EVALUATION TECHNICAL REPORT

Issue:

Arca LTEF 004/2000-SunScreen™ EFS 3.0 Revision B
TTAP - FER - 0014
Stealth Mode Operation

July 24, 2000

Prepared for:
Sun Microsystems
901 San Antonio Road
Palo Alto, CA 94303-4900

Prepared by:
Arca Systems, Inc.
An Exodus Communications Company
10220 Old Columbia Road, Suite G-H
Columbia, MD 21046

Submitted to:
TTAP Oversight Board
9800 Savage Rd.
Ft. Meade, MD 20755

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

FOREWORD

This report, the SunScreen EFS 3.0 Revision B Stealth Mode Evaluation Technical Report (ETR), is issued by Arca Systems, Inc., a Licensed Trust Technology Assessment Program Evaluation Facility (LTEF), in cooperation with the National Security Agency and National Institute for Standards and Technology. The purpose of this ETR is to document the results of the security evaluation performed on the SunScreen EFS 3.0 Revision B Stealth Mode Product by the ARCA LTEF. The requirements for this evaluation are detailed in International Standard ISO/IEC 15408:1999, The Common Criteria for Information Technology Security Evaluation (CC 2.1), and the Common Methodology for Information Technology Security Evaluation (CEM) Version 1.0. This evaluation followed all processes and procedures as defined in the CC and CEM, and meets the quality standards set forth by the ARCA LTEF.

Approved:

Stephen P. Nardone
Vice President and Director ARCA LTEF
Arca Systems, Inc.

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1 BACKGROUND 1
1.2 EVALUATION BACKGROUND 2
1.3 OBJECTIVES 2
1.4 SCOPE 2
1.5 STRUCTURE 2
2. ARCHITECTURAL DESCRIPTION OF THE TOE 3
2.1 STATEMENT OF THE TOE 3
2.1.1 Hardware 3
2.1.2 Software 4
2.2 EVALUATED CONFIGURATION 4
2.2.1 Scope of Evaluation 7
2.3 TOE COMPONENTS 7
2.3.1 Solaris Kernel 7
2.3.2 Solaris I&A 7
2.3.3 Solaris Syslog 8
2.3.4 Solaris Network Stack 8
2.3.5 SunScreen Screen 8
2.3.6 SunScreen Admin Interface 8
2.3.7 SunScreen HA 9
2.3.8 SunScreen Audit 10
2.3.9 SunScreen SKIP 10
2.3.10 SecurID Client 11
3. EVALUATION 12
3.1 EVALUATION METHODS, TECHNIQUES AND STANDARDS 12
3.2 EVALUATION TOOLS 12
3.3 CONSTRAINTS 12
3.4 ASSUMPTIONS 12
4. RESULTS OF THE EVALUATION 13
4.1 CLASS ASE – SECURITY TARGET EVALUATION 13
4.1.1 ASE_DES.1 13
4.1.2 ASE_ENV.1 13
4.1.3 ASE_INT.1 14
4.1.4 ASE_OBJ.1 14
4.1.5 ASE_PPC.1 15
4.1.6 ASE_REQ.1 15
4.1.7 ASE_SRE.1 16

4.1.8 ASE_TSS.1 17

4.2 CLASS ACM – CONFIGURATION MANAGEMENT 18
4.2.1 ACM_CAP.2 18

4.3 CLASS ADO - DELIVERY AND OPERATIONS 18
4.3.1 ADO_DEL.1 18
4.3.2 ADO_IGS.1 19

4.4 CLASS ADV – DEVELOPMENT ACTIVITY 19
4.4.1 ADV_FSP.1 19
4.4.2 ADV_HLD.1 20
4.4.3 ADV_RCR.1 21

4.5 CLASS AGD - GUIDANCE DOCUMENTATION 22
4.5.1 AGD_ADM.1 22
4.5.2 AGD_USR.1 23

4.6 CLASS ATE - TESTS 24
4.6.1 ATE_COV.1 24
4.6.2 ATE_FUN.1 24
4.6.3 ATE_IND.2 26

4.7 CLASS AVA - VULNERABILITY ASSESSMENT 28
4.7.1 AVA_SOF.1 28
4.7.2 AVA_VLA.1 29

5. CONCLUSION AND RECOMMENDATIONS 31

5.1 CONCLUSION 31

5.2 RECOMMENDATIONS 31

6. LIST OF EVALUATION EVIDENCE 32

7. LIST OF ACRONYMNS 34

8. OBSERVATION REPORTS 35

1. INTRODUCTION

The following table provides the required identification information for the evaluation.

Evaluation Scheme Identifiers	United States Trust Technology Assessment Program
ETR Configuration Control Identifiers	SunScreen EFS 3.0 Revision B Stealth Mode Operation EVALUATION TECHNICAL REPORT Document Reference: Arca LTEF 004/2000-TOE Reference
ST Configuration Control Identifiers	SunScreen EFS 3.0 Revision - Stealth ST, Arca LTEF 002/2000-SUN Stealth Mode Security Target
TOE Configuration Control Identifiers	SunScreen EFS 3.0 Revision B Stealth Mode, running on Sun MicroSystems Solaris 2.6 or 2.7, Intel or SPARC hardware base
TOE Developer	Sun Microsystems, Inc.
Sponsor	Sun Microsystems, Inc.
Evaluators	Arca Systems Christopher J. Romeo Eric Winterton Kris Winkler Cornelius J. Haley Government Participants Jeff Johnston William Simpson
Certifers	Mario Tinto Gary Grainger

1.1 BACKGROUND

The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called TTAP Evaluation Facilities (TEFs) using the current NSA evaluation methodology and proposed evaluation methodology for Evaluation Assurance Level (EAL) 1 and EAL 2 in accordance with cooperative research and development agreements. The program focuses on products with features and assurances characterized by the Common Criteria (CC) EAL 1 through EAL 4. In addition, TEFs are allowed to conduct PP and ST evaluations.

The TTAP Oversight Board assigns a Certifier(s) to monitor the TEFs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a TEF and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is be added to NSA's Evaluated Products List.

The TTAP is migrating to the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). Under the Mutual Recognition

Arrangement (MRA), evaluation facilities conducting CC evaluations must apply the Common Evaluation Methodology (CEM). In anticipation of the final version of the CEM and its application, the TTAP Oversight Board has requested all TEFs to use the CEM when conducting CC evaluations, as appropriate.

1.2 EVALUATION BACKGROUND

Arca Systems has been contracted by Sun Microsystems, Inc. to perform a product evaluation of the SunScreen EFS 3.0 Revision B Firewall. This Task is referred to as the TOE evaluation.

The evaluation began in February 2000 and was completed in July 2000.

1.3 OBJECTIVES

The objectives of this Evaluation Technical Report (ETR) are:

- To describe the work performed during the evaluation
- To present the results obtained and conclusions drawn from this work. This not only includes the evidence in support of evaluation verdicts/conclusions but also covers any TOE re-use and re-evaluation issues.

1.4 SCOPE

This ETR covers the entire evaluation of the vendor's Security Target and TOE.

1.5 STRUCTURE

The structure of this document follows that suggested by the CEM 99/045, Part 2 Evaluation Methodology, chapter 4). It is divided up into eight chapters as detailed below:

Chapter 1 - The introduction to the ETR covering the evaluation background, and the ETR's objectives, scope and structure.

Chapter 2 - The TOE's architectural description, including its functionality.

Chapter 3 - The evaluation details, addressing its history, scope and any assumptions/constraints.

Chapter 4 - The summary of evaluation results for the ASE evaluation and the TOE evaluation.

Chapter 5 - The evaluation team's conclusions and recommendations.

Chapter 6 - A list of Evaluation Evidence used.

Chapter 7 - List of Acronyms used in the ETR.

Chapter 8 - Observation Reports that uniquely identifies the ORs raised during the evaluation and their status.

2. ARCHITECTURAL DESCRIPTION OF THE TOE

2.1 STATEMENT OF THE TOE

The Target of Evaluation consists of the SunScreen EFS 3.0 Revision B Firewall product. This product is provided by Sun Microsystems, Inc.

SunScreen EFS is a software package that is installed on a Solaris-based machine to provide network based access control decisions. SunScreen EFS functions as a firewall and a router for hosts on the network it is protecting.

SunScreen EFS allows division of a network into discrete areas, each served by an interface that provides customized fine-grain access control. Using filtering rules, SunScreen EFS 3.0 Revision B controls the access from one area of a network to another, as well as access to the Internet or other external networks.

SunScreen EFS consists of a rules-based, dynamic packet-filtering engine for network access control, and an encryption and authentication engine that enables the creation of virtual private network (VPN) gateways by integrating public-key encryption technology.

