LANCOM Advanced Mesh VPN

Classic VPN scenarios in site connectivity are usually star-shaped (hub & spoke). The connected branches (spokes) set up VPN tunnels to one or more hubs. In such traditional scenarios, a hub & spoke network design is a logical topology decision, because data flows mainly between the branch and the headquarters, since central servers are located there, such as the ERP system, databases or web servers.

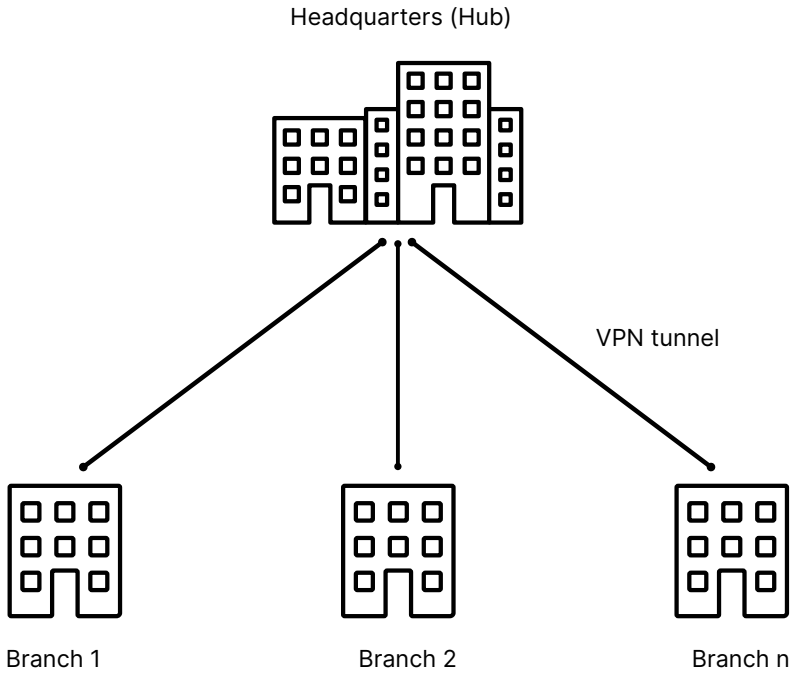

Figure 1:
Classic site networking
(hub & spoke)

The advantages of this star-shaped network design are the simple structure and the central control in the headquarters. The disadvantage, however, is that all data traffic—including that between individual branches, such as telephony or file exchange via a file server—always takes place indirectly via the headquarters. As a result, the headquarters Internet connection is burdened with data traffic between the branches and thus becomes the bottleneck of the entire communication.

