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

HOBLink VPN

Das IPsec-VPN von HOB

Oktober 2008

Technology
Future
Communication

In diesem Whitepaper sind die wichtigsten Informationen über das Produkt HOBLink VPN (Version 1.8) sowie seine Vorteile beschrieben. Detaillierte Informationen finden Sie im Administrator-Handbuch von HOBLink VPN.

Allgemein

Die weltweite Verfügbarkeit von preisgünstigen, zuverlässigen und den jeweiligen technischen Anforderungen angepassten Internetanschlüssen veranlasst Unternehmen dazu, das Internet als Netzwerk-Infrastruktur für die Unternehmenskommunikation zu nutzen. Leider bringt das Internet nicht nur Vorteile mit, sondern auch so manchen Nachteil. Der für Unternehmen wesentliche Nachteil besteht in der mangelhaften Sicherheit der Kommunikation in Bezug auf Authentifizierung der Kommunikationspartner, sowie Integrität und Vertraulichkeit der Daten.

Bei den Kommunikationswegen früherer Zeiten (Ende-zu-Ende Wählleitungen, Standleitungen, Paketvermittlungsnetze wie X.25/Datex-P etc.) wurde dem Kommunikations-Dienstleistungserbringer entsprechendes Vertrauen entgegengebracht. Beim Internet trifft das jedoch nicht mehr zu, nicht zuletzt aufgrund der unüberschaubaren Anzahl von Providern, die an einem Kommunikationsweg beteiligt sein können. Hier muss letztlich der Anwender selbst geeignete Maßnahmen ergreifen, um den erforderlichen Sicherheitsstandard zu erreichen. Eine allgemein anerkannte Maßnahme bildet die im Jahr 1998 mit den RFCs 2401 ff standardisierte VPN-Technologie mit den Protokollfamilien IPsec und IKE/ISAKMP. Der Name VPN (Virtuelles Privates Netzwerk) gibt dabei einen Hinweis darauf, dass der Anwender mit Hilfe dieser Technik seine eigene Netzwerkstruktur auf der Basis des Internet aufbauen kann, die seine Bedürfnisse bezüglich der o.g. Sicherheitskriterien erfüllt. IPsec ist auf der Netzwerkebene (Layer 3) angesiedelt. Es stellt somit eine Netzwerk-Infrastruktur für alle IP-Protokolle zur Verfügung und ist transparent für alle darauf aufsetzenden Transportprotokolle und Anwendungsprogramme.

HOBLink VPN

Das Produkt HOBLink VPN stellt eine reine Software-Implementierung der IPsec-VPN-Technologie dar. Diese Software wird auf Standard-Windows-Computern installiert, von Windows 2000 bis Windows 2008 Server, und von Standard 32 Bit x86 Prozessoren über EM64T bis zu Intels Itanium. Diese Software-Lösung bietet gegenüber einer Appliance den enormen Vorteil einer beliebigen Skalierbarkeit, sowohl bezüglich der Leistungsfähigkeit eines Systems, als auch bezüglich der eingesetzten Hardware-Komponenten zur Unterstützung unterschiedlicher Netzwerk-Topologien und Internet-Anschlusstechniken. Die jeweils benötigte Hardware kann mit preisgünstigen Standard-PC-Komponenten bzw. mit entsprechenden Adaptern realisiert werden. Insbesondere der Austausch dieser Standardkomponenten ist preisgünstig und leicht durchführbar.

Die Installationssoftware für HOBLink VPN enthält drei Komponenten, die optional ausgewählt werden: die eigentliche VPN-Software sowie die Komponenten EA-Server und EA-Admin. Die Abkürzung „EA“ steht dabei für „Enterprise Access“, die für die meisten HOB-Produkte verwendete zentrale Komponente zur unternehmensweiten Konfiguration und Administration. HOBLink VPN ist in das Konzept von HOB Enterprise Access integriert. Wenn ein Unternehmen durch den Einsatz eines anderen HOB-Produktes bereits

einen EA-Server betreibt, kann dieser auch für HOBLink VPN verwendet werden. Die VPN-spezifischen Komponenten des EA-Admin sind die Konfiguration, das Remote Management, das Lesen von Logdateien und die Verwaltung von Benutzerzertifikaten. Das Zusatzprogramm HOB Security-Manager zur Erstellung von Wurzel- und Endzertifikaten ist ebenfalls im EA-Admin enthalten, und zwar in zwei Ausprägungen: Für die IPsec-VPN-Verbindungen und für die administrativen SSL-Verbindungen. Diese Komponenten zur zentralen Verwaltung und Konfiguration der VPN-Clients und –Gateways und zur Erstellung einer eigenen PKI sind bereits im Basispaket von HOBLink VPN enthalten und müssen nicht extra lizenziert werden.

