	Administrators ensure there are no general purpose computing or storage repository capabilities (e.g. the ability to execute arbitrary code or applications, compilers, web servers, database servers or user applications) available on the Gateway or Configuration workstation platform of the TOE.

3.3.3 Assumptions on Connectivity aspects of the Operational Environment:

Table 9 - Assumptions on Connectivity Aspects of the Operational Environment

Assumption	Description
A.CONNECT	All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
A.NO_BYPASS	It is assumed that no information can flow between the internal and external networks unless it passes through the applicable Stealth Gateway.
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communications links to such systems.

4 Security Objectives

4.1 Security Objectives for the Stealth Portion of the TOE

Table 10 - Security Objectives for the Stealth Portion of the TOE

#	TOE Objective	Description
1	O.AUDIT_PROTECTION	The TSF must provide the capability to protect audit information associated with individual users.
2	O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.
3	O.AUDITING	The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.
4	O.AUTHORIZATION	The TSF must ensure that only authorized users gain access to the TOE and its resources
5	O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-2 validated cryptomodules running a FIPS-approved mode for cryptographic services implementing FIPS-approved security functions and random number generation services used by cryptographic functions. The TSF must ensure that only the users that encrypted data may receive that data decrypted.
6	O.DISCRETIONARY_ACCESS	The TSF must control accessed to resources based on identity of users. The TSF must allow authorized users to specify which resources may be accessed by which users.
7	O.LEGAL_WARNING	The TSF must provide a mechanism to advise users of legal issues involving use of the TOE prior to allowing the user to access resources controlled by the TSF.
8	O.LIMIT_AUTHORIZATION	The TSF must provide the capability to limit the extent of each user's authorizations.
9	O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
10	O.PROTECT	The TSF must protect its own data and resources and must maintain a domain for its own execution that protects it from external interference or tampering.
11	O.PROTECT_IN_TRANSIT	The TSF shall protect user and TSF data when it is in transit from one portion of a distributed TOE to another.
12	O.RESIDUAL_INFORMATION	The TSF must ensure that any information contained in a protected resource is not released when the resource is reused.
13	O.ROBUST_ ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
14	O.SECURE_PATH	The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when passing TSF or user data between distributed parts of the TOE.
15	O.USB_PROTECT	The Gateway component of the TSF shall protect the USB port of the Gateway Hardware device to prevent the transfer of data to or from the Gateway appliance.

4.1.1 Rationale for the Security Objectives for the TOE

4.1.1.1 Mappings of TOE Security Objectives to Threats and OSP

The following table shows the mapping of security objectives for the TOE to threats countered by that objective and/or the OSP enforced by that objective.

Table 11 - Mapping of TOE Security Objectives to Threats and OSP

		Threats																OSP			
#	TOE Objective	T.ADMIN_ERROR	T.AUDIT_COMPROMISE	T.CONFIG_CORRUPT	T.CRYPTO_COMP	T.EAVESDROP	T.MASQUERADE	T.OBJECTS_NOT_CLEAN	T.SPOOFING	T.SYSACC	T.UNATTENDED_SESSION	T.UNAUTH_ACCESS	T.UNAUTH_MODIFICATION	T.UNDETECTED_ACTIONS	T.UNIDENTIFIED_ACTIONS	T.USB_DEVICE	T.USER_CORRUPT	P.ACCOUNTABILITY	P.AUTHORIZATION	P.AUTHORIZED_USERS	P.NEED_TO_KNOW	P.WARN
1	O.AUDIT_PROTECTION		X											X								
2	O.AUDIT_REVIEW													X								
3	O.AUDITING													X				X				
4	O.AUTHORIZATION						X			X	X	X								X		
5	O.CRYPTOGRAPHY				X							X					X					
6	O.DISCRETIONARY_ACCESS																X				X	
7	O.LEGAL_WARNING																					X
8	O.LIMIT_AUTHORIZATION																		X			
9	O.MANAGE	X											X	X				X	X		X	
10	O.PROTECT		X	X								X	X				X					
11	O.PROTECT_IN_TRANSIT					X																
12	O.RESIDUAL_INFORMATION							X													X	
13	O.ROBUST_ ACCESS						X															
14	O.SECURE_PATH								X													
15	O.USB_PROTECT															X						

4.1.1.2 Security Objectives Rationale for Threats and OSP

This section presents the rationale that justifies the security objectives for the TOE is suitable to counter those threats to be countered by the TOE and justifies the security objectives are suitable to enforce the OSP.

O.AUDIT_PROTECTION

This security objective is necessary to counter the threat T.AUDIT_COMPROMISE as it specifies that the TOE will provide a means to protect TOE audit logs stored within the TOE. This objective also counters the threat: T.UNDETECTED_ACTIONS as it protects audit logs and therefore makes them available for review.

O.AUDIT_REVIEW

This security objective is necessary to counter the threat T.UNDETECTED_ACTIONS as it specifies that the TOE provides the capability to selectively view audit information, and alert the administrator of identified potential security violations.

O.AUDITING

This security objective is necessary to counter the threat T.UNDETECTED_ACTIONS and implement the P.ACCOUNTABILITY policy as it specifies that the TOE provides the capability to detect and create records of security-relevant events associated with users.

O.AUTHORIZATION

Ensuring that the TOE and its resources are protected from unauthorized access counters the threats T.UNAUTH_ACCESS and T.SYSACC since the execution of these threats relies upon unauthorized access to the TOE. T.MASQUERADE is also mitigated by this objective because it ensures that only authorized users are allowed access to a resource. Additionally, this objective implements the policy P.AUTHORIZED_USER by ensuring that only authorized users gain access to the TOE and its resources. T.UNATTENDED_SESSION is mitigated by ensuring the TOE does not allow unauthorized access to the TOE and its resources.

O.CRYPTOGRAPHY

This security objective is necessary to counter the threat T.CRYPTO_COMP as it specifies that the TOE uses NIST FIPS 140-2 validated cryptographic services. By ensuring that only users that encrypted data may receive that data decrypted the threat T.USER_CURRUPT and T.UNAUTH_ACCESS are countered because access to decrypted data from a user other than the user that encrypted the data is prevented

O_DISCRETIONARY_ACCESS

By ensuring that authorized users can define which users can access their resources, the threat T.USER_CORRUPT is countered because the TSF enforces the authorized users' restrictions thus preventing users from accessing data not allowed by the user authorized to restrict access to that data. This objective ensures that the TSF enforces the restrictions to resources defined by the authorized users, thereby implementing the policy P.NEED_TO_KNOW

O.LEGAL_WARNING

By ensuring that users are aware of legal issues involving use of the TOE before access to resource is allowed implements the policy P.WARN because it provides the users with a warning of the ramifications of unauthorized use of the TOE.

O.LIMIT_AUTHORIZATION

By providing a capability to limit the extent a user's authorizations, the policy P.AUTHORIZATION is implemented because each user's authorizations can be limited.

O.MANAGE

By ensuring that all the functions and facilities necessary to support the authorized administrator in managing TOE security are provided, support is provided to mitigate T_ADMIN_ERROR, and to implement the P.ACCOUNTABILITY, P.AUTHORIZED_USERS, and P.NEED_TO_KNOW policies because it requires the system to provide functionality to support the management of audit, resource protection, and system access protection. Threats T.UNDETECTED_ACTIONS and T.UNIDENTIFIED_ACTIONS are mitigated by ensuring the TOE offers the necessary management functions for the authorized administrator to securely manage the TOE.

O_PROTECT

By ensuring that the TSF protects itself including its data and resources from external tampering, the threats T.UNAUTH_ACCESS and T.CONFIG_CORRUPT are countered. Additionally, support to counter the threats T.USER_CORRUPT, T.UNAUTH_MODIFICATION and T.AUDIT_COMPROMISE are supported. Ensuring that unauthorized access to the TSF data and resources is prevented disallows the above threats from being executed since they rely upon

unauthorized access to TSF data or the modification of the TSF to a state where the security functions are not enforced thereby ensuring that the TSF is never bypassed.

O.PROTECT_IN_TRANSIT
This security objective is necessary to counter the threat T.EAVESDROP as it specifies that the TOE protects user and TSF data when in transit from one portion of a distributed TOE to another.

O_RESIDUAL_PROTECTION
By ensuring that information in a protected resource is not released when the resource is recycled, the threat T.OBJECTS_NOT_CLEAN is countered because the TSF will always remove data from resources between uses by different users. This objective supports the policy P.NEED_TO_KNOW because it enforces the restrictions on resources defined by authorized users by ensuring that information is not left behind in a resource that may have different restrictions placed upon it.

O.ROBUST_ACCESS This security objective is necessary to counter the threat T. MASQUERADE as it specifies that the TOE will provide mechanisms that control a user's logical access to the TOE.

O.SECURE_PATH
This security objective is necessary to counter the threat T.SPOOFING as it specifies that the TOE provides a means to ensure that users are not communicating with some other entity pretending to be the TOE when passing TSF and user data between distributed parts of the TOE.

O.USB_PROTECT
This security objective is necessary to counter the threat T.USB_DEVICE as it specifies that the Gateway Component of the TSF provides mechanisms that prevent the transfer of data from a USB device to the Gateway appliance through the USB port.

4.2 Security Objectives for the TOE Operational Environmental

Table 12 - Security Objectives for the TOE Operational Environmental	
Objective	Description
OE.ADMINISTRATOR	Authorized administrators are trained as to establishment and maintenance of security policies and practices; are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.AUTHORIZATION	The OE must ensure that only authorized users gain access to the TOE and its resources
OE.CERT	The OE shall supply public/private keys pairs for network users and supports export of public keys for use by TOE Administrators in securing Stealth key material for storage and distribution.
OE.CREDENTIAL	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner which maintains IT security objectives.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives. The authorized administrator installing the Client Workstation use administrative passwords for the Configuration workstation where the client workstation software is generated and the Client Workstation where the software is to be installed.
OE.NO_BYPASS	Information cannot flow among the internal and external networks unless it passes through the Stealth Gateway.
OE.NO_GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications), storage repository capabilities or public data on the Gateway or Configuration workstation platform 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 physical attack which might compromise IT security objectives.
OE.ROBUST_ACCESS	The OE will provide mechanisms that control a user's logical access to the TOE.

4.2.1 Rationale for the Security Objectives for the TOE Operational Environment

4.2.1.1 Mappings of Security Objectives to Threats, OSP, and Assumptions

The following table shows the mapping of security objectives for the TOE operational environment to threats countered by that objective, the OSP enforced by that objective, and/or the assumption upheld by that objective.

Table 13 - Mapping of TOE Operational Environment Security Objectives to Threats, OSP, and Assumptions															
		Threats, OSP, and Assumptions													
#	TOE Objective	A.LOCATE	A.PROTECT	A.CERT	A.COOP	A.ENDP_INSTALL	A.MANAGE	A.NOGENPUR	A.CONNECT	A.NO_BYPASS	A.PEER	TE.MASQUERADE	TE.SYSACC	TE.UNAUTH_ACCESS	PE.AUTHORIZED_USERS
1	OE.ADMINISTRATOR						X								
2	OE.AUTHORIZATION											X	X	X	X
3	OE.CERT			X											
4	OE.CREDENTIAL				X										
5	OE.INSTALL					X	X				X				

Table 13 - Mapping of TOE Operational Environment Security Objectives to Threats, OSP, and Assumptions															
		Threats, OSP, and Assumptions													
#	TOE Objective	A.LOCATE	A.PROTECT	A.CERT	A.COOP	A.ENDP_INSTALL	A.MANAGE	A.NOGENPUR	A.CONNECT	A.NO_BYPASS	A.PEER	TE.MASQUERADE	TE.SYSACC	TE.UNAUTH_ACCESS	PE.AUTHORIZED_USERS
6	OE.NO_BYPASS									X					
7	OE.NO_GENPUR							X							
8	OE.PHYSICAL	X	X						X						
9	OE.ROBUST_ACCESS											X			

4.2.1.2 Security Objectives Rationale for Threats

This section presents the rationale that justifies the security objectives for the TOE operational environment are suitable to counter those threats to be countered by the TOE operational environment.

OE.AUTHORIZATION

The OE provides mechanisms to ensure that the TOE and its resources are protected from unauthorized access; this assists in countering the threats TE.UNAUTH_ACCESS and TE.SYSACC since the execution of these threats relies upon unauthorized access to the TOE. TE.MASQUERADE is also mitigated by this objective because it ensures that only authorized users are allowed access to a resource.

OE.ROBUST_ACCESS

This security objective is necessary to counter the threat TE. MASQUERADE as it specifies that the OE will provide mechanisms that control a user's logical access to the TOE.

4.2.1.3 Security Objectives Rationale for OSP

This section presents the rationale that justifies the security objectives for the TOE operational environment are suitable to enforce the OSP for the TOE operational environment.

OE.AUTHORIZATION

This objective assists in the implementation of the policy PE.AUTHORIZED_USER by ensuring that only authorized users gain access to the TOE and its resources.

4.2.1.4 Security Objectives Rationale for Assumptions

This section presents the rationale that justifies the security objectives for the TOE operational environment are suitable to uphold the assumptions made for the TOE operational environment.

OE.ADMINISTRATOR

By ensuring that authorized administrators are non-hostile, are properly trained, and follow guidance the assumption A.MANAGE is addressed.

OE.CERT

By ensuring the operational environment supplies the proper key pairs for users, the assumption A.CERT is addressed.

OE.CREDENTIAL

By ensuring that access credentials are adequately protected addresses the assumption A.COOP because it ensures that only those users that are authorized are allowed to gain access to the TOE which supports a benign environment and cooperative users.

OE.INSTALL

By ensuring that the TOE is delivered, installed, managed, and operated in a secure manner, the assumptions A. MANAGE and A.PEER are addressed. This objective ensures that the TOE is managed and administered in a secure manner by a competent and security aware individual in accordance with the administrator documentation. By ensuring the installation of the Client Workstation is accomplished by authorized administrator, the assumption A.ENDP_INSTALL is accomplished.

OE.NO_BYPASS

By ensuring no information can flow to or from an external network the assumption A.NO_BYPASS is addressed.

OE.NO_GENPUR

By ensuring no general purpose computing allowed on the Configuration workstation and Gateway appliance, the assumption A.NO_GENPUR is addressed.

OE.PHYSICAL

By ensuring that the responsible individuals ensure that the TOE is protected from physical attack, the assumptions A.LOCATE, A.PROTECT, and A.CONNECT are addressed because the objective ensures that the TOE is protected from unauthorized physical access.

5 Extended Components Definition

This section provides definition of the extended security functional and assurance requirements; the components that are CC Part 2 extended, and CC Part 3 extended, i.e., NIAP interpreted requirements, and explicit requirements.

5.1 Extended Security Function Requirements Definitions

This section defines the extended security functional requirements for the TOE. The security functional requirement components in this security target are CC Part 2 extended.

Table 14 - TOE Security Functional Requirements CC Part 2 Extended				
#	SFR	Description	Dependencies	Hierarchical to
1	FAU_GEN_EXP.1	Audit data generation	FPT_STM.1	None
2	FPT_USB_EXP.1	USB Device Protection	None	None

5.1.1 Class FAU: Security Audit

5.1.1.1 Audit data generation (FAU_GEN_EXP.1)

Family Behavior

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component leveling

FAU_GEN_EXP Security Audit data generation	1

FAU_GEN_EXP.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

Management: FAU_GEN_EXP.1

There are no management activities foreseen.

Audit: FAU_GEN_EXP.1

There are no auditable events foreseen.

5.1.1.1.1 Audit data generation (FAU_GEN_EXP.1)

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXP.1.1 **The TSF shall be able to generate an audit record of the following auditable events: [assignment: *specifically defined auditable events*].**

FAU_GEN_EXP.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, and

b) For each audit event type, [assignment: other audit relevant information]. .

5.1.2 Class FPT: TOE Protection

5.1.2.1 USB Device Protection (FPT_USB_EXP)

Family Behavior

This family provides requirements that address protection of the USB port.

Component leveling

FDP_USB_EXP USB Device Protection	1

FDP_USB_EXP.1 USB Device Protection requires the USB port be protected, not allowing data be transferred to or from the system via the USB device.

Management: FPT_USB_EXP.1

There are no management activities foreseen.

