Configure network routing and endpoints

- Administrators use network routes to control the flow of traffic through a network.
- Azure virtual networking provides capabilities to help you customized the routes.

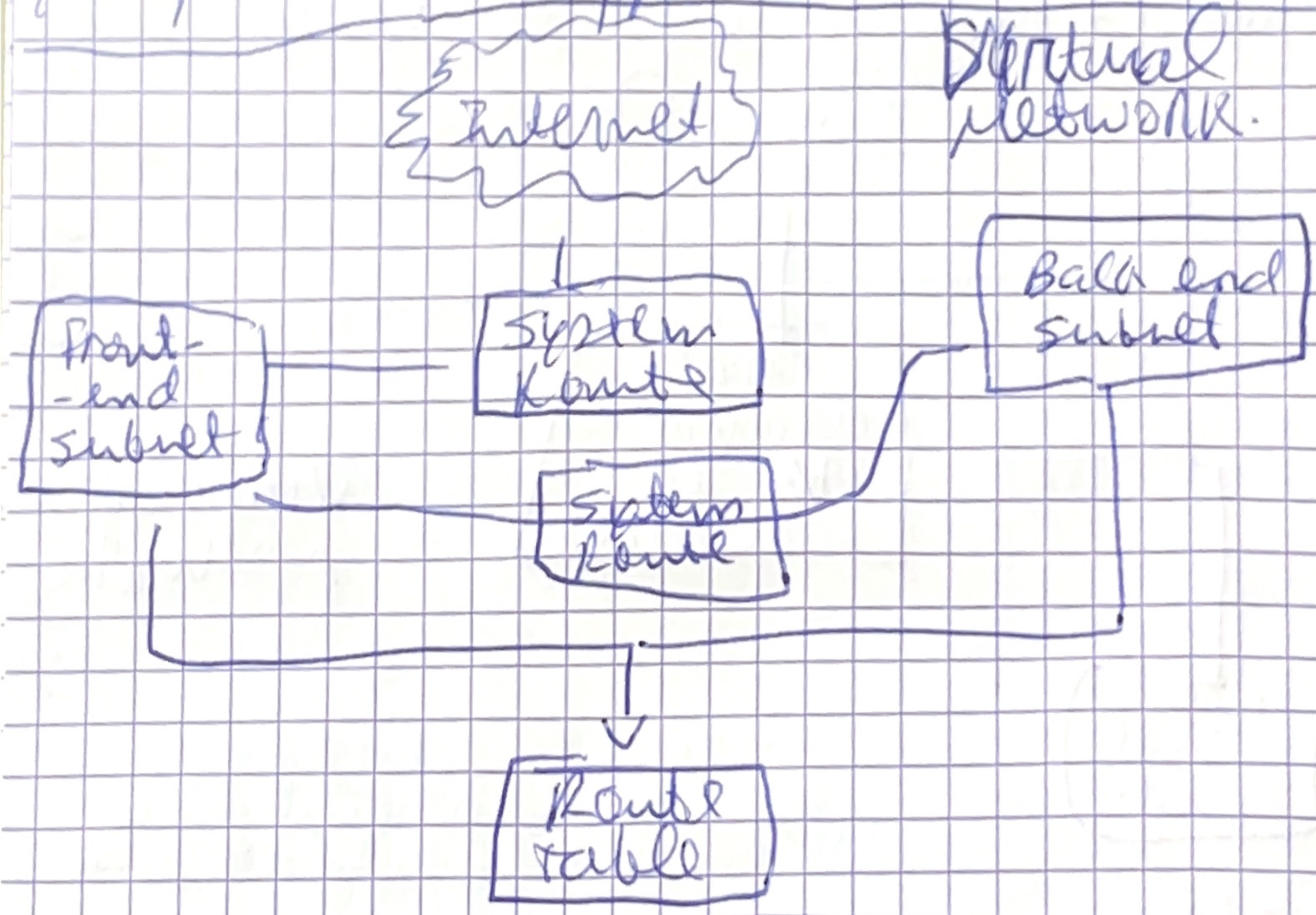
Review system routes

- Azure uses system routes to direct network traffic between virtual machines, on-premise networks and the internet.
- Information about system routes is recorded in a route table.

