LANCOM Advanced Mesh VPN

Klassische VPN-Szenarien in der Standortvernetzung sind in der Regel sternförmig (Hub & Spoke) aufgebaut. Dabei bauen die angebundenen Filialen (Spokes) VPN-Tunnel zu einer oder mehreren Zentralen (Hubs) auf. In solchen traditionellen Szenarien ist ein Hub & Spoke-Netzwerk-Design eine logische Topologieentscheidung, denn es fließen Daten hauptsächlich zwischen Filiale und Zentrale, da dort zentrale Server stehen, z. B. das Warenwirtschaftssystem, Datenbanken oder Webserver.

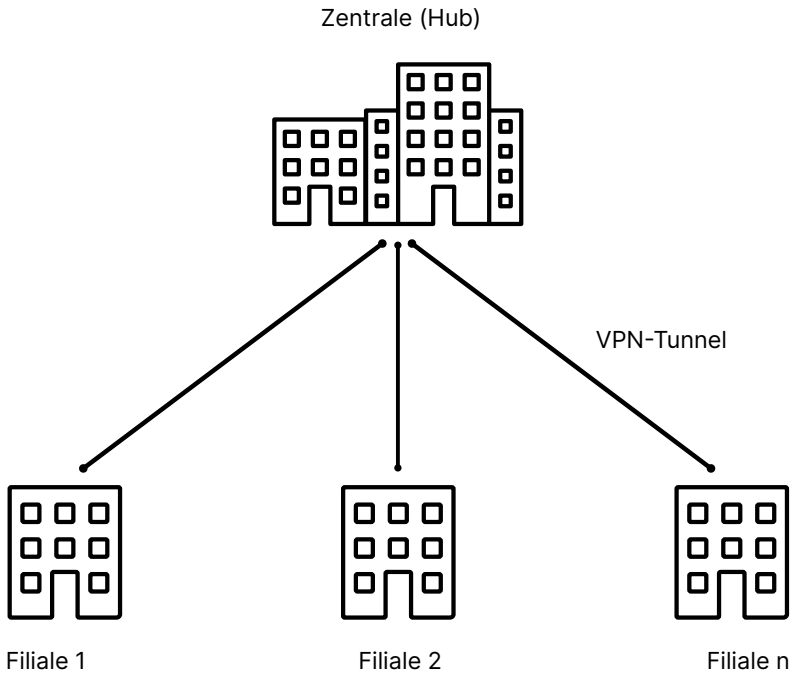

Abbildung 1: Klassische Standortvernetzung (Hub & Spoke)

Die Vorteile dieses sternförmigen Netzwerkdesigns sind der einfache Aufbau und die zentrale Steuerung in der Zentrale. Der Nachteil ist jedoch, dass sämtlicher Datenverkehr – auch der zwischen einzelnen Filialen wie z. B. Telefonie oder Dateiaustausch über einen File-Server – immer über den indirekten Weg über die Zentrale erfolgt. Dadurch wird die Internetanbindung der Zentrale mit dem Datenverkehr zwischen den Filialen belastet und somit zum Flaschenhals der gesamten Kommunikation.

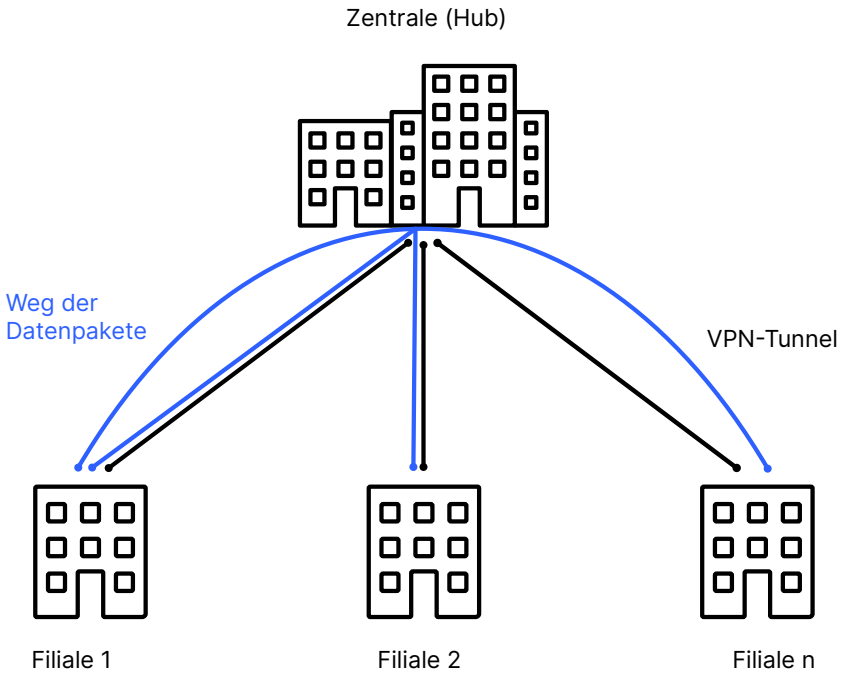

Abbildung 2: Datenaustausch zwischen Filialen bei klassischer Standortvernetzung (Hub & Spoke)

