

Table of Contents

- 1 Introduction
- 2 SecureOffice WebShield Benefits
- 2 SecureOffice WebShield Features
- 2 Key Components for Secure Web Browsing
- 3 Architecture
- 3 Implementation
- 3 Certification and Accreditation
- 4 Hardware Requirements and Supporting Configurations
- 4 Conclusion

Technical Abstract

SecureOffice WebShield

Introduction

A SecureOffice Cross-Domain Transfer Solution

Today, mission-critical resources are delivered over the Internet along with e-commerce applications, news, email, and numerous other software applications and Internet services. With the proliferation of web-based resources and services comes the risk of web-based attacks, which can lead to the leaking of confidential information. Internet servers that connect private and public systems and information can become a potential gateway to corporate proprietary and confidential data (for example, personnel, financial, project, and security information). In the ongoing protection of national security, government workers require secure access to the information contained on web sites at various classification levels.

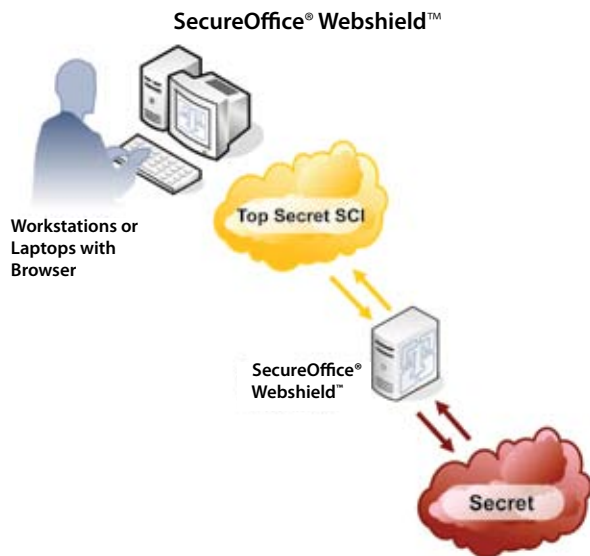
Trusted Computer Solutions (TCS) developed the SecureOffice® WebShield™ (MDDS)¹ Cross-Domain Solution to provide browse-down capabilities from high classification domains to lower classified and unclassified domains. WebShield allows you to transparently protect your entire network (i.e., not just a single local server), while maintaining the current server infrastructure.

SecureOffice WebShield was designed to meet and exceed the requirements for a Protection Level 4 (PL4) system under the Director of Central Intelligence Directive 6/3 (DCID 6/3) and Department of Defense (DoD) Information Assurance Certification and Accreditation Program (DIACAP). The technical design is based on secure systems engineering practices and trusted operating system security enforcement at the server level.

Trusted operating systems extend the capabilities found in standard operating systems by providing additional safeguards against internal and external threats. The employment of Discretionary Access Controls (DAC), Mandatory Access Controls (MAC), Multi-Level Security (MLS), and Type Enforcement (TE) offers powerful and customizable levels of protection for users and data. Additional security policy enforcement mechanisms are required to meet the “trusted” designation and include protection profiles that must be engineered in the operating system. These protection profiles include Labeled Security Protection Profile (LSPP), Controlled-Access Protection Profile (CAPP), and Role-Based Access Control (RBAC). The combination of these security attributes provides full segregation and protection of all data on the system.

SecureOffice WebShield runs on the Red Hat® Enterprise Linux® version 5 (RHEL5) operating system. RHEL5 is the first secure Linux operating system to receive an Evaluation Assurance Level 4 (EAL4) under the National Information Assurance Partnership (NIAP) against the Common Criteria requirement associated with Cross-Domain Solutions, which includes LSPP, CAPP, and RBAC protection profiles.

¹MDDS, Multi Domain Dissemination System, is another name for WebShield as listed on the Unified Cross-Domain Management Office (UCDMO) approved list.



SecureOffice WebShield Features

The key attributes of SecureOffice WebShield include a host of security and manageability features.

