Az-VNET

Tuesday, October 8, 2024

00:41

Earlier, while developing and deploying software applications, companies had been facing common issues like network attacks, data leaks, poor network connectivity, time-consuming processes in building network topologies, and inadequate diversion of network traffic.

With this going on, Microsoft saved the day, right on time Microsoft [Azure](https://www.simplilearn.com/azure-cloud-architect-certification-training-course) addressed these issues and launched Azure Virtual Network, which helped companies communicate securely with other networks and maintain a cost-efficient cloud environment.

**What Is Azure Virtual Network?**

* + An [Azure](https://www.simplilearn.com/tutorials/azure-tutorial/what-is-azure) Virtual Network (VNet) is a network or environment that can be used to run VMs and applications in the cloud.
  + When it is created, the services and Virtual Machines within the Azure network interact securely with each other.

**Advantages of Using Azure Virtual Network**

Some of the major advantages of using Microsoft Azure VNet are as follows:

* + It provides an isolated environment for your applications
  + A subnet in a VNet can access the public internet by default
  + We can easily direct traffic from resources
  + It is a highly secure network
  + It has high network connectivity
  + It builds sophisticated network topologies in a simple manner

Moving on, let's have a look at the components of Azure VNet.

**Components of Azure VNet**

Azure networking components provide a wide range of functionalities that can help companies build efficient cloud applications that meet their requirements.

The components of Azure Networking are listed below, and we have explained each of these components in a detailed manner:

* + Subnets
  + Routing
  + Network Security Groups

**Subnets**

* + Subnets let users segment the virtual network into one or more sub-networks.
  + These sub-networks can be separated logically, and each subnet consists of a server.
  + We can further divide a subnet into two types:
  + Private
  + Public
  + Private - Instances can access the Internet with NAT (Network Address Translation) gateway that is present in the public subnet.
  + Public - Instances can directly access the internet.

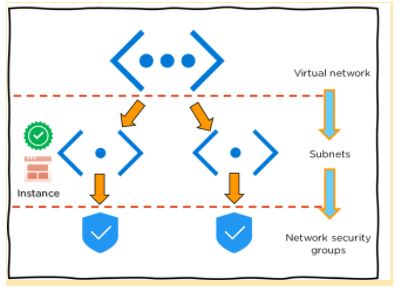
**Routing**

* + It delivers the data by choosing a suitable path from source to destination.
  + For each subnet, the virtual network automatically routes traffic and creates a routing table.

**Network Security Groups**

* + It is a firewall that protects the virtual machine by limiting network traffic.
  + It restricts inbound and outbound network traffic depending upon the destination [IP addresses](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-an-ip-address), port, and protocol.

**How to Launch an Instance using Azure VNet?**



* + First, create a virtual network in the [Azure cloud](https://www.simplilearn.com/azure-cloud-services-and-its-importance-article)
  + Next, create subnets into each virtual network
  + Now, assign each subnet with the respective instance or Virtual Machine
  + After which you can connect the instance to a relevant Network Security Group
  + Finally, configure the properties in the network security and set policies
  + As a result, you will be able to launch your instance on Azure