WebShield

Securing HTTP traffic throughout the enterprise

Forcepoint developed WebShield as a mechanism by which users can securely access multiple networks at varying security levels from a single desktop device. Forcepoint WebShield promotes more complete information browsing and discovery, which in turn increases users' ability to carry out their missions or job requirements.

Key Benefits

- Supports service-based server-to-server access through HTTP
- Supports standard web browsers and requires no software installation on the user's desktop
- Provides seamless access to web-based resources at lower levels
- Includes customizable virus scanning, dirty word search, file typing, and active content blocking
- Increases productivity while maintaining a high level of security
- Provides accountability for user actions with a Strong Authentication option
- Supports local, site, and regional site-to-site load distribution and failover

Cross-Domain Transfer for Secure Information Sharing

Today, agencies operate in a climate where there is an increasing need to quickly and securely share and gain access to information housed on widely dispersed networks of varying sensitivity levels. More and more mission-critical resources are being delivered over various networks, along with applications, news, email, and numerous other software applications and services. All of these combine to heighten the risk of web-based attacks. Internet servers that connect private and public systems and information become potential gateways to proprietary and confidential data.

Forcepoint WebShield

Forcepoint WebShield is a Commercial-Off-The-Shelf (COTS) data guard that provides secure web search and browse-down capabilities from high-side networks to lower level networks. WebShield allows for the transparent protection of the entire network (i.e., not just a single local server). Security officers can use WebShield to control what data users retrieve. Users surfing lower-level networks can be restricted to specific servers and file types as defined by security policies. All processing is performed at the incoming information level; therefore, the request is processed at the high-side level and the server response is processed at the server level. All requests, responses, and transfers go through various security controls such as dirty word search, virus scan, and malicious content checks. Organizations can also place restrictions on the low-side network to limit data accessed by high-side users.

The standard WebShield configuration allows secure "on-demand" web browsing from one security domain to another. This on-demand approach eliminates data duplication and streamlines network traffic, without the inherent risks and slowdowns that can come with traditional methods of transferring information between levels.

WebShield acts as a web proxy, forwarding requests and corresponding responses from one security domain to the other (Figure 1). Web clients, or browsers, on the high side can access lower-level web servers. WebShield can also support global deployments of more than 100,000 users, which are load balanced at a local and regional level, and provide failover in the event of an outage.

WebShield Architecture

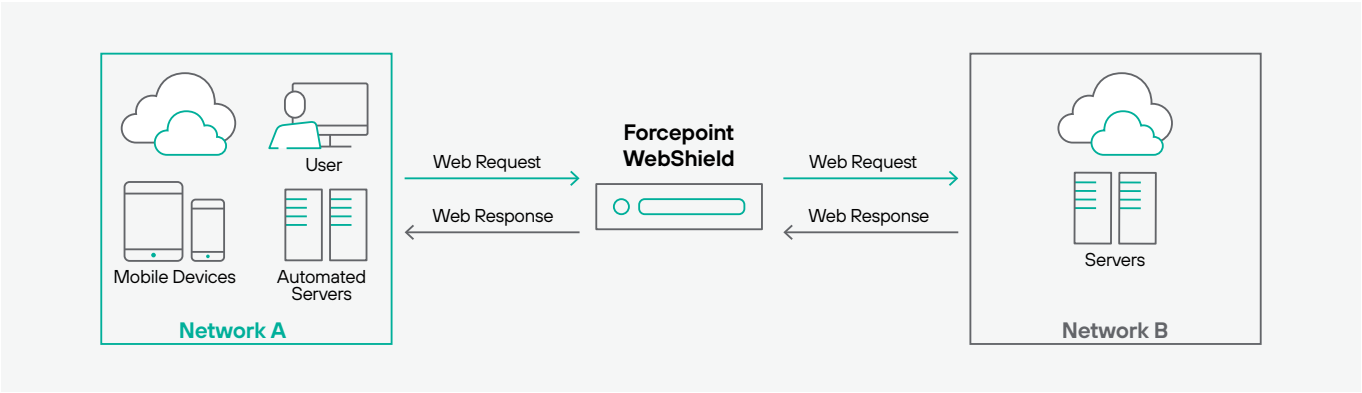

Figure 1

WebShield is used in operational systems worldwide. As part of those systems, WebShield provides intelligence and operations analysts the capability to securely access information at different classification levels and the ability to securely share information with coalition and multinational networks.

