TLS Proxy: Custom domain support for App Service using Application Gateway

Contents

Overview

This document describes the configuration of a Private Link-enabled Azure App Service fronted by Azure Application Gateway. It uses a custom domain like https://appservice.contoso.corp for client requests and yet ensures that requests for this App Service go through Application Gateway, which uses the default FQDN of that App Service in its backend.

Pre-requisites

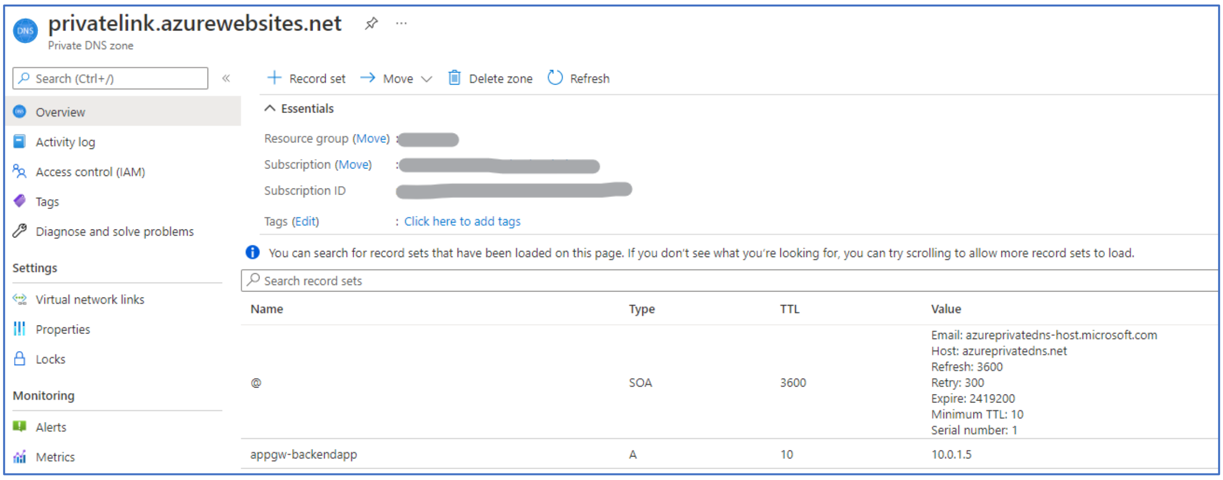
1. App Service Plan
2. Application Gateway using L7 capabilities (HTTP/HTTPS)

Solution

1. Create Web App in an App Service Plan. This can be accessed using its default FQDN from public internet.

2. Enable Private Link on the Web App. This creates Private DNS Zone linked to Application Gateway's virtual network and creates an A-Record pointing to Private IP of the Web App. Follow this documentation for more details.

   Here is how the DNS record for the private link should look:



privatelink.azurewebsites.net

Private DNS zone

Resource group (Move) : [redacted]

Subscription (Move) : [redacted]

Subscription ID [redacted]

Tags (Edit) : Click here to add tags

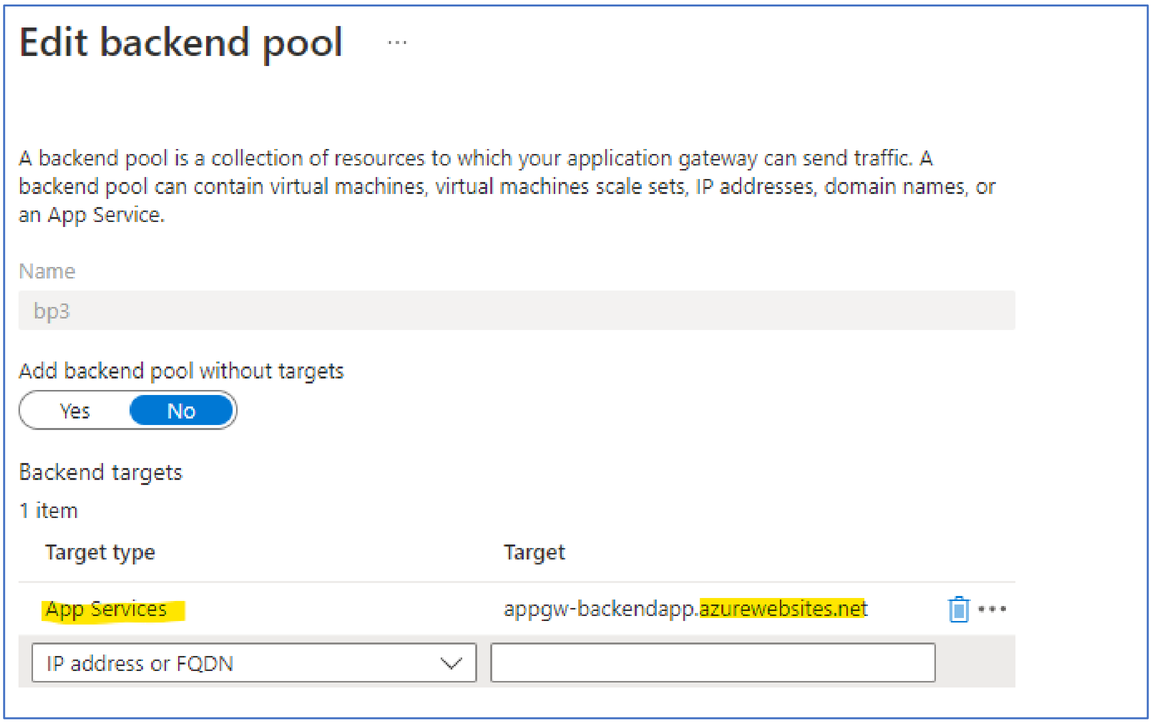
You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1
appgw-backendapp	A	10	10.0.1.5

