Azure Application Gateway Configuration v2s.0

Contents

1 Introduction

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers.

Application Gateway supports autoscaling, TLS offloading, and end-to-end TLS, a web application firewall (WAF), cookie-based session affinity, URL path-based routing, multisite hosting, and other features.

Application Gateway supports HTTP, HTTPS, HTTP/2, and WebSocket.

To this end, it is acknowledged that this is a living document, meant to reflect the design as new standards/changes come online within the environment.

1.1 Purpose

The purpose of this document is to provides a guide for configuring the Azure Application Gateway.

1.2 Audience

This document is for the infrastructure-specific architectural design as it relates to the SAP infrastructure on Azure Cloud. The target audience is intended to be Azure Technologists, BASIS Administrators and SAP Technical Architects. This document assumes a fundamental understanding of SAP Technical Architecture concepts. It may also be referenced by Equinor enterprise architects, infrastructure architects, security & compliance, and cybersecurity teams.

2 Support Matrix from SAP

The Azure Application Gateway is currently being used for SAP BusinessObjects Business Intelligence platform (Bobj) (SID: BIQ, BIP) and Fiori for S/4HANA On-Premise Edition (SID: FD2,FQ2,FIP).

SID	Frontend URL	Frontend IP	Backend IP	Backend Port
FD2	https://launchpad-dev.bhfworks.net	10.213.37.68	10.213.36.73	44380
FQ2	https://launchpad-qa.bhfworks.net	10.214.25.197	10.214.24.70	44380
BIQ	https://boe-qa.bhfworks.net/BOE/BI https://boe-qa.bhfworks.net/BOE/CMC	10.214.25.196	10.214.24.14 10.214.24.16	8443
BLQA	https://blqa.brighthousefinancial.com	52.165.218.52 10.214.25.202	10.214.24.70	44380
BLPROD	https://blprod.brighthousefinancial.com	20.65.122.178 10.213.33.75	10.213.34.82	44380
FIP	https://launchpad.bhfworks.net/	10.213.33.80	10.213.34.82 10.213.34.84	44380
BIP	https://boe.bhfworks.net/BOE/BI https://boe.bhfworks.net/BOE/CMC http://boe.bhfworks.net/BOE/BI	10.213.33.70	10.213.34.14 10.213.34.16 10.213.34.14 10.213.34.16	8443 8080

SID	LISTNERS	RULES	BACKEND POOL NAME	HTTP SETTINGS	HEALTH PROBES	REWRITES
FD2	Httpslistener01	Rule01	Backendpool	HTTP01	Healthprobe01	Rewrite01
FQ2	Https	Rule01	Backendpool01	HTTPS01	Healthprobe01	Rewrite01
BIQ	Listner443	Rule01	Backendpool01	HTTP01	Healthprobe01	NA
BLQA	Listner443	Rule01	Backendpool01	HTTP01	HEALTHPROBE01	Rewrite01
BLPROD	BLPROD-LISTENER-HTTPS	BLPROD-APPGW-RULE-01	BLPROD-APPGW-BACKENDPOOL-01	BLPROD-APPGW-HTTP01	BLPROD-APPGW-HEALTHPROBE-01	NA

FIP	FIP-LISTENER-HTTPS	FIP-APPGW-RULE-01	FIP-APPGW-BACKENDPOOL-01	FIP-APPGW-HTTP-01	FIP-APPGW-HEALTHPROBE-01	FIP-APPGW-REWRITE-01
BIP	BIP-LISTENER-HTTPS	BIP-APPGW-RULE-01	BIP-APPGW-BACKENDPOOL-01	BIP-APPGW-HTTP-01	BIP-APPGW-HEALTHPROBE-01	NA
	BIP-LISTENER-HTTP	BIP-APPGW-RULE-01		BIP-APPGW-HTTP-02	BIP-APPGW-HEALTHPROBE-01	NA

3 Prerequisites for installation

1. Public and Private IP addresses
2. SSL Certificates (.pfx is required)
3. App Gateway's subnet

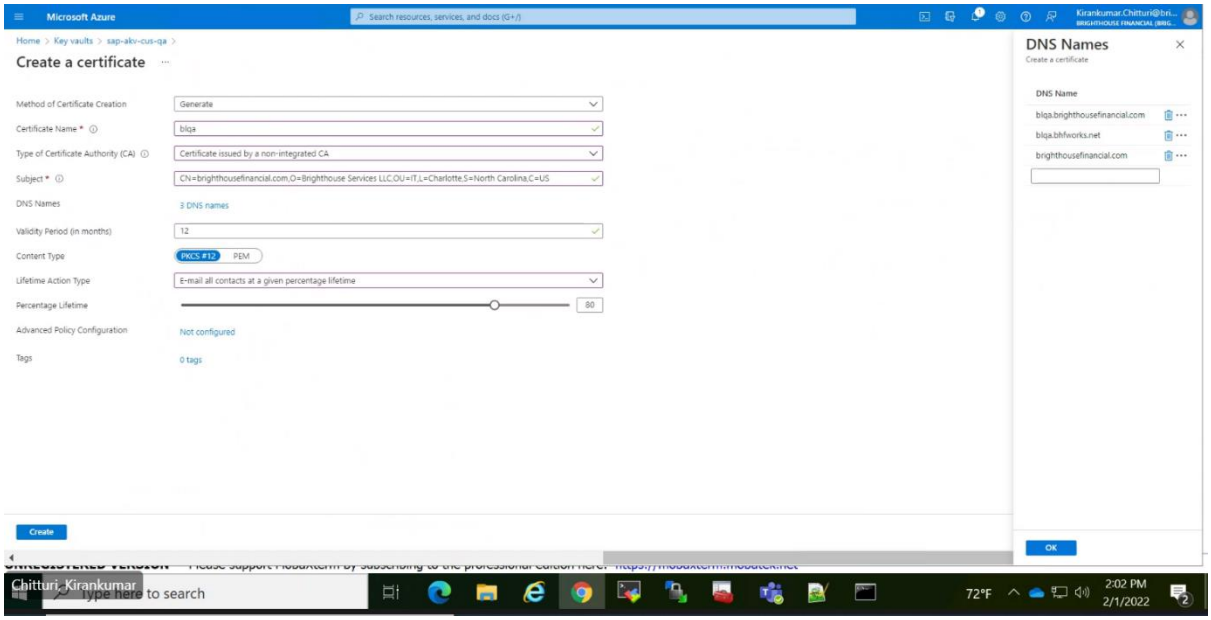
4 Create and merge a certificate signing request in Key Vault

This was used only for configuring BLQA and BLPROD

Azure Key Vault supports storing digital certificates issued by any certificate authority (CA). It supports creating a certificate signing request (CSR) with a private/public key pair. The CSR can be signed by any CA (an internal enterprise CA or an external public CA). A certificate signing request (CSR) is a message that you send to a CA in order to request a digital certificate.

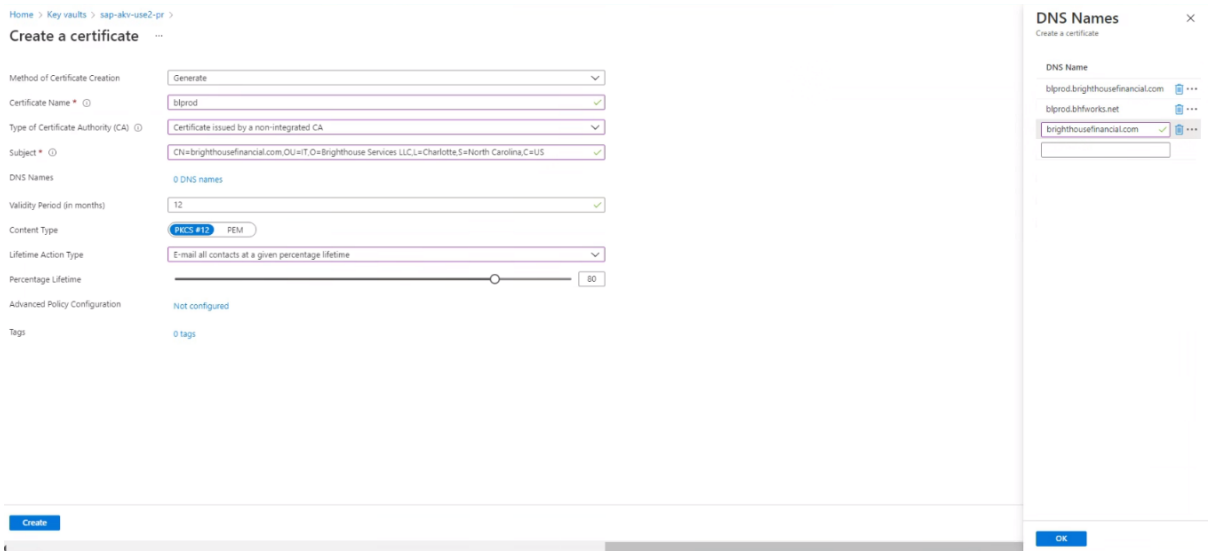
Follow these steps to add a certificate

1. Go to the key vault that you want to add the certificate to.
2. On the properties page, select Certificates.
3. Select the Generate/Import tab.
4. On the Create a certificate screen, choose the following values:
    a. For **BLQA**
        - **Method of Certificate Creation:** Generate
        - **Certificate Name**:blqa
        - **Type of Certificate Authority (CA):** Certificate issued by a non-integrated CA.
        - **Subject**: CN=brighthousefinancial.com,O=Brighthouse Services LLC, OU=IT, L=Charlotte,S=North Carolina,C=US



b. For **BLPROD**

- **Method of Certificate Creation:** Generate
- **Certificate Name**:blqa
- **Type of Certificate Authority (CA):** Certificate issued by a non-integrated CA.
- **Subject**: CN=brighthousefinancial.com,O=Brighthouse Services LLC, OU=IT, L=Charlotte,S=North Carolina,C=US



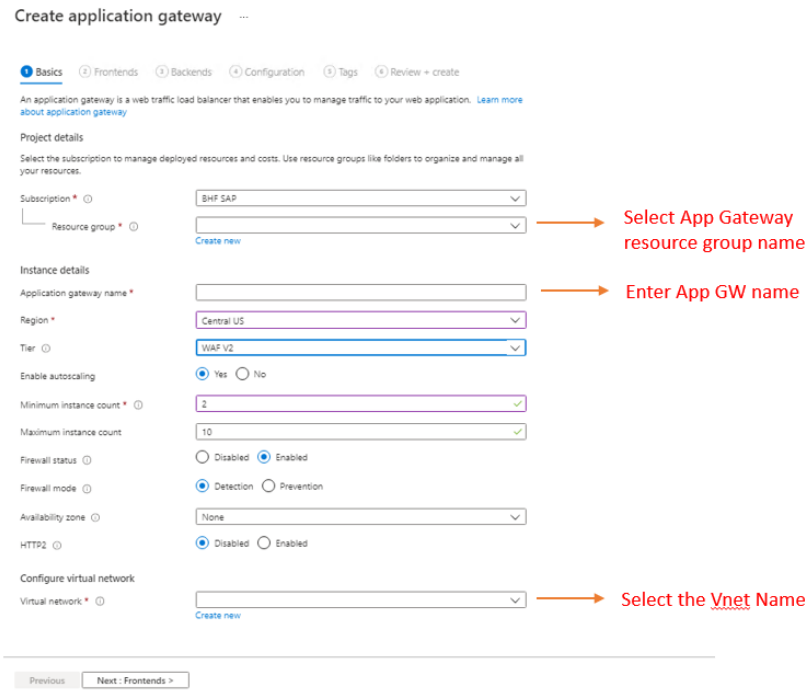
5. Select the other values as desired, and then select Create to add the certificate to the **Certificates** list.
6. In the Certificates list, select the new certificate. The current state of the certificate is disabled because it hasn't been issued by the CA yet.
7. On the Certificate Operation tab, select Download CSR.
8. Share the CSR file to BHF and have them sign the CSR (.csr).
9. After the request is signed, select Merge Signed Request on the Certificate Operation tab to add the signed certificate to Key Vault.

5 Configuring App Gateway

Configuring Application gateway consists of 6 steps

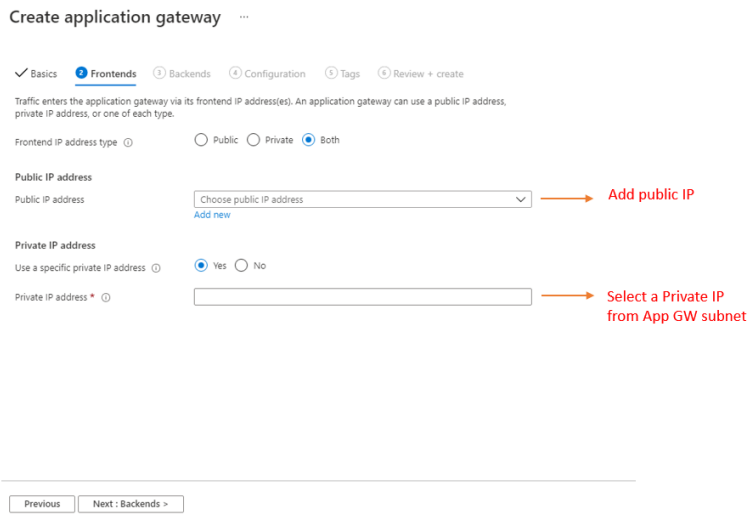
5.1 Basics

Update all the fields as per the requirements



5.2 Frontends

A frontend IP address is the IP address associated with an application gateway. You can configure an application gateway to have a public IP address, a private IP address, or both. An application gateway supports one public or one private IP address.

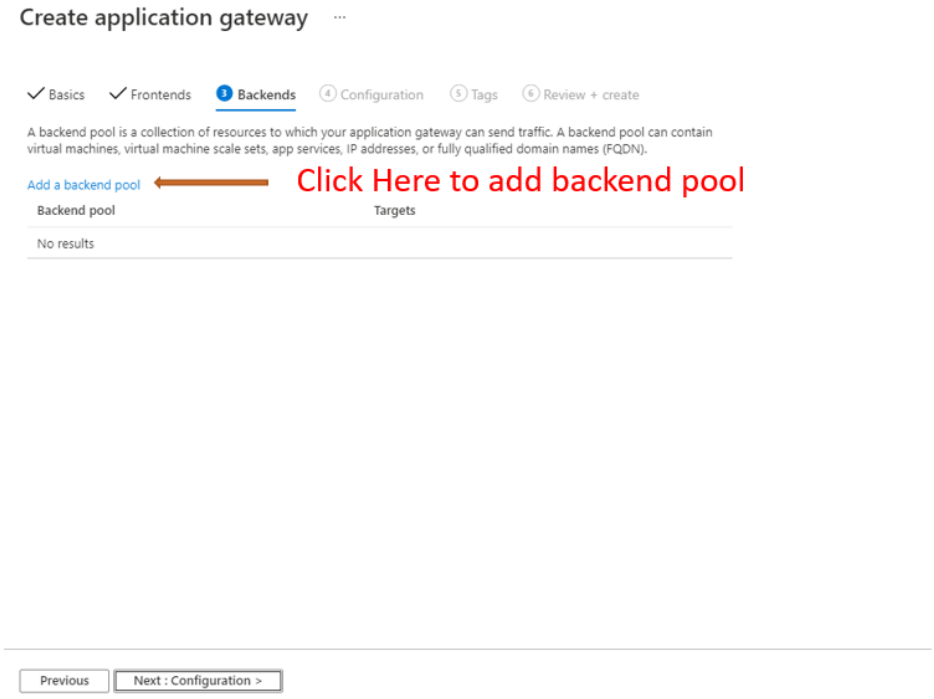


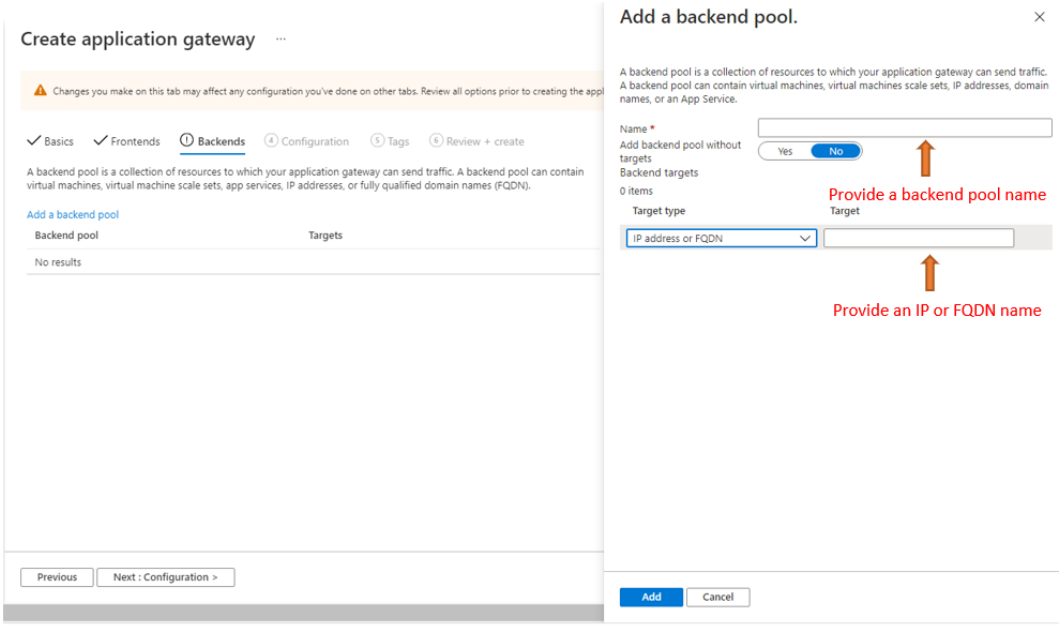
5.3 Backends

A backend pool routes request to backend servers, which serve the request. Backend pools can contain:

- NICs
- Virtual machine scale sets
- Public IP addresses
- Internal IP addresses
- FQDN
- Multitenant backends (such as App Service)

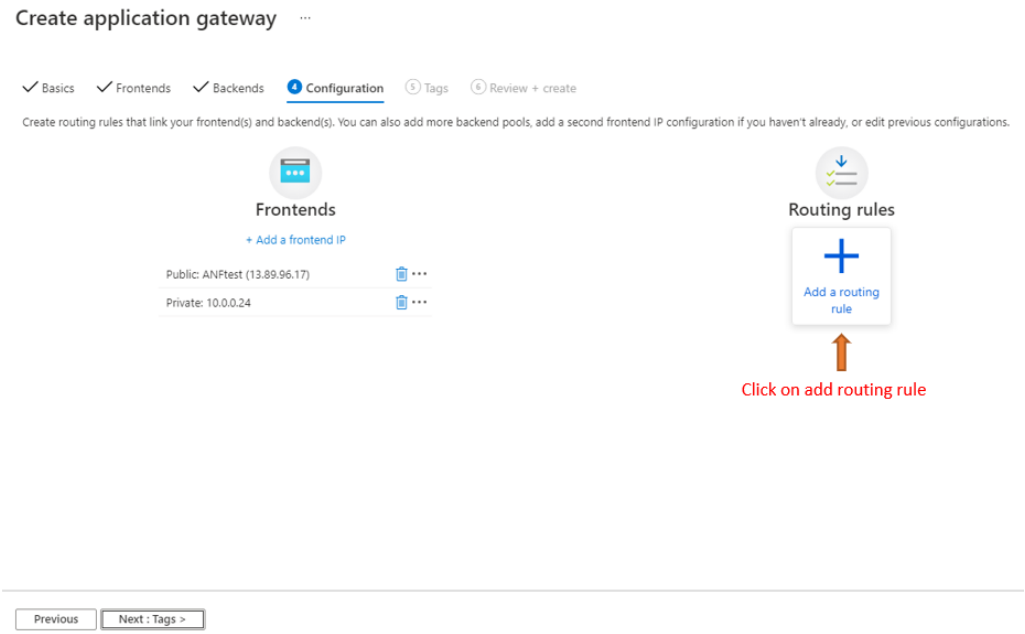
Application Gateway backend pool members aren't tied to an availability set. An application gateway can communicate with instances outside of the virtual network that it's in. As a result, the members of the backend pools can be across clusters, across datacenters, or outside Azure, as long as there's IP connectivity.





