



Secure Business Connectivity

HOB RD VPN NetAccess 1.4

**Der vollständige Netzwerk-Zugriff auf alle Ressourcen im
Netzwerk der Zentrale – Flexibel, sicher, kostensparend**

HOB Remote Desktop VPN NetAccess – Allgemeine Beschreibung 3

Secure Remote Access – warum? 3

Secure Remote Access mit HOB – Ihr Wettbewerbsvorteil! 3

HOB RD VPN: Arbeiten, egal wo – Browser genügt! 3

Flexibilität weltweit! 3

Technisch Spitze 4

Kostensparend auf Euro und Cent! 4

Zertifiziert nach Common Criteria! 4

Einsatzmöglichkeiten von HOB RD VPN NetAccess 1.4 5

HOB RD VPN NetAccess 1.4 – Funktionalität 6

Überblick 6

Der HOB PPP Tunnel aus Sicht des Anwenders 6

Reconnect nach kurzen Unterbrechungen der Leitung 7

Der HOB WebSecureProxy in der Firmen-Zentrale 7

Der Web-Server integriert im HOB WebSecureProxy 7

Einspeisen der Netzwerk-Pakete ins Netz der Firmen-Zentrale 8

Die Authentifizierung am HOB RD VPN 9

HOB Enterprise Access für zentrale Konfiguration 10

Ausfallsicherheit 10

Optionale Produkte 10

HOB SCS – Unix-basiertes Betriebssystem . 10

Highlights von HOB RD VPN NetAccess 11

Vorteile von HOB WebSecureProxy auf einen Blick 11

Sicherheit und Performance 11

High Performance auf Standard-Hardware .. 11

Unterstützung von Tokens zur Authentifizierung 11

Unterstützung von Client-side-SSL-Zertifikaten z.B. auf Smartcards 11

Sichere E-Mails auf mobilen Endgeräten 11

Zentrale Administration über HOB Enterprise Access Administration 12

Integrity Check bevor der Client zugreifen darf 12

Ein TCP-Port ist genug 12

Anti Split Tunneling 12

Unterstützung für IPv6 12

Systemvoraussetzungen 12

HOB WebSecureProxy 12

Clients 13

Unternehmensprofil 14

Kontakte und Adressen 14

HOB Remote Desktop VPN NetAccess – Allgemeine Beschreibung

Secure Remote Access – warum?

Moderne Unternehmen stehen mehr denn je vor einer großen Herausforderung: Höchstmögliche Effizienz in allen Bereichen. Im IT-Umfeld ist dies vor allem durch zwei Maßnahmen zu erreichen: Zentralisierung der Anwendungen bei gleichzeitiger Dezentralisierung der Arbeitsplätze. Speziell die Ergänzung oder gar der teilweise Ersatz traditioneller Büroarbeitsplätze durch Home Offices kommt dabei nicht nur dem Unternehmen, sondern auch dem Wunsch der Menschen entgegen: Laut einer Forsa-Umfrage möchten rund zwei Drittel der Bundesbürger gerne regelmäßig zu Hause arbeiten. Manager auf Dienstreisen und Außendienstmitarbeiter oder Servicepersonal müssen ebenfalls regelmäßig außerhalb des Unternehmens arbeiten. Dazu kommen Wunsch oder Notwendigkeit vieler Firmen, auch Kunden oder Partner in das Firmennetz einzubeziehen, um einen noch schnelleren und besseren Service zu gewährleisten.

Secure Remote Access mit HOB – Ihr Wettbewerbsvorteil!

Die Möglichkeit sicher, kostengünstig, zuverlässig, überall und jederzeit auf die unterschiedlichsten Unternehmens-Ressourcen von diversen Plattformen und Endgeräten aus zugreifen zu können wird daher für viele Unternehmen zukünftig ein nicht zu unterschätzender Wettbewerbsvorteil sein.

HOB RD VPN: Arbeiten, egal wo – Browser genügt!

Nutzen Sie diese Herausforderung zu Ihrem Vorteil mit HOB RD VPN! Die innovative Software-Lösung ermöglicht Ihnen die schnelle und sichere Bereitstellung aller Ihrer Geschäftsdaten und Anwendungen. Sie liefert Ihnen und Ihren Mitarbeitern – ganz unkompliziert auf Knopfdruck – Intranet, Server oder den Arbeitsplatzrechner virtuell nach Hause, ins Hotel oder ans Abflug-Gate. Und wenn Ihr Rechner ausgeschaltet ist? Kein Problem: Starten Sie ihn einfach per Mausklick!

