Remote Access via Hardware Appliances or via Software?

When it comes to remote access solutions, the customer has the choice between hardware appliances for the gateway into the company headquarters or the use of a purely software-based solution.

When a hardware appliance is used, the question immediately arises: What happens in the event of a hardware failure, e.g., with spare parts? With hardware, one must always consider the possibility of a failure, due to moving parts and problems caused by incidental heating. Hard drives and power supply units often break down.

When a hardware appliance is used, the administrators have to learn how to work with it, both with the appliance's hardware as well as with the software running on it. More than one administrator has to learn this, as remote access should, of course, always be available.

The hardware appliance has to be integrated into the company network, network settings as well as, for example, DNS access have to be configured.

Often all users who are to have access and be able to authenticate themselves must be entered into the hardware appliance. This means additional work for zero-day users or when an employee leaves the company.

Data backups must be made for the configuration and other software in the hardware appliance.

Does a hardware appliance have advantages as compared to a standard server, e.g., due to special hardware components?

These days, hardware appliances for remote access are based on standard servers; they may have more network interface cards (NICs) built into them.

With switches, which are built with ASICs, i.e., with hardware logic, due to the fast connections, software cannot switch the packets very quickly. But routers and everything else used for access over the public Internet use standard components; fast Internet connections are also very expensive. The Internet connections used for remote access can run very well with standard components; the logic is implemented in the software and not in ASICs.

If the number of users connected over remote access grows, then a larger capacity hardware appliance must be purchased. This means additional cost.

How is this with a software solution for remote access?

The software is installed on standard servers; in the computer centers one can find brand name servers which also can be used for remote access.

Administrators are very well versed in the hardware and basic software components used. Additional training for these components is not necessary. Also, the integration into the network functions with remote access software solutions exactly as with other software.

Standard servers also provide support for encryption, which is used for remote access.
The prevalent encryption algorithm today is AES, Advanced Encryption Standard. AES is secure and widely disseminated. New Intel CPUs provide AES encryption in the hardware, directly in the CPU. Intel calls this function AES-NI. Other processor manufacturers also offer AES encryption in hardware or have this function in the roadmap.

Brand name servers are often already equipped with several network cards (NICs), installing additional network cards requires very little effort and they are also economical. When deployed in the DMZ (demilitarized zone), different network cards are often used, one for the public Internet and one for access to the corporate network.

Brand name servers have specific management functions integrated. Administrators are familiar with the management functions of the deployed brand name servers, having to manage other hardware, such as appliances for remote access, means additional work.

Software solutions for remote access can also be operated virtually, e.g., with VMware or Microsoft Hyper-V. If one server fails or maintenance work needs to be done, the installed software can be transferred to another server quickly and easily.

Software solutions can be well integrated into the corporate infrastructure. Belonging to this is access to the LDAP system, in which all user settings are stored. Often, Active Directory from Microsoft is the LDAP system used.

Backing up data can be done with tools that are already in service.

Integration with Kerberos is possible: this provides users with secure single sign on for remote access. The logs generated during the remote access operation can be archived, making auditing possible.

Each of the software solution’s configurations can be saved to a repository; this serves, on the one hand, the documentation, on the other hand, in the event of an auditing, older configurations can be accessed.

Summary: The use of a purely software-based solution offers many advantages. Administration is less burdened, the company saves on cost.

Sometimes the following argument is made for a hardware appliance: It is hardened and thus more secure. I know of no technical factor that justifies this statement.
Conversely, it is true that the better administrators know the solution, the less often will a security gap result from incorrect configurations.

And it is easier for administrators to gain proficiency with a software-based remote access solution.

HOB RD VPN is certified by the German Federal Office for Information Security according to the Common Criteria EAL 4+ (Certificate # BSI-DSZ-CC-0832-2014).
HOBLink VPN Gateway is certified “Security Made in Germany”.