Routing traffic in the network (VNet)

How the teaffic flow from one network to another (one subnet to another)

Route Table contains – destination port and next hop address.

Route Table basically contains the source to destination data transferring and how does data flows

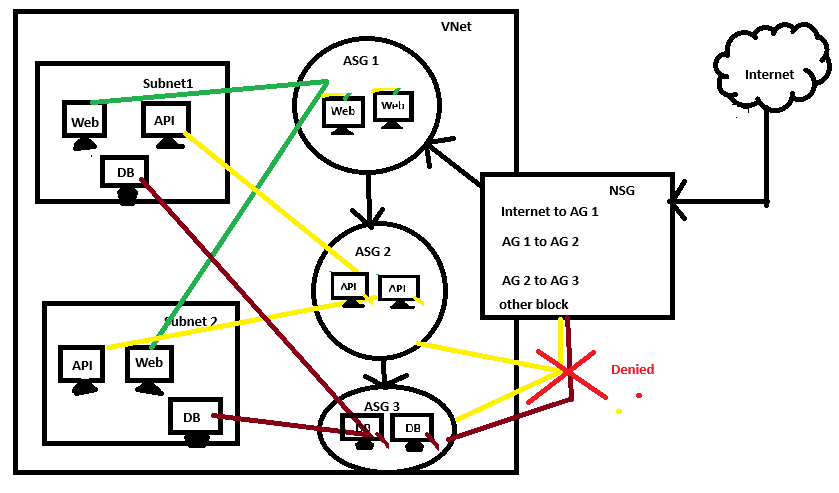
Route table will be associated with subnet’s.

One route table can be associated with multiple subnets, but one subnet will be associated with only one route table.

The application group helps to apply same security rules on NSG for multiple servers, it can be applied at subnet level or vnet level.

The servers we are grouping together in one application group, will be targeted at once.

Ex- the network traffic will flow flow, from ASG 1 to 2 to 3 out side network will not have direct access to API and DB server. Even the web will not have direct access to DB servers.



Routing-

Routing is a technology that used for sending data from source to destination.

It can be from internet (client) to the destination server or from server to (internet)

Example- internet to server may be client http request trying to access a website hosted on the server.

Or

A outside mail or any data is coming to any of one server.

Or

It can be one vnet or subnet system sending data to another subnet server.

Example- server to internet can be one of my employee is using a system in my network and browsing for a site from internet.

How routing works-

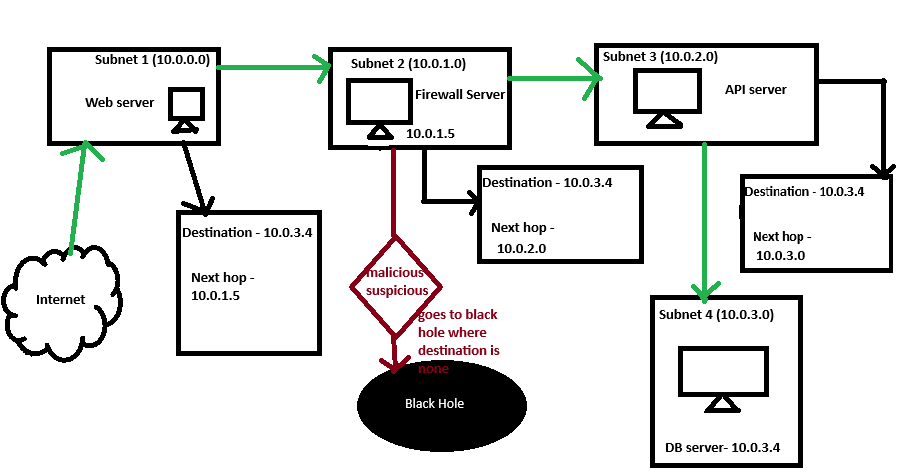
Routing works in such a way that while the traffic is flowing from source to destination, it can be any source to destination.

Fron subnet to another subnet. From a subnet to internet. Here we can attach route table with subnet and decide how our traffic will flow.

If I want that the server should not have access to the internet. I can create a route table and attach to the subnet by blocking internet.

If I want the subnet will only have access from another subnet then again from that subnet to another subnet. I can mention that by adding routing table.