SunScreen also offers high availability (HA) configurations. HA provides fault tolerance by maintaining multiple firewalls that are watching the same network traffic. If the active firewall has a hardware failure, a passive firewall can become the active firewall. For additional information, see section 2.3.7 (SunScreen HA).

SunScreen EFS is administered through a graphical user interface (GUI) via a secure Web browser connection. SKIP encryption is used to protect remote administration sessions. SunScreen also provides four application proxies: FTP, HTTP, SMTP and Telnet.

2.1.1 HARDWARE

The TOE has the following requirements for hardware.

Hardware	All SPARC and UltraSPARC platforms developed to the SPARC version 9 specification, and 486 and Pentium Intel platforms that are capable of running the Solaris 2.7 or 2.6 Operating Environments.
Disk Space	Minimum of 1 Gbyte (>300Mbytes free)
Memory	Minimum of 32Mbytes, 64 Mbytes strongly recommended.

Network Interfaces	For SPARC systems: 10-Mbps or 100-Mpbs Ethernet Interfaces (le, qe, hme, be, qfe)*. For Intel systems: 10 Mbps or 100 Mbps Ethernet Interfaces (dnet, elxl)*. HA requires two or more Screens be connected via a non-switched hub. * Stealth mode supports only 10-Mbps or 100Mbps Ethernet NICs on the corresponding Sun Hardware Compatibility Lists: Hardware Compatibility List for Solaris 2.6, April 2000 or Solaris 2.7 Hardware Compatibility List, June 2000.
Media	CD-ROM drive and diskette drive

The hardware bases supported include both the SPARC/UltraSPARC lines and the 486/Pentium lines. The SPARC/UltraSPARC machines are proven to be compatible through the SPARC version 9 specification. This specification is used and tested against all Sun manufactured equipment, and provides assurance that each SPARC/UltraSPARC hardware base is providing the same interfaces, at the hardware level. The 486/Pentium platforms are constrained to those platforms that are supported by the Solaris 2.7 and 2.6 Operating Environments. Both Solaris 2.7 and 2.6 provide a hardware compatibility guide. This guide can be used to determine a correct platform to operate the TOE on an Intel system.

2.1.2 SOFTWARE

The TOE has the following requirements for software.

Operating System	Solaris 2.7 or 2.6 Operating Environment for SPARC and Intel Platforms
Web Browser	HotJava 1.1.5
Firewall Software	SunScreen EFS 3.0 Revision B, includes all software packages required on the Screen to implement the TOE.
Third Party Software	SecurID (SunScreen EFS is compatible with ACE/Server version 3.0.1 and higher)

2.2 EVALUATED CONFIGURATION

The evaluated configuration consists of a SunScreen EFS 3.0 Revision B firewall. The firewall operates as a packet filter firewall and operates in stealth mode. Stealth mode means that the firewall interfaces are not visible on either the internal or external networks. There are no IP addresses assigned to the external or internal interfaces. A separate NIC is used to connect the optional remote adminsitration statement. This admin NIC does contain an IP address. An example of the stealth mode firewall configuration is demonstrated below in Figure 1.

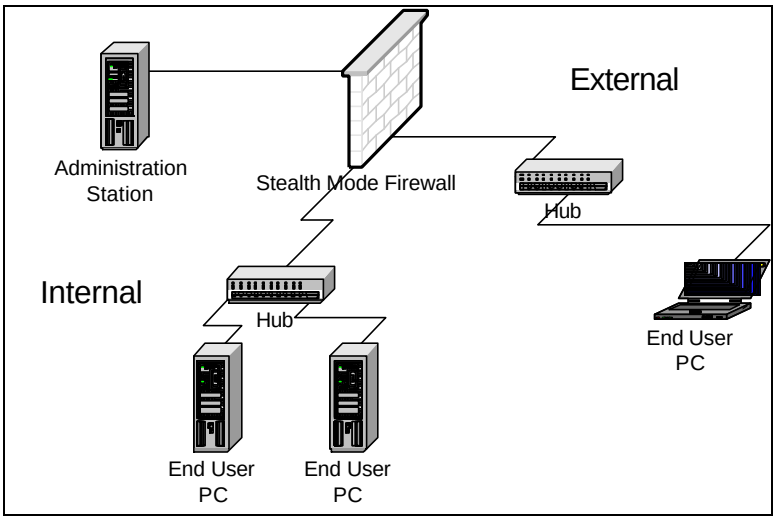

Figure 1: Stealth Mode Firewall Configuration

Both Local and Remote administration are supported by the TOE. Local Administration means that the Administration Station is resident on the same machine as the Screen itself. Since no network traffic is generated between the Administration Station and the Screen, local administration does not require, nor utilize, encryption. Remote Administration means that administration of the Screen is conducted on an Administration Station which is a separate machine from the Screen. Remote Administration uses encrypted communication between the Screen and the Administration Station to protect access and to limit the management of a Screen to an authorized Administration Station. The data which the administrator sees is protected, so the information about the security policy in place on the Screen cannot be obtained by others. The Simple Key Management for Internet Protocols (SKIP) is used within the TOE to provide the encryption between the remote Administration Station and the Screen.

A series of assumptions exists for the evaluated configuration.

- The TOE is assumed to be physically protected. This means that the firewall iteself is stored in a locked room.
- The TOE is assumed to not contain any general purpose computing services. This includes web servers, file servers or any other type of service other than operating as a firewall.
- The TOE is assumed to not host any public data.

SunScreen SKIP provides hosts that use the Solaris operating system with the ability to encrypt any protocol within the TCP/IP protocol suite (thereby establishing a VPN connection between hosts). VPN traffic through or to a SunScreen must satisfy the screen's defined policy. SKIP was included in the evaluated configuration, but the following facets of SKIP were not evaluated:

- Strength of the SKIP protocol
- Setting up User SKIP connections
- Strength of the selected encryption algorithm

The TOE requires installation of the SunScreen SKIP to allow the capability of remote administration.

High availability is provided by utilizing multiple firewalls, with one firewall operating as the primary firewall and up to thirty-one other firewalls providing backup services. Each firewall in a cluster sees all the network traffic that the active firewall sees. If the active firewall halts due to a failure, one of the secondary firewalls will take over. The network configuration for high availability mode includes an external network, internal network and a dedicated HA network. The dedicated HA network contains an interface in each firewall that performs heart-beat operations and policy updates. An example of the stealth mode high availability firewall configuration is demonstrated below in Figure 2.

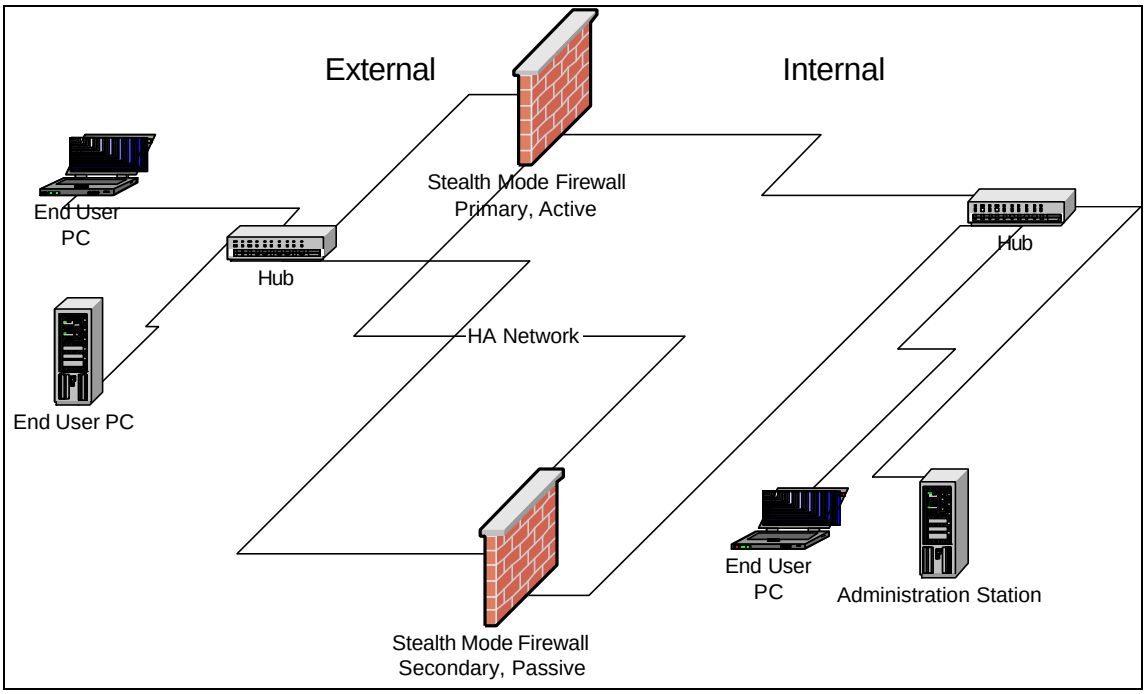

Figure 2: Stealth Mode High Availability Firewall Configuration

There are three system features that were evaluated, but are not mandatory for the firewall to operate:

- remote administration
- token-based authentication
- High Availability Firewall.

