



HOB GmbH & Co. KG
Schwadmühlstr. 3
90556 Cadolzburg

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

WhitePaper

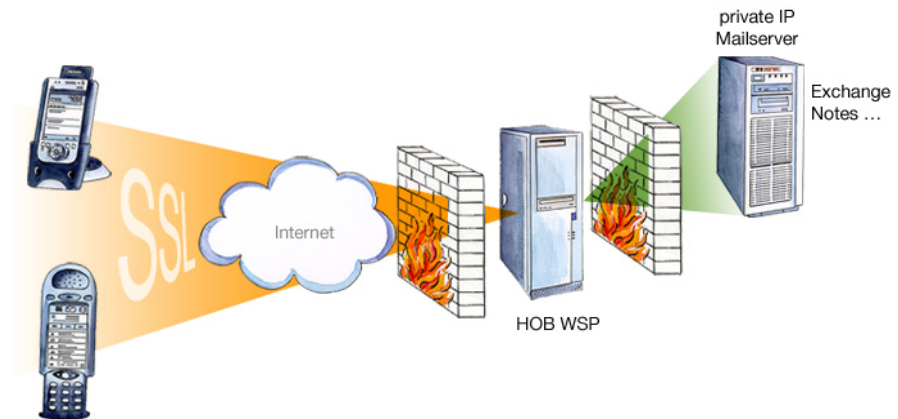
HOB WebSecureProxy as an SSL Terminal for E-Mail Clients

November 2005



HOB WebSecureProxy as an SSL Terminal for E-Mail Clients

Best placed in the DMZ, the HOB WebSecureProxy is an SSL gateway that SSL-encrypts the e-mail traffic on the client side and transfers it unencrypted to the mail server on the LAN side. This effectively protects the mail server against any attacks coming over the Internet.



The HOB WebSecureProxy provides you with two different methods of protecting your e-mail with SSL:

1. Using the SSL encryption functionality integrated in the e-mail client

Many modern e-mail clients have SSL functionality integrated into them. The usual mail receipt protocol is either POP3 or IMAP4. Depending on which is being used, when SSL encryption is activated, SSL-encrypted e-mail will be received over either POP3S on the mail server port 995 or over IMAP4S on port 993. SSL-protected e-mail is sent over SMTPS on the mail server port 465. These are the default ports for these actions. For HOB WebSecureProxy authentication, a certificate signed by an external CA (Certificate Authority) is required.

The advantage of this security method is that no additional software need be installed on the client system (not even any HOB software).

The HOB WebSecureProxy is configured via an XML file. The HOB WebSecureProxy configuration for the previously described scenario would appear as follows:

```
<sslgate-configuration>
  <general>
    <report-intv>1800</report-intv>
    <prot-event-log>YES</prot-event-log>
    <network-statistic-level>9</network-statistic-level>
  </general>

  <connection>
    <name>SSLGATE001</name>
    <gateport>993</gateport>
    <gate-in-ineta>10.0.0.150</gate-in-ineta>
    <SSL-config-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.cfg
    </SSL-config-file>
    <SSL-certdb-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.cdb
    </SSL-certdb-file>
    <SSL-password-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.pwd
    </SSL-password-file>
    <max-session>50</max-session>
    <serverineta>mail.company.com</serverineta>
    <serverport>143</serverport>
    <timeout>3600</timeout>
  </connection>

  <connection>
    <name>SSLGATE002</name>
    <gateport>465</gateport>
    <gate-in-ineta>10.0.0.150</gate-in-ineta>
    <SSL-config-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.cfg
    </SSL-config-file>
    <SSL-certdb-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.cdb
    </SSL-certdb-file>
    <SSL-password-file>
      C:\Program Files\HOBLink\WebSecureProxy\sslsettings\
      hserver.pwd
    </SSL-password-file>
    <max-session>50</max-session>
    <serverineta>mail.company.com</serverineta>
    <serverport>25</serverport>
    <timeout>3600</timeout>
  </connection>
</sslgate-configuration>
```

Explanation of the Tags Used:

<sslgate-configuration>

The <sslgate-configuration> tag marks the beginning of the XML configuration. The entire HOB WebSecureProxy configuration is found between this tag and its counterpart, the </sslgate-configuration> tag.

<general>

The general behavior of the tag HOB WebSecureProxy is defined in this tag, e.g., the logging interval.

<report-intv>

This tag enables the output of statistical data on the use of threads, memory, etc. to the event log or console. In this sample configuration, the data will be output every 1800 seconds.

<prot-event-log>

The <prot-event-log> tag enables the output of error messages and events.

<network-statistic-level>

The <network-statistic-level> tag defines the output of network utilization data. Possible parameters are: 1 to 9, minimum to maximum data output.

<connection>

This tag is used to configure the connection, e.g., to define the listening port or target address. This tag may be used several times within a HOB WebSecureProxy configuration, i.e., you may define several connections.

<name>

The <name> tag defines the name of the connection configuration, in this case, SSLGATE001. This setting must be made.

<gateport>

The <gateport>tag defines the listening port for an incoming connection. In this configuration, port 993 for IMAPS is opened in the first <connection> tag, and port 465 for SMTPS is opened in the following <connection> tag.

<gate-in-ineta>

This optional tag is only used for multi-homed systems. It defines the network adapter via the IP address.

<SSL-config-file>, <SSL-certdb-file>, <SSL-password-file>

Path to the SSL certificate, configuration file and password file.

<max-session>

This tag contains the definition of the maximum number of concurrently active sessions (connections) within this configuration.

<serverineta>

The mail server's IP address. Here: mail.company.com

<serverport>

Target port on the mail server. Here: 143 for IMAP4 and 25 for SMTP.

<timeout>

Optional. Defines the length of time to expire before a connection timeout will be designated a failure.

With this configuration, the HOB WebSecureProxy will provide you with two 1:1 connections.

E-Mail Client Configuration

In the local e-mail client, create an account that will have the HOB WebSecureProxy as the target address for incoming (POP3 or IMAP4) and outgoing (SMTP) mail, instead of the mail server. Enable the option "SSL-connection required."

Client-Side SSL Communication over the HOB Universal Client

The HOB Universal Client can be installed on the client or downloaded via the Web browser. The HOB Universal Client encrypts the data exchanged between the e-mail-client and the HOB WebSecureProxy. The e-mail client itself need not be SSL-capable. The exchanged data can also be compressed with V42.bis before being sent, accelerating e-mail traffic. All communications between the HOB Universal Client and the HOB WebSecureProxy go over just one IP port.

E-Mail Client Configuration

In the local e-mail client, create an account that will address the local host instead of the mail server. The HOB Universal Client receives the data, compresses and SSL-encrypts them, and forwards them to the HOB WebSecureProxy. The option "SSL-connection required" is not to be set for this configuration.