



HOB GmbH & Co. KG
Schwadernühlstr. 3
90556 Cadolzburg

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

WhitePaper

HOB WebSecureProxy

Verschlüsselung, Absicherung,
Leistungsfähigkeit, Ausfallsicherheit

November 2010

Der HOB WebSecureProxy

Die Nutzung des Internet für B2B-Anwendungen erfordert eine sorgfältige Prüfung der notwendigen Securitymaßnahmen. So ist auf die folgenden Anforderungen ein besonderes Augenmerk zu legen:

- Verschlüsselung und Integrität der Daten
- Absicherung der Anwendungsserver/Webservices
- Hohe Leistungsfähigkeit
- Hohe Ausfallsicherheit

So unterschiedlich die Anforderungen auch sind, mit dem HOB WebSecureProxy und den HOB Connectivity Clients, verfügbar für den IBM Mainframe, den Microsoft Windows Terminal Server und zahlreiche andere Zielsysteme, werden alle Anforderungen abgedeckt.

Verschlüsselung und Integrität der Daten

Die Firma Netscape, Internet Pionier bei der Browsertechnologie, führte in ihrer Version 2 des Netscape Navigator die SSL Verschlüsselung (Secure Socket Layer) zur sicheren Kommunikation zwischen dem Browser und dem Webserver ein.

SSL ist ein Mix aus symmetrischer und asymmetrischer Verschlüsselung. Für die symmetrische Verschlüsselung können verschiedene Algorithmen verwendet werden, beispielsweise DES, Triple DES bzw. 3DES, RC2, RC4, und der relativ neue AES (Advanced Encryption Standard). Die symmetrische Verschlüsselung erfordert auf der Sender- wie Empfangsseite die Kenntnis des Schlüssels. Dieser ist auf sicherem Wege vor der verschlüsselten Kommunikation auszutauschen.

Zu diesem Zweck wird beim SSL-Verbindungsaufbau zunächst asymmetrisch verschlüsselt. Hierbei verschlüsselt der Sender seine Nachricht mit dem öffentlichen Schlüssel des Empfängers. Nur der rechtmäßige Empfänger ist dadurch in der Lage die gesendeten Daten mit seinem geheimen Privatschlüssel zu dekodieren. Der Vorteil der asymmetrischen Verschlüsselung liegt in der einfachen Schlüsselverteilung, nur die öffentlichen Schlüssel werden ausgetauscht. Der Nachteil dieser Verschlüsselung liegt in dem relativ hohen Rechenaufwand. Genau aus diesem Grunde findet sich in der SSL Verschlüsselung eine Kombination aus beiden Varianten. Der RSA Algorithmus sowie der Diffie-Hellman Algorithmus seien als zwei Vertreter der asymmetrischen Verschlüsselung genannt.

Neben der Verschlüsselung der Daten spielt natürlich auch deren Unveränderbarkeit eine wichtige Rolle. So muss unbedingt gewährleistet sein, dass der Empfänger nach der Dekodierung der Daten wieder die ursprünglich gesendeten Daten erhält. Eine mögliche Veränderung der gesendeten und verschlüsselten Daten durch einen Angreifer darf bei der Dekodierung nicht unentdeckt bleiben. Die Integrität der Daten muss also gewährleistet sein. Aus Datenblöcken ermittelte Hash-Werte ermöglichen diese Sicherheit. Innerhalb der SSL Verschlüsselung wird dies durch Hash-Algorithmen wie MD5 oder SHA-1 erreicht.

Der HOB WebSecureProxy unterstützt die SSL Verschlüsselung in vollem Umfang. Er stellt sich zur Clientseite als eine SSL Gegenstelle dar. Zur Serverseite hin wird dagegen ohne SSL Verschlüsselung kommuniziert. Alle vorab genannten Verschlüsselungsalgorithmen werden vom HOB WebSecureProxy unterstützt. Deren Konfiguration erfolgt mit dem von HOB im Programmpaket HOBLink Secure mitgelieferten Security Manager.

Absicherung der Anwendungsserver/Webservices

Wie bereits erläutert findet die SSL gesicherte Kommunikation zwischen dem HOB WebSecureProxy und dem Client statt, während vom HOB WebSecureProxy zur Serverseite hin ohne SSL kommuniziert wird. Es handelt sich also um eine 3-tier Lösung.

Der HOB WebSecureProxy stellt sich als zentrale Anlaufstelle für Anfragen von Clients aus dem Internet dar. Vorzugsweise in der DMZ platziert, leitet er die Anfragen an den entsprechenden Server weiter. Dies geschieht allerdings nur bei erfolgreicher Authentisierung der Clients. Der HOB WebSecureProxy ist für die folgenden Plattformen verfügbar:

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

Authentisierung

Je nach Anforderung kann das verwendete SSL Protokoll eine Server- bzw. eine Clientauthentisierung leisten. Im ersten Fall ist das von einer CA (Certificate Authority) signierte Serverzertifikat auf dem HOB WebSecureProxy hinterlegt, wogegen an den Clients überall das gleiche Zertifikat vorhanden ist. Eine Clientauthentifizierung ist so nicht möglich, nur die Zugehörigkeit zu der Gruppe der Zertifikatsbesitzer ist feststellbar. Der Client kann hingegen die Echtheit der SSL Gegenstelle anhand des Serverzertifikates prüfen. Erhält jeder Client sein eigenes Zertifikat so ist auch eine Client Authentisierung möglich.