Remote administration is performed using a separate dedicated computer. When remote administration is not in use, the administrator operates the administrative GUI from the local firewall console. Token authentication is optional with this TOE, depending on whether the installing site wishes to utilize SecurID for authentication. High Availability is optional,

depending on whether the site determines that they wish to protect themselves against down time due to hardware failure.

2.2.1 SCOPE OF EVALUATION

This evaluation encompasses a specific set of SunScreen capabilities that were evaluated not for their advertised functionality, but rather for their security relevance. That is, while a particular capability may be implied the evaluation was concerned primarily with whether SunScreen policy and self-protection was maintained. The evaluation did not focus upon whether the capability operated as advertised. The specific capabilities are VPN, NAT, HA and alternate authentication servers.

VPN The team evaluated VPN with the focus on VPN traffic through or to a SunScreen satisfying the screen's defined policy. Stipulations as to what was not evaluated for VPN are specified in section 2.2.

NAT The team evaluated Network Address Translation (NAT) to ensure that NAT did not violate or bypass the firewall policy. The team did not address the accuracy of translation performed by NAT, because we did not deem this as security relevant.

HA HA was evaluated to determine it's ability to fail-over correctly when a hardware failure occurred on the active screen. HA was not evaluated as to it's robustness of recognizing failures that were outisde of the active screen.

Authentication Servers
The team evaluated the SecurID client software to ensure that SunScreen enforced the decisions obtained from the clients. The team did not examine how well those clients obtained the data from their servers or how secure the alternate authentication servers were. These issues are covered by IT requirements for the environment.

2.3 TOE COMPONENTS

The SunScreen EFS 3.0 Revision B firewall consists of a collection of subsystems. The following sections describe the TOE components.

2.3.1 SOLARIS KERNEL

The Solaris Kernel subsystem provides process separation, object reuse protection and an accurate time.

2.3.2 SOLARIS I&A

The Solaris I&A subsystem provides user authentication for administrators locally accessing the system console. This subsystem includes applications used to sign onto the system and change a user's password.

The Solaris I&A subsystem may be configured to utilize the SecurID ACE/Client to provide additional authentication services. SecurID ACE/Client is part of the evaluated TOE. It's use is optional and configurable.

2.3.3 SOLARIS SYSLOG

The syslog subsystem provides a general-purpose logging facility. Syslog is a host-configurable, uniform system logging facility. The system uses a centralized system logging process. Individual programs that need to have information logged send the information to syslog. The messages can then be logged to various files, devices, or computers, depending on the sender of the message and its severity.

SunScreen EFS 3.0 Revision B uses the syslog subsystem to record audit information and events from the firewall software.

2.3.4 SOLARIS NETWORK STACK

The SunScreen EFS operating in stealth mode does not use the TCP/IP stack. The kernel module is implemented above the network interface module. Packets cannot enter the SunScreen EFS system without passing through the packet filter, which is located within the network interface driver.

2.3.5 SUNSCREEN SCREEN

The SunScreen EFS 3.0 Revision B subsystem consists of a packet filter, application proxies and network address translation.

SunScreen EFS 3.0 Revision B provides high-performance stateful packet filtering. Packet filtering enables a screen, which sits between the client and server, to examine each data packet as it arrives. Based on information in the packet, state retained from previous events, and a set of security policy rules, the screen either passes the data packet or blocks and drops it.

Common objects are used through the administrative interface to represent the configurable components of the policy. Common objects include address, screen, state engine, service, interface, certificate, and time.

Network address translation enables a screen to map an internal network address to a different network address. As it passes packets between an internal host and a public network, the addresses in the packet are replaced with new addresses transparently, checksums and sequence numbers are corrected in both the IP header and the TCP or UDP header, and the state of the address map is monitored.

Packet checksums and sequence numbers are correctly updated when NAT is in use. NAT is stateful, which increases the efficiency of lookups in the address translation table by using address hashes and checksum adjustments that use differential checksum calculations.

2.3.6 SUNSCREEN ADMIN INTERFACE

SunScreen EFS allows secure, web based administration. The administration tasks can be performed from the local machine or from a remote workstation. All administrative configuration is performed over a SKIP encrypted link. . The remote administration station is assumed to be physically protected from harm.

The SunScreen EFS administration GUI uses Java applets to administer and monitor Screens. The Java code on the browser runs in a Java sandbox and the JVM on a Screen only executes Java code from the local file system, not the network. Communication between a screen and an administration station are protected by SKIP encryption and require an Admin SKIP certificate.

The ssadm daemon is the piece of software that runs on the firewall and accepts administrative sessions from the GUI, administrative sessions from the ssadm command line and policy updates from a primary firewall to secondary firewalls in both HA and central management modes. The ssadm daemon uses the ssadm protocol, which has a number of parameters that allow administrative commands to be executed on the firewall. The administrative GUI builds commands that are sent to the ssadm daemon. For policy updates, commands are built from the primary firewall and pushed to the secondary firewalls.

SunScreen EFS provides centralized management of multiple Screens using a set of common objects through a specific, primary Screen. An administrator can also monitor logs on individual Screens or monitor logs of a centralized management group. Centralized management uses the ssadm interface to push policy updates to secondary screens.

Many different Administration stations can manage the primary Screen. There is no defined limit to the number of different Administration stations that can manage the primary Screen. SunScreen EFS provides a locking mechanism that is used to prevent multiple administration stations from simultaneously editing policies on the same screen. The policy list page can be locked for modification when opened by an administrator. Other administrators are allowed to view the policy lists when another administrator has locked them. The lock is released when the administrator saves their changes or logs out of the administration interface.

A Command Line Interface is available to administer the screen from the screen's console. The ssadm command contains a number of parameters that encompass the tasks performed using the GUI.

2.3.7 SUNSCREEN HA

HA enables the deployment of multiple screens together in situations where the connection between a protected inside network and a insecure outside network is critical. HA was evaluated for its ability to maintain secure state and continue policy enforcement after certain types of screen failures.

One member of the HA cluster, the active HA screen, performs packet filtering, network address translation, logging, and encryption/decryption of packets traveling between the inside and outside networks. The other members of the HA cluster, which can be as many as 31 passive HA

screens, receive the same packets, perform the same calculations as the active HA screen, and mirror the state of the active HA screen, but they do not forward traffic between the inside network and the outside network. Mirroring the state of the active screen does not include generation of audit data. Only the active screen is generating audit data.

If the active HA screen fails, one of the passive HA screens takes over (failover) as the active HA screen and begins routing and filtering network traffic within seconds. Because the passive HA screens mirror the active HA screen, few connections are lost if a failover occurs.

Once the HA cluster is running, the active and passive screens poll each other every few seconds to verify connectivity and status. If the active screen fails or becomes unavailable, the passive screen that has been running the longest takes over as the active screen within 15 seconds. During this time (before the passive screen takes over), no traffic will go through the active or passive firewall.

When setting up an HA cluster, one screen is designated as its primary HA screen and configured with the policy's configuration objects. This includes named screen objects, like address or service with attributes that include these settings, and policy rules that the HA cluster will use. When the security policy is activated, the SunScreen EFS 3.0 Revision B and SunScreen SKIP policies are copied from the primary HA screen to the secondary screens in the HA cluster. When a configuration is activated, the active screen transfers the configuration including certificates, local keys, addresses, security policy rules, and more to all other HA screens.

2.3.8 SUNSCREEN AUDIT

SunScreen Audit allows administrators to search, sort, and filter log messages and find critical information. Logs are monitored in real time using the browser and the command line. Thus, administrators can review activity as it happens.

SunScreen EFS audits attempts to violate the network access policy. SunScreen EFS provides flexible logging of packets. The firewall provides the ability to audit at the granularity of a single rule. Packets may be logged if they do or do not match a particular rule. The value of log size and information to be recorded in the administrative log files is established during the setup of the SunScreen EFS.