Security:

- Active content filtering; such as, Java Applets, Java™ Scripts, ActiveX™, and other Multi-purpose Internet Mail Extensions (MIME) types
- Complete file protection and management to include virus scan (optional), file type, dirty word search, archive, and audit policies
- Strong authentication support using DoD/IC PKI (X.509 digital certificates)
- Secure Sockets Layer (SSL) connections to the client to provide privacy
- Runs on the EAL4+ NIAP certified RHEL5 operating system
- Strengthened security from pairing the SELinux TE and MLS security models
- Configurable archive and auditing processes

Manageability:

- User access through standard Internet Explorer, Firefox, or Netscape browsers
- Requires no software installation on user's workstation
- Wide range of commodity hardware supported
- Operates on a mainstream, open source operating system
- Complete archive and audit management capabilities

Key Components for Secure Web Browsing

Active Content Blocking

Responses from the server(s) can be scanned to identify and remove a wide range of active content. WebShield can be configured to block Java, Java Script, ActiveX and other kinds of active content (or mobile code). This prevents a data driven attack from a low side server.

Content Filtering

SecureOffice WebShield performs bi-directional content filtering with configurable filters that scan user requests and server responses based on security parameters established by the system administrator. Forms and URL strings in all user requests are scanned prior to transmission to the lower-level server. If any outgoing data breaches the site's security policy, the request is rejected. All server replies are carefully scrutinized before forwarding to the user.

SecureOffice WebShield Benefits

SecureOffice WebShield provides benefits for Budget Stakeholders, Administrators, Security Officers, and Certification and Accreditation Officers.

For **Budget Stakeholders**, SecureOffice WebShield provides a low total cost of ownership (TCO) by using commodity hardware and requiring minimal training and maintenance costs. Current staff can easily support SecureOffice WebShield, with no additional engineering resources required to manage or maintain the implementation(s). SecureOffice WebShield is installed on a single server that runs the open, mainstream RHEL5 operating system, offering lower-priced hardware platform choices to further reduce the TCO over proprietary and government-developed systems.

Administrators benefit from a low-maintenance solution that enforces security requirements. Internet Explorer®, Firefox®, and Netscape® customers can use their current browsers, eliminating additional product support requirements. Full support of DoD and Intelligence Community (IC) Public Key Infrastructure (PKI) means that current systems do not require duplication.

SecureOffice WebShield requires a trusted operating system as the mechanism for security policy enforcement and meets **Security Officer**, agency, and accreditor requirements for secure web browsing. All processing is performed at the level of the incoming information; therefore, the user request is pro-

cessed at the high side level and the server response is processed at the server level. All requests go through Dirty Word Search, and all responses go through virus scan and malicious content checking.

Security Officers can use WebShield to control where users go and the types of data users retrieve. Users surfing lower-level networks can be restricted to servers defined by security policies. Organizations can also place restrictions on the low-side network to limit data accessed by high-side users. The WebShield Strong Authentication implementation requires user authentication using a Department of Defense (DoD) X.509 Digital Certificate and user ID/password before accessing the destination web site.

Certification and Accreditation Officers

benefit from simple, cost-effective accreditation processes that are both attainable and repeatable. From inception, the SecureOffice WebShield development team involved government certifiers and designed the product to meet the stringent security policies for Cross-Domain Solutions. TCS has fielded hundreds of applications that are part of accredited systems and has engineered its products to satisfy Cross-Domain Security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) Cross-Domain Solutions C&A processes.

WebShield is accredited in operational systems worldwide and is the browse-down component of the Defense Intelligence Agency's (DIA) Multi-Domain Dissemination System (MDDS).

Dirty Word Search

SecureOffice WebShield Dirty Word Search scans user requests for sensitive or “dirty” words that should not be viewable on the low side network. The process ignores spaces, carriage returns, and other formatting information. Therefore, if “Top Secret” is listed as a dirty word, “T O P S E C R E T” and other variations are identified. Dirty words can span lines, contain embedded white space, and be embedded within other words. If dirty words are found the request is denied and logged.

