Implementing Azure Point to Site VPN Gateway for Azure microservices Architecture using Private Endpoints

In this blog, I will be creating Point to Site VPN Gateway for the Azure Serverless Architecture to ensure the Security and compliance.

Problem Statement:

As we are moving most of the applications to cloud, what security practices we are following to our resources in the cloud is the biggest question. Although Azure has the best security standards which we can leverage for Azure Services without any custom code (E.g., Azure Active Directory Authentication, Conditional Access Policies), it's not always 100% secure as it is flowing through the **public internet**. At any cost, we should not be satisfied with our architecture.

As an example, if we are developing Azure Static Web app (Global Service) for hosting Single Page Public Application with backends Azure Functions, Azure API Management Service, Key Vault, Service Bus, App Configuration, Logic App, Azure Storage accounts and with Azure B2C as Identity provider, whoever is having the URL of the web app can directly access the application along with its backend services. In case if we are following Agile methodology for Continuous Deployment, we would be deploying till the UAT Stage incrementally.

It will be prone to attacks due to below reasons,

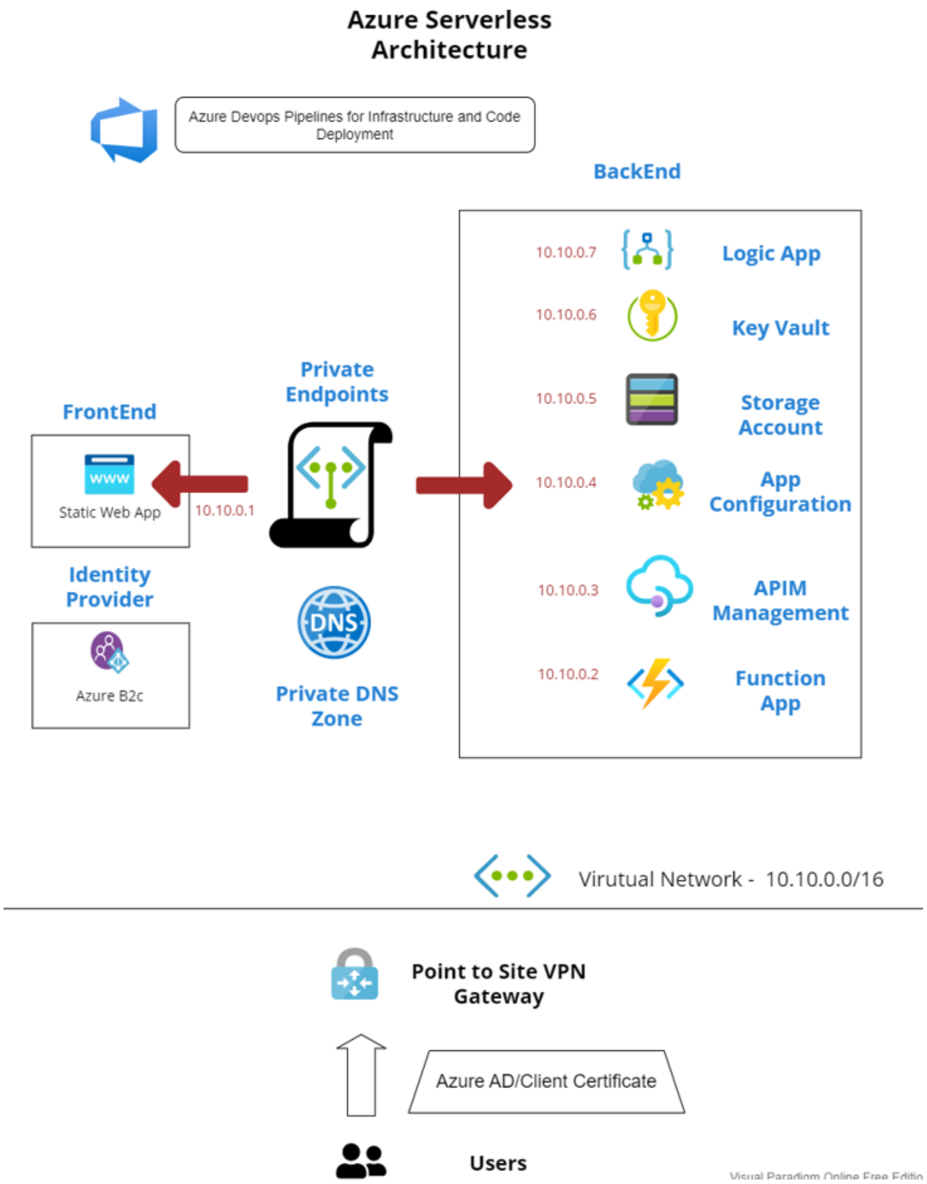
1. Since our application is on public internet, attackers/outsiders can have access to NonProd or Prod Environments and they may get more insights on our application before it goes to Production.
2. Exposing of Backend flow in internet
3. DDOS Attack

Solution/Architecture

In order to protect our microservices, we can create private endpoint to those An IP address from the selected virtual network subnet will be assigned dynamically/manually to ensure the access to the services only from that virtual network. Then create Point to Site VPN gateway using Azure AD authentication or Client Certificate and connect it with virtual network.