Die Module

Ein IPsec-VPN besteht aus Gateways und Clients. Zwischen Gateways werden sogenannte VPN-Tunnel aufgebaut. Die an den Gateways angeschlossenen Firmen-Netze werden über diese Tunnel verbunden. Gateways sind damit die „Router“ für das VPN, denn sie verteilen eingehende Datenpakete aus den angeschlossenen Intranets in die VPN-Tunnel zu den jeweiligen VPN-Gegenstellen - Gateways und Clients. Clients dagegen stellen auf Benutzer-PCs installierte Software dar, die dem Benutzer durch einen Tunnel zu einem Gateway den Zugriff auf ein angeschlossenes (privates Firmen-) Netzwerk ermöglicht. Eine dedizierte Hardware-Komponente ist somit nur für das Gateway möglich.

Mit HOBLink VPN steht dem Kunden ein System zur Verfügung, das sich als Gateway und Client einheitlich darstellt. Es gibt nur eine Installationssoftware und eine gemeinsame Konfigurations- und Administrationsoberfläche. Dieser Vorteil der einheitlichen Bedienungsoberfläche für Gateways und Clients vermindert den Schulungs- und Verwaltungsaufwand erheblich.

Installation

Die Installation von HOBLink VPN ist sehr einfach, sie kann von jedem PC-Anwender mit Administrationsrechten durchgeführt werden. Es ist möglich, eine automatisierte und kundenspezifische Installation zusammenzustellen. Die Automatisierung wird durch die Aufzeichnung einer Installation mit allen Eingabedaten erreicht. Durch das Starten der Installation mit dem Kommando „setup.exe /r“ läuft die Installation im sog. Record-Modus und erstellt die Protokolldatei „setup.iss“ im Windows-Verzeichnis.

Befindet sich diese Datei später bei weiteren Installationen in dem Ordner, in dem das Installationsprogramm gestartet wird, so wird die Installation von HOBLink VPN automatisch im sog. Silent-Modus ausgeführt. Dabei werden die Benutzereingaben aus der vorher erstellten Protokolldatei gelesen. Ein Anwender muss eine derart vorbereitete Installations-CD nur noch in das CD-Laufwerk einlegen und per einfachen Mausklick die Installation starten. Während der Installation sind dann keinerlei Benutzereingaben (wie z.B. Auswahl der zu installierenden Komponenten, Lizenzschlüssel u.a.) mehr erforderlich. Darüber hinaus können lokale Konfigurationsdateien in einem AddOn-Verzeichnis mitgeliefert werden. Alle im AddOn-Verzeichnis vorhandenen Dateien und Verzeichnisse werden bei der Installation in das Installationsverzeichnis kopiert. Damit können zusätzliche kundenspezifische Dateien und Verzeichnisse installiert werden.

Beispiele für derartige kundenspezifische Installationsdaten sind: Das Startregelwerk, die Startoptionen, oder Zertifikate für die VPN-Verbindungen oder auch für die SSL-gesicherten administrativen Verbindungen. Für den anschließenden Betrieb von HOBLink VPN sind keine Administratorrechte mehr erforderlich.

Zentrale Administration

Die Administration der VPN-Komponenten kann sowohl lokal als auch zentral erfolgen. Bei der zentralen Administration kommt der bereits genannte EA-Server zum Einsatz, der wiederum entweder mit lokaler Speicherung arbeitet oder auch einen LDAP-Dienst (z.B. Microsoft Active Directory) zur Speicherung der Verwaltungsdaten nutzen kann. In beiden Fällen erfolgt die Speicherung der Konfigurationsdaten in einer Verzeichnisstruktur, so dass mit Vererbung über die Baumstruktur und/oder über die Gruppenzugehörigkeit von Benutzern bzw. Gateway-Objekten gearbeitet werden kann. Damit können einzelne Datenobjekte sowie Zusammenfassungen von Konfigurationsparametern in sog. Vorlagen, ja sogar ganze Benutzerkonfigurationen an strategischen Punkten im Verzeichnisbaum angelegt und an die jeweils benötigten Stellen vererbt werden.

