**VPN: (Virtual Private Network)**Creating a secure tunnel over an unsecure network, such as internet is called vpn.  
 **🔹 Route-Based VPN**

* **Traffic Control**: Uses routing tables and tunnel interfaces (like virtual interfaces) to send traffic through the VPN.
* **Tunnel Interface**: Creates a logical tunnel interface (e.g., Tunnel0) and routes traffic to that interface.
* **Flexibility**: More flexible and scalable; supports dynamic routing protocols (like OSPF, BGP).
* **Use Case**: Preferred for site-to-site VPNs with complex topologies, multiple subnets, or dynamic routing needs.
* **It encrypts all the data that goes through the interface**.

**Command:**ip route 192.168.2.0 255.255.255.0 Tunnel0  
  
**🔹 Policy-Based VPN**

* **Traffic Control**: Uses Access Control Lists (ACLs) or Security Policies to specify which traffic should go through the VPN.
* **Tunnel Interface**: No dedicated tunnel interface — traffic is matched to policies.
* **Simplicity**: Simpler to configure for small, static environments.
* **Limitations**: Does not support dynamic routing or multiple subnets easily.
* **If the traffic matches the policy, it’s encrypted by IPSec.**

**Command**:

access-list VPN\_ACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

crypto map VPN\_MAP 10 match address VPN\_ACL