



BENEFITS

- Enables Web browsing from high networks to Web servers on lower-classified networks
- Filters incoming and outgoing data according to established security policy
- Provides virus scanning, dirty word search, file type and active content blocking
- Increases productivity while maintaining a high level of security
- Provides accountability for user actions with Strong Authentication
- Removes browser processing from desktop through available virtual Web browsing option

HIGH-TO-LOW BROWSING OF NETWORKS

SecureOffice® WebShield™ is a secure Web proxy for high-to-low Web browsing, permitting authorized users on classified networks to browse select servers on lower-classified networks. Serving as a PL-4 boundary device, it prevents penetration into higher classified networks from lower level domains. For example, WebShield protects the Joint Worldwide Intelligence Communications System (JWICS) from the Secret Internet Protocol Router Network (SIPRNET) while allowing JWICS users to safely and securely browse the SIPRNET.

Control of User Browsing and External Responses and Requests

WebShield enables organizations 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, and organizations can place restrictions on the low-side network that limit the data the high-side user can access. The Strong Authentication option requires users to authenticate to WebShield with a Department of Defense (DoD) X.509 Digital Certificate and user id/password before they are permitted access through the proxy device.

Filtering of All Incoming and Outgoing Data

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.

WebShield Security Features

WebShield provides multiple security features for safe and reliable Web browsing. The system can be configured to filter active content such as Java Applets, Java Scripts, ActiveX®, and other Multipurpose Internet Mail Extensions (MIME) types. Strong authentication is offered using DoD or Intelligence Community X.509 digital certificates. WebShield also establishes SSL connections to the client to provide privacy. Optional virus scanning is available.

WebShield also provides role-based administration (RBAC), mandatory access controls (MAC), use of least privilege and removal of the super-user root account. An additional security feature included from the SecureOffice® Foundation™ package is kernel-level IP packet filtering. The new Virtual Browsing option removes all processing and the potential for security breaches, from the desktop. The Web browser executes on a remote isolated server and the contents are then displayed at the desktop, enabling more secure remote browsing.

Top-Level Security Approval

WebShield has been National Security Agency (NSA)-assessed and has received Defense Intelligence Agency (DIA) approval. Additionally, WebShield is the browse-down component of DIA's Multi-Domain Dissemination System (MDDS).

Ease of Maintenance and Functionality

No software modifications are required to the client workstation. Any commercial Web browser may be used to take advantage of WebShield capabilities.