Abgelaufene Zertifikate oder gesperrte Benutzer können über eine – lokal am HOB WebSecureProxy verfügbare – CRL (Certificate Revocation List) verwaltet werden. Eine Online-Prüfung der von einer CA signierten Clientzertifikate ist mittels des OCSP-Protokolls (Online Certificate Status Protocol, RFC 2560) ebenso möglich. Binnen weniger Sekunden kann so, über den Zugriff des HOB WebSecureProxy auf einen OCSP-Responder, die Gültigkeit eines Zertifikates geprüft werden.

Die Client-Zertifikate liegen im Fall höchster Security auf einer SmartCard, eine Ablage im Filesystem bzw. auf USB Sticks ist jedoch ebenso möglich.

Geschieht die Authentisierung über Timecode-Tokens, wie beispielsweise RSA SecurID oder andere RADIUS Protokoll fähige Authentisierungslösungen, besitzt der HOB WebSecureProxy eine geeignete Schnittstelle zum jeweiligen Authentisierungsserver. Alle Clientanfragen werden dementsprechend bereits am HOB WebSecureProxy geprüft und nur bei positivem Ergebnis an den entsprechenden Server weitergeleitet.

Abschottung

Durch den HOB WebSecureProxy werden nur erfolgreich authentifizierte Benutzer auf den entsprechenden Server weitergeleitet. Dementsprechend wird der Server wirksam vor direkten Angriffen aus dem Internet abgeschottet.

Zum einen kann für jede genutzte Proxy-Umleitung die Öffnung eines eigenen beliebigen Ports zur Clientseite hin konfiguriert werden. So beispielsweise Port 5000 für HOB Web-to-Host Connectivity und Port 5001 für HOB Windows Terminal Server Connectivity usw..

Zum anderen kann sämtliche Connectivity über einen einzigen Proxy-Port realisiert werden. In diesem WSP-SOCKS-Mode kommuniziert der HOB-Client die gewünschte Gegenstelle an den HOB WebSecureProxy. Ebenso kann der HOB WebSecureProxy mittels Web-Server-Gate Funktionalität auf HTTPS-Anfragen eines Webbrowsers reagieren und diese an einen Webserver weiterleiten, hierbei wird sowohl HTTP wie auch HTTPS unterstützt. Das HOB WSP Web-Server-Gate interpretiert die Webseiten neu, HTML- und Javascript-Links werden für den Browser am Client automatisch umgesetzt. Letztere Funktionalität ist wesentlicher Bestandteil sogenannter SSL-VPNs. Der integrierte Target-Filter lässt die Benutzer nur auf die für sie bestimmten Webserver zugreifen.

Über die WSP-SOCKS-Mode Funktionalität ist der HOB WebSecureProxy auch in der Lage Verbindungskonfigurationen von HOB Clients zu überschreiben. Die Konfiguration des Zugriffs auf firmeninterne Server geschieht also an zentraler Stelle, am HOB WebSecureProxy. Ein weiterer Vorteil des WSP-SOCKS-Mode liegt in der Öffnung eines einzigen Ports in der Firewall.

Hohe Leistungsfähigkeit

HOB begann seine Firmengeschichte im IBM Mainframe Umfeld. Noch heute ein Bereich bei dem es auf höchste Verfügbarkeit und Leistungsfähigkeit ankommt. Aufgrund dieser jahrelangen Erfahrung in der Hostprogrammierung hat man bei HOB das Know-How hochleistungsfähige und dennoch Ressourcen schonende Software zu programmieren. So ist der HOB WebSecure-Proxy beispielsweise in der Lage ca. 10.000 parallele SSL-Sessions auf einer \$ 5000 Standard Windows Workstation zu verwalten. Diese hohe Leistungsfähigkeit resultiert aus der weiter entwickelten internen Architektur des HOB WebSecureProxy, die auf der Basis leistungsfähiger Transaktionsmonitore, wie beispielsweise CICS auf dem Mainframe, basiert. Ein minimales Datenvolumen der in SSL eingepackten Datenströme ist eine weitere Folge dieser Architektur. Im Gegensatz zu den meisten SSL-VPN Lösungen findet keine weitere Einbettung der Nutzdaten in HTTP-Anfragen statt. Ein unnötiger Protokoll-Overhead wird somit vermieden. HOB schlägt für die Hardware keine teure Server-Hardware vor, stattdessen kostengünstigere Workstations mit hoher CPU-Leistung und genügend Speicher.

Die zunehmende Nutzung mobiler Clients via UMTS wird die Einführung des IPv6 Protokolls beschleunigen. Die hierfür notwendige Unterstützung ist bereits jetzt im HOB WebSecureProxy integriert. Die Anbindung großer, mobiler Nutzerzahlen an zentrale Serverdienste ist somit generell möglich.