3. Configuration guide for Application Gateway.

    a. Backend Target – Select “IP address or FQDN” to specify the default FQDN of the App Service.



Edit backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name

bp3

Add backend pool without targets

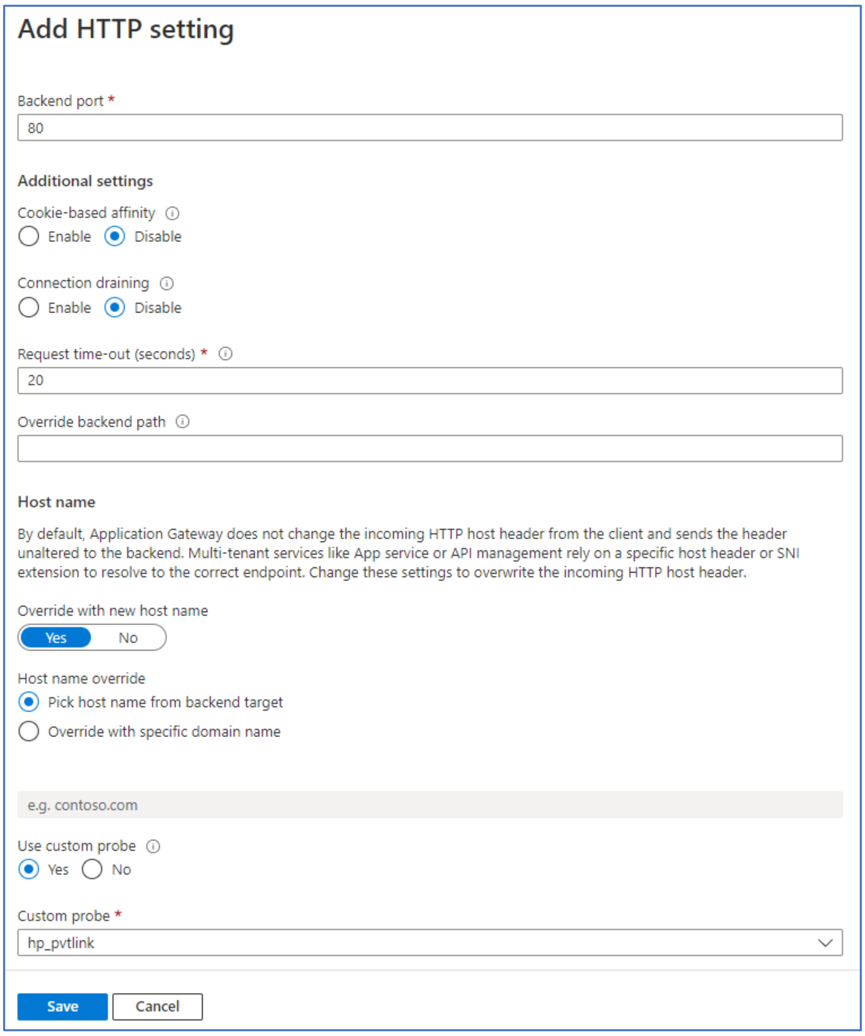
Yes [✓ No]

Backend targets

1 item

Target type	Target
App Services	appgw-backendapp.azurewebsites.net
IP address or FQDN	

b. For HTTP Settings:
App Service serves using HTTP by default on port 80 and using HTTPS on port 443. To enable HTTPS, the HTTP settings below need to be modified accordingly with “Use well known CA certificate” enabled.