[More Info - Azure Micrososervices Architecture Design]

Architecutre Diagram



Overview of Services Involved

Private Endpoint: It creates a network interface card in the selected Virtual Network with private IP address and bring that service inside the virtual network to access privately and securely via Azure Private Link. More Info - Azure Private Endpoint

Private DNS Zone: It manages DNS resolution inside the virtual network(Note: No need to create any DNS records, will be done automatically) More Info - Azure Private DNS Zone

Point to Site VPN Gateway: A Secure Tunnel gateway for the clients outside of virtual network to access the resources or applications. More Info - Azure Point to Site VPN

SKU/tier Required for the each services in order to private endpoint feature.

Resource	Minimum SKU/Tier Required for Private Endpoint Support
Static Web App	Standard
KeyVault	Standard
Stoarage Account	General Purpose v2
Azure Functions/Web Apps	Premium - P1V2
Logic App	Standard
ServiceBus	Premium
App Configuration	Standard
API Management	Developer

Private Endpoint Availability of Azure Resources

Implementation

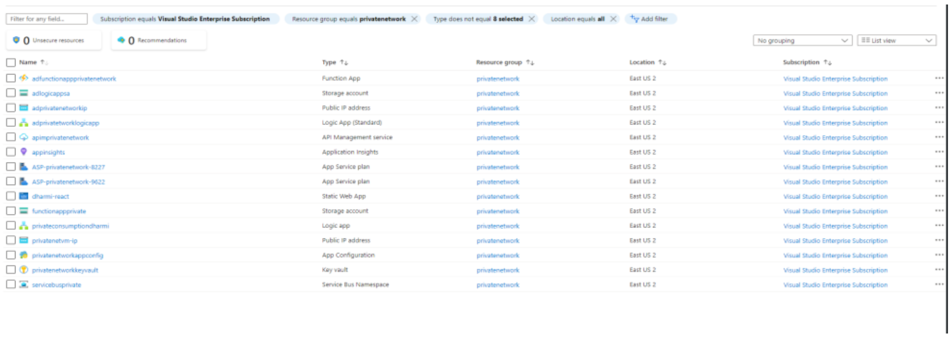
Prerequisites:

1. Active Azure Subscription/trail. To start free Azure Trail
2. Global Admin rights in Azure to consent for the installation of VPN Client App.

Step 1: Create Required Infrastructure in Azure

Provision your infrastructure resources in Azure manually or using Infrastructure templates.

Github - Azure Infrastructure Template



Filter for any field... | Subscription equals **Visual Studio Enterprise Subscription** | Resource group equals **privatenetwork** | Type does not equal **8 selected** | Location equals **all** | Add filter

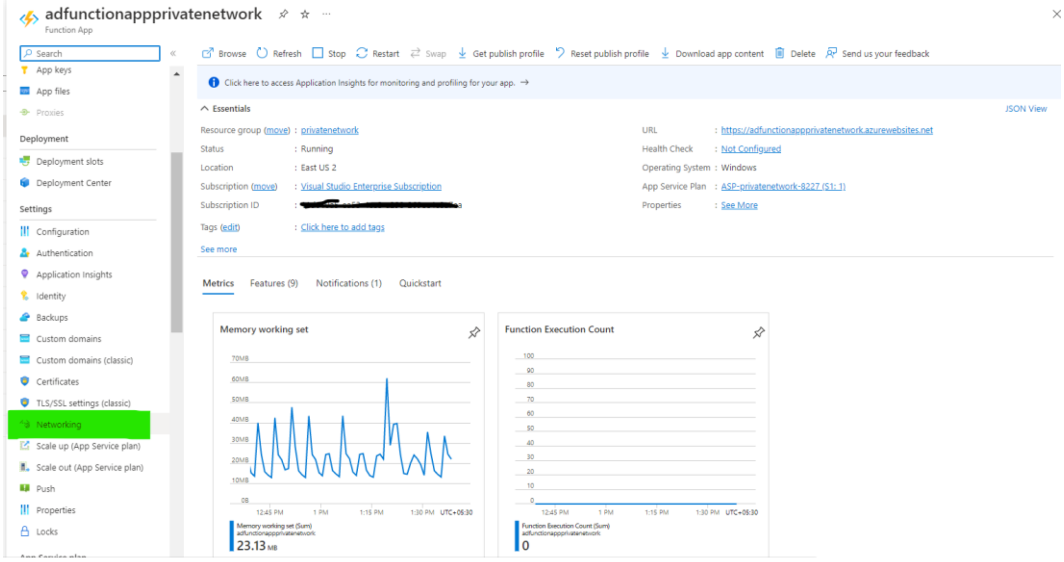
0 Unsecure resources | 0 Recommendations | No grouping | List view

□ Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
□ adfunctionappprivatenetwork	Function App	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ adlogicappsa	Storage account	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ adprivatenetworkip	Public IP address	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ adprivatetworklogicapp	Logic App (Standard)	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ apimprivatenetwork	API Management service	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ appinsights	Application Insights	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ ASP-privatenetwork-8227	App Service plan	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ ASP-privatenetwork-9622	App Service plan	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ dharmi-react	Static Web App	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ functionappprivate	Storage account	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ privateconsumptiondharmi	Logic app	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ privatenetvm-ip	Public IP address	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ privatenetworkappconfig	App Configuration	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ privatenetworkkeyvault	Key vault	privatenetwork	East US 2	Visual Studio Enterprise Subscription
□ servicebusprivate	Service Bus Namespace	privatenetwork	East US 2	Visual Studio Enterprise Subscription

Step 2: Set up Private Endpoint for the Resources:

I'm sharing the steps Involving in Azure function Private Endpoint.

