LANCOM White Paper

Home office – working securely from home

Digital technologies are a basis for greater flexibility in today's working world, and they make life easier for many employees: Reconciling work and family life, unnecessary travel to in-person meetings, the responsibility for remote sales regions, working as a sales representative for foreign companies—these are typical issues where the answer is a home office. Even in unusual situations, such as extreme weather, quarantine or flooding, a company that enables its employees to work from home puts business-continuity management into practice and stays functional. However, there are still companies that continue to have concerns about implementing telework, among other things for reasons of security and cost. This white paper presents solutions for implementing a modern, secure, and cost-effective VPN infrastructure.

VPN – extending the company network into the home

"My home is my office“ is no longer a distant dream, but a simple and economic reality thanks to today’s networking solutions. Site connectivity uses technology to completely integrate teleworking stations into company networks. The attraction of these solutions is that employees can work from home just as if they were in the office—with complete access to e-mail, networks, servers, telephone, and digital services. Even the devices located at the home offices are remotely configured by the central IT department. An inexpensive networking medium comes with the standard Internet line via DSL, cable or even mobile, which practically every household has today. The connection is secured by a virtual private network (VPN).

In the same way as a company networks its sites, VPN enables mobile employees and home offices to be quickly and, most importantly, securely integrated into the company network. The only requirement is one small software tool: A VPN client on your laptop or PC. Once configured, one click is all it takes to establish a strongly encrypted VPN channel over the best available medium. Mobile devices such as smartphones and tablet PCs can also communicate securely with the company via VPN. An app is used to establish a secure VPN connection to the central company gateway.

Home office is gaining ground in Germany too

Companies have recognized the potential of teleworking. In 2014 only around 20% of German companies allowed employees to work from home, although that share almost doubled over the next four years: By 2018, 39% of companies offered teleworking to their employees, as reported by the German digital association, Bitkom[1]. 46% of respondents also believe that teleworking will become increasingly common in the next five years—although a full 50% do not expect any increase at all.

[1] https://www.bitkom.org/Presse/Presseinformation/Vier-von-zehn-Unternehmen-setzen-auf-Homeoffice

The kind of concerns that companies raise about using home offices can be resolved with clear rules with regard to home-office working. Concerns about data security (22%) and the costs for equipping home workplaces (12%) are also named. However, modern VPN solutions offer secure encryption and are also quite inexpensive.

The solution for the secure home office – LANCOM Advanced VPN Client

The LANCOM Advanced VPN Client for the operating systems Windows and macOS provides users with a secure VPN tunnel to access the company network with a single click. Whether the user is in the home office, abroad or on the train is immaterial. Equipped with a stateful inspection firewall, the software VPN client automatically detects secure and unsecure networks for protected communication over the Internet at all times.

VPN tunnels are established using state-of-the-art encryption technologies such as the modern and efficient VPN protocol IKEv2. Also, the LANCOM Advanced VPN Client supports the latest encryption algorithms including AES-CBC or AES-GCM, the signature functions SHA-256, SHA-384 or SHA-512, and current Diffie-Hellmann groups.

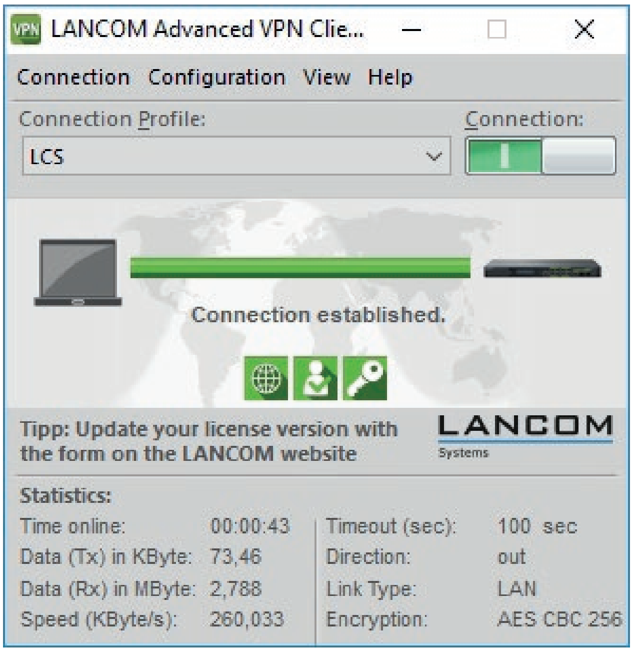
The VPN handshake between the VPN gateway at the company and the software VPN client takes place in different ways—depending on the company's size and requirements:

- For small to medium-sized companies, this is very easy to set up and operate by entering a password (authentication by pre-shared key – PSK)
- For larger scenarios with higher security requirements: The use of IKEv2 with digital certificates
- For large-scale scenarios with Windows server infrastructure: IKEv2 EAP for authentication via the Windows server by means of user name and password
- For large-scale scenarios with central user administration: Direct and inexpensive authentication via a RADIUS server

With the support of both IPv4 and the increasing number of IPv6 connections, smooth workflows are assured. And thanks to seamless roaming, VPN connections remain intact even when changing the connection medium. For example, this keeps VPN connections alive even when traveling by train and moving between mobile phone cells. Likewise, users in buildings roaming from cellular to Wi-Fi or Ethernet enjoy an "always on" experience.

