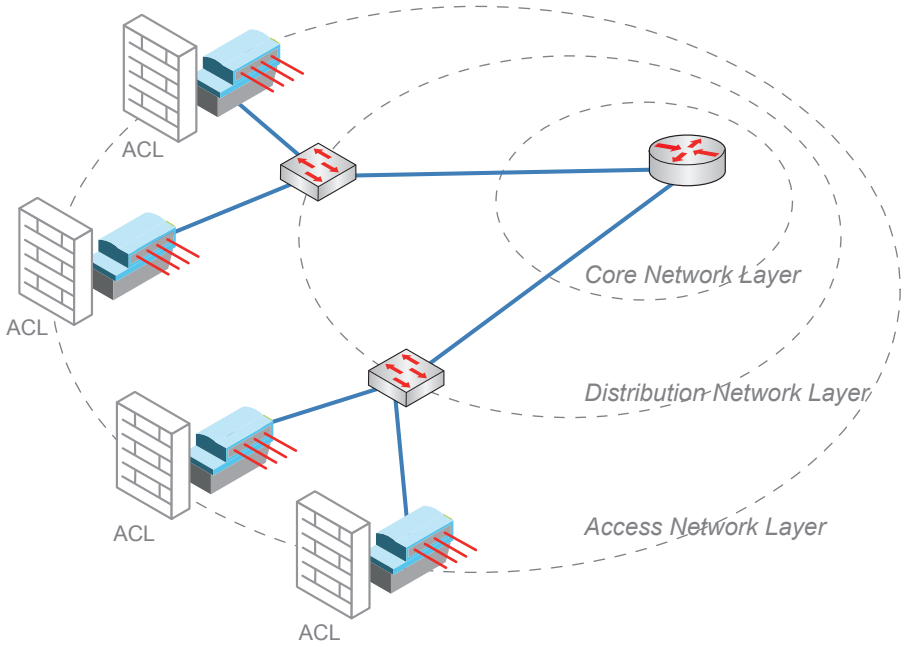
Application Note

Contakt:
Nexans Deutschland GmbH
Advanced Networking Solutions
Phone: +49(0) 2166 27-2220
E-Mail: sales.ans@Nexans.com

Increased network security in FTTO infrastructures through Access Control Lists (ACL / NACL)



The topic of IT security has become increasingly important in recent years and has become an integral part of planning modern corporate IT networks. IT security is not just about technology and protocols. The human factor is just as important - if not even more so! After all, most cyber-attacks start with nothing more than a single email.

In order to increase security in Fibre To The Office (FTTO) networks, a technical security measure has been introduced in addition to client and user authentication: The use of Network Access Control Lists (NACL or ACL for short). With a Network Access Control List, network traffic can be permitted or denied based on the source, destination or package used. Depending on where Access Control List is introduced, it can prevent unwanted packet flow within a network, whilst also offering protection against attacks, for example in firewalls.

Correct placement is everything:

In the past, Access Control Lists were often implemented in the central Layer 3 core switches, because this was the only location offering sufficient computing power. Now, these security measures can also be mapped in network devices in the access layer to limit unwanted incoming packet flow.

Access Control Lists can also be configured in Nexans LANactive GigaSwitch systems. This significantly increases security in FTTO networks and limits unwanted data traffic where it originates: decentral in the access layer.

www.nexans.de/ans - kd-1748e01