Copyright (c) Microsoft Corporation. All rights reserved.

Licensed under the MIT License.

Change Request for Azure VPN

# Summary:

Microsoft Azure will have two sites, which will have Active/Active gateways between Azure and Enterprise network.

The Active/Active Connection will be leveraging BGP routing to enable resiliency between the connections and the core network at the Enterprise.

Note: The BGP addresses that are advertised from the Enterprise (customer premise) should suppress the advertisement of the default route address 0.0.0.0/0, unless it is a policy requirement. There are many services in Azure that are going to leverage the default route, for example Azure Storage.



# Details:

Azure will have two Local Network Gateway for two of the connections that will define the IP address, ASN Number and BGP address of the VPN connections. The goal of the gateway is to have redundancy by having BGP routing the ability

## Local Network Gateway Enterprise1

The first VPN connection pairs details will be defined in this connection document.

Tunnel IP Address:

ASN Number:

BGP Neighbors Address:

Weight:

## Local Network Gateway Enterprise2

Tunnel IP Address:

ASN Number:

BGP Neighbors Address:

Weight:

## VPN Tunnel in Site 1

Site1 Tunnel Address1:

Site1 Tunnel Address2:

ASN Number: **65521**

Neighbor Address 1: **10.128.63.228**

Neighbor Address 2: **10.128.63.229**

## VPN Tunnel in Site 2

Site2 Tunnel Address1:

Site2 Tunnel Address2:

ASN Number: **65522**

Neighbor Address 1: **10.128.127.228**

Neighbor Address 2: **10.128.127.228**

# VNETs and Subnets

For the configuration of the access control list (ACL) required to segment traffic use the following summaries. The VNET table shows the summaries of what type of workload will be used. For example, if you want to segment the workloads that are PreProduction and only allow these workloads to talk with developers and other PreProduction networks, an ACL can be established to summarize these workloads and what they are allowed to talk with.

The next level of granularity, and probably priority is the subnets. Each subnet will define a tier in the network that the workload is allowed to perform. Typically DMZ subnets are designed to be the only workloads that are authorized to have an internet endpoint.

## VNETs:

|  |  |  |
| --- | --- | --- |
| vnet\_prod\_w1 | 10.128.0.0 | /20 |
| vnet\_hbi\_w1 | 10.128.16.0 | /20 |
| vnet\_preprod\_w1 | 10.128.32.0 | /20 |
| vnet\_storage\_w1 | 10.128.48.0 | /21 |
| vnet\_services\_w1 | 10.128.56.0 | /21 |
| vnet\_prod\_w2 | 10.128.64.0 | /20 |
| vnet\_hbi\_w2 | 10.128.80.0 | /20 |
| vnet\_preprod\_w2 | 10.128.96.0 | /20 |
| vnet\_storage\_w2 | 10.128.112.0 | /21 |
| vnet\_services\_w2 | 10.128.120.0 | /21 |

Subnets that have the possibility for Internet Endpoints these are the DMZ Subnets

|  |  |
| --- | --- |
| 10.128.8.0 | /24 |
| 10.128.9.0 | /24 |
| 10.128.22.0 | /24 |
| 10.128.23.0 | /24 |
| 10.128.35.0 | /25 |
| 10.128.35.128 | /25 |
| 10.128.43.0 | /25 |
| 10.128.43.128 | /25 |
| 10.128.60.0 | /25 |
| 10.128.61.0 | /25 |
| 10.128.63.112 | /28 |
| 10.128.63.192 | /28 |
| 10.128.72.0 | /24 |
| 10.128.73.0 | /24 |
| 10.128.86.0 | /24 |
| 10.128.87.0 | /24 |
| 10.128.99.0 | /25 |
| 10.128.99.128 | /25 |
| 10.128.107.0 | /25 |
| 10.128.107.128 | /25 |
| 10.128.124.0 | /24 |
| 10.128.125.0 | /24 |