2.3.9 SUNSCREEN SKIP

SunScreen SKIP is an IP-layer encryption package integrated into SunScreen EFS 3.0 Revision B. SunScreen SKIP is based on the Simple Key-management for Internet Protocols (SKIP) standard for key management for IP encryption. SunScreen SKIP operates at the network (IP) layer, and is transparent to virtually all applications. Secure communication is possible with all IP (TCP and UDP) applications without modification or knowledge of SKIP. SunScreen SKIP lets computers communicate privately and securely over non-secure public networks. VPN traffic through or to a SunScreen must satisfy the screen's defined policy. It provides a solution to the problem of maintaining Intranet security. By authenticating as well as encrypting the IP traffic stream, SunScreen SKIP achieves the goal of securing internal corporate communication.

SunScreen SKIP provides several network security services:
- Access control to protect corporate data resources from unauthorized use
- Encryption and decryption services to ensure the confidentiality of information sent over a network
- Authentication to ensure the integrity of the information transferred from one host to another and the identity of the sender and receiver
- Key and certificate management to provide efficient, cost-effective administration of the basic building blocks of a security policy

2.3.10 SECURID CLIENT

ACE/Server provides centralized, strong authentication services, ensuring that only authorized users gain access to resources. ACE/Server lets you create a secure perimeter around your network, ensuring that only authorized users are permitted to enter beyond the network perimeter.

SecurID uses a two-factor authentication scheme. One factor is a pseudo-random number generator. The second factor is a personal identification number (PIN). SecurID utilizes encryption and authentication mechanisms that are proprietary to RSA Security, Inc. With ACE/Server and SecurID, only those with the correct combination of the user's PIN and token code will be allowed access to the network.

SecurID authentication provides two forms of association with the SunScreen user model. In one form, a particular token is associated with a specific SunScreen user. In the other form, a general mapping of all SecurID tokens is performed. Configuration of SecurID authentication is performed using the SunScreen administrative interfaces.

The SunScreen EFS administrative interface and proxy authentication modules provide a client interface to the RSA SecurID token card. The username/SecurID tokens are managed by the SecurID ACE/Server.

3. EVALUATION

3.1 EVALUATION METHODS, TECHNIQUES AND STANDARDS

This evaluation was performed using the Common Criteria for Information Technology Security Evaluation (CC 2.1), which is also recognized as International Standard ISO/IEC 15408:1999. The Common Evaluation Methodology (CEM) Version 1.0 governed the work performed by the evaluation team.

The evaluation team performed a Security Target evaluation using the CC 2.1 ASE class. The Security Target evaluated was "SunScreen EFS 3.0 Revision - Stealth ST, Arca LTEF 002/2000-SUN Stealth Mode Security Target". The TOE evaluation was performed at Evaluation Assurance Level (EAL2).

The evaluation team created a test plan that contained some sample tests from the vendor functional test suite, some functional test cases to supplement the vendors tests and the required vulnerability assessment and penetration test cases.

3.2 EVALUATION TOOLS

Arca Systems has created a vulnerability scanning tool referred to as "FrameWork". The version of the Framework tool used for this test was v1.3.1. The evaluation team also used NAI CyberCop v5.5 for Windows NT. Both sets of tools were used in the vulnerability assessment portion of the evaluation testing.

The FrameWork tool was designed to execute vulnerability scanning tools against a collection of hosts. The FrameWork tool contains scanning tools collected from various underground Internet sources. The version number of FrameWork is updated when new vulnerability scanning tools are added.

Vulnerability scanning tools catalog the various services that are running on a system, and report or attempt to exploit vulnerable versions.

3.3 CONSTRAINTS

None

3.4 ASSUMPTIONS

None

4. RESULTS OF THE EVALUATION

4.1 CLASS ASE – SECURITY TARGET EVALUATION

The evaluation team performed multiple reviews of the Security Target. Through those reviews, the evaluators worked with the vendor to verify that the comments generated by the evaluation team were addressed and that the Security Target is both a clear and concise representation of the TOE.

4.1.1 ASE_DES.1

The evaluation team reviewed the TOE description throughout the evaluation.

The Security Target describes the TOE as a packet filter firewall. This satisfies the requirement that the product and system type of the TOE be specified.

The Physical scope and boundaries of the TOE are defined using both high level descriptions of the physical components that make up the TOE (Screen, Administration Station) and the hardware and software that are included as part of the evaluated configuration.

The Logical scope and boundaries are presented as the software based components of the TOE. These include pieces of the Solaris operating system (I&A, syslog, network protocol stack), SunScreen (packet filter, administrative interfaces, audit), SKIP and SecurID client software. The SecurID server software are excluded from the TOE.

The TOE description is coherent and internally consistent, as well as consistent with other parts of the ST. The measurement of DES coherence and internal consistency was performed by iterative review of the TOE description. This review focused upon clarity of the information presented, which security features are being evaluated, and which product features are excluded from evaluation.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_DES.1, resulting in a verdict of PASS.

4.1.2 ASE_ENV.1

The evaluation team reviewed the environment section and analyzed the assumptions and threats that are specified for this TOE. The ST identifies assumptions in the following categories: personnel, physical environment and management of the TOE. There are assumptions limiting the scope of the defined threats and identifying dependencies on the environment.

The ST identifies threats addressed by the TOE in the following categories: bypass of the TOE due to a flaw in the TOE's implementation, modification of the TOE's security critical data, and misuse of TOE audit facilities. A threat addressed by the operating environment is specified and details an administrator that may improperly configure the TOE due to inexperience.

This ST does not contain Organizational Security Policies.

The threats and assumptions are clear and internally consistent. The measurement of clarity and consistency was performed by iterative review of the TOE security environment. This review focused upon the clarity of the information presented, the appropriateness of threats for the stated threat agent, and the validity of the set of threats (and the set of assumptions) as a whole.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_ENV.1, resulting in a verdict of PASS.

4.1.3 ASE_INT.1

The evaluation team reviewed the introduction section of the Security Target and determined that the Security Target contains the text specified by the CEM.

The introduction contains the title, version, publication date, authors, identity of the TOE, version of TOE and CC version. The Overview section of the ST is specified in a narrative form. Conformance to the CC 2.1 is specified as EAL 2.

The introduction is coherent, internally consistent and consistent with the other parts of the ST. The measurement of coherency and consistency was performed by iterative review of the TOE introduction. This review focused upon the clarity of the information presented, the accuracy of the information as compared to the TOE description, the accuracy of the ST overview, and the accuracy of the CC conformance claim.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_INT.1, resulting in a verdict of PASS.

4.1.4 ASE_OBJ.1

The evaluation team reviewed the objectives section of the Security Target. The objectives are correctly split between the TOE and its environment.

The evaluation team ensured that all objectives were listed in the table contained within the rationale section and existed in the Security Target. The team traced each objective and analyzed the threats it claimed to counter. The team concluded that all the objectives mapped back to threats to be countered. No organizational security policies were contained within this ST.

The security objectives for the environment are traced back to threats. The team traced the security objectives outlined for the environment back to the threat specified in the environment section and analyzed whether the objective met the threat. The team determined that appropriate justification is provided for each threat listed in the ST. Organizational security policies do not exist within this ST.

The assumptions for the environment are translated directly into the security objectives for the environment. The evaluation team determined that this is acceptable and that all assumptions map to the objectives because the objectives were created directly from the assumptions.

The security objectives are coherent, complete and internally consistent. The measurement of completeness, coherency and consistency was performed by iterative review of the TOE security objectives. This review focused upon the clarity of the information presented; the sufficiency of the security objectives to counter the stated threats, policies and assumptions; and the validity of the security objectives as a set.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_OBJ.1, resulting in a verdict of PASS.

4.1.5 ASE_PPC.1

No protection profile claims were made for this ST.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_PPC.1, resulting in a verdict of PASS, trivially.

4.1.6 ASE_REQ.1

The evaluation team reviewed the functional and assurance requirements contained within the ST.

The evaluation team reviewed each of the security functional requirements and determined that all the functional requirements were identified and drawn from CC 2.1 Part 2. The evaluation team verified the functional requirements, line by line, against CC Part 2.
All cited elements and components are from CC Part 2 and are correctly reproduced.

The TOE security assurance requirements are identified as EAL2, from the CC 2.1 part three. The assurance components are correct, verified line-by-line against part three of the CC, and are correctly reproduced. EAL 2 is specified as the EAL for this evaluation.

The statement of TOE security assurance requirements is appropriately justified in the ST. The vendor states in the ST that EAL 2 is chosen because a low to moderate level of independently assured security is required. The vendor also states that the threat environment is consistent with the low to moderate level, and that the threat of malicious attack is not greater than moderate. The evaluation team agrees with the statements presented above.

The security requirements for the IT environment are identified. They are specified in a separate section of the ST.

