Systemarchitektur LANCOM Trusted Access

Traditionelle VPN-basierte Sicherheitskonzepte basieren auf dem Vertrauen in interne Netzwerke und gewähren Benutzern und Geräten standardmäßig Zugriff auf Ressourcen und Anwendungen. Das Zero-Trust-Prinzip stellt dieses Modell in Frage und führt eine strikte Zugriffskontrolle ein, bei der alle Zugriffsanfragen unabhängig vom Standort des Benutzers überprüft werden.

Dieses Techpaper beschreibt die Systemarchitektur der LANCOM Trusted Access-Lösung. Es erklärt die Rollen und Aufgaben der beteiligten Komponenten: dem LANCOM Trusted Access Client, dem LANCOM Trusted Access Controller und dem LANCOM Trusted Access Gateway.

Systemarchitektur

Die Systemarchitektur der LANCOM Trusted Access-Lösung umfasst die folgenden Komponenten:

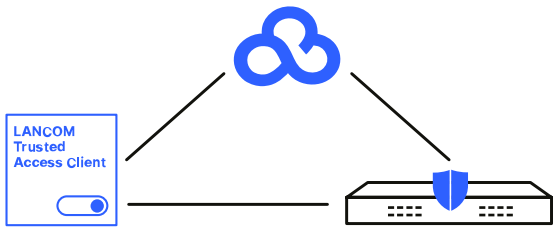

Abbildung 1:
Komponenten des
LANCOM Trusted Access

LANCOM Trusted Access Client

Der LANCOM Trusted Access Client (LTA-Client) ist eine Software, welche auf einem Endgerät wie einem Notebook installiert wird. Dabei wird der LTA-Client vom LANCOM Trusted Access Controller (LANCOM Management Cloud, LMC) verwaltet, identifiziert und für den Zugriff auf Netzwerkressourcen authentifiziert. Die Authentifizierung erfolgt über eine zentrale Benutzerdatenbank („Identity Provider“, z. B. ein Active Directory oder eine LMC-interne Benutzerverwaltung), die Benutzeridentitäten und Authentifizierungsinformationen enthält.

LANCOM Trusted Access Controller

Die LANCOM Management Cloud dient als LANCOM Trusted Access Controller (LTA-Controller) und verwaltet die Zugriffsrichtlinien sowie die Konfiguration des LTA-Clients. Sie übernimmt die Rolle der Überprüfung der Identität und Authentifizierung von Benutzern über einen Identity Provider. Der LTA-Controller ermöglicht zudem die granulare Steuerung des Zugriffs auf Ressourcen und Anwendungen. Zusätzlich unterstützt ein benutzerdefiniertes Real-Time Dashboard dabei, die Netzwerkaktivitäten anzuzeigen, die Netzwerkressourcen zu überwachen und somit den Status der Netzwerksicherheit 24/7 im Blick zu behalten.

LANCOM Trusted Access Gateway

Das LANCOM Trusted Access Gateway (LTA-Gateway) ist ein VPN-fähiger Router oder eine Firewall und ermöglicht eine sichere Verbindung zwischen dem LTA-Client und den ihm erlaubten Anwendungen. Der LTA-Client baut eine verschlüsselte VPN-Verbindung mit dem LTA-Gateway auf und erhält daraufhin ausschließlich Zugriff auf ihm zugewiesene Ressourcen und Anwendungen.

Betriebsmodi

Mittels Tunnel-Modus kann ausgewählt werden, ob der gesamte Netzwerkverkehr der LTA-Benutzer über den Tunnel zum Gateway geleitet wird (Full Tunnel) oder nur selektiv (Split Tunnel).

