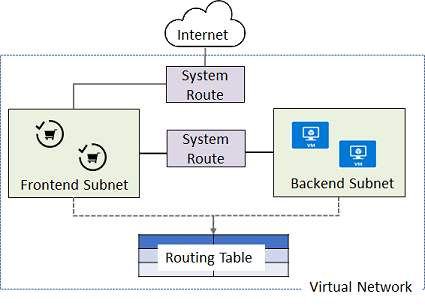
Network Route Table

How the data is travelling on the network? Route table is the one which takes care of it. On the network, we got a route table and this route table will have route rules which are responsible for guiding the packets to reach their destination. Similarly, it happens in virtual network.

When you add Virtual Machines (VMs) to a Virtual Network (VNet) in Azure, you will notice that the VMs are able to communicate with each other over the network automatically. And there are certain predefined rules which we call as system routes and they are responsible for guiding the traffic.

You need not specify a gateway, even though VMs ate in different subnets. The same is true for communication from the VMs to the public internet, and even to your on-premises network when a hybrid connection from Azure to your own data centre is present.



The flow of communication is possible because Azure uses a series of system routes to define how IP traffic flows.

System routes control the flow of communication in the following scenarios

* From within the same subnet
* From a subnet to other within a VNet
* From VMs to Internet
* From a VNet to other VNet through a VPN Gateway
* From a VNet to other VNet through VNet Peering
* From a VNet to your on-premises network through a VPN Gateway
* (Site to site connection)

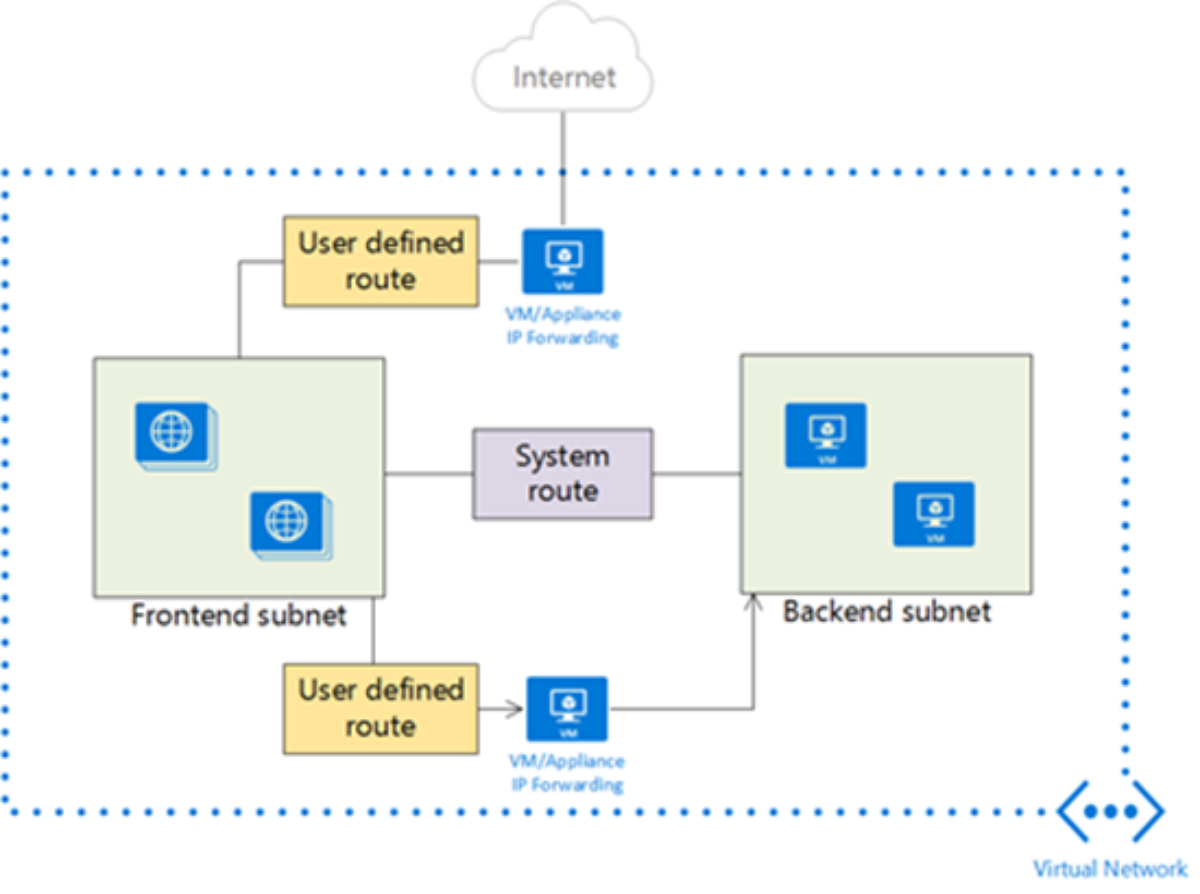
System routes take care of how data packets should move from one IP to other