Audit: FPT_USB_EXP.1

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

- Minimal: Triggering of the USB Protection routine described in FPT_USB_EXP.1.1

5.1.2.2 FPT_USB_EXP.1 USB Device Protection

Hierarchical to: None

Dependencies: None

FPT_USB_EXP.1.1 **The TSF shall be able to detect the insertion of [assignment: list of the types of devices] into the USB port and take action to protect all TSF data from access via the USB port of the Gateway appliance.**

FPT_USB_EXP.1.2 **Upon detection of a device specified, the TSF shall take the following actions: [assignment: *specify the action to be taken*].**

5.2 Extended Security Assurance Requirement Definitions

There are no explicit Security Assurance Requirements defined in this Security Target.

5.3 Rationale for Explicitly Stated Security Requirements

This section presents the rationale for the inclusion of the explicit requirements found in this Security Target.

5.3.1 Rationale for Explicitly Stated Security Function Requirements

The following rational is presented for the explicit security function requirements defined in this security target.

FAU_GEN_EXP.1 Audit Generation

This SFR is explicit, as the Stealth TOE does not have the ability to enable or disable the audit function; the requirement to generate audit events for successful events was removed as this is detrimental to performance.

FPT_USB_EXP.1 USB Device Protection

This SFR is explicit as Part II of the Common Criteria does not include an SFR that describes USB port protection. This security function is considered critical in environments where USB port access must be restricted.

5.3.2 Rationale for Explicitly Stated Security Assurance Requirements

There are no explicit security assurance requirements; therefore, no rational is presented.

6 Security requirements

This section describes the security functional and assurance requirements for the TOE; those that are CC Part 2 conformant, CC Part 2 extended, CC Part 3 conformant and CC Part 3 extended.

6.1 TOE Security Functional Requirements: Operating System

The following SFRs are included by reference from the Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target for CC evaluation VID: 10184. They pertain to OS functions relied upon by the Stealth portion of the TOE.

The Microsoft XP Embedded Operating System is installed on the Stealth Gateway appliance; the Microsoft XP Professional Operating System is installed on the Client Workstation and Configuration Workstation. Both were evaluated under NIAP CC evaluation VID 10184.

Table 15 - TOE Security Functional Requirements for Windows Server XP 2003 , VID 10184.

#	SFR	Description
1	FAU_GEN.1[9]	Audit Data Generation
2	FAU_GEN.2	User Identity Association
3	FAU_SAR.1(a)[10]	Audit Review
4	FAU_SAR.2	Restricted Audit Review
5	FAU_SAR.3(a)	Selectable Audit Review by Searching and Sorting
6	FAU_SAR.3(b)	Selectable Audit Review by Searching
7	FAU_SEL.1	Selective Audit
8	FAU_STG.1	Protected Audit Trail Storage
9	FAU_STG.3(a)[11]	Action in Case of Possible Audit Data Loss
10	FAU_STG.4(a)[12]	Prevention of Audit Data Loss
11	FAU_STG.4(b)	Prevention of Audit Data Loss
12	FDP_ACC.2 (a)	Discretionary Access Control Policy
13	FDP_ACF.1 (a)	Discretionary Access Control Functions
14	FDP_RIP.2	Object Residual Information Protection
15	FIA_AFL.1	Authentication Failure Handling
16	FIA_ATD.1(a)[13]	User Attribute Definition
17	FIA_SOS.1(a)[14]	Verification of Secrets
18	FIA_UAU.1	Timing of Authentication
19	FIA_UAU.6	Re-authenticating
20	FIA_UAU.7	Protected Authentication Feedback

[9] Audit generation will cover only those SFRs in this table.
[10] Reference in Windows ST [12] does not include iteration identifier “(a)”
[11] Reference in Windows ST [12] does not include iteration identifier “(a)”
[12] Reference in Windows ST [12] does not include iteration identifier “(a)”
[13] Reference in Windows ST [12] does not include iteration identifier “(a)”
[14] Reference in Windows ST [12] does not include iteration identifier “(a)”

Table 15 - TOE Security Functional Requirements for Windows Server XP 2003 , VID 10184.		
#	SFR	Description
21	FIA_UID.1	Timing of Identification
22	FIA_USB.1_EX	User-Subject Binding
23	FMT_MOF.1(a)	Management of Audit
24	FMT_MOF.1(b)	Management of TOE TSF Data in Transmission
25	FMT_MOF.1(c)	Management of Unlocking Sessions
26	FMT_MSA.1(a)	Management of DAC Object Security Attributes
27	FMT_MSA.3(a)	Static Attribute Initialization
28	FMT_MSA_EX.2	Valid Password Security Attributes
29	FMT_MTD.1(a)	Management of the Audit Trail
30	FMT_MTD.1(b)	Management of Audited Events
31	FMT_MTD.1(c)	Management of User Attributes
32	FMT_MTD.1(d)	Management of Authentication Data
33	FMT_MTD.1(e)	Management of Account Lockout Duration
34	FMT_MTD.1(f)	Management of Minimum Password Length
35	FMT_MTD.1(g)	Management of TSF Time
36	FMT_MTD.1(i)	Management of Advisory Warning Message
37	FMT_MTD.1(j)	Management of Audit Log Size
38	FMT_MTD.1(k)	Management of User Inactivity Threshold
39	FMT_MTD.1(l)	Management of General TSF Data
40	FMT_MTD.1(m)	Management of Reading Authentication TSF Data
41	FMT_MTD.1(n)	Management of Password Complexity Requirement
42	FMT_MTD.1(o)	Management of User Private/Public Key Pair
43	FMT_MTD.2	Management of Unsuccessful Authentication Attempts Threshold
44	FMT_REV.1(a)	Revocation of User Attributes
45	FMT_REV.1(b)	Revocation of Object Attributes
46	FMT_SAE.1	Timed–limited Authorization
47	FMT_SMF.1(a)[15]	Specification of Management Functions
48	FMT_SMR.1(a)[16]	Security Roles
49	FMT_SMR.3	Assuming Roles
50	FPT_STM.1	Reliable Time Stamps
51	FTA_SSL.1	TSF-Initiated Session Locking
52	FTA_SSL.2	User-Initiated Session Locking
53	FTA_TAB.1	Default TOE Access Banners

[15] Reference in Windows ST [12] does not include iteration identifier "(a)"
[16] Reference in Windows ST [12] does not include iteration identifier "(a)"

6.2 TOE Security Functional Requirements: Operating System, Modified

The following SFR(s) are modified from the Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target for CC evaluation VID: 10184. They pertain to OS functions relied upon by the Stealth portion of the TOE.

6.2.1.1.1 FAU_STG.4(b) Prevention of audit data loss: Gateway Appliance

FAU_STG.4.1 (b) The TSF shall ***overwrite the oldest stored audit records*** and ***take no other actions*** if the audit trail is full.

6.3 Security Function Requirements – RSAENH

This section describes the functional requirements for the RSAENH portion of the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, "Conformance Claims."

Table 16 - TOE Security Functional Requirements for RSAENH

#	SFR	Description	Dependencies	Hierarchical to	Operations
54	FCS_CKM.1(a)	Cryptographic key generation: Symmetric keys RSAENH	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	None	A – I
55	FCS_CKM.4(a)	Cryptographic key destruction	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	None	A – I
56	FCS_COP.1(a)	Cryptographic operation: RSA Key Wrapping - RSAENH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I
57	FCS_COP.1(b)	Cryptographic Operation: Random Number Generator - RSAENH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I

6.3.1 Class FCS: Cryptographic support

6.3.1.1 FCS_CKM Cryptographic Key Management

6.3.1.1.1 FCS_CKM.1(a) Cryptographic key generation: Symmetric keys - RSAENH

FCS_CKM.1.1(a) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **none** and specified cryptographic key sizes **256 bits** that meet the following: **random number generator (RNG) as specified in FCS_COP.1(b)**
.

6.3.1.1.2 FCS_CKM.4(a) Cryptographic key destruction - RSAENH

FCS_CKM.4.1(a) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **cryptographic key zeroization method** that meets the following **FIPS 140-2 Level 1**.

6.3.1.2 FCS_COP Cryptographic Operations

6.3.1.2.1 FCS_COP.1(a) Cryptographic operation: RSA Key Wrapping - RSAENH

FCS_COP.1.1(a) The TSF shall perform **Key Wrapping** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits** that

meet the following: **PKCS #1 v2.1: RSA Cryptography Standard as specified in FIPS 140-2 Annex A.**

6.3.1.2.2 FCS_COP.1(b) Cryptographic Operation: Random Number Generator - RSAENH

FCS_COP.1.1(b) The TSF shall perform **Random Number Generation** in accordance with a specified cryptographic algorithm **RNG using SHA-1** and cryptographic key size **none** that meet the following **FIPS-186-2 Appendix 3 as specified in FIPS 140-2 Annex C**.

6.4 Security Function Requirements: SecureParser

This section describes the functional requirements for the SecureParser portion of the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, "Conformance Claims."

Table 17 - TOE Security Functional Requirements for SecureParser

#	SFR	Description	Dependencies	Hierarchical to	Operations
58	FCS_CKM.1(b)	Cryptographic key generation: AES symmetric keys - SecureParser	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	None	A - I
59	FCS_CKM.4(b)	Cryptographic key destruction - SecureParser	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	None	A – I
60	FCS_COP.1(c)	Cryptographic operation: Encryption/decryption- SecureParser	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I
61	FCS_COP.1(d)	Cryptographic operation: Data Authentication - SecureParser	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I
62	FCS_COP.1(e)	Cryptographic operation: AES Key Wrapping - SecureParser	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I
63	FCS_COP.1(f)	Cryptographic Operation: Random Number Generator - SecureParser	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A – I

6.4.1 Class FCS: Cryptographic support

6.4.1.1 FCS_CKM Cryptographic Key Management

6.4.1.1.1 FCS_CKM.1(b) Cryptographic key generation: AES Symmetric keys - SecureParser

FCS_CKM.1.1(b) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **none** and specified cryptographic key sizes **256 bits** that meet the following: **random number generator (RNG) as specified in FCS_COP.1(f)**

6.4.1.1.2 FCS_CKM.4(b) Cryptographic key destruction - SecureParser

FCS_CKM.4.1(b) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **cryptographic key zeroization method** that meets the following **FIPS 140-2 Level 1**.

6.4.1.2 FCS_COP Cryptographic Operations

6.4.1.2.1 FCS_COP.1(c) Cryptographic operation: Encryption/decryption- SecureParser

FCS_COP.1.1(c) The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES CTR** and cryptographic key sizes **256 bits** that meet the following: **FIPS 197 (AES), FIPS 140-2.**

6.4.1.2.2 FCS_COP.1(d) Cryptographic operation: Data Authentication - SecureParser

FCS_COP.1.1(d) The TSF shall perform **data authentication** in accordance with a specified cryptographic algorithm **HMAC SHA1** and cryptographic key sizes **160 bits** that meet the following: **FIPS 140-2, FIPS PUB 180-2 Secure Hash Standard**

6.4.1.2.3 FCS_COP.1(e) Cryptographic operation: AES Key Wrapping - SecureParser

FCS_COP.1.1(e) The TSF shall perform **Key Wrapping** in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **256 bits** that meet the following: **Advanced Encryption Standard (AES) Key Wrap Algorithm RFC 3394**.

6.4.1.2.4 FCS_COP.1(f) Cryptographic Operation: Random Number Generator - SecureParser

FCS_COP.1.1(f) The TSF shall perform **Random Number Generation** in accordance with a specified cryptographic algorithm **RNG using AES** and cryptographic key size **none** that meet the following: **ANSI X9.31 Appendix A.2.4 as specified in FIPS 140-2 Annex C**.

Application Note: *FIPS 140-2 Annex C specifies Approved Random Number Generators. The RNG meets National Institute of Standards and Technology, NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 31, 2005.*

6.5 Security Function Requirements - Stealth

This section describes the functional requirements for the Stealth portion of the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, “Conformance Claims.”

Table 18 - TOE Security Functional Requirements for Stealth

#	SFR	Description	Dependencies	Hierarchical to	Operations
64	FAU_GEN_EXP.1	Audit data generation	FPT_STM.1	None	A
65	FAU_SAR.1(b)	Security audit review: Web GUI	FAU_GEN.1	None	A - I
66	FAU_STG.3(b)	Action in case of possible audit data loss: Gateway Appliance	FAU_STG.1	None	A – I
67	FCS_CKM.2	Cryptographic key distribution	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None	A
68	FDP_ACC.1	Subset access control: Web and Configuration GUI	FDP_ACF.1	None	A
69	FDP_ACF.1(b)	Security attribute based access control: Web and Configuration GUI	FDP_ACC.1 FMT_MSA.3	None	A - I
70	FDP_IFC.2(a)	Complete information flow control: STP	FDP_IFF.1	FDP_IFC.1	A - I
71	FDP_IFC.2(b)	Complete information flow control: Gateway to External Network	FDP_IFF.1	FDP_IFC.1	A - I
72	FDP_IFF.1(a)	Simple security attributes: STP	FDP_IFC.1 FMT_MSA.3	None	A - I
73	FDP_IFF.1(b)	Simple security attributes: Gateway to External Network	FDP_IFC.1 FMT_MSA.3	None	A - I
74	FDP_ITT.1	Basic internal transfer protection	[FDP_ACC.1 or FDP_IFC.1]	None	A - S
75	FIA_ATD.1(b)	User attribute definition: Web GUI	None	None	A – I - R
76	FIA_SOS.1(b)	Verification of secrets: Web and Configuration GUI	None	None	A - I
77	FIA_UAU.2	User authentication: Web and Configuration GUI	FIA_UID.1	FIA_UAU.1	S
78	FIA_UID.2	User identification: Web and Configuration GUI	None	FIA_UID.1	None
79	FMT_MOF.1(d)	Management of security functions behavior: Configuration GUI	FMT_SMR.1 FMT_SMF.1	None	S – A – I
80	FMT_MSA.1(b)	Management of security attributes: Configuration GUI	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	None	A – I
81	FMT_MSA.1(c)	Management of security attributes	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	None	A – I
82	FMT_MSA.2	Secure security attributes: Configuration GUI	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1	None	A

Table 18 - TOE Security Functional Requirements for Stealth					
#	SFR	Description	Dependencies	Hierarchical to	Operations
			FMT_SMR.1		
83	FMT_MSA.3-NIAP-0442	Static attribute initialization: Configuration GUI	FMT_MSA.1 FMT_SMR.1	None	S - A
84	FMT_MTD.1(p)	Management of TSF data: Configuration GUI	FMT_SMR.1 FMT_SMF.1	None	S - A - I - R
85	FMT_MTD.1(q)	Management of TSF data: Web GUI	FMT_SMR.1 FMT_SMF.1	None	S - A - I - R
86	FMT_MTD.1(r)	Management of TSF data: Web GUI	FMT_SMR.1 FMT_SMF.1	None	S - A - I - R
87	FMT_SMF.1(b)	Specification of Management Functions	None	None	A – I
88	FMT_SMR.1(b)	Security roles	FIA_UID.1	None	A - I
89	FPT_ITT.1	Basic internal TSF data transfer protection	None	None	S
90	FPT_USB_EXP.1	USB Device Protection	None	None	A

6.5.1 Class FAU: Security Audit

6.5.1.1 FAU_GEN_EXP Audit data generation

6.5.1.1.1 FAU_GEN_EXP.1 Audit data generation

Management: FAU_GEN_EXP.1

There are no management activities foreseen.

Audit: FAU_GEN_EXP.1

There are no auditable events foreseen.

FAU_GEN_EXP.1.1 The TSF shall be able to generate an audit record of the following auditable events: ***Auditable events as specified in Table 19 - Auditable Events.***

FAU_GEN_EXP.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, and

b) *For each audit event type,* ***details as specified in Table 19 - Auditable Events****.*

Table 19 - Auditable Events			
#	SFR[17]	Audit events prompted by requirement	Additional Information in audit record (FAU_GEN.1.2(b))
54	FCS_CKM.1(a)	Generation of keys - RSAENH	Failure of key generation
58	FCS_CKM.1(b)	Generation of keys - SecureParser	Failure of key generation
67	FCS_CKM.2	Cryptographic key distribution	Failure of the operation
55	FCS_COP.1(a)	Cryptographic Operations	Success/Failure of cryptographic operation

[17] A deletion of CC text was performed on the SFR descriptions in this column to provide clarity and increased readability of the table.