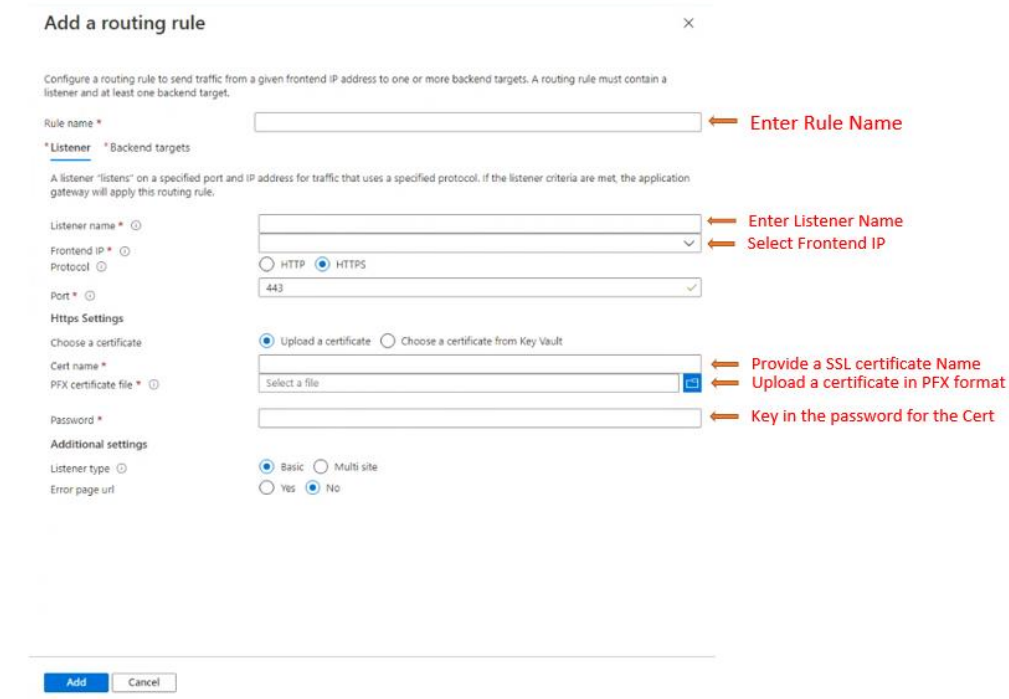
5.4 Configuration

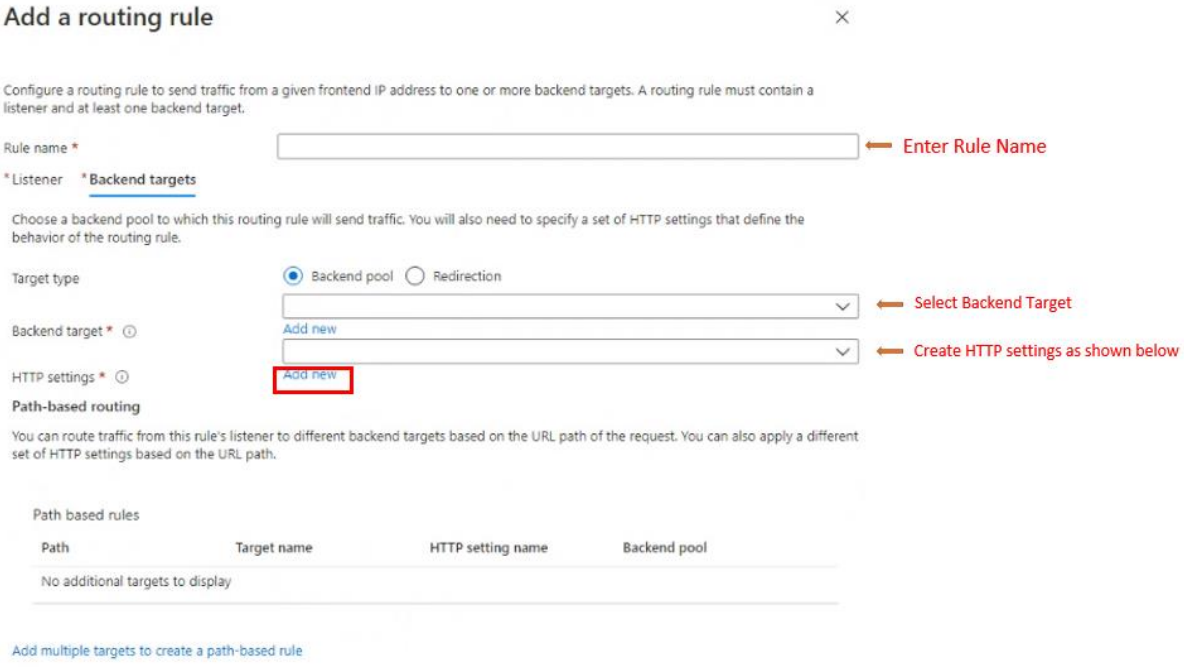
Request routing rules: A request routing rule is a key component of an application gateway because it determines how to route traffic on the listener. The rule binds the listener, the back-end server pool, and the backend HTTP settings.

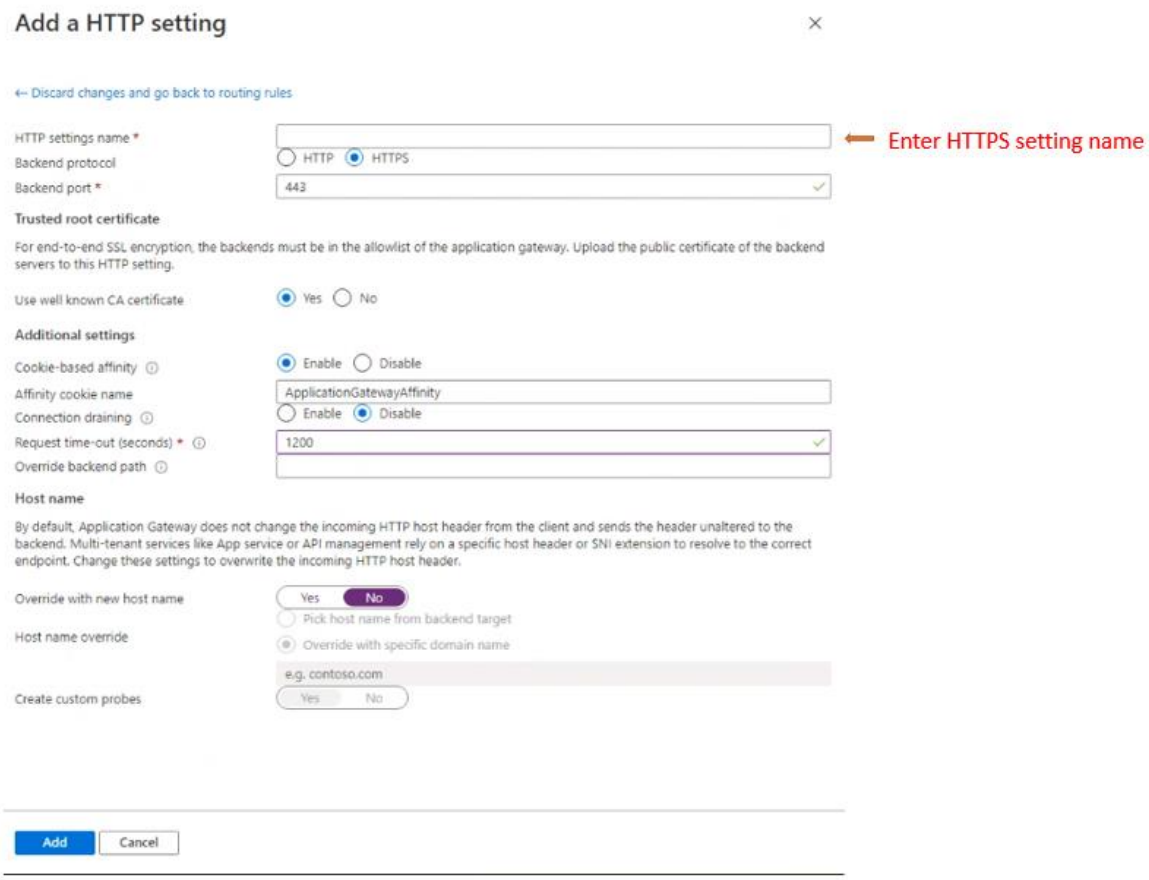


Listener Configuration

A listener is a logical entity that checks for incoming connection requests. A listener accepts a request if the protocol, port, hostname, and IP address associated with the request match the same elements associated with the listener configuration.


Add a routing rule
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name *
Enter Rule Name
*Listener *Backend targets
A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.
Listener name *
Enter Listener Name
Frontend IP *
Select Frontend IP
Protocol
HTTP HTTPS
Port *
443
Https Settings
Choose a certificate
Upload a certificate Choose a certificate from Key Vault
Cert name *
Provide a SSL certificate Name
PFX certificate file *
Select a file
Upload a certificate in PFX format
Password *
Key in the password for the Cert
Additional settings
Listener type
Basic Multi site
Error page url
Yes No
Add
Cancel


Add a routing rule
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name *
Enter Rule Name
*Listener *Backend targets
Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.
Target type
Backend pool Redirection
Backend target *
Add new
Select Backend Target
HTTP settings *
Add new
Create HTTP settings as shown below
Path-based routing
You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.
Path based rules
Path
Target name
HTTP setting name
Backend pool
No additional targets to display
Add multiple targets to create a path-based rule



5.5 Tags

Provide the relevant tags as per the requirement.

5.6 Review + create

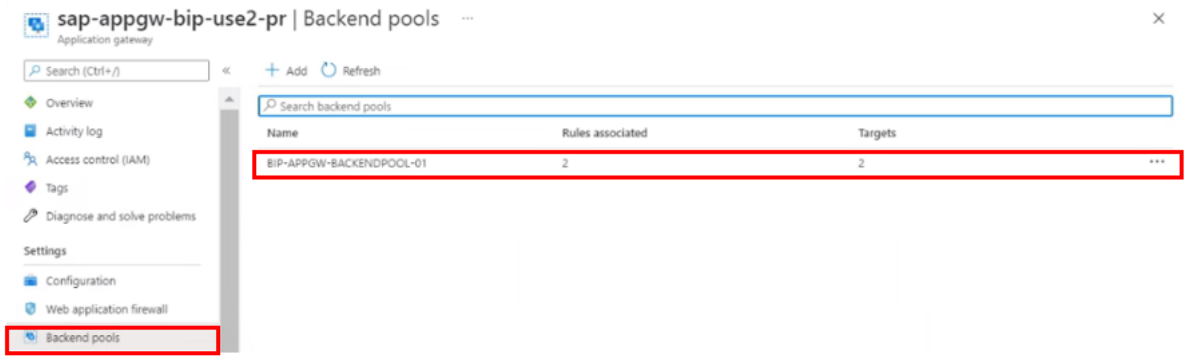
Review all the fields and create the application gateway.

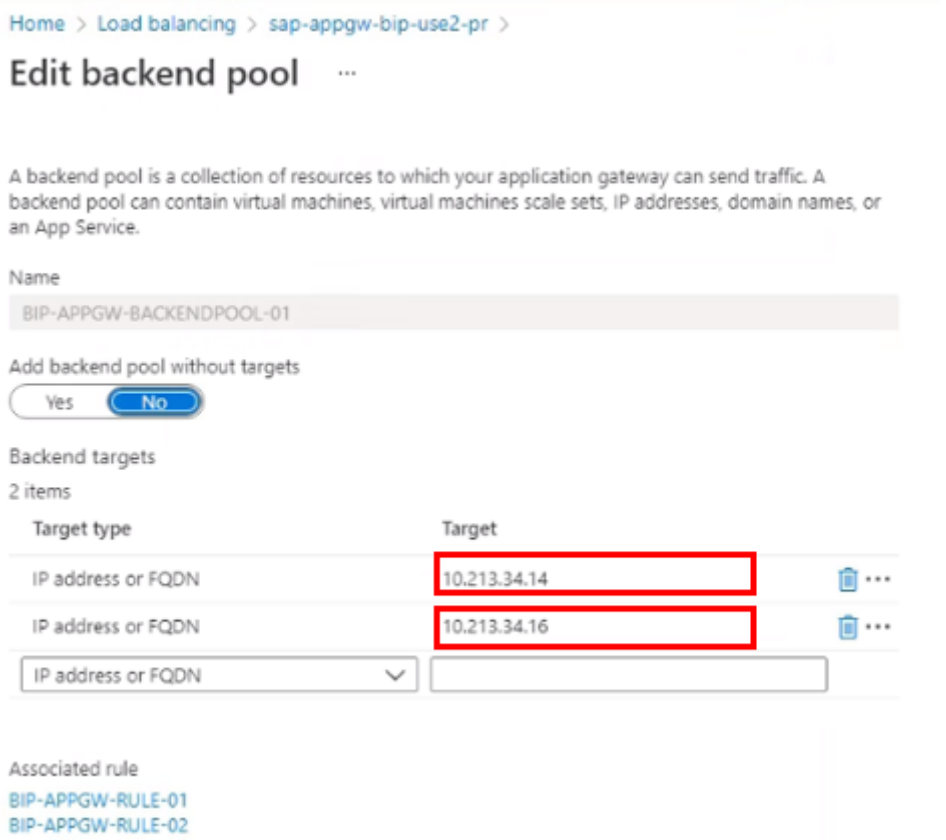
6 Additional Configuration Changes

For SAP BusinessObjects Business Intelligence platform (Bobj) (SID: BIP, BIQ)

