National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Unisys Corporation,
70 E Swedesford Rd
Malvern, PA

UNISYS Stealth Solution for Networks

Report Number:	**CCEVS-VR-10304-2011**
Dated:	**18 April 2011**
Version:	**0.2**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Kenneth Elliott
Aerospace Corporation
Columbia, MD

Shaun Gilmore
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Ryan Day
Kenji Yoshiro
InfoGard Laboratories, Inc.
San Luis Obispo, California

Table of Contents

1 Executive Summary 4
2 Operational Environment of the TOE 4
3 Identification of the TOE 5
4 Interpretations 5
5 Architectural Information 6
6 Documentation 10
6.1 Design Documentation 11
6.2 Guidance Documentation 12
6.3 Configuration Management and Lifecycle 12
6.4 Test Documentation 13
6.5 Vulnerability Assessment Documentation 14
6.6 Security Target 14
6.7 Site Audit 14
7 IT Product Testing 14
7.1 Developer Testing 14
7.2 Evaluation Team Independent Testing 15
7.3 Vulnerability Analysis 15
8 Evaluated Configuration 16
9 Results of the Evaluation 16
9.1 Evaluation of the Security Target (ASE) 16
9.2 Evaluation of the Development (ADV) 17
9.3 Evaluation of the Guidance Documents (AGD) 17
9.4 Evaluation of the Life Cycle Support Activities (ALC) 17
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 18
9.6 Vulnerability Assessment Activity (AVA) 18
9.7 Summary of Evaluation Results 18
10 Validator Comments/Recommendations 18
11 Security Target 19
12 Terms 19
12.1 Terminology 19
12.2 Acronyms 23
12.3 Common Criteria Related Acronyms 23
13 References 24

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Unisys Stealth Solution for Network, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the Unisys Stealth Solution for Network product was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States and was completed in April, 2011. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1r3 July 2009, Evaluation Assurance Level 4 (EAL 4) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1r3, July 2009.

The Unisys Stealth Solution for Network provides secure communications on a new or existing network (intranet) through the addition of the Unisys Stealth Solution for Network 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. In the evaluated configuration, one gateway device is allowed, and a user can be a member of only one 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.

2 Operational Environment of the TOE

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 Server 2003 SP2

3 Identification of the TOE

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation and Validation Scheme
Evaluated Target of Evaluation	Unisys Stealth Solution for Networks
Protection Profile	N/A
Security Target	UNISYS Stealth Solution for Networks Security Target Version 2.7 March 15, 2011
Dates of Evaluation	July 2008 – April 2011
Conformance Result	EAL 4 augmented ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1R3, July 2009
Evaluation Technical Report (ETR)	10-1455-R-0052 V1.0
Sponsor/Developer	Unisys
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino, Ryan Day
CCEVS Validators	Kenneth Elliott, Aerospace Corp. Columbia, MD
	Shaun Gilmore, National Security Agency, Ft. Meade, MD

Table 1: Product Identification

4 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation. The Evaluation Team determined that NIAP Interpretation I-0482 applied to the ST.

The TOE is also compliant with all International interpretations with effective dates on or before July 22, 2008.

5 Architectural Information

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 a filter (termed 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 do not use the STP.

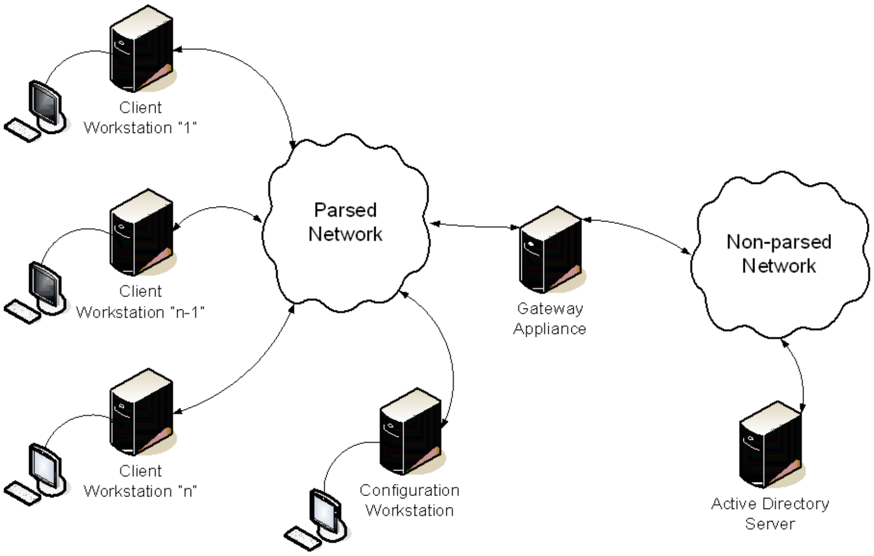

Figure 1 - TOE Network Topology and Communications Paths

The following specific requirements are levied on the product in order for it to be considered in an “evaluated configuration”:

- 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.

