SECURE VNET HUB USING AZURE FIREWALL MANAGER

STEP-01 CREATE TWO SPOKE VNETS AND SUBNETS

Text, letter

Description automatically generated

Graphical user interface, text, application

Description automatically generated

REPEAT SAME STEPS AS ABOVE, BUT NAME IT SPOKE-02, ADDRESS SPACE:10.1.0.0/16, SUBNET NAME WORKLOAD-02-SN AND SUBNET ADDRESS RANGE 10.1.1.0/24

STEP-02 CREATING SECOND VIRTUAL HUB

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

FROM THE IMAGE ABOVE, I CONFIGURED THE AZURE FIREWALL MANAGER FOR THIS LAB TO ON THE BASIC OF THINGS AS YOU CAN BE MORE AGGRESSIVE ON YOUR CONFIGURATIONS SUCH AS CHOOSING TIER OF FIREWALL, CONFIGURING FIREWALL POLICIES, NUMBER OF PUBLIC ADDRESSES, AVAILABILITY ZONES, CHOOSING A SECURITY PARTNER SUCH AS CHECKPOINT OR ASA.

STEP-03 CONNECTING HUB AND SPOKE VNETS

Graphical user interface, application

Description automatically generated

REPEAT SAME STEPS FOR CONNECTION TO SPOKE-02. EVERYTHING IS GOING TO BE THE SAME BUT THE VNET

NOTE: YOU CAN ALSO CONFIGURE ROUTING TABLES, BUT FOR THIS LAB I CHOOSE NOT TO IMPLEMENT THEM

Graphical user interface, table

Description automatically generated

YOU SHOULD SEE SUCCEEDED IF THE CONNECTION WAS CONFIGURED PROPERLY AS SHOWN ABOVE.

STEP-04 DEPLOYING THE SERVERS

Graphical user interface, application, table

Description automatically generated

Table

Description automatically generated

Graphical user interface, text, application

Description automatically generated

REPEAT STEPS FOR SPOKE-02

STEP-05 CREATING A FIREWALL POLICY TO SECURE HUB

GO TO AZURE FIREWALL MANAGER 🡪 AZURE FIREWALL POLICIES 🡪 CREATE AZURE FIREWALL POLICY

NOTE: BELOW ARE JUST RULES, BUT YOU CAN CONFIGURE THE POLICY TO DO A LOT MORE SUCH AS CONFIGURING THE FOLLOWING: DNS SETTINGS, TLS INSPECTION, IDPS, OR THREAT INTELLIGENCE

Graphical user interface, text, application, email

Description automatically generated

ABOVE IMAGE IS APPLICATION RULE

Graphical user interface, text, application, email

Description automatically generated

ABOVE IMAGE IS A DNAT RULE ALLOWING REMOTE ACCESS TO SPOKE 1 TO ACCESS ITS PRIVATE NETWORK

Graphical user interface, application, Word

Description automatically generated

THIS RULE IS NETWORKING RULE ALLOWING ANY REMOTE CONNECTION TO SPOKE 2 PRIVATE NETWORK

\*\* ONCE YOU CONFIGURED YOUR HUBS AND PEERED THE CONNECTION YOU SHOULD SEE YOUR FIREWALL MANAGER MANAGE AS BELOW

Graphical user interface, application

Description automatically generated

STEP-06 ASSOCITATE FW POLICY WITH HUB

GO TO FIREWALL MANAGER 🡪 AZURE FW POLICIES 🡪 SELECT THE HUB/VNET YOUR WANTING TO CONNECT 🡪 MANAGE ASSOCIATIONS AND ADD

Graphical user interface, text, application

Description automatically generated

STEP-07 ROUTING TRAFFIC TO HUB

TO GET TO THE BELOW IMAGE: FIREWALL MANAGR 🡪 VIRTUAL HUBS UNDER DEPLOYMENTS 🡪 SELECT THE HUB 🡪 SECURITY CONFIGURATION UNDER SETTINGS

Graphical user interface, text, application, email

Description automatically generated

ONCE YOU HIT SAVE YOU SHOULD GET A POP UP AS SHOWN BELOW

Text

Description automatically generated with low confidence

JUST CLICK OK TO PROCEED

NOTE: THIS COULD TAKE A FEW MINUTES AS IT IS UPDATING THE ROUTING TABLES

WHEN THE CONNECTION FINISHES YOU SHOULD SEE THE FIREWALL SYMBOL NEXT TO YOUR HUBS INTERNET AND PRIVATE TRAFFIC AS SHOWN BELOW

Graphical user interface, application

Description automatically generated

STEP-08 TEST THE FIREWALL AND RULES

RDP IN SPOKE-01 AND ATTEMPTING TO BROWSE THE NET USING GOOGLE WHILE GETTING DENIED WERE BOTH SUCCESFFUL. MEANING CONNECTION WAS CONFIGURED PROPERLY AND SO WAS THE APPLICATION POLICY WE CREATED.

Graphical user interface, text, application, email

Description automatically generated

TO CHECK THE NETWORKING RULE. I WAS ABLE TO CONNECT SPOKE-02 VIA PRIVATE IP AS SHOWN BELOW

Graphical user interface

Description automatically generated

FOR MORE INFORMATION ABOUT SPOKE AND HUB NETWORK CHECK OUT: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

Hub Vnets – Centralized Point for connectivity to any On-Prem network.

Spoke Vnets – Isolate workloads in their own Vnet and managed separately from any other Spoke Vnets. Each Spoke Vnet can include multiple Tiers.

Vnet Peering (Securing Vnets/ Hub Vnets) allowing for non-transitive, low latency connections between Vnets. Vnets allow for traffic exchange using Azure backbone Without the need for a router.