The term VPN is familiar to many people and has been increasingly discussed in recent months. After all, a VPN enables secure access to internal IT resources – even for devices that are located outside the company network. And this is urgently needed, especially when working from the home office. But what exactly is a VPN and what is hidden behind all the abbreviations and terms that are often mentioned in this context – such as VPN gateway, Site-to-Site-VPN, Per-App-VPN, Split Tunneling, SDK or ZTNA? We explain what it is and reveal that a VPN solution today can do much more than you think.
VPN and its endpoints

The abbreviation VPN stands for Virtual Private Network. A VPN is a protected connection that enables employees to gain secure access to sensitive internal data even outside the company network – via a so-called tunnel. The ends of the tunnel are called VPN endpoints and have different names on the company and user side:

- **VPN gateway**: The VPN gateway is the endpoint on the company side. It forms the barrier to the company network. If a device wants to access the internal network, it must first authenticate itself at the gateway.

- **VPN client**: The endpoint on the user side is a VPN client that must be installed on the laptop, tablet or smartphone. It is responsible for logging on to the VPN gateway and, after successful authentication, establishes the encrypted tunnel to the gateway.

The users can be individual persons or entire networks:

- **Site-to-Site-VPN**: A Site-to-Site-VPN connects complete networks with each other. This is the case, for example, when devices from different company locations are to access the network of the main site.

- **Client-to-Site-VPN**: A Client-to-Site-VPN is used when individual users connect to the corporate network from outside the corporate network – for example, from their home office, on the train or at the airport.

How much VPN do you want?

A VPN can be used to different degrees. The possibilities depend, among other things, on the operating system and – if it is a solution integrated into the Unified Endpoint Management System – on the UEM provider. Basically, however, the following approaches can be distinguished:

<table>
<thead>
<tr>
<th>Per-Device-VPN</th>
<th>Per-User-VPN</th>
<th>Per-App-VPN</th>
<th>Per-Account-VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>all connections of an end device are secured via VPN</td>
<td>all connections in a specific user context are secured via VPN</td>
<td>only certain applications/programs are secured via VPN</td>
<td>only certain accounts are secured via VPN (this means that a VPN is only used, for example, when the e-mail client connects to an internal server, but not for private accounts)</td>
</tr>
</tbody>
</table>

The usage can be limited even further: For example, you can specify that a connection is only tunneled for certain web pages. If an employee accesses the intranet via the Safari browser, a VPN is used. If he visits the public company website, he can do so without VPN. This is called **split tunneling**.
That’s all?

For years, the term VPN was always used in the same way and was clear to administrators: VPN stood for security. But security is not equal to security. Today, VPN technologies can solve the security aspect in a completely different way and go far beyond previous approaches. Two terms were introduced in this context:

01 Strict access control using „Zero Trust Network Access“ (ZTNA):

Some VPN solutions make it possible to handle access requests based on the „Zero Trust“ approach. This means that no user is trusted until he proves that he is actually allowed access to the resources. This is done with very precise and identity-based access control.

02 Contextual access management using a „Software Defined Perimeter“ (SDP):

VPN solutions can proceed in an especially intelligent way during user verification by controlling not only his access data, but also real-time contextual information such as the time of access, the location of the device or the network used. If these factors in combination do not result in a risk, the request is approved. But – in line with the „least privilege“ idea – only for the application for which the user has requested access. If something changes in the individual factors, the access permission can be withdrawn again.
More than “just” security

If you look at today’s VPN solutions, you will see that many providers have also developed in other regards in recent years. They have added features to their solutions that improve even more aspects of mobile working:

01 Stable connections:

VPN solutions can also ensure that network quality is improved, and connections are kept even when changing networks. In particular, video conferences, which are so important today, can be conducted smoothly.

02 Better cost control:

VPN solutions can provide insight into the use of applications and data and set restrictions. These can be used to define when, for example, a private app like Netflix may be used – e.g. not during working hours, where productivity is affected, and not outside WiFi networks, where the company tariff is impacted.

03 User-friendly authentication:

Some VPN solutions allow authentication at the VPN gateway using a certificate located on the end device. This is much more secure than logging in with a user name and password – and above all, more convenient. The same applies to cloud services: Here, a VPN can be used for authentication and thus enable secure and above all simple access to cloud services.

Today’s VPN solutions not only ensure that data is just as well protected on the road as it is in the corporate network. They contribute to more reliable connections, better cost control, and a more user-friendly and secure login. This not only increases the security of mobile working, but also the productivity and satisfaction of employees.
Want to learn more about VPN security?

Contact us if you would like to learn more about the features of modern VPN solutions and take advantage of a 30-day trial of a proven solution.

+ 49 221 474 550
+1 310 980 2781
sales@ebf.com
www.ebf.com

About EBF

Your Digital Workplace and Enterprise Mobility Advisor

EBF is your ideal specialist partner for the workplace of the future. We work with our customers and partners to design solutions for complex enterprise mobility challenges and develop customized digital workplace concepts. Our products, services, and solutions make digital, mobile, and flexible working a reality, increasing employee and company productivity while maintaining the highest security standards, with a manageable IT workload, and leading to positive user experiences. We can help you make your company a truly digital workplace.