Table 19 - Auditable Events			
#	SFR[17]	Audit events prompted by requirement	Additional Information in audit record (FAU_GEN.1.2(b))
56	FCS_COP.1(b)	Cryptographic Operations	Success/Failure of cryptographic operation
59	FCS_COP.1(c)	Cryptographic Operations	Failure of cryptographic operation
60	FCS_COP.1(d)	Cryptographic Operations	Failure of cryptographic operation
61	FCS_COP.1(e)	Cryptographic Operations	Failure of cryptographic operation
62	FCS_COP.1(f)	Cryptographic Operations	Failure of cryptographic operation
72	FDP_IFF.1(a)	Opening of a tunnel between a client workstation and Gateway appliance to access the external network	Source, Category, Computer ID
73	FDP_IFF.1(b)	Opening of a tunnel between a client workstation and Gateway appliance to access the external network	Source, Category, Computer ID
74	FDP_ITT.1	Opening of a tunnel between a client workstation and Gateway appliance to access the external network	Source, Category, Computer ID
77	FIA_UAU.2	Unsuccessful use of the authentication mechanism for Administration sessions	Date/Time, Type of event
78	FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided for Administration sessions	Date/Time, Type of event, user identity provided
79	FMT_MOF.1(d)	All modifications in the behavior of the functions of the TSF	Date/Time of change, Type of change event
80	FMT_MSA.1(b)	All modifications of the values of security attributes.	Date/Time of change, Type of change event
81	FMT_MSA.1(c)	All modifications of the values of security attributes.	Date/Time of change, Type of change event
87	FMT_SMF.1(b)	Use of the management functions by Administrator personnel	Date/Time of change, Type of change event
88	FMT_SMR.1(b)	Modifications to the group of users that are part of a role	Date/Time of change, Type of change event
89	FPT_ITT.1(c)	Opening of a tunnel between a client workstation and Gateway appliance to access the external network	Source, Category, Computer ID
90	FPT_USB_EXP.1	Activation of USB port protection routine	Date/Time, Type of event

Stealth Application Note: *FAU_GEN_EXP.1 refers to the audit generation of only the Stealth component of the TOE, however, it relies on the OS portion of the TOE to store protect, and manipulate the audit records.*

6.5.1.2 Security audit review (FAU_SAR)

6.5.1.2.1 FAU_SAR.1(b) Security audit review: Web GUI

FAU_SAR.1.1(b) The TSF shall provide the ***Audit Administrator*** with the capability to read ***all audit information specified in FAU_GEN_EXP.1.2, except items 54, 58, 67, 55, 56, 59, 60, 61, and 62*** from the audit records.

FAU_SAR1.2(b) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.5.1.3 Security audit event storage (FAU_STG)

6.5.1.3.1 FAU_STG.3 (b) Action in case of possible audit data loss: Gateway Appliance

FAU_STG.3.1 (b) The TSF shall

Case 1: display a yellow light on the log status indicator to notify the Audit Administrator;

Case 2: display a red light on the log status indicator to notify the Audit Administrator and close all existing non-admin tunnels, and prohibit the creation of any new non-admin tunnels

if the audit trail exceeds

Case 1: 80% of total allocated audit storage space

Case 2: 90% of total allocated audit storage space.

6.5.2 Class FCS: Cryptographic support

6.5.2.1 FCS_CKM Cryptographic Key Management

6.5.2.1.1 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Manual methods and Automated methods** that meets the following:

- **Manual Methods:**
  - **a. The TSF shall support manual distribution of symmetric key in accordance with NIST Special Publication 800-57 "Recommendation for Key Management," Section 8.1.5.2.2.1, "Manual Key Distribution".**
- **Automated method (session keys)**
  - **a. The STP shall automatically distribute symmetric keys in accordance with the NIST AES Key Wrap Specification (November 16, 2001).**[18]

6.5.3 Class FDP: User Data Protection

6.5.3.1 Access Control Policy (FDP_ACC)

6.5.3.1.1 FDP_ACC.1 Subset access control: Web and Configuration GUI

FDP_ACC.1.1 The TSF shall enforce the ***Gateway Access Control Policy*** on

users of administrative interfaces as subjects,

the Web GUI and Configuration GUI as objects,

and the execution of Web and Configuration GUI commands as operations.

6.5.3.2 Access Control Functions (FDP_ACF)

6.5.3.2.1 FDP_ACF.1(b)Security attribute based access control: Web and Configuration GUI

FDP_ACF.1.1(b) The TSF shall enforce the ***Gateway Access Control Policy*** to objects based on the following:

[18] Compliance to the referenced specification is a vendor assertion.

users of administrative interfaces as subjects,

the Web GUI and Configuration GUI as objects, and

the authenticated identity of the subject as security attribute.[19]

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

access is granted to the object if the authenticated identity of the subject is authorized access.

FDP_ACF.1.3(b) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***no additional rules.***

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***no additional rules.***

6.5.3.3 Information flow control policy (FDP_IFC)

6.5.3.3.1 FDP_IFC.2(a) Complete information flow control: STP

FDP_IFC.2.1(a) The TSF shall enforce the ***Stealth Tunneling Protocol (STP)*** on ***processes acting on behalf of authorized users as subjects*** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2(a) The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.5.3.3.2 FDP_IFC.2(b) Complete information flow control: *Gateway to External Network*

FDP_IFC.2.1(b) The TSF shall enforce the ***Gateway Protocol (GP)*** on ***processes acting on behalf of authorized users as subjects*** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2(b) The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.5.3.4 Information flow control flow functions (FDP_IFF)

6.5.3.4.1 FDP_IFF.1(a) Simple security attributes: *STP*

FDP_IFF.1.1(a) The TSF shall enforce the ***Stealth Tunneling Protocol*** based on the following types of subject and information security attributes:

- ***Processes acting on behalf of authorized users as subjects***
- ***Network packets transmit and received as information controlled, and***
- ***The network protocol and data encryption/decryption keys as security attributes.***

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

The data encryption key used to encrypt data on behalf of the source subject is identical to the data decryption key used to decrypt data on

[19] Only users who are members of the Admin COI may access the gateway, membership in the Admin COI is based on identity.

behalf of the destination subject, resulting in the successful decryption of the network packet.

FDP_IFF.1.3(a) The TSF shall enforce the following additional rules: ***None***

FDP_IFF.1.4(a) The TSF shall explicitly authorize an information flow based on the following rules:

- ***The network protocol (transmit or received) is DHCP or ARP***
- ***The network protocol transmit is IGMP.***

FDP_IFF.1.5(a) The TSF shall explicitly deny an information flow based on the following rules:

- ***The network protocol received is IGMP***
- ***The network protocol (transmit or received) is RIP, RIP-2, IGRP, EIGRP, OSPF***

6.5.3.4.2 FDP_IFF.1(b) Simple security attributes: *Gateway to External Network*

FDP_IFF.1.1(b) The TSF shall enforce the ***Gateway Protocol*** based on the following types of subject and information security attributes:

- ***Processes acting on behalf of authorized users as subjects***
- ***Network packets as information controlled, and***
- ***The network protocol, IP address, and port number as security attributes.***

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

The network packet's IP address, protocol, and port number are matched in the (per COI) permit filtering criteria specified by the Security Administrator.

FDP_IFF.1.3(b) The TSF shall enforce the following additional rules: ***None***.

FDP_IFF.1.4(b) The TSF shall explicitly authorize an information flow based on the following rules: ***The network protocol is RIP, RIP-2, IGRP, EIGRP, OSPF, ARP, or DHCP***

FDP_IFF.1.5(b) The TSF shall explicitly deny an information flow based on the following rules: ***The network protocol is IGMP***.

6.5.3.5 Internal TOE transfer (FDP_ITT)

6.5.3.5.1 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the ***Stealth Tunneling Protocol*** to prevent the **disclosure, modification, loss of use** of user data when it is transmitted between physically-separated parts of the TOE.

6.5.4 Class FIA: Identification and Authentication

6.5.4.1 User attribute definition (FIA_ATD)

6.5.4.1.1 FIA_ATD.1(b) User attribute definition: *Web GUI*

FIA_ATD.1.1(b) **Refinement:** The Web GUI shall maintain the following list of security attributes belonging to individual audit Administrators:[20]

- ***Username***
- ***Password***[21]

6.5.4.2 Specification of secrets (FIA_SOS)

6.5.4.2.1 FIA_SOS.1(b) Verification of secrets: Web and Configuration GUI

FIA_SOS.1.1(b) The TSF shall provide a mechanism to verify that secrets meet the following requirements: ***Passwords must be between 8 and 15 characters and have at least one upper and lower case letter, one digit and one special character***.

6.5.4.3 User authentication (FIA_UAU)

6.5.4.3.1 FIA_UAU.2 User authentication: Web and Configuration GUI

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.

6.5.4.4 User Identification (FIA_UID)

6.5.4.4.1 FIA_UID.2 User identification: Web and Configuration GUI

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

6.5.5 Class FMT - Security Management

6.5.5.1 Management of security functions behavior (FMT_MOF)

6.5.5.1.1 FMT_MOF.1(d) Management of security functions behavior: *Configuration GUI*

FMT_MOF.1.1(d) The TSF shall restrict the ability to **determine the behavior of, modify the behavior of** the functions:

- ***that protect TOE Data during transmission between separate parts of the TOE***

to ***the Security Administrator***.

6.5.5.2 Management of security attributes (FMT_MSA)

6.5.5.2.1 FMT_MSA.1(b) Management of security attributes: *Configuration GUI*

FMT_MSA.1.1(b) The TSF shall enforce the ***Gateway Access Control Policy*** to restrict the ability to **create, modify** the security attributes

- ***SecureParser M, SecureParser N, Maximum Queue Depth,***
- ***Audit Administrator Username,***

[20] Security attributes for non-privileged users are maintained within user profiles maintained by the WIN XP OS. Refer to Section 6.1, Table 15 FIA_ATD.1(a).
[21] The password is maintained as a hashed value

- ***Audit and security administrator passwords,***
- ***IP Addresses,***

to ***the Security Administrator***.

6.5.5.2.2 FMT_MSA.1(c) Management of security attributes

FMT_MSA.1.1(c) The TSF shall enforce the ***Gateway Access Control Policy*** to restrict the ability to **query** the security attributes

- ***Audit Administrator Username,***

to ***the Security Administrator***.

6.5.5.2.3 FMT_MSA.2 Secure security attributes: *Configuration GUI*

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for

- ***SecureParser N value, M value, and Max Queue depth***

6.5.5.2.4 FMT_MSA.3-NIAP-0442[22] Static attribute initialization*: Configuration GUI*

FMT_MSA.3.1-NIAP-0442 The TSF shall enforce the ***Stealth Tunneling Protocol*** to provide default values for the following security attributes that are used to enforce the SFP

- ***SecureParser M value,***
- ***SecureParser N value, and***
- ***Max Queue depth***

FMT_MSA.3.2-NIAP-0442 The TSF shall ensure that the default values for the attributes satisfy the following rules

- ***SecureParser M value (2 <= M <= N)***
- ***SecureParser N value (M <= N <= 7)***
- ***Max Queue depth = 3 to 7 inclusive***

FMT_MSA.3.3-NIAP-0442 For each of the following attributes, the TSF shall allow alternative initial values to be specified by the indicated roles to override the default values for these attributes when an object or information is created:

- ***SecureParser N value : Security Administrator***
- ***SecureParser M value : Security Administrator***
- ***Max Queue depth : Security Administrator***

*6.5.5.3*Management of TSF data (FMT_MTD)

6.5.5.3.1 FMT_MTD.1(p) Management of TSF data*: Configuration GUI*

FMT_MTD.1.1(p) **Refinement:** The Configuration GUI shall restrict the ability to **modify** the

- ***User names and passwords***
- ***Time***
- ***Date***
- ***Cryptographic key parameters***
- ***Endpoint Parameters data (Gateway)***
- ***Gateway Configuration data (IP, Parsed Network settings etc)***

[22] As modified by NIAP interpretation I-0482,

- ***Admin/Workgroup Key Assignments (loading) on a Gateway***

to ***the Security Administrator***.

6.5.5.3.2 FMT_MTD.1(q) Management of TSF data: Web GUI

FMT_MTD.1.1(q) **Refinement:** The Web GUI shall restrict the ability to **query** the

- ***Stealth Audit logs Gateway Configuration data (IP, Parsed Network settings etc)***
- ***Admin/Workgroup Key Assignments on a Gateway***
- ***Active Tunnels: Endpoint IP address, Tunnel State, Frames sent, Frames received, Lost frames, Crypto key ID***
- ***Admin, Workgroup keys in use for the specific gateway***

to ***the Audit Administrator***.

6.5.5.3.3 FMT_MTD.1(r) Management of TSF data: *Web GUI*

FMT_MTD.1.1(r) **Refinement:** The Web GUI shall restrict the ability to **delete, query,** and save the

- ***Application Log records, System log records,***

to the ***Audit Administrator***.

6.5.5.4 Specification of Management Functions (FMT_SMF)

6.5.5.4.1 FMT_SMF.1(b) Specification of Management Functions

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

- ***Security Management (Configuration Utility/Keymaker)***
  - ***Configure security attributes listed in FMT_MSA.1(b), (c)***
  - ***Create new Audit Administrator Accounts***
  - ***Generate Admin, Service, Workgroup keys***
  - ***Set Date/Time on Gateway machine***
  - ***Create Workgroup tuples file***
  - ***Configure Gateway/Parsed network settings (i.e.: IP Address)***
  - ***Assign admin, service and workgroup keys to a specific Gateway appliance***
- ***Security Management (Web GUI)***
  - ***View Audit Logs***
  - ***Backup Log Files***
  - ***Download Log Files***
  - ***Delete Log Files***
  - ***Reset selected Tunnel***
  - ***Terminate selected Tunnel***
  - ***Export active Tunnel list***

6.5.5.5 Security management roles (FMT_SMR)

6.5.5.5.1 FMT_SMR.1(b) Security roles

FMT_SMR.1.1(b) The TSF shall maintain the roles

- ***Security Administrator***
- ***Audit Administrator***
- ***Non-privileged user***

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

6.5.6 Class FPT: Protection of the TSF

6.5.6.1 Integrity of exported TSF data (FPT_ITI)

6.5.6.1.1 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.

6.5.6.2 USB Device Protection (FPT_USB_EXP)

6.5.6.2.1 FPT_USB_EXP.1 USB Device Protection: Gateway appliance

FPT_USB_EXP.1.1 The TSF shall be able to detect the insertion of ***any device that identifies itself as a non-network drive***[23] into the USB port and take action to protect all TSF data from access via the USB port.

FPT_USB_EXP.1.2 Upon detection of a device specified, the TSF shall take the following actions:

- ***Force an immediate full restoration to the factory default configuration.***
- ***Force shutdown***

6.6 Security Assurance Requirements for the TOE

This Security Target is Evaluation Assurance Level 4 (EAL 4) augmented as shown in Table 20 – Assurance Requirements below. The security assurance requirements for the TOE consist of the following components that are CC Part 3 conformant and CC Part 3 conformant as summarized in Table 20 below and detailed in the following subsections. These requirements are included by reference.

Table 20 – Assurance Requirements

Assurance Class	Assurance Component	Assurance Components Description
Development	ADV_ARC.1	Security Architectural Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life-cycle Support	ALC_CMC.4	Product support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures

[23] This is a Windows XP designation

	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw Reporting Procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Because this ST includes third party components and components previously evaluated, the Security Assurance Requirements summarized in Table 20are not applied to all SFRs specified in this ST; Table 21 - Assurance Measures Applied by SFR, maps each SFR to the specific assurance measure applied in this evaluation. An 'X' indicates the assurance component has been met in this evaluation, a '-' indicates it has not met in this evaluation.