We can actually control how the traffic flow.



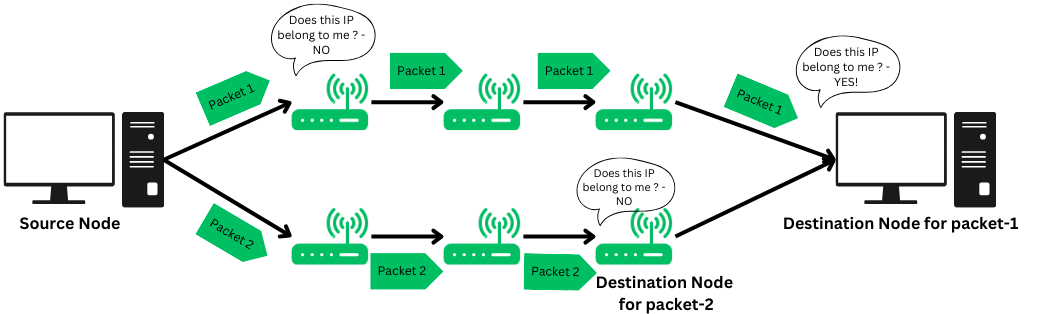
In the above example diagram traffic comes from internet which need to get some data from db server.

1. Traffic hits to web server, here we will block access to other sebnet server. So traffic can not directly goes to any other server,
2. Then from web server we will redirect the traffic to our firewall server in firewall subnet. Here the traffic will be filtered out. Of the request find as a suspicious activity then it will redirect to blackhole where destination is none. Else it will route to next hop address.
3. And finally from api subnet to db server.

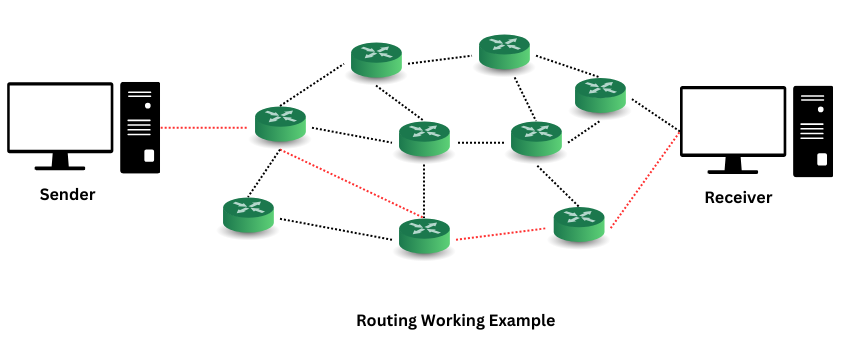
This is how by adding the route table we can control the traffic flow.

In each table the actual destination and the next hop address will be given that’s helps request to reach actual destination by going through next hop only. And here in next hop we can make our firewall to sit and filter the traffic.

If here the route table contain 2 or more possible path to redirect the traffic. The path will be chosen as per routing algorithm.



Example image



**Routing Table**: A data table stored in routers (and sometimes in networked devices) that lists known paths to various network destinations. It contains:

* **Destination**: IP range that specifies where packets should be routed.
* **Next Hop**: The next device (or IP) in the path to the destination.
* **Metric**: A value indicating the "cost" of a path (e.g., distance, speed, reliability).

Lab session with routing—

By Default, azure allow vnet all resource communication and to allow internet, that’s the azure default route.

Step 1.

Create virtual network

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 2.

Verify the resource mapping (diagram) from Network watcher

* Once you setup any resource in a location in that location network watcher will be set up.

For example we created the vnet in east us and a default subnet has been created in that we can see a network watcher has been created for east us.

A screenshot of a computer

Description automatically generated

See the diagram of your resources you created. network watchers gives entire diagram of your resources based on a location then based on main resources and then to sub resource.

1. Go to Network Watcher

A screenshot of a computer

Description automatically generated

Here we can see the all-network watcher created. This also helps us to troubleshoot on any kind of network issue.

1. Navigate to Topology, here we can see all locations where we have created our resources

A screenshot of a computer

Description automatically generated

Click on “+” symbol at location in which we want to see resources. Shows in above image.