A Flexible Guardian

Forcepoint WebShield is a highly secure cross-domain data guard that is tailored for standard web protocols such as hypertext transfer protocol (HTTP). The product allows applications that would not otherwise be considered cross-domain to function in a cross-domain manner with the added assurance of a guard monitoring the data flow. The following are some examples of Forcepoint WebShield applications in use today:

Seamless Cross-Domain Content Discovery

One of the many applications adapted for Forcepoint WebShield allows for seamless cross-domain content discovery through federated search engines. Users access a web-based federated search engine (for example, Vivismo) within a web browser to initiate a search request. The search engine sends the request to Forcepoint WebShield, which then performs the necessary validation checks and permits (or denies) the request to search and return results from other networks.

Secure Chat Mechanism

A standard Forcepoint WebShield environment can be used to support multilevel chat (i.e., chat or instant messaging between security levels). A web-based chat client sends the basic chat (XMPP) traffic through HTTP so that Forcepoint WebShield can read and validate the messages.

Web-Based Application Data Transfers

An example of a web-based application used for mission-critical geographic data transfer is Google Earth. Google Earth utilizes the OpenGIS KML Encoding Standard (OGC KML). OGC KML is an XML language used for geographic visualization. Soldiers in-theater can update real-time geographic coordinates and map tags for analysis by battlefront superiors. Because each group operates at different classification levels, Forcepoint WebShield guards the access and sharing of data.

Real-Time Data Access and Manipulation

Forcepoint WebShield provides real-time data validations that enable organizations to keep one instance of information at the lowest level necessary. This eliminates the need for replicating multiple copies on various networks, while allowing time-sensitive data to be accessed and updated by people from all permitted security levels–ensuring that users are working with the same information. For example, users in the field who are responsible for creating individual work products, such as mapping information, can work at a lower level to maintain the data coming in from the field. At the same time, the users responsible for analyzing those work products and making critical mission decisions can remain in their higher-level work environment. All users are assured of having real-time access to the most current information without duplicating data at both levels.

Multilevel Web-Based Email

When utilizing a high-side web-based email application, high-side users with email accounts at lower levels can access all of their email from one application. The traffic is checked and verified through Forcepoint WebShield.

Secure Wiki Page Authoring

Many agencies use internal wikis, defined as "a collaborative website set up to allow user editing and adding of content." To foster this free flow of information while preserving a high degree of security, two cross-domain information transfer systems are used–Forcepoint WebShield and Forcepoint Trusted Gateway System. By using Forcepoint Trusted Gateway System and Forcepoint WebShield in an integrated fashion, users can securely upload files or images to the low-side resident wiki. The data is thoroughly scanned according to site security policy through Forcepoint Trusted Gateway System (virus scan, dirty word search, content inspection) and securely transferred to the wiki through Forcepoint WebShield.

WebShield Security Controls

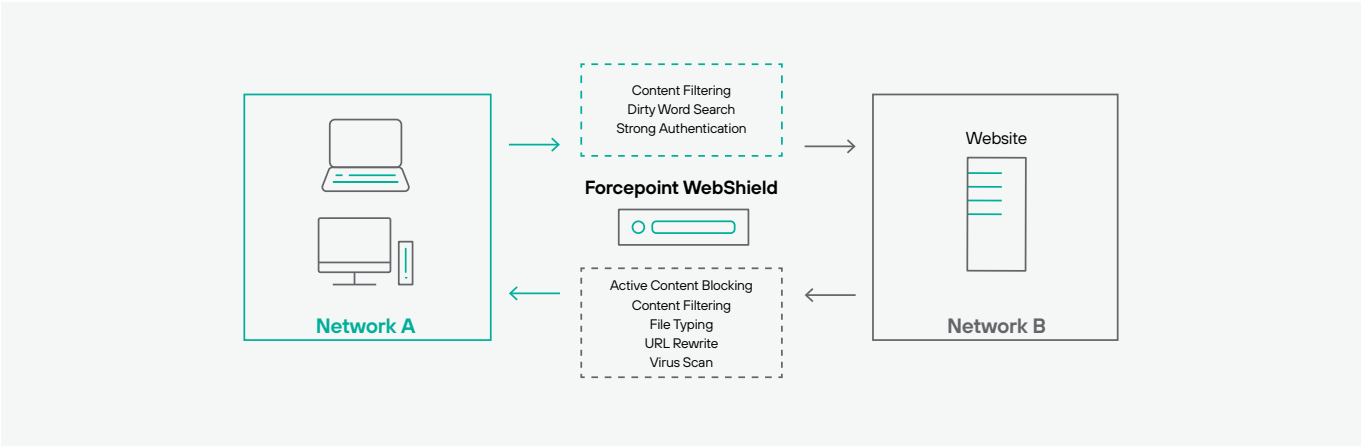

Figure 2

Request/Transfer Security Controls

Forcepoint WebShield can be configured to protect the high-side client browser or initiating application from malicious pages or data by scanning for viruses, filtering content, and blocking content as the requests pass through the system.