Table 21 - Assurance Measures Applied by SFR

		Assurance Measures																								
#	SFR	ADV_ARC.1	ADV_FSP.4	ADV_IMP.1	ADV_TDS.3	AGD_OPE.1	AGD_PRE.1	ALC_CMC.4	ALC_CMS.4	ALC_DEL.1	ALC_DVS.1	ALC_FLR.2	ALC_LCD.1	ALC_TAT.1	ASE_CCL.1	ASE_ECD.1	ASE_INT.1	ASE_OBJ.2	ASE_REQ.2	ASE_SPD.1	ASE_TSS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_VAN.3
Windows XP OS SFRs																										
1	FAU_GEN.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
2	FAU_GEN.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
3	FAU_SAR.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
4	FAU_SAR.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
5	FAU_SAR.3(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
6	FAU_SAR.3(b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
7	FAU_SEL.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	-	-	-	-	-
8	FAU_STG.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
9	FAU_STG.3 (a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
10	FAU_STG.4 (a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
11	FAU_STG.4 (b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	-	-	-	-	-
12	FDP_ACC.2 (a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
13	FDP_ACF.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
14	FDP_RIP.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
15	FIA_AFL.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
16	FIA_ATD.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
17	FIA_SOS.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
18	FIA_UAU.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
19	FIA_UAU.6	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
20	FIA_UAU.7	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
21	FIA_UID.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
22	FIA_USB.1_EX	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
23	FMT_MOF.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	-	-	-	-	-
24	FMT_MOF.1(b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	-	-	-	-	-
25	FMT_MOF.1(c)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
26	FMT_MSA.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
27	FMT_MSA.3(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
28	FMT_MSA_EX.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
29	FMT_MTD.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
30	FMT_MTD.1(b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
31	FMT_MTD.1(c)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
32	FMT_MTD.1(d)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
33	FMT_MTD.1(e)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
34	FMT_MTD.1(f)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
35	FMT_MTD.1(g)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
36	FMT_MTD.1(i)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
37	FMT_MTD.1(j)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
38	FMT_MTD.1(k)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
39	FMT_MTD.1(l)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
40	FMT_MTD.1(m)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-

Table 21 - Assurance Measures Applied by SFR																										
		Assurance Measures																								
#	SFR	ADV_ARC.1	ADV_FSP.4	ADV_IMP.1	ADV_TDS.3	AGD_OPE.1	AGD_PRE.1	ALC_CMC.4	ALC_CMS.4	ALC_DEL.1	ALC_DVS.1	ALC_FLR.2	ALC_LCD.1	ALC_TAT.1	ASE_CCL.1	ASE_ECD.1	ASE_INT.1	ASE_OBJ.2	ASE_REQ.2	ASE_SPD.1	ASE_TSS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_VAN.3
41	FMT_MTD.1(n)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
42	FMT_MTD.1(o)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
43	FMT_MTD.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
44	FMT_REV.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
45	FMT_REV.1(b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
46	FMT_SAE.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
47	FMT_SMF.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
48	FMT_SMR.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
49	FMT_SMR.3	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
50	FPT_STM.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
51	FTA_SSL.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
52	FTA_SSL.2	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
53	FTA_TAB.1	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	X	-	-
RSHENH SFRs																										
54	FCS_CKM.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
55	FCS_CKM.4(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
56	FCS_COP.1(a)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
57	FCS_COP.1(b)	-	-	-	-	X	X	-	-	-	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
SecureParser SFRs																										
58	FCS_CKM.1(b)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
59	FCS_CKM.4(b)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
60	FCS_COP.1(c)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
61	FCS_COP.1(d)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
62	FCS_COP.1(e)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
63	FCS_COP.1(f)	-	X	-	-	X	X	X	X	X	-	-	-	-	X	X	X	X	X	X	-	X	-	-	-	-
Stealth SFRs																										
64	FAU_GEN_EXP.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
65	FAU_SAR.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
66	FAU_STG.3(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
67	FCS_CKM.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
68	FDP_ACC.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
69	FDP_ACF.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
70	FDP_IFC.2(a)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
71	FDP_IFC.2(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
72	FDP_IFF.1(a)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
73	FDP_IFF.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
74	FDP_ITT.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
75	FIA_ATD.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
76	FIA_SOS.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
77	FIA_UAU.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
78	FIA_UID.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
79	FMT_MOF.1(d)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
80	FMT_MSA.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
81	FMT_MSA.1(c)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
82	FMT_MSA.2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
83	FMT_MSA.3-NIAP-0442	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
84	FMT_MTD.1(p)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
85	FMT_MTD.1(q)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 21 - Assurance Measures Applied by SFR																									
		Assurance Measures																							
#	SFR	ADV_ARC.1	ADV_FSP.4	ADV_IMP.1	ADV_TDS.3	AGD_OPE.1	AGD_PRE.1	ALC_CMC.4	ALC_CMS.4	ALC_DEL.1	ALC_DVS.1	ALC_FLR.2	ALC_LCD.1	ALC_TAT.1	ASE_CCL.1	ASE_ECD.1	ASE_INT.1	ASE_OBJ.2	ASE_REQ.2	ASE_SPD.1	ASE_TSS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_VAN.3
86	FMT_MTD.1(r)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
87	FMT_SMF.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
88	FMT_SMR.1(b)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
89	FPT_ITT.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
90	FPT_USB_EXP.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

6.7 Security Requirements Rationale

6.7.1 Security Function Requirements Rationale

Table 22 - TOE SFR to Objective Mapping satisfies the requirement to trace each SFR back to the security objectives for the TOE.

Table 22 - TOE SFR to Objective Mapping																
		TOE Objective														
#	SFR	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITING	O.AUTHORIZATION	O.CRYPTOGRAPHY	O.DISCRETIONARY_ACCESS	O.LEGAL_WARNING	O.LIMIT_AUTHORIZATION	O.MANAGE	O.PROTECT	O.PROTECT_IN_TRANSIT	O.RESIDUAL_INFORMATION	O.ROBUST_ACCESS	O.SECURE_PATH	O.USB_PROTECT
1	FAU_GEN.1			X												
2	FAU_GEN.2			X												
3	FAU_SAR.1(a)			X						X						
4	FAU_SAR.2			X												
5	FAU_SAR.3(a)			X						X						
6	FAU_SAR.3(b)			X						X						
7	FAU_SEL.1			X												
8	FAU_STG.1	X		X												
9	FAU_STG.3(a)			X						X						
10	FAU_STG.4(a)	X		X						X						
11	FAU_STG.4(b)	X		X						X						
12	FDP_ACC.2(a)						X									
13	FDP_ACF.1(a)						X									
14	FDP_RIP.2												X			
15	FIA_AFL.1				X											
16	FIA_ATD.1(a)				X		X		X							

Table 22 - TOE SFR to Objective Mapping																
		TOE Objective														
#	SFR	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITING	O.AUTHORIZATION	O.CRYPTOGRAPHY	O.DISCRETIONARY_ACCESS	O.LEGAL_WARNING	O.LIMIT_AUTHORIZATION	O.MANAGE	O.PROTECT	O.PROTECT_IN_TRANSIT	O.RESIDUAL_INFORMATION	O.ROBUST_ACCESS	O.SECURE_PATH	O.USB_PROTECT
17	FIA_SOS.1(a)				X											
18	FIA_UAU.1				X											
19	FIA_UAU.6				X											
20	FIA_UAU.7				X											
21	FIA_UID.1				X											
22	FIA_USB.1_EX			X			X									
23	FMT_MOF.1(a)									X						
24	FMT_MOF.1(b)									X						
25	FMT_MOF.1(c)				X					X						
26	FMT_MSA.1(a)						X			X						
27	FMT_MSA.3(a)						X			X						
28	FMT_MSA_EX.2										X					
29	FMT_MTD.1(a)			X						X						
30	FMT_MTD.1(b)			X						X						
31	FMT_MTD.1(c)								X	X	X					
32	FMT_MTD.1(d)				X					X						
33	FMT_MTD.1(e)				X					X						
34	FMT_MTD.1(f)				X					X						
35	FMT_MTD.1(g)			X						X						
36	FMT_MTD.1(i)							X		X						
37	FMT_MTD.1(j)			X						X						
38	FMT_MTD.1(k)				X											
39	FMT_MTD.1(l)									X						
40	FMT_MTD.1(m)									X	X					
41	FMT_MTD.1(n)									X						
42	FMT_MTD.1(o)									X						
43	FMT_MTD.2				X					X						
44	FMT_REV.1(a)								X	X						
45	FMT_REV.1(b)						X			X						
46	FMT_SAE.1				X					X						
47	FMT_SMF.1(a)									X						
48	FMT_SMR.1(a)								X	X						
49	FMT_SMR.3									X						
50	FPT_STM.1									X						
51	FTA_SSL.1				X											
52	FTA_SSL.2				X											
53	FTA_TAB.1							X								
54	FCS_CKM.1(a)					X										
55	FCS_CKM.4(a)					X										
56	FCS_COP.1(a)					X										
57	FCS_COP.1(b)					X										
58	FCS_CKM.1(b)					X										
59	FCS_CKM.4(b)					X										

Table 22 - TOE SFR to Objective Mapping																
		TOE Objective														
#	SFR	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.AUDITING	O.AUTHORIZATION	O.CRYPTOGRAPHY	O.DISCRETIONARY_ACCESS	O.LEGAL_WARNING	O.LIMIT_AUTHORIZATION	O.MANAGE	O.PROTECT	O.PROTECT_IN_TRANSIT	O.RESIDUAL_INFORMATION	O.ROBUST_ACCESS	O.SECURE_PATH	O.USB_PROTECT
60	FCS_COP.1(c)					X										
61	FCS_COP.1(d)					X										
62	FCS_COP.1(e)					X										
63	FCS_COP.1(f)					X										
64	FAU_GEN_EXP.1			X												
65	FAU_SAR.1(b)		X													
66	FAU_STG.3(b)	X														
67	FCS_CKM.2					X										
68	FDP_ACC.1													X		
69	FDP_ACF.1(b)													X		
70	FDP_IFC.2(a)														X	
71	FDP_IFC.2(b)														X	
72	FDP_IFF.1(a)														X	
73	FDP_IFF.1(b)														X	
74	FDPITT.1											X				
75	FIA_ATD.1(b)				X									X		
76	FIA_SOS.1(b)				X											
77	FIA_UAU.2				X									X		
78	FIA_UID.2				X									X		
79	FMT_MOF.1(d)									X						
80	FMT_MSA.1(b)									X						
81	FMT_MSA.1(c)									X						
82	FMT_MSA.2					X				X						
83	FMT_MSA.3-NIAP-0442									X						
84	FMT_MTD.1(p)									X						
85	FMT_MTD.1(q)									X						
86	FMT_MTD.1(r)									X						
87	FMT_SMF.1 (b)									X						
88	FMT_SMR.1(b)									X						
89	FPT_ITT.1											X			X	
90	FPT_USB_EXP.1															X

6.7.1.1 Security Function Requirements Rationale for the OS

The following paragraphs present the rationale that demonstrate that the SFRs meet all security objectives for the TOE

O.AUTHORIZATION

- FIA_ATD.1(a) and FMT_MTD.1(d) define data to be used for authentication per user and restrict the ability to initialize authentication data to only authorized administrator, and the ability to modify authentication to authorized administrators and authorized users.
- FIA_AFL.1, FMT_MTD.1 (e) and FMT_MTD.2 allow the authorized administrator the ability to set thresholds on the amount of attempts to logon that can be made before a user is locked out and the duration the account locked out.
- FIA_SOS.1(a) defines a metric the authentication mechanism must meet.
- FIA_UAU.1, FIA_UID.1 and FIA_UAU.7 require a user to be identified and authenticated before any other TSF-mediation action on their behalf, with the exception of web server access, is allowed and prevent the user requesting access from receiving insightful authentication feedback during the authentication.
- FIA_UAU.6 requires a user to be authenticated prior to changing their password.
- FTA_SSL.1, FTA_SSL.2, FMT_MOF.1 (c), FMT_MTD.1 (k) allow for the authorized user to define and modify a period of user inactivity before the session is locked and for the authorized user or authorized administrator to unlock a locked session as well as initiate the locking of a session. Unlocking a session by an authorized user requires re-authentication.
- FMT_MTD.1 (f), and FMT_SAE.1 provide the administrator with the ability to define authentication parameters that further restrict the authentication mechanism which provides access to the TOE.
- These requirements together restrict access to the TOE by enforcing authentication and identification of users based on the user accounts including user attributes and limits defined by the authorized administrator.

O.DISCRETIONARY_ACCESS

- FDP_ACC.2(a) and FDP_ACF.1(a) define the discretionary Security Functional Policy (SFP) that identifies the subjects and objects which the policy covers, the security attributes that access to objects is based upon, and the rules of access between subjects and objects. The discretionary SFP allows for the control of access to resources based on the user identity. FIA_ATD.1(a) and FIA_USB.1_EX define the security attributes associated with users that used to enforce the SFPs.
- FMT_MSA.1(a), and FMT_REV.1(b) restrict the ability to modify object security attributes to authorized users, ensures that the default values are known (permissive or restrictive) for the security attributes used to enforce the SFPs, and ensures that only authorized users can revoke the security attributes used to enforce the SFPs.
- These requirements together allow the users the ability to specify, modify, and revoke how objects they are authorized to control can be shared; ensures that the system enforces the sharing specified; and that the security attributes of the users cannot be modified by other than the authorized administrator.
- Each of the above requirements together ensure that access is controlled to resources based on user identity and allow authorized users to specify which resources may be accessed by which users.

O.AUDITING

- FAU_GEN.1, FAU_GEN.2, FIA_USB.1_EX, FPT_STM.1, and FMT_MTD.1(g) define the events that must be auditable and ensures that each event shall identify the user that caused the event and the time the event occurred.
- FAU_SAR.1(a), FAU_SAR.2, FAU_SAR.3(a), FAU_SAR.3(b), FAU_STG.1, FAU_STG.3(a),
- FAU_STG.4 (a), FAU_STG.4 (b), FMT_MTD.1(j), FMT_MTD.1(a), and FMT_MTD.1(b) ensure that the audit trail is complete and that audit events can be selected and reviewed by only the authorized administrator, and that the audit log (system log) can be managed appropriately by the authorized administrator. Additionally, FAU_SEL.1 provides the capability to the authorized administrator to select the events that will be audited based upon specific attributes (pre-selection of audit events).

- Each of the above requirements together ensure the generation of audit records, the adequacy of the content of audit records, and that the audit records are available to and managed by the authorized administrator.

O.AUDIT_ PROTECTION

- FAU_STG.1, FAU_STG.4 (a) and FAU_STG.4 (b), require the TOE to restrict access to the audit trail and to prevent the loss of audit data.
- By restricting access to the audit trail and preventing the loss of audit data the requirements together ensures the protection of audit records.

O.RESIDUAL_INFORMATION

- FDP_RIP.2 requires the TSF to purge residual data associated with objects and subjects prior to reuse.
- Each of the above requirements together ensure that residual data associated with objects and subjects are purged, thereby ensuring that information contained in protected resources does not remain available when the resource is reused.

O.MANAGE

- FAU_SAR.1(a), FAU_SAR.3(a), FAU_SAR.3(b), FAU_STG.3(a), FAU_STG.4 (a), FAU_STG.4 (b), FMT_MTD.1(a), FMT_MTD.1(b), and FMT_MTD.1(j) ensure the authorized administrator can manage audit records.
- FMT_MSA.1(a), FMT_MSA.3(a), FMT_MTD.1(c) and FMT_REV.1(a) ensure the authorized administrator can manage attributes used to enforce the SFPs.
- FMT_MTD.1(d), FMT_MTD.1(e), FMT_MTD.1(f), FMT_MTD.1(i), FMT_MTD.2, FMT_MOF.1(c), and FMT_SAE.1 ensure the authorized administrator can manage authentication related data. FMT_MTD.1(l), FMT_MTD.1(g), FMT_MTD.1(n) restrict the ability to modify TSF data (including the password complexity requirements). FMT_MTD.1(m) prevents all users (including the authorized administrator) from reading passwords. FMT_MTD.1(o) restricts the initialization of the user security attribute private/public key pair to authorized users and the authorized administrator.
- FMT_SMR.1(a), and FMT_SMR.3 ensure the role of the authorized administrator is enforced.
- FMT_SMF.1(a) ensures the authorized administrator is provided the capability to change and maintain security relevant data (e.g. audit policy, account policy, etc).
- FMT_MOF.1(a) and FMT_MOF.1(b) ensure the authorized administrator can manage the audit function and the function to protect TSF data during transmission.
- Together the above requirements ensure that the administrator can manage data (audit records, attributes used to enforce the SFPs, authentication data), manage functions (audit, protection of data in transmission, replication of TSF data), and ensure that the authorized user and administrator roles are enforced.
- Each of the above requirements contributes to and together ensures that the authorized administrator can manage the TOE securely.

O.PROTECT

- FMT_MTD.1(c) ensures that user security attributes which the SFPs are based upon can only be initialized and modified by an authorized administrator. FMT_MSA_EX.2 ensures that only valid password values are accepted by the TOE as security attributes supporting the ability for the TOE to protect itself. FMT_MTD.1(m) protects the TOE authentication data by preventing authentication from being read by any user (including the administrator).
- Together the requirements ensure that the TSF data is protected from modification, protected in transmission, and that the TSF cannot be modified in an unauthorized manner.
- Each of the above requirements contributes to and together ensures that a separate domain is maintained for the TSF and the TSF protects its own data and resources.