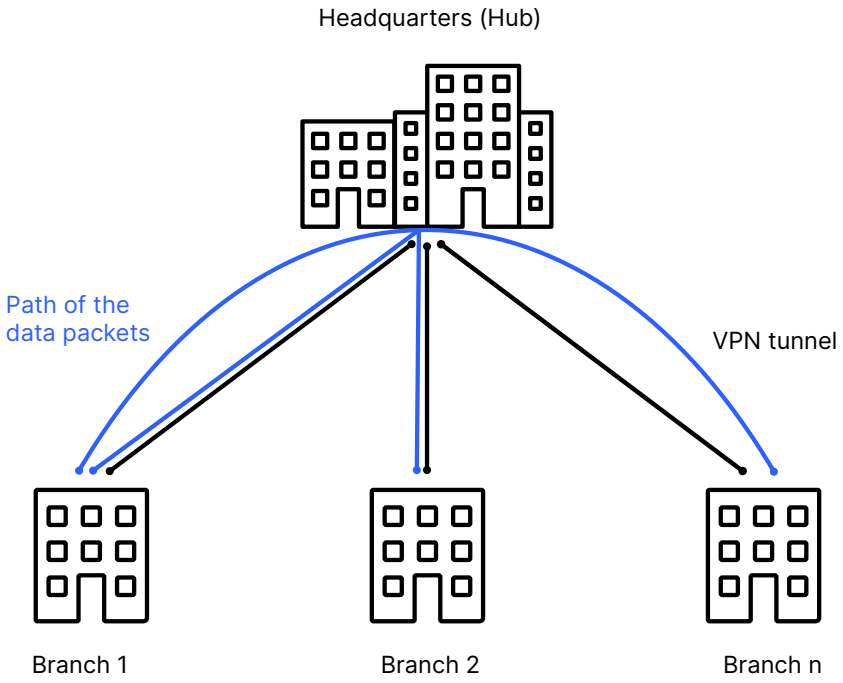

Figure 2:
Data exchange between branches with classic site networking (hub & spoke)

If inter-branch traffic is the largest portion of the traffic relationship, a practical approach is to manually configure direct VPN tunnels between branches. This case is referred to as a VPN mesh scenario. In simple scenarios, the manual approach works well. However, if there are many branches and many possible VPN tunnels, this rigid, individual, and fixed configuration approach no longer scales.

LANCOM offers the Advanced Mesh VPN as a solution in this scenario. The starting point is a classic star-shaped VPN structure, where each of the branches connects to the headquarters via VPN tunnel. In the event of data traffic between two branches, a VPN tunnel is dynamically established directly between them. The data now flows directly through a VPN tunnel between the branches without the data going via the headquarters.

The initial data packets have to take the long route from branch A via the headquarters to the second branch B. Only when the first data packets are received at the target branch does the target branch initiate a dynamic VPN tunnel to the branch that was the origin of the initial data packet. If no data flows for a time, the tunnel is dynamically terminated again.

The advantage: Significantly less traffic in the headquarters and, as a result, higher performance throughout the entire corporate network.

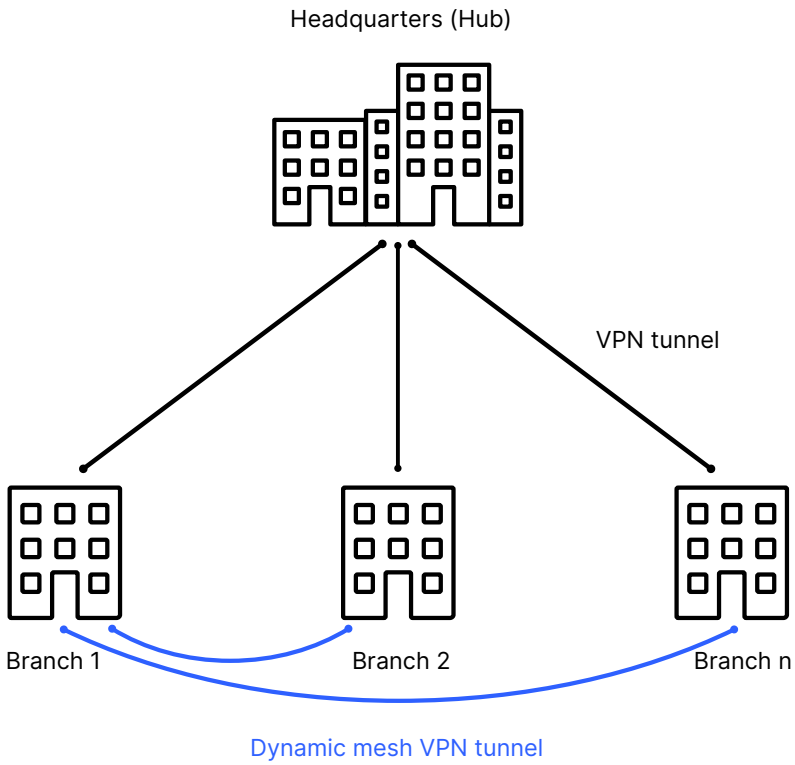

Figure 3:
Site networking via Advanced Mesh VPN

Steps to configure Advanced Mesh VPN

1. Configuring the VPN tunnel between the branch office and headquarters.
2. Creating a Mesh VPN tunnel template in the IKEv2 peer table that contains the shared VPN properties such as encryption method, PSK, or certificate for the dynamic Mesh VPN tunnel.
3. Activation of the Mesh VPN feature and configuration of the global mesh parameters on all relevant VPN routers.

