HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg

Tel: 09103 / 715-0
Fax: 09103 / 715-271
E-Mail: support@hob.de
Internet: www.hob.de

WhitePaper

HOB WebSecureProxy

Encryption, Security,
Performance, Failsafety

March 2010

Technology
Future
Communication

The HOB WebSecureProxy

Using the Internet for B2B applications requires a careful look at the necessary security measures. The following demands require special attention:

- Data encryption and integrity
- Securing the application server / Web services
- High performance
- Failsafe performance

As various as these demands are, the HOB WebSecureProxy and the HOB Connectivity Clients, available for IBM Mainframes, Microsoft Windows Terminal Servers and numerous other target systems, cover all of them.

Data Encryption and Integrity

Netscape, the Internet pioneer in browser technology, introduced SSL encryption (Secure Socket Layer) in the Netscape Navigator v. 2. SSL serves to secure communications between a browser and a Web server.
SSL uses a mix of symmetric and asymmetric encryption. For the symmetric encryption, various algorithms can be used, for example, DES, 3DES, RC2, RC4, or AES (Advanced Encryption Standard), etc. Symmetric encryption requires that both the sender as well as the recipient know the key used. This key has to be exchanged in a secure manner before encrypted communication can take place.
To create this secure key transfer, the SSL connection is asymmetrically encrypted in the beginning stage. Here, the sender encrypts the sent message with the recipient's public key. The only person who can decrypt this message is the recipient whose public key was used to encrypt it. This recipient uses his private key for decryption. The advantage of asymmetric encryption is found in the simple key exchange, where only the public keys are exchanged. The disadvantage of this encryption method lies in the relatively high demand it places on computing power. This is why SSL encryption uses a mix of both these methods. The RSA algorithm and the Diffie-Hellman algorithm are two of the best-known representatives of asymmetric encryption.

In addition to ensuring privacy (data encryption), the integrity of the data must be ensured. It is of the utmost importance that the sent data are not secretly altered during transmission. A possible alteration of the sent and encrypted data by an attacker must be discovered during decryption. The data's integrity must be ensured. Hash values determined on the basis of data blocks provide this security. SSL encryption uses hash algorithms such as MD5 or SHA-1 to achieve this.
The HOB WebSecureProxy fully supports SSL encryption. It presents itself to the client side as an SSL terminal. It communicates to the server side without SSL encryption. All the above-mentioned encryption algorithms are supported by the HOB WebSecureProxy. They are configured by the HOB Security Manager, a component of HOBLink Secure and included in the scope of delivery.

Securing the Application Server/Web Services

As already mentioned, the SSL-secured communication takes place between the HOB WebSecureProxy and the client, whereas the HOB WebSecureProxy communicates with the server side without SSL. This, then, is a 3-tier solution.
The HOB WebSecureProxy presents itself as a central collection point for client requests from the Internet. Preferably placed in the DMZ, it forwards the requests to the corresponding server. This only occurs after the client has been successfully authenticated.
The HOB WebSecureProxy is available fort he following platforms:

- Windows (x86, EM64T, Itanium)
- Linux (x86, EM64T, Itanium)
- Sun Solaris (Sparc, EM64T)
- HP-UX (PA-Risc, Itanium)
- IBM AIX
- Open Unix

Authentication

Depending on the requirements, the deployed SSL protocol can perform either a server or a client authentication. In the first case, a server certificate signed by a CA (Certificate Authority) is stored on the HOB WebSecureProxy, whereas the clients all have the same certificate. Clients cannot be authenticated using this method; it can only be determined whether the client belongs to the group of this certificate's owners. The client can, however, determine the authenticity of the SSL terminal via the server certificate. If each client has their own certificate, then client authentication is also possible.

Expired certificates or blocked users can be administrated over a CRL (Certificate Revocation List), which is locally available on the HOB WebSecureProxy. An online inspection of a client certificate signed by a CA can be performed using the OCSP protocol (Online Certificate Status Protocol, RFC 2560). Within just a few seconds, the validity of a certificate can be checked via the HOB WebSecureProxy by accessing an OCSP responder.
For the highest level of security, the certificates are stored on a Smartcard; they can also be stored on a file system or on USB sticks.
If the authentication is carried out using Timecode tokens, for example, RSA SecurID or other RADIUS-protocol-capable authentication solutions, the HOB WebSecureProxy has a suitable interface for the corresponding server. All client requests are accordingly checked by the HOB WebSecureProxy and only forwarded to the server if approved.