Flexibilität weltweit!

HOB RD VPN ist eine Software-Suite, die speziell für den sicheren Zugriff von TCP/IP-Netzen, also Internet, WiFi / WLAN oder UMTS, auf unterschiedlichste Ressourcen im Firmennetzwerk konzipiert wurde. Damit bietet Ihnen HOB eine einzigartige, durchgängige Software-basierte Lösung für den Remote-Zugriff vom Firmennetz bis zum Frontend. Dabei ist es unerheblich, ob sich Ihre Daten und Anwendungen auf Windows Terminal Servern, virtualisierten Windows-Systemen, Unix/Linux-Servern, einem klassischen Host oder sogar Einzelplatzrechnern befinden. Je nach Konfiguration und Autorisierung können Sie und Ihre

Mitarbeiter auf Ihre Dateien zugreifen, diese mit dem Zielsystem austauschen und drucken. Genauso, als säßen Sie direkt an Ihrem Arbeitsplatz in der Firma! Mit HOB RD VPN können Sie die Kommunikation über WLAN/WiFi aber auch innerhalb des Firmennetzwerks absichern.

Technisch Spitze

Traditionell eher unbewegliche Hardware-Appliance-Lösungen können mit Hilfe von HOB RD VPN durch eine flexible und schnell anzupassende „Software-Appliance“ ersetzt werden – in Anbetracht der zunehmenden Virtualisierung ein immer wichtigerer Aspekt! Eine technische Spitzenleistung ist HOB mit der Skalierbarkeit von HOB RD VPN gelungen: Auf Standard-Servern mittlerer Größenordnung wurde die Lösung mit 10.000 gleichzeitigen Verbindungen erfolgreich getestet.

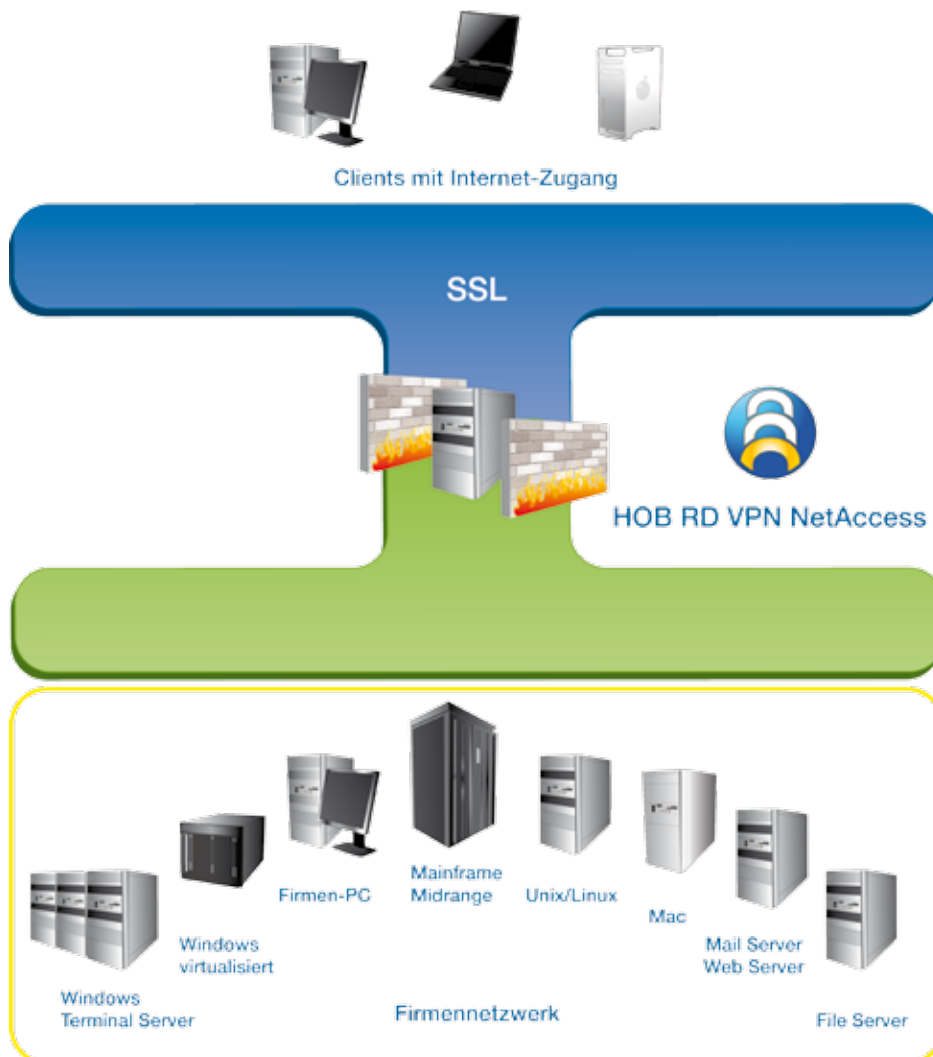
Kostensparend auf Euro und Cent!