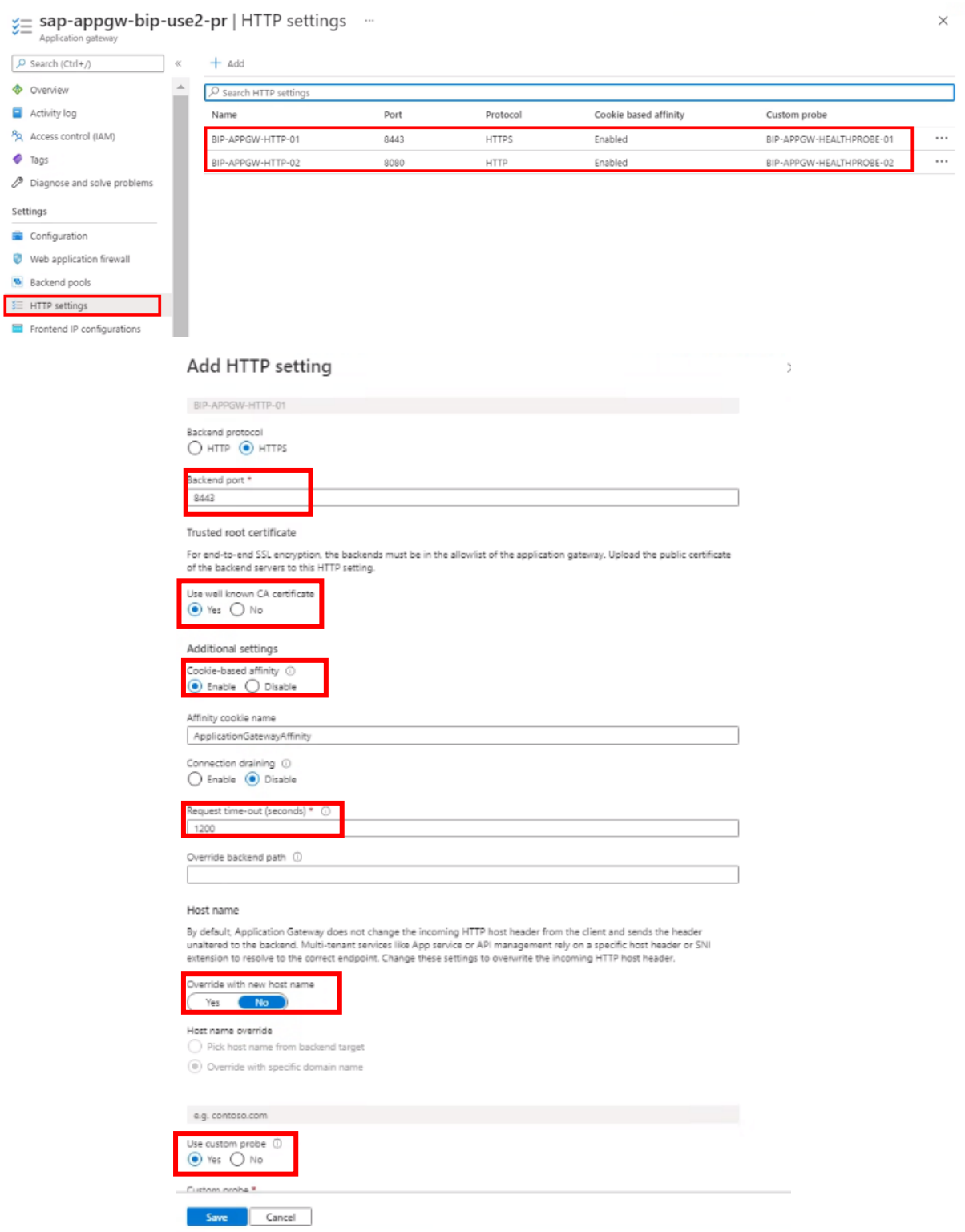
5.1. BIP Configuration

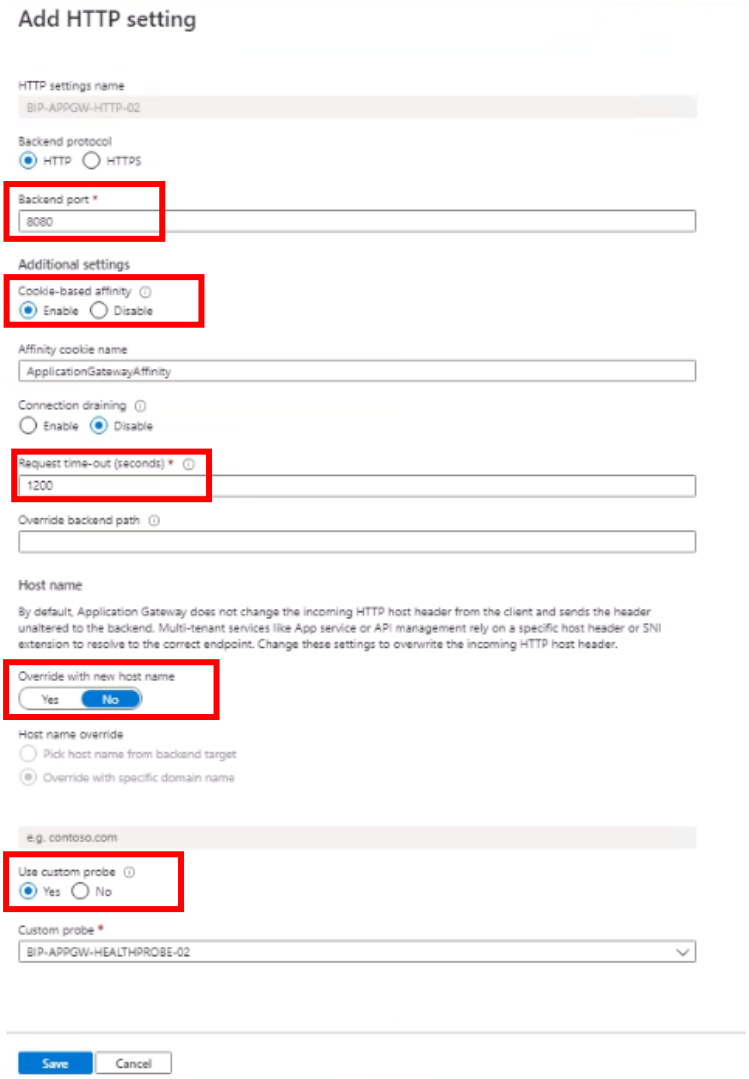
5.1.1. Backend Pool



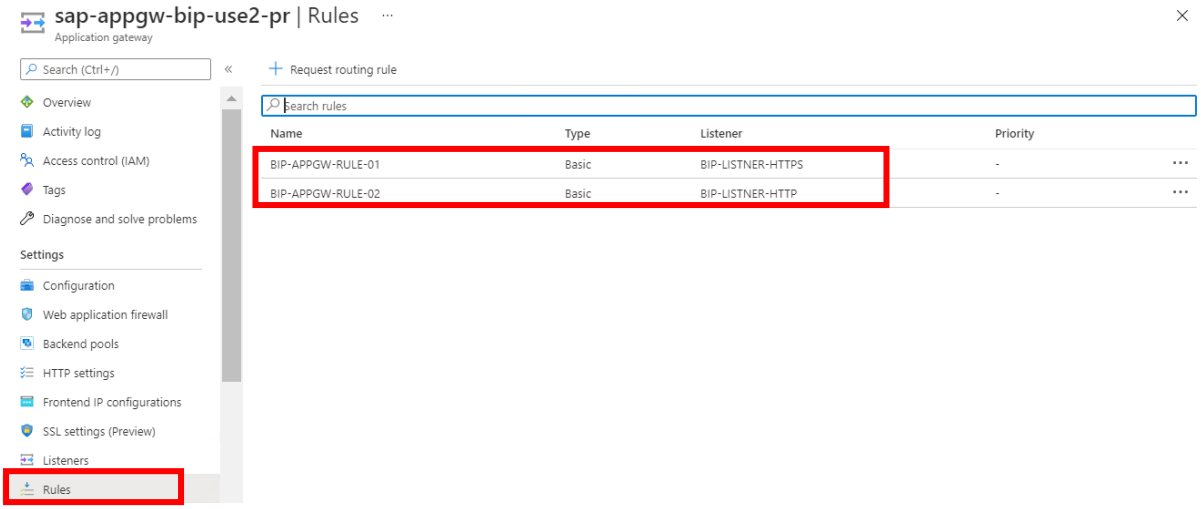


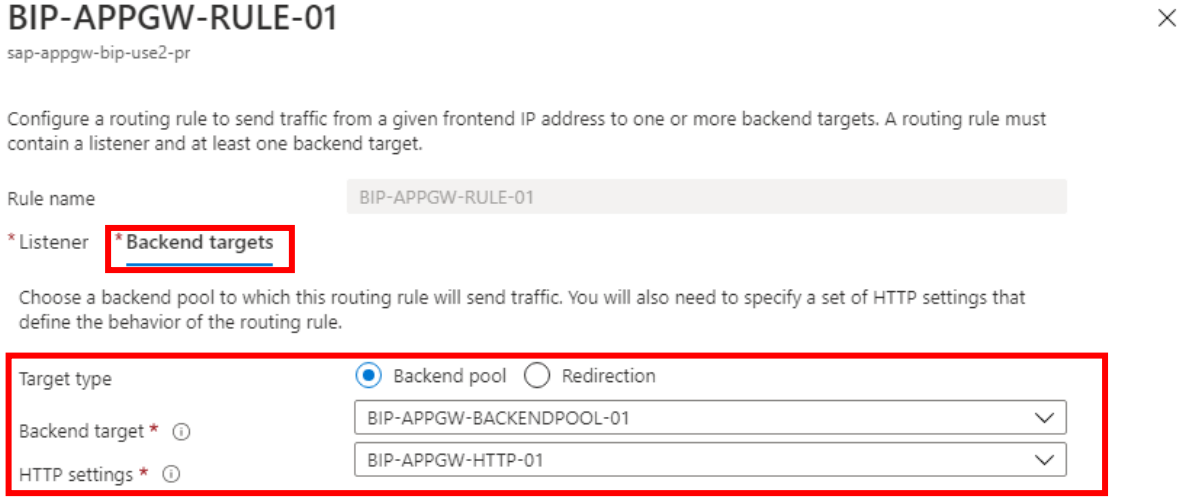
5.1.2. Backend Pool



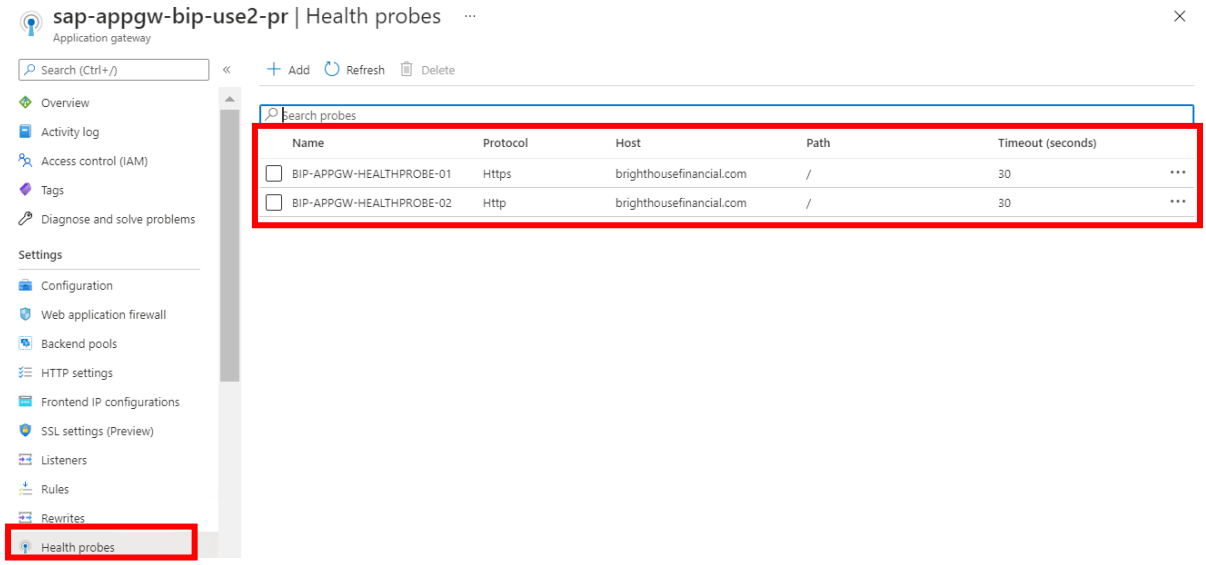

Add HTTP setting
HTTP settings name
BIP-APPGW-HTTP-02
Backend protocol
HTTP
HTTPS
Backend port *
8080
Additional settings
Cookie-based affinity
Enable
Disable
Affinity cookie name
ApplicationGatewayAffinity
Connection draining
Enable
Disable
Request time-out (seconds) *
1200
Override backend path
Host 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 *
BIP-APPGW-HEALTHPROBE-02
Save
Cancel

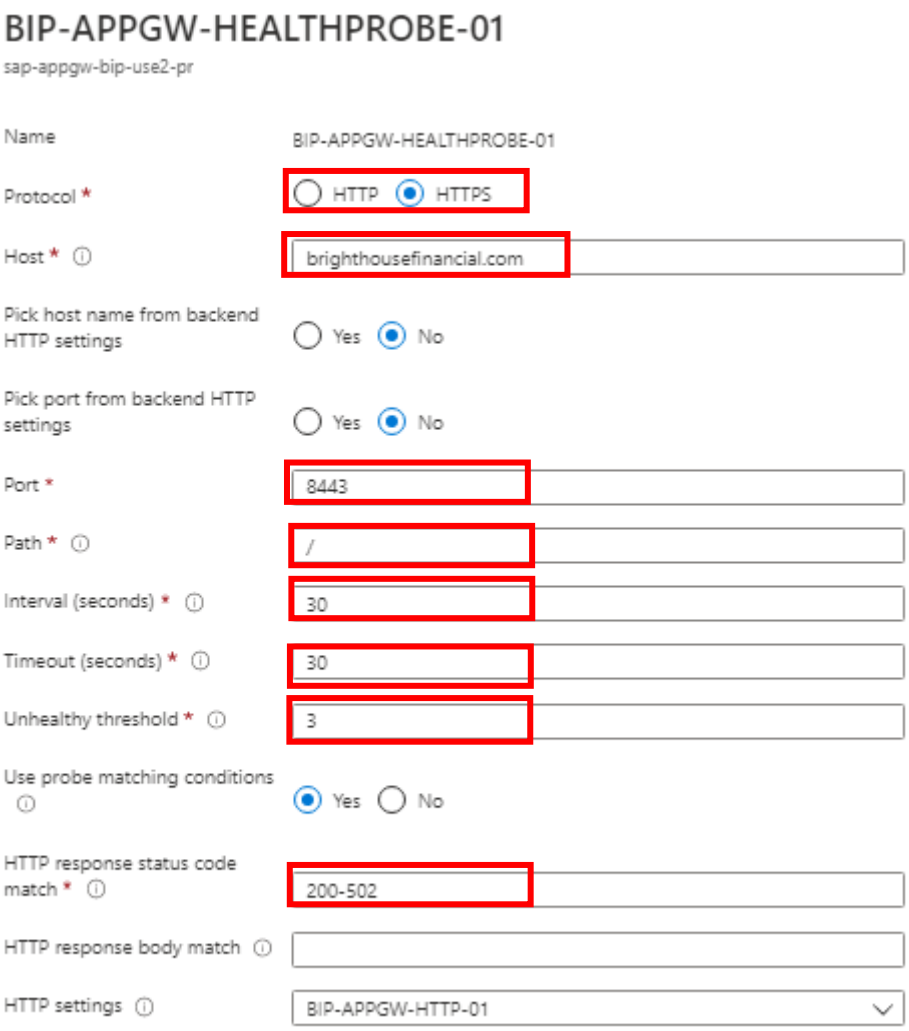
5.1.3. Rules

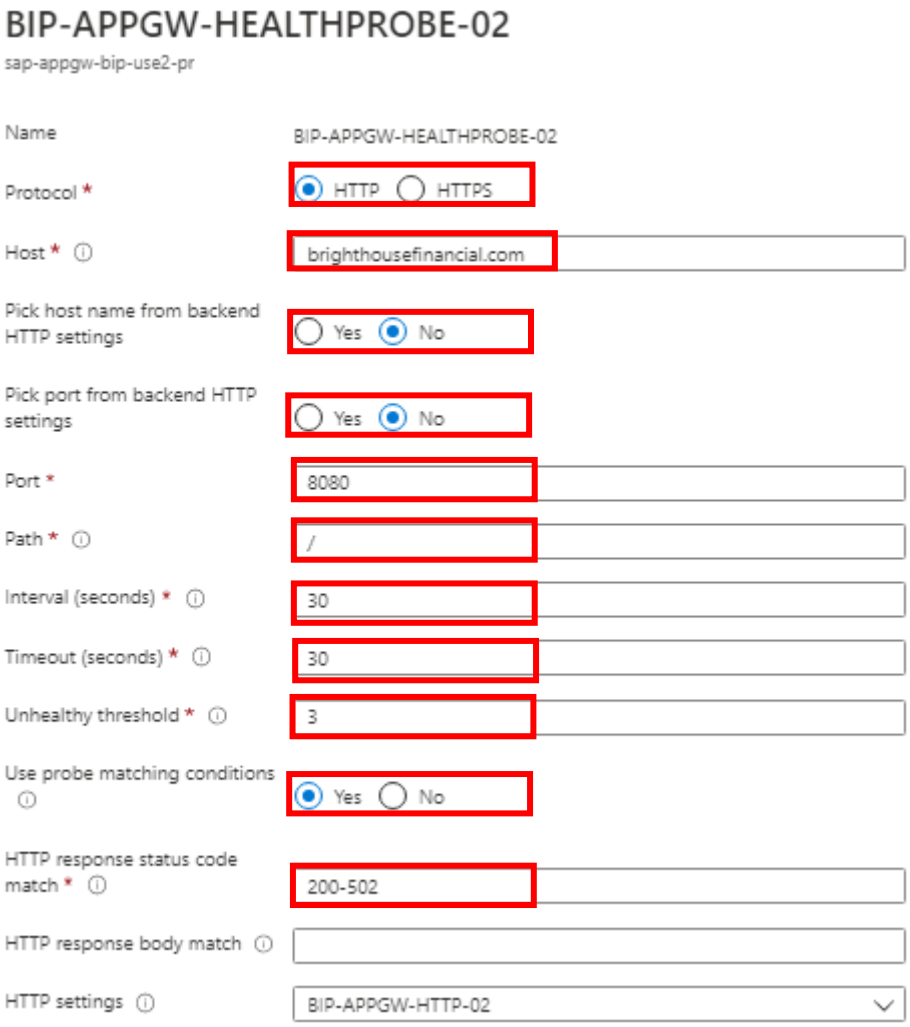

sap-appgw-bip-use2-pr | Rules
Application gateway
Search (Ctrl+/)
Request routing rule
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
HTTP settings
Frontend IP configurations
SSL settings (Preview)
Listeners
Rules
Search rules
Name
Type
Listener
Priority
BIP-APPGW-RULE-01
Basic
BIP-LISTNER-HTTPS
BIP-APPGW-RULE-02
Basic
BIP-LISTNER-HTTP



5.1.4. Health Probe



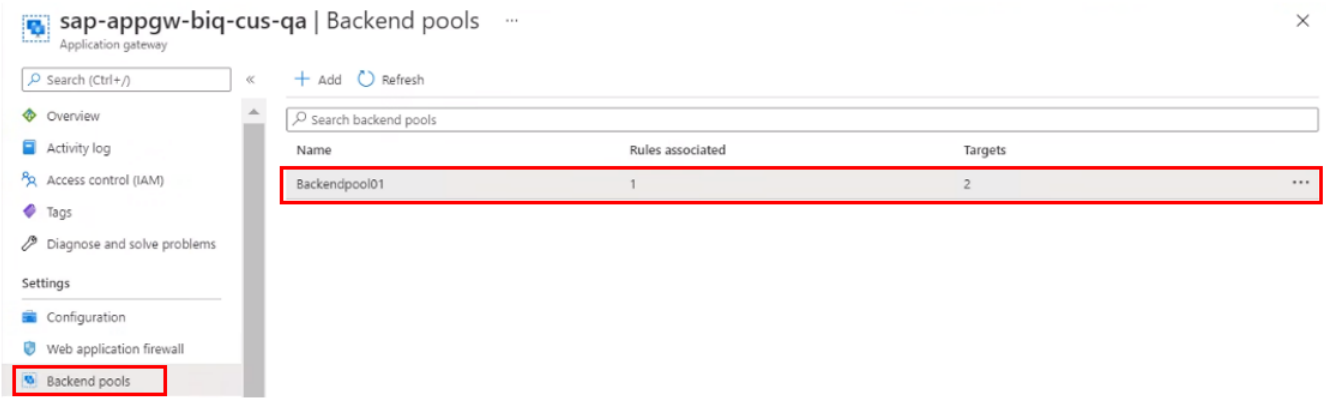

BIP-APPGW-HEALTHPROBE-01
sap-appgw-bip-use2-pr
Name
BIP-APPGW-HEALTHPROBE-01
Protocol *
HTTP
HTTPS
Host *
brighthousefinancial.com
Pick host name from backend HTTP settings
Yes
No
Pick port from backend HTTP settings
Yes
No
Port *
8443
Path *
/
Interval (seconds) *
30
Timeout (seconds) *
30
Unhealthy threshold *
3
Use probe matching conditions
Yes
No
HTTP response status code match *
200-502
HTTP response body match
HTTP settings
BIP-APPGW-HTTP-01

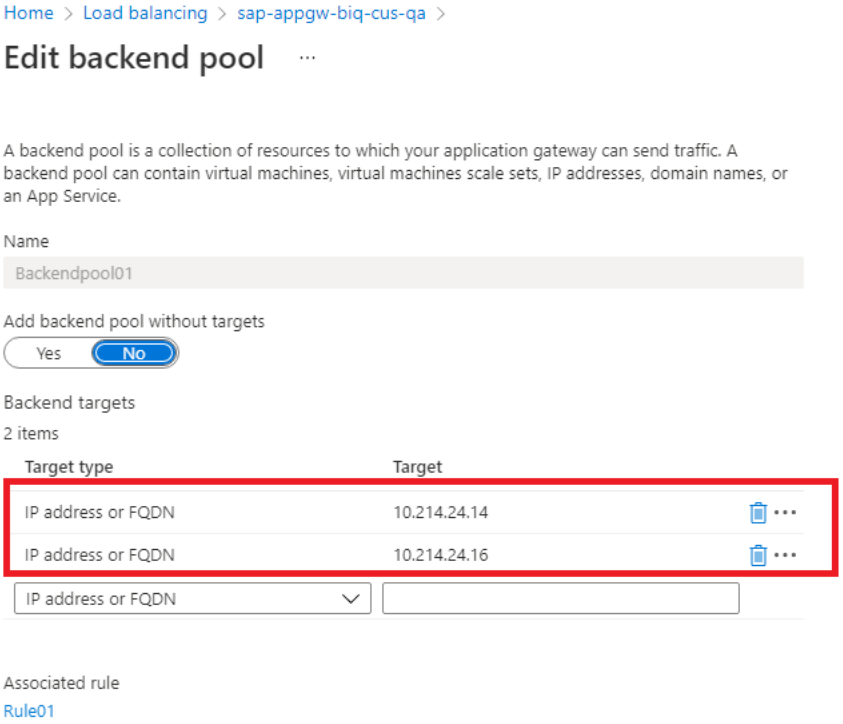


5.2. BIQ Configuration

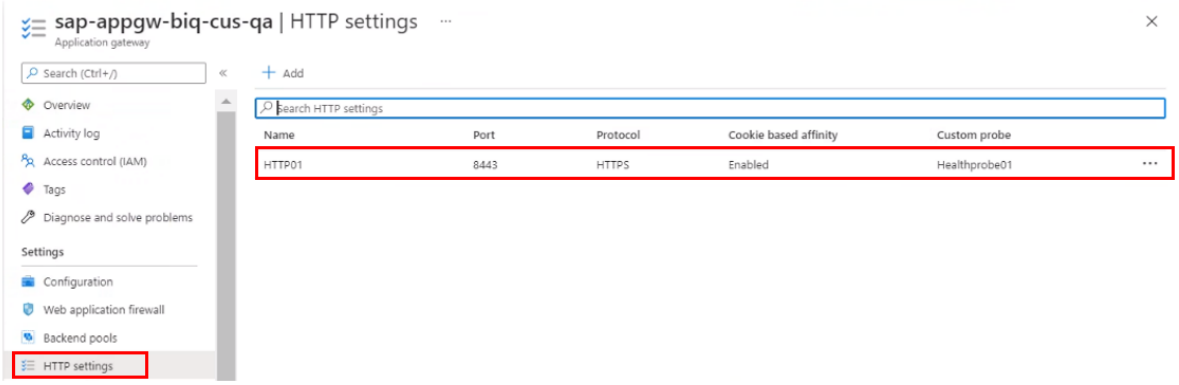
Verify the settings below and modify and accordingly