Information about the system routs is recorded in a route table. A route table consists of a set of rules, called routes, that specifies how packets should be routed in a virtual network. The route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Packets are matched to the routes using the destination. The destination can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route is not found, then the packet is dropped.

**User defined Routes**

For most cases, you will only need the system routes already defined by Azure. However you may need to create a route table and add one or more routes in specific cases. Such as

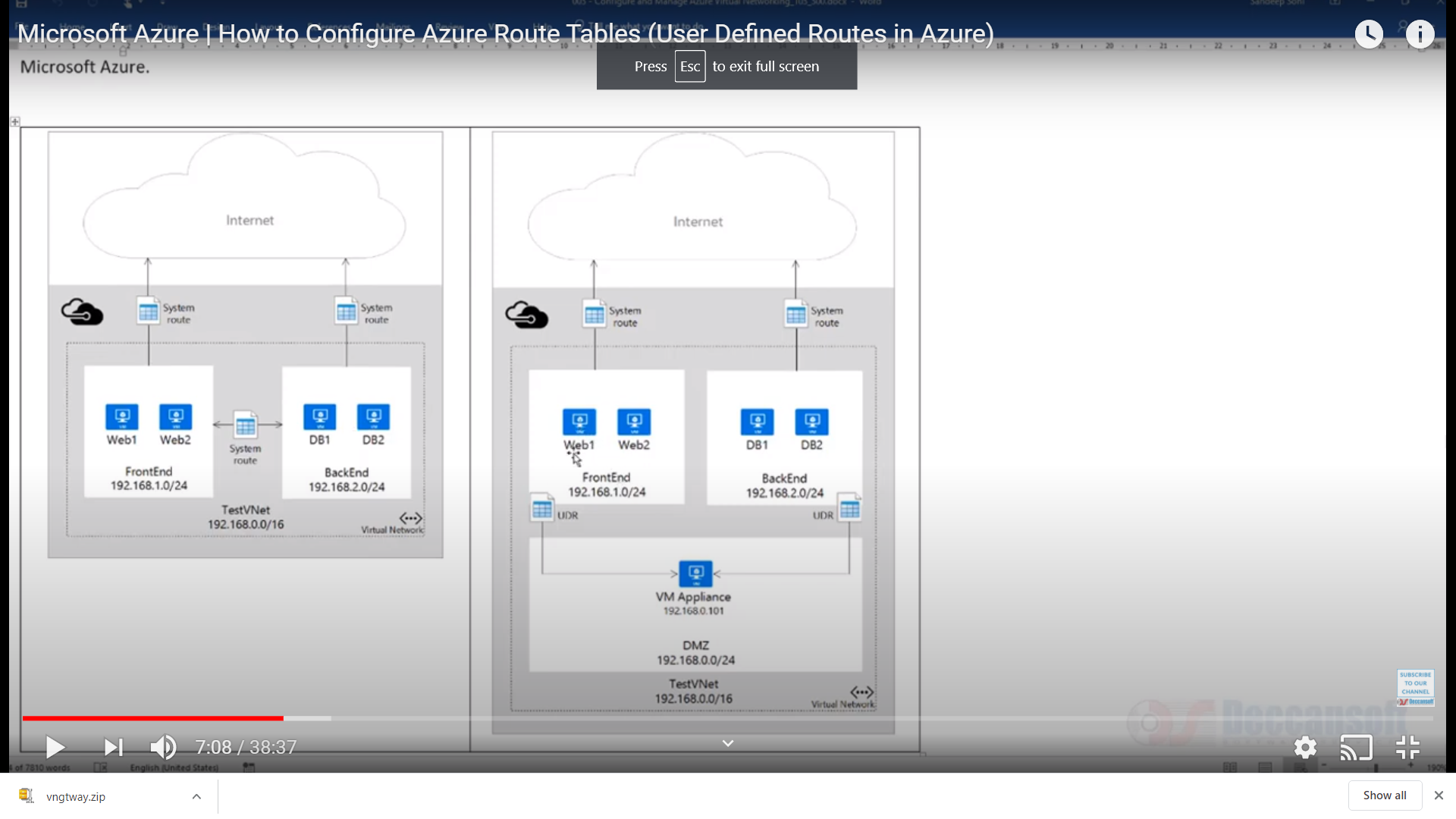
* Use of virtual appliances in An Azure environment (Ex. Firewall), Data will be forwarded through firewall, it will decide whether to pass data or lock data / Log some data for analysis/ For checking some company policy and then transfer to other machines)
* Force tunnelling to the Internet via your on-premises network