The Dirty Word Search module also allows for the designation of “clean” words, which are common words that contain within them dirty words. For example, the word “secretary” contains the word “secret” but it is considered a false positive and can be ignored. Administrators can create and customize a master list of both dirty and clean words, as well as create lists that are specific to different configuration contexts. This is needed in cases where text might be in different encoded formats.

File Type Verification

Three different varieties of file type checking are employed in SecureOffice WebShield. Extension matching, TCS signature algorithm, and the Universal Atomic Disintegrator (UAD) algorithm from CyberSoft™ allow user-configurable file type verification options. The file verification signatures can be customized to accommodate unique file types, configured by both source and destination policies.

Virus Scanning

SecureOffice WebShield incorporates CyberSoft VFind™ to scan files. WebShield can also be customized to exclude certain trusted types from virus scanning to enhance performance.

Architecture

WebShield is a web proxy that protects internal clients that access external resources. Internal clients attempting to access an external web server (e.g., on SIPRNET) must first go through WebShield. All web-based traffic is filtered and logged by WebShield, which provides identification and authentication of the user’s X.509 certificate against an internal Certificate Store including all known root Certificate Authorities. The certificate is also compared against the Certificate Revocation List, which can be updated automatically based on site security policies.

WebShield provides support for secure socket layer (SSL) v3 encryption, X.509 digital certificates, virtual private network (VPN) capabilities, and Apache hypertext transfer protocol (HTTP) server features such as host aliasing and site mirroring.

The standard WebShield configuration consists of a single virtual host configured as a proxy, which allows secure web browsing from one security domain to another. In the DoD realm, a user on a network at one level (e.g., JWICS) can browse web servers on a network at a lower level (e.g., SIPRNET). In this architecture, where web clients or browsers are considered “trusted” users who need access to “untrusted” web servers, WebShield acts as a standard web proxy and securely forwards requests from one security domain to the other. WebShield can be configured to protect the client browser from malicious pages by scanning for viruses, filtering content, and censoring content as pages pass through the system. Active content filtering provides the ability to parse web pages and remove HTML content based on a set of configuration rules. Content censoring blocks files based on the extension (implied content type) or signature matching (an indication of the file content type).

Strong Authentication Configuration

When configured for Strong Authentication, WebShield utilizes a pair of virtual hosts. The first virtual host is a proxy server, which rewrites requests into SSL requests and redirects them to the second virtual host. The second virtual host is configured as an SSL server and requires an X.509 certificate. If a client certificate is installed on the web browser, WebShield verifies the certificate using the configured verification criteria. If a client certificate is not installed, the request is forbidden.

Implementation

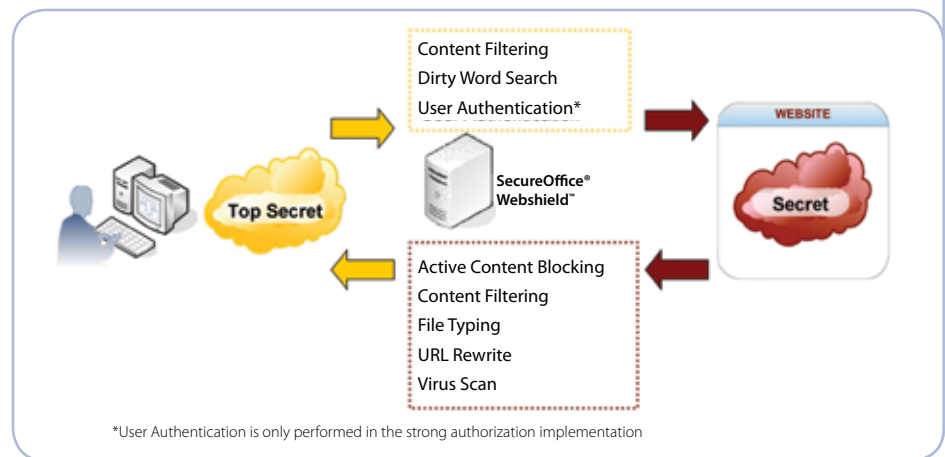
When TCS brings SecureOffice WebShield to your environment, the company leverages more than a decade of experience implementing Cross-Domain Solutions using a proven process tailored for each customer’s mission. The objective is to deploy a functional, manageable, and creditable solution within which users and system administrators are productive. TCS has learned that engaging customers with engineers in a project team approach is the most effective method in achieving this objective. Most SecureOffice WebShield implementations entail two parallel but equally important paths: technical implementation and C&A support.