Einzigartig an HOB RD VPN ist, dass die Software nur einmal zentral auf dem Server in der Firmenzentrale installiert wird. Anschließend kann der Zugriff sofort von jedem beliebigen Client via Internet und Browser erfolgen. Auch das oft so heikle Thema Drucken wird mit HOB RD VPN einfach gelöst: Der Anwender kann seine Dokumente einfach auf einem Drucker ausgeben, der am lokalen Rechner angeschlossen ist. Druckertreiber auf den Unternehmensservern werden damit überflüssig. Hoher Administrationsaufwand und regelmäßige Aktualisierungen auf den Clients gehören der Vergangenheit an!

Zertifiziert nach Common Criteria!

In seiner Software-Suite hat HOB die Vorteile herkömmlicher SSL VPNs und IPsec VPNs miteinander verschmolzen und so eine Lösung geschaffen, die höchste Sicherheits- und Compliance-Anforderungen erfüllt. Dies wird u.a. durch verschlüsselte Verbindungen, gängige Authentifizierungsverfahren wie Token, Smartcard (auch via PKCS#11) und SSLClient- Zertifikate erreicht. Bei Bedarf kann konfiguriert werden, dass die Verbindung in das Firmennetz erst dann aufgebaut wird, wenn sichergestellt ist, dass das Endgerät über ein Antivirusprogramm inklusive aktueller Virensignaturen verfügt. Insofern ist es nur eine logische Konsequenz, dass die zentralen Bestandteile dieser Lösung vom Bundesamt für Sicherheit in der Informationstechnik (BSI Zertifikat BSI-DSZCC- 0260-2004) zertifiziert wurde.

Einsatzmöglichkeiten von HOB RD VPN NetAccess 1.4



HOB RD VPN NetAccess 1.4 – Funktionalität

Überblick

Der HOB PPP Tunnel ist Teil der umfassenden Security-Lösung HOB RD VPN. Beim PPP Tunnel erhält der Benutzer vollständigen Netzwerk-Zugriff auf alle Ressourcen im Netzwerk der Zentrale.

Der Netzwerk-Zugriff funktioniert auch umgekehrt, von der Zentrale aus auf alle Ressourcen am Client.

Der Zugriff ist äußerst performant durch Komprimierung. Durch Authentifizierung und SSL-Verschlüsselung ist der Zugriff sicher. SSL als Übertragungs-Protokoll hat den Vorteil, dass es von allen Netzwerk-Devices unterstützt wird; dies ist bei vergleichbaren Lösungen mit IPSec nicht der Fall. Bei kurzen Unterbrechungen der Leitung zum Client erfolgt automatisch ein Reconnect.

Der HOB PPP Tunnel unterstützt als Client-Plattformen Windows Vista, Windows 7, Apple Mac, Linux, FreeBSD und Solaris.

Der HOB PPP Tunnel aus Sicht des Anwenders

Der Anwender startet seinen Browser und verbindet sich zum HOB RD VPN in der Zentrale seiner Firma. Dort muss er sich (nach Verfahren wie unten beschrieben) authentifizieren und erhält das Grund-Bild des HOB RD VPN. Soweit vom Administrator vorgegeben erscheint dort der Menü-Punkt „Start PPP Tunnel“.