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 2 – Unisys Software and Table 3- Third Party Software Components.

Table 2 – 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 3- 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

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] 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[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

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

[4] SP2 with patches to SP3

[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”

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 3, 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.
- One Configuration Workstation, customer provided
    - General purpose workstation: must meet hardware requirements specified above
    - Must be configured as specified in TOE guidance.

The TOE provides the following security services: Audit (related to the functioning of the "tunnels" and TOE configuration), Cryptography (used to protect communications and enforce COI restrictions), User Data Protection (traffic filtering as well as protection provided through the underlying Windows OS), Identification and Authentication (for administrators of the TOE, and of users through Windows mechanisms), Security Management, and Protection of the TSF.

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.

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.

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.

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.

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.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Unisys Stealth Solution for Network Security Target. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.

- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered as PDFs on the installation media.

6.1 Design Documentation

Document	Revision	Date
Unisys Stealth Solution for Network Architectural Design	0.622	November 11, 2010
UNISYS® Stealth Solution for Networks 1.4.482 Design Documentation Functional Specification (ADV_FSP.4)	0.84	November 12, 2010
UNISYS® Stealth Solution for Networks 1.4.482 Security Architecture Description (ADV_ARC.1)	0.43	November 12, 2010
Apache-tomcat-6.0.18-src Source Code (component)	6.0.18	August 2007
Universal Serial Bus Specification	2.0	April 27, 2000
SeucreParser SecureParser API Reference Version 4.7	1.0	June 2010
SecureParser KeyStore Module v2.0 Specification Version 4.7	2.1	June 2010
SecureParser SecureParser Specification Version 4.7	1.5	June 2010
DIM-EAL-1.4-2010-10-22-14-21-01.zip DOXYGEN	1.4	October 22, 2010
SFR Mapping Reformatted		November 8, 2010
Unisys Stealth Solution for Network Common Criteria User Interface Guide	82264169-001	September 3, 2010
Hypertext Transfer Protocol -- HTTP/1.1		June 1999

Document	Revision	Date
NDIS Library Function References		October 5, 2010
RSAENH		
Winsock Reference (Windows)		November 4, 2010
Windows XP Enhanced Cryptographic Provider (RSAENH) FIPS 140-2 Documentation Security Policy	1.1	April 24, 2008

6.2 Guidance Documentation

Document	Revision	Date
Stealth Solution for Networks **Hardware Installation Instructions**	**82264052-000, Release 1.0**	August 2010
Stealth Solution for Networks **Administration and Operations Guide**	82264045-000	August 2010
Stealth Solution for Networks **Planning and Installation Guide**	82264078-000	August 2010
Unisys Stealth Solution for Network Common Criteria Supplement	**82264151-001**	September 30, 2010
Unisys Stealth Solution for Network Common Criteria User Interface Guide	**82264169-001**	September 30, 2010

6.3 Configuration Management and Lifecycle

Document	Revision	Date
UNISYS® Stealth Solution for Networks Common Criteria Configuration Management ALC_CMC.4, ALC_CMS.4 EAL 4 + ALC_FLR.2	0.92	August 1, 2010
UNISYS® Stealth Solution for Networks Common Criteria Secure Delivery Document EAL 4 + ALC_FLR.2	0.8	August 31, 2010

UNISYS® Stealth Solution for Networks Common Criteria Configuration Management ALC_DVS.1 EAL 4 + ALC_FLR.2	0.8	August 31, 2010
UNISYS® Stealth Solution for Networks Common Criteria Life-Cycle Definition Document EAL 4 + ALC_FLR.2	0.2	August 27, 2008
UNISYS® Stealth Solution for Networks Common Criteria Tools and Techniques Document EAL 4 + ALC_FLR.2	0.7	August 27, 2010
UNISYS® Stealth Solution for Networks Common Criteria Flaw Remediation Document EAL 4 + ALC_FLR.2	0.3	August 6, 2010
Product Management Process Guide	7810 6689 Revision H3	September 2003
Introduction to the Service System and the Engineering PRIMUS Application System (EPAS)	RSS-165.8	June 19, 2003
PRODUCT REALIZATION Field Change Notice (FCN) Process	0000025964 Revision B	August 22, 2006
Field Change Notice Sample	4000 0669-001	January 23, 2003
Primus Service Request		September 22, 2008
Stealth L1 – Integration and Function testing UCF process		July 25, 2008
System Test & Integration - System Testing Process	4310 7937 Revision 4	May 12, 2003
Tracker - Process and Procedures Guide	RSS-260	September 26, 2002
ReleaseCenter Process Document for Generating Windows-based Software	2337 5850	December 27, 2004
Using SharePoint in Information Development	38468914 Version E	October 2008
Unisys Information Security Concept of Operations	4.0	May 7, 2008