1. Go the Azure Function and select networking from the left side bar.



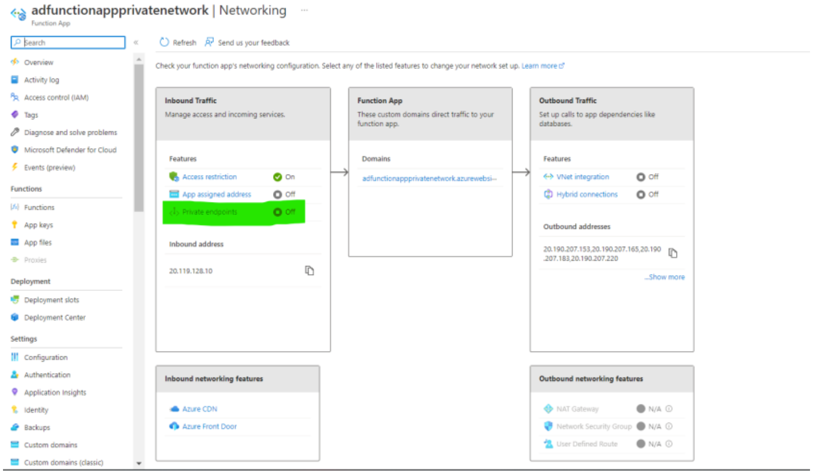
adfunctionappprivatenetwork
Function App

Click here to access Application Insights for monitoring and profiling for your app. →

Essentials

Resource group (move)	: privatenetwork
Status	: Running
Location	: East US 2
Subscription (move)	: Visual Studio Enterprise Subscription
Subscription ID	: [redacted]
Tags (edit)	: Click here to add tags
URL	: https://adfunctionappprivatenetwork.azurewebsites.net
Health Check	: Not Configured
Operating System	: Windows
App Service Plan	: ASP-privatenetwork-8227 (S1: 1)
Properties	: See More

2. Select the option private endpoint form inbound Traffic.



adfunctionappprivatenetwork | Networking
Function App

Check your function app's networking configuration. Select any of the listed features to change your network set up. Learn more

Inbound Traffic
Manage access and incoming services.

Features

Access restriction	On
App assigned address	Off
Private endpoints	Off

Inbound address
20.119.128.10

Function App
These custom domains direct traffic to your function app.

Domains
adfunctionappprivatenetwork.azurewebsi...

Outbound Traffic
Set up calls to app dependencies like databases.

Features

VNet integration	Off
Hybrid connections	Off

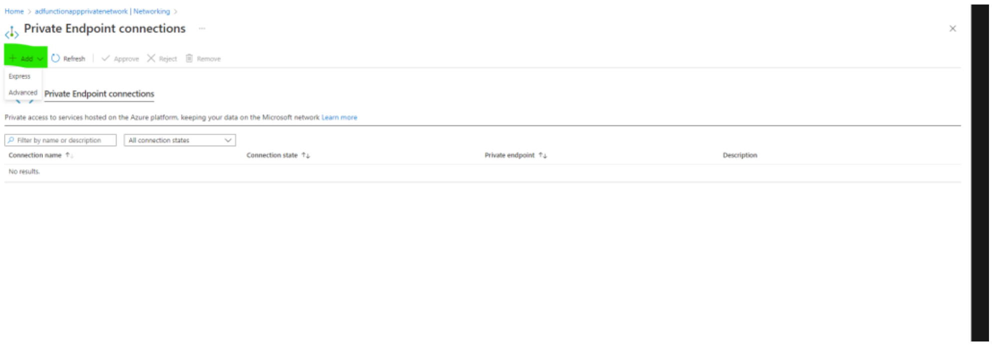
Outbound addresses
20.190.207.153,20.190.207.165,20.190.207.183,20.190.207.220
...Show more

Inbound networking features
Azure CDN
Azure Front Door

Outbound networking features

NAT Gateway	N/A
Network Security Group	N/A
User Defined Route	N/A

3. Click Add -> Express(for quick create) or Advanced for more options. I'm using advanced option.

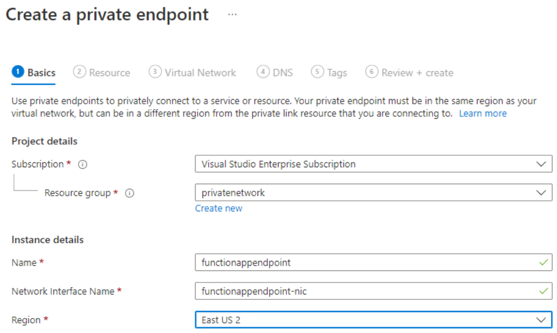


Home > adfunctionappprivatenetwork | Networking >
Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network Learn more

Connection name	Connection state	Private endpoint	Description
No results.			

4. Select Subscription, Resource Group, private endpoint name



Create a private endpoint ···

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : Visual Studio Enterprise Subscription

