System architecture LANCOM Trusted Access

Traditional VPN-based security concepts are based on trust in internal networks and grant users and devices access to resources and applications by default. The Zero Trust principle challenges this model and introduces strict access control, where all access requests are verified regardless of the user's location.

This techpaper describes the system architecture of the LANCOM Trusted Access solution. It explains the roles and tasks of the components involved: the LANCOM Trusted Access Client, the LANCOM Trusted Access Controller, and the LANCOM Trusted Access Gateway.

System architecture

The system architecture of the LANCOM Trusted Access solution comprises the following components:

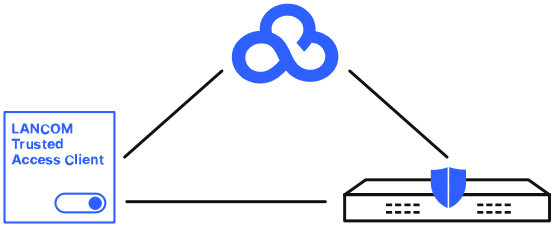

Figure 1: Components of the LANCOM Trusted Access

LANCOM Trusted Access Client

The LANCOM Trusted Access Client (LTA client) is software that is installed on an end device such as a notebook. The LTA client is managed, identified, and authenticated for access to network resources by the LANCOM Trusted Access Controller (LANCOM Management Cloud, LMC). Authentication takes place via a central user database (“identity provider”, e.g. an Active Directory or an LMC-internal user administration), which contains user identities and authentication information.

LANCOM Trusted Access Controller

The LANCOM Management Cloud serves as the LANCOM Trusted Access Controller (LTA Controller) and manages the access policies and the configuration of the LTA

client. It assumes the role of verifying the identity and authentication of users via an identity provider. The LTA controller also enables granular control of access to resources and applications. In addition, a custom real-time dashboard supports viewing network activity, monitoring network resources, and thus keeping an eye on the status of network security 24/7.

LANCOM Trusted Access Gateway

The LANCOM Trusted Access Gateway (LTA gateway) is a VPN-capable router or firewall and enables a secure connection between the LTA client and the applications it is allowed to access. The LTA client establishes an encrypted VPN connection with the LTA gateway and is then granted access exclusively to resources and applications assigned to it.

Operating modes

Tunnel mode can be used to select whether all network traffic of LTA users is routed to the gateway via the tunnel (Full Tunnel) or only selectively (Split Tunnel).

Split Tunnel

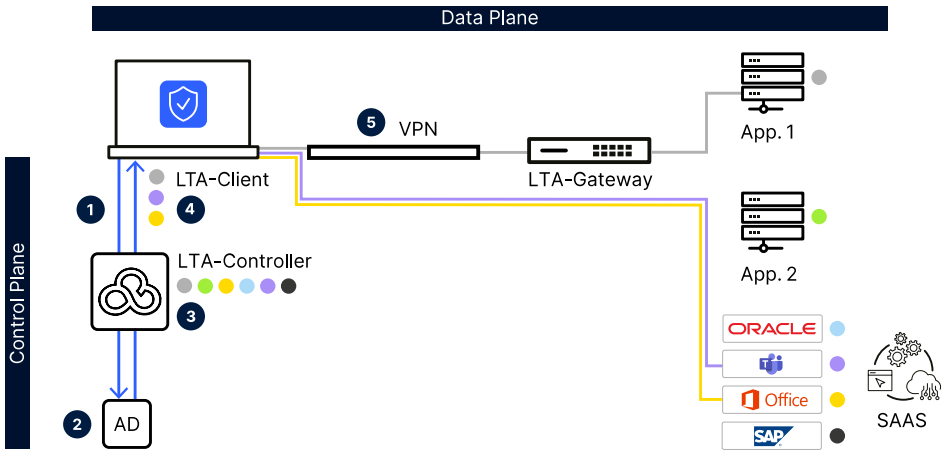

Figure 2:
LANCOM Trusted Access
in Split Tunnel mode

When Split Tunneling is used, the exchange of user data for internal applications takes place between the LANCOM Trusted Access Client and the LANCOM Trusted Access Gateway. For configured networks such as external cloud applications, the data traffic is decoupled directly to the Internet. An anti-virus program or a local firewall installed on the connected clients protects external data traffic.