The operations are identified consistently throughout the document. The vendor has utilized bold and italic typefaces to identify operations.

All assignments and selections have been made. The evaluation team reviewed each requirement and determined that all assignments and selection statements had been completed.

The evaluation team reviewed the security functional requirements and verified that the operations were performed correctly. This was assured through a requirement by requirement analysis. The team looked at each requirement and analyzed it against the rules for operations.

All of the dependencies are satisfied within the ST, except for ADV_SPM.1 as a dependency for FMT_MSA.2. The rationale for not providing a model is deemed acceptable.

The evaluation team confirmed that the ST contains a Strength of Function specified as basic. The ST specifies that FIA_UAU.1 has an SOF metric. The minimum strength of function level is specified as basic, with a low attack potential.

The rationale that the security requirements trace back to the security objectives was validated by the team. The team reached this conclusion by tracing the security requirements to the security objectives. The trace consisted of ensuring that each requirement pointed to an objective.

The rationale that the security requirements for the IT environment trace back to security objectives is acceptable. The team reached this conclusion by tracing the security requirements to the security objectives. The trace ensured that each requirement for the IT environment adequately pointed to an objective for the IT environment.

Appropriate justification is provided that the requirements meet the objectives. The determination of appropriate justification required the team to review each requirement and objective in detail, to validate that the rationale was correct.

Justification is provided that the requirements for the IT environment meet the objectives. Appropriate justification was measured by the team by analyzing the rationale provided. The team determined that the rationale provided appropriate justification.

The evaluation team has determined that there are no contradictions among the SFR's of the ST, and thus, the ASE requirement for internal consistency is satisfied.

The requirements are coherent, complete and internally consistent. The measurement of completeness, coherency and consistency was performed by iterative review of the TOE security functional requirements. This review focused upon the clarity of the information presented; the accuracy of the operations upon requirements; the sufficiency of SFRs to satisfy the security objectives; and the validity of the requirements as a set.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_REQ.1, resulting in a verdict of PASS.

4.1.7 ASE_SRE.1

No explicitly stated IT security requirements were specified for this ST.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_SRE.1, resulting in a verdict of PASS, trivially.

4.1.8 ASE_TSS.1

The evaluation team reviewed the TOE Summary Specification to determine that the TSS meets the requirements and represents the TOE.

The TSS provides a high level definition of the security functions and assurance measures. This is done through the explanatory text for each function.

Each security function maps to at least one security functional requirement. The team validated this by performing a mapping between each TSS security function and the security functional requirements.

The TSS uses an informal style and contains details necessary for understanding the security functions intent. The team determined this by reading the text provided in the TSS.

The evaluation team concluded that the nature of the TSS organization ensures that all security mechanisms mentioned are traced back to a security function.

The TSS contains an appropriate justification for each security function. The evaluation team validated this by analyzing each justification and determining that each security function is appropriately rationalized. The justifications provided demonstrate that the IT security functions are adequate to address the security functional requirements.

The TSS rationale is found to be consistent for the SOF for the Security Functional Requirements. The evaluation team determined that the SOF claim for the authentication mechanism is identical to the SOF for the SFR.

The TSS rationale describe how the IT security functions meet the security functional requirements. The evaluation team verified that each assurance measure is traced to at least one TOE security assurance requirement. The TSS rationale demonstrates that the assurance measures meet the TOE security assurance requirements.

The TSS points out the probabilistic mechanism specified for this ST is part of the I&A security function. While this isn't explicitly stated, it is indicated by the corresponding SOF claim. The only SOF claim in the TSS applies to the I&A security function. A claim of SOF-basic is made for this security function.

The TSS is complete, coherent and internally consistent. The measurement of completeness, coherency and consistency was performed by iterative review of the TOE Summary Specification. This review focused upon the description of security functions and how they correspond to all SFR's; and the review of the requirements to determine if there are any contradictions.

Verdict: The evaluation team has determined that the Security Target meets the requirements specified for ASE_TSS.1, resulting in a verdict of PASS.

4.2 CLASS ACM – CONFIGURATION MANAGEMENT

4.2.1 ACM_CAP.2

The evaluation team reviewed the evidence presented as the CM document. This document contains the justification that the vendor has performed due diligence in regard to configuration management.

The evaluation team checked that the version of the TOE provided for evaluation is uniquely referenced. The team determined that the TOE is referenced as SunScreen EFS 3.0 Revision B.

The evaluation team checked that the TOE provided for evaluation is labeled with its reference. The team verified the existence of this reference by reviewing the product as it is delivered, including the software CD-ROM, the manuals included in the shrink wrap box and the administrative interface following installation. The TOE reference is also available via a query of the executing TOE software.

The evaluation team checked that the TOE references used are consistent. This consistency checking was performed throughout the evaluation, including document reviews and interaction with the TOE during testing.

The evaluation team confirmed that the CM documentation provided includes a configuration list. This configuration list was reviewed and quantified by the team.

The evaluation team confirmed that the configuration list identifies the configuration items that comprise the TOE. This check was performed by reviewing the ST and determining if what was specified as the TOE was tracked on the configuration list. Additional assurance was gained during testing activities, when the team closely interacted with the TOE by installing and configuring it.

The evaluation team examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified. The evaluation team checked that the configuration list uniquely identifies each configuration item.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ACM_CAP.2, resulting in a verdict of PASS.

4.3 CLASS ADO - DELIVERY AND OPERATIONS

4.3.1 ADO_DEL.1

The evaluation team examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user's site.

The evaluation team examined the delivery procedures and determined that the chosen procedure and the part of the TOE it covers are suitable to meet the security objectives. This exercise

examined the security objectives specified in the ST and analyzed the delivery procedures to ensure that all the objectives were covered.

The evaluation team examined the aspects of the delivery process and determined that the delivery procedures are used. The evaluation team ordered a copy of the SunScreen EFS 3.0 Revision B firewall and received it via a shipping company.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ADO_DEL.1, resulting in a verdict of PASS.

4.3.2 ADO_IGS.1

The evaluation team checked that the procedures necessary for the secure installation, generation and start-up of the TOE were provided. The team verified that the vendor delivered the IGS document. This TOE has a collection of documents that make up the secure installation, generation and start-up instructions.

The evaluation team examined the provided installation, generation, and startup procedures and determined that they describe the steps necessary for secure installation, generation and start-up of the TOE. The team performed an initial review of the document and performed a more thorough review during team testing. During team testing, the team used the IGS documents to bring up the TOE in the evaluated configuration. Comments were issued to the vendor to improve the IGS documents, as a result of the team test.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ADO_IGS.1, resulting in a verdict of PASS.

4.4 CLASS ADV – DEVELOPMENT ACTIVITY

4.4.1 ADV_FSP.1

The evaluation team examined the functional specification and determined that it contains all necessary informal explanatory text. This work unit was considered to be not applicable, because the entire FSP is informal.

The evaluation team examined the functional specification and determined that it is internally consistent. This consistency review was performed throughout our analysis of the FSP, and was closed when the vendor had addressed all of our comments.

The evaluation team examined the functional specification and determined that it identifies all of the external TOE security function interfaces. The evaluation team performed an analysis and generated a list of additional interfaces that had not been initially considered by the vendor. The vendor and the team had follow-up discussions and concluded that some of the teams suggested interfaces should be included and some should not.

The evaluation team examined the functional specification and determined that it describes all of the external TOE security function interfaces.

The evaluation team examined the presentation of the TSFI and determined that it adequately and correctly describes the behavior of the TOE at each external interface describing effects, exceptions and error messages.

The evaluation team examined the functional specification and determined that the TSF is fully represented. This representation analysis was performed by reviewing the User Guide, the Admin Guide, and the TSS section of the ST. The evaluation team applied their understanding of the product to the TSF. This analysis used the team's search for other external interfaces as a basis to determine that the TSF was fully represented.

The evaluation team examined the functional specification and determined that it is a complete instantiation of the TOE security functional requirements. The team's purpose in judging completeness is to ensure that all ST security functional requirements are covered by the Functional Specification. The analysis was performed by reviewing the TSS section of the ST and creating a map between the TSS and the FSP.

The evaluation team examined the functional specification and determined that it is an accurate instantiation of the TOE security functional requirements. The team's purpose in judging accuracy is to determine that the detail information in the Functional Specification is exactly as it is specified in the ST. The analysis was performed by reviewing the TSS section of the ST and creating a map between the TSS and the FSP. Performing the mapping allowed the team to correlate the information in the TSS with the FSP. The mapping indicated completeness, but the process involved in creating the mapping let the team to conclude that the FSP accurately instantiated the TSS.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ADV_FSP.1, resulting in a verdict of PASS.