Wird dieser Menü-Punkt angewählt dann startet der PPP Tunnel, in der Task-Bar von Windows erscheint ein Tray-Icon.

Mit dem Browser können nach dem Start des PPP Tunnels andere Web-Seiten angewählt werden. Auch beim Schließen des Browsers bleibt der PPP Tunnel erhalten.

Der Benutzer kann jetzt über den PPP Tunnel auf alle Ressourcen im Netzwerk der Zentrale zugreifen, alle Protokolle wie TCP, UDP oder ICMP gehen durch den PPP Tunnel.

Die Steuerung des PPP Tunnels erfolgt über das Tray-Icon. Klickt der User auf das Tray-Icon, so erscheint eine Statistik. Von dem Fenster mit der Statistik aus kann der Benutzer auch den PPP Tunnel beenden.

Für die Benutzung des PPP Tunnels ist nichts lokal installiert und der Benutzer muss auch keine Administrator-Rechte besitzen. Insbesondere werden keine speziellen Treiber am Client verwendet. Lediglich eine Java Virtual Machine (JVM) muss auf dem Client installiert sein.

Ist am Rechner des Benutzers der PPP Tunnel gestartet, dann kann der Benutzer gleichzeitig auf andere Ressourcen im Internet zugreifen; der Benutzer kann auch andere Funktionen des HOB RD VPN benutzen, bei richtiger Installation in der Zentrale gehen diese Verbindungen dann nicht über den PPP Tunnel. Man nennt dies auch Split-Tunnel.

Durch die Windows-Firewall am Client kann ein Administrator auch Zugriff auf andere Ressourcen im Internet sperren, wenn Split-Tunnel nicht erwünscht ist. Dazu konfiguriert der Administrator die Windows-Firewall im Client entsprechend, dies ist keine Funktion von HOB RD VPN.

Reconnect nach kurzen Unterbrechungen der Leitung

Geht kurzzeitig die Netzwerk-Verbindung des Clients verloren, so muss der Benutzer (nachdem die Verbindung wieder aktiv ist) den PPP Tunnel nicht neu starten sondern der PPP Tunnel resynchronisiert sich automatisch mit dem Netzwerk in der Zentrale. In den meisten Fällen laufen Anwendungen am Client ohne Störung weiter.

Die Netzwerk-Verbindung des Clients geht unter anderem dann verloren wenn der Provider die DSL-Leitung kurz unterbricht und danach die DSL-Leitung neu aufgebaut wird. Die meisten Provider tun dies einmal täglich.

Der HOB WebSecureProxy in der Firmen-Zentrale

Kernkomponente von HOB RD VPN ist die Server-Komponente HOB WebSecureProxy. Die aktuelle Version des WebSecureProxy oder kurz WSP ist 2.2, verfügbar für Windows, Linux und Unix in insgesamt 11 verschiedenen plattform-spezifischen Versionen.

Der WSP kann auch in HOB SCS laufen, dem Open-Source Unix-based Server-Betriebssystem von HOB. HOB SCS steht für Secure Communications Server.

Der WSP arbeitet mit SSL-Verschlüsselung. HOB SSL unterstützt alle gängigen Verschlüsselungs-Algorithmen, auch AES (Advanced Encryption Standard) mit bis zu 256 Bit Schlüssellänge.

Der Web-Server integriert im HOB WebSecureProxy

Der HOB WSP hat einen eingebauten Web-Server, die Komponenten des HOB PPP Tunnels werden von diesem integrierten Web-Server heruntergeladen. Es werden ca. 300 Kilobytes heruntergeladen. Dies dauert nur wenige Sekunden.

Sind die Client-Komponenten des HOB PPP Tunnels einmal heruntergeladen, so müssen diese nicht bei jeder neuen Verbindung wieder heruntergeladen werden; die Komponenten

werden am Client gecacht. Werden im WSP neuere Komponenten installiert, so stellt dies ein Client beim nächsten Verbindungs-Aufbau fest und lädt dann diese neueren Komponenten herunter.

Der WSP benötigt für die Server-Authentifizierung über SSL ein Zertifikat nach X.509 welches z.B. auch in Web-Servern mit SSL /HTTPS benutzt wird.