Resource group * : privatenetwork

Create new

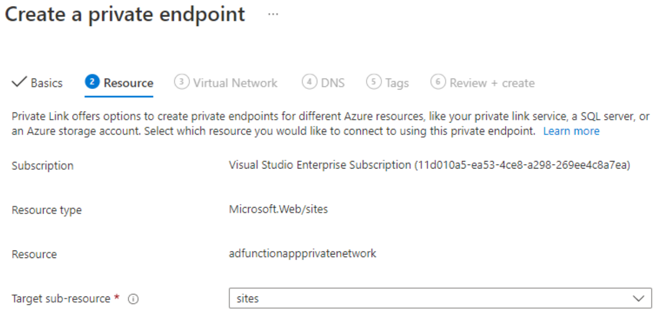
Instance details

Name * : functionappendpoint

Network Interface Name * : functionappendpoint-nic

Region * : East US 2

5. Based on the resource, all option will be auto populated in resource tab



Create a private endpoint ···

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

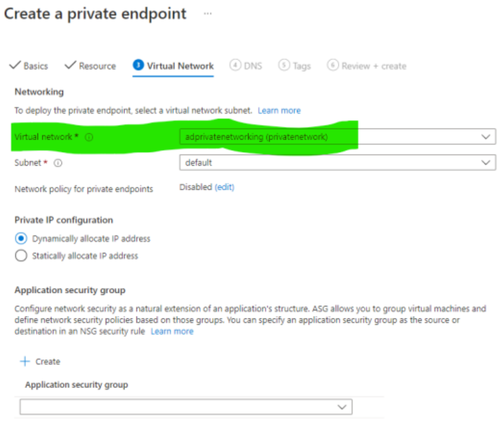
Subscription: Visual Studio Enterprise Subscription (11d010a5-ea53-4ce8-a298-269ee4c8a7ea)

Resource type: Microsoft.Web/sites

Resource: adfunctionappprivatenetwork

Target sub-resource * : sites

6. Select the Virtual network where you want to establish the private link for the resource. Allocate Private IP either static or dynamically.



Create a private endpoint ···

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network * : adprivatenetworking (privatenetwork)

Subnet * : default

Network policy for private endpoints: Disabled (edit)

Private IP configuration

● Dynamically allocate IP address

○ Statically allocate IP address

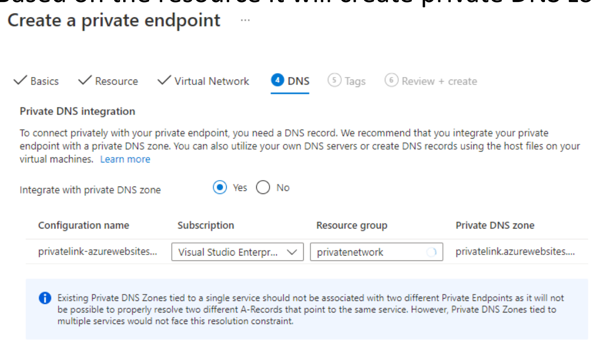
Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule Learn more

+ Create

Application security group

7. Based on the resource it will create private DNS zone aswell.



Create a private endpoint ···

Private DNS integration

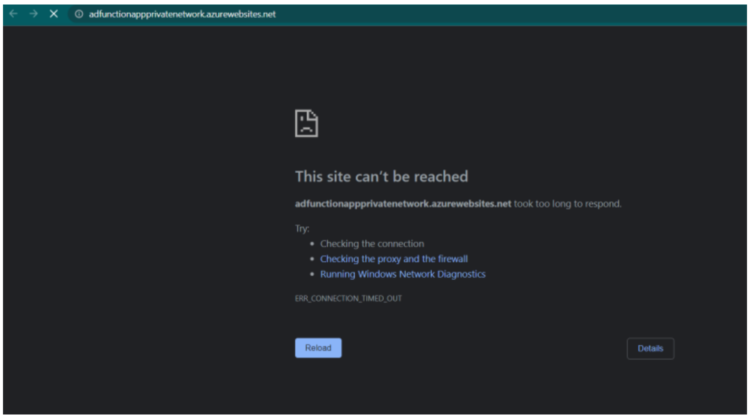
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more

Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-azurewebsites...	Visual Studio Enterpr...	privatenetwork	privatelink.azurewebsites....

Existing Private DNS Zones tied to a single service should not be associated with two different Private Endpoints as it will not be possible to properly resolve two different A-Records that point to the same service. However, Private DNS Zones tied to multiple services would not face this resolution constraint.

8. Review and create.
9. Once you have done with the setup, you won't be able to access the function app from public internet.



This site can't be reached

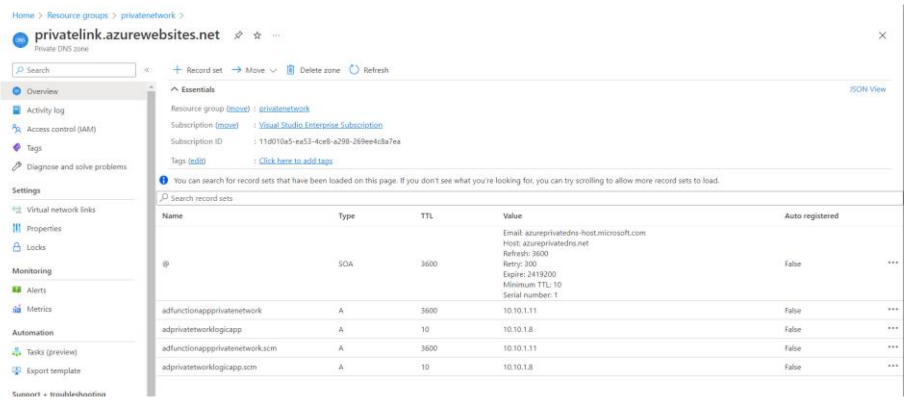
adfunctionappprivatenetwork.azurewebsites.net took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

10. One Private DNS also be created after private endpoint creation.



Resource group (move) : privatenetwork
Subscription (move) : Visual Studio Enterprise Subscription
Subscription ID : 11d010a5-ea53-4ce8-a298-269ee4c8a7ea
Tags (edit) : Click here to add tags

