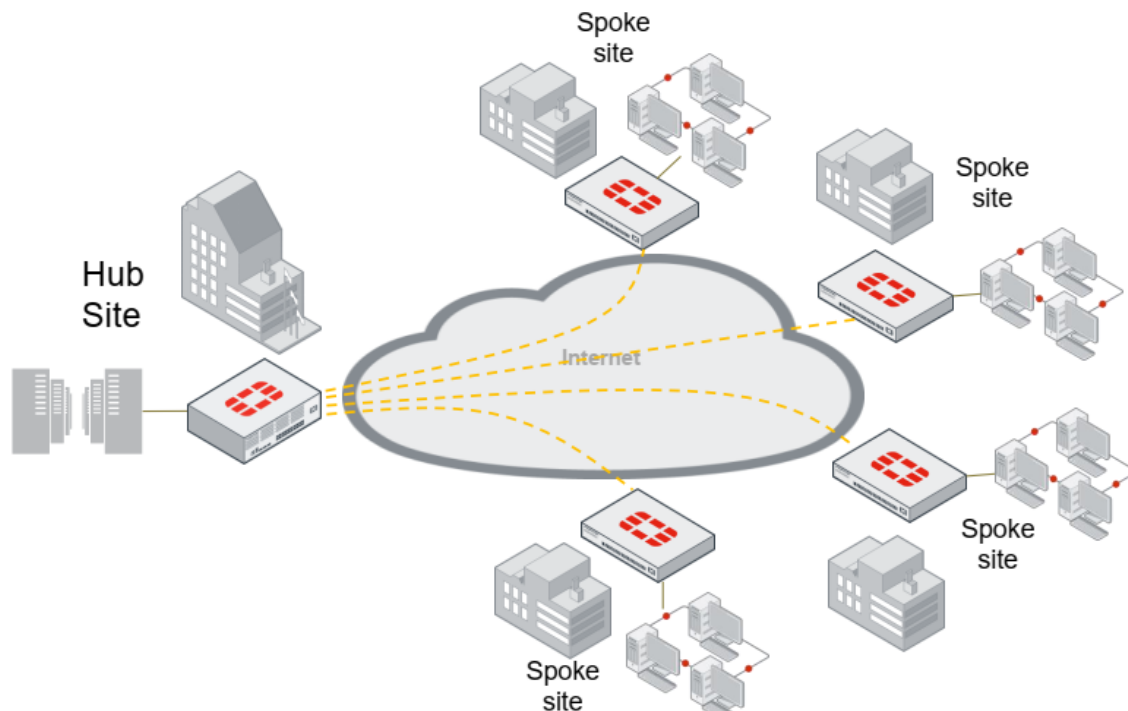


ADVPN:

If you are familiar with Cisco's DMVPN, the concepts are same instead Fortinet's calls their implementation ADVPN. We can achieve a fully meshed network by using ADVPN (Auto Discovery VPN). To better understand ADVPN let's first discuss IPsec VPN Topologies.

Hub and Spoke:

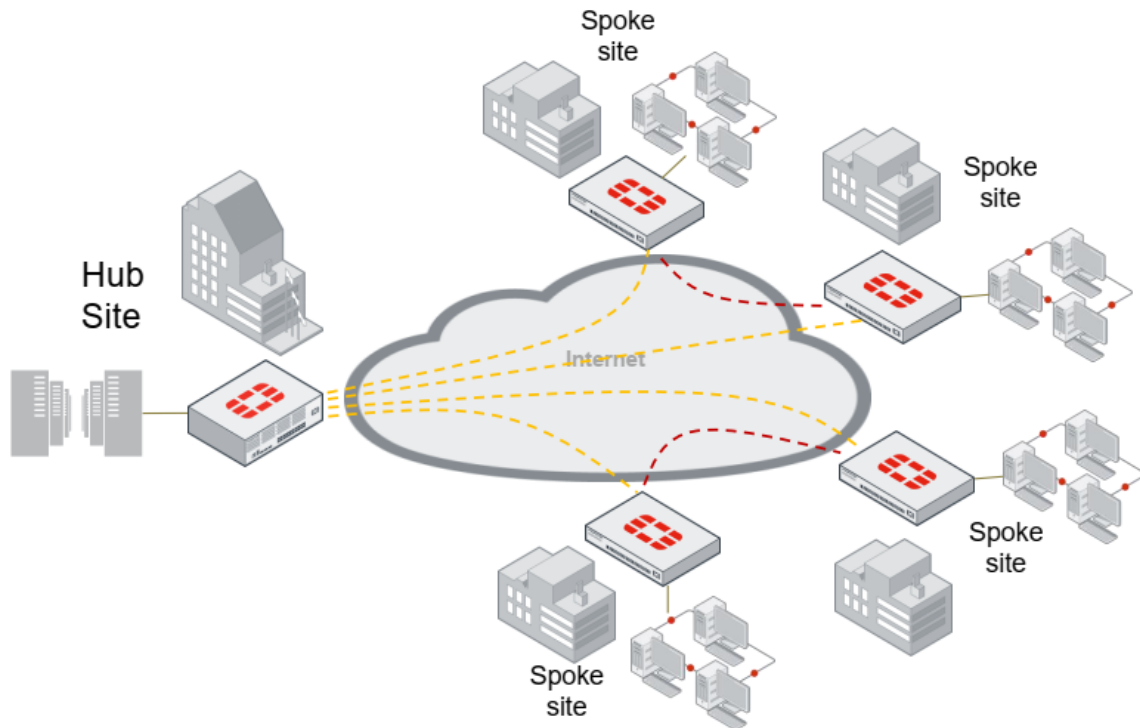
In this type of topology, we have a central device, called the hub, that is connected to multiple other devices named as the spokes. where main office act as a hub while other branches act as spokes. All the spoke sites are connected to each other via hub site. So, basically the network communication between any two spoke sites travel through the hub. One central FortiGate (hub) has multiple VPNs to other remote FortiGates (spokes). Hub nodes concentrate Spoke nodes in a Star topology. Spoke to Spoke traffic must go through the Hub there should be delay and latency. Needlessly consume resources on Hub site such as CPU, memory and Internet link. Hub is a single point of failure, if the main office network fails, entire enterprise network communication may fail. WAN network topology also has redundancy issues. The main advantage of hub and spoke technology is that it is cost effective. It is relatively easy to set up and maintain.