4.4.2 ADV_HLD.1

The evaluation team examined the high-level design and determined that it contains all necessary informal explanatory text. The entire high-level design is informal, so this unit (ADV_HLD.1-1) is not applicable.

The evaluation team examined the presentation of the high-level design and determined that it is internally consistent. This consistency review was performed throughout our analysis of the HLD, and was closed when the vendor had addressed all of our comments.

The evaluation team examined the high-level design and determined that the TSF is described in terms of subsystems. The evaluation team examined the high-level design and determined that it describes the security functionality of each subsystem.

The evaluation team checked the high-level design to determine that it identified all hardware, firmware, and software required by the TSF. The team interpreted this requirement to mean that the hardware, software or firmware that are being identified must also include those which are part of the IT security environment. The team came to this conclusion based on text provided in the CEM for

ADV_FSP.1-8. The team determined that the hardware, software and firmware required by the TSF were identified in the HLD.

The SecurID server is identified as a component that the TSF relies upon. The HLD refers to an external ACE Server. The ACE Server is not limited by a hardware base. It is a software package, Ace/Server version 3.0.1 and greater.

The evaluation team examined the high-level design and determined that it includes a presentation of the functions provided by the supporting protection mechanisms in the underlying hardware, firmware, or software. This included information pertaining to functions provided by the supporting protection mechanisms within the TOE. It also includes functions provided by the supporting protection mechanisms in the IT environment (e.g. SecurID pin and token code authentication features).
The evaluation team checked that the high-level design identifies the interfaces to the TSF subsystems and determined that the identification is properly presented.

The evaluation team checked that the high-level design identifies which of the interfaces to the subsystems of the TSF are externally visible. The HLD presented for this evaluation outlines external interfaces.

The evaluation team examined the high-level design and determined that it is an accurate instantiation of the TOE security functional requirements. The team's purpose in judging accuracy of the HLD is to ensure that each security function is accurately described and that there are no inconsistencies between the TOE SFR's and the IT requirements for the environment. The analysis was performed by reviewing the TSS section of the ST and creating a map between the TSS and the HLD. Performing the mapping allowed the team to correlate the information in the TSS with the HLD. The mapping indicated completeness, but the process involved in creating the mapping let the team to conclude that the HLD accurately instantiated the TSS.

The evaluation team examined the high-level design and determined that it is a complete instantiation of the TOE security functional requirements. The team's purpose in judging completeness of the HLD is to verify that the ST security functional requirements are covered by the HLD. The analysis was performed by reviewing the TSS section of the ST and creating a map between the TSS and the HLD. Performing the mapping allowed the team to correlate the information in the TSS with the HLD. The mapping indicated completeness.
Verdict: The evaluation team has determined that the TOE meets the requirements specified for ADV_HLD.1, resulting in a verdict of PASS.

4.4.3 ADV_RCR.1

The evaluation team examined the correspondence analysis between the TOE summary specification and the functional specification and determined that the functional specification is a correct and complete representation of the TOE security functions. This analysis was performed by reviewing the RCR and validating that the TSS and the functional specification created a correct and complete representation of the TOE security functions. Deficiencies were found and

reported to the vendor. The vendor addressed the deficiencies, which resulted in a correct and complete representation of the TOE security functions.

The evaluation team examined the correspondence analysis between the functional specification and the high-level design and determined that the high-level design is a correct and complete representation of the functional specification. The team created a map between the FSP and HLD. The team compared this map to the RCR and deficiencies were found and reported to the vendor. The vendor addressed the deficiencies, which resulted in a correct and complete representation of the functional specification.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ADV_RCR.1, resulting in a verdict of PASS.

4.5 CLASS AGD - GUIDANCE DOCUMENTATION

4.5.1 AGD_ADM.1

The evaluation team examined the administrator guidance and determined that it describes the administrative security functions and interfaces available to the administrator of the TOE. The administrator guidance for the TOE is made up of the Sun EFS 3.0 Revision B Administrator Guide, the Sun EFS 3.0 Revision B Reference Manual, the Sun EFS 3.0 Revision B Administrator Guide Addendum, the Sun EFS 3.0 Revision B Installation Guide and the Solaris 2.6/Solaris 2.7 System Administration Manuals. Between all of these manuals, the administrator guidance describes the security functions and interfaces available to the administrator of the TOE.

The evaluation team examined the administrator guidance and determined that it describes how to administer the TOE in a secure manner. The Sun EFS 3.0 Administrator Guide provides a description of what an administrator needs to do to operate a secure firewall. The guide takes them through what a firewall is and covers how to decide what users, services and rules are required for their installation. The Administrator Guide also covers secure use of the TOE through the GUI and command line administrative interfaces.

The evaluation team examined the administrator guidance and determined that it contains warnings about functions and privileges that should be controlled in a secure processing environment. The Administrator Guide Addendum contained the warnings that the administrators need to be aware of.

The evaluation team examined the administrator guidance and determined that it describes all assumptions regarding user behavior that are relevant to the secure operation of the TOE. The administrator guide references the Sun EFS 3.0 User Guide Addendum as the location of the assumptions regarding user behavior. The evaluation team determined that these assumptions about user behavior were adequate to satisfy this work unit.

The evaluation team examined the administrator guidance and determined that it describes all security parameters under the control of the administrator indicating secure values as appropriate.

The evaluation team examined the administrator guidance and determined that it describes each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. The list of security relevant events is contained within the Sun EFS 3.0 Revision B Administrator Guide Addendum.

The evaluation team examined the administrator guidance and determined that it is consistent with all other documents supplied for evaluation. The team generated a list of consistency comments that were addressed by the vendor. These comments included updates to the administrator guide requested by the team to better notify the administrator to issues dealing with secure administration of the TOE.

The evaluation team determined that the administrator guidance includes warnings about the security concerns for the alternate authentication mechanisms provided by the IT environment. These warning are consistent with the IT security requirements for the environment found in the ST.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for AGD_ADM.1, resulting in a verdict of PASS.

4.5.2 AGD_USR.1

The evaluation team examined the user guidance and determined that it describes the security functions and interfaces available to the non-administrative users of the TOE.

The evaluation team examined the user guidance and determined that it describes the use of user-accessible security functions provided by the TOE.

The evaluation team examined the user guidance and determined that it contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. The evaluation team determined that there are no warnings provided in user guidance. There are very limited things a user can do within this TOE. The main interaction the user has with the TOE is through a proxy. There are no warnings about the operation of proxies from a user perspective, and the evaluation team feels that none are justified.

The evaluation team examined the user guidance and determined that it presents all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

The evaluation team examined the user guidance and determined that it is consistent with all other documentation supplied for evaluation.

The evaluation team examined the user guidance and determined that the requirements for the IT environment do not affect the advice to the users of this TOE.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for AGD_USR.1, resulting in a verdict of PASS.

4.6 CLASS ATE - TESTS

4.6.1 ATE_COV.1

The evaluation team examined the test coverage evidence and determined that the correspondence between the tests identified in the test documentation and the functional specification is accurate. The entire team performed coverage analysis, by splitting the requirements and analyzing the vendor test coverage for all of the functional requirements. EAL2 does not require the vendor test coverage to be complete. The vendor test suite tended to be weakest in the area of testing administrative roles. The team augmented its own set of tests to augment all areas with weak or incomplete vendor coverage. The vendor test suite when combined with the team test suite provided complete coverage of the security functional requirements.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ATE_COV.1, resulting in a verdict of PASS.

4.6.2 ATE_FUN.1

The evaluation team checked that the test documentation includes test plans, test procedure descriptions, expected test results and actual test results. The test plan was provided by the vendor as a collection of HTML documents. The vendor submitted an entire test suite, including the test plan, test matrices and the test results. This test suite is a hierarchical collection of directories that split the test suite into functional components. Additional files within the directories contained information that is considered part of the vendors' test plan. These additional files specified test procedure descriptions and any setup considerations that were necessary to complete a test case. The test procedure descriptions included sufficient detail to also serve as test procedures.

Actual test results and expected test results are included within the test suite. Some test cases did not specify expected test results, due to the simplicity of the test case. The evaluation team accepted this because the expected test results could be easily inferred.

The evaluation team checked that the test plan identified the security functions to be tested. The evaluation team examined the test plan and determined that it describes the goal of the tests performed. Each goal is specified in the test design document for each test. During the review for test coverage, the team sampled the test cases for each functional requirement.

The evaluation team examined the test plan and determined that the TOE test configuration is consistent with the configuration identified for evaluation in the ST. The evaluation team compared the TOE test configuration found in the Sun test plan with the TOE described in the ST. The team determined that the configuration used for functional testing by Sun was consistent with the ST.