Full Tunnel as a component of Trusted Internet Access

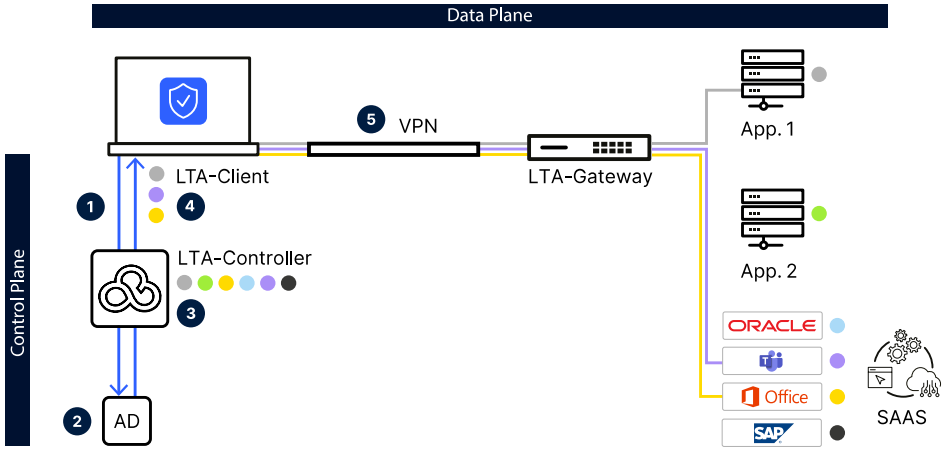

Figure 3:
LANCOM Trusted Access
in Full Tunnel mode

For increased security, all traffic, regardless of source and destination, is routed through the VPN tunnel when Full Tunneling is used. This means that security mechanisms such as content filtering (both LCOS-based and LCOS FX-based LTA gateways) or, in the case of the latter through the optional Full License, functions such as anti-virus, content filtering, IDS/IPS and SSL inspection can be used for this data traffic, especially for externally connected clients. The operating mode as a combination of Full Tunnel operation and activated security mechanisms on the LTA gateway is called **Trusted Internet Access**.

Process description

In order for a user to gain access to the applications intended for them, the steps described below are carried out:

Identification and authentication (Control Plane)

1. The LTA client sends the user's identification to the LTA controller which passes the further login to the corresponding identity provider (IdP).
2. The IdP (Active Directory or local user database) validates the credentials.
3. The LTA controller authorizes the LTA client to establish the connection to the LTA gateway and checks its security compliance (operating system version, virus protection, or local firewall).
4. The LTA client receives the configuration data for establishing the VPN connection to the LTA gateway, including the access rights assigned to it.

Connection establishment and data traffic (Data Plane)

5. The LTA client establishes a secure VPN connection to the LTA gateway, which only allows it access to applications it is permitted to use. Any user data is exchanged exclusively between the LTA client and the LTA gateway, without decoupling via the LTA controller.

Separation of Control Plane and Data Plane

Only the data exchange for user authentication takes place via the LANCOM Trusted Access Controller (LANCOM Management Cloud). All other user data passes directly between the LANCOM Trusted Access Client and the LANCOM Trusted Access Gateway—without going via an external cloud. At the same time, all components involved are developed in Germany, and all cloud data is also hosted in data centers in Germany.

The LANCOM Trusted Access solution thus stands for the highest level of data security and data protection. It is subject to and complies with European legal standards, is therefore DSGVO-compliant, and is a convincing IT security solution made in Germany.

Microsegmentation

After application approval has been implemented on specific applications for individual users or user groups, microsegmentation can be used to further increase network security. If local applications or servers are networked via switches, these individual resources can be isolated in a network. This is most easily done by configuring private VLANs (PVLAN) on the associated switch ports to isolated mode. This measure severely restricts communication between devices on these ports, reducing the attack area for potential threats. In this way, sensitive data and applications on a network can be better protected because they can communicate only within their isolated range, while maintaining the performance and efficiency of the overall network.

Summary

The LANCOM Trusted Access solution offers a trusted system architecture that is based on the zero-trust principle and extends traditional VPN-based security concepts. Strict access control and verification of all access requests regardless of the user's location ensure a high level of security.