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

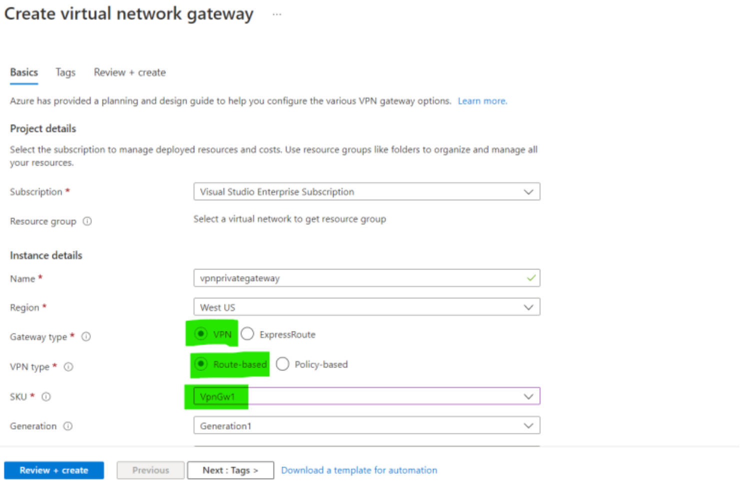
Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
adfunctionappprivatenetwork	A	3600	10.10.1.11	False
adprivatetworklogicapp	A	10	10.10.1.8	False
adfunctionappprivatenetwork.scm	A	3600	10.10.1.11	False
adprivatetworklogicapp.scm	A	10	10.10.1.8	False

Note: The creation of private endpoint process is same for all resources

Step 3: Setting up Point to Site VPN Connection:

Note: For implementing Azure AD based authentication for VPN gateway we need at least **VpnGw1** sku. For Client Certificate authentication basic sku is enough. Here, I'm going to setup Azure AD based authentication.

1. Create a VPN Gateway with the options mentioned and select the virtual network.


Create virtual network gateway

Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

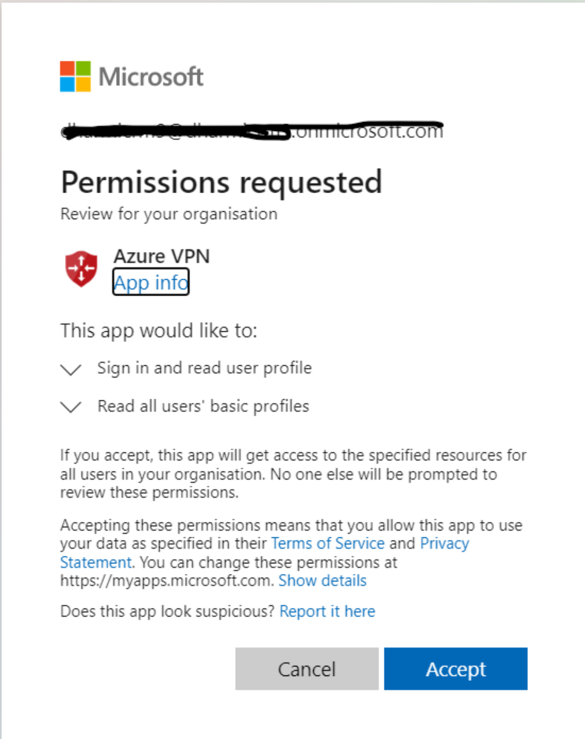
Subscription *	Visual Studio Enterprise Subscription
Resource group	Select a virtual network to get resource group

Instance details

Name *	vpnprivategateway
Region *	West US
Gateway type *	● VPN ○ ExpressRoute
VPN type *	● Route-based ○ Policy-based
SKU *	VpnGw1
Generation	Generation1

Step 4: Authorize the Azure VPN application

1. Login to Azure portal as Global Admin and open the link Azure VPN Application to give consent for installing the VPN Client App in your tenant.



[redacted].onmicrosoft.com

Permissions requested

Review for your organisation

Azure VPN

App info

This app would like to:

Sign in and read user profile

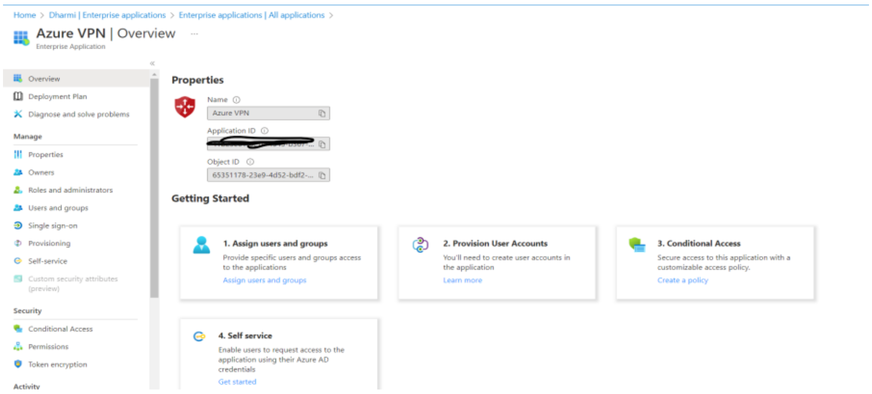
Read all users' basic profiles

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

2. Note the Application ID of Azure VPN application. Azure Portal -> Azure Active Directory -> Enterprise Application -> Azure VPN



Properties

Name: Azure VPN

Application ID: [redacted]

Object ID: 65351178-23e9-4d52-bdf2-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Provision User Accounts
You'll need to create user accounts in the application
Learn more