Einspeisen der Netzwerk-Pakete ins Netz der Firmen-Zentrale

Der HOB WSP Version 2.2 hat keine speziellen Funktionen für den PPP Tunnel, die Daten des PPP Tunnels werden nur ver- und entschlüsselt. Im Firmen-Netz läuft das HOB Programm xbiggw16 welches die TCP-Verbindung zum Client aufsplittet und zu L2TP über UDP umsetzt.

Diese L2TP Pakete gehen dann zu einer Hardware / Software Komponente die nicht von HOB geliefert wird und die Pakete ins Netzwerk einspeist.

Diese L2TP Funktionalität ist ein Industrie-Standard und entsprechend in vielen Komponenten eingebaut.

Solche Komponenten können z.B. sein:

- Microsoft Windows RRAS
- Linux mit L2TP Server wie z.B. OpenSwan
- Router mit integrierten L2TP Server

Es kann vorteilhaft sein, die Netzwerk-Pakete aus dem PPP Tunnel direkt im Firmen-Netzwerk einzuspeisen, nicht in der DMZ. Die Security wird bei dieser Lösung weiterhin in der DMZ terminiert.

Der Client bekommt über PPP eine IP-Adresse und routet Pakete aus diesem Adressbereich über den PPP Tunnel.

Bekommt der Client eine IP-Adresse aus der DMZ, so kann er alle Geräte in der DMZ erreichen, Geräte im eigentlichen Firmennetz nur über optionales NAT (Network Address Translation).

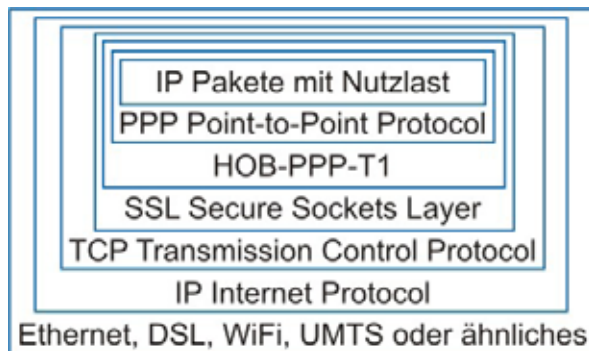
Bekommt der Client aber eine IP-Adresse aus dem Firmen-Netzwerk, so können alle Geräte direkt erreicht werden.

Teil des HOB PPP Tunnels ist eine Komponente welche NAT im IP-Header und in DNS-UDP-Paketen durchführt. Dadurch können mit dem PPP Tunnel im Firmen-Netzwerk mehrere von einander getrennte Netzwerke (Sub-Netze) erreicht werden.

Diese Komponente ist xl-sdh-ppp-pf-01 welche als Zusatz (Server-Data-Hook) im WebsecureProxy läuft.

Diese Komponente dient optional auch als DNS-Server; bestimmte URLs können über diesen integrierten DNS-Server aufgelöst werden was die Adressen aus dem DNS-Server im Firmen-Netzwerk überschreibt.

Grund für diesen DNS-Server ist es dass bestimmte URLs, welche sowohl eine Adresse im public Internet als auch (unterschiedlich) im Firmen-Netzwerk haben, so aufgelöst werden dass andere Komponenten des HOB RD VPN die Verbindung nicht über den PPP Tunnel aufbauen sondern weiterhin direkt über das public Internet.



HOB PPP Tunnel Netzwerk Stack

Die Authentifizierung am HOB RD VPN

Authentifiziert sich ein Benutzer, so kann dies auf drei unterschiedliche Arten erfolgen, in der jeweiligen Installation festgelegt:

- Userid und Passwort
- Token mit one-time-password wie RSA SecurId, Secure Computing Premier Access oder VASCO DigiPass
- Zertifikat für Client-Authentifizierung über SSL (gespeichert z.B. auf einer Smart-Card)

Die Authentifizierung erfolgt über den Browser der über SSL / HTTPS mit dem WSP verbunden ist. Deshalb ist bereits die Authentifizierung verschlüsselt und sicher.

Der HOB WSP hat eine integrierte Radius-Schnittstelle so dass die Authentifizierung gegenüber allen gängigen Radius-Servern erfolgen kann.

Integriert im HOB WSP ist auch eine OCSP-Schnittstelle (Online Certificate Status Protocol) damit überprüft werden kann ob Client-SSL-Zertifikate gültig sind.