1. Then we can see all the main resources in that locations. In my case I have 2 VNet in the location

A screenshot of a computer

Description automatically generated

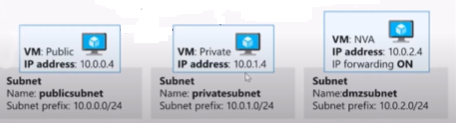
1. To see all the resources inside the vnet, click on “+” option of the Vnet.  
   in my case I did not deploy anything so I just have default subnet in that.

A screenshot of a computer

Description automatically generated

Step 3.

Create 3 subnets in the VNet



We will be implementing the above diagram, where we will create 3 subnets. In 3 subnets we will create 3 Virtual Machines.

1st subnet will be public, and the vm in it will have public ip.

The 2nd subnet will be the private one the vm in it will not have public ip, only the private ip will be assigned.

And finally the 3rd subnet will be our firewall subnet, in this we will configure a vm that will act like a NVA (Network virtual appliance) which acts like a fire wall.

And we will map routing table that the request from public subnet public vm should not reach to private vm. The traffic must goes through firewall.

Step 4.

Create subnet public. (10.0.0.0/24), and Create a public VM in it.

A screenshot of a computer

Description automatically generated

Create vm “public”

A screenshot of a computer

Description automatically generated

Step 5.

Create Private subnet (10.0.1.0/24), and private vm.

A screenshot of a computer

Description automatically generated

Create Private VM

A screenshot of a computer

Description automatically generated

Step 6.

Create firewall subnet (10.0.2.0/24)

In this subnet we will setup our NVA server which is “ Network virtual Appliance” , this server will be assigned few features, that it can act like a firewall or a proxy server. All the network will be traced up in this server.

Note- the NVA server subnet should be a different subnet, never create NVA server where other servers exist, that will cause network loop issue.

NVA server will also have only private ip.

Public ip only for the public server, in real time which is a web server.

Creating firewall or NVA subnet.

Make sure to choose route server in subnet purpose selection.

A screenshot of a computer

Description automatically generated

Create NVA server

A screenshot of a computer

Description automatically generated

Step 7.

Check resources from network topology. We can see all 3 subnets resources.

A screenshot of a computer

Description automatically generated

Step 8.

We should enable ping on those servers, to check ping and network trace.

Go to server powershell.

A screenshot of a computer

Description automatically generated

Run below script

>> Get-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)"

A screenshot of a computer

Description automatically generated

If output enabled is false, we can enable it.

>> Enable-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)"

Do it for all 3 vms.

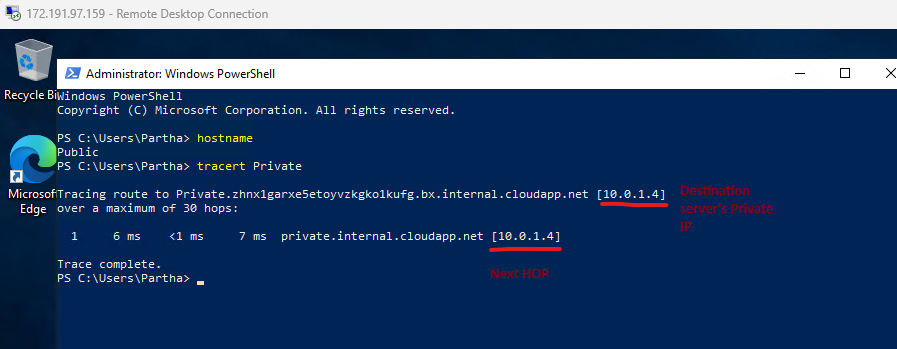
Step 9.

Verify the route on the private server which is on private subnet.

* Go to public server (login to it). And run the below command.