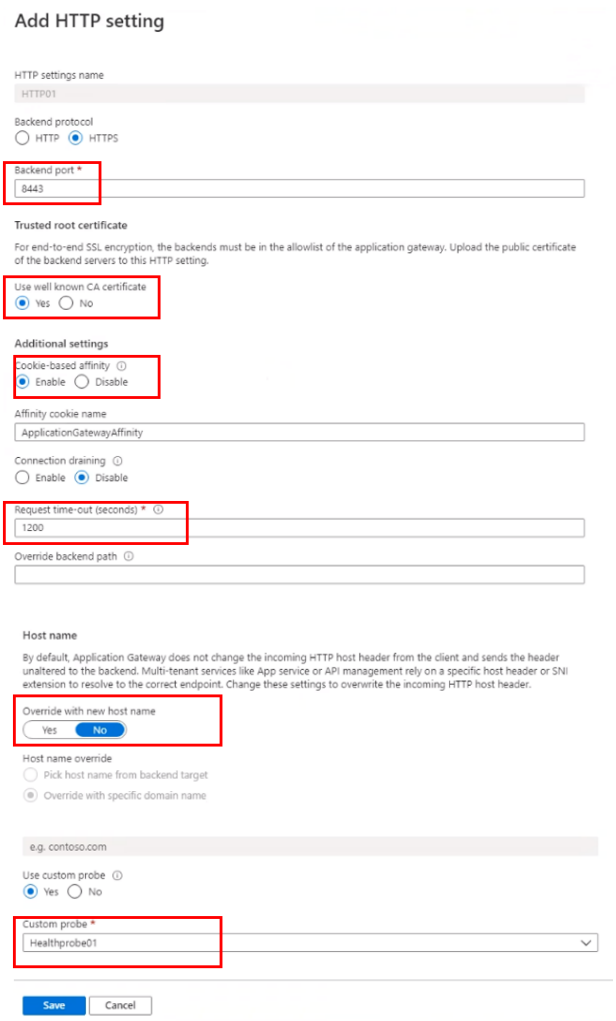
5.2.1. Backend Pool



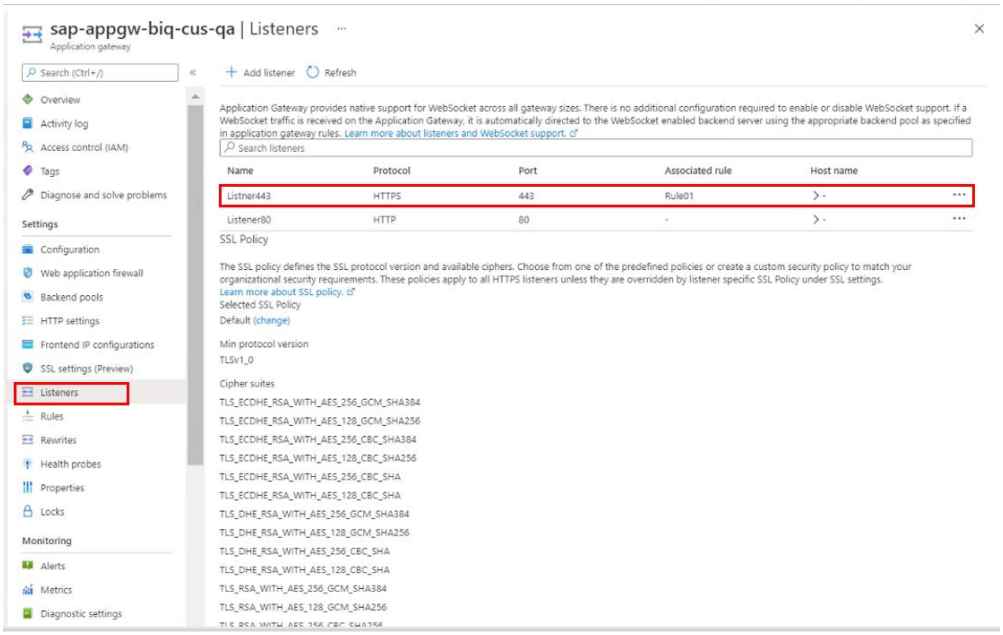


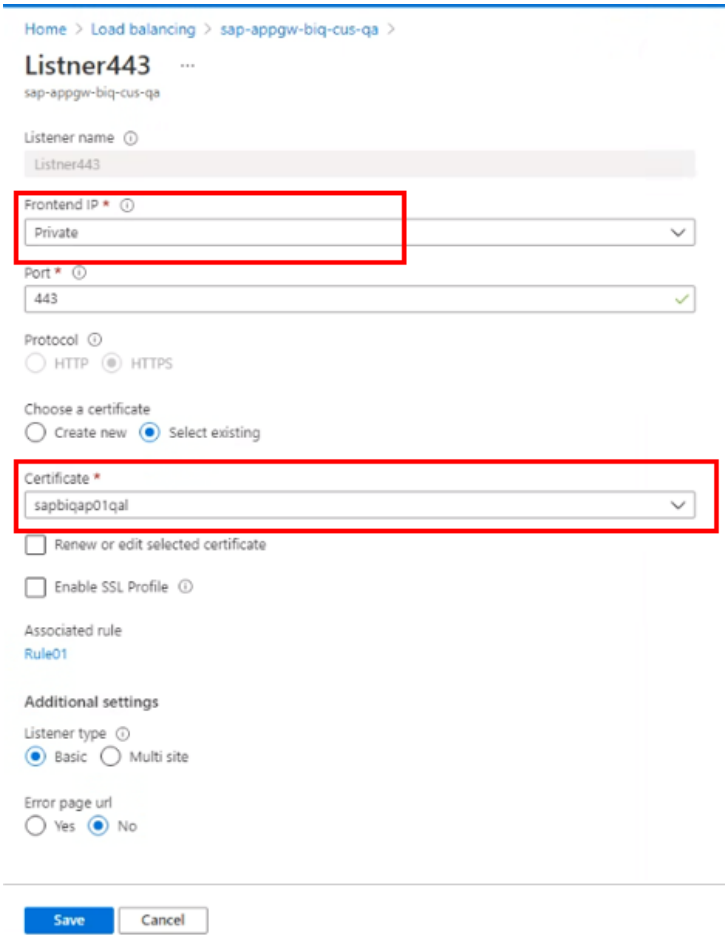
5.2.2. HTTP Settings



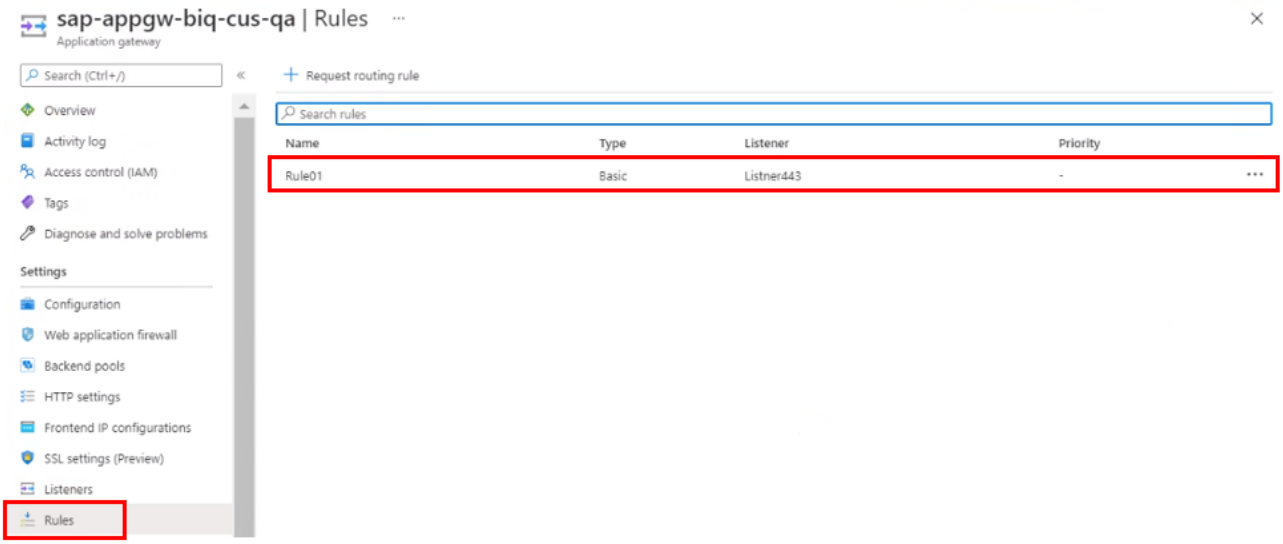

Add HTTP setting
HTTP settings name
HTTP01
Backend protocol
HTTP
HTTPS
Backend port *
8443
Trusted root certificate
For end-to-end SSL encryption, the backends must be in the allowlist of the application gateway. Upload the public certificate of the backend servers to this HTTP setting.
Use well known CA certificate
Yes
No
Additional settings
Cookie-based affinity
Enable
Disable
Affinity cookie name
ApplicationGatewayAffinity
Connection draining
Enable
Disable
Request time-out (seconds) *
1200
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 *
Healthprobe01
Save
Cancel

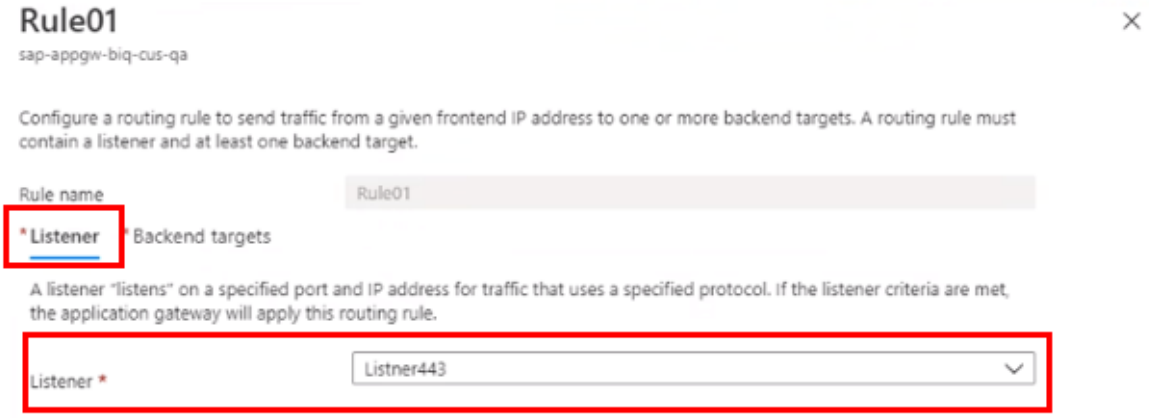
5.2.3. Listener Settings Rules

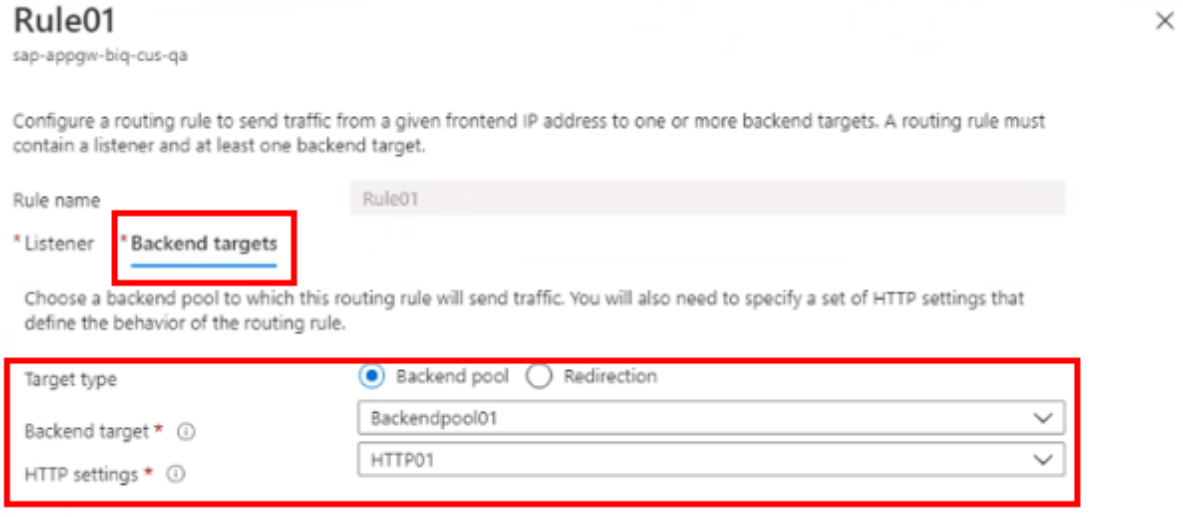




5.2.4. Rules

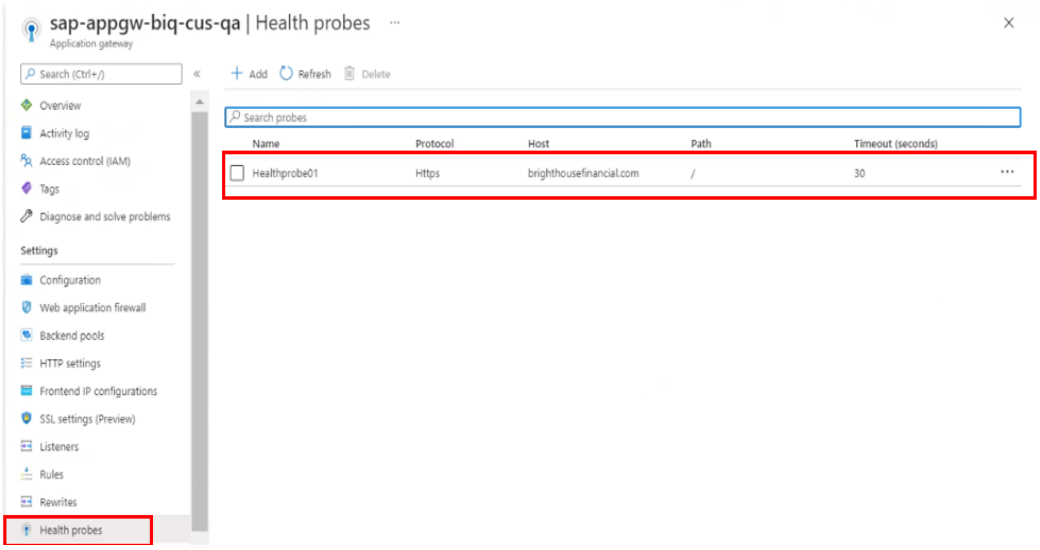

sap-appgw-biq-cus-qa | Rules
Application gateway
Search (Ctrl+/)
Request routing rule
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
HTTP settings
Frontend IP configurations
SSL settings (Preview)
Listeners
Rules
Search rules
Name
Type
Listener
Priority
Rule01
Basic
Listner443
-

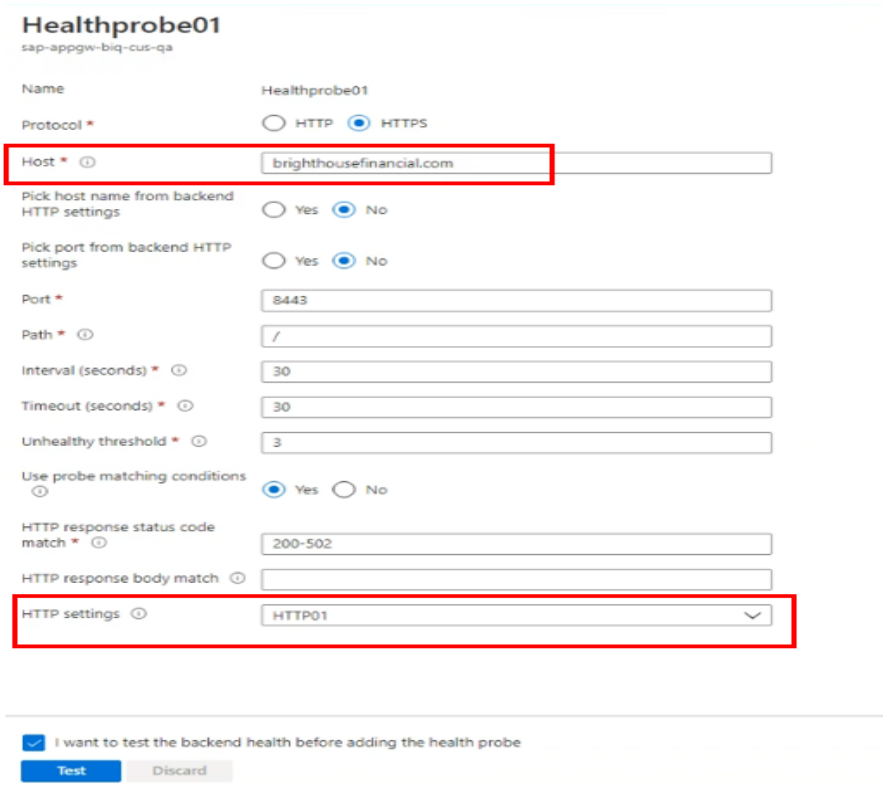

Rule01
sap-appgw-biq-cus-qa
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name
Rule01
* Listener
* Backend targets
A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.
Listener *
Listner443


Rule01
sap-appgw-biq-cus-qa
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name
Rule01
* Listener
* Backend targets
Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.
Target type
Backend pool
Redirection
Backend target *
Backendpool01
HTTP settings *
HTTP01

5.2.5. Heath Probe Configuration

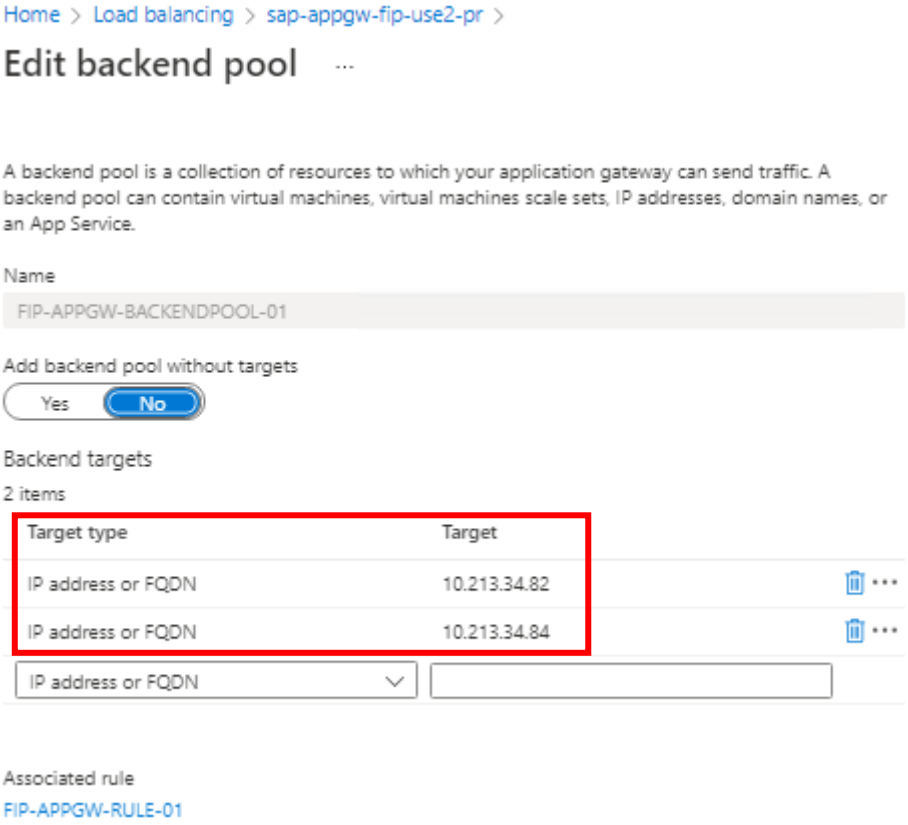
By default, an application gateway monitors the health of all resources in its backend pool and automatically removes unhealthy ones. It then monitors unhealthy instances and adds them back to the healthy backend pool when they become available and respond to health probes.



