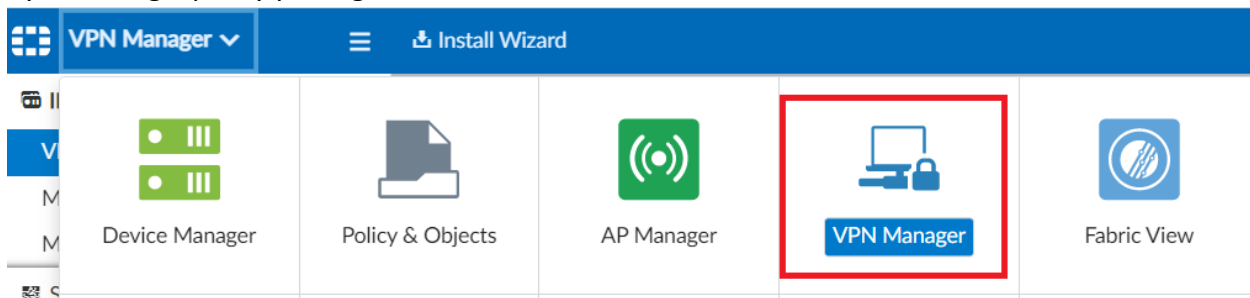


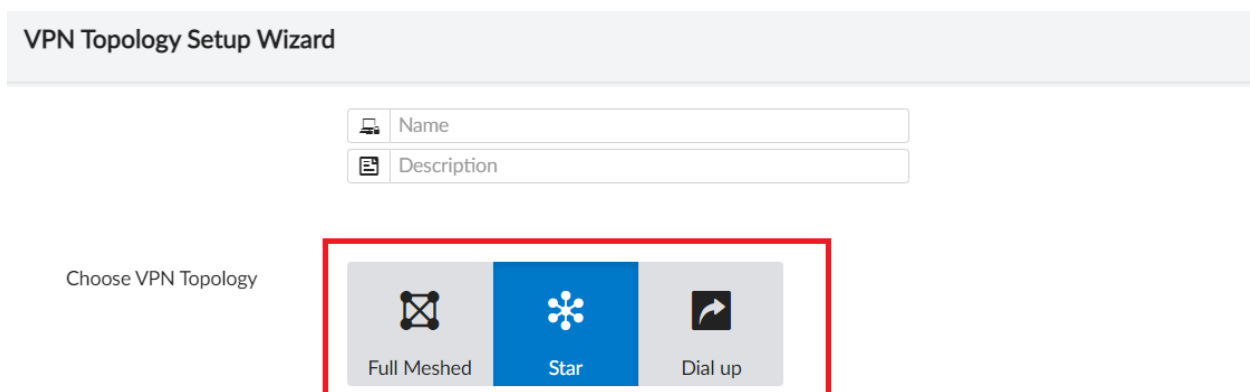
VPN Manager:

VPN Manager pane on FortiManager is more convenient when you want deploy a complex VPN topology, such as a **hub and spoke** topology, that involves multiple FortiGate devices. The configured IPsec tunnels can then be used as overlay links in SD-WAN. VPN Manager reduces the administrative overhead, while ensuring that **phase 1** and **phase 2** settings match across multiple devices for proper tunnel operation. VPN Manager is disabled by default, and you must enable it on a per-ADOM basis. When you use the VPN Manager, the settings are stored as objects in the objects database. You then push the IPsec VPN settings to one or more devices by installing a policy package.



VPN Community:

The first step to configure a VPN topology using VPN Manager is to create a VPN community. A VPN community is a **group of IPsec gateways** that share the same phase 1 and phase 2 settings. The goal is to simplify configuration and avoid configuration mismatch when the devices in the community try to establish tunnels among them. When you configure a VPN community, you must define the common phase 1 and phase 2 settings to use by all devices in the community. For SD-WAN, you must disable the **VPN Zone setting**. Otherwise, FortiManager places the IPsec tunnels inside interface zones. Because SD-WAN does not support the use of interface zones as members, you cannot use the IPsec tunnels as overlays if you keep VPN Zone enabled. FortiManager supports three types of communities. IPsec VPN communities are also sometimes called VPN topologies.



Full Meshed:

Each gateway has a tunnel to every other gateway. Type of site-to-site WAN topology in which each network device is connected to every other device through a dedicated link.

Star:

Each gateway has one tunnel to a central hub gateway. Each FortiGate is defined as either a hub or spoke. 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.

Dial up:

Like the star topology, except that tunnels are always initiated from the dial-up clients to the dialup servers. A dial-up client is a FortiGate device that has a dynamic IP address. The dial-up server, is assigned with a fixed and fully reachable IP address. The tunnel must be initiated from the remote device.

Gateway:

The next step is to add gateways to the community. There are two types of gateways. A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets, then passes the data packets to the local network. It also encrypts, encapsulates, and sends the IPsec data packets to the gateway at the other end of the VPN tunnel. The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet.

Managed Gateway:

Managed gateways are FortiGate devices in the current ADOM. FortiManager can push the settings to all the managed gateways during installation. When you create a new managed gateway, FortiManager displays a wizard that walks you through the managed gateway configuration.

External Gateway:

External gateways are VPN gateways that are third-party devices or FortiGate devices in a different ADOM. The administrator must manually apply the VPN configuration for external gateways.

VPN Security Policies:

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, only a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy, the virtual interface is the source. In the other policy, the virtual interface is the destination. The Action for both policies is Accept. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

For a policy-based VPN, one security policy enables communication in both directions. You must select IPSEC as the Action and then select the VPN tunnel dynamic object you have mapped to the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently.

Map View:

Displays a world map showing IPsec VPN tunnels. The Map View pane shows IPsec VPN connections on an interactive world map (Google Maps). Select a specific community from the tree menu to show only that community's tunnels. Hovering the cursor over a connection will highlight the connection and show the gateway, ADOM, and city names for each end of the tunnel.

Monitor:

Displays a list of IPsec VPN tunnels, and allows you to bring the tunnels up or down. Go to **VPN Manager > Monitor** to view the list of IPsec VPN tunnels. You can also bring the tunnels up or down on this pane. Select a specific community from the tree menu to show only that community's tunnels.

SSL-VPN:

Create, monitor, and manage SSL-VPN settings. You can also create, edit, and delete portal profiles for SSL-VPN settings. You can use the **VPN Manager > SSL-VPN** pane to create and monitor Secure Sockets Layer (SSL) VPNs. You can also create and manage SSL VPN portal profiles.