Certification and Accreditation

SecureOffice WebShield is engineered to satisfy the Cross-Domain Security requirements imposed by C&A processes such as Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) Cross-Domain Solutions.

TCS is involved in C&A process development and improvements for a variety of directives and programs. Active participation in the accreditation communities and accreditation authorities ensures that the products, processes, and documentation evolve to meet changing requirements. Involvement and continued leadership in many of the key forums and process assessments provide TCS with the depth and breadth of experience needed to field operational systems.

For those instances in which customers need a head start on the C&A process and desire to do the rest of the work themselves, TCS can provide templates (based on availability) to complete and facilitate the appropriate C&A process.



Hardware Requirements and Supported Configurations

Recommended User Requirements

- Internet Explorer 6 and 7
- Firefox 2.x
- Netscape 4.76 and 8.1
- Contact TCS for additional information regarding unlisted browsers

Recommended Minimum WebShield Server Sizing

- 2 GHz Core 2 Duo or better
- 4 GB RAM
- 2 x 73 GB HDD
- CD writer (for audit archival)
- 2 Network interface cards

Contact TCS for additional information on configuration and sizing recommendations for your specific environment.

Conclusion

With hundreds of government clients and more than a decade of success, TCS is an industry leader in Cross-Domain Solutions. The company's SecureOffice products offer simple solutions that enable government and industry to securely access and transfer information, striking the right balance between information protection and information sharing—a vital component of national security. SecureOffice WebShield provides a secure solution to the difficult problem of web browsing without sacrificing user access to information or productivity for both enterprise and local installations. Through SecureOffice WebShield, users have the capability to browse web sites on lower level networks securely. SecureOffice WebShield is designed to satisfy the information assurance accrediting community requirements to eliminate any potential leaks and risks.

Internet servers that connect private and public systems and information can become a potential gateway to corporate proprietary and confidential data (e.g., personnel, financial, project, and security information). WebShield provides a mechanism to transparently protect your entire network (i.e., not just a single local server), while allowing you to maintain the current server infrastructure on your existing corporate intranet.



Genuine Innovation in Cross-Domain Solutions on Linux with IBM and Red Hat

IBM, TCS, and Red Hat bring to government the first Cross-Domain Solutions on a Linux trusted operating system. Playing to each company's strength, the alliance offers the reliability of over 100 years of hardware innovation from IBM, the security of accredited Cross-Domain Solutions installed in operational systems from TCS; and the flexibility of an open, mainstream operating system from Red Hat.

About Trusted Computer Solutions, Inc.

Founded in 1994, Trusted Computer Solutions (TCS) is an industry leader in Cross-Domain Solutions. The company's SecureOffice® Suite of software products enable government and industry to securely share information, striking the right balance between information protection and information sharing, a vital component to national security. All SecureOffice products adhere to the most stringent security standards set by US Government Agencies such as the Defense Intelligence Agency and the National Security Agency. SecureOffice products, which run on trusted versions of Linux and UNIX, are installed and accredited in operational systems around the world today protecting our nation's most sensitive digital information. TCS is headquartered in Herndon, VA with offices in Champaign, IL and San Antonio, TX.

For more information, visit www.TrustedCS.com



TCS Corporate Office

2350 Corporate Park Drive Suite 500
Herndon, VA 20171
703.318.7134

TCS Trusted Operating Systems Lab

2021 S First St Suite 207
Champaign, IL 61820
217.384.0028

TCS Texas Office

10010 San Pedro Suite 220
San Antonio, TX 78216
210.340.3151

SecureOffice is a registered trademark of Trusted Computer Solutions, Inc. Linux is a registered trademark of Linus Torvalds. All other trademarks and registered trademarks are the property of their respective owners.