Split Tunnel

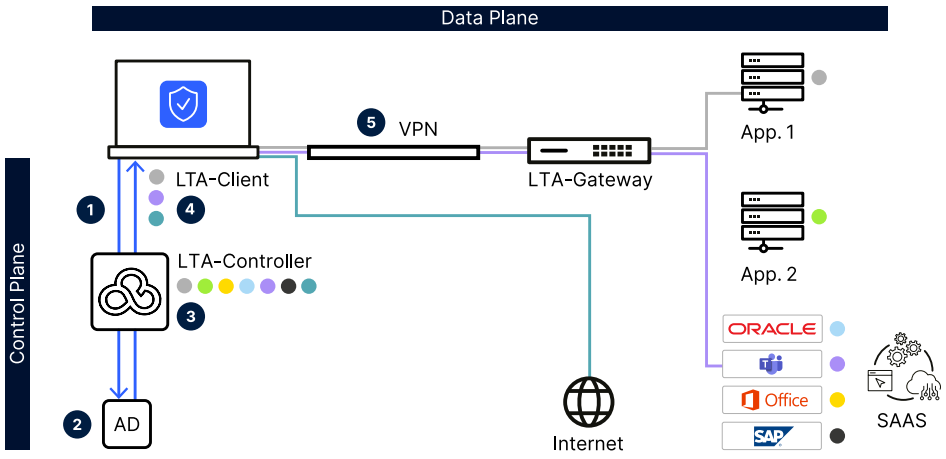

Abbildung 2:
LANCOM Trusted Access
im Split Tunnel-Betrieb

Bei Einsatz von Split Tunneling erfolgt der Austausch von Nutzdaten sowohl für interne Applikationen als auch für konfigurierte Netzwerke (einschließlich externer Cloud-Anwendungen) zwischen dem LANCOM Trusted Access Client und dem LANCOM Trusted Access Gateway. Anfragen zu nicht konfigurierten Zieladressen – etwa allgemeine Browserzugriffe – werden hingegen direkt ins Internet ausgekoppelt. Hierbei sichern auf den angebundenen Clients ein installiertes Anti-Virus-Programm oder eine lokale Firewall den externen Datenverkehr ab.

Full-Tunnel als Bestandteil von Trusted Internet Access

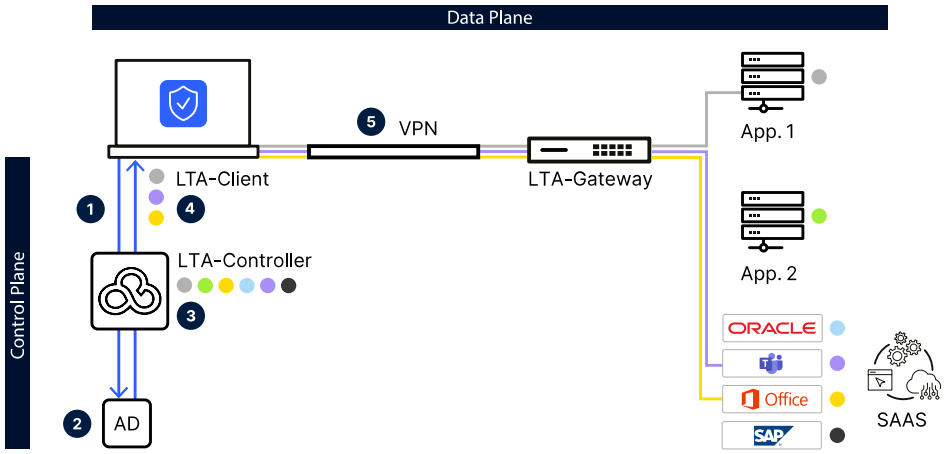

Abbildung 3:
LANCOM Trusted Access
im Full Tunnel-Betrieb

Für erhöhte Sicherheit wird bei Einsatz von Full Tunneling der gesamte Datenverkehr, unabhängig von Quelle und Ziel, durch den VPN-Tunnel geleitet. Somit können für diesen Datenverkehr insbesondere bei extern angebundenen Clients Sicherheitsmechanismen wie Content Filter (sowohl LCOS-basierte als auch LCOS FX-basierte LTA-Gateways) oder bei letzteren durch die optionale Full License auch Funktionen wie Anti-Virus, Content Filter, IDS/IPS und SSL Inspection zum Einsatz kommen. Der Betriebsmodus als Kombination aus Full Tunnel-Betrieb und aktivierten Sicherheitsmechanismen auf dem LTA-Gateway wird **Trusted Internet Access** genannt.

Ablaufbeschreibung

Damit ein Benutzer Zugriff auf für ihn vorgesehene Anwendungen erhält, erfolgen die im Folgenden beschriebenen Schritte:

Identifikation und Authentifizierung (Control Plane)

1. Der LTA-Client sendet die Identifikation des Benutzers an den LTA-Controller welcher die weitere Anmeldung an den entsprechenden Identity Provider (IdP) übergibt.

