HOB GmbH & Co. KG
Schwadermuehlstr. 3
90556 Cadolzburg
Germany

Tel: 09103 / 715-0
Fax: 09103 / 715-271
E-mail: support@hobsoft.com
Internet: www.hobsoft.com

WhitePaper

HOBLink VPN

The IPsec VPN from HOB

March 2010

Technology
Future
Communication

This whitepaper contains the most important information on the product HOBLink VPN (version 1.8) as well as a description of its advantages. Detailed information can be found in the HOBLink VPN Administrators Guide.

General

The worldwide availability of economical, reliable and technically well-adapted Internet connections has encouraged enterprises to use the Internet as a network infrastructure for corporate communications. Unfortunately, the Internet brings not only advantages, but also risks. The biggest risk for enterprises is the insufficient security of communications as regards authentication of the communication partners, as well as the integrity and confidentiality of the data.

With earlier communications methods (end-to-end dial-up lines, leased lines, packet switching networks such as X.25/Datex-P, etc.) the communications service provider was quite simply trusted. With the Internet, that is no longer the case; not least because of the unknown number of Internet service providers that can be involved in a communication path. Here, the user himself has to take measures to achieve the required security level. A widely accepted measure is the standardized (in 1998 with the RFCs 2401 ff) VPN technology with the protocols IPsec and IKE/ISAKMP. As the name VPN (Virtual Private Network) implies, the user can use this technology to create his own network infrastructure based on the Internet, which infrastructure will satisfy the above-mentioned security requirements. IPsec is implemented on the network layer (layer 3). It is thus a network infrastructure available to all IP protocols and is transparent for all transport protocols and applications based on this protocol.

HOBLink VPN

The product HOBLink VPN is a pure software implementation of the IPsec VPN technology. This software is installed on standard PCs running Windows 2000 to Windows 2008 Server, and having standard 32 bit x86 processors over EM64T to Intel's Itanium. This software solution has a major advantage over an appliance: its scalability, both as regards the performance capability of a system, as well as the hardware components deployed to support various network topologies and Internet connection methods. The required hardware can be put together using economical, standard PC components, or with the appropriate adapters. These components can also be easily exchanged at a very low cost.

The installation software for HOBLink VPN contains three components, which can be optionally selected: there is the actual IPsec VPN software, and the administration components EA Server and EA Administration. The abbreviation "EA" stands for "Enterprise Access," which is the central administration and configuration software that can be deployed for the majority of HOB products. HOBLink VPN is fully integrated into the HOB Enterprise Access design. If a corporation already has an HOB product deployed and is already using an EA Server, this can also be used for HOBLink VPN. The VPN-specific components of EA Admin are the configuration, Remote Management, readout of log files and the management of user certificates. The add-on program HOB Security Manager for generating root and end certificates is also contained in EA Admin, and that in

two different versions: For the IPsec VPN connections and for the administrative SSL connections. These components for central management and configuration of the VPN clients and gateways and for the creation of a PKI are already included in the HOBLink VPN basic package and need not be additionally licensed.

The Modules

An IPsec VPN consists of gateways and clients. The so-called VPN tunnel is built between the gateways. The corporate networks linked to the gateways are connected over these tunnels. Gateways are thus the “routers” for the VPN, as they distribute incoming data packets from the connected Intranets in the VPN tunnel to the corresponding VPN peers, i.e., gateways and clients. Clients, on the other hand, are represented by the software installed on the users’ PCs, and allow the user to access a connected (private corporate) network over a gateway. A dedicated hardware component is thus only possible for the gateway.

With HOBLink VPN the customer has at his disposal a system that consists of both a gateway and a client. Only one installer is needed for these two components, which also have a common configuration and administration GUI. This advantage of having a uniform user interface for gateways and clients reduces the training and administration workload considerably.

Installation

Installing HOBLink VPN is very easy and can be done by any PC user with administrator rights. It is possible to construct an automated and customer-specific installation. Automation is achieved by recording an installation with all of the entry data. By starting the installation with the command “setup.exe/r,” the installation will run in “Record mode” and create the protocol file “setup.iss” in the Windows directory.

When this file is saved to the same folder in which the installation program is launched, the installation of HOBLink VPN will automatically be executed in silent mode. Hereby the user information will be read out of the previously created protocol file. A user has only to place such a prepared installation CD into the CD drive and start the installation with a mouse click. During installation, no user entries at all (e.g., selection of component to be installed, license keys, etc.) are required. Additionally, local configuration files can be delivered in an add-on folder. All files and folders in the add-on folder are copied to the installation directory during installation. Thus additional, customer-specific files and folders can be installed.

