HOB Cloud Suite 2.1

This document provides an insight into HOB software principles and philosophy. It outlines the resulting design, features and use-cases of the product.

Introduction

If you have corporate applications in your datacenter, or the cloud, and need to connect not only local users, but also a mobile workforce or your partners – then you will find this document useful. Remote access landscapes with “a history” typically lack a flawless and clear design.

IT professionals know: such environments are complex, heterogeneous - they tend to rely on various gateways and clients. They require high maintenance effort, have a considerable attack surface and most of the time still do not result in end-user satisfaction.

Principles

We at HOB believe in the strength of carefully designed and engineered connectivity software. This has always included efficiency and security aspects, and both are fundamental paradigms of our software development.

Beyond functionality, our priority is to provide tools that excel in the fields of scalability and standards compliance, making sure that no resources are wasted and interoperability with existing infrastructure is seamless.

The IT services known today as “cloud” emerged from various services that have been the focus of HOB software development for decades, because they involved remote computing. Our view on cloud services is based on the NIST Cloud Model (see NIST Special Publication 800-145). We added, however, the Managed Services as an additional layer on top of SaaS and put Community Cloud a bit aside due to its low adoption rate.

The server components of HOB products generally run on a large variety of platforms, ranging from bare metal or virtualized x86 Windows, BSD or Linux to IaaS cloud infrastructures.
In keeping with the philosophy outlined above, HOB came up with HOB RD VPN, a **rigorously efficient concept** that eliminates all superfluous detours and bypasses. In this product, the most popular HOB client components are combined with the WebSecureProxy (WSP) gateway. The result is a versatile all-purpose connectivity platform that enables secure remote access to virtually all relevant back-end infrastructure architectures.

For the gateway component WSP, HOB relies on mature concepts that originate from the days when compute resources were scarce and bandwidths next to non-existent. The use of assembly language and the “Transaction Program Monitor” principles results in unmatched gateway efficiency.

At the same time, HOB also provides an **enterprise-grade IPsec VPN gateway** that is as platform-agnostic as any HOB server component and very useful in various site-to-site scenarios.

The combination of both products, HOB RD VPN and HOBLInk VPN Gateway, turned out to be an ideal starting point for a **Cloud Connection and Security Broker** product. It is a multi-functional security control that operates from either the corporate datacenter or a cloud platform. It strengthens and complements services of other security product categories, for instance Cloud Access Security Brokers (CASB).

Many CASB-systems are only available as cloud services, rather SaaS-centric or originate from the IPS/IDS world. In consequence, they focus on specific aspects of enterprise security.
The HOB concept is to provide a broad coverage of use-cases. We prefer pro-active security to reactive techniques. This means we avoid vulnerabilities by design instead of remediating them with detection and prevention mechanisms. As an example, with a properly configured remote desktop connection, some kinds of attacks just will not work (due to the lack of full network access). Our culture of out-of-the-box thinking produces additional smart security features like this one: when the user transfers files or data (using the clipboard), our product is capable of invoking a malware scanner to guarantee that only “clean” data reaches the target platform. In order to avoid access methods with intrinsic exposure potential, especially client-to-site-tunnels, we use methods known as “sandboxing” to encapsulate applications. We also understand that sometimes those rather risky access types are unavoidable and therefore offer them as well, in the shape of a platform-independent PPP-tunnel. Here again, we put an idea on top and implemented an active tunnel management technique that avoids a negative feedback loop known as “TCP meltdown” which often impairs tcp-over-tcp-tunnels.

On the other hand, conventional connectivity products tend to lack sophisticated security technology such as proprietary and certified crypto-modules or an all-round design approach that covers all aspects in terms of

- Access paths - including screen-based interaction like for Remote Desktop sessions, protocol-based interaction like for file transfer or telephony
- Client devices - including all popular operating systems for the various device classes
- Scalability and elasticity - ranging from single all-in-one access hubs to meshed clusters with hybrid cloud integration

HOB Cloud Suite Characteristics

The combination of HOB RD VPN and HOBLink VPN Gateway enables companies to use the same software-based connectivity suite throughout the entire cloud journey. It covers multi-cloud scenarios and works across service models, be it IaaS or SaaS. Whatever type of user interface is required to connect remote users, be it direct browser access, classic remote desktop clients or tunneling – every option is on board.