Ausfallsicherheit

Neben der hohen Leistungsfähigkeit spielt gerade bei Großinstallationen die Verfügbarkeit eine immens wichtige Rolle. Um das Risiko von Hardware-Ausfällen zu minimieren, wird der HOB WebSecureProxy mehrfach installiert. Clientanfragen werden in diesem Fall über eine einzige URL auf die installierten HOB WebSecureProxies verteilt. Redundanz ist hier das Mittel zum Zweck.

Die interne Architektur des HOB WebSecureProxies tut ihr weiteres, um eine maximale Verfügbarkeit zu erreichen. So lässt sich die Funktion des HOB WebSecureProxy durch einen Server-Data-Hook beliebig erweitern. Dieser – unter Windows eine DLL – kommuniziert über eine HOB interne Schnittstelle mit dem HOB WebSecureProxy. Zusätzliche Funktionalitäten können so hinzugefügt werden ohne den HOB WebSecureProxy in seinen Kernfunktionen umschreiben zu müssen. Fehler in neuen Versionen werden so minimiert. Falls doch Fehler auftreten sollten, lässt ein aus der UNIX Welt bekannter Core-Dump die Fehlererkennung und Behebung auch unter Windows deutlich zuverlässiger und schneller vonstatten gehen.

Das Ändern der Konfiguration ist im laufenden Betrieb durch den Administrator problemlos möglich. Nach der Änderung der Konfigurationsdatei wird diese vom HOB WebSecureProxy dynamisch nachgeladen. Bestehende Verbindungen/Sessions bleiben davon unberührt, wogegen neu aufgebaute Sessions die neue Konfiguration berücksichtigen.

Weitere Besonderheiten

Neben den genannten sicherheitstechnischen Vorteilen gibt es noch weitere zahlreiche Vorteile, die für den Einsatz des HOB WebSecureProxy sprechen.

So besitzt der HOB WebSecureProxy innerhalb des HOB RD VPN-Lösungsszenarios (HOB Remote Desktop VPN) wichtige Schlüsselfunktionen. Das HOB RD VPN beschreibt drei Bereiche:

HOB WTS Computing

Hierbei handelt es sich um den sicheren remote Zugriff auf Microsoft Windows Terminal Server Farmen aus dem Internet. Der HOB WebSecureProxy ist hierbei als einzige Instanz direkt aus dem Internet erreichbar. Die Benutzer verbinden sich über den HOB RDP Client mit dem HOB WebSecureProxy und müssen sich dort authentifizieren. War dieser Vorgang erfolgreich, so verteilt der HOB WebSecureProxy die Anfragen über das HOB Load Balancing auf den am wenigsten ausgelasteten Windows Terminal Server. Die Verteilung berücksichtigt hierbei die tatsächliche Auslastung der jeweiligen CPU und weiterer, konfigurierbarer Parameter wie z.B. freier Arbeitsspeicher, etc.. Selbstverständlich werden Benutzer, deren Verbindung ungewollt getrennt wurde, wieder mit dem richtigen Server verbunden.

HOB VDI Business

Statt Windows Terminal Servern, kommen hier Windows XP, Windows Vista oder Windows 7 Systeme als RDP-Gegenstelle (Anmerkung: sofern die jeweilige Windows-Variante RDP Zugriff unterstützt) zum Einsatz. HOB empfiehlt die Verwendung moderner Blade Systeme als Basishardware. Der HOB WebSecureProxy verteilt die RDP-Anfragen auf die zur Verfügung stehenden Maschinen. Der Benutzer erhält so einen ortsunabhängigen Zugriff auf ein leistungsfähiges Windows Einzelplatzsystem. Ideal für leistungshungrige Anwendungen oder nicht Terminal Server-fähige Anwendungen. Kosteneinsparungen sind hier durch den Einsatz von Thin Clients oder älterer PC Hardware, auch mit Linux-Systemen, möglich. Der HOB VDI Agent, installiert auf jedem Blade System, ermöglicht eine Priorisierung bestimmter Blade Systeme und sorgt weiter für die korrekte Übermittlung des Besetzt-/Unbesetzt-Status an den HOB WebSecureProxy. In Verbindung mit VMware ist auch die Nutzung virtueller Windows Gastssysteme als RDP Gegenstelle möglich.

HOB Desktop-on-Demand

Diese Lösung ermöglicht dem Benutzer den Zugriff auf seinen eigenen Arbeitsplatz PC (ausgestattet mit Windows XP, Windows Vista oder Windows 7) innerhalb der Firma auch über das Internet. Mittels des HOB WebSecureProxy spielt es dabei keine Rolle, ob der Zielrechner ausgeschaltet ist oder nicht. Durch die integrierte Wake-on-LAN Funktionalität kann der HOB WebSecureProxy, auch aus der DMZ heraus, den geforderten Rechner aktivieren. Der Zugriff auf alle am Zielrechner vorhandenen Anwendungen und Daten wird so realisiert – selbstverständlich bei höchster Sicherheit.

Weitere Informationen zu HOB RD VPN erhalten Sie auf der HOB Website (www.hob.de).

©HOB GmbH & Co. KG – akt. 24.11.10 MH