Shielding

The HOB WebSecureProxy only allows authenticated users to gain access to the corresponding server. Thus the server is effectively shielded against attacks coming out of the Internet. For example, all connections can be implemented over just one port: this is a major security advantage. In this WSP-SOCKS mode the HOB client informs the HOB WebSecureProxy of the desired terminal. The HOB WebSecureProxy can also react to HTTPS requests from a Web browser and forward these to the Webserver / Webservices. This can be done over either HTTP or HTTPS. The HOB WSP Web-Server-Gate reinterprets the Web pages, HTML and JavaScript links are automatically converted for the browser on the client. This function is an important part of the so-called SSL-VPNs. The integrated target filter allows users to access only those Web servers for which they are authorized. The WSP-SOCKS mode also enables the HOB WebSecureProxy to overwrite HOB client connection configurations. Access to internal company servers is thus configured at a central location: the HOB WebSecureProxy. An additional security advantage of the WSP-SOCKS mode is that all connections can be implemented by opening just one port in the firewall.

High Performance

HOB's initial IT activities centered on the IBM Mainframe environment. Today, this is still an area where the highest degree of availability and performance are required. Due to our many years of host programming, we at HOB have the know-how to program highly performant yet resource-sparing software. The HOB WebSecureProxy can, for example, administrate about 10,000 parallel SSL sessions running on one $5,000 Windows

Terminal Server. This high performance is a result of the further development of the HOB WebSecureProxy's internal architecture, which is based on powerful transaction monitors, similar to CICS on the Mainframe. The minimal data volume of the data streams encoded with SSL is another result of this architecture. Differently from most SSL-VPN solutions, there is no further embedding of the useful data in HTTP requests. This eliminates unnecessary protocol overhead. For the hardware side, HOB recommends inexpensive workstations with high CPU power and sufficient memory instead of expensive server-hardware.
The growing use of mobile clients via UMTS will accelerate the introduction of the IPv6 protocol. The HOB WebSecureProxy already supports this protocol. Thus the connection of a large number of mobile users to a central server service is possible.

High Failsafe Quality

In addition to high performance, availability, especially for large installations, is of great importance. To minimize the risk of hardware-failure, multiple instances of the HOB WebSecureProxy should be installed. Client requests are then distributed over a single URL to the installed HOB WebSecureProxies. Hereby, redundancy is the way to go.
The HOB WebSecureProxy's internal architecture does its part to achieve maximum availability. For example, the functionality of the HOB WebSecureProxy can be extended as required via the Server-Data-Hook. This – under Windows as a DLL – communicates with the HOB WebSecureProxy over an HOB internal interface. Extra functionalities can therefore be added to the HOB WebSecureProxy without having to reconfigure the core functions. This minimizes errors in new versions. In the event that an error does occur, our UNIX-style core-dump greatly facilitates error recognition and resolution, even for Windows.
The administrator can easily change the configuration while the WebSecureProxy is running. After the configuration file has been edited, it is dynamically reloaded by the HOB WebSecureProxy. Existing connections / sessions are not affected by this, whereas newly established sessions inherit the new configuration.

Additional Benefits

In addition to the above-mentioned security-related advantages, there are numerous other benefits to be had from deploying the HOB WebSecureProxy.
The HOB WebSecureProxy plays a key role in HOB RD VPN-solution scenarios (HOB Remote Desktop VPN). HOB RD VPN comprises three areas:

HOB WTS Computing

This solution provides Internet users with secure remote access to Microsoft Windows Terminal Server farms. Hereby, the HOB WebSecureProxy is the only instance that can be reached directly from the Internet. Users connect over the HOB RDP client to the HOB WebSecureProxy and have to authenticate themselves there. After a successful authentication, the HOB WebSecureProxy distributes the requests via HOB Load Balancing to the Windows Terminal Server with the least load. The HOB Load Balancer uses the actual CPU load and other, configurable parameters such as free working memory, etc. to determine which WTS is currently best-suited to accept the connection. Of course, users whose sessions are inadvertently interrupted are reconnected to the same server that they were previously using.

HOB VDI Business

As an alternative to Windows Terminal Servers, virtual machines running Windows XP Professional, Windows Vista or Windows 7 and hosted on servers can also be accessed. Here, too, the HOB software manages load balancing for the individual virtual machines. In combination with VMware, virtual Windows XP Pro / Windows Vista guest systems can be used to provide secure remote access to your workforce.

HOB Desktop-on-Demand

This solution allows users remote access to their own workstation PC's (equipped with Windows XP Professional or Windows Vista) on the company premises from a LAN, WAN or even over the Internet – from anywhere in the world. Thanks to the HOB WebSecureProxy, it makes no difference whether the target computer is switched on or not. Using the integrated Wake-on-LAN functionality, the HOB WebSecureProxy can boot the required computer. The user thus has access to all applications and data on the target computer – and this is, of course, all done with the highest level of security.

For further information on HOB RD VPN please visit the HOB Website, www.hobsoft.com.

Dipl.-Ing. Swen Baumann
Product Manager