Active Content Blocking

Server responses can be scanned to identify and remove a wide range of active content. Forcepoint WebShield can be configured to block Java Applets, Java Script, ActiveX, and other kinds of content (or mobile code). This prevents a data-driven attack from a low-side server. Content blocking is based on the extension (implied content type) or signature matching (an indication of the file content type).

Content Filtering

Active content filtering provides the ability to parse web pages and remove HTML content based on a set of configuration rules. The bi-directional content filters within Forcepoint WebShield scan user requests and server responses based on system administrator-established security parameters. Forms and URL strings in all user requests are scanned prior to transmission to the lower-level server. If any outgoing data is considered a breach of the site security policy, the request is rejected. All server replies are carefully scrutinized before forwarding to the user.

Dirty Word Search

Forcepoint WebShield scans user requests for sensitive or "dirty" words that should not be viewable on the low-side network. 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. Administrators can create and customize a master list of both dirty and clean words. Once these lists are configured, each request is searched against the list for matches. In the case of a denial, the user must resubmit the request without the identified word(s) to proceed.

File Type Verification

Forcepoint WebShield's file type verification is performed through several different mechanisms, such as extension matching, Forcepoint signature algorithm, and a third-party algorithm. All of these mechanisms are configurable to accommodate unique file types.

Virus Scanning

Virus scanning in Forcepoint WebShield is provided through a third-party engine that is licensed separately. Forcepoint WebShield allows customization to exclude certain trusted file types from virus scanning to enhance performance.

Protecting Communication

Forcepoint WebShield is a web proxy that protects internal clients (e.g., web browsers) that access external resources (e.g., networks at different classification levels). Forcepoint WebShield provides support for Secure Socket Layer (SSL) encryption, X.509 digital certificates, virtual private network (VPN) capabilities, and Apache HTTP server features such as host aliasing and site mirroring.

Strong Authentication Configuration

Within Forcepoint WebShield, the Strong Authentication option leverages the Intelligence and Defense Public Key Infrastructures (PKI) X.509 digital certificate and a certificate revocation list (CRL) in addition to IP address, username, and password. Strong Authentication ensures that only authenticated users have access to Forcepoint WebShield.

Administration and Management

Administration and management of a Forcepoint WebShield implementation is performed by system administrators with the appropriate permissions. Permissions are defined in the guard itself or remotely through the Remote Access Console (RAC). RAC is used to centrally manage the servers within the enterprise. This deployed and accredited capability allows the administrator to remotely access the Protection Level

4 (PL4)-capable servers over a secure connection. RAC is a secure, scalable remote access solution that can be utilized from any authorized location on the network where the servers reside. RAC provides KVMover—IP capabilities that enable an authorized user "console" access as if he or she were seated at the attached device.

Log Management

Forcepoint WebShield supports local and centralized log management and off-the-box notifications/alerts, which allow administrators to monitor the health and wellness of the system.

Auditing

Forcepoint WebShield supports a local and centralized audit repository to track use and activity. This audit data can also be pushed to a centralized enterprise audit storage location.

Certification and Accredidation (C&A)

Forcepoint WebShield is engineered to satisfy cross-domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) C&A processes. Forcepoint's cross-domain products are installed and accredited in operational systems around the world.

Conclusion

With hundreds of government clients and more than a decade and a half of success, Forcepoint is an industry leader in cross-domain solutions. The company's products have a proven track record of proactively preventing government and commercial organizations from being compromised, while fostering the secure access and transfer of information. This allows Forcepoint cross-domain solutions to strike the right balance between information protection and information sharing—a vital component to national security. Forcepoint WebShield is a secure browse-down and discovery solution that solves the difficult problem of satisfying security needs while enhancing information access and sharing. Forcepoint WebShield is designed to satisfy the information assurance accrediting community requirements, eliminate potential leaks and risks, and provide users with an easy-to-use workflow application. All Forcepoint solutions have been designed to meet or exceed extensive and rigorous security C&A testing by the Defense Intelligence Agency (DIA) and the National Security Agency (NSA) for simultaneous connections to various networks at different security levels. Forcepoint offers an experienced professional services team to guide customers through the technical implementation and C&A processes.