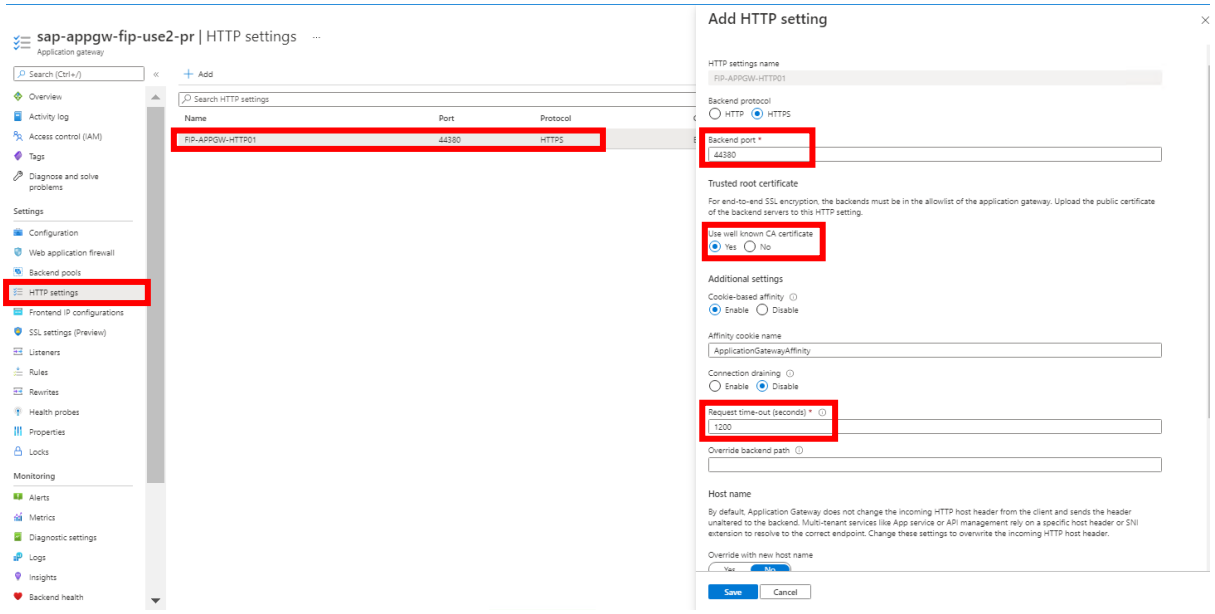


5.3. FIP Configuration

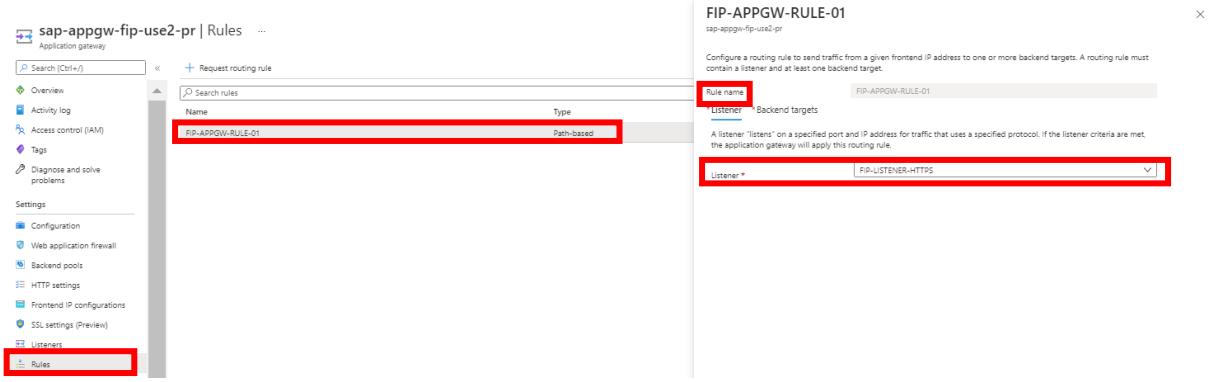
5.3.1. Backend Pool

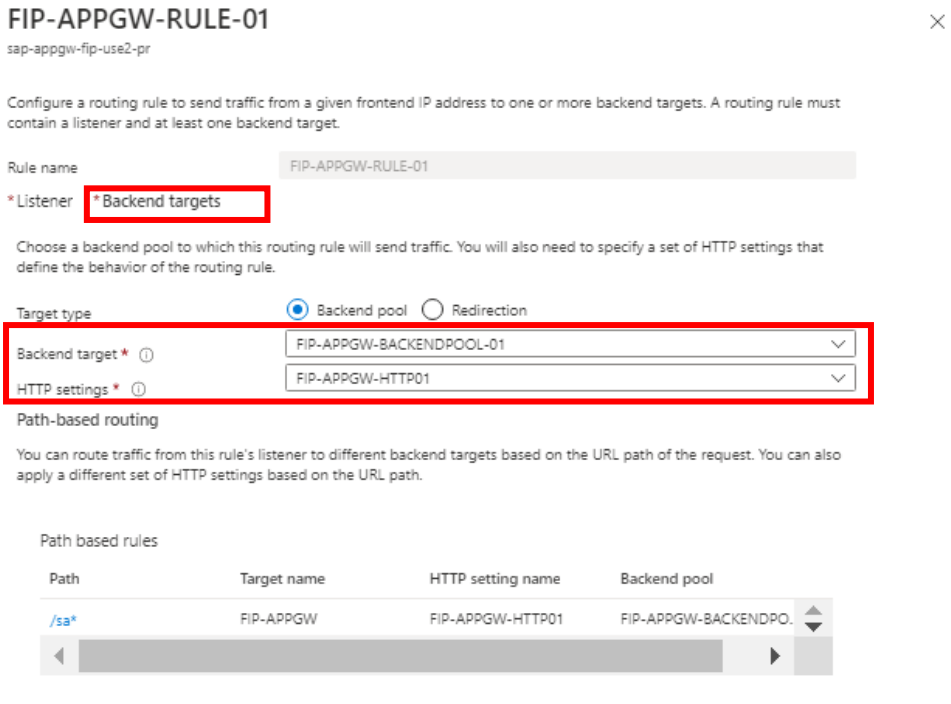


5.3.2. HTTP Settings

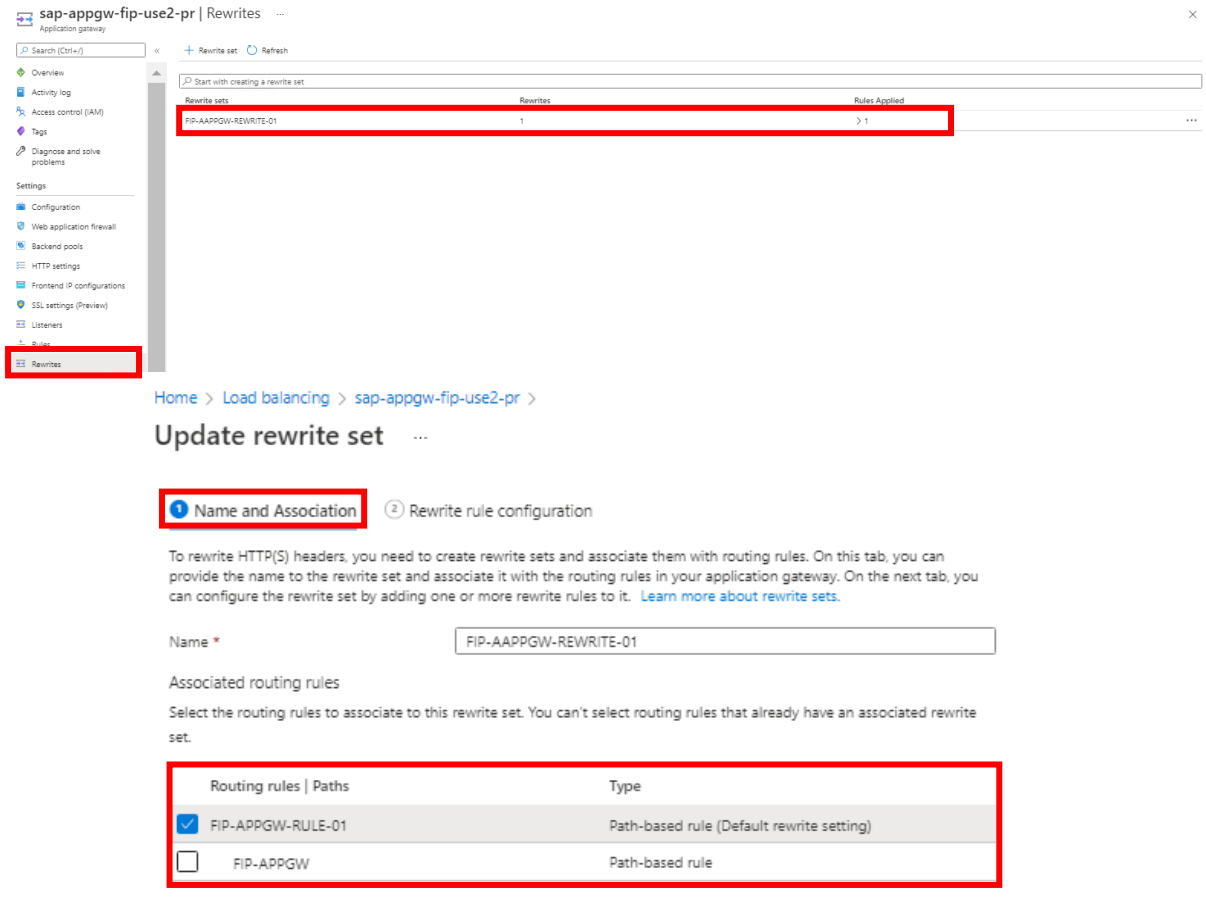


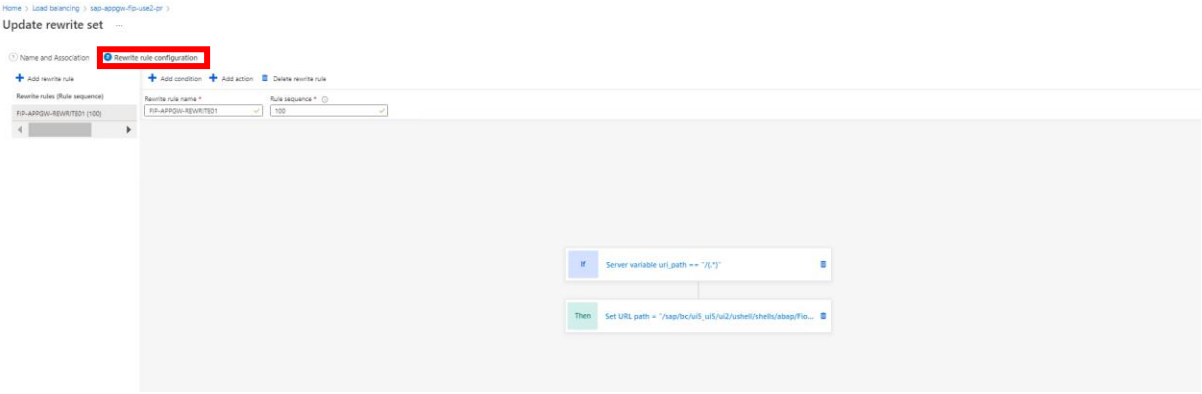
5.3.3. Rules



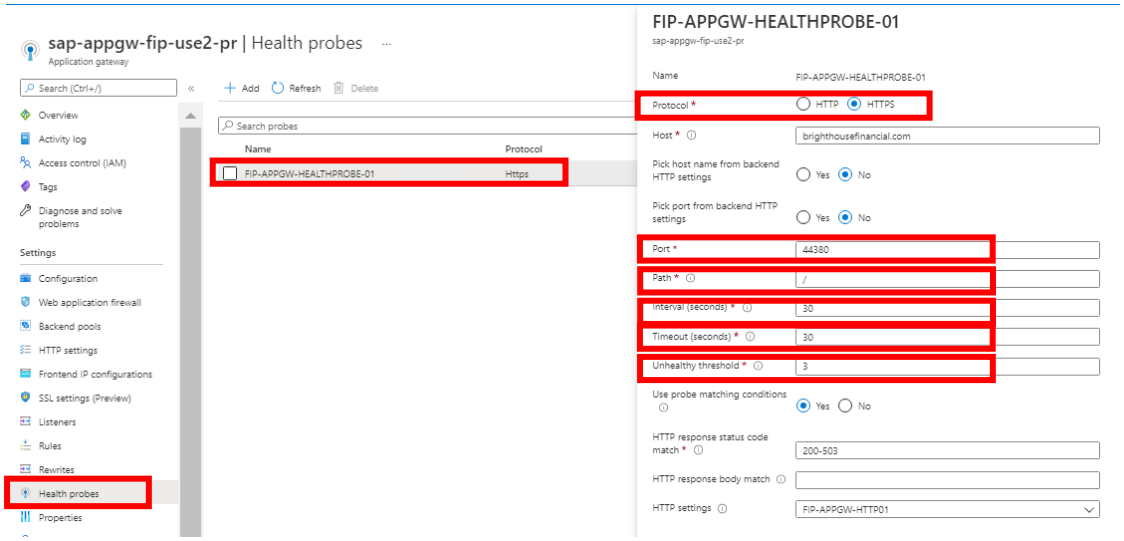


5.3.4. Rewrites



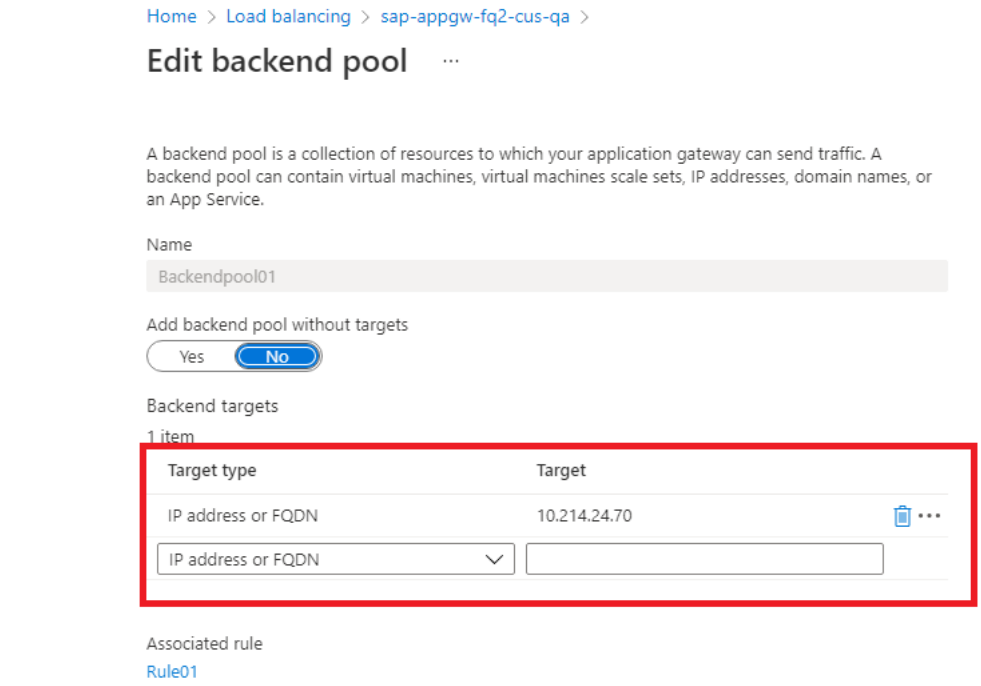


5.3.5. Health Probe

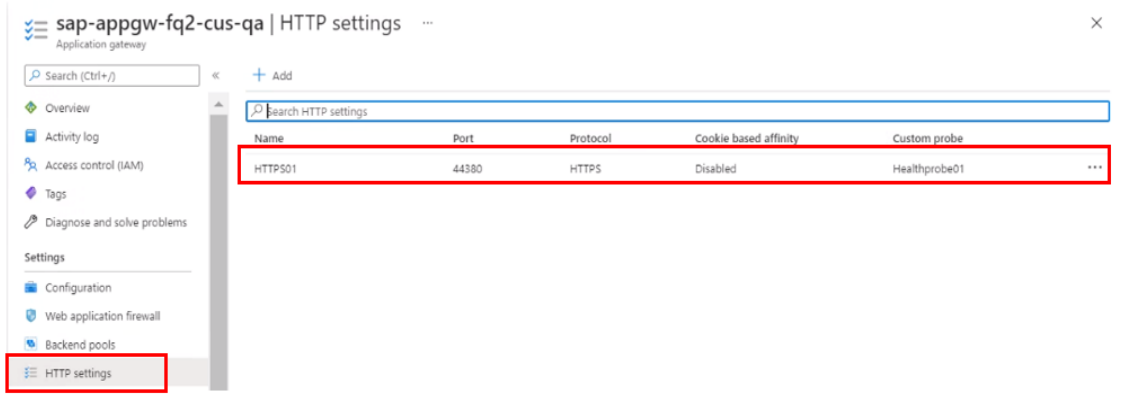


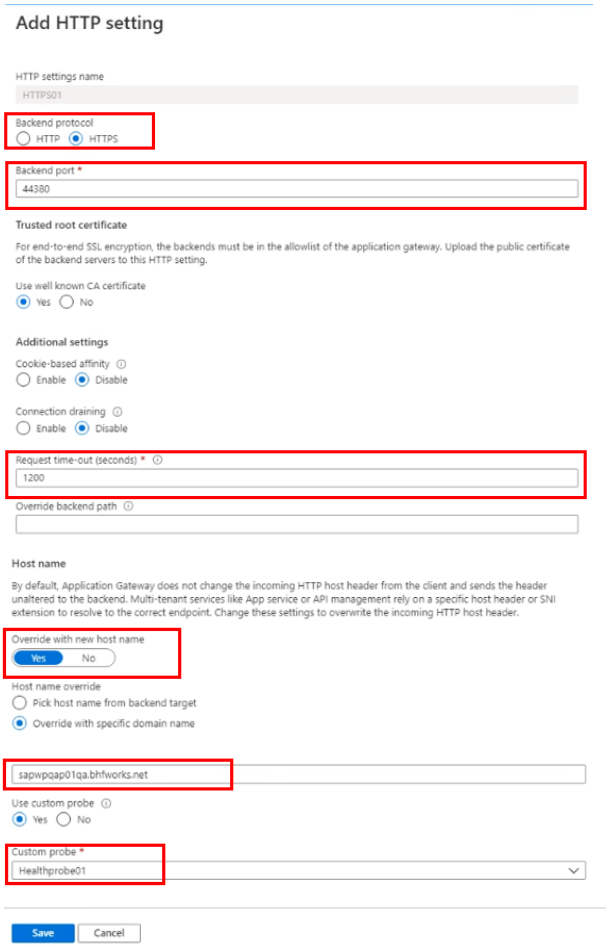
5.4. FQ2 Configuration

5.4.1. Backend pools

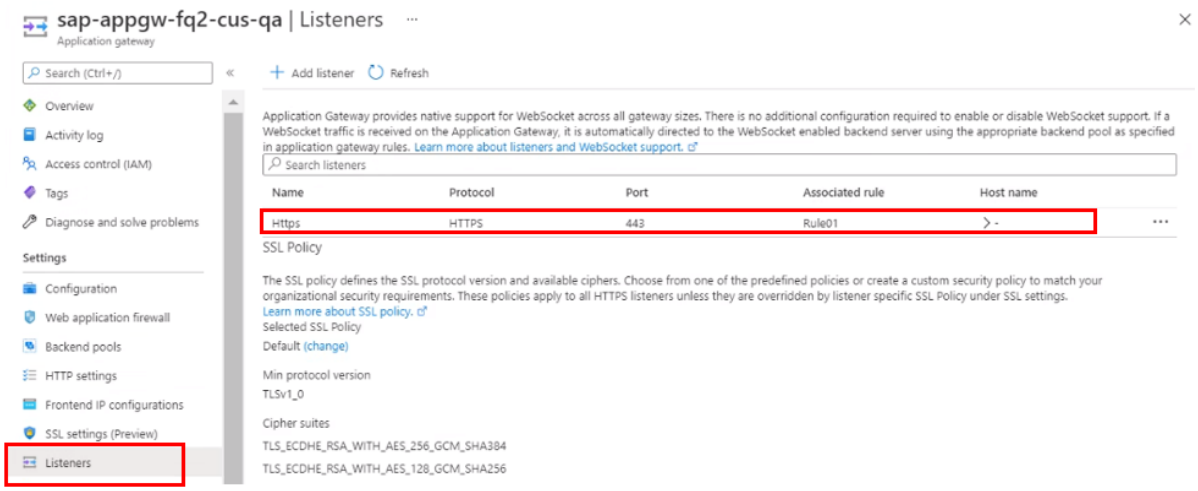


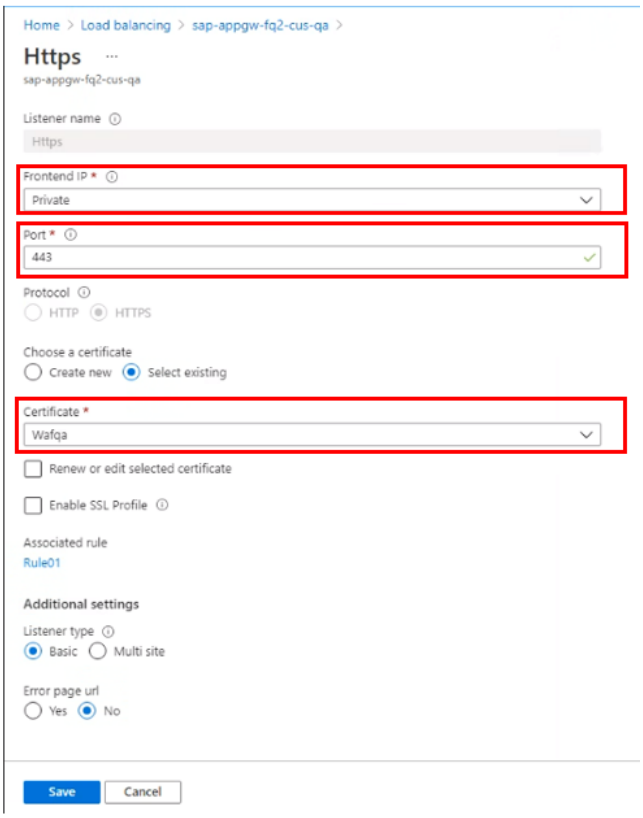
5.4.2. HTTP settings



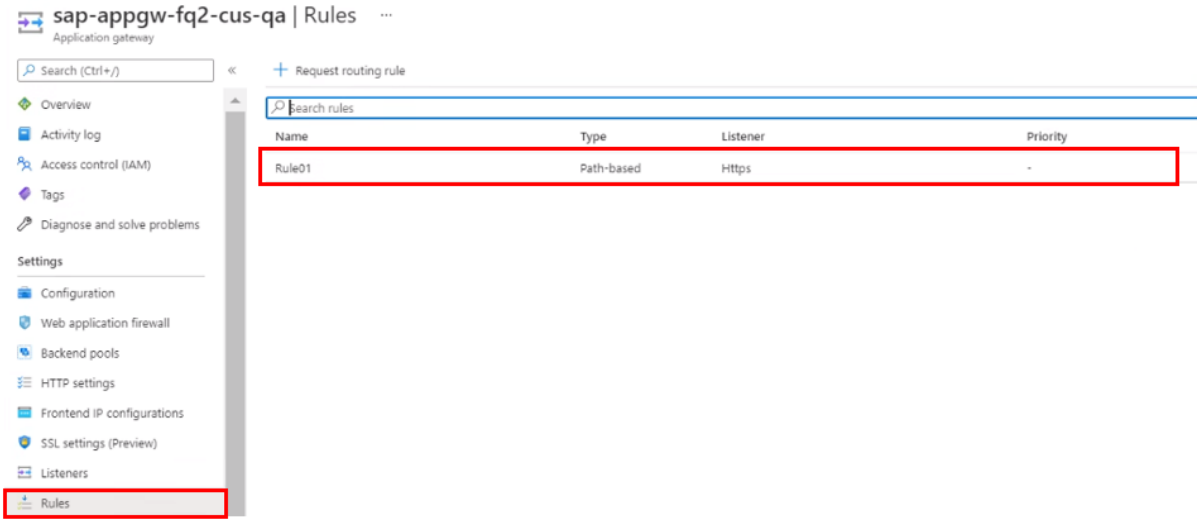


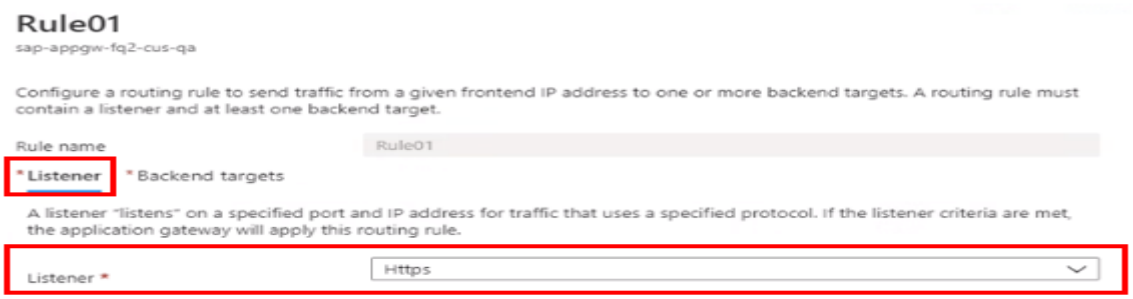
5.4.3. Listeners




Home > Load balancing > sap-appgw-fq2-cus-qa >
Https
sap-appgw-fq2-cus-qa
Listener name
Https
Frontend IP *
Private
Port *
443
Protocol
HTTP HTTPS
Choose a certificate
Create new Select existing
Certificate *
Wafqa
Renew or edit selected certificate
Enable SSL Profile
Associated rule
Rule01
Additional settings
Listener type
Basic Multi site
Error page url
Yes No
Save
Cancel

5.4.4. Rules


sap-appgw-fq2-cus-qa | Rules
Application gateway
Search (Ctrl+/)
Request routing rule
Search rules
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
HTTP settings
Frontend IP configurations
SSL settings (Preview)
Listeners
Rules
Name
Type
Listener
Priority
Rule01
Path-based
Https
-


Rule01
sap-appgw-fq2-cus-qa
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name
Rule01
* Listener
* Backend targets
A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.
Listener *
Https

Rule01

sap-appgw-fq2-cus-qa

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name: Rule01

* Listener | * Backend targets

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type: (•) Backend pool ( ) Redirection

Backend target * : Backendpool01

HTTP settings * : HTTPS01

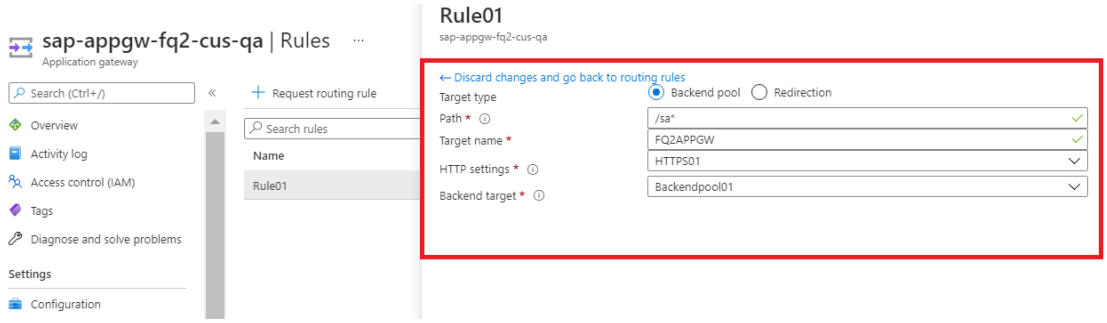
Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