Add HTTP setting

Backend port *

80

Additional settings

Cookie-based affinity ⓘ

○ Enable ● Disable

Connection draining ⓘ

○ Enable ● Disable

Request time-out (seconds) * ⓘ

20

Override backend path ⓘ

Host name

By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name

[✓ Yes] No

Host name override

● Pick host name from backend target

○ Override with specific domain name

e.g. contoso.com

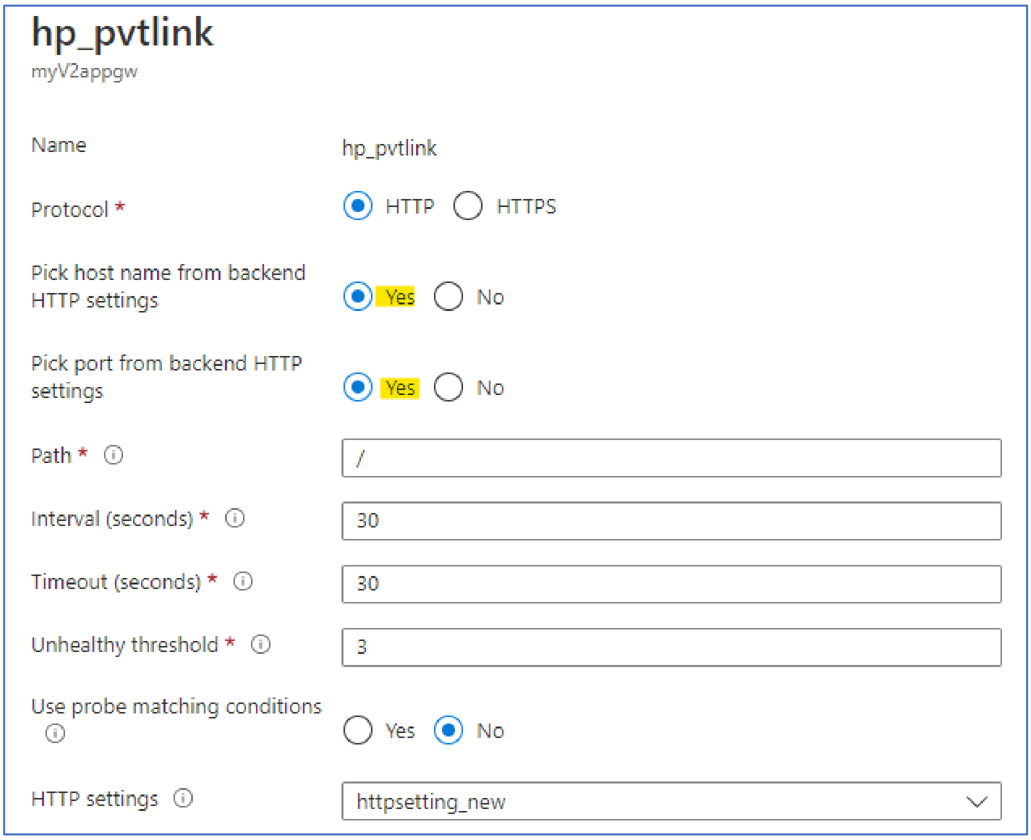
Use custom probe ⓘ

● Yes ○ No

Custom probe *

hp_pvtlink

c. (Optional) - Creating a Health probe,

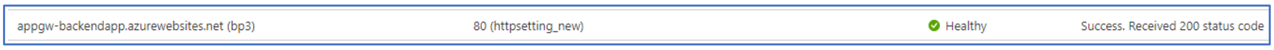


hp_pvtlink

myV2appgw

Name	hp_pvtlink
Protocol *	● HTTP ○ HTTPS
Pick host name from backend HTTP settings	● Yes ○ No
Pick port from backend HTTP settings	● Yes ○ No
Path * ⓘ	/
Interval (seconds) * ⓘ	30
Timeout (seconds) * ⓘ	30
Unhealthy threshold * ⓘ	3
Use probe matching conditions ⓘ	○ Yes ● No
HTTP settings ⓘ	httpsetting_new

4. You can verify the configuration by checking if the backend comes up as healthy.



appgw-backendapp.azurewebsites.net (bp3)	80 (httpsetting_new)	✓ Healthy	Success. Received 200 status code

Before we proceed, ensure the custom domain’s DNS resolves to Application Gateway IP.

5. Visit the custom domain URL from a browser client and verify that the Web App is reached.

Callouts/Caveats

1. Enabling Private Link on the App service through the Azure Portal automatically generates the required Private DNS zone, Virtual Network Link (to the Application gateway's Vnet) and A-record (pointing to private IP of App service). While configuring through Azure SDK client these resources can be created manually.

2. Due to current limitation with Application Gateway, any PaaS service's default FQDN should be added to the backend pool **after** configuring the private link, otherwise the default FQDN continues to point to its public IP. [ETA for this fix: Early 2022. As a workaround, you can even perform any PUT operation on gateway which will refresh its DNS.]

3. While configuring Private Link from clients other than portal, the subnet in which the endpoint would reside must have "privateLinkServiceNetworkPolicies" property disabled. More on this here.

4. App service expects its hostname to be passed in the host header of the request. Hence, it is essential to use "Host name override" in the HTTP setting. If default FQDN is used in the backend pool, hostname can be picked from the backend target itself.

5. This document assumes that the Listener is created with HTTPS protocol and an appropriate certificate.

ETA

Private Preview: 15 Feb, 2022

--End of File-----------------------------------