Integrity Check bevor der Client zugreifen darf

Der Client kann optional nach bestimmten Kriterien überprüft werden bevor der Zugriff auf firmeninterne Daten erlaubt wird. Dies wird bei Bedarf bei der Installation im Firmennetz festgelegt.

HOB Enterprise Access für zentrale Konfiguration

Die Konfigurations- und Authentifizierungs-Daten wie Userid und Passwort sind entweder im XML-File der WSP-Konfiguration abgespeichert (HOB RD VPN Compact, in Vorbereitung) oder in der Komponente HOB Enterprise Access.

HOB Enterprise Access benutzt entweder eine integrierte Datenbank oder die Daten werden in einem LDAP-Server abgelegt. HOB Enterprise Access unterstützt alle gängigen LDAP-Server wie auch Microsoft Active Directory oder OpenDS.

Legt HOB Enterprise Access Daten in einem LDAP-Server ab so werden die entsprechenden Strukturen durch eine Schema-Erweiterung angelegt.

Ausfallsicherheit

In größeren Installationen können alle Komponenten des HOB RD VPN im Firmennetz redundant ausgelegt werden. Man hat keinen single-point-of failure und unterbrechungsfreier Betrieb ist möglich.

Optionale Produkte

HOB SCS – Unix-basiertes Betriebssystem

HOB SCS (Secure Communication Server) ist ein gehärtetes, stabiles Unix-basiertes Betriebssystem, das bewährte Open Source Technologien nutzt. Durch die Verbindung von HOB SCS mit HOB RD VPN wird HOB SCS zur vollwertigen Software-Appliance. Installation, Wartung und Administration werden minimiert. HOB SCS in Verbindung mit HOB RD VPN bietet zusätzliche Vorteile hinsichtlich Sicherheit, Stabilität, Performance und Skalierbarkeit.

Highlights von HOB RD VPN NetAccess

Vorteile von HOB WebSecureProxy auf einen Blick

- Hochgradig skalierbar
- Gestestet mit 10.000 parallelen Verbindungen
- Schnittstellen zu Radius und OCSP
- 10 plattformspezifische Versionen

Sicherheit und Performance

Der HOB WebSecureProxy (WSP) ist das zentrale Sicherheitselement der HOB RD VPN-Lösung. Er wird auf einem Server in der DMZ installiert und ermöglicht die SSL-gesicherte Kommunikation der Client-Anfragen zu firmeninternen Servern und Applikationen. Unterstützt werden alle gängigen Verschlüsselungsverfahren inklusive AES mit bis zu 256 Bit Schlüssellänge. Im HOB WSP ist ein Web-Server integriert, der HTML-Anmeldeseiten und die Zugriffssoftware für den Client (z.B. HOB PPP Tunnel) als Java-Applet bereitstellt. Die Authentifizierung erfolgt bereits vor dem Laden des Applets, um erhöhte Sicherheit zu gewährleisten. Der HOB WSP kann auf vielen Plattformen eingesetzt werden, ist hoch skalierbar und daher für kleine wie große Installationen geeignet. Selbst im Rahmen umfangreicher IT-Infrastrukturen werden nur wenige, leistungsfähige Server benötigt. Dies reduziert die Störanfälligkeit gegenüber herkömmlichen SSL-Appliance Boxen und ist zudem kostengünstig.

High Performance auf Standard-Hardware

Auch bei großen Benutzerzahlen ist eine hohe Performance sichergestellt – dies zeigen Tests mit 10.000 gleichzeitigen Verbindungen auf einem Server mittlerer Größenordnung.

Unterstützung von Tokens zur Authentifizierung

Zusätzliche Sicherheit kann durch die Verwendung von Authentifizierungssystemen, sog. Tokens, erreicht werden. Unterstützt werden alle Systeme mit RADIUS-Schnittstelle, u.a. RSA SecurID, SafeWord PremierAccess und Vasco Digipass.

Unterstützung von Client-side-SSL-Zertifikaten z.B. auf Smartcards

HOB RD VPN unterstützt die Verwendung von Client-Zertifikaten, die beim SSL Verbindungsaufbau ausgelesen werden.