Für den Administrator ergeben sich daraus zwei große Vorteile: Der Konfigurationsaufwand wird erheblich reduziert und die Gefahr von Fehlkonfigurationen wird geringer. Gerade die Parameter zur Konfiguration von IKE und IPsec in kommunizierenden VPN-Geräten müssen übereinstimmen bzw. bei optionalen Parametern Schnittmengen bilden. Kleinste Fehler führen dazu, dass keine VPN-Verbindung zustande kommt. Durch die Möglichkeit der Vererbung können Objekte (wie z.B. IP-Netze) oder Vorlagen ein einziges Mal an zentraler Stelle im Verzeichnis angelegt und an die einzelnen Client- und Gateway-Konfigurationen vererbt werden. Damit ist die Übereinstimmung dieser Konfigurationsparameter in den jeweiligen Geräten sichergestellt.

Ein der IPsec-Protokollfamilie nachgesagter Nachteil bezüglich der Komplexität der Konfiguration wird somit bei HOBLink VPN mehr als kompensiert.

Zusätzlich ergibt sich daraus die Möglichkeit mit Pre-Shared Key Authentifizierung zu arbeiten, wobei viele Gegenstellen den selben Pre-Shared Key verwenden können, ohne dass dieser den Gegenstellen bekannt ist, da er in einer geerbten Konfiguration nicht sichtbar ist. Außerdem kann damit eine VPN-Gegenstelle gezwungen werden, mit einer zentral vorgegebenen Konfiguration zu arbeiten, die natürlich auch das Paketfilter-Regelwerk enthält, mit dem z.B. Split-Tunneling unterbunden werden kann.

HOB empfiehlt seinen Kunden generell, mit der zentralen Administration zu arbeiten. VPN-Clients und -Gateways bauen eine SSL-gesicherte Verbindung zum zentralen EA-Server auf, um von dort die VPN-Konfigurationsdaten zu laden. Dieser hat die Daten entweder in einer lokalen Verzeichnisstruktur oder in einem LDAP-Verzeichnis gespeichert. Der EA-Server unterstützt folgende LDAP-Server: Microsoft Active Directory, IBM Directory Server, iPlanet Directory Server, Novell Directory Server, Siemens DirX LDAP, OpenLDAP, und ein „Generischer LDAP-Server“ ist konfigurierbar.

Zur gegenseitigen Authentifizierung der Kommunikationspartner (Gateways und Clients) unterstützt HOBLink VPN alle gängigen Methoden: Pre-Shared Key, Benutzername/Passwort, RADIUS (auch mit entsprechenden One-Time-Passwort Tokens, mit oder ohne Challenge), LDAP sowie RSA- und DSA-

Zertifikate. Smartcards für Benutzer-Zertifikate werden über das Microsoft Crypto-API unterstützt.
Bei den rein technischen Merkmalen glänzt HOBLink VPN mit seiner Vollausstattung. Dazu einige Beispiele: Als Verschlüsselungsalgorithmen werden neben Oldtimern wie Blowfish, DES und 3DES u.a. auch das für Software-Verschlüsselung optimierte AES mit bis zu 256 Bit langen Schlüsseln angeboten. Für die Schlüsselerzeugung sind die Diffie-Hellman Gruppen bis MODP 8192 Bit und die Elliptic Curve Gruppen bis zu ECN GF571 implementiert. Selbstverständlich werden die IPsec-Protokolle AH und ESP einzeln oder auch in Kombination unterstützt, wobei zusätzlich noch eine Komprimierung der Daten (IPCOMP) aktiviert werden kann. Weitere Parameter wie „Perfect Forward Secrecy“ (PFS), Replay Detection und SA-Lifetimes für IKE und IPsec sind einstellbar. Für das IKE-Protokoll stehen die Modi “Main Mode”, “Aggressive Mode” und “Hybrid Aggressive Mode” mit XAUTH zur Verfügung.

Sicherheit

Ein weiterer erheblicher Nachteil des Internet besteht in den vielfältigen Angriffsmöglichkeiten für die angeschlossenen Geräte. Davon sind zunächst einmal die genannten Gateways und Clients gleichermaßen betroffen, insbesondere wenn sie mit einer öffentlichen IP-Adresse direkt an das Internet angeschlossen und damit aus dem Internet erreichbar sind. HOBLink VPN kann jedoch unerwünschten Datenverkehr verhindern.