Setup instructions and detailed step-by-step instructions can be found here.

How is the dynamic setup of a Mesh VPN done?

1. Branch A sends data packets over the existing static VPN tunnel via the headquarters to branch B.
2. The router at branch B detects a new session because data packets from an unknown subnet arrive via the VPN tunnel from the headquarters.
3. Branch B sends an encrypted manufacturer-specific IKEv2 message to the headquarters. The message contains the private subnets or IP addresses of the desired communication relationship and the public IP address of branch office B.

4. The headquarters receives the vendor specific IKEv2 message in the VPN tunnel from branch B and forwards it to branch A via the VPN tunnel to branch A.
5. Branch A receives the headquarters' vendor specific IKEv2 message.
6. Branch A creates a dynamic Mesh VPN tunnel and establishes it directly to the IP address of branch B. The router takes the necessary information from the vendor specific IKEv2 message (gateway IP address, subnet, etc.).
7. Branch B accepts the tunnel setup by branch A and updates its local routing table to include the subnet at branch A with the destination gateway that is the public IP address at branch A. The private subnet of branch A is used by IKEv2 routing as an IKEv2 message during VPN tunnel establishment and is more specific than the route to the headquarters.
8. Data now flows directly between branches A and B, since the routes at both ends now point to the dynamic VPN tunnel.
9. If no further data is transmitted after the timeout, the Mesh VPN tunnel is terminated.

Notes

→ The first data packets initially flow via the tunnel to the main office and then trigger the establishment of a dynamic tunnel.

→ A ping to the LAN IP address of the router at the peer does not trigger the establishment of a Mesh VPN tunnel. Only data packets to endpoints in the LAN will trigger tunnel establishment, as only these can be correctly identified by the router-firewall. However, a ping to a (possibly non-existent) IP address in the LAN does however trigger the establishment of a VPN mesh tunnel.

→ Ongoing firewall sessions relating to the data packets first sent via the headquarters are moved to the newly established mesh tunnel after the Mesh VPN tunnel was set up successfully (session switchover).

→ The branch that is to accept a dynamic Mesh VPN tunnel must have a public IP address (IPv4 or IPv6) and be reachable from the outside. Routers with a cellular connection usually do not have a public IP address.

→ LANCOM Advanced Mesh VPN is a vendor-specific implementation based on IKEv2 and only works between LCOS-based LANCOM VPN routers. The LANCOM Advanced VPN Client does not support this.

→ The security is based entirely on IKEv2/IPsec and can handle all settings such as PSK, certificates, encryption algorithms, or LANCOM HSVPN from IKEv2.

→ All routers involved (branch office, main office) require LCOS 10.70 or higher.

Licensing

Mesh VPN tunnels are counted separate from and in addition to normal VPN tunnels. If the licenses for Mesh VPN tunnels are exhausted, no mesh tunnel is set up and the data continues to travel the longer route via the main office. Central-site devices are limited to a maximum of 200 mesh tunnels, whatever their configuration.

The following Mesh VPN licenses apply (depending on the number of normal VPN tunnels):

Category	Devices	Number of licenses	
		VPN tunnel	Mesh VPN tunnel
CPE	R88x, 88x VoIP, 1640E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx with VPN 25	25	50
CPE	19xx	25	50
CPE	19xx with VPN 50	50	100
CPE	19xx with VPN 100	100	200
Central-site	ISG-1000	100	200
Central-site	ISG-4000	200	200
Central-site	ISG-5000	100	200
Central-site	ISG-8000	250	200

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