Note:
- Personal firewalls provide valuable protection for systems against unwanted intrusions. Many organizations use personal firewalls on each system in addition to network firewalls as part of an overall defense-in-depth strategy.
- It's especially important to use personal firewalls when accessing the Internet in a public place. Free Wi-Fi Internet access is often available in public places, such as airports, hotels, and many fast-food establishments, such as Starbucks and McDonald's. However, connecting to a public Wi-Fi hot spot without the personal firewall enabled is risky, and never recommended.

Please identify different types of VPN.

VPN
- Virtual private network.
A method that provides access to a private network over a public network such as the Internet. VPN concentrators are dedicated devices used to provide VPN access to large groups of users.

Always-On VPN
- Can be used with both site-to-site VPNs and remote access VPNs. When used with a site-to-site VPN, the two VPN gateways maintain the VPN connection; Several vendors has always-on VPNs for remote access VPNs. They attempt to create the VPN connection as soon as the user's device connects to the Internet. For a home user, this might be right after the user turns on a desktop PC or laptop computer. When configured on mobile devices, such as cell phones, the device will connect to the always-on VPN anytime the device connects to an Internet connection. As an example, if a user visits a coffee shop that has free Internet access and the user connects to the network, the device will automatically connect to the always-on VPN.

Site-to-site VPN
- Includes two VPN servers that act as gateways for two networks separated geographically; it connects both networks without requiring additional steps on the part of the user. Users in the remote office can connect to servers in the headquarters location as easily as if the servers were in the remote office. Connecting to the remote server might be slower than connecting to a local server, but, otherwise, it is transparent to end users.

Remote Access VPN
- Connecting to internal networks from remote locations; The VPN client first connects to the Internet using a broadband connection to an Internet Service Provider (ISP). After connecting to the Internet, the VPN client can then initiate the VPN connection; the end user makes the direct connection to the VPN server and is very much aware of the process;

Public and Private VPNs
- When using a VPN concentrator, you would typically place it in the DMZ. The firewall between the Internet and the DMZ would forward VPN traffic to the VPN concentrator. The concentrator would route all private VPN traffic to the firewall between the DMZ and the intranet.
- Access over a public network is a core security concerns with VPNs. Different tunneling protocols encapsulate and encrypt the traffic to protect the data from unauthorized disclosure. The tunnel prevents anyone from reading the data transferred through it.