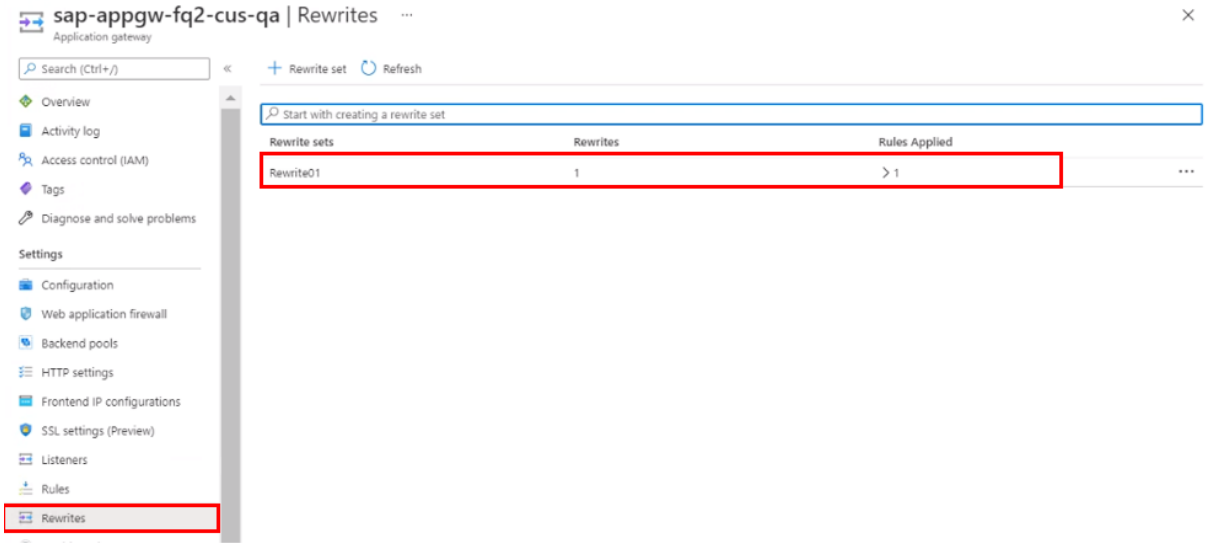
Path based rules

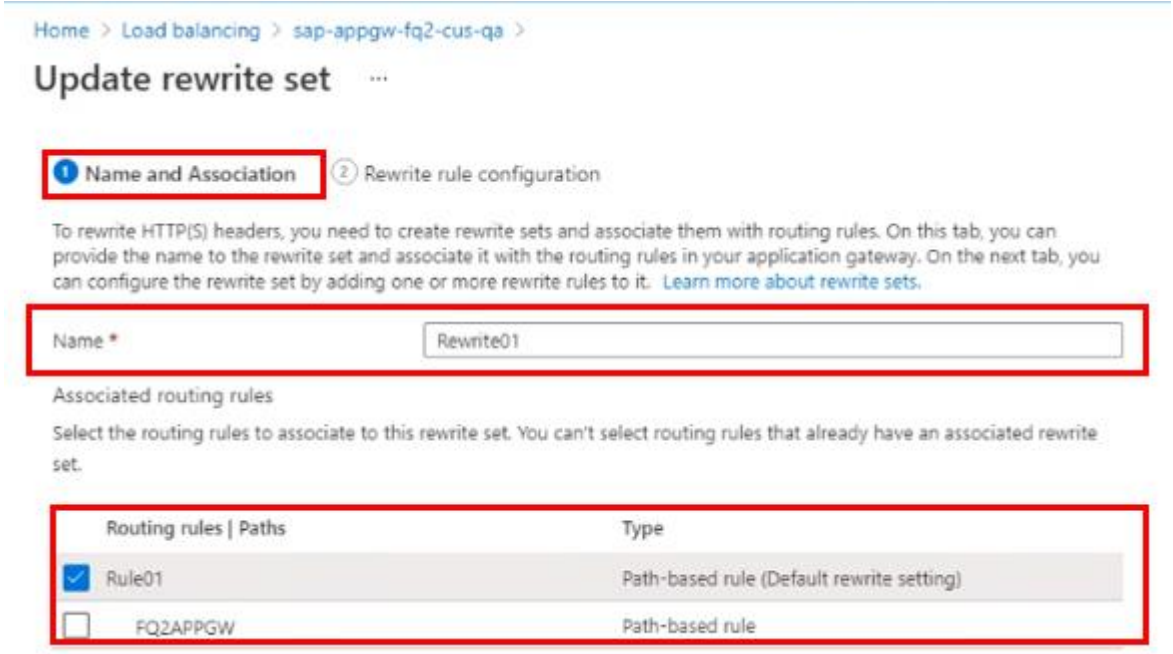
Path	Target name	HTTP setting name	Backend pool	
/sa*	FQ2APPGW	HTTPS01	Backendpool01	•••

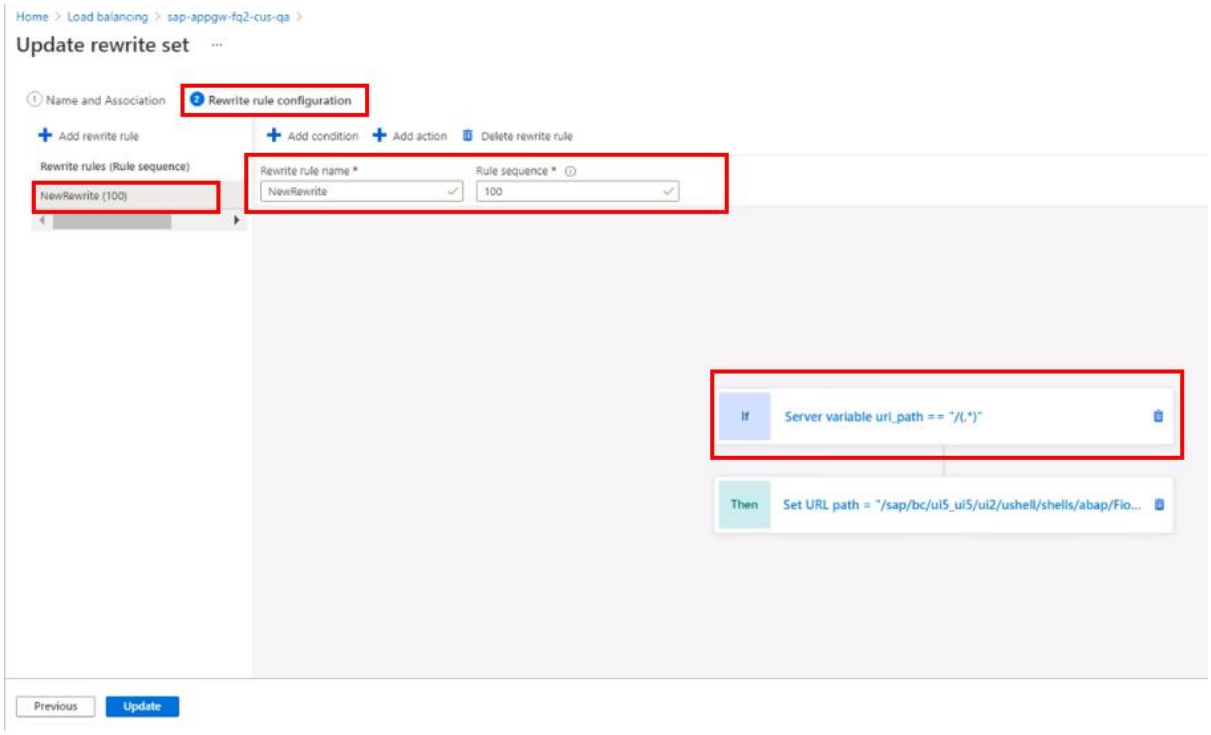
Add multiple targets to create a path-based rule

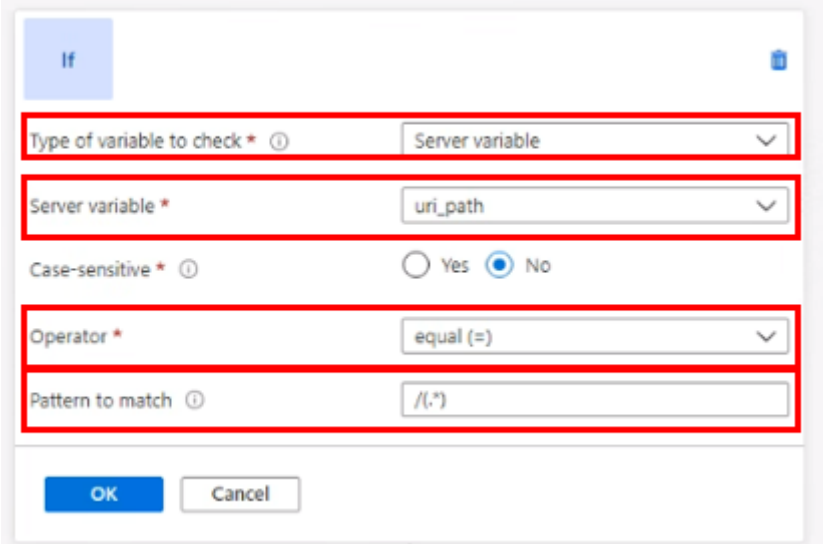


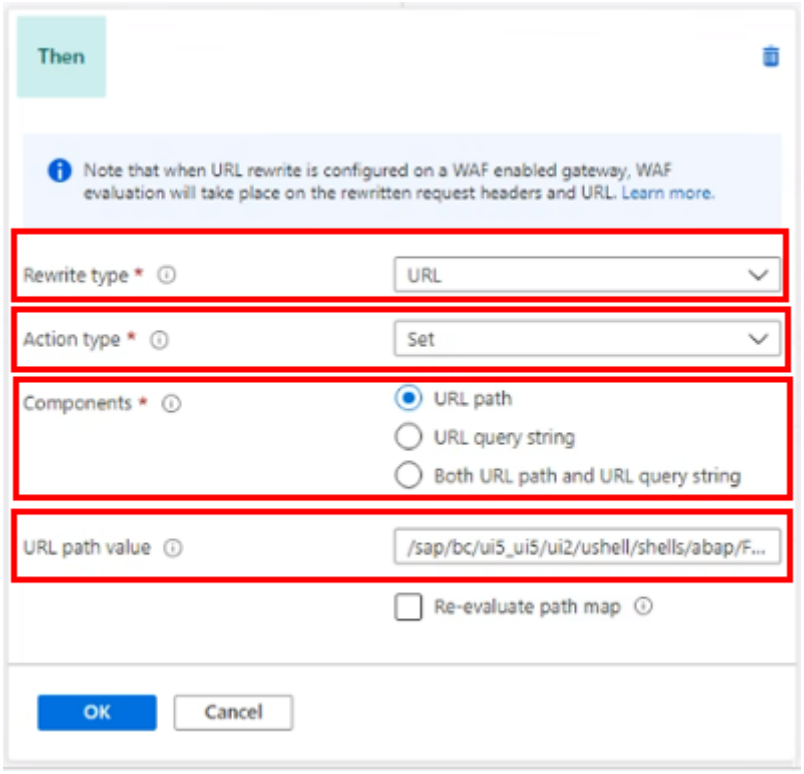
5.4.5. Rewrites



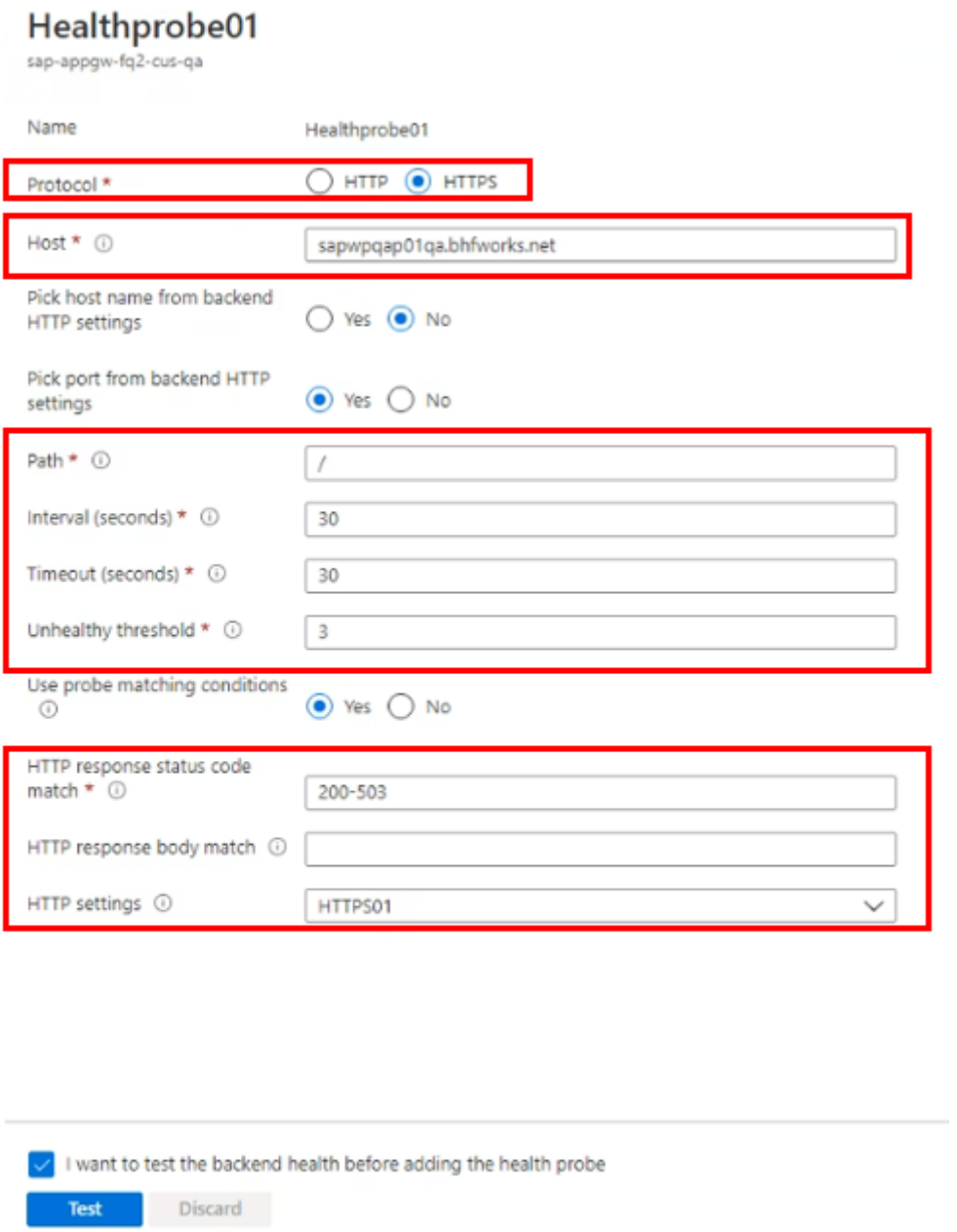



Home > Load balancing > sap-appgw-fq2-cus-qa >
Update rewrite set
Name and Association
Rewrite rule configuration
Add rewrite rule
Add condition
Add action
Delete rewrite rule
Rewrite rules (Rule sequence)
NewRewrite (100)
Rewrite rule name *
NewRewrite
Rule sequence *
100
If
Server variable uri_path == "/(.*)"
Then
Set URL path = "/sap/bc/ui5_ui5/ui2/ushell/shells/abap/Fio...
Previous
Update


If
Type of variable to check *
Server variable
Server variable *
uri_path
Case-sensitive *
Yes
No
Operator *
equal (=)
Pattern to match
/(.*)
OK
Cancel