O.LEGAL_WARNING

- FTA_TAB.1 requires the TOE to provide the capability of displaying a banner before login.
- FMT_MTD.1(i) restricts the modification of the banner content to an authorized administrator.
- Each of the above requirements together ensure that a banner can be displayed before login containing a warning defined by an authorized administrator to advise users of legal issues involving the misuse of the TOE before access to resources is allowed.

O.LIMIT_AUTHORIZATION

- FMT_SMR.1(a); FIA_ATD.1(a); FMT_MTD.1(c); and FMT_REV.1(a) require the TOE to provide the capability to limit user authorizations by the definition of roles, the user privileges, and the revocation of security-relevant authorizations.
- By ensuring that the security attributes associated with users can only be assigned and revoked by the administrator and that the security attributes allow for specific roles to be enforced, these requirements ensure that the capabilities of users can be limited.
- Each of the above requirements together ensures the capability to limit the extent of each user's authorizations.

6.7.1.2 Security Function Requirements Rationale for Stealth

O.AUDITING

- FAU_GEN_EXP.1specifies that the Stealth TOE generates audit records for security related events.

O.AUTHORIZATION

- FIA_SOS.1(b) defines a metric the authentication mechanism must meet.
- FIA_UAU.2 and FIA_UID.2 require a user to be identified and authenticated before any other TSF-mediation action on their behalf is allowed.
- FIA_ATD.1(b) defines the data to be used for authentication on the Web GUI.

O.MANAGE

- FMT_MOF.1(d) provides that the TOE's management function can only be accessed and utilized (modified) by authorized personnel.
- FMT_MTD.1(p) specifies the TSF data that can be created and modified by use of the TOE's management functions by Security administrators.
- FMT_MTD.1(q) specifies the TSF data that can be queried by use of the TOE's management functions by the Audit administrator role.
- FMT_MTD.1(r) specifies that audit log records can be deleted by the Audit Administrator role.
- FMT_SMR.1(b) defines the roles provided by the Stealth TOE.
- FMT_SMF.1(b) specifies the management functions supported by the Stealth TOE.
- FMT_MSA.1(b), (c) specifies that the TOE enforces the Stealth Tunneling Protocol (STP) to restrict the ability to query, modify, or delete the applicable security attributes to the Security Administrator. FMT_MSA.1(c) specifies security attributes that can be queried, modified or deleted by Security Administrators.
- FMT_MSA.2 specifies that the TSF accepts only secure values for security attributes which support aspects such as the use of cryptography for protection of communication and data transfer during Stealth management console and Endpoint (workgroup) sessions with the Gateway.
- FMT_MSA.3-NIAP-0442 specifies that the TSF enforces restrictive security attributes used to enforce the STP.

O.AUDIT_REVIEW

- FAU_SAR.1(b) specifies that Audit Administrators are given the capability to read audit information from the audit records, and the records are provided in a suitable manner for interpretation.

O.AUDIT_PROTECT

- FAU_STG.3(b) specifies that the TOE (Gateway machine) shall notify the Audit Administrator if the audit trail exceeds the Security Administrator set audit storage allocation.

O.CRYPTOGRAPHY

- FCS_CKM.1(a) specifies that the RSAENH module generate Symmetric cryptographic keys using a PRNG with specified key lengths that adhere to specified standards.
- FCS_CKM.1(b) specifies that the SecureParser module generates Symmetric cryptographic keys using a PRNG with specified key lengths which adhere to specified standards.
- FCS_CKM.4(b) specifies that the SecureParser module provide the capability to destroy Stealth session keys adhering to requirements within FIPS 140-2. FCS_CKM.4(a) specifies that the RSAENH module provides the capability to destroy cryptographic keys adhering to requirements within FIPS 140-2.
- FCS_COP.1(c) specifies that the SecureParser module perform STP encryption/decryption using AES with specified key sizes that conform to specified standards.
- FCS_COP.1(d) specifies that SecureParser module performs Hashing using SHA1 using a FIPS validated cryptographic module.
- FCS_COP.1(e) specifies that the SecureParser module perform key wrapping using AES 256 per the specified standards.
- FCS_COP.1(a) specifies that the RSAENH module perform key wrapping using RSA per the specified standards.
- FCS_COP.1(b) specifies that the RSAENH module employ a PRNG for key generation per the listed standards.
- FCS_COP.1(f) specifies that the SecureParser module employ a PRNG for key generation per the listed standards.
- FMT_MSA.2 specifies that the TSF accept only secure values for security attributes which support aspects such as the use of cryptography for protection of communication and information flow between Stealth Endpoints.
- FCS_CKM.2 specifies that the TSF distribute cryptographic keys using manual and automated methods per the listed standards.

O.PROTECT_IN_TRANSIT

- FPT_ITT.1 specifies that the TOE protect TSF data from disclosure, modification when it is transmitted between Stealth Endpoints.
- FDP_ITT.1 specified user data is protected while transmitted between separate TOE components (Stealth Endpoints).

O.SECURE_PATH

- FPT_ITT.1 specifies that the TOE protect TSF data from disclosure, modification when it is transmitted between Stealth Endpoints.
- FDP_IFC.2(a), FDP_IFF.1(a) specifies that the TOE enforce the STP for information flows between Stealth Client and Configuration workstation Endpoints and Stealth Gateways.
- FDP_IFC.2(b), FDP_IFF.1(b) specifies that the TOE enforce the Gateway Protocol on information flows between the Gateway and external networks.

O.USB_PROTECT

- FPT_USB_EXP.1 specifies that the Gateway component of the TSF protects the USB port of the Gateway Hardware device by overwriting configuration data with factory defaults and rebooting if a block level USB device is placed in the USB port of the Gateway Hardware.

O.ROBUST_ACCESS

- FIA_UAU.2 specifies that the TOE requires successful user authentication prior to granting access to the TSF for (Apache Tomcat) Web GUI Gateway Sessions and Configuration Utility Gateway Sessions.
- FIA_UID.2 specifies that the TOE requires successful user identification prior to granting access to the TSF for (Apache Tomcat) Web GUI Gateway Sessions and Configuration Utility Gateway Sessions.

- FIA_ATD.1(b) specifies that the (Apache Tomcat) TSF maintains the security attributes Username, Password for use in identifying and authenticating Web GUI Gateway sessions and Configuration Utility Gateway sessions
- FDP_ACC.1 and FDP_ACF.1(b) defined the Gateway Access control SFP and specifies that the associated username and password must be provided in order to access security management objects through the Web GUI or Configuration Utility interfaces.

6.7.1.3 Security requirement dependency analysis

Table 23 - SFR Component Dependency Mapping maps the dependencies that exist for each SFR. If the column labeled “satisfied” shows a dependency that has not been resolved, the rationale is provided in the text following the table, why this dependency does not apply for the TOE.

Table 23 - SFR Component Dependency Mapping

#	Component	Dependencies	Satisfied
1	FAU_GEN.1	FPT_STM.1	FPT_STM.1
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
3	FAU_SAR.1(a)	FAU_GEN.1	FAU_GEN.1
4	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1(a)
5	FAU_SAR.3(a)	FAU_SAR.1	FAU_SAR.1(a)
6	FAU_SAR.3(b)	FAU_SAR.1	FAU_SAR.1(a)
7	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1(a-g, i-o)
8	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
9	FAU_STG.3(a)	FAU_STG.1	FAU_STG.1
10	FAU_STG.4 (a)	FAU_STG.1	FAU_STG.1
11	FAU_STG.4 (b)	FAU_STG.1	FAU_STG.1
12	FDP_ACC.2 (a)	FDP_ACF.1	FDP_ACF.1 (a)
13	FDP_ACF.1 (a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 (a) FMT_MSA.3(a)
14	FDP_RIP.2	None	N/A
15	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
16	FIA_ATD.1(a)	None	N/A
17	FIA_SOS.1(a)	None	N/A
18	FIA_UAU.1	FIA_UID.1	FIA_UID.1
19	FIA_UAU.6	None	N/A
20	FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
21	FIA_UID.1	None	N/A
22	FIA_USB.1_EX	FIA_ATD.1	FIA_ATD.1 (a)
23	FMT_MOF.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
24	FMT_MOF.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
25	FMT_MOF.1(c)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
26	FMT_MSA.1(a)	[FDP_ACC.1 FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 (a) - FMT_SMR.1(a) FMT_SMF.1(a)
27	FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1(a)
28	FMT_MSA_EX.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_ACC.2 (a) - FMT_MSA.1(a) FMT_SMR.1(a)
29	FMT_MTD.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
30	FMT_MTD.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
31	FMT_MTD.1(c)	FMT_SMR.1	FMT_SMR.1(a)

Table 23 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied
		FMT_SMF.1	FMT_SMF.1(a)
32	FMT_MTD.1(d)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
33	FMT_MTD.1(e)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
34	FMT_MTD.1(f)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
35	FMT_MTD.1(g)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
36	FMT_MTD.1(i)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
37	FMT_MTD.1(j)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
38	FMT_MTD.1(k)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
39	FMT_MTD.1(l)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
40	FMT_MTD.1(m)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
41	FMT_MTD.1(n)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
42	FMT_MTD.1(o)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(a) FMT_SMF.1(a)
43	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	FMT_SMR.1(a) FMT_SMF.1(a)
44	FMT_REV.1(a)	FMT_SMR.1	FMT_SMR.1(a)
45	FMT_REV.1(b)	FMT_SMR.1	FMT_SMR.1(a)
46	FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1(a) FPT_STM.1
47	FMT_SMF.1(a)	None	N/A
48	FMT_SMR.1(a)	FIA_UID.1	FIA_UID.1
49	FMT_SMR.3	FMT_SMR.1	FMT_SMR.1(a)
50	FPT_STM.1	None	N/A
51	FTA_SSL.1	FIA_UAU.1	FIA_UAU.1
52	FTA_SSL.2	FIA_UAU.1	FIA_UAU.1
53	FTA_TAB.1	None	N/A
54	FCS_CKM.1(a)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1(b) - FCS_CKM.4a
55	FCS_CKM.4(a)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(a) - -
56	FCS_COP.1(a)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not satisfied - - FCS_CKM.4(a)
57	FCS_COP.1(b)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not satisfied - - FCS_CKM.4(a)
58	FCS_CKM.1(b)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1(f) - FCS_CKM.4(b)
59	FCS_CKM.4(b)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(b) - -
60	FCS_COP.1(c)	[FDP_ITC.1 or	FCS_CKM.1(b)

Table 23 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied
		FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	- - FCS_CKM.4(b) [58]
61	FCS_COP.1(d)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not satisfied - - FCS_CKM.4(b) [58]
62	FCS_COP.1(e)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1(b) [57] - - FCS_CKM.4(b) [58]
63	FCS_COP.1(f)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not satisfied - - FCS_CKM.4(b) [58]
64	FAU_GEN_EXP.1	FPT_STM.1	FPT_STM.1 [49]
65	FAU_SAR.1(b)	FAU_GEN.1	FAU_GEN_EXP.1 [63]
66	FAU_STG.3(b)	FAU_STG.1	FAU_STG.1 [8]
67	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1(b) [57] - - FCS_CKM.4(b) [58]
68	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 [69]
69	FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 [68] FMT_MSA.3-NIAP-0442 [83]
70	FDP_IFC.2(a)	FDP_IFF.1	FDP_IFF.1(a) [72]
71	FDP_IFC.2(b)	FDP_IFF.1	FDP_IFF.1(b) [73]
72	FDP_IFF.1(a)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2(a) [70] FMT_MSA.3-NIAP-0442 [83]
73	FDP_IFF.1(b)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2(b) [71] FMT_MSA.3-NIAP-0442 [83]
74	FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.2(a) [70]
75	FIA_ATD.1(b)	None	N/A
76	FIA_SOS.1(b)	None	N/A
77	FIA_UAU.2	FIA_UID.1	FIA_UID.2 [78]
78	FIA_UID.2	None	N/A
79	FMT_MOF.1(d)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
80	FMT_MSA.1(b)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 [68] - FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
81	FMT_MSA.1(c)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 [68] - FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
82	FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_ACC.1 [68] - FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
83	FMT_MSA.3-NIAP-0442	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b), (c) [80, 81] FMT_SMF.1(b) [87]
84	FMT_MTD.1(p)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
85	FMT_MTD.1(q)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]

Table 23 - SFR Component Dependency Mapping			
#	Component	Dependencies	Satisfied
86	FMT_MTD.1(r)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1(b) [88] FMT_SMF.1(b) [87]
87	FMT_SMF.1(b)	None	N/A
88	FMT_SMR.1(b)	FIA_UID.1	FIA_UID.2 [78]
89	FPT_ITT.1	None	N/A
90	FPT_USB_EXP.1	None	N/A

Rationale for unsatisfied dependencies:

- FCS_COP.1(a) – The RSA public/private key pairs used for key wrap are pre-installed on the TOE during the installation process, as covered by assumption A.CERT.
- FCS_COP.1(b) – The RNG algorithm depends on a SHA-1 algorithm, it does not require the import of user data, with or without security attributes, or cryptographic key generation to correctly.
- FCS_COP.1(d) – The SHA-1 is an algorithm that does not require the import of user data, with or without security attributes, or cryptographic key generation to perform correctly.
- FCS_COP.1(f) – The RNG algorithm depends on an AES algorithm, it does not require the import of user data, with or without security attributes, or cryptographic key generation to perform correctly.

6.7.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the Common Criteria EAL4 assurance package augmented with ALC_FLR.2. The Common Criteria allows assurance packages to be augmented, which allows the addition of assurance components from the Common Criteria not already included in the EAL.

Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures and correcting security flaws (ALC_FLR.2). The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL4 augmented) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE

Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 4, EAL 4 is an appropriate level of assurance for the TOE described in this ST. Therefore, EAL4 augmented is an appropriate level of assurance for the TOE.

Table 24 shows the matrix of Security Assurance requirements; the ST assurance levels are shown in **BOLD** text, which clearly demonstrates that this Security Target meets EAL4+.

Table 24 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	**1**	1	1	1
	ADV_FSP	1	2	3	**4**	5	5	6
	ADV_IMP				**1**	1	2	2
	ADV_INT					2	**3**	3
	ADV_SPM						1	1
	ADV_TDS		1	2	**3**	4	5	6
Guidance Documents	AGD_OPE	1	1	1	**1**	1	1	1
	AGD_PRE	1	1	1	**1**	1	1	1
Life-cycle Support	ALC_CMC	1	2	3	**4**	4	5	5
	ALC_CMS	1	2	3	**4**	5	5	5
	ALC_DEL		1	1	**1**	1	1	1
	ALC_DVS			1	**1**	1	2	2
	ALC_FLR							
	ALC_LCD			1	**1**	1	1	2
	ALC_TAT				**1**	2	3	3

Security Target Evaluation	ASE_CCL	1	1	1	**1**	1	1	1
	ASE_ECD	1	1	1	**1**	1	1	1
	ASE_INT	1	1	1	**1**	1	1	1
	ASE_OBJ	1	2	2	**2**	2	2	2
	ASE_REQ	1	2	2	**2**	2	2	2
	ASE_SPD		1	1	**1**	1	1	1
	ASE_TSS	1	1	1	**1**	1	1	1
Tests	ATE_COV		1	2	**2**	2	3	3
	ATE_DPT			1	**2**	3	3	4
	ATE_FUN		1	1	**1**	1	2	2
	ATE_IND	1	2	2	**2**	2	2	3
Vulnerability Assessment	AVA_VAN	1	2	2	**3**	4	5	5

Table 25 - SAR Component Dependency Mapping, maps the dependencies that exist for each SAR to demonstrate all SAR dependencies are satisfied.