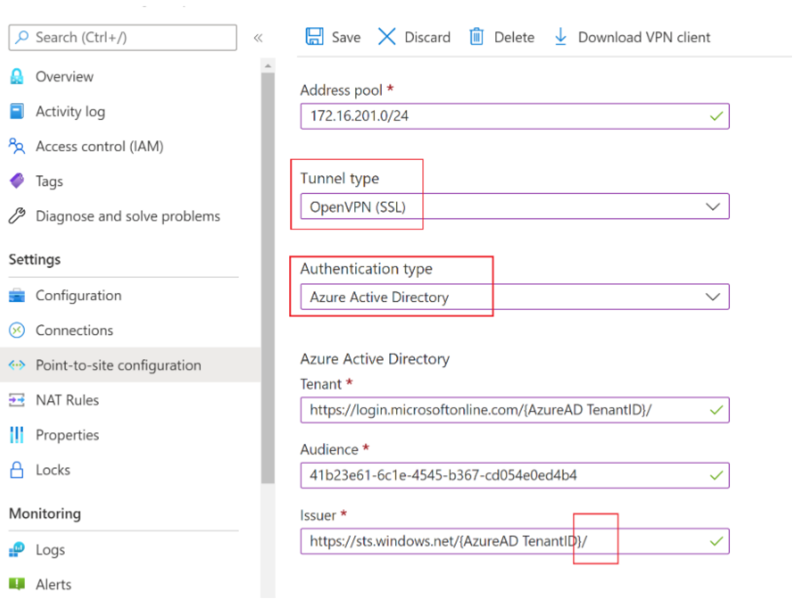
3. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

4. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

3. Also note the tenant ID from the overview page of azure active directory.

Step 5: Configure Azure AD Authentication in VPN Gateway

1. Go to Azure VPN Gateway you create and select Point-to-Site configuration and click configure now.
2. Give the IP address range for the address pool for the clients who will be connecting to this VPN gateway.
3. Select Tunnel type as OpenVPN(SSL) and Authentication type as Azure Active Directory.
4. In Tenant, replace AzureAD TenantID with your tenantID.
5. In Audience, replace with Application ID of VPN Client App.
6. In Issuer, replace with you tenantID for AzureAD TenantID



Address pool *
172.16.201.0/24

Tunnel type
OpenVPN (SSL)

Authentication type
Azure Active Directory

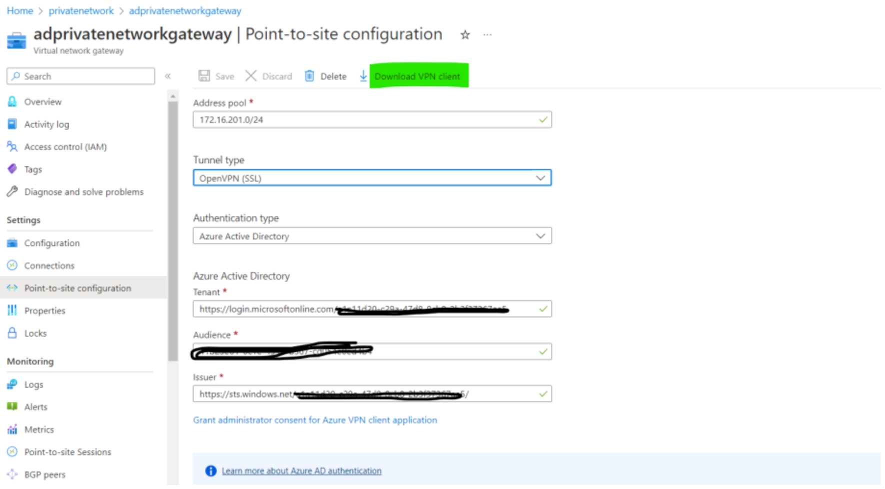
Azure Active Directory

Tenant *
https://login.microsoftonline.com/{AzureAD TenantID}/

Audience *
41b23e61-6c1e-4545-b367-cd054e0ed4b4

Issuer *
https://sts.windows.net/{AzureAD TenantID}/

7. Once all are done, click Download VPN Client at top.



Address pool *
172.16.201.0/24

Tunnel type
OpenVPN (SSL)

Authentication type
Azure Active Directory

Azure Active Directory

Tenant *
https://login.microsoftonline.com/[redacted]

Audience *
[redacted]

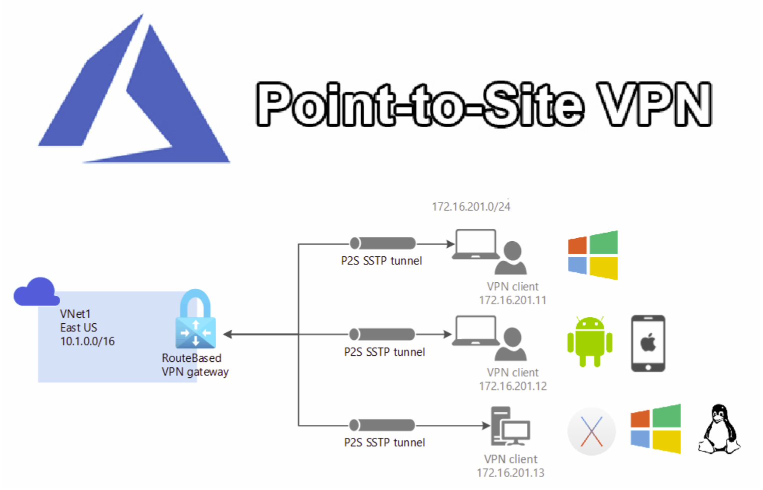
Issuer *
https://sts.windows.net/[redacted]/