>> tracert your-destination-vm-name

Ex- tracert Private

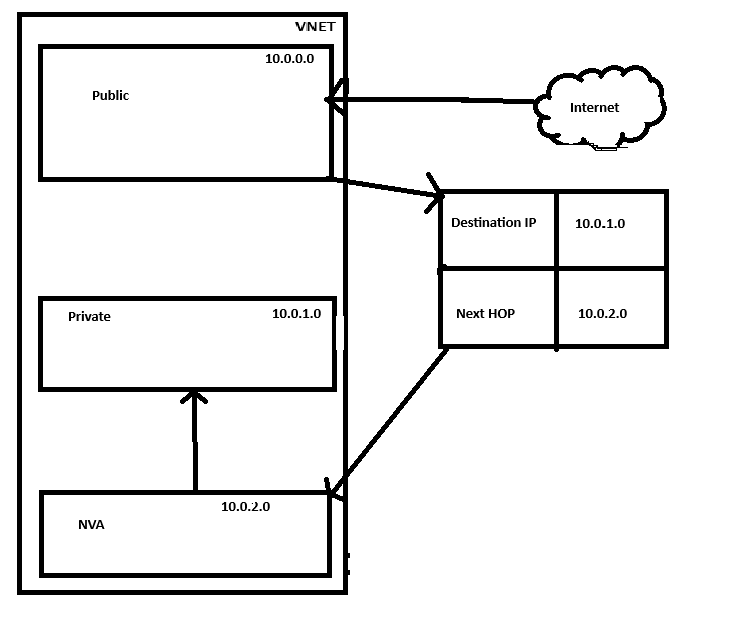


We can see the output that it’s directly able to reach out to the server on next hop only.

But here we want that next hop will be the NVA server and from that to destination private server.

Step 10.

Our Goal-



Step 11.

Configure the NVA virtual machine that it can act as a router.

* Login to NVA server. This server have private ip only so we can take rdp from public vm by private ip.

A computer screen shot of a computer

Description automatically generated

* Open “regedit” on the nva server, which is registry editor.

A screenshot of a computer

Description automatically generated

* Go for hkey local machine

A screenshot of a computer

Description automatically generated

* Go for system, and under system go for current control set.

A screenshot of a computer

Description automatically generated

* Then go for services and find Tcpip

A screenshot of a computer

Description automatically generated

* And navigate to parameter, you will find a option called “IpEnableRouter”

A screenshot of a computer

Description automatically generated

* Double click on IpEnableRouter and set the default value to “1”. Initially it will be “0”.

A screenshot of a computer

Description automatically generated

Save the change and restart the server.

Step 12.

* Go to azure portal. Navigate to NVA server, go for networking and go to it’s NIC.

Go for ip forwarding and enable it.

A screenshot of a computer

Description automatically generated

Step 13.

Create Route table

* Go to azure portal and search for route table.

A screenshot of a computer

Description automatically generated

* Create route table, provide required details and create.

A screenshot of a computer

Description automatically generated

Step 14.

Add route.

* Go to Route table, navigate to route and click on add button to add route.

A screenshot of a computer

Description automatically generated

* Provide the name for the route. It’s totally user define name. I am naming it as public to private subnet route

A screenshot of a computer

Description automatically generated

* Put the destination type. It can be both either a ip address range or a service tag. Service tag which we can applied on the servers tagged together ex- in same nsg or asg.

In out case destination is private subnet so I am choosing ip address and provoding my private ip address range as destination

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Choose Next hop type

It can be any other virtual network, any gate way or none.

None is the one which goes to black hole.

In my case I have configured a server NVA (network virtual appliance) for navigating and filtering the traffic. So I am choosing virtual appliance.

A screenshot of a computer

Description automatically generated

* In virtual hop address provide private ip of NVA server.