Table 25 - SAR Component Dependency Mapping		
Component	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Yes – ADV_FSP.4 Yes – ADV_TDS.3
ADV_FSP.4	ADV_TDS.1	Yes – ADV_TDS.3
ADV_IMP.1	ADV_TDS.3 ALC_TAT.1	Yes – ADV_TDS.3 Yes - ALC_TAT.1
ADV_TDS.3	ADV_FSP.4	Yes - ADV_FSP.4
AGD_OPE.1	ADV_FSP.1	Yes - ADV_FSP.4
AGD_PRE.1	None	--
ALC_CMC.4	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	Yes – ALC_CMS.4 Yes – ALC_DVS.1 Yes - ALC_LCD.1
ALC_CMS.4	None	--
ALC_DEL.1	None	--
ALC_DVS.1	None	--
ALC_FLR.2	None	--
ALC_LCD.1	None	--
ALC_TAT.1	ADV_IMP.1	Yes - ADV_IMP.1
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes – ADV_FSP.4 Yes - ATE_FUN.1
ATE_DPT.1	ADV_ARC.1 ADV_TDS.2 ATE_FUN.1	Yes - ADV_ARC.1 Yes – ADV_TDS.3 Yes - ATE_FUN.1
ATE_FUN.1	ATE_COV.1	Yes - ATE_COV.1
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes – ADV_FSP.4 Yes – AGD_OPE.1 Yes – AGD_PRE.1 Yes – ATE_COV.1 Yes - ATE_FUN.1
AVA_VLA.3	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	Yes - ADV_ARC.1 Yes - ADV_FSP.4 Yes - ADV_TDS.3 Yes – ADV_IMP.1 Yes – AGD_OPE.1 Yes - AGD_PRE.1 Yes – ATE_DPT.2

7 TOE Summary Specification

7.1 Implementation description of TOE SFRs

This section provides evaluators and potential consumers of the TOE with a high-level description of how the developer intends to satisfy each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. This sections refers to SFRs defined in Section 6.1, "TOE Security Functional Requirements: Operating System," Section 6.2, "TOE Security Functional Requirements: Operating System, Modified," Section 6.3, "Security Function Requirements – RSAENH," Section 6.4, "Security Function Requirements: SecureParser," and Section 6.5, "Security Function Requirements - Stealth."

To avoid confusion, those SFRs from Section 6.5, "Security Function Requirements - Stealth," are underlined for clarity.

The following TOE specific terminology is presented to aid in the understanding of the following sections.

- Stealth
  - The Unisys Stealth Solution for Network is the Unisys product marketing nomenclature to indicate the "Stealth" gateway hides all devices on the internal secure network from the external unsecure network.
- Community of Interest (COI)
  - This term is used to define groups that are allowed to communicate with network resources in the unparsed network. This term is independent of what users are members of the COI.
  - A user may be a member of multiple COI; however, a user can only have one COI active at a time.
  - User-to-COI assignments are made by the Security Administrator.
- Gateway
  - A Gateway is an appliance that bridges Stealth-enabled network devices to non-Stealth networks.
- Endpoint
  - An endpoint is a software agent that is installed on all Stealth-enabled clients and servers within the Stealth network, including the Gateway appliance, which supports secure communications through the enforcement of the STP.
- SecureParser®
  - SecureParser® is the cryptographic "Bit-Splitting and Restoring" engine employed by the TOE; this software resides with the Endpoint.

7.2 TOE Security Functions

The TOE consists of the following Security Functions:

- Audit services
- Cryptographic services
- User data protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

7.2.1 Security Audit

The Stealth portion of the TOE generates audit records to provide an audit trail of security relevant actions such as configuration, account management, generation and assignment of cryptographic keys, tunnel establishment between endpoints and data transfer via the parsed network. FAU_GEN_EXP.1

Audit records generated by Stealth software use the underlying Windows XP event logging mechanism; two types of records are generated, application and system. Routine success events such as the construction of a tunnel and events such as the failure of tunnel establishment are reported in a system log; the application log details Gateway settings and application configuration changes.

The XP OS provides the event log mechanism, which is used to record audit records, select which events to record, protect audit records, and provides utilities to review the audit records, including those logged by the OS on the behalf of Stealth. FAU_GEN.1, FAU_GEN.2, FAU_SAR.1(a), FAU_SAR.2, FAU_SAR.3 (a), FAU_SAR.3 (b), FAU_SEL.1

Audit logs maintained on the Gateway appliance are available for review by the Audit Administrator using a browser accessing a Web GUI server on the Gateway appliance. FAU_SAR.1(b) The audit records related to the SFRs listed in Table 26 - Auditable Events, are stored on the configuration workstation. These records must be viewed using the WIN XP tools available. FAU_SAR.1(a), FAU_SAR.2, FAU_SAR.3(a) and FAU_SAR.3(b).

Table 26 - Auditable Events

#	SFR	Audit events prompted by requirement
54	FCS_CKM.1(a)	Generation of keys - RSAENH
58	FCS_CKM.1(b)	Generation of keys - SecureParser
67	FCS_CKM.2	Cryptographic key distribution
55	FCS_COP.1(a)	Cryptographic Operations
56	FCS_COP.1(b)	Cryptographic Operations
59	FCS_COP.1(c)	Cryptographic Operations
60	FCS_COP.1(d)	Cryptographic Operations
61	FCS_COP.1(e)	Cryptographic Operations
62	FCS_COP.1(f)	Cryptographic Operations

The Gateway appliance restricts access to audit records to properly authenticated Audit Administrators using a username/password authentication via the Web GUI interface. Audit records cannot be modified by any user and are stored within the file system of the underlying XP OS. Audit Administrators may download, archive or delete selected audit log records through the Web GUI.

The Gateway appliance protects against audit record loss by alerting the audit administrator via a yellow indicator on the Web GUI interface when the available audit log space is 80% full, additionally the indicator turns red if the log space is 90% full; these settings are hard coded and not configurable. Additionally, when the audit trail storage becomes 90% full, all non-admin STP tunnels are closed, and no new non-admin tunnels are allowed to be created, effectively shutting down Stealth operations. FAU_STG.3(b)

Stealth-generated audit records for client workstations (not the Configuration workstation) are stored on the Gateway appliance; these records are transmit from the client workstation via a Stealth tunnel to the Gateway appliance. The Gateway appliance is factory configured so the underlying XP OS mechanisms overwrite the oldest audit records if the audit trail is full; 100 Mbytes is available for audit record storage. FAU_STG.4(b)

Audit records pertaining to the key management functions done on the Configuration workstation are stored in that workstation's log. All audit records are stored on the XP OS file system and protected by XP OS access control mechanisms. FDP_ACC.2 (a), FDP_ACF.1 (a) The XP OS supports the configuration of a maximum size for stored audit record files and upon reaching that configured limit, produce an alarm to the authorized administrator indicating the configured maximum size has been reached.

FAU_STG.4(a) The authorized administrator on the Gateway appliance is the Audit Administrator; on the Configuration and Client workstations, it is the WIN XP system administrator. FAU_STG.1, FAU_STG.3(a)

7.2.2 Secure Communications

The TOE enforces the Stealth Tunneling Protocol (STP) to secure communications made within the internal network and the Gateway Protocol (GP) to limit communications between the internal and external networks.

Table 27 – Protocol Information Flow Control

Protocol	Stealth Tunneling Protocol	Gateway Protocol
DHCP	always permit	always permit
IGMP (Tx)	always permit	always deny
IGMP (Rx)	always deny	always deny
RIP	always deny	always permit
RIP-2	always deny	always permit
IGRP	always deny	always permit
EIGRP	always deny	always permit
OSPF	always deny	always permit
ARP	always permit	always permit
All other	None	Allow/deny based on COI filters

7.2.2.1 Key Definition and Usage

The TOE uses several types of keys to accomplish its functions, session, COI keys, and wrapping keys. Session and COI keys are 256 bits in length; the length of wrapping keys is dependent on the cryptographic certificate deployed by the end user.

7.2.2.1.1 Session Keys

Symmetric session keys are used to protect each endpoint-to-endpoint tunnel. For each direction of the tunnel (endpoint A to endpoint B, and B to A), there are session keys that control AES-256 encryption/decryption, bit-split/restore, and data integrity operations. These keys are randomly generated at the time of tunnel initiation, and are destroyed when the tunnel is terminated. Each time A and B establish a new tunnel to each other, a new set of session keys is generated.

7.2.2.1.2 COI Keys

COI keys are shared symmetric keys that must be made available to users in their User Profile when they logon. Membership in a COI is defined by having access to that COI's key. COI keys, therefore, are very important, and must be protected while they are being distributed. Key Wrapping keys protect the COI keys while they are being distributed; these are described in Section 7.2.2.1.3 below.
The primary purpose of a COI key is the secure exchange of session keys between Stealth endpoints. To establish a tunnel, endpoints send each other special network packets, INIT protocol data units (PDUs). An INIT PDU contains the session keys applicable to that particular tunnel, allowing the two endpoints to synchronize with each other. To protect those session keys while in flight, the INIT PDU is encrypted (AES Key Wrap) and split using the agreed upon COI key. FCS_CKM.2

While COI keys' explicit function is to protect the exchange of session keys, they have an equally important implicit function, namely the virtualization of the network into COIs. Since an INIT PDU is protected with a COI key, it follows that to restore that PDU the receiving endpoint must possess the same COI key. Therefore, endpoints that do not share a COI key can not communicate with each other. And, since all incoming and outgoing packets are processed by the Stealth endpoint software, endpoints are not visible at the network layer across COIs, or from non-Stealth devices.

There are three types of COI keys: Administrative (Admin) Keys, Service Keys, and Workgroup Keys. The selection of COI keys is determined by the identity of the logged on user. Once the user logs on, the COI keys are available in his user profile.

The first type of COI key that is defined is an Admin Key. The Admin Key allow access to the administrative functions of the gateway. Only workstations whose user has an Admin key as one of his COI keys can access the configuration and monitoring functions of the gateway appliance. Admin keys are only special from the perspective of the gateway. To a workstation, an Admin key is the same as any normal COI key. A gateway, however, recognizes tunnels established with its Admin key and passes traffic through that tunnel to/from the upper layer IP stack of the appliance. Only tunnels established with the Admin key can pass traffic up/down the local Gateway stack; traffic from tunnels established with the Admin key cannot pass traffic to the un-parsed network. This limits access to the administrative functions of the appliance to only those users who are authorized as administrators by virtue of the fact that they are granted an Admin key.

On a Client workstation prior to logon, no user-specific COI keys are defined, so a well-known Service key is used to communicate with a DNS server, a Domain Controller, and an Active Directory for domain authentication.. This Service key is common for all devices which log on through the same set of servers (DNS, DC, AD, etc.). The Service key is provisioned on the device at the time the Stealth endpoint software is installed and is stored in the WIN XP registry. Filters are defined on the gateway appliance to specify what type of traffic (TCP/UDP, port numbers) will be forwarded to/from what non-un-parsed IP addresses.

The most common type of tunnel is established using a normal user workgroup key. Tunnels established with Workgroup keys can pass data between the Stealth and non-Stealth networks, but they may not access the administrative functions of the gateway. Filters may also be defined for Workgroup keys to deny access to configured un-parsed IP addresses or to deny the use of protocols such as TCP or UDP, and specific TCP/UDP ports numbers.

7.2.2.1.3 Key-Wrapping Keys

Because possession of a COI key defines membership in that COI, and those keys are shared among all members of the COI, they must be protected while they are stored or distributed. This is analogous to the common key distribution problem. In effect, an administrator creates a COI key, then distributes it to the user who logs in at an arbitrary workstation. The method of protecting keys for distribution is generally referred to as “key wrapping”.

Key wrapping is accomplished by encrypting the key material, in this case the COI key, with one of a pair of asymmetric encryption keys. Asymmetric key pairs have the property that data encrypted with one of the keys can only be decrypted with the other one, and vice versa. Typically, one of the keys is considered a private key, and one is considered a public key. The private key is kept secret by the owner of the key pair, while the public key is freely distributed.

So, when someone wants to send data that only the owner of the key pair can read, they encrypt, or wrap, the data with the public key. Only the owner of the private key can then decrypt, or unwrap, it. In the case of key wrapping, the key material is the data to be sent or distributed.

For user-based key wrapping, the owner of the key pair is the user who logs on to the workstation, not the workstation itself. Having COI keys that are wrapped with user-specific public keys integrates key management with the enterprises’ identity management systems. So, when an administrator adds a user to a COI, the COI key, which is stored wrapped with the administrator’s public key, is rewrapped for that specific user. The wrapped key is then stored in such a way that when the user logs on to Windows, his profile is populated with the wrapped key. This fully integrates with Microsoft Active Directory environment.

The bottom line is that a user’s role determines what COIs he is a member of, and hence what network resources are available to him.FCS_CKM.2.1

7.2.2.1.4 Tuples file

The mapping of user to a specific COI is accomplished using a tuples file stored in the user's profile. This file is manually distributed to each Client Workstation as described in Section 7.2.2.4. The tuples file contains user-specific configuration, a combination of keys and other data to determine encryption and access privileges used for Stealth sessions.

7.2.2.2 Stealth Tunneling Protocol

The STP is implemented in the Endpoint software as a device driver that modifies the network stack, operating at the top of Link Layer (L2) and below the Network Layer (L3) of the OSI network protocol model. The Endpoint software acts as a filter, intercepting and examining all network packets.

The TOE passes selected network traffic that meet the STP based on the network protocol; i.e., all DHCP network packets are passed through the filter unchanged, all IGMP receive packets are rejected (dropped silently), all IGMP transmit packets are transmitted unchanged, and all other networks packets are treated as follows:

- Packets flowing from L3 to L2 (transmit packets) are encrypted using an AES 256-bit algorithm, split using a cryptographically secure algorithm (cryptographic bit-splitting), appended with a SHA-1 HMAC , then passed to L2 to be transmitted to the destination specified by the destination IP address.
- Conversely, packets flowing from L2 to L3 (receive packets) are authenticated using the SHA-1 HMAC, restored using the inverse of the splitting algorithm (cryptographic bit-restoring), decrypted using an AES 256-bit algorithm, and passed to L3.
- Any packet failing HMAC integrity checking, bit-restoration, or decryption is silently discarded.

The Stealth Tunneling Protocol uses a single key to encrypt, split, and generate the HMAC used to protect and verify the integrity of the information used to establish a tunnel between the two endpoints. This key, referred to as a workgroup key, is shared between endpoints and defines membership in a COI. The information exchanged includes three session keys, which are then used to encrypt, split, and generate the HMAC for the actual data packets. There are a set of three session keys (encryption, splitting, and HMAC) for each direction.

Each user is provisioned with workgroup keys associated with a specific community of interest (COI). Only members of a specified COI possess the same workgroup key and therefore, only members of a specified COI can communicate (encrypt/decrypt data blocks). In the evaluated configuration, a user can be a member of only one COI[24].

Cryptographic bit-splitting is the process of using a key-based information distribution algorithm to split a block of data, by bits, into multiple constituent blocks. Cryptographic bit-restoring is the inverse of splitting such that the constituent data blocks are recombined to produce the original block. During splitting, a network packet from L3 is split into N packets referred to as shares (where N ≥ 2, such that some subset of them (M, where M <= 2) are required to restore the original packet. After splitting into N shares, the shares are signed and sent on to L2 of the network stack for transmission. If N > M, then only M received shares are required to recover all data to fully reconstruct the original packet, therefore, the availability of information is increased as some loss can be tolerated. The constants M & N are based on a security administrator configurable parameter; however, 2 ≤ M ≤ N ≤ 7. If M = 2 and N = 7, any 2 shares received of the 7 transmitted can fully reconstruct the original data stream.

Only members of a specified COI possess the same workgroup key and therefore, only members of a specified COI can communicate (split/restore blocks). FDP_ITT.1, FDP_IFC.2 a; FDP_IFF.1(a)

[24] The Security Administrator is a special case and is a member of two COIs, the Service and Admin.

7.2.2.3 Gateway Protocol

Information flow between the internal and external networks must pass through a Gateway appliance, allowing the TOE to enforce the Gateway Protocol (GP) to limit the flow of information between the internal and external network based on the Layer 4 protocol, IP address, and port numbers (The port numbers only apply to TCP and UDP).

The GP is implemented in the Endpoint software as a device driver that modifies the network stack, operating at the top of Link Layer (L2) and below the Network Layer (L3) of the OSI network protocol model. The GP acts as a filter, intercepting and examining all network packets.

The GP passes network traffic based on the network protocol; i.e., all RIP, RIP-2, IGRP, EIGRP, OSPF, ARP, and DHCP network packets are passed through the filter unchanged, all IGMP packets are rejected, and all other networks packets are passed through a filter that either allows or denies information flow based on security administrator supplied rules. Management of these rules is covered in Section 7.2.5, "Security Management. " FDP_IFC.2 b; FDP_IFF.1(b)

Support from the SecureParser and RSAENH for the underlying cryptographic operations is required for the Stealth portion of the TOE operation. RSAENH is used for generation, wrapping, and unwrapping of COI keys; SecureParser is used for generation, exchange (using COI workgroup keys), key unwrapping, data encryption, HMAC, and usage of session keys. Section 7.2.2.4 details the workflow for these operations. The SFRs required from RSAENH are FCS_CKM.1(a), FCS_CKM.4(a), FCS_COP.1(a), and FCS_COP.1(b); those required from SecureParser are FCS_CKM.1(b), FCS_CKM.4(b), FCS_COP.1(c), FCS_COP.1(d), FCS_COP.1(e), and FCS_COP.1(f).