Will th

If we create User defined route, we tell that any traffic that originates from any Vm which is in the Frontend subnet, it should actually get routed rom Virtual Appliance and Virtual Appliance will then forward it to Backend Subnet.

Rule like

If Frontend is the destination, then the next hop should be Virtual Appliance.



Here VMs in FrontEnd Server can communicate with VMs in Backend subnets

But now we wanted traffic to flow through a Virtual Appliance which is a VM itself.

**Azure** network **virtual appliance** is used in the **Azure** application to enhance high availability. It is used as an advanced level of control over traffic flows, such as when building a demilitarized zone (DMZ) in the cloud.

In computer security, a DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet

Force tunnelling to the Internet via your on-premises network.

Each route table can be associated to multiple subnets, whereas a subnet can only be associated to a single route table.

User defined routes are only applied to traffic leaving a subnet. You cannot create routes to specify how traffic comes into a subnet from the Internet.

Also the appliance you are forwarding traffic to cannot be in the same subnet, where the traffic originates. Always create a separate subnet for your appliance.

NVAs are the VMS which help with network functions like routing and firewall optimizations. Some of the cases where virtual appliance can be used are

* Monitoring traffic with an Intrusion Detection System (It’s a device or software application that monitors a network or systems for malicious activity or policy violations)
* Controlling traffic with firewall

The Virtual appliance VM must be able to receive incoming traffic that is not addressed to itself. To allow VM to receive traffic addressed to other destinations you must enable IP Forwarding for the VM.

Network Route Table

• When you add virtual machines (VMs) to a virtual network (VNet) in Azure, you will notice that the VMs are able to communicate with each other over the network, automatically. You do not need to specify a gateway, even though the VMs are in different subnets. The same is true for communication from the VMs to the public Internet, and even to your on-premises network when a hybrid connection from Azure to your own datacenter is present.

• This flow of communication is possible because Azure uses a series of system routes to define how IP traffic flows.

System routes control the flow of communication in the following scenarios:

 From within the same subnet.

 From a subnet to another within a VNet.

 From VMs to the Internet.

 From a VNet to another VNet through a VPN gateway.

 From a VNet to another VNet through VNet Peering (Service Chaining).

 From a VNet to your on-premises network through a VPN gateway.

Information about the system routes is recorded in a route table. A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Packets are matched to routes

using the destination. The destination can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route can't be found, then the packet is dropped.

User-Defined Routes

For most environments, you will only need the system routes already defined by Azure.

However, you may need to create a route table and add one or more routes in specific cases, such as:

o Use of virtual appliances in your Azure environment.

o Force tunneling to the Internet via your on-premises network.