The evaluation team examined the test plan and determined that it is consistent with the test procedure descriptions. The test plan and test procedures are consistent. Sampling was performed by looking at the test cases and using representative examples from each of the test areas.

The evaluation team checked that the test procedure descriptions identified each security function behavior to be tested. The security function behaviors to be tested are enumerated in the test procedure descriptions. While this is not perfect, and is not always spelled out, it can be inferred by the name of the test cases and other evaluator knowledge. Sampling was performed by looking at the test cases and using representative examples from each of the test areas.
The evaluation team examined the test procedure descriptions and determined that sufficient instructions are provided to establish reproducible initial test conditions including ordering dependencies if any. The Sun test procedure descriptions were used to determine this information.

The evaluation team examined the test procedure descriptions and determined that sufficient instructions are provided to have a reproducible means to stimulate the security functions and to observe their behavior. The team reviewed the test procedure descriptions and the test plan and determined that sufficient instructions are provided.

The evaluation team examined the test procedure descriptions and determined that they are consistent with the test procedures. The test procedure descriptions and test procedures are identical for this TOE.

The evaluation team examined the test documentation and determined that sufficient expected tests results are included. Expected test results could be deduced from the test plan, the test procedure descriptions and the test matrices.

The evaluation team checked that the expected test results in the test documentation are consistent with the actual test results provided. The team determined that a pass result in the test matrices indicates that the actual and expected results are the same.

The following paragraphs are a report of the developer testing effort, outlining the testing approach, configuration, depth and results.

Sun's focus for the EFS v3.0 test run was to add testing for the new features of the product. The existing product features were tested by test cases that already existed within the test suite.

The new features that were included and tested in EFS 3.0 are:

- Centralized Management of Multiple Screens
- Administrative Roles for READ , WRITE and ALL
- Improved Java GUI
- New Command Line Interface
- Enhanced Log Management
- Time Based Rules

- New NAT
- Merge of SPF and EFS Proxies for HTTP, SMTP, FTP and Telnet Installation using Solaris Web Start
- Other non-security related product enhancements.

All the features described in the bulleted list above were tested following the Test Design and Test Case documents to verify correct behavior. These tests were performed manually for most of the areas since at the time of the test runs there were only limited automations in place.

The configuration tested by the vendor included a mix of SPARC and x86 systems running both the Solaris 2.6 and Solaris 2.7 operating system.

The goal of Sun's test effort was to document the planned Quality Assurance activities. SunScreen EFS v3.0 progressed through an Alpha release, and several Beta release builds, prior to First Commercial Ship (FCS). QA did not perform regression testing for every beta release build of the product after the code freeze. Once an area was tested, Sun did not retest unless there were changes to the modules due to a bug fix.

- Test results were recorded using a format designated by Sun. Fields exist within to clearly indicate the Pass/Fail status of a test as well as a BugID if necessary. Sun's main goal is to catch all the bugs as early as possible. The full QA test cycle must be completed for before FCS. The goal for FCS is to deliver software with no programming errors and the product functioning as specified.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ATE_FUN.1, resulting in a verdict of PASS.

4.6.3 ATE_IND.2

The evaluation team examined the TOE and determined that the test configuration is consistent with the configuration under evaluation as specified in the ST. The equipment used for testing consisted of both SPARC and Intel hardware platforms, running the Solaris 2.7 operating system. These hardware platforms are identified in the ST.

The evaluation team examined the TOE and determined that it has been installed properly and is in a known state. The team followed the instructions for installation provided by the IGS documentation during the setup and installation of the testing platform.

The evaluation team examined the set of resources provided by the developer and determined that they are equivalent to the set of resources used by the developer to functionally test the TSF. The equipment used by the team for testing consisted of both SPARC and Intel hardware platforms with equivalent to those used by the vendor during its testing effort. The evaluation team also had Solaris 2.6 and 2.7 software configurations available for its testing effort.

The ST's describes multiple hardware platforms, operating systems and operating modes for which this evaluation applies. The team did not test all combinations of these configurations, instead the team attempted to get a sampling of these configurations. The team performed testing on both hardware platforms using only Solaris 2.7. Solaris 2.6 was not part of the team testing configuration. Solaris 2.6 was not tested by the evaluation team because operating system drivers were not available for the equipment in the team's hardware testing platforms. The team felt that this was acceptable for several reasons. First, the vendor performed testing of EFS 3.0 against both Solaris 2.6 and 2.7 configurations, and provided evidence of this testing to the team. Second, Solaris' role is to provide EFS with a software environment that allows EFS to run on either an Intel or SPARC hardware platform (and with a variety of network cards). Thus, the value of the evaluation team testing each operating system (or each network card) is very limited.

Configuration Name	Hardware Platform	Software Platform	Firewall Mode
Routing Standalone	Intel	Solaris 2.7	Routing Mode
Stealth Standalone	SPARC	Solaris 2.7	Stealth Mode
Routing HA	SPARC	Solaris 2.7	Routing Mode

The following hardware was used during testing of the actual TOE.

- Gateway G6 – 333c (Used as the Intel Routing Mode firewall)
- Two Sun Ultra 1 systems (One used as Administration station, one used as a firewall)
- Sun Ultra 2 (Used as the secondary, passive firewall during the HA test

The evaluation team test plan included a subset of vendor tests. The set of vendor tests that the evaluation team repeated included both automated and manual tests. The subset of tests repeated by the evaluation team exercised the remote and local administration capabilities of the firewall.

The evaluation team produced test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible. The "SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report" describes the configurations exercised during team testing, the team tests performed, the vendor tests repeated, the team vulnerability testing and the results observed from all testing. The evaluation team ran all tests described in chapter 6 of the "SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report" against a Routing Mode screen and against a Stealth Mode screen. Team testing occurred on stand-alone screens and on high availability screen clusters.

The evaluation team conducted testing. Testing occurred at the lab's testing facility and included team test plan development, hardware setup, software installation, configuration troubleshooting, and actual test execution. Since multiple network configurations were tested, the installation process was repeated several times. Despite this, the actual test execution accounted for a majority of time dedicated to hands on testing. Also, the time necessary for installation and testing accounted for almost two thirds of the teams test effort. That is, team test plan

development, hardware setup and configuration troubleshooting consumed less than one third of the time the team dedicated to testing. Each configuration described in the “SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report” was exercised during team testing.

The evaluation team recorded the following information about the tests that compose the test subset: a) identification of the security function behavior to be tested; b) instructions to connect and setup all required test equipment as required to conduct the test; c) instructions to establish all prerequisite test conditions; d) instructions to stimulate the security function; e) instructions for observing the behavior of the security function; f) descriptions of all expected results and the necessary analysis to be performed on the observed behavior for comparison against expected results. This information was documented in the “SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report”.

The evaluation team checked that all actual test results from both the team and the vendor tests performed during the team testing effort, are consistent with the expected test results. That is, the team observed that the actual results from testing (including both new team tests and repeated vendor tests) matched the expected results.

The evaluation team confirmed that vendor testing results were valid by executing a random sample of vendor tests. The team also exercises many of the security mechanisms described by the Security Target using independently derived tests. The team testing when viewed in combination with vendor tests exercised all security mechanisms and provided complete coverage of the security functional requirements.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for ATE_IND.1, resulting in a verdict of PASS.

4.7 CLASS AVA - VULNERABILITY ASSESSMENT

4.7.1 AVA_SOF.1

The evaluation team checked that the developer has provided a SOF analysis for each security mechanism for which there is a SOF claim in the ST expressed as a SOF rating. A rating of SOF-BASIC is provided in the ST. The CC states: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential".

The team reviewed the SOF Analysis provided by the vendor and found that all mechanisms with a SOF claim provide protection against casual breach of TOE security by attackers possessing a low attack potential. The team based this upon a presumption that such attackers would primarily base their attacks on repetitive (possibly systematic) use of a mechanism rather than detailed analysis of the fundamental properties of the mechanism. Thus, if an attacker could make N guesses before the mechanism resets (e.g. a password change event) then the name space for the mechanism must be N*10^6 (i.e. a probability of 1 in one million).

The evaluation team checked that the developer has provided a SOF analysis for each security mechanism for which there is a SOF claim in the ST expressed as a metric.

The evaluation team examined the SOF analysis and determined that any assertions or assumptions supporting the analysis are valid.

The evaluation team examined the SOF analysis and determined that any algorithms, principles, properties and calculations supporting the analysis are correct.

The evaluation team examined the SOF analysis and determined that each SOF claim is met or exceeded.