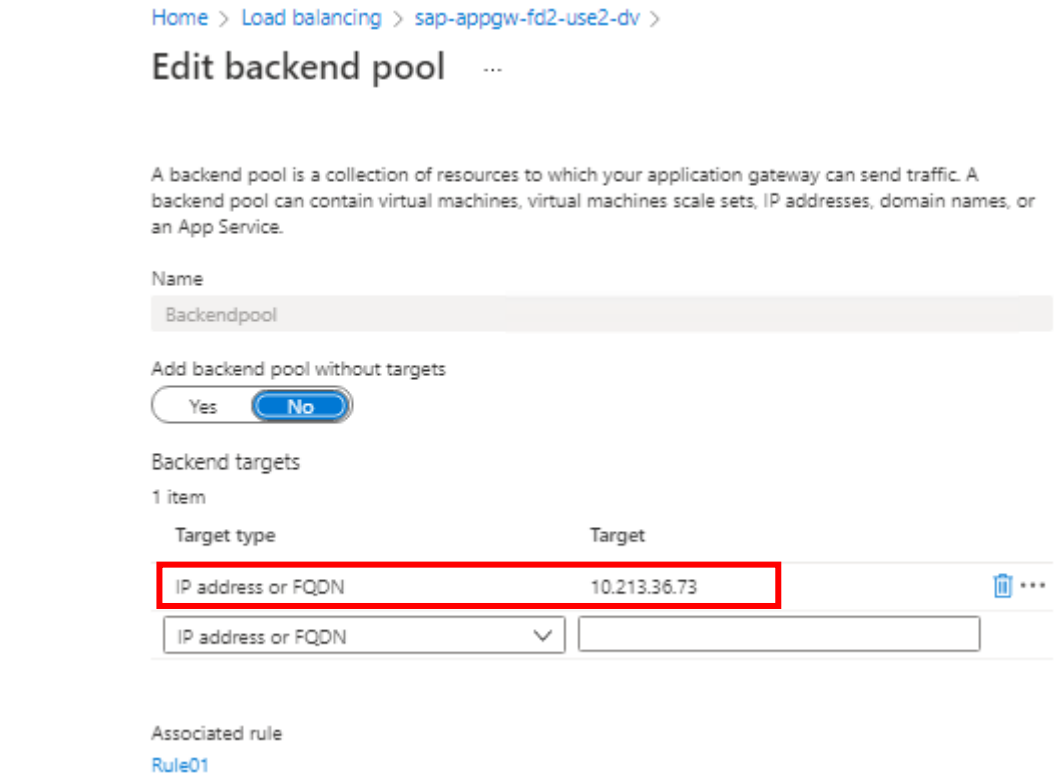


5.4.6. Health Probe

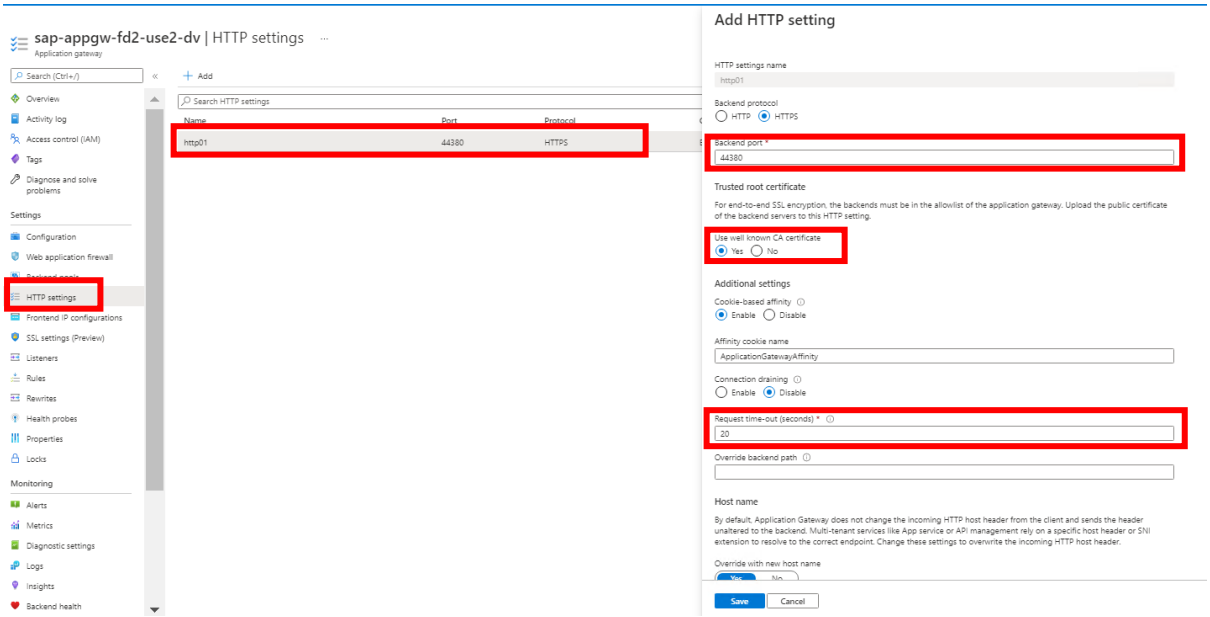


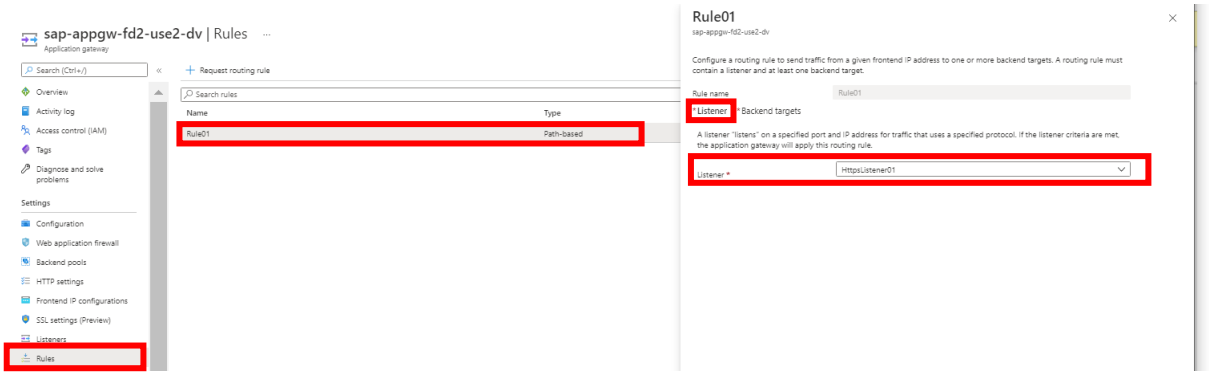
5.5. FD2 Configuration

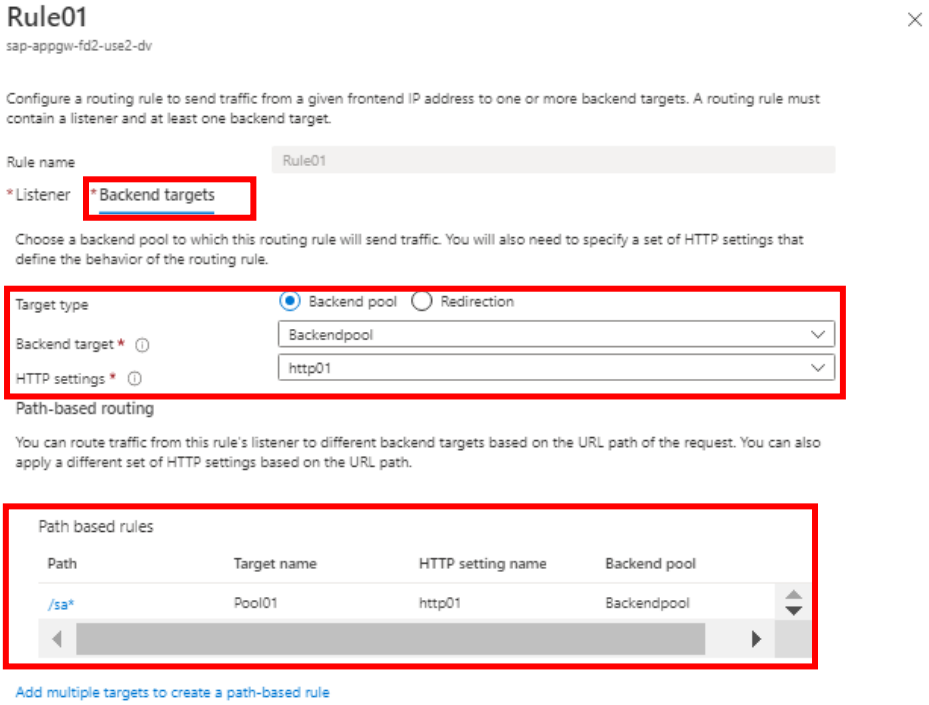
5.5.1. Backend Pool



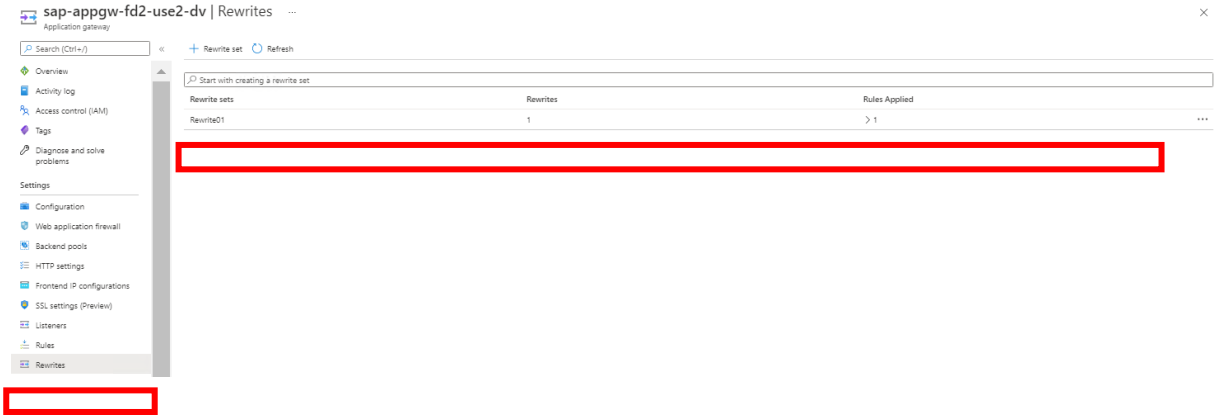
5.5.2. HTTP Settings

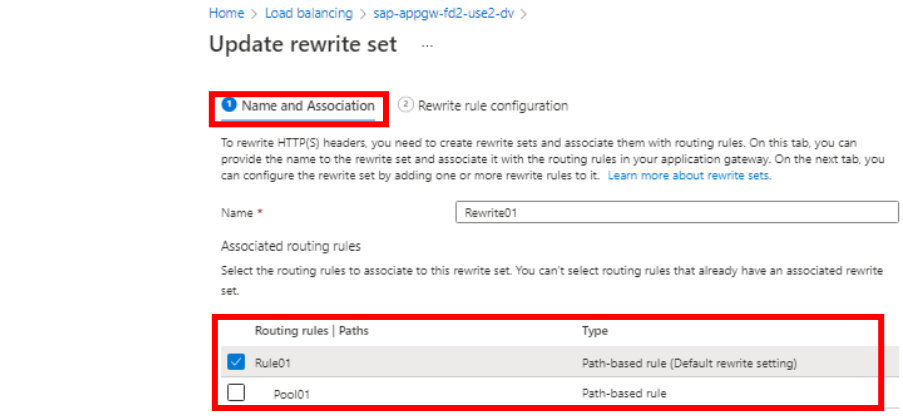


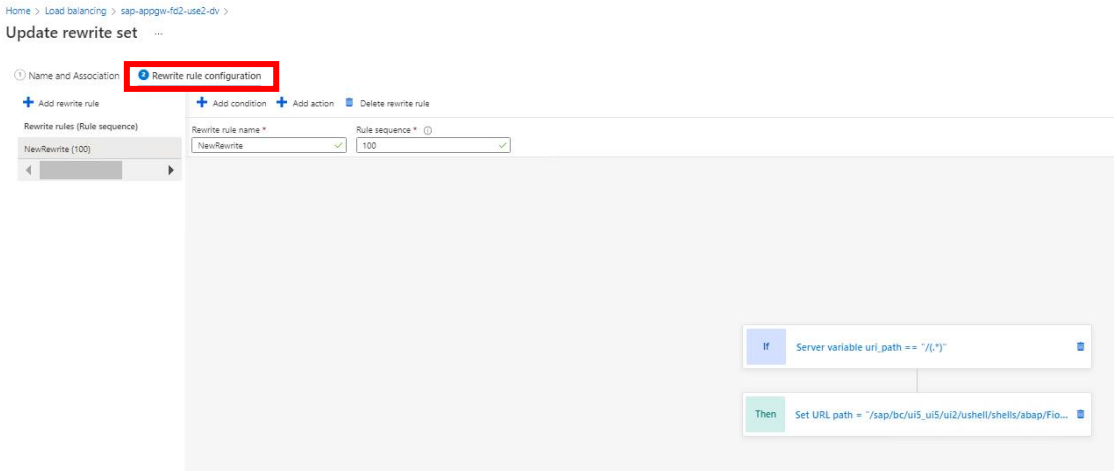




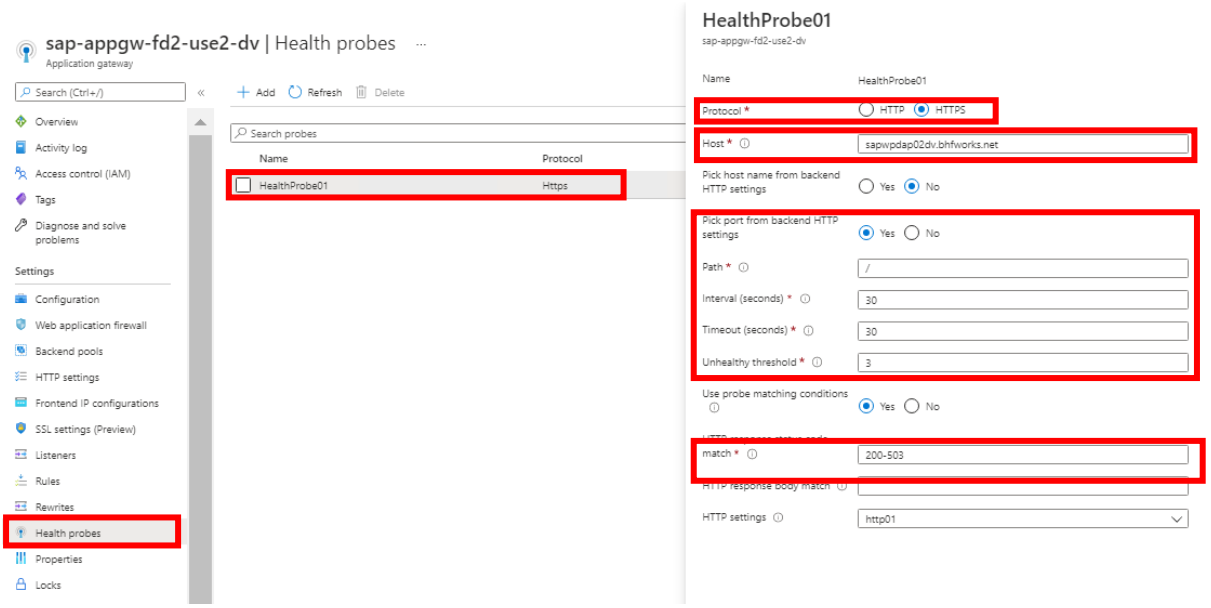
5.5.3. Rewrites





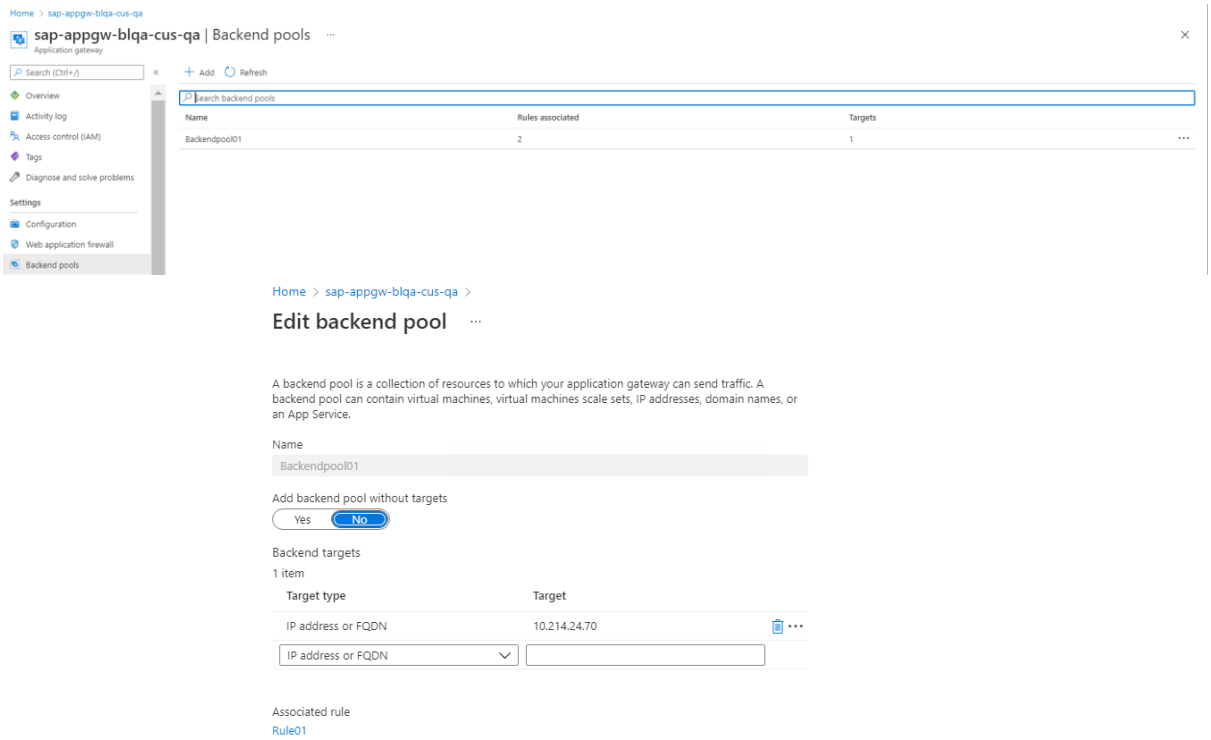


5.5.4. Health Probes

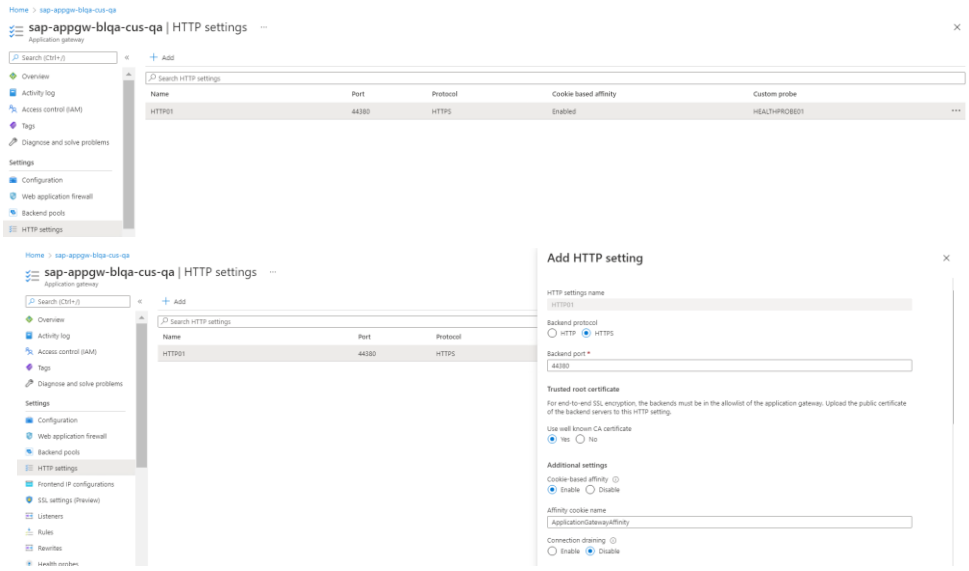


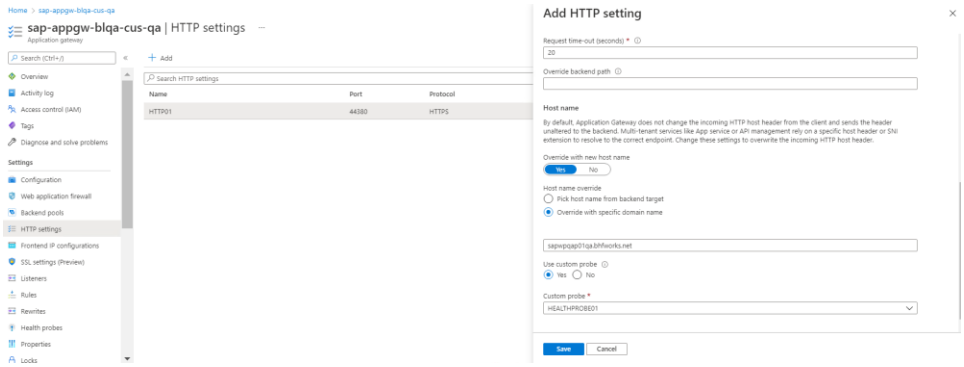
5.6. BLQA Configuration

5.6.1. Backend Pool

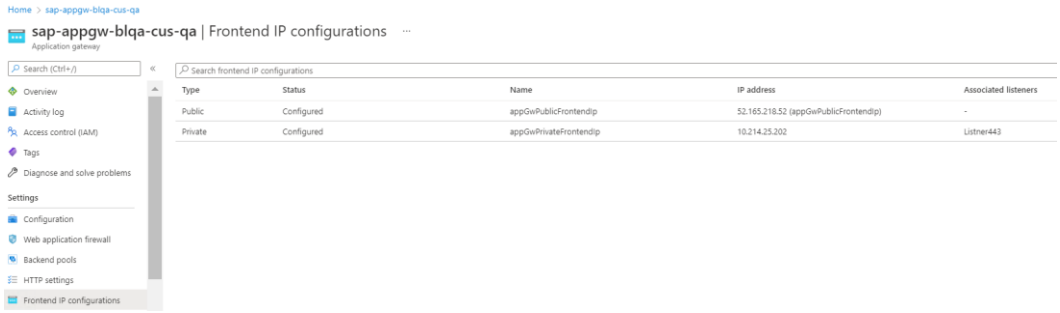


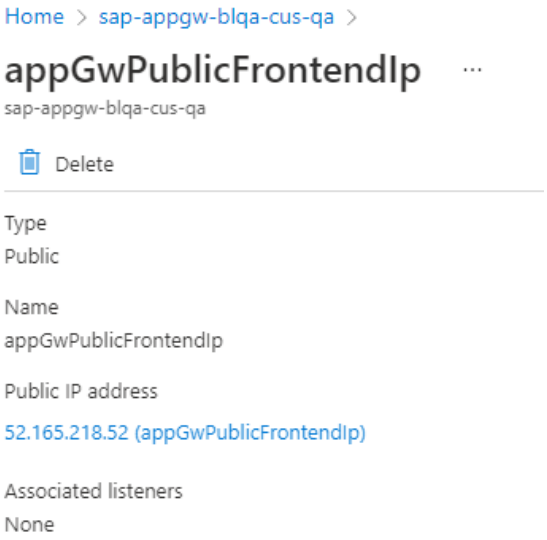
5.6.2. HTTP Settings

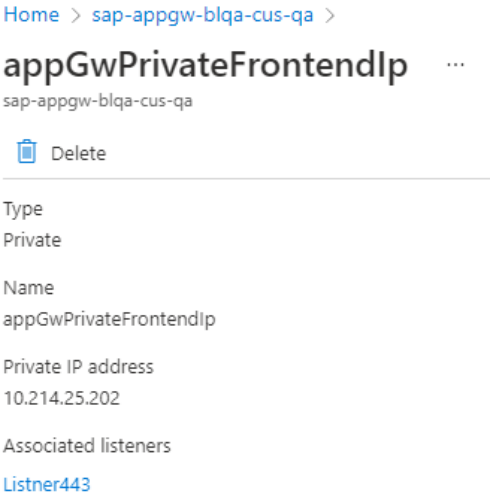




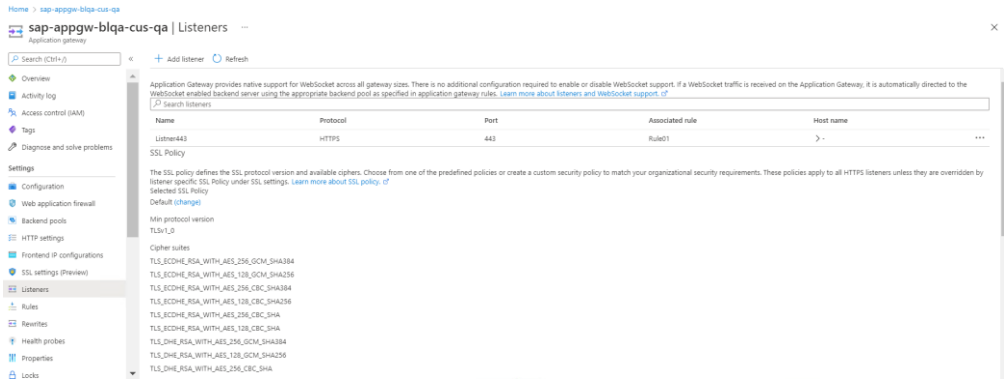
5.6.3. Frontend IP Configurations

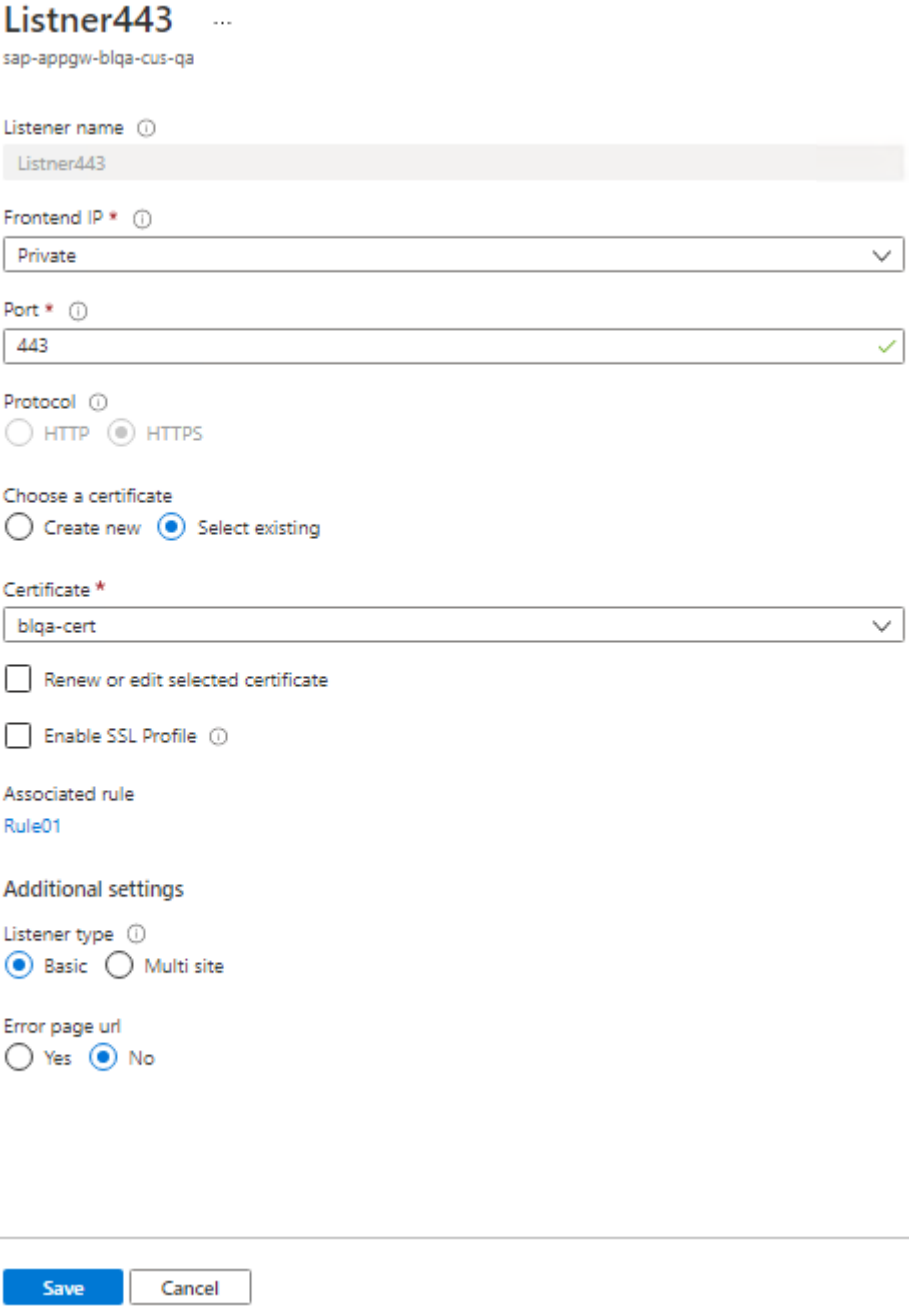




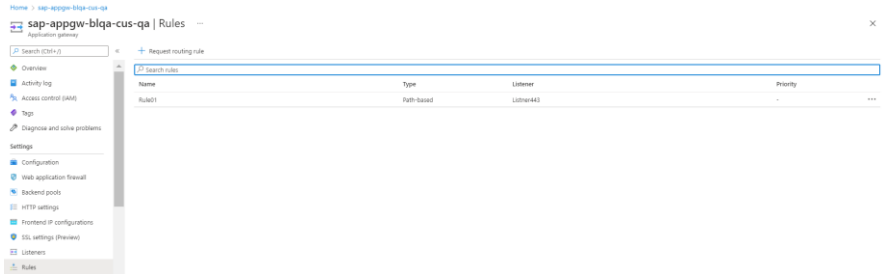


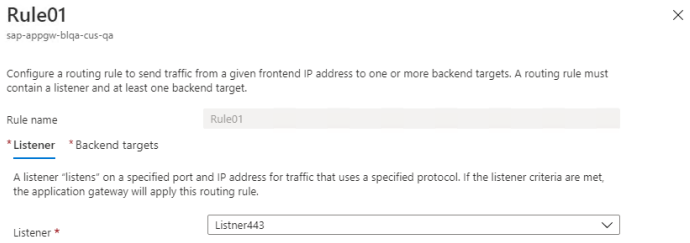
5.6.4. Listeners

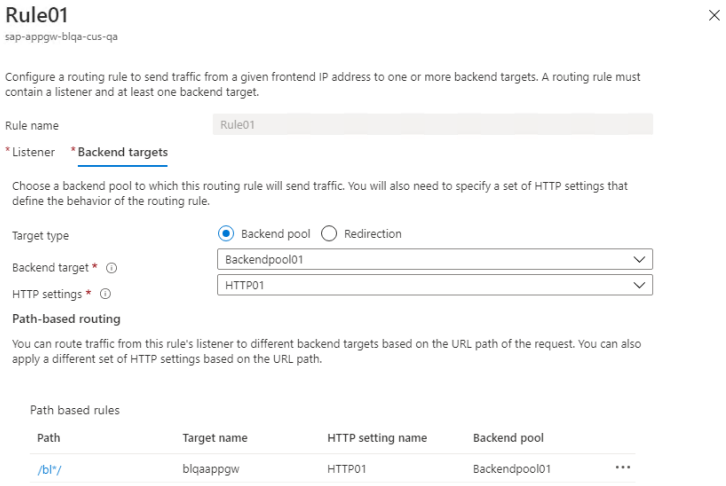



Listner443
sap-appgw-blqa-cus-qa
Listener name
Listner443
Frontend IP *
Private
Port *
443
Protocol
HTTP
HTTPS
Choose a certificate
Create new
Select existing
Certificate *
blqa-cert
Renew or edit selected certificate
Enable SSL Profile