Wenn der Datenverkehr zwischen den Filialen der größte Anteil der Verkehrsbeziehung darstellt, ist es ein praktischer Lösungsansatz, direkte VPN-Tunnel zwischen den Filialen manuell zu konfigurieren. In diesem Fall spricht man von einem VPN-Mesh-Szenario. In einfachen Szenarien funktioniert dieser manuelle Ansatz noch gut. Wenn es allerdings viele Filialen gibt und viele mögliche VPN-Tunnel, so skaliert dieser starre, einzeln und fest konfigurierte Ansatz nicht mehr.

LANCOM bietet für dieses Szenario die Lösung Advanced Mesh VPN. Hierbei besteht zunächst eine klassische sternförmige VPN-Struktur, in der alle Filialen zu Beginn einen VPN-Tunnel zur Zentrale aufbauen. Gibt es nun Datenverkehr zwischen den Filialen, so wird dynamisch ein VPN-Tunnel als Abkürzung zwischen den beiden beteiligten Filialen aufgebaut. Die Daten fließen nun direkt in einem VPN-Tunnel zwischen den Filialen, ohne dass die Daten den Weg über die Zentrale gehen.

Dabei fließen nur die ersten Datenpakete immer den langen Weg von der Filiale A über die Zentrale zur zweiten Filiale B. Erst beim Empfang der ersten Datenpakete in der Zielfiliale initiiert die Zielfiliale einen dynamischen VPN-Tunnel zur Filiale mit dem Ursprung des Datenpakets. Fließen nach einiger Zeit keinen Daten mehr, so wird der Tunnel dynamisch wieder abgebaut.

Der Vorteil: Deutlich weniger Traffic in der Zentrale und einhergehend höhere Performance im gesamten Unternehmensnetzwerk.

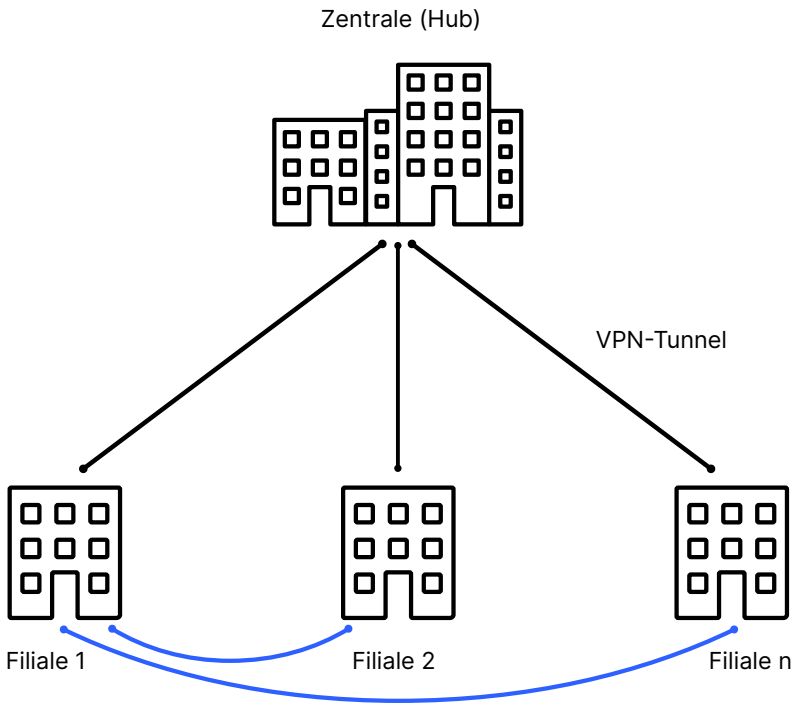

Abbildung 3: Standortvernetzung über Advanced Mesh VPN

Schritte zur Konfiguration von Advanced Mesh VPN

1. Konfiguration der statischen VPN-Tunnel zwischen Filiale und Zentrale.
2. Anlegen einer Mesh-VPN-Tunnel-Vorlage (Template) in der IKEv2-Gegenstellen-Tabelle, die die gemeinsamen VPN-Eigenschaften wie Verschlüsselung, PSK oder Zertifikat für die dynamischen Mesh-VPN-Tunnel enthält.
3. Aktivierung der Mesh-VPN-Funktionalität und Konfiguration der globalen Mesh-Parameter auf allen beteiligten VPN-Routern.

Hinweise zur Einrichtung sowie eine ausführliche Schritt-für-Schritt-Anleitung finden Sie hier.

Wie erfolgt der dynamische Aufbau eines Mesh-VPNs?