7.2.2.4 Workgroup COI Key Generation and Distribution Using User Certificates and Profiles

The generation, distribution, and use of Community of Interest (COI) keys, using the User Profile usage model, is described below. Fundamental tenets of the usage model are:

1) Workgroup keys are never stored in clear-text
2) Workgroup keys are never transmitted, either electronically or by hand, in clear-text
3) Workgroup keys are never used or manipulated by Stealth software in clear-text
4) Workgroup keys are stored, transmitted, and used only when "wrapped" (i.e. encrypted) using a public key specific to the user who will logon to the client machine.

Several cryptographic components are required during the workgroup key generation, distribution, and use process:

a) RSAENH Cryptographic Service Provider (CSP) on the Configuration workstation
b) RSAENH CSP on the client workstation
c) SecureParser keystore on the client workstation
d) An X.509 certificate containing an RSA key pair specific to the Administrator who logs onto the Configuration workstation
e) An X.509 certificate containing an RSA key pair specific to the user who logs onto the client workstation
f) An X.509 certificate (derived from the one in e) containing the RSA public key of the user logged onto the client workstation[25]
g) An X.509 certificate, exported by the SecureParser keystore, containing the root RSA public key of the SecureParser keystore

[25] The certificate in f) contains the public key from the certificate in e). There is no mathematical manipulation of the key. It is exported from RSAENH.

h) An X.509 certificate, exported by the Gateway's RSAENH CSP, containing the RSA public key of the Gateway which was created when the Gateway was updated from the factory-default configuration

The numbered items (1-5) below are a high-level sequence of operations. The workflow (pseudo-code) that follows after these bullets details these steps.

The generation and management of user certificates is out of the scope of the Stealth product. Workflow for generation, distribution, and use of a COI key:

1. The Security Administrator is established as the WIN XP system administrator on the Configuration Workstation
2. The Security Administrator creates a COI on the Configuration Workstation
3. The COI is added to the Gateway by the Security Administrator
4. A client user is enrolled in a COI by the Security Administrator
5. The COI key is manually distributed to the client workstation by the Security Administrator
6. The client user logs onto the workstation, making the COI key available for use

One-time Activities (initial configuration):

1. A Security Administrator is established as a WIN XP system administrator
   1.1. The Security Administrator logs onto Administrative workstation;
   1.2. {Admin.Pub, Admin.Priv} certificate is installed in Administrator's Personal Keystore managed by Windows;
2. The Security Administrator creates a COI
   2.1. Security Administrator runs the Key Utility
   2.2. Security Administrator creates a new COI
      2.2.1. RSAENH CSP is called to create a 256-bit AES key, Key
      2.2.2. Key~Admin is exported from RSAENH CSP, wrapped with Administrator's Public key
      2.2.3. Key is deleted from RSAENH
      2.2.4. Key~Admin is stored on the Administrative workstation's disk
   2.3. Security Administrator creates a User Group assigned to COI
3. The COI is added to the Gateway by the Security Administrator
   3.1. Security Administrator adds a Gateway appliance in the Key Utility during initial configuration
   3.2. Security Administrator adds the COI to the Gateway in the Key Utility
   3.3. Security Administrator runs the WrapKeys utility, specifying the Gateway's IP address and "-a"
      3.3.1. Key~Admin is imported into RSAENH
      3.3.2. Key~Gateway is exported from RSAENH using the {Gateway.Pub} certificate which was installed in Admin's Personal certificate store when the Gateway was first configured
      3.3.3. Key is deleted from RSAENH
      3.3.4. Key~Gateway is stored on the Configuration workstation's disk
   3.4. Security Administrator uploads the Key~Gateway to the Gateway using the Config Utility
   3.5. The Gateway makes the Key~Gateway available for use
      3.5.1. Stealth Logon Service running on the Gateway extracts SecureParser's public root key in {SecureParser.Pub}
      3.5.2. Logon Service imports {SecureParser.Pub} into its certificate store
      3.5.3. Key~Gateway is imported into RSAENH keystore
      3.5.4. Key~SecureParser is exported from RSAENH, wrapped with SecureParser.Pub
      3.5.5. Key is deleted from RSAENH
      3.5.6. Key~SecureParser is imported into SecureParser's keystore

One-time Activities (per-client user configuration):

4. A client user is enrolled in a COI
   4.1. Security Administrator installs {User.Pub} in Admin's Personal certificate store
   4.2. Security Administrator runs the WrapKeys utility, specifying "User" and "Group"
      4.2.1. Key~Admin is imported into RSAENH, since it is associated with Group
      4.2.2. Key~User is exported from RSAENH, wrapped in User.pub
      4.2.3. Key is deleted from RSAENH
      4.2.4. Key~User is stored on the Configuration workstation's disk in a folder specific to User in a file named "<COI name>.BLO".
      4.2.5. A tuples file, "WRKGRPTUPLES" is created in the User specific folder with the format: <COI count>{<Default Gateway IP address><BLO file name>}, where there are <COI count> <Default Gateway IP address><BLO file name> tuples.
5. The COI key(s) are manually distributed to each client workstation by the Security Administrator FCS_CKM.2
   5.1. {User.Pub, User.Priv} is installed in User's Personal certificate store on the client workstation
   5.2. The "WRKGRPTUPLES" file and the .BLO file containing the wrapped Key~User is stored in the Windows user profile for User (c:\Documents and Settings\User\Application Data\Unisys\MLS\WGT)

Ongoing activities (use):

6. The client user logs onto the workstation, making the COI key available for use
   6.1. User logs on to client workstation
   6.2. Stealth Logon Service extracts SecureParser's public root key in {SecureParser.Pub} , which was created when the workstation was booted
   6.3. Logon Service imports {SecureParser.Pub} into User's Personal certificate store
   6.4. Key~User is imported into RSAENH keystore
   6.5. Key~SecureParser is exported from RSAENH , wrapped with SecureParser.Pub
   6.6. Key is deleted from RSAENH
   6.7. Key~SecureParser is imported into SecureParser's keystore

7.2.3 Identification and authentication

Identification and authentication by the Configuration and Client workstations is provided using the XP OS "Logon" mechanisms. FIA_UAU.1, FIA_UID.1 On the Configuration workstation, the XP OS is configured to use local authentication; on the Client workstation(s) XP OS is configured to use Active Directory for authentication.

In both cases, the underlying XP OS:

- maintains the user's security attributes FIA_ATD.1(a),
  - COI keys
- handles authentication failures FIA_AFL.1,
- verifies the passwords meet established metrics. FIA_SOS.1(a),
- provides obscured feedback during authentication FIA_UAU.7,
- re-authenticated the user when authentication data is changed. FIA_UAU.6, and
- associates user security attributes with subjects acting on behalf of that user. FIA_USB.1_EX

After authentication, user access to resources is controlled by the access control mechanisms covered in Section 7.2.4. On the Configuration workstation, access is limited to the Security Administrator by the underlying XP OS access control mechanisms. FDP_ACC.2(a), FDP_ACF.1(a) On both the Configuration and Client workstations, access to the Web GUI is by Internet Explorer 8 browser; although access to the browser is available to all users for general use, only users who are members of the Admin COI may access the gateway.

The Gateway appliance is headless, i.e., no user can directly logon via the XP OS; access to the Gateway appliance is limited to the Configuration utility on the Configuration workstation and the Web GUI on any workstation within the Stealth-enabled network. When a user attempts to logon to the Gateway appliance via the client-side Configuration utility, the Gateway configuration server-side utility (running on the Gateway appliance) requires additional identification and authentication. Only users possessing the Security Administrator's credentials, username and password, can successfully logon to the Gateway appliance server-side configuration utility. The server-side configuration utility user authentication relies on the underlying XP OS mechanisms, specifically, the Windows "LogonUser" function to authenticate the username and password on the appliance. This authentication is done locally, and does not use Active Directory. FIA_UAU.1, FIA_UID.1.

When the audit administrator attempts to logon to the Gateway appliance using the Web GUI, identification and authentication is required by the Tomcat servlet container based upon user identification and password. FIA_UAU.2, and FIA_UID.2.

The quality of passwords, for both the server-side configuration utility and server-side Web GUI, are enforced by the client-side configuration utility. FIA_SOS.1(b) At initial system startup, the default configuration utility password is required to be changed by the security administrator. The metrics used for the initial password and all subsequent password changes relies on the configuration utility. Similarly, when the audit administrators' passwords are created or subsequently changed through the configuration utility, the configuration utility verifies that the passwords meet the same criteria. When an audit administrator attempts a logon via the Web GUI, the Tomcat servlet container authenticates using the username/password pair created by the configuration utility. The sequence is:

- A Web GUI account is added using the configuration utility after verifying the password against the password pattern defined in the configuration utility, with the password stored as a SHA-256 hash.
- A configuration utility "Save" operation generates an updated tomcat-users.xml file containing username/hashed password pair(s), and restarts the Tomcat daemon.
- Tomcat picks up the Web GUI account information from the tomcat-users.xml file on restart.

After the configuration utility updates the tomcat-users.xml file the Web GUI security attributes, username and hashed password, are maintained by Tomcat. FIA_ATD.1(b),

The TOE does not allow any access to the Internet Explorer 8 browser (to access the Web GUI) or the configuration workstation's client-side configuration utility prior to successful identification and authentication by the underlying XP OS mechanisms, i.e., a user must have successfully logged on to either the Client Workstation or the Configuration workstation. FIA_UID.1.2, FIA_UAU1.2

The server-side interfaces, Tomcat and the configuration utility, require that the XP OS allow access prior to identification and authentication; both the Tomcat servlet container and the server-side configuration utility provide these identification and authentication internally. FIA_UID.1.1, FIA_UAU.1.1

The Configuration Utility requires access to the Gateway for management, and provides for identification and authentication.

The underlying XP OS allows access by the Web GUI to the Tomcat servlet container and by the client-side Configuration utility to the server-side Configuration utility prior to identification and authentication of a user.

7.2.4 User Data Protection

TOE user data protection provides access control for the WEB GUI and Configuration utility administrative interfaces through enforcement of the Gateway Access Control Policy (GACP) mechanism. Only users who are members of the Admin COI may access the gateway. The procedure to obtain membership in the Admin COI is described in Section 7.2.2.4. FDP_ACC.1, FDP_ACF.1(b)

Access to the client-side configuration utility is controlled by the access permissions enforced by the underlying XP OS access control mechanisms. Only an authenticated security administrator has access to execute the client-side configuration utility; this is controlled by the file access permissions in the underlying XP OS file system. Additionally, the security administrator must be a member of the Windows Administrators Group FDP_ACC.2 (a), and FDP_ACF.1 (a)

The Stealth portion of the TOE relies on underlying XP OS mechanisms for residual information protection; this requires reusable objects containing user data be zeroized before they can be reused by a different process. This ensures that all memory allocated and used by Stealth processes is cleared before allocation to another process. FDP_RIP.2.

7.2.5 Security Management

The Stealth TOE supports three operational roles: security administrator, audit administrator and user. The security and audit administrators are authorized administrators; the security administrator is the privileged system administration except for audit functions, the audit administrator has privilege to access all audit functions as well as view other security attributes. A user is a non-privileged entity that is authorized by the DAC policy to modify the value of object security attributes he owns, authorized to modify their own authentication data, and create objects. FMT_SMR.1(b)
The Security Administrator and user roles map directly to the roles defined by the underlying XP OS mechanisms. FMT_SMR.1(a)

The Stealth TOE provides three management interfaces, the Configuration Utility (GUI), the Web GUI, and a key management application.

7.2.5.1 Configuration Utility (GUI)

The TOE provides a Configuration GUI security management interface on the Configuration Workstation that allows Security Administrators to perform detailed Gateway management. The Configuration GUI is a client/server program; the client executing on the Configuration workstation, the server executing on the Gateway appliance. The underlying XP OS access control mechanisms limit access to the Configuration GUI client to the Security Administrator. When the security administrator executes the client side program, a login screen is presented that requires the security administrator identify and authenticate to the server.

During the first login after installation, the Configuration GUI require the password be changed from the factory default; both the Web GUI and Configuration GUI passwords are subject to following metrics:

- Passwords must be between 8 and 15 characters and
- have at least one upper and lower case letter, one digit and one special character for the following set: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /.

Upon successful authentication, the authorized administrator may access the utilities to manage the Stealth TOE. FIA_UAU.2, FIA_UID.2, FDP_ACC.1, FDP_ACF.1(b), FIA_SOS.1(b),

The TSF restricts the ability to modify the behavior of the secure tunnels that allow the secure transmission of TOE data between the Gateway, Configuration workstation and the client workstations to the Security Administrator; i.e., only users possessing the security administrator's credentials can access the utilities via the Configuration GUI. FMT_MOF.1(d)

The Configuration GUI allows the Security Administrator to configure and manage the Gateway appliance settings, create and modify Audit Administrator accounts, create and modify tunnel/packet splitting parameters, loading cryptographic keys on the Gateway appliance and configure network addresses. FMT_MTD.1(p),

The Configuration GUI supports:

- The configuration of Gateway appliance name and internal network IP addresses.
- The configuration of Endpoint parameters used for establishing secure sessions between endpoints, allowing configuration of the SecureParser "N" parameter (total shares generated),

SecureParser “M” parameter (min. for reassembly), and Max queue depth. The constants M & N are based on a security administrator configurable parameter; however they are constrained such that , 2 ≤ M ≤ N ≤ 7. FMT_MOF.1(d), FMT_MSA.1(b), FMT_MSA.2, FMT_MSA.3-NIAP-0442

- The loading of Workgroup keys to the particular client Endpoint as described in Section 7.2.2.4, “Workgroup COI Key Generation and Distribution Using User Certificates and Profiles”**.** The Service Key is stored in the client endpoint workstation’s XP OS registry.
- Adding new Audit administrator accounts. This interface also allows the configuration of initial password credentials for newly created Audit administrators.
- Query the Audit administrator username FMT_MSA.1(c)

Installation packages for Client workstations are generated through the Configuration GUI during the installation and provisioning process. The installation package consists of an installation file, registry entries and an installation batch file. The utility uses the Chilkat Zip Self-Extractor to build the installation package which is then saved to a portable media device (i.e.: USB drive) and is manually installed on applicable client workstation for specified users. The self-extracting installation package must be executed by a user with administrator privileges. The only key put in the registry of the client workstations is the Service Key. Other values (M, N, etc.) are also placed in the registry by executing a .REG file. FCS_CKM.2, FMT_MSA.3-NIAP-0442

The Configuration Utility also has a Help menu that provides the Security Administrator access to the help information about the Configuration Utility. All of these screens are informational with no input capability. There are no error messages associated with the help screens

7.2.5.2 The Web GUI

The Web GUI security management interface is a browser based interface supported by an Tomcat servlet container running on the Gateway appliance. The Audit Administrators accesses this interface using an Internet Explorer browser from any other Stealth-enable platform in the internal network that has the Audit administrator’s profile loaded. Upon navigating to the applicable Gateway URL, the Audit Administrator enters the Username/Password combination to log onto the Web GUI application on the Stealth Gateway appliance. The Apache Tomcat component maintains the user security attributes, validates the user ID and password, authorizes the session and presents the administrative interface pages.

The Audit Administrator uses the Web GUI Interface through browser sessions to review audit logs backup and manage logs, view parsing parameters, review Gateway operational status, monitor Stealth tunnel statistics and reset and/or terminate tunnels. The Web GUI interface provides a navigation menu for accessing appliance status, appliance configuration, key configuration, view logs, log management and help. FMT_SMF.1(b), FMT_MTD.1(q), FMT_MTD.1(r)

The Appliance Status screen is the initial screen presented to Audit Administrators following login. This GUI interface provides a listing of Active Tunnels and includes the following data for each Active Tunnel listed: IP Address, State, Frames sent, Frames received, Lost frames, and applicable Crypto Key ID. Also provided within this interface is a Reset button which allows the Administrator to reset an Active Tunnel session and a Terminate button which will begin the tear-down process of tunnels through the TERM packet process. The TERM PDU is sent by either endpoint of a tunnel to notify the other endpoint that it is stopping processing (i.e. closing) the tunnel. There is no response to the TERM PDU, as it is a notification only, not a request. After the terminating endpoint issues the TERM, it all information about the tunnel, including the reference from the tunnel to the COI key and session keys, is deleted. This interface also allows the Audit Administrator to export the active tunnel list in Excel, XML or PDF format.