Grant administrator consent for Azure VPN client application

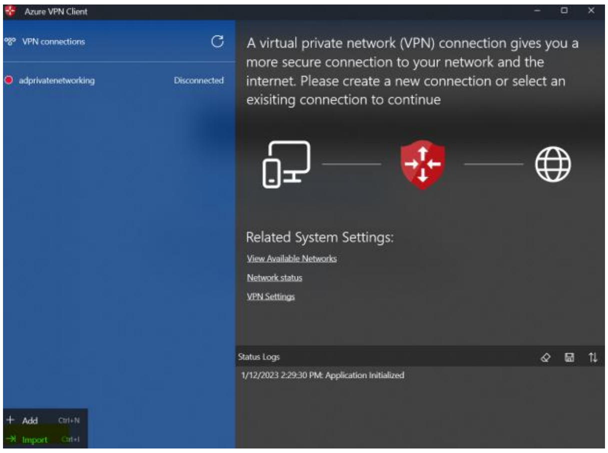
Learn more about Azure AD authentication

8. The downloaded zip file will have below two files. Inside Azure VPN folder vpn gateway config file will be available.

Step 6: Setting up VPN Client in Windows Desktop



1. Install Azure VPN Client from Microsoft app store.
2. Open Azure VPN Client and select import



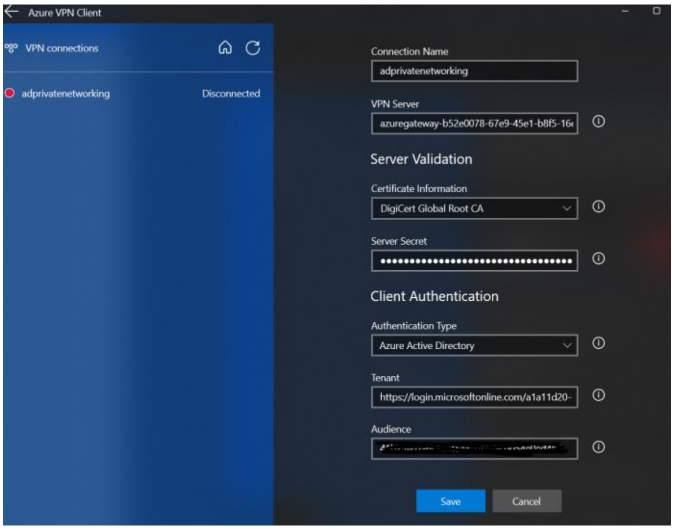
adprivatenetworking Disconnected

A virtual private network (VPN) connection gives you a more secure connection to your network and the internet. Please create a new connection or select an exisiting connection to continue

Related System Settings:
View Available Networks
Network status
VPN Settings

Status Logs
1/12/2023 2:29:30 PM: Application Initialized

3. Select the xml file which you have downloaded form previous step and save.



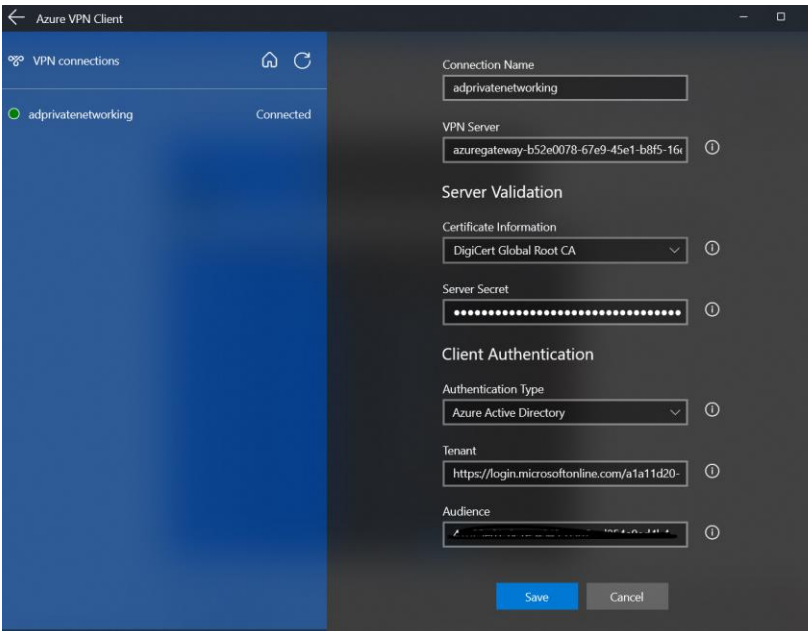
adprivatenetworking Disconnected

Connection Name: adprivatenetworking
VPN Server: azuregateway-b52e0078-67e9-45e1-b8f5-16(

Server Validation
Certificate Information: DigiCert Global Root CA
Server Secret: ••••••••••••••••••••••••••••••••

Client Authentication
Authentication Type: Azure Active Directory
Tenant: https://login.microsoftonline.com/a1a11d20-
Audience: [redacted]

4. Go to windows settings -> network and internet -> VPN Settings -> connect to your vpn. It will prompt for Azure Active Authentication.