2. Der IdP (Active Directory oder lokale Benutzerdatenbank) validiert die Anmeldeinformationen.
3. Der LTA-Controller autorisiert den LTA-Client für den Verbindungsaufbau zum LTA-Gateway und überprüft seine Security Compliance (Betriebssystemversion, Virenschutz oder lokale Firewall).
4. Der LTA-Client erhält die Konfigurationsdaten für den VPN-Verbindungsaufbau zum LTA-Gateway inklusive der ihm zugewiesenen Zugriffsrechte.

Verbindungsaufbau und Datenverkehr (Data Plane)

5. Der LTA-Client baut eine sichere VPN-Verbindung zum LTA-Gateway auf, welches ihm ausschließlich Zugriff auf ihm erlaubte Anwendungen ermöglicht. Jegliche Nutzdaten werden ausschließlich zwischen LTA-Client und LTA-Gateway ausgetauscht, ohne Auskopplung über den LTA-Controller.

Trennung von Control Plane und Data Plane

Ausschließlich der Datenaustausch zur Benutzerauthentifizierung findet über den LANCOM Trusted Access Controller (LANCOM Management Cloud) statt. Alle weiteren Nutzdaten verlaufen direkt zwischen LANCOM Trusted Access Client und LANCOM Trusted Access Gateway – ohne über eine externe Cloud zu gehen. Gleichzeitig werden alle beteiligten Komponenten in Deutschland entwickelt und auch das Hosting sämtlicher Cloud-Daten erfolgt in Rechenzentren in Deutschland.

Somit steht die LANCOM Trusted Access-Lösung für höchste Datensicherheit und höchsten Datenschutz. Sie unterliegt und entspricht europäischen Rechtsstandards, ist somit DSGVO-konform und überzeugt als IT-Security-Lösung Made in Germany.

Mikrosegmentierung

Nachdem die Anwendungsfreigabe auf bestimmte Anwendungen für einzelne Benutzer oder Benutzergruppen implementiert wurde, kann über Mikrosegmentierung eine weitere Steigerung der Netzwerksicherheit erreicht werden. Sind lokale Anwendungen oder Server über Switches vernetzt, können diese einzelne Ressourcen in einem Netzwerk isoliert werden. Dies geschieht am einfachsten durch die Konfiguration von privaten VLANs (PVLAN) auf den zugehörigen Switch-Ports in den isolierten Modus. Durch diese Maßnahme werden die Kommunikationsmöglichkeiten zwischen den Geräten auf diesen Ports stark eingeschränkt, wodurch die Angriffsfläche für potenzielle Bedrohungen reduziert wird. Auf diese Weise können sensible Daten und Anwendungen in einem Netzwerk besser geschützt werden, da sie nur innerhalb ihres isolierten

Bereichs kommunizieren können, während gleichzeitig die Leistung und Effizienz des Gesamtnetzwerks erhalten bleibt.

Fazit

Die LANCOM Trusted Access-Lösung bietet eine vertrauenswürdige Systemarchitektur, die auf dem Zero-Trust-Prinzip basiert und traditionelle VPN-basierte Sicherheitskonzepte zeitgemäß erweitert. Durch die strikte Zugriffskontrolle und die Überprüfung aller Zugriffsanfragen unabhängig vom Standort des Benutzers wird ein hohes Maß an Sicherheit gewährleistet.

Der Ablauf der Identifikation, Authentifizierung und des Verbindungsaufbaus zeigt einen transparenten und effektiven Prozess auf, der die Sicherheit und Kontrolle über die Netzwerkressourcen maximiert. Die LANCOM Trusted Access-Lösung bietet Unternehmen und Organisationen die Möglichkeit, ihre Netzwerksicherheit 24/7 im Blick zu behalten und sich vor Bedrohungen aus dem Internet zu schützen.

Somit bietet die LANCOM Trusted Access-Lösung eine zukunftssichere und moderne Sicherheitsarchitektur, die den steigenden Anforderungen an die IT-Sicherheit gerecht wird und gleichzeitig die Flexibilität und Mobilität der Benutzer erhält. Mit dem Wechsel zu einem Zero-Trust-Ansatz können Unternehmen sicherstellen, dass nur autorisierte Benutzer und Geräte Zugriff auf sensible Ressourcen haben und so ein Höchstmaß an Schutz vor internen und externen Bedrohungen gewährleisten. Die LANCOM Trusted Access-Lösung bietet somit eine erhebliche Verbesserung der Netzwerksicherheit in Unternehmen im Vergleich zu traditionellen VPN-Lösungen.