The identification, authentication, and connection establishment process demonstrates a transparent and effective process that maximizes security and control over network resources. The LANCOM Trusted Access solution offers companies and organizations the opportunity to keep an eye on their network security 24/7 and protect themselves against threats from the Internet.

Thus, the LANCOM Trusted Access solution offers a future-proof and modern security architecture that meets the increasing demands on IT security while maintaining user flexibility and mobility. By switching to a zero-trust approach, companies can ensure that only authorized users and devices have access to sensitive resources, guaranteeing the highest level of protection against internal and external threats. The LANCOM Trusted Access solution thus offers a significant improvement in enterprise network security compared to traditional VPN solutions.

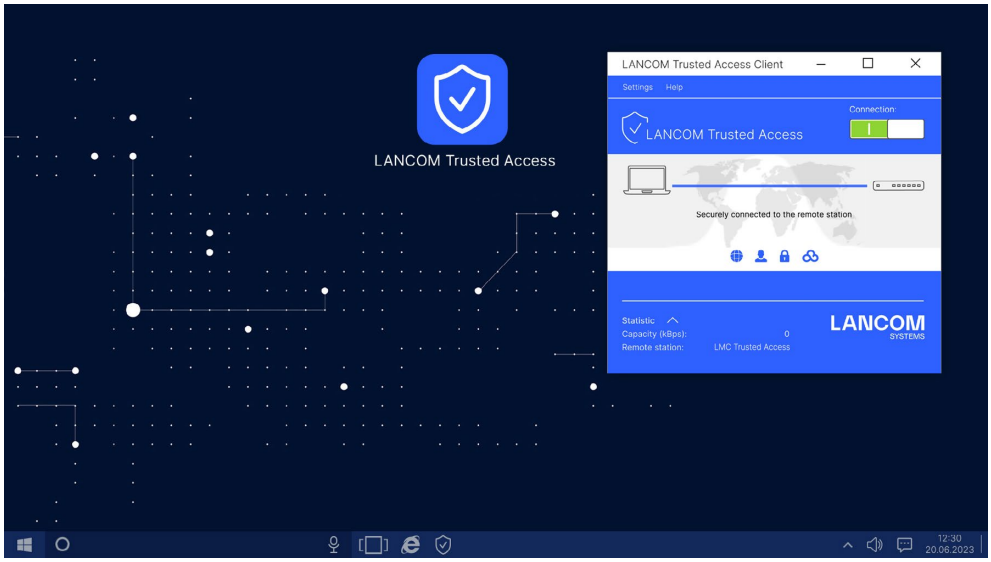

Figure 4:
LANCOM Trusted Access Client

What is the difference between the LANCOM Trusted Access Client and the LANCOM Advanced VPN Client?

Features	Advanced VPN Client	Trusted Access Client
Operating mode	Unmanaged	Cloud managed
Commissioning	Manual pre-configuration of all access parameters per client	Zero-touch / auto-configuration: No pre-configuration is required. Users are automatically assigned to the correct project based on their email domain. All client configuration and assignment is done centrally via the LMC.
Monitoring	–	✓ Central monitoring dashboard in the LMC
Access rights	Full access to the intranet	Individual applications or alternatively in smaller deployment scenarios with full access to the intranet. However, it is recommended to limit the access per user group to the required applications and to separate the local applications from each other on the network side.
Lateral protection (e. g. against ransomware)	– Entire intranet accessible	✓ When using application filtering in conjunction with micro-segmentation (Private VLAN)
Endpoint security	–	✓ Clients can be specified that virus scanners and firewalls must be active on each client and that there is a minimum version or patch level for the operating system. Clients that do not comply with the specifications can be blocked automatically.
Client configuration / change management	Manual per client	Automatic / central via LMC
Central user management	–	✓ Via Active Directory or user tables in the LMC
Two- or multi-factor authentication (2FA / MFA)	–	✓ Only when using Microsoft Active Directory; not in conjunction with local user table
Licensing	License must be activated manually per client	Licensing is carried out centrally via LMC (pre-paid or pay-per-use)
Regular software updates	–	✓ Included over the entire term

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com