6.4 Test Documentation

Document	Revision	Date
EAL 4 (+ ALC_FLR.2) Tests Activity ATE *UNISYS® Stealth Solution for Network 1.4.2*	1.1	September 30, 2010

Document	Revision	Date
InfoGard Independent and Penetration Test Plan	1.1	October 15, 2010

6.5 Vulnerability Assessment Documentation

Document	Revision	Date
Unisys Stealth Solution for Network Common Criteria Vulnerability Analysis AVA_VAN.3 EAL 4	1.0	November 10, 2010

6.6 Security Target

Document	Revision	Date
Unisys Stealth Solution for Network Security Target	2.7	March 15, 2011

6.7 Site Audit

Document	Revision	Date
Unisys Site Audit Master Checklist	1.0	October 30, 2009
Unisys Site Audit Checklist - Irvine	0.2	August 30, 2010

7 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

7.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. The Developer testing effort thoroughly tested the available interfaces to the TSF.

The evaluation team verified that the Developer's testing tested every aspect of every SFR defined in the ST. This analysis ensures adequate coverage for EAL 4. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

7.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing at InfoGard. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions with open parameters (e.g. text fields, unbounded number fields)

The evaluation team reran all of the Developer's test cases and specified 4 additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once and the evaluation team verified that each test passed.

7.3 Vulnerability Analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis and penetration tests.

The evaluators performed a vulnerability analysis of the TOE to identify any obvious vulnerabilities in the product and to determine if they are exploitable in the intended environment for the TOE operation. In addition, the evaluation team performed a public domain search for potential vulnerabilities. The public domain search did not identify any known vulnerabilities in the TOE as a whole or any components of the TOE.

Based on the results of the evaluation team's vulnerability analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with Enhanced-Basic attack potential. The evaluation team conducted testing using the same test configuration that was used for the independent testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing and the design activity to devise the penetration tests. The penetration tests attempted to use the interfaces of the TOE in unexpected ways that the evaluators believed might cause the TOE to behave in unexpected ways and potentially violate the SFRs.

8 Evaluated Configuration

The evaluated configuration consists of the following components, however, the number of Gateway appliances, client workstations, and administrative workstations 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.
- One Administrative Workstation, customer provided
  - General purpose workstation: must meet hardware requirements specified above
  - Must be configured as specified in TOE guidance.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 and CEM version 3.1. The evaluation determined the UNISYS Stealth Solution for Networks to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the UNISYS Stealth Solution for Networks product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

1. The TOE contains a number of third-party (non-Unisys) components, most notably Windows 2003 and Apache Tomcat. For Windows 2003, the evaluation approach was to analyze the changes (SP2 to SP3 plus additional hotfixes) to the base evaluated version and to ensure that the changes had no overt affect on the Windows security functionality as it was used by the TOE. Similarly, the portions of Tomcat that that are

exposed to users of the TOE were analyzed in the context of their use in the TOE. The implication is that the analysis and testing performed on these third-party product is commensurate with the analysis and testing performed on the Unisys-developed parts of the TOE, but there is no statement about the security properties of the third-party products outside of this evaluation (that is, using Tomcat in another environment will require additional analysis; the results of this analysis will likely have little applicability).

11 Security Target

Unisys Stealth Solution for Network Security Target, Version 2.7, March 15, 2011.

12 Terms

12.1 Terminology

Table 4 - 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 Admin 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.

Table 4 - Terminology

Term	Description
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 refers to a group of Stealth Client users with access to particular resources fronted by a Stealth Gateway. External resources have a Stealth Workgroup key associated with it and the Stealth Clients that are authorized to access this resource hold the required key and make up the COI.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to disclosure of data.
Configuration Utility	Refers to the GUI administrative interface that is accessed exclusively by Security Administrators using a client based interface from the Administrator 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.
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

Table 4 - Terminology

Term	Description
	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 Administrator 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 Administrator 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 personnel management applications).
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	A parsed network sends and receives data encrypted and split into packets using the SecureParser technology with each packet going over a different path in the network.
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).

Table 4 - Terminology

Term	Description
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 Administrator 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 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-

Table 4 - Terminology	
Term	Description
	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.
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.

12.2 Acronyms

Table 5 - 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
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

12.3 Common Criteria Related Acronyms

Table 6 - 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

Table 6 - CC Related Acronyms

Acronym	Acronym Description
DAC	Discretionary Access Control
DOD	Department of Defense
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

13 References

Table 7 - Common Criteria v3.1 References

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

Table 8 – Supporting Documents

Reference	Description	Version	Date
[5]	NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revised)	---	March, 2007
[6]	NIST Special Publication 800-56 Recommendation On Key Establishment Schemes, [http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf].	Draft 2.0	January 2003
[7]	NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography		March, 2007