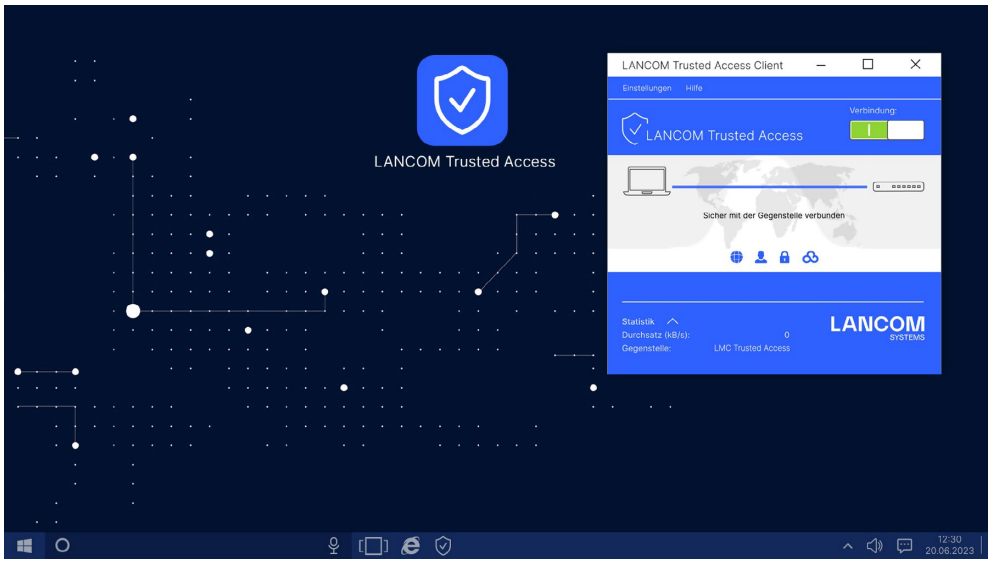

Abbildung 4:
LANCOM Trusted Access Client

Was unterscheidet den LANCOM Trusted Access Client vom LANCOM Advanced VPN Client?

Features	Advanced VPN Client	Trusted Access Client
Betriebsart	Unmanaged	Cloud-managed
Inbetriebnahme	Manuelle Vorkonfiguration aller Zugangsparameter pro Client	Zero-touch / Auto-Konfiguration: Es ist keine Vorkonfiguration notwendig. Benutzer werden anhand ihrer E-Mail-Domäne automatisch dem richtigen Projekt zugeordnet. Die Client-Konfiguration und -Zuordnung erfolgt zentral über die LMC.
Monitoring	–	✓ Zentrales Monitoring-Dashboard in der LMC
Zugriffsrechte	Vollzugriff auf das Intranet	Einzelne Applikationen oder alternativ in kleineren Einsatzszenarien mit Vollzugriff auf das Intranet. Es wird jedoch empfohlen, den Zugriff pro Benutzergruppe auf die benötigten Anwendungen zu limitieren und die lokalen Anwendungen netzseitig voneinander zu trennen.
Lateraler Schutz (z. B. gegen Ransomware)	– Gesamtes Intranet erreichbar	✓ Bei Verwendung der Anwendungsfilterung in Verbindung mit Mikrosegmentierung (Private VLAN)
Endpoint Security	–	✓ Es kann Clients vorgegeben werden, dass Virenscanner und Firewall auf jedem Client aktiv sein müssen und es eine Mindestversion bzw. ein Patch-Level für das Betriebssystem gibt. Clients, die den Vorgaben nicht entsprechen, können automatisch blockiert werden.
Client-Konfiguration / Change-Management	Manuell pro Client	Automatisch / zentral via LMC
Zentrales User-Management	–	✓ Via Active Directory oder Benutzertabellen in der LMC
Zwei- oder Multi-Faktor-Authentifizierung (2FA / MFA)	–	✓ Nur bei Nutzung von Microsoft Active Directory; nicht in Verbindung mit lokaler Benutzertabelle
Lizenzierung	Lizenz muss pro Client manuell aktiviert werden	Lizenzierung erfolgt zentral über die LMC (pre-paid oder pay-per-use)
Regelmäßige Software-Updates	–	✓ Inkludiert über die gesamte Laufzeit

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