1. Filiale A sendet Datenpakete in den VPN-Tunnel über den bestehenden statischen VPN-Tunnel zur Zentrale an Filiale B.
2. Der Router in Filiale B erkennt eine neue Session, da Datenpakete von einem unbekannten Subnetz in dem VPN-Tunnel von der Zentrale ankommen.
3. Filiale B sendet eine verschlüsselte herstellerspezifische IKEv2-Nachricht an die Zentrale. Die Nachricht enthält die privaten Subnetze bzw. IP-Adressen der gewünschten Kommunikationsbeziehung und die öffentliche IP-Adresse der Filiale B.

4. Die Zentrale empfängt die herstellerspezifische IKEv2-Nachricht im VPN-Tunnel von Filiale B und leitet sie über den VPN-Tunnel, der zur Filiale A führt, an Filiale A.
5. Filiale A empfängt die herstellerspezifische IKEv2-Nachricht der Zentrale.
6. Filiale A erzeugt einen dynamischen Mesh-VPN-Tunnel und baut diesen direkt zur IP-Adresse der Filiale B auf. Die notwendigen Informationen zum Aufbau des Tunnels entnimmt der Router aus der herstellerspezifischen IKEv2-Nachricht (Gateway IP-Adresse, Subnetz etc.).
7. Filiale B nimmt den Tunnelaufbau von Filiale A an und aktualisiert ihre lokale Routing-Tabelle auf das Subnetz von Filiale A mit Ziel-Gateway der öffentlichen IP-Adresse von Filiale A. Das private Subnetz der Filiale A wird per IKEv2-Routing als IKEv2-Nachricht während des VPN-Tunnelaufbaus verwendet und ist spezifischer als die Route in die Zentrale.
8. Es fließen nun Daten direkt zwischen Filiale A und B, da die Routen auf beiden Seiten auf den dynamischen VPN-Tunnel zeigen.
9. Werden nach einem Timeout keine Daten mehr übertragen, so wird der Mesh-VPN-Tunnel abgebaut.

Hinweise

→ Die ersten Datenpakete fließen immer zuerst über den Tunnel zur Zentrale und lösen dann den Aufbau eines dynamischen Tunnels aus.

→ Ein Ping auf die LAN-IP-Adresse des Routers der Gegenseite löst keinen Mesh-VPN-Tunnelaufbau aus. Nur Datenpakete an Endpunkte im LAN lösen einen Tunnelaufbau aus, da nur diese von der Router-Firewall korrekt erkannt werden können. Ein Ping an eine (ggf. nichtexistierende) IP-Adresse im LAN löst aber den Aufbau eines VPN-Mesh-Tunnels aus.

→ Bestehende Firewall-Sessions der ersten Datenpakete über die Zentrale werden nach erfolgreichem VPN-Mesh-Tunnelaufbau auf den neu aufgebauten Mesh-Tunnel umgezogen (Session Switchover).

→ Die Filiale, die einen dynamischen VPN-Mesh-Tunnel annehmen soll, muss über eine öffentliche IP-Adresse (IPv4 oder IPv6) verfügen und von außen erreichbar sein. Router mit einer Mobilfunkverbindung verfügen in der Regel nicht über eine öffentliche IP-Adresse.

→ LANCOM Advanced Mesh VPN ist eine herstellerspezifische Implementierung basierend auf IKEv2 und funktioniert nur zwischen LCOS-basierten LANCOM VPN-Routern. Der LANCOM Advanced VPN Client unterstützt dies nicht.

→ Die Sicherheit basiert vollständig auf IKEv2 / IPSec und kann alle Einstellungen wie PSK, Zertifikate, Verschlüsselungsalgorithmen oder LANCOM HSVPN von IKEv2 verwenden.

→ Alle beteiligten Router (Filiale, Zentrale) benötigen LCOS 10.70 oder höher.

Lizenzierung

Mesh-VPN-Tunnel werden separat und zusätzlich zu den normalen VPN-Tunneln gezählt. Sind die Lizenzen für Mesh-VPN-Tunnel erschöpft, so wird kein Mesh-Tunnel aufgebaut und die Daten laufen weiterhin den längeren Weg über die Zentrale. Zentralseitige Geräte sind auf 200 Mesh-Tunnel in allen Ausbaustufen begrenzt.

Die folgenden Mesh-VPN-Lizenzen gelten (in Abhängigkeit der Anzahl der normalen VPN-Tunnel):

Kategorie	Geräte	Anzahl Lizenzen	
		VPN-Tunnel	Mesh-VPN-Tunnel
CPE	R88x, R90x, 88x VoIP, 1640E, 1650E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx mit VPN 25	25	50
CPE	19xx	25	50
CPE	19xx mit VPN 50	50	100
CPE	19xx mit VPN 100	100	200
Zentrale	ISG-1000	100	200
Zentrale	ISG-4000	200	200
Zentrale	ISG-5000	100	200
Zentrale	ISG-8000	250	200

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