Especially in hotels or public hotspots, firewalls often block IPsec communication (ports 500 or 4500). However, by initiating the connection via the IPsec-over-HTTPS (based on the NCP VPN Path Finder technology), the IPsec VPN is encapsulated in an additional SSL header (port 443, as with HTTPS).

Furthermore, the company network is relieved of load if Internet traffic can be routed directly to the Internet, such as when an employee is in a trusted network. Data intended for the company network is still routed through the VPN tunnel (split tunneling). However, if the employee is in an open, unencrypted Wi-Fi, i.e. with an unsecure connection, all data is securely encrypted by the VPN tunnel to the central office, and from there it is securely routed to the Internet (full tunneling).



Connection Profile: LCS

Connection:

Connection established.

Tipp: Update your license version with the form on the LANCOM website

Statistics:

Time online:	00:00:43	Timeout (sec):	100 sec
Data (Tx) in KByte:	73,46	Direction:	out
Data (Rx) in MByte:	2,788	Link Type:	LAN
Speed (KByte/s):	260,033	Encryption:	AES CBC 256

Despite the wide range of features, configuring the LANCOM Advanced VPN Client on employee laptops is easy: VPN access to the company headquarters is easily set up with a 1-Click setup wizard. The configuration is exported to a file and then imported to the VPN client as a profile. It includes all of the information about the configuration of the VPN peer at the headquarters, and is supplemented by randomly generated values, such as the pre-shared key. This allows multiple VPN access accounts to be created for employees and set up in the shortest possible time—a real time saver for administrators.

A collection of helpful instructions for the configuration are available in the LANCOM Knowledge Base.

A worthwhile investment

The investment in security infrastructures for mobile working is manageable. On the company side, a single device is all you need, namely a VPN-capable router, a central VPN gateway or a VPN-capable firewall. The only equipment you need on the employee laptops is the inexpensive LANCOM Advanced VPN Client—which is also compatible with products from many manufacturers..

An investment that pays off—on both sides.

Teleworking spares employees their commute, which saves time and fuel costs. Companies improve employee productivity and can cut down on office space to save on rent and running costs. What's more: You position your company as flexible and family-friendly and score points in the tough competition for specialists and managers.

Summary

Our world is constantly changing—mobility is becoming a vital factor for many companies and their employees. A VPN client enables employees to use their laptops to connect to the Internet and enjoy secure access to your company network and confidential data, wherever they are. This gives them maximum flexibility, whether they are traveling on business or working from home. Companies often cite security and costs as arguments against the use of home offices. However, these turn into potential savings with a modern and efficient VPN solution from LANCOM.

Frequently Asked Questions (FAQ)

Can I extend my LANCOM router with additional VPN connections?

With the LANCOM VPN Option, the number of VPN channels can be extended depending on the LANCOM device. For example, all LANCOM routers of the 17xx series are shipped with 5 VPN tunnels and can also be expanded to up to 25 tunnels. See: https://www.lancom-systems.com/products/software-options/lancom-vpn-option/

Can I import my VPN profile into several end devices and apply it simultaneously?

VPN user profiles can basically be imported into several VPN client installations (e.g. different computers). However, only one session at a time is possible per VPN profile.

Where can I see how many VPN connections are active?

Active VPN client connections can be clearly viewed via LANmonitor.

As an administrator, can I deactivate VPN connections centrally?

Selected VPN dial-up connections can be deactivated via LANconfig or WEBconfig if required.

What scope of functionalities does the demo version of the LANCOM Advanced VPN Client offer?

The LANCOM Advanced VPN Client offers a free 30-day demo version with the full range of functions. Please note: A maximum of three unlicensed VPN connections can be established to the remote VPN station.

Can I also use the LANCOM Advanced VPN Client in combination with LANCOM R&S®Unified Firewalls?

Yes, with the current operating system LCOS FX 10.4, LANCOM R&S®Unified Firewalls offer the option of setting up import profiles for the LANCOM Advanced VPN Client.