Sichere E-Mails auf mobilen Endgeräten

Der HOB WebSecureProxy kann auch zur Abschottung eines E-Mail-Servers vor dem direkten Zugriff aus dem Internet dienen. Die Kommunikation zwischen E-Mail-Client und HOB WSP erfolgt dabei über POP3S, IMAPS und/oder SMTPS.

Zentrale Administration über HOB Enterprise Access Administration

Mit Hilfe von HOB Enterprise Access, der zentralen Benutzerverwaltung, kann der Administrator sämtliche Konfigurationsdaten zentral verwalten. HOB Enterprise Access unterstützt LDAP oder greift über diese Schnittstelle auf Verzeichnisdienste wie z.B. Microsoft Active Directory oder OpenDS zu.

Integrity Check bevor der Client zugreifen darf

Der Client kann optional nach bestimmten Kriterien überprüft werden bevor der Zugriff auf firmeninterne Daten erlaubt wird. Dies wird bei Bedarf bei der Installation im Firmennetz festgelegt.

Ein TCP-Port ist genug

Jegliche Kommunikation in das Firmennetz kann über einen einzigen TCP-Port erfolgen, üblicherweise über den HTTPS-Port 443.

Anti Split Tunneling

Mit HOB Anti Split Tunneling können Sie verhindern, dass ein Benutzer auf andere Netzwerke zugreift, während er mit HOB RD VPN arbeitet. Dadurch erhöhen Sie die Sicherheit des Systems deutlich.

Unterstützung für IPv6

Der HOB WebSecureProxy unterstützt Verbindungen mit dem Client über IPv6.

Systemvoraussetzungen

■ HOB WebSecureProxy

- Windows (x86, EM64T, Itanium)
- Oracle Solaris (Sparc, x86-EM64T)
- IBM AIX
- HP-UX (Itanium)
- Linux (x86, EM64T, Itanium)

Der HOB WSP Version 2.2 hat keine speziellen Funktionen für den PPP Tunnel, die Daten des PPP Tunnels werden nur ver- und entschlüsselt. Im Firmen-Netz läuft das HOB Programm xbiggw16 welches die TCP-Verbindung zum Client aufsplittet und zu L2TP über UDP umsetzt.

Diese L2TP Pakete gehen dann zu einer Hardware / Software Komponente die nicht von HOB geliefert wird und die Pakete ins Netzwerk einspeist.

Diese L2TP Funktionalität ist ein Industrie-Standard und entsprechend in vielen Komponenten eingebaut.

Solche Komponenten können z.B. sein:

- Microsoft Windows RRAS
- Linux mit L2TP Server wie z.B. OpenSwan
- Router mit integrierten L2TP Server

■ Clients

- Windows 7
- Windows Vista
- Mac OS X 10.4 oder neuer
- Linux (x86, EM64T)
- FreeBSD
- Oracle Solaris

Auf der Client-Seite kann jeder beliebige Browser mit voller Unterstützung von Java (1.4.2 oder höher) verwendet werden.

Unternehmensprofil

Die HOB GmbH & Co. KG ist ein mittelständisches deutsches Unternehmen, das innovative Software-Lösungen entwickelt und weltweit vermarktet.

Die Kernkompetenzen des bereits 1964 gegründeten und erfolgreichen Unternehmens umfassen Server-based Computing, sicheren Remote-Access sowie VoIP und Virtualisierung, die in kleinen, mittleren und Großunternehmen zum Einsatz kommen. Produkte sind durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) nach Common Criteria zertifiziert.

HOB beschäftigt in seiner Cadolzheimer Zentrale und seinen Geschäftsstellen weltweit ca. 120 Mitarbeiter, die Hälfte davon in der Entwicklung. HOB unterhält Niederlassungen in Frankreich, Malta, Niederlande sowie USA und Mexiko.

Kontakte und Adressen

HOB GmbH & Co. KG

Schwadermühlstr. 3
90556 Cadolzburg
Telefon (09103) 715 0
Telefax (09103) 715 271

E-Mail
marketing@hob.de
support@hob.de

Telefon Hotline
(09103) 715 3161

Fax Hotline
(09103) 715 271

Auslandsniederlassungen

Eindhoven, Malta, New York, Paris

Besuchen Sie uns im World Wide Web:

<http://www.hob.de>
<http://www.hobsoft.com>