Examples of such customer-specific data are: The startup rules, the startup options, or certificates for the VPN connections or also for the SSL-encrypted administrative connections. To subsequently operate HOBLink VPN, no further administrator rights are needed.

Central Administration

The VPN components can be both locally as well as centrally administrated. For central administration, the above-mentioned EA Server is used, which works with either locally saved data or an LDAP service (e.g., Microsoft Active

Directory) for storing the administrative data. In both cases, the configuration data are saved to a directory structure, so that users or gateway objects can inherit settings over the tree structure or via assignment to groups. Thus individual data objects as well as grouped configuration parameters, even entire user configurations, can be created in templates at strategic points in the directory structure and then bequeathed to the corresponding positions.

The administrator this results in two big advantages: Configuration time and effort are considerably reduced and the risk of a faulty configuration is greatly diminished. It is necessary that the parameters for the configuration of IKE and IPsec in communicating VPN devices correspond to each other or, respectively, with optional parameters, form intersections. The most minor errors here would prevent any VPN connection from being made. The possibility of inheriting rights or settings enables one to create objects (e.g., IP networks) or templates only once at a central location and then bequeath them to the individual client and gateway configurations. Thereby the conformity of the configuration parameters in the corresponding devices assured.

Thus, the complexity of making configurations for the IPsec protocol suite, often seen as a disadvantage, is more than compensated for by HOBLink VPN.

Additionally resulting from this is the possibility to use pre-shared keys for authentication, whereby many terminals can use the same pre-shared key without the terminals being aware of this, as it is not visible in an inherited configuration. This can also be used to force a VPN terminal to work with a centrally assigned configuration which, of course, also contains the packet filter rule policy with which, for example, split tunneling can be prohibited.

HOB recommends its customers in general to use central administration. VPN clients and gateways establish an SSL-encrypted connection to the central EA Server, and loads the VPN configuration data from it. The EA Server has the data stored in either a local directory structure or in an LDAP directory. The EA Server supports the following LDAP servers: Microsoft Active Directory, IBM Directory Server, iPlanet Directory Server, Novell Directory Server, Siemens DirX LDAP, and OpenLDAP. You can also configure a “generic LDAP server,” if so desired.

For mutual authentication of the communication partners (gateways and clients), HOBLink VPN supports all current methods: Pre-shared key, username/password, RADIUS (also with corresponding one-time password tokens, with or without challenge), LDAP as well as RSA and DSA certificates. Smartcards for user certificates are supported via the Microsoft Crypto-API. HOBLink VPN impresses with its full assortment of state-of-the-art technical features. Here are just some examples: Supported encryption algorithms, in addition to the standard Blowfish, DES and 3DES, also include software-encryption optimized AES with up to 256-bit key lengths. The Diffie-Hellman groups up to MODP 8192 bit and the Elliptic Curve groups up to ECN GF571 are implemented for key generation. Of course, the IPsec protocols AH and ESP are supported either individually or in combination, whereby additional data compression (IPCOMP) can be activated. Further parameters, such as “Perfect Forward Secrecy” (PFS), Replay Detection and SA Lifetimes for IKE and IPsec can also be set. For the IKE protocol, the modes “Main Mode,” “Aggressive Mode” and “Hybrid Aggressive Mode” with XAUTH are available.

Security

A serious risk in using the internet is to be found in the multitude of possible attacks on the connected devices. The above-mentioned gateways and clients are equally affected by this, especially when they are directly connected to the Internet over a public IP address. HOBLink VPN can, however, block undesired data traffic.

The ***BITS driver (Bump In The Stack)***, integrated into the kernel during installation, inspects all IP packets in accordance with the configured firewall security policy. During installation, this driver is automatically connected to all existing network adapters and dial-up lines, and will also automatically be connected to all subsequently installed ones. Not only all incoming packets are subject to packet inspection, but outgoing packets are also inspected, corresponding to a “Stateful Inspection Engine.” This means, for example, that first an outgoing connection must be established before an incoming IP packet belonging to this connection is allowed to pass. After the TCP connection has been terminated, no packets at all are allowed to pass until a new connection in the permitted direction has been established.