Der bei der Installation in den Kernel eingebundene ***BITS-Treiber (Bump Into The Stack)*** kontrolliert alle IP-Pakete entsprechend des konfigurierten Firewall-Regelwerks. Dieser Treiber wird bei der Installation automatisch auf alle vorhandenen und ebenso später auf alle nachträglich installierten Netzwerk-Adapter und Wählverbindung gebunden. Die Kontrolle der IP-Pakete erstreckt sich nicht nur auf alle eingehenden Pakete, sondern auch auf die ausgehenden Pakete, entsprechend einer „Stateful Inspection Engine“. Dies bedeutet z.B., dass zuerst eine ausgehende Verbindung aufgebaut werden muss, bevor ein zu dieser Verbindung gehörendes eingehendes IP-Paket durchgelassen wird. Nach Beendigung der TCP-Verbindung wird überhaupt kein Paket mehr durchgelassen, solange bis eine neue Verbindung in der zugelassenen Richtung aufgebaut wurde.

Eine Besonderheit von HOBLink VPN besteht darin, dass es zwischen zwei Regelwerken umschaltet. Das lokal konfigurierte sog. Startregelwerk gilt immer dann, wenn VPN nicht gestartet ist, z.B. direkt nach dem Starten des PCs. Insbesondere dann, wenn die Konfigurationsdaten von einem zentralen EA-Server geladen werden, muss eine Internetverbindung bestehen, bevor VPN gestartet werden kann. In dieser Phase könnte bereits ein Angriff erfolgen. Dieser wird jedoch durch eine entsprechende Einstellung des Startregelwerks verhindert. Diese Firewall-Regelwerke sind nicht nur im Gateway implementiert, sondern auch im Client.

Verbindungen

HOBLink VPN ist in der Lage, alle in einem Windows-Betriebssystem darstellbaren Internet-Verbindungen zu verwenden. Bei der Verwendung fester IP-Adressen wird der VPN-Adapter, über den IPsec-Pakete gesendet und empfangen werden, anhand der IP-Adresse automatisch ermittelt. Im einfachsten Fall, wenn nur eine einzige Netzwerkverbindung zur Verfügung steht, ist dazu keine Konfiguration erforderlich, auch dann wenn die IP-

Adresse dynamisch ist. Stehen mehrere Verbindungen (LAN und WAN) zur Verfügung, dann wird, wenn vorhanden, eine bereits aufgebaute Wählverbindung verwendet. Andernfalls ist eine Konfiguration im eingebauten Netzwerk-Verbindungsmanager erforderlich. Dort kann eine priorisierte Liste von Internetverbindungen (LAN und WAN) konfiguriert werden.

HOBLink VPN kann dann insbesondere auch Wählverbindungen (wie z.B. DSL) starten und beenden. Steht eine Verbindung gerade nicht zur Verfügung, dann kann HOBLink VPN automatisch die nächste Verbindung verwenden bzw. auch starten. Besonders für VPN-Clients ist dies eine sehr vorteilhafte Funktion. Auch während einer bestehenden VPN-Verbindung wird erkannt, wenn die Internetverbindung nicht mehr zur Verfügung steht. Dann startet HOBLink VPN automatisch die nächstmögliche Internetverbindung und einen neuen VPN-Tunnel, so dass der Benutzer sofort wieder auf das Firmennetzwerk zugreifen kann.

Wählverbindungen sind durch den breiten Einsatz von preisgünstigen DSL-Internetverbindungen sehr häufig anzutreffen. Meistens werden dabei dynamisch zugewiesene IP-Adressen verwendet. HOBLink VPN ist speziell daraufhin optimiert, dass es mit derartigen Internetanschlüssen arbeiten kann. Durch die direkte Unterstützung des Dynamischen DNS ist es sogar möglich, VPN-Verbindungen zu einem VPN-Gateway aufzubauen, das sich an einem DSL-Anschluss mit dynamischer IP-Adresse befindet.
VPN-Geräte (Clients und Gateways) können i.d.R. mehrere VPN-Verbindungen gleichzeitig aufbauen, üblicherweise im sog. Tunnel-Modus. Gateways können dabei mehrere Tunnel zu mehreren anderen Gateways betreiben.