The main design concepts and features of HOB Cloud Suite

- Secure Cloud Access
  - Modular design allows set-up on one single server or functional segregation
  - Supports physical or virtual platforms, runs on premise and in IaaS cloud environments
  - Multi-tenancy capability
  - Perfect companion for your cloud migration
  - Server components run on all major OS platforms
• **SSL Connectivity**
  - Optimized for each supported hardware and OS platform
  - Pure software – runs on all modern server OSes and virtualization platforms (can also be deployed on HOB’s hardened appliance operating system)
  - Modular design that makes development of additional features easy; currently available modules include server-based antivirus checking and mail server protection
  - Proprietary, closed-source, certified TLS 1.2 implementation with optimized performance
  - Uses hardware crypto support (if available)
  - Mandates SSL (TLS) encryption for all external communication (internet-facing side)
  - Controls outgoing communication with target filtering
  - Provides the access and download point for the clients
  - Protects internal web applications
  - Active-active n-node cluster capability including load balancing
  - Designed for use in the DMZ

• **IPsec Connectivity**
  - Proprietary, closed-source, certified IPsec (AH and ESP in tunnel mode) and IKE/ISAKMP (RFC 2401-ff) implementation
  - NAT-T (Traversal) / UDP Encapsulation - IPsec over any router, firewall and WLAN hotspot
  - Full-featured certificate management, includes certificate import and export

• **Central administration**
  - Role-based user administration (RBAC)
  - Schema- and template-based connection configuration
  - Integration interfaces supporting popular enterprise standards
    - directory services (LDAP / Active Directory)
    - multi-factor authentication (RADIUS)
      - A large number of two-factor authentication products is supported
    - single sign-on (Kerberos; HOB RD VPN only);
  - Full-featured certificate management, includes certificate import and export

• **Omni-client support**
  - Various connectors based on universal (Java, HTML5) or platform dependent technology establish graphical sessions to Microsoft Remote Desktop Servers, 3rd party terminal servers or VNC
  - Mobile apps for file transfer and IP telephony extend the remote office to smartphones and tablets
  - Multi-platform legacy emulations connect to systems such as IBM mid-range or mainframe computers, Linux/Unix and SIEMENS machines
  - Universal VPN tunnel app using PPP
  - Universal SSL tunneling client
  - Client compliance check (can be mandated)
• Complementary Targets
  • RDP Gateway for macOS (enables secure remote access to Apple workplace computers)
  • RDP Gateway for X.11 (enables secure graphical Unix remote access with contemporary RDP protocol)

• Complementary Implementation Options
  • HOB RD VPN is available as a software appliance featuring HOB Secure Communications Servers, a freeBSD-based, hardened OS platform
With its rich feature-set, HOB Cloud Suite goes beyond the capabilities of both SSL VPNs and IPsec VPNs and reflects the idea of a universal connectivity hub. It was specifically designed to support any kind of cloud transformation state, with a certain focus on hybrid IaaS/PaaS multi-cloud scenarios.

The starting point can be, as depicted above, an HOB RD VPN implemented on bare metal servers in the corporate DMZ. This ensures best performance and high availability (note that the HOB cluster technology does both HA and load balancing). Most of the functionality, such as access to internal web applications, is accessible directly from the browsers of the client systems (e.g., laptops or mobile devices). Some more advanced features require very simple, straightforward starting processes (no admin rights required) or a mobile app.

**Hybrid (IaaS) Cloud integration** can be covered similarly with the help of an IPsec tunnel (either HOBLink VPN Gateway or the flavor provided by the CSP) that is established between the CSP and the corporate datacenter. HOB RD VPN resides either in the local DMZ (recommended) or on CSP VMs.

Depicted below: implementation option with clustered WSP in public IaaS cloud, resulting in a fault tolerant, load-balanced remote access experience.

**Multi-Cloud environments** are best reflected by a cascade of HOBLink VPN gateways and either one single HOB RD VPN access point – or various, depending on factors such as latencies between the clouds and load balancing considerations.

Best practices for **SaaS integration** consist in a HOB Cloud Suite in a corporate datacenter or, in hybrid cloud scenarios, using the gateway that resides on the existing IaaS cloud platform. The advantages over direct SaaS access are the central encryption, IAM and policy enforcement.
Detailed cloud setup guides are available, especially for Amazon Web Services® and Microsoft® Azure®. HOB strongly recommends customers to refer to the comprehensive product documentation for configuration best practices, which includes examples, general infrastructure environment considerations and PKI setup advice. HOB provides complementary products that enable remote sessions (RDP) to Apple® Mac® or (Unix/Linux) X.11 platforms.

Security Methodology

From a security concept point of view, the product contributes and adds quality to a number of fields:

**Confidentiality and integrity** are ensured (mainly) by the use of TLS and IPsec-encryption. HOB relies on own protocol implementations that have been rigorously tested and undergone certifications (the SSL (TLS) module was subject to a Common Criteria EAL 4+ certification, usually recognized as maximum for software products, by the German Federal Office of Information Security).

Note: The cryptographic engine of HOB includes contemporary algorithms such as SHA-256 hash, AES-GCM symmetric and EC-DHE (RSA) key exchange. The protocol versions are TLS 1.0 thru 1.2 with 1.3 being in preparation. The modules leverage CPU-based crypto-routines, if available.