The evaluation team examined the SOF analysis and determined that all functions with a SOF claim meet the minimum strength level defined in the ST.

The evaluation team examined the functional specification, the high-level design, the user guidance and the administrator guidance to determine that all probabilistic or permutational mechanisms have a SOF claim.

The evaluation team examined the SOF claims to determine that they are correct.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for AVA_SOF.1, resulting in a verdict of PASS.

4.7.2 AVA_VLA.1

The evaluation team examined the developer's vulnerability analysis and determined that the search for obvious vulnerabilities has considered all relevant information. The vendor's analysis focused primarily on a search for vulnerabilities in public sources. It also included analysis of vulnerabilities that the product was designed to counter.

The evaluation team examined the developer's vulnerability analysis and determined that each obvious vulnerability is described and that a rationale is given for why it is not exploitable in the intended environment for the TOE.

The evaluation team examined the developer's vulnerability analysis and determined that it is consistent with the ST and the guidance. The TOE as described by the ST and configured per the installation instructions, and operated per the administration guidance is capable of countering the vulnerabilities identified in the vulnerability analysis.

The evaluation team devised penetration tests, building on the developer vulnerability analysis. The evaluation team's penetration tests concentrated upon attacks aimed at compromising the firewall through network protocols.

The evaluation team produced penetration test documentation for the tests that build upon the developer vulnerability analysis, in sufficient detail to enable the tests to be repeatable. The test

documentation included: a) identification of the obvious vulnerability the TOE is being tested for; b) instructions to connect and setup all required test equipment as required to conduct the penetration test; c) instructions to establish all penetration test prerequisite initial conditions; d) instructions to stimulate the TSF; e) instructions for observing the behavior of the TSF; f) descriptions of all expected results and the necessary analysis to be performed on the observed behavior for comparison against expected results; g) instructions to conclude the test and establish the necessary post-test state for the TOE.

The evaluation team conducted penetration testing, building on the developer vulnerability analysis. The evaluation team did not attempt to exploit any of the vulnerabilities identified in the developer's analysis. Rather, the team focused upon extending the penetration testing into new areas.

The evaluation team recorded the actual results of the penetration tests. These results are included in a separate chapter in the "SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report".

The evaluation team examined the results of all penetration testing and the conclusions of all vulnerability analysis to determine that the TOE, in its intended environment, has no exploitable obvious vulnerabilities. The TOE as described by the ST and configured per the installation instructions, and operated per the administration guidance is capable of countering the vulnerabilities identified in the vulnerability analysis.

The evaluation team recorded the penetration testing approach, test configuration, depth and results in the "SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Team Test Report".

The evaluation team discovered no exploitable vulnerabilities.

Verdict: The evaluation team has determined that the TOE meets the requirements specified for AVA_VLA.1, resulting in a verdict of PASS.

5. CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is a Pass.

This ST was not conformant with any Protection Profile.

5.2 RECOMMENDATIONS

None

6. LIST OF EVALUATION EVIDENCE

The following table outlines the evaluation evidence. The issuing body for all of the documentation was Sun Microsystems.

Title	Unique Reference	ETR Reference
SunScreen EFS 3.0 Revision - Stealth ST	Arca LTEF 002/2000-SUN Stealth Mode Security Target	[ST]
Sun Microsystems SunScreen™ EFS 3.0 Revision B Configuration Management	Arca LTEF 010/2000 Sun CM Final Version 1.0	[CM]
Sun Microsystems SunScreen™ EFS 3.0 Revision B Delivery Procedures	Arca LTEF 009/2000 Sun DEL Final Version 1.0	[DEL]
SunScreen™ EFS 3.0 Revision B - Installation Guide	Arca LTEF 019/2000 Sun IG Final Version 1.0	[IGS]
SunScreen™ EFS 3.0 Revision B - Administrator Guide	Arca LTEF 020/2000 Sun AG Final Version 1.0	[ADMA]
SunScreen™ EFS Release 3.0 Installation Guide	Revision B Part #805-7746-11	[IGS]
SunScreen™ EFS Release 3.0 Administration Guide	Revision B Part #805-7745-11	[ADM]
SunScreen™ SKIP User's Guide	Release 1.5 Revision B part #805-7875-11	[SKIPUG]
SunScreen™ EFS 3.0 Revision B - User Guide	Arca LTEF 018/2000 Sun UG Final Version 1.0	[USR]
Binary Code License		[BCL]
Start Here		[SH]
Release Notes		[RN]
Solaris ™2.6 man pages	N/a	[MAN26]
Solaris™ 2.7 man pages	N/a	[MAN27]
SKIP™ man pages.	N/a	[SKIPMAN]
Solaris 2.6 System Administration: Volume I	802-5750–10 August 1997	[SAG26]
Solaris 2.7 System Administration: Volume I	805-3727–10 October 1998	[SAG271]
Solaris 2.7 System Administration: Volume II	805-3728–10 October 1998	[SAG272]
SunScreen™ EFS 3.0 Revision B Stealth Mode Operation Security Functional Specification	Arca LTEF 014/2000 Sun SMSFS Final Version 1.0	[FSP]
SunScreen™ EFS 3.0 Revision B Stealth Mode Operation High-Level Design	Arca LTEF 013/2000 Sun SMHLD Final Version 1.0	[HLD]
SunScreen™ Technical White Paper.	Copyright 1999	[HLDWP]

SunScreen™ EFS 3.0 Revision B Stealth Mode Operation Representation Correspondence	Arca LTEF 015/2000 Sun SMRCR Final Version 1.0	[RCR]
Reference Manual	Part #805-7746-11	[RM]
SunScreen EFS 3.0 Test Coverage Document	1.0	[TC]
SunScreen EFS 3.0 Test Plans	3.0	[TP]
SKIP 1.5 Test Plans	1.5	[SKIPTP]
TOE Deliverable	3.0	[TOE]
Sun Microsystems SunScreen™ EFS 3.0 Revision B Strength of Function	Arca LTEF 008/2000 Sun SOF Final Version 1.0	[SOF]
SunScreen™ EFS 3.0 Revision B - VLA - Vulnerability Analysis	Arca LTEF 017/2000 Sun VLA Final Version 1.0	
Hardware Compatibility List for Solaris 2.6	April 2000	[HCL2.6]
Solaris 2.7 Hardware Compatibility List	June 2000	[HCL2.7]
SunScreen EFS 3.0 Revision B Routing and Stealth Mode Evaluation Testing Report	Arca LTEF 005/2000 - Test Reference	[TR]
SunScreen EFS 3.0 Revision B- Stealth	Arca LTEF 007/2000-SUN Stealth Mode Product Bulletin	[PB]

7. LIST OF ACRONYMNS

ATM	Asynchronous Transfer Mode
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
DLPI	Data Link Provider Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FDDI	Fiber Distributed Data Interface
FCS	First Commercial Ship
FSP	Functional Specification
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability
HLD	High Level Design
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
JVM	Java Virtual Machine
Mbps	Megabit Per Second
NAT	Network Address Translation
NIC	Network Interface Card
OR	Observation Report
P1,P2,P3	Software Bug Severity Levels
PCI	Peripheral Connect Interface
PIN	Personal Identification Number
QA	Quality Assurance
RADIUS	Remote Authentication Dial-In User Service
SKIP	Simple Key-management for Internet Protocols
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEF	Trusted Evaluation Facility
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VPN	Virtual Private Network

8. OBSERVATION REPORTS

OR Identifier	Brief Summary	Status
OR-SUNEFS-001	If Sun's cryptographic module is not FIP 140-1 Level 1 certified, is the only other option to remove FCS_COP.1 from our ST, in the way that Cisco did for the PIX evaluation? Sun provides SKIP encryption, but it has not yet been validated against FIPS 140-1.	Closed
OR-SUNEFS-002	FIA_UAU.4 - Strength of Function shall be demonstrated for the single-use authentication mechanism(s) by demonstrating compliance with the Statistical random number generator tests and the Continuous random number generator test found in section 4.11.1 of FIPS PUB 140-[5]. Does this statement mean that the strong authentication mechanism included in a TOE must be FIPS 140-1 certified before it can be included or does it have to be designed to meet FIPS 140-1 certification?	Closed
OR-SUNEFS-003	Sun would like to include the widest possible base of hardware configurations for this TOE. We believe Sun should only need to perform functional testing against a representative sample of the hardware included in the TOE.	Closed
OR-SUNEFS-004	Arca is suggesting that we write the Security Target to say that the EFS 3.0 product is compliant with the Application FW PP when operating in routing mode, and is compliant with the Traffic Filter FW PP when operating in stealth mode.	Closed