LANCOM SYSTEMS

lancom-systems.com

LCOS 10.72

More power for branch networking

With the new LCOS version 10.72 Rel, including Advanced Mesh VPN, you not only significantly improve the performance of classic VPN scenarios, but also expand the options for realizing individual networking topologies freely and flexibly. Instead of routing all data traffic via the central gateway, direct VPN tunnels are dynamically established from branch to branch as required.

- → Traffic Shaping
- → Maximum protection of minors
- → Two-factor authentication – double security for your VPN

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.72

LCOS 10.72 Highlights	
Advanced Mesh VPN	With classic, star-shaped VPN site networks, in which all branches are only connected via the headquarters and not directly to each other, the Internet line of the headquarters quickly becomes the bottleneck of the entire communication. With Advanced Mesh VPN, the branch offices are now directly interconnected, resulting in significantly less traffic at the headquarters and thus higher performance. The VPN tunnels are established dynamically as soon as data traffic is transported from one branch office to another. If there is no more communication, the VPN connection is terminated dynamically as well.
Protection of minors according to official regulations	With LCOS 10.72 RelI, you can now maximize the protection of underage end users, e.g. in schools or youth facilities. For example, the official website list of the „Bundesprüfstelle für jugendgefährdende Medien" (German Federal Review Board, BPjM) is now also part of the LANCOM Content Filter Option or available separately via the software extension LANCOM BPjM Filter Option. This means that URLs whose content is officially classified as harmful are not accessible to the relevant target group in Germany. Continuous updates and extensions of this list are guaranteed.
Two-factor authentication – double security for your VPN	Whenever a high level of security for your sensitive data is required or, for example, compliance guidelines in your company demand it, double protection of network access via your LANCOM Advanced VPN Client is ideal. Thanks to two-factor authentication (IKEv2 EAP-OTP), you can now protect VPN access and thus also your network from unauthorized access. You can specify that users can only log in via the LANCOM Advanced VPN Client if they use two-factor authentication when logging in. In this case, the VPN password is supplemented by a time-based one-time password, which can be generated in an authentication app (e.g. Google Authenticator) on the cell phone. This feature can be used with all devices that have at least 25 VPN tunnels (either already integrated or upgraded with LANCOM VPN Option).

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com

LANCOM, LANCOM Systems, LCOS, LANcommunity, and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions. 12/22