Administration features such as Role-Based Access Controls (RBAC) and standard interfaces to directory, authentication and single sign-on products support the confidentiality objective.

The built-in antivirus interface supports the integrity objective as well as the configurable, granular compliance check that helps to ensure the trustworthiness of the client platform.

**Availability** is ensured by the active-active “geo-cluster” design of the HOB RD VPN gateway. This is a default feature that comes at no extra cost – customers can set up as many cluster nodes as they want. The cluster balances the load of its nodes automatically. The proxy does not require downtimes for configuration changes (all new connections are spun up with changed parameters).

The compelling and logical design makes HOB RD VPN a real asset in the Governance, Risk and Compliance (GRC) context. It provides a single point for policy enforcement and transparency without introducing the risk of a single point of failure. The controls outlined above can directly mitigate many of the usual risks connected to remote access. The target filtering mechanism addresses compliance concerns.

By putting the omni-client support concept first, HOB ensures that end-user acceptance is high and helps to reduce shadow IT. At the same time, this contributes to a positive general perception towards corporate IT services.

The gateways used in this product provide effective security controls as called for in various standards, especially:

- **ISO/IEC 27001** “Information technology – Security techniques – Information security management systems – Requirements” (a well-known standard for ISMS) and
HOB Cloud Suite supports and/or enforces controls (fully or partially) as called for by **NIST SP800-53 Rev.4**:

Cost Considerations

Compared to conventional cloud access solutions, HOB Cloud Suite shows considerable cost advantages. The main factors include:

- The product comes with a wide array of connectivity options (for various clients and a multitude of target systems). It is not limited to “web-based access” or “IPsec tunnel” and greatly reduces cost for remote access software.
- Includes enterprise features such as a PKI tool or active-active n-node cluster capability that are otherwise subject to extra license fees.
- Reduces investments in detection and prevention systems on the client side, especially DLP.
- Industry standard software interfaces result in seamless integration into existing infrastructures.
- Surpassingly resource-efficient design, combined with the support of datacenter-grade server architecture, allows implementation on low-profile industry-standard hardware and cloud VMs.

HOB provides an optional **on-demand emergency licensing** that entitles customers to use the product for their entire work force (unlimited users and connections) to mitigate the negative effects of disasters.

The license model of HOB CloudSuite is data transfer based software lease (pure OPEX).

Supporting Ecosystem

For customer convenience, HOB Cloud Suite is available as a pre-installed and configured virtual instance and as a virtual machine.

The HOB product lifecycle management ensures a constant flow of improvements on all levels.

The support infrastructure includes
- Project supervision by a Key Account Manager
- (Sub)Project management by Technical Account Managers (SPOC)
- Product integration and setup by Field Engineers
- Q&A sessions and regular deep-dive webinars from field engineers
- On-site administrator training and product certification
- Germany-based operations support (up to 24x7)
Recap: HOB Cloud Suite Advantages at a Glance

- Connectivity Hub – simplifies the Cloud Journey for both, users and IT operations, by providing a single point of access no matter what type of client is used or which back-end infrastructure is in place, and adapts easily to changing environments
- Security Control – provides enterprise-grade authentication, access control and data-in-transit encryption with all industry standard integration options

Glossary

<table>
<thead>
<tr>
<th>ABBREVIATION</th>
<th>MEANING</th>
<th>EXPLANATION</th>
</tr>
</thead>
</table>
| CSP          | Cloud Service Provider | Company that sells cloud services. According to NIST cloud model, the characteristics of such services are:  
On-demand self service  
Measured service (pay per use)  
Rapid Elasticity  
Resource Pooling (shared compute resources)  
Broad Network Access |
| DLP          | Data Loss Prevention | Security product designed to protect company data against unwanted disclosure, for instance by downloading files on USB sticks. |
| DMZ          | Demilitarized Zone | Part of a corporate network that serves as a buffer between internal LAN and internet. All internet facing servers are located there and all incoming connections are terminated and inspected there. The technical setup is often outlined by two (logical) firewalls. |
| HA           | High Availability | This term is often used as a synonym for clustering (redundancy of compute resources to cover single instance failures). In fact, the term HA covers every measure that prevents service failures caused by single system failures. |
| IPS / IDS    | Intrusion Prevention / Detection System | Either host- or network based category of anti-malware products that strive to avoid or identify unauthorized access to computers or networks |
| ISMS         | Information Security Management System | A set of rules and processes within an organization that sustainably defines, manages, controls, supports and continuously improves information security; term often used in an ISO 27001 context. |
| RDP          | Remote Desktop Protocol | Proprietary Microsoft protocol that displays single applications or entire desktops generated by one system (usually a remote desktop server) on another (referred to as "client"), giving the latter keyboard and mouse full control over the session. |