A unique feature of HOBLink VPN is that it switches between two security policies. The locally configured, so-called Startup Options Policy is used when VPN is not started, e.g., directly after the PC is started. Especially when the configurations data are loaded from a central EA Server, there must already be an Internet connection before VPN can be started. In this phase, an attack could already take place. This, however, is prevented by an appropriate setting in the Startup Options Policy. These firewall rule policies are not only implemented in the gateway, but also in the client.

Connections

HOBLink VPN is capable of using all Internet connections that can be established with a Windows OS. When using fixed IP addresses, the VPN adapter, over which the IPsec packets are sent and received, is automatically determined via the IP address. In the simplest case, when only one network connection is available, no configuration is required, not even if the IP address is a dynamic one. If several connections (LAN and WAN) are available, then, if a dial-up connection has already been established, this will be used. If no dial-up connection already exists, a configuration must be made in the integrated Network Connection Manager. There, a prioritized list of Internet connections (LAN and WAN) can be configured.

HOBLink VPN can then also start and stop dial-up connections (e.g. DSL). If a connection is not immediately available, then HOBLink VPN can automatically use the next connection, or start it. This is a very advantageous function, especially for VPN clients. Even during an existing VPN connection, it can be detected whether the Internet connection will no longer be available. Then HOBLink VPN automatically starts the next possible Internet connection and a new VPN tunnel, so that the user can immediately re-access the enterprise network.

Dial-up connections are frequently used due to the wide-spread deployment of economical DSL Internet connections. For these, dynamically assigned IP addresses are most used. HOBLink VPN is specially optimized to work with such Internet ports. By directly supporting the dynamic DNS it is even possible to establish VPN connections to a VPN gateway that is on a DSL port with a dynamic IP address.

VPN devices (clients and gateways), as a rule, can make several VPN connections simultaneously, usually in the tunnel mode. Hereby, gateways can operate several tunnels to several other gateways.

The amount of these tunnels is often limited, especially with hardware solutions.
The software solution HOBLink VPN, however, has no restrictions here, neither as regards the amount of terminals nor the number of VPN tunnels. Another distinctive feature of the HOBLink VPN client is that it can support several gateway terminals simultaneously. Many VPN clients from other manufacturers can support VPN connections to only one terminal, from which they have also loaded the configuration.

With HOBLink VPN the configuration is loaded from an integrated service (EA Server), which is operated independently of VPN. The HOBLink VPN Client is not subject to any restrictions as regards VPN peers and the number of tunnels. When using virtual adapters and virtual IP addresses, an additional adapter is automatically installed for each additional peer gateway. The corresponding virtual IP addresses can each be determined either in the client configuration, or they can be assigned to the client for the corresponding virtual adapter via the IKE configuration mode from the peer gateway.

A gateway can simultaneously terminate IPsec tunnel connections at several adapters. Thereby, for example, in addition to the normal VPN connections over the Internet, a WLAN can be connected, from which VPN clients have access to the enterprise network over VPN connections.

Simple implementations of IKE and IPsec sometimes don't function in environments with so-called NAT devices, e.g., in the form of an Internet access router. There are however various methods that enable the operation of IPsec VPNs also in such, very often occurring, constellations. In HOBLink VPN, these methods are completely implemented: Automatic detection of NAT devices, encapsulating the IPsec packets in UDP, and UDP session keep-alive (see RFCs 3715, 3947, 3948, etc.). The configuration controls how these methods are used. For UDP encapsulation of the IPsec packets, there are three ways to go: generally always, generally never, or automatically, depending on the availability of a NAT device. The third possibility requires that the automatic detection of NAT devices is set to active. UDP encapsulation increases overhead due to the additional UDP protocol. Whether it is really required depends on other operational conditions and especially on the technical possibilities of the NAT device. With UDP session keep-alive, small packets with one Byte reference data are sent in configurable intervals, in order to sustain the entry in the NAT device's NAT table. Most NAT devices delete these table entries, especially for UDP connections, after a short time, usually after 30 seconds. In VPN, these configuration options can be made for each VPN peer or VPN tunnel. Thus an optimal adjustment on the corresponding, different operational conditions is possible.

HOBLink VPN as Access Router

The HOBLink VPN Gateway can also function as an Internet access router. A separate Internet router is then no longer needed. The NAT functionalities implemented in HOBLink VPN enable dynamic and static NAT for normal Internet connections. The diverse translation possibilities allow translation of source addresses, target addresses and port numbers. NAT can also be used for connections that are led through the IPsec VPN. Here it is even possible to

translate entire IP networks. This enables you to construct virtual VPN networks.

Richard Wunderlich
HOB GmbH & Co. KG
Edition: March 2010