A screenshot of a computer

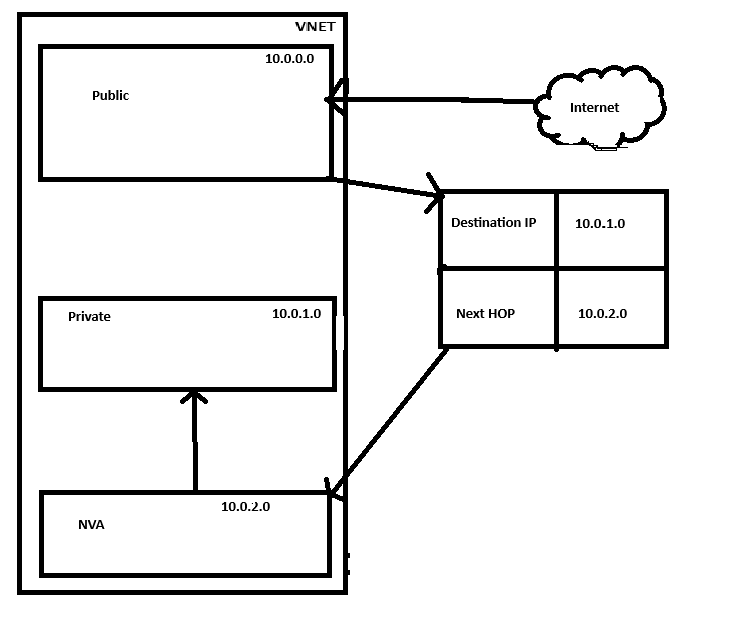
Description automatically generated  
  
Note- if it shows error, please make sure there is no space before ip. Sometime during copying the ip it takes a space before ip. If it please remove that space.

The route will be added, we can also check the configuration and also can make change

Step 15.

Associate the route table to a subnet.

* Under the route table session go for subnets and go for associate subnet.
* Here we will associate it to our public subnet. Because the traffic coming to our public subnet need to follow the route rule and re direct.



A screenshot of a computer

Description automatically generated

Now what ever traffic goes from public subnet they will follow the routing command.

Step 16.

Check the network topology now expand the NIC of Public VM and NVA VM.

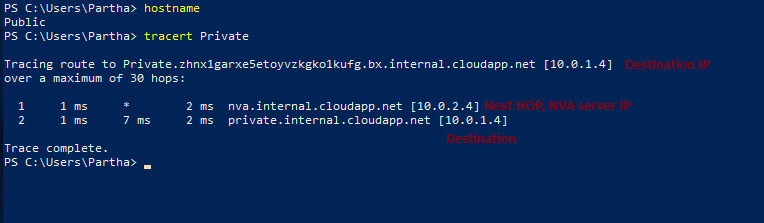
You will see the route added and traffic forwarding enabled. Nothing to do change here.

Step 17.

Now Go to Public VM and tracert (trace route) for private vm.

Now we will see the route is not directly reaching to private vm.

It’s routing via NVA server



If we want to route more then we can do that as well.

Step 18.

Let’s consider a scenario where my routing subnet contains more then 1, i.e 2 vm those are able to do traffic forwording, and route table is added for both path. 2 rule with 2 hop. How that will work.

1. Create snapshot of NVA vm and create 2nd NVA VM by using snap shot disk
2. Check configuration such as ping enabled and route service fixed to 1 as we did for previous NVA vm.

It will be enabled as we created as same vm by taking smapshot of that vm -> create new disk by snapshot -> create new vm by that disk

1. Go for nic and do ip forwording enabled.
2. Adding another route, as we can not give the same destination in 2 different route rule.

In first rule it was siubnet range. In 2nd I am adding the private vm ip and /32 that indicates to that server only

A screenshot of a computer

Description automatically generated

In next hop I have given the 2nd NVA server ip

1. Lets check

Did not worked.

A computer screen shot of a blue screen

Description automatically generated

Reason-

If your route table directs all traffic for 10.0.1.0/24 to the NVA, it should already be passing through the NVA for all internal addresses within that range. Therefore, the second, more specific route (10.0.1.4/32) may not show up explicitly in the traceroute because it is already being handled by the first route.

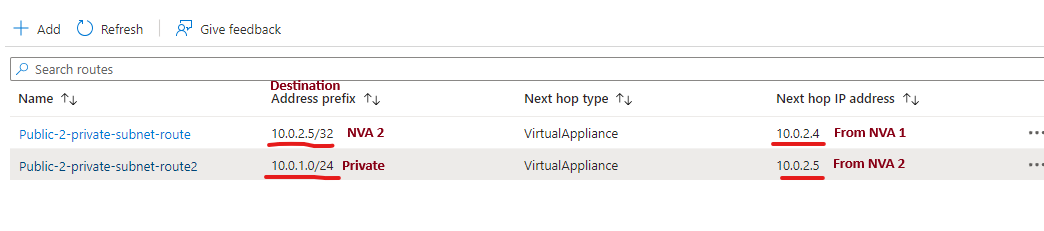
Let’s do another try

Lets redirect route form NVA 1 to NVA 2 and then NVA 2 to destination.

This will be from web server to nva 2 from nva 1

A screenshot of a computer

Description automatically generated



Do Test

Did not work