Things to Know

- Azure uses system routes to control traffic for virtual machines in various scenarios:
  - Traffic between virtual machines in the same subnet.
  - Traffic between virtual machines in different subnets in the same virtual network.
  - Traffic from virtual machines to the internet.
- A route table contains a set of rules that specify how packets should be routed in a virtual network.
- Route tables record information about the system routes, where the tables are associated to subnets.
- Each packet leaving a subnet is handled based on the associated route table.
- Packets are matched to routes by

using the destination. This destination can be a IP address virtual network gateway or a virtual appliance or the internet.
- when a matching route can't be found the packet is dropped.



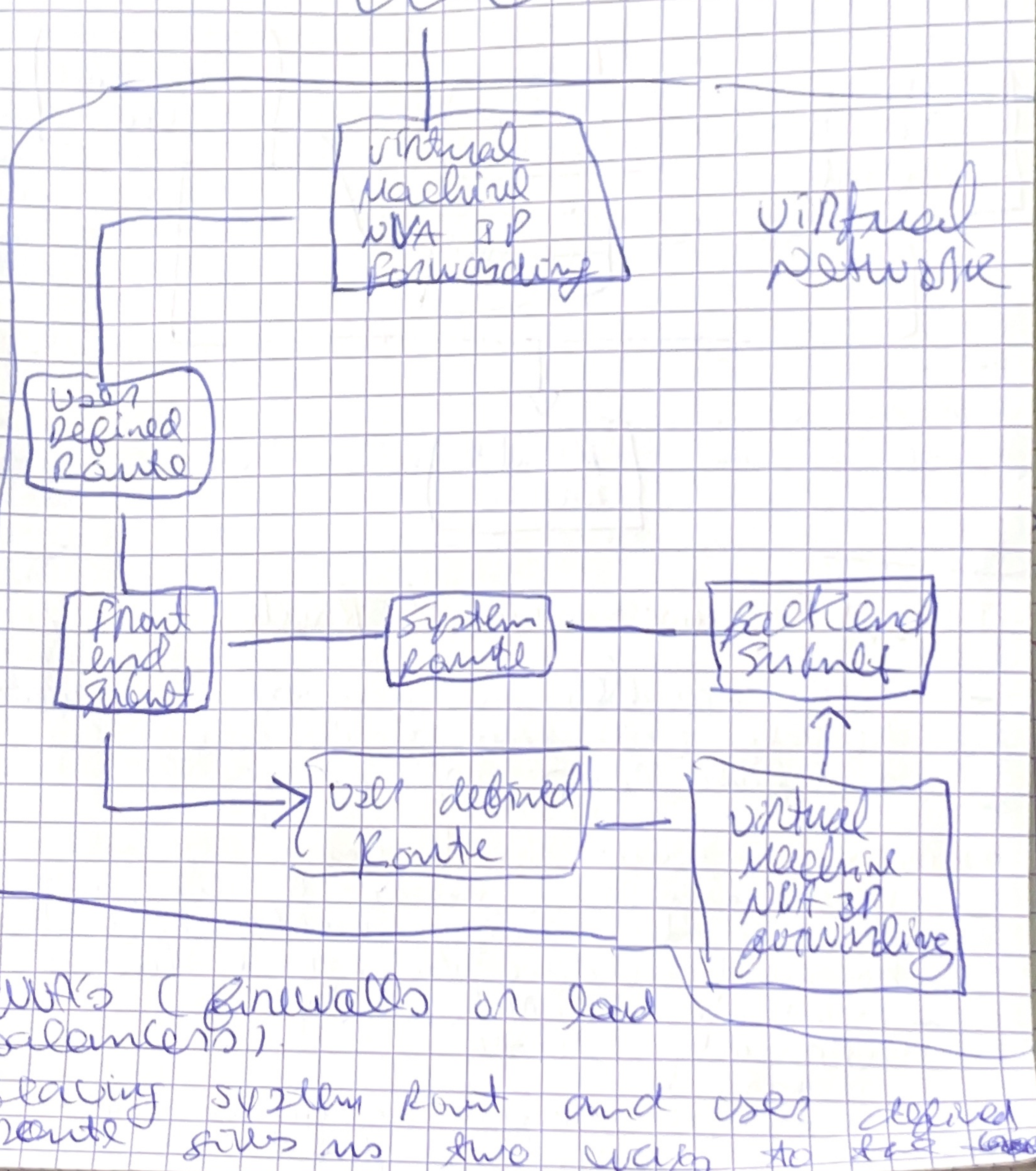
Identify user-defined Routes

- Azure handles the network configuration herself but you should config a user defined route (UDR)

Things to know about user-defined Routes

- UDRs control network by defining routes that specify next traffic flow
- The next traffic flow point can be:
  - virtual network Gateway
  - virtual network
  - Internet
  - network virtual appliance (NVA).
- It also accesses route tables

- each route table can be associated to multiple subnets.
- Each subnet can be associated to one route table only.
- there are no charges for creating route tables in Microsoft Azure.



NVA's (firewalls or load balancers).

Having system Route and user defined route gives us two ways to [illegible]