Hub and Spoke refers to a one-to-multi-point topology variation. All clients connect through a central hub. As the name implies, any traffic from a branch office to another branch office must transit through the hub. Easily manage the VPN configuration and firewall policies. System requirements are minimal for the FGT devices that function as branch offices because each FortiGate must maintain only one tunnel or two SA.

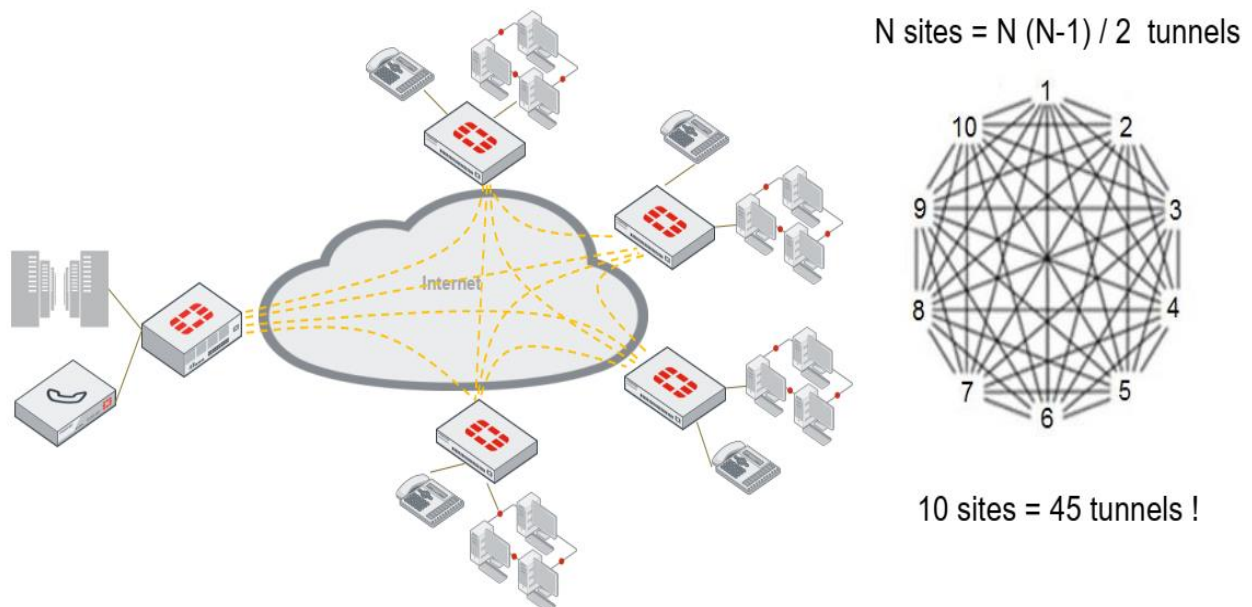
Partial Mesh:

Typically, a Hub-and-Spoke topology with additional direct tunnels between some Spokes. A middle ground between Hub-and-Spoke and Full-Mesh topologies. Partial Mesh attempts to compromise minimizing required resources as well as latency. Partial mesh can be appropriate if communication is not required between every location.



Full Mesh:

Mesh network topology is a type of site-to-site WAN topology in which each network device is connected to every other device through a dedicated link. There is no concept of a central hub which acts as a central point of communication. So, if we have n devices in the network then each device must be connected with $(n-1)$ devices. Further, the number of links in a mesh topology of n devices can be calculated by a simple formula i.e. $n(n-1)/2$. Direct connectivity between all sites. Efficient for Spoke-to-Spoke traffic. Complex configuration. Not scalable. The cost of implementation is high. Full mesh on the other hand connects every location every other location.



Full-Mesh topology, which enables direct spoke-to-spoke communication at the expense of a higher cost and increased administrative overhead. However, this is not always practical, or even feasible, especially in large networks.