adprivatenetworking Connected

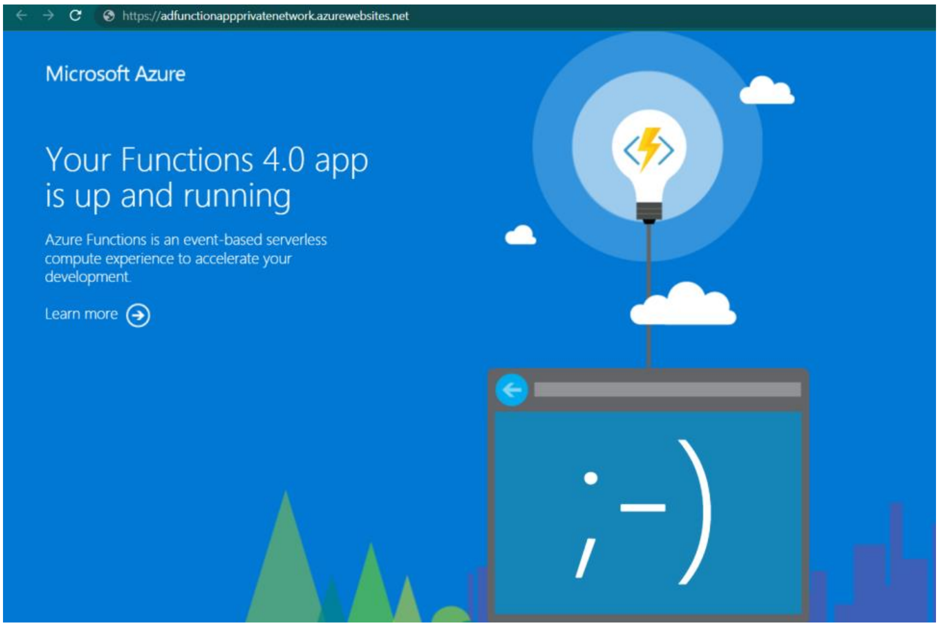
Connection Name: adprivatenetworking
VPN Server: azuregateway-b52e0078-67e9-45e1-b8f5-16(

Server Validation
Certificate Information: DigiCert Global Root CA
Server Secret: ••••••••••••••••••••••••••••••••

Client Authentication
Authentication Type: Azure Active Directory
Tenant: https://login.microsoftonline.com/a1a11d20-
Audience: [redacted]

.

5. After successful login you will be able to access the services.

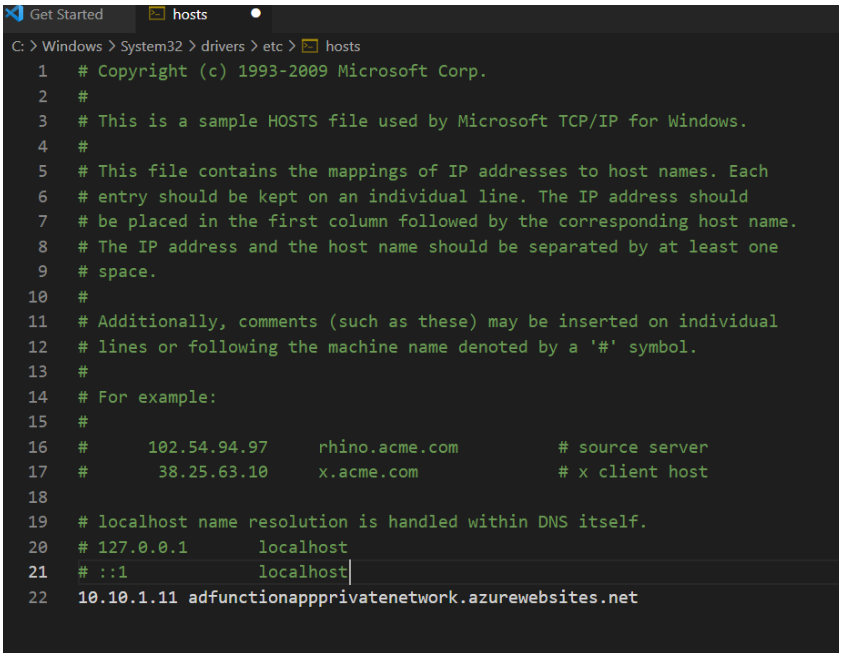


Your Functions 4.0 app is up and running

Azure Functions is an event-based serverless compute experience to accelerate your development.

Note: if it’s not working. Go to C:/windows/system32/drivers/etc/host file and add the Ip and domain as follow.

10.10.1.2(private ip) adfunctionappprivatenetwork.azurewebsites.net(domain).



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1             localhost
10.10.1.11 adfunctionappprivatenetwork.azurewebsites.net
```

Challenges in implementing the solution

1. Most of the resources don't support private endpoint in basic sku tier. Eg., Service Bus premium tier is too expensive in order to implement private networking.
2. As we are developing microservices architecture, we should ensure intercommunication between the resources also.

Business Benefit

1. Secure access to the Azure resources from certain Network.
2. Using Secure tunnel VPN Gateway for the clients who are not in the virtual network.
3. No need of whitelisting the IPs and Vnet Integration.
4. Private DNS zones will be created automatically for DNS resolution.

Best Practices/Bonus Points:

1. Always deploy your infrastructure and code changes separately.
2. Private Endpoint links limits Private Endpoint Limits
3. Use System managed or user assigned identity for inter-communication between the resources

References:

1. Sample Github Code for Microservice and infrastructure template: Github Code Sample Code
2. VPN using Azure AD Authentication: More Info - Azure Ad Authentication
3. VPN using Certificate Authentication: More Info - Certificate Authentication

Published by – Dharmeshwaran S

Linkedin
Github