Die Anzahl dieser Tunnel ist häufig begrenzt, insbesondere bei Hardwarelösungen.
Die Softwarelösung HOBLink VPN dagegen hat diesbezüglich keinerlei Beschränkungen, weder hinsichtlich der Anzahl der Gegenstellen noch der Anzahl der VPN-Tunnel. Eine weitere Besonderheit des HOBLink VPN Clients besteht darin, dass er mehrere Gateway-Gegenstellen gleichzeitig unterstützen kann. Viele VPN-Clients anderer Hersteller können VPN-Verbindungen nur zu einer einzigen Gegenstelle herstellen, von der sie auch die Konfiguration geladen haben.

Bei HOBLink VPN erfolgt das Laden der Konfiguration von einem eigenen Dienst (EA-Server), der unabhängig von VPN betrieben wird. Der HOBLink VPN Client unterliegt bezüglich der VPN-Gegenstellen und der Anzahl der Tunnel keinerlei Beschränkungen. Bei der Verwendung von virtuellen Adaptern und virtuellen IP-Adressen wird automatisch für jedes weitere Gegenstellen-Gateway ein weiterer virtueller Adapter installiert. Die jeweiligen virtuellen IP-Adressen können jeweils entweder in der Client-Konfiguration festgelegt werden, oder sie werden dem Client für den jeweiligen virtuellen Adapter über den IKE-Konfigurations-Modus vom Gegenstellen-Gateway auferlegt.

Ein Gateway kann IPsec-Tunnelverbindungen an mehreren Adaptern gleichzeitig terminieren. Dadurch kann z.B. neben den normalen VPN-Verbindungen durch das Internet zusätzlich etwa ein WLAN angeschlossen werden, aus dem heraus VPN-Clients über VPN-Verbindungen Zugriff auf das Firmennetz erhalten.

Einfache Implementierungen von IKE und IPsec funktionieren manchmal nicht in Umgebungen mit sog. NAT-Geräten, z.B. in Form eines Internet-Zugangsrouter. Es gibt jedoch verschiedene Techniken, die den Betrieb von IPsec-VPN auch in solchen, häufig anzutreffenden, Konstellationen ermöglichen. In HOBLink VPN sind diese Techniken vollständig implementiert: Automatische Erkennung von NAT-Geräten, Einpacken der IPsec-Pakete in

UDP, und UDP-Session Keepalive (s.u.a. RFCs 3715, 3947, 3948). Der Einsatz dieser Techniken wird von der Konfiguration gesteuert. Für das Einpacken der IPsec-Pakete in UDP (UDP-Encapsulation) gibt es drei Möglichkeiten: generell immer, generell nie, oder automatisch in Abhängigkeit vom Vorhandensein eines NAT-Gerätes. Die dritte Möglichkeit setzt voraus, dass die automatische Erkennung von NAT-Geräten aktiviert ist. UDP-Encapsulation vergrößert den Overhead durch das zusätzliche UDP-Protokoll. Ob es tatsächlich erforderlich ist hängt von weiteren Betriebsbedingungen und insbesondere von den technischen Möglichkeiten des NAT-Gerätes ab. Beim UDP-Session Keepalive werden in konfigurierbaren zeitlichen Abständen kleine Pakete mit einem Byte Nutzdaten gesendet, um den Eintrag in der NAT-Tabelle des NAT-Gerätes aufrecht zu erhalten. Die meisten NAT-Geräte löschen diese Tabelleneinträge gerade für UDP-Verbindungen nach kurzer Zeit, typisch 30 Sekunden. Diese Konfigurationsmöglichkeiten in HOBLink VPN können pro VPN-Gegenstelle bzw. pro VPN-Tunnel erfolgen. Somit ist eine sehr detaillierte optimale Anpassung an die jeweils unterschiedlichen Betriebsbedingungen möglich.

HOBLink VPN als Zugangsrouter

Das HOBLink VPN Gateway kann auch als Internet-Zugangsrouter arbeiten. Ein separater Internet-Router ist dann nicht mehr erforderlich. Die in HOBLink VPN implementierten NAT-Funktionalitäten ermöglichen dynamisches und statisches NAT für normale Internetverbindungen. Die vielfältigen Übersetzungsmöglichkeiten erlauben das Übersetzen von Quelladresse, Zieladresse und Portnummer. NAT kann auch für Verbindungen eingesetzt werden, die durch das IPsec-VPN geleitet werden. Hier ist es sogar möglich, ganze IP-Netze zu übersetzen. Dies ermöglicht die Bildung virtueller IP-Netze.

Richard Wunderlich
HOB GmbH & Co. KG
Stand 02.10.2008