

# Pattern implementation for network secure ingress

Article • 08/01/2023

Network secure ingress encapsulates several design patterns, including the patterns for global routing, global offloading, and health endpoint monitoring. You can use the pattern implementation in this article as a gateway for any HTTP or HTTPS workload that requires high availability or reliability by providing secure global routing to workloads in differing regions with low-latency failover.

## Video: Network secure ingress implementation