Associated rule
Rule01
Additional settings
Listener type
Basic
Multi site
Error page url
Yes
No
Save
Cancel

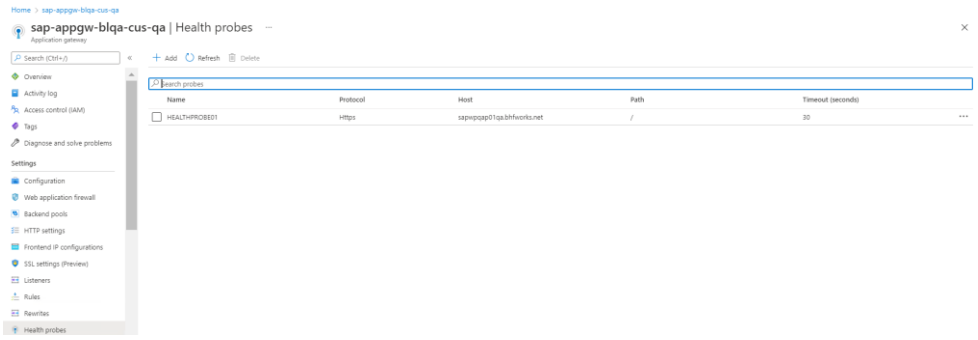
5.6.5. Rules

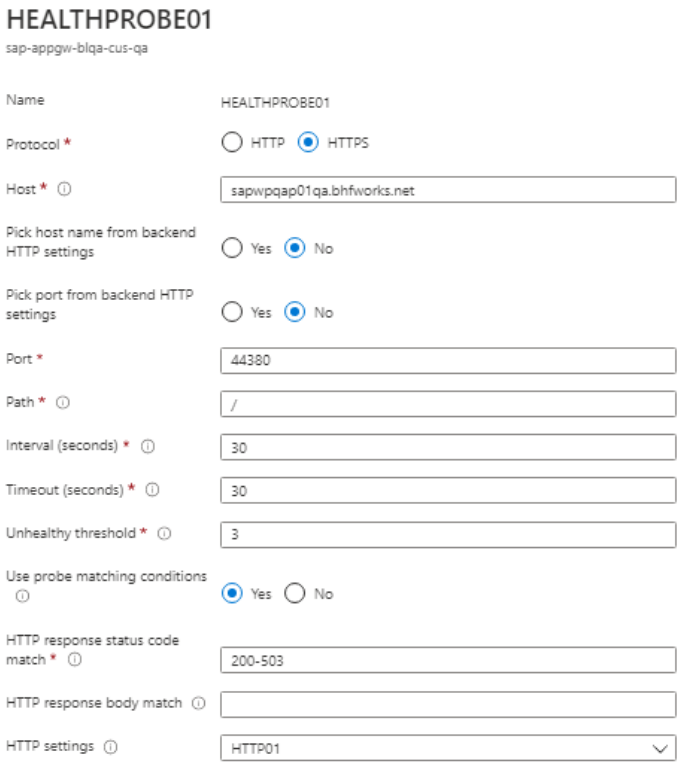

sap-appgw-blqa-cus-qa | Rules
Request routing rule
Search rules
Name
Type
Listener
Priority
Rule01
Path-based
Listner443





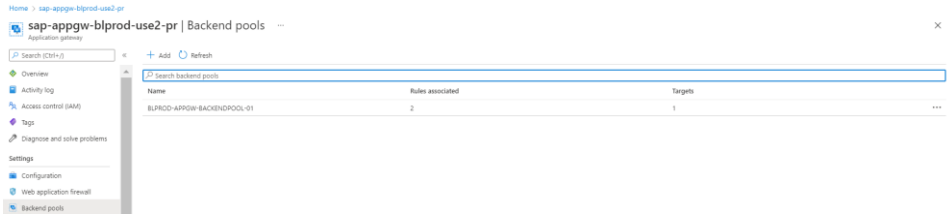
5.6.6. Health Probes

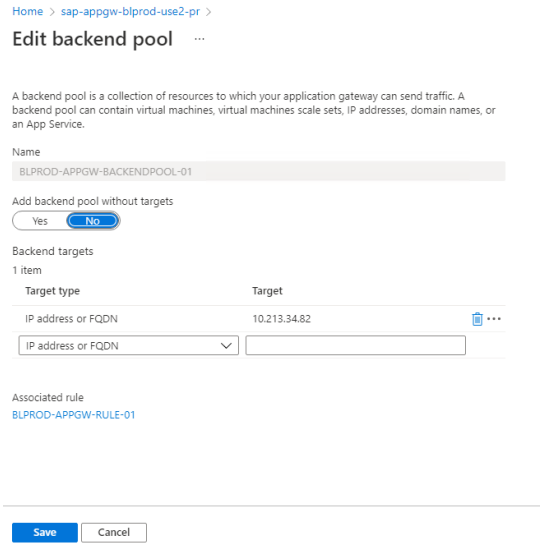




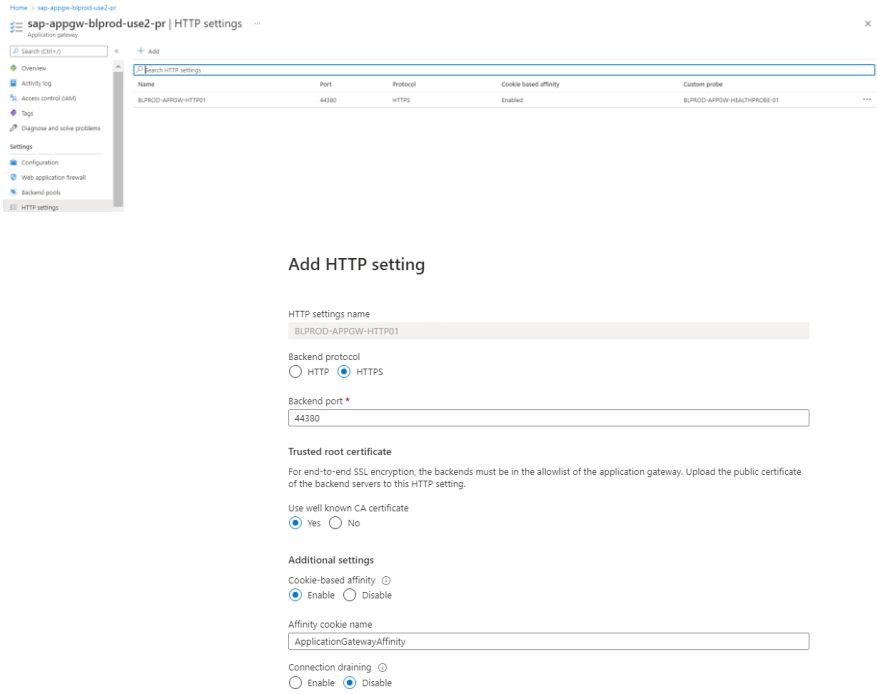
5.7. BLPROD Configuration

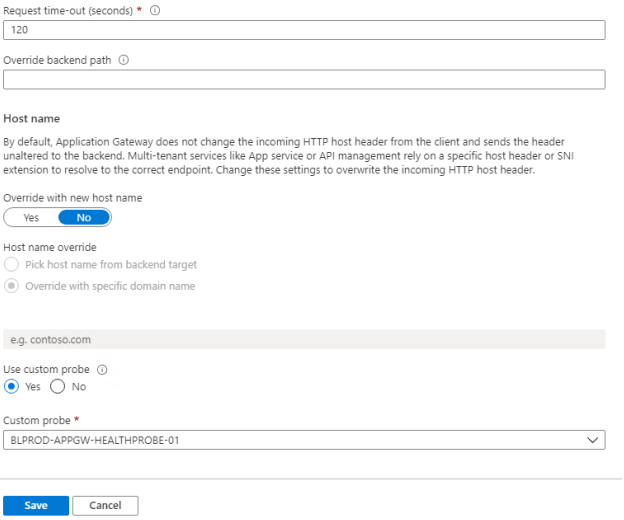
5.7.1. Backend Pool



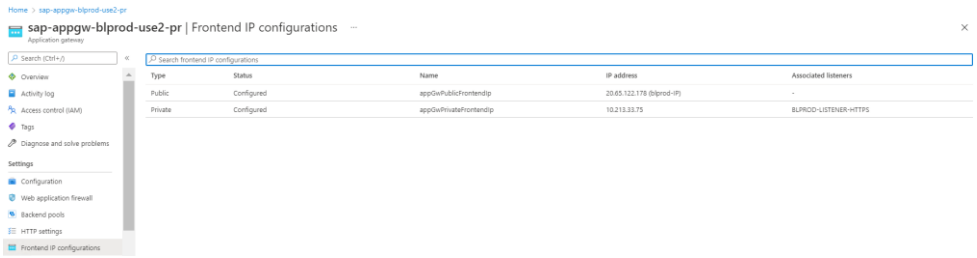


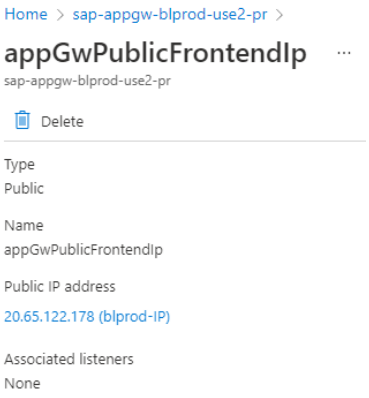
5.7.2. HTTP Settings

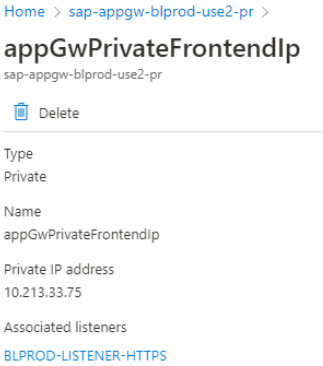




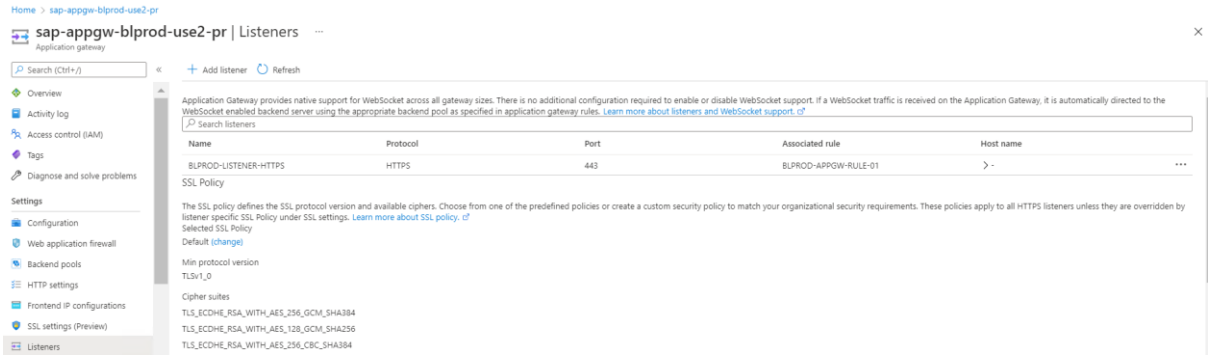
5.7.3. Frontend IP Configurations

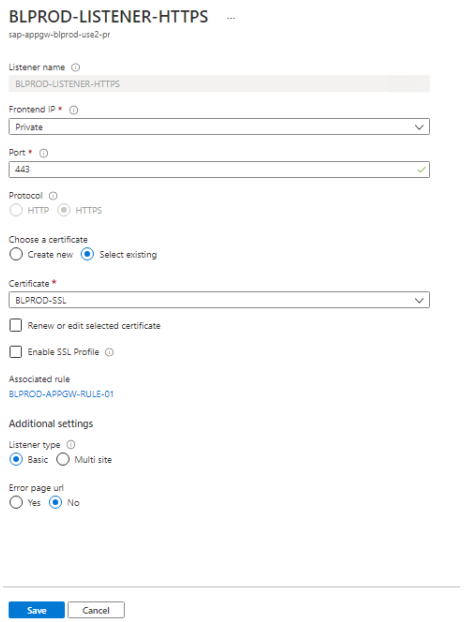




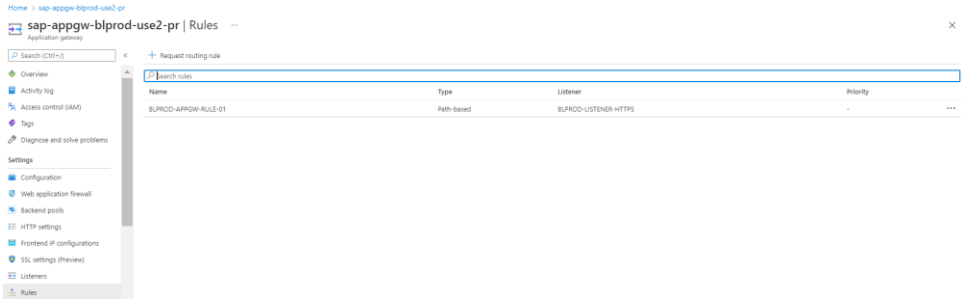


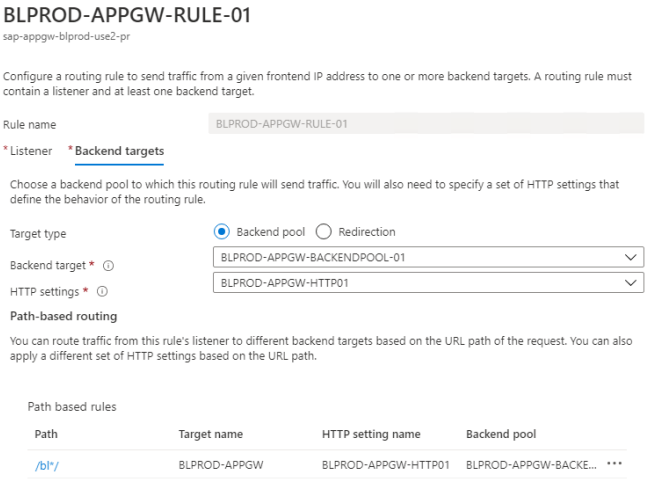
5.7.4. Listeners



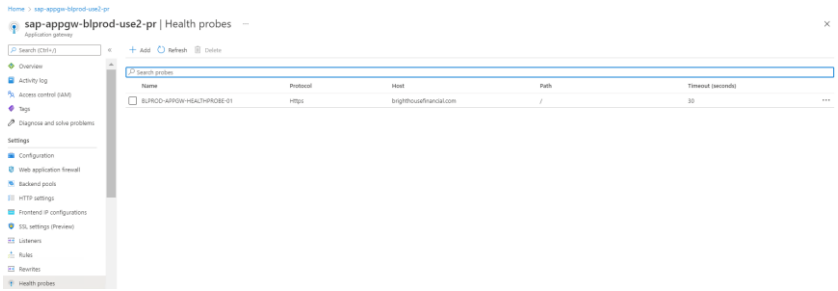


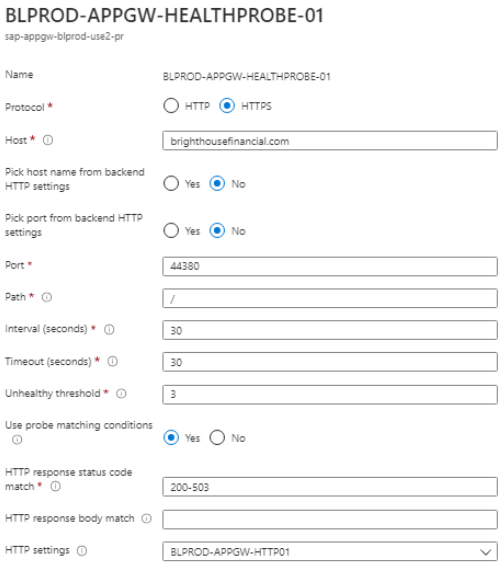
5.7.5. Rules





5.7.6. Health Probes





Revision History

Version	Date	Author	Approvers	Changes
1.0	29/11/2021	Aniudh Voruganti	Sasikumar Sampath	Initial Draft
2.0	16/02/2022	Aniudh Voruganti	Sasikumar Sampath	Blackline QA and Prod configuration added