The Appliance Configuration GUI page presents a read-only screen which displays the following Endpoint parameter settings as established for the applicable Stealth Gateway appliance: SecureParser “N” value, SecureParser “M” value, Max. Queue Depth and the applicable Service key in use.

The Key Configuration screen portion of the GUI allows the Audit Administrator to view which Admin and Workgroup keys (by name) are configured for use by the particular Gateway in use. The value of keys is not visible to anyone.

The View Logs screen portion of the GUI provides the interface used to view audit logs as described in Section 7.2.1 – Security Audit above. This interface imports event log data stored by the underlying XP OS into the GUI page and populates a table. This interface allows the viewing of the application and system log categories. This screen also allows the download of audit logs in Excel, XML, or PDF formats.

The log management screen allows the backup or download of audit records for archiving purposes; log files may be deleted by selecting the applicable log records by checking the applicable check box next to the record and pressing the delete button. This screen also allows the download of audit logs in Excel, XML, PDF or EVT formats.
This interface also includes an indicator for log status; green for normal, yellow for log is 80% full (action should be taken), and red for the log is 90% full (action is required).

7.2.5.3 The Key Management Utility.

The TOE provides a key management utility (Key Utility) on the Configuration workstation to generate and organize workgroup keys used by the TOE. The underlying XP OS access control mechanisms limit access to the key management utility to the Security Administrator.

The Security Administrator uses the key management application as the interface to generate workgroup keys and create tuples; support from RSAENH is required for the generation, wrapping, and unwrapping of COI keys. These are manually distributed to the applicable client workstation as described in Section 7.2.2.4, "Workgroup COI Key Generation and Distribution Using User Certificates and Profiles"**.**
FCS_CKM.2.1, FMT_SMF.1(b)

7.2.5.4 WIN XP Management Support

General management of the Configuration Workstation and Client Workstations depends on the underlying XP OS for the management SFRs listed in Table 28 – Management SFRs. The XP OS ST [12] details these SFRs.

Table 28 – Management SFRs

SFR	SFR Description
FMT_MOF.1(a)	Management of Audit
FMT_MOF.1(b)	Management of TOE TSF Data in Transmission
FMT_MOF.1(c)	Management of Unlocking Sessions
FMT_MSA.1(a)	Management of DAC Object Security Attributes
FMT_MSA.3(a)	Static Attribute Initialization
FMT_MSA_EX.2	Valid Password Security Attributes
FMT_MTD.1(a)	Management of the Audit Trail
FMT_MTD.1(b)	Management of Audited Events
FMT_MTD.1(c)	Management of User Attributes
FMT_MTD.1(d)	Management of Authentication Data
FMT_MTD.1(e)	Management of Account Lockout Duration
FMT_MTD.1(f)	Management of Minimum Password Length
FMT_MTD.1(g)	Management of TSF Time
FMT_MTD.1(i)	Management of Advisory Warning Message
FMT_MTD.1(j)	Management of Audit Log Size
FMT_MTD.1(k)	Management of User Inactivity Threshold
FMT_MTD.1(l)	Management of General TSF Data
FMT_MTD.1(m)	Management of Reading Authentication TSF Data
FMT_MTD.1(n)	Management of Password Complexity Requirement
FMT_MTD.1(o)	Management of User Private/Public Key Pair
FMT_MTD.2	Management of Unsuccessful Authentication Attempts Threshold
FMT_REV.1(a)	Revocation of User Attributes

Table 28 – Management SFRs	
SFR	SFR Description
FMT_REV.1(b)	Revocation of Object Attributes
FMT_SAE.1	Timed–limited Authorization
FMT_SMF.1(a)[26]	Specification of Management Functions
FMT_SMR.1(a)[27]	Security Roles
FMT_SMR.3	Assuming Roles

7.2.6 Protection of the TOE

The TSF protects all TSF data transmitted between different parts of the TOE using the Stealth Tunneling Protocol. FPT_ITT.1

The Gateway appliance protects against USB devices that may inject malicious code by forcing the restoration of the factory default Stealth software and shutdown if a DriveType of "Fixed" is plugged into a USB port.

The Configuration Utility backend program, which is always executing on the Gateway appliance, polls Windows once per second looking for a newly inserted block-mode device (any device which can function as a storage medium, e.g. a flash drive, an external hard drive, a CD-ROM, or DVD). It looks through the list of drives (e.g. a:, b:, c:, d:, etc.) for a DriveType of "Fixed" that is not C:, or a non-network drive that is ready (Not DeviceNotReady). This code detects devices such as thumb drives, external hard drives, CD/DVDs, MP3 players, and smart phones.

When such a device is detected:

1. The uninstall portion of the appliance's installation process is launched;
2. The uninstall process shuts down the Logon Service;
3. The Logon Service sends an IOCTL to the driver to terminate all open tunnels;
4. The Configuration Utility password, network configuration, and Stealth endpoint settings are reset to factory defaults;
5. The loaded version of all Stealth software is uninstalled from the appliance;
6. The appliance is automatically rebooted;
7. Upon reboot, the factory-default installation files are copied from a protected portion of the hard drive;
8. The factory-default installation is launched;
9. Upon completion of the (silent) installation, the appliance is shutdown;

FPT_USB_EXP.1

The appliance synchronizes the time at system start-up as well as during operation using a Network Time Protocol (NTP) service, NTP, thereby providing an accurate time reference for the TOE. The TOE implementation conforms to RFC 1305v3, "Network Time Protocol"; this protocol carries on an exchange of time data with an authoritative time source to allow the TOE maintain accurate time; however, the exchange to time data does not occur during the time a user is logged on to a workstation. The NTP service sets the system clock and keeps it synchronized with a NTP server; the Configuration Workstation is used as the NTP server.

The Network Time Protocol is initiated by the Client and Gateway NTP client, which makes requests for time synchronization to the NTP server residing on the Configuration workstation, exchanging packets that contain time information as well as sanity checks with its time servers at poll intervals. When the time server receives the packet, it will in turn store its own timestamp and a transmit timestamp into the packet and send it back to the client (the TOE). The client will in turn log its receipt time and estimate the travelling time of the packet.

[26] Reference in Windows ST [12] does not include iteration identifier "(a)"
[27] Reference in Windows ST [12] does not include iteration identifier "(a)"

The Configuration workstation is configured during the installation process to act as the NTP server for the TOE, which requires the registry be modified. Therefore, when NTP reads the windows registry at initial startup; the registry specifies the synchronization sources, modes and other related information. The NTP server depends on the underlying XP OS real time clock to provide accurate time. FPT_STM.1

7.2.7 TOE Access

Control of the establishment of user sessions on the Configuration Workstation and Client Workstations depends on the underlying XP OS for the TOE access SFRs listed in Table 29 – TOE Access SFRs. The XP OS ST [12] details these SFRs.

Table 29 – TOE Access SFRs

SFR	SFR Description
FTA_SSL.1	TSF-Initiated Session Locking
FTA_SSL.2	User-Initiated Session Locking
FTA_TAB.1	Default TOE Access Banners

Terminology

Table 30 - Terminology	
Term	Description
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access control	Security service that controls the use of resources and the disclosure and modification of data.
Accountability	Tracing each activity in an IT system to the entity responsible for the activity.
Administrative-user	Refers in a general sense to Administrators of the Stealth Gateway appliance. These are Security Administrators and/or Audit Administrators.
Administrator	An authorized user who has been specifically granted the authority to manage some portion or all of the TOE and thus whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Asymmetric cryptographic system	A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).
Asymmetric key	The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system.
Attack	An intentional act attempting to violate the security policy of an IT system.
Audit Administrator	Audit Administrators accesses Stealth Gateways using a Browser installed on the Client Platforms and through the Admin Interface can monitor tunnel statistics, Gateway operations and review audit logs and set parsing parameters but cannot perform Gateway configuration.
Authentication	Security measure that verifies a claimed identity.
Authentication data	Information used to verify a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Authorized user	An authenticated user who may, in accordance with the TSP, perform an operation.
Availability	Timely, reliable access to IT resources.
CAP	Composed Assurance Package
Client User	Client Users use Stealth client platforms to access information protected by Stealth Gateway sessions but are not Administrative-users. Since Stealth is transparent to these users, they are simply users of the information resources and not of Stealth itself.
Community of Interest	This term is used to define groups that are allowed to communicate with network resources in the unparsed network. This term is independent of what users are members of the COI.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to disclosure of data.
Configuration GUI	Same as Configuration Utility
Configuration Utility	Refers to an administrative GUI that is accessed exclusively by Security Administrators using a client-side interface from the Configuration workstation. This interface is used for configuration of the Stealth Gateway.
Critical cryptographic security parameters	Security-related information (e.g., cryptographic keys, cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.
Cryptographic boundary	An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.

Table 30 - Terminology	
Term	Description
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines: − the transformation of plaintext data into ciphertext data, − the transformation of ciphertext data into plaintext data, − a digital signature computed from data, − the verification of a digital signature computed from data, or − a data authentication code computed from data.
Cryptographic module	The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic module security policy	A precise specification of the security rules under which a cryptographic module must operate.
Dedicated Computer	A platform or desktop computer that is committed to only configuring and reconfiguring Stealth Gateway Machine(s). The dedicated computer generates & stores keys and Stealth Server backup images.
Defense-in-depth	A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.
Discretionary Access Control (DAC)	A means of restricting access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Embedded cryptographic module	One that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).
Enclave	A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or based on physical location and proximity.
Entity	A subject, object, user or external IT device.
External Network	Within this Security Target this refers to resources outside the parsed network that are accessed by the Gateway appliance on behalf of Client Users. Through A.PEER, these resources are assumed to be within a trusted enclave.
Gateway (appliance)	aka Stealth Gateway – refers to the TOE appliance installed and connected to each external network supported by Stealth to facilitate Endpoint to Endpoint secure communications between the external network and the parsed intranet. Includes an Endpoint as part of the Stealth Software installed within the appliance.
Identity	A means of uniquely identifying an authorized user of the TOE.
Keymaker	The Key Generation Utility application running on the Configuration Workstation. Used to generate Admin, Workgroup and Service keys (via RSAENH) for use with the TOE.
Max. Queue Depth	This value specifies how many consecutive packets can be lost before the tunnel must be torn down and re-established.
Stealth tunnels	Refers to point to point communication dialogs between unique pairs of nodes.
Client Endpoint	Refers to the Stealth Endpoint installed on Stealth Client platforms within the parsed (internal) network, on Gateway appliances, and on the dedicated Configuration workstation platform.
Named object	An object that exhibits all of the following characteristics: - The object may be used to transfer information between subjects of differing user identities within the TSF. - Subjects in the TOE must be able to request a specific instance of the object. - The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.
National Security Systems	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command and control of military forces; (d) involves equipment that is an integral part of a weapon or weapon system; or (e) is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and

Table 30 - Terminology	
Term	Description
	personnel management applications).
Non-parsed network	Same as “unparsed network”
Non-persistent key	A cryptographic key, such as a key used to encrypt or decrypt a single message or a session that is ephemeral in the system.
Object	An entity under the control of the TOE that contains or receives information and upon which subjects perform operations.
Operating environment	The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.
Operational key	Key intended for protection of operational information or for the production or secure electrical transmissions of key streams.
Parsed Network	Parsed network – The parsed network is the network “behind” the Stealth Gateway. All communications in the parsed network are within STP tunnels.
Persistent key	A cryptographic key which must be maintained between sessions or processes. Generally, a key is persistent because the data it protects is persistent (e.g., an encrypted file) or because it is tied to a user (e.g. a user’s private key). Contrast with a session key such as an IPsec key which protects data in transit.
Persistent storage	All types of data storage media that maintain data across system boots (e.g., hard disk, CD, DVD).
Public object	An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.
Resource	A fundamental element in an IT system (e.g., processing time, disk space, and memory) that may be used to create the abstractions of subjects and objects.
Role	A unique set of TOE-defined functionality limited to a specific set of authorized users.
Secure State	Condition in which all TOE security policies are enforced.
SecureParser	Technology from Security First Corporation that “is based on the simple concept of randomly splitting data, either previously encrypted or unencrypted, at the bit level into any number of “shares” which are then geographically dispersed. This “splitting” and dispersing of data is designed to meet three goals: (1) enhance security (2) allow data recovery and redundancy (3) authorize sharing of data.”
SecureParser “M”	The configured “M” value is the number of shares needed to reassemble the data.
SecureParser “N”	The configured “N” value is the number of parsed data packets created from the original data.
Security Administrator	Security Administrators accesses Stealth Gateways using the client based GUI interface from the Configuration workstation and through this interface may configure the Gateway, set security parameters and create/modify Audit Administrator accounts. Gateway performance statistics and audit logs are not viewed using this interface.
Security attributes	TSF data associated with subjects, objects and users that is used for the enforcement of the TSP.
Security-enforcing	A term used to indicate that the entity (e.g., module, interface, subsystem) is related to the enforcement of the TOE security policies.
Security-supporting	A term used to indicate that the entity (e.g., module, interface, subsystem) is not security-enforcing however, its implementation must still preserve the security of the TSF.
Single-level system	A system that is used to process data of a single security level.
Special Character	Refers to the following characters used as part of a strong password: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
Split key	A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables.
Stealth Client	Refers to the client endpoint software installed on platforms in the Operational Environment which establishes secure sessions and access through Stealth Gateways.
Subject	An active entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security

Table 30 - Terminology	
Term	Description
	policies.
Symmetric key	A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.
System High environment	An environment where all authorized users, with direct or indirect access, have all of the following: a) valid security clearances for all information within the environment, b) formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, sub-compartments and/or special access information), and c) valid need-to-know for some of the information contained within the environment.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
Tomcat	Tomcat is an open-source servlet container.
Tuple	A combination of keys, and other data, to determine encryption & access privileges used for Stealth sessions. For example, the workgroup tuple is made from the workgroup ID, the workgroup key, the encryption mode, and the Stealth Solution for LAN hostname.
Unparsed network	The unparsed network is the network “in front of” the Stealth Gateway. No communication in the unparsed network is done over STP. This may be use interchangeably with “non-parsed network.”
User	Any person who interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.
Web GUI	Refers to a browser based operational interface used exclusively by Audit Administrators using Client Platforms. This interface allows access to status/statistics screens to view Gateway operational performance and allows viewing and export of Gateway audit logs.

8 Acronyms

Table 31 - TOE Related Acronyms	
Acronym	Acronym Description
ARP	Address Resolution Protocol
BLOB	Binary Large Object
CAC	Common Access Card
COI	Community of Interest
CSP	Cryptographic Service Provider (i.e.: Microsoft RSAENH)
EIGRP	Enhanced Interior Gateway Routing Protocol
FIPS	Federal Information Processing Standard
GACP	Gateway Access Control Policy
GP	Gateway Protocol
IGRP	Interior Gateway Routing Protocol
JNI	Java Native Interface
NDIS	Network Driver Interface Specification
OSPF	Open Shortest Path First Protocol
OWASP	Open Web Application Security Project
PEM	Privacy Enhanced Mail
RIP2	Routing Information Protocol (2)
RMI	Remote Method Invocation
STP	Stealth Tunneling Protocol

Table 32 - CC Related Acronyms	
Acronym	Acronym Description
CAP	Composed Assurance Package
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
DAC	Discretionary Access Control
DOD	Department of Defense
DOD	See DOD
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

9 References

Table 33 - TOE Guidance Documentation		
Reference	Description	Control Number
[1]	Unisys Stealth Solution for Network Administration and Operations Guide	8226 4045-000
[2]	Unisys Stealth Solution for Network Planning and Installation Guide	8226 4078-000
[3]	Unisys Stealth Solution for Network Hardware Installation Instructions	8226 4052-000
[4]	Unisys Stealth Solution for Network Common Criteria User Interface Guide	8226 4169-000
[5]	Unisys Stealth Solution for Network Error Message Table	8226 7824-000
[6]	Unisys Stealth Solution for Network Common Criteria Supplement	8226 4151-001

Table 34 - Common Criteria v3.1 References			
Reference	Description	Version	Date
[7]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001	V3.1 R3	July 2009
[8]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2009-07-002	V3.1 R3	July 2009
[9]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2009-07-003	V3.1 R3	July 2009
[10]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2009-07-004	V3.1 R3	July 2009

Table 35 – Supporting Documents			
Reference	Description	Version	Date
[11]	NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revised)	---	March, 2007
[12]	Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target	3.0	November 19, 2007