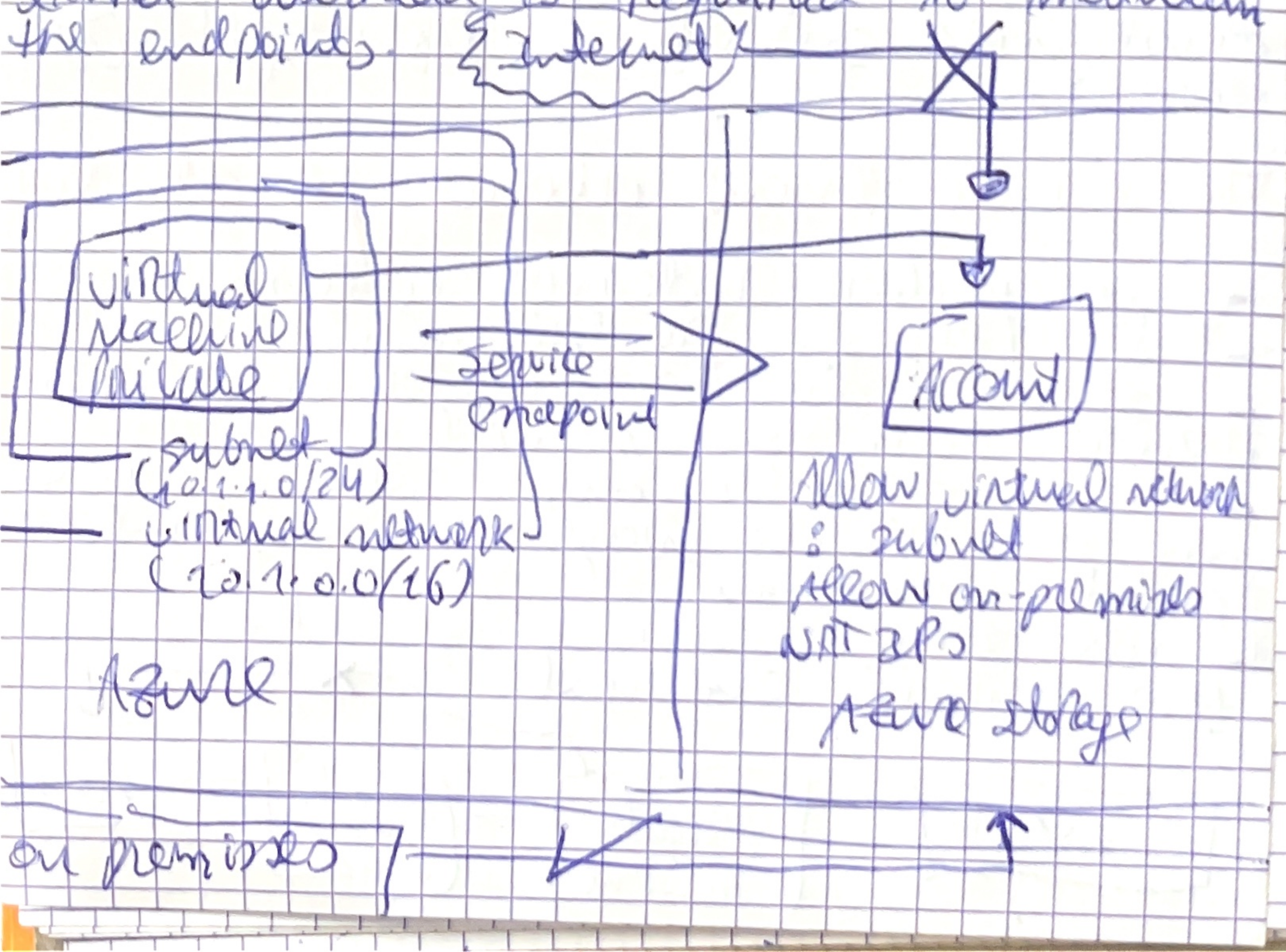
Traffic

Service endpoints

- to make connections between services not accessible over the internet.
- to allow private communications

Things to know about service endpoints

- can extend your virtual network identity to our Azure services resources
- we can use virtual network rules on it.
- it can remove public internet access to resources and allow traffic only privately.
- always make the connection directly with the service without going for the internet
- configured through the subnet. No extra overhead is required to maintain the endpoints.



Things to consider when using Service Endpoints

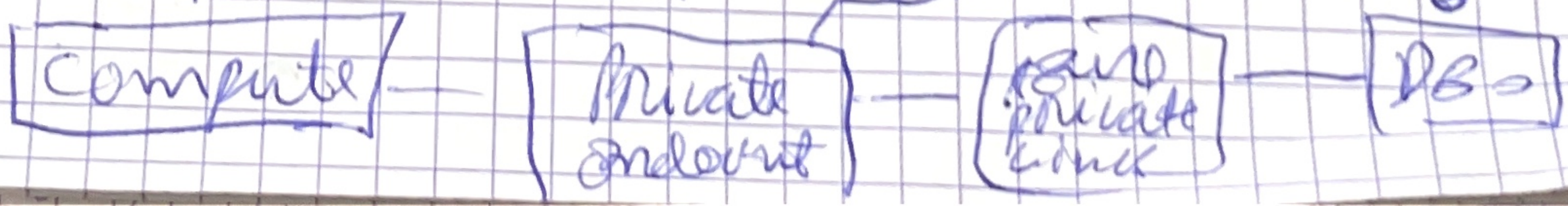
- consider improved security for resources
- Implementing it will remove internet access.
- consider optimal routing for service traffic avoids
- This creates tunneling
- consider direct traffic to the Microsoft network
- This allows direct access to resources.
- consider easy config and maintenance.

Identify private link uses

- Provides private connectivity from a virtual network to a customer owned or Microsoft PAAS services.

Things to know about private link

- No public internet access.
- No Region restrictions.
- services decentralized/developed in azure can be brought to it.
- can deliver our own services in a private way to customers private networks.
- All traffic can be routed through the private endpoint.



Things to consider when using Azure Private Link

- Private connectivity to services on Azure.
- Integration with on-premises and peered networks
- Protection against data exfiltration for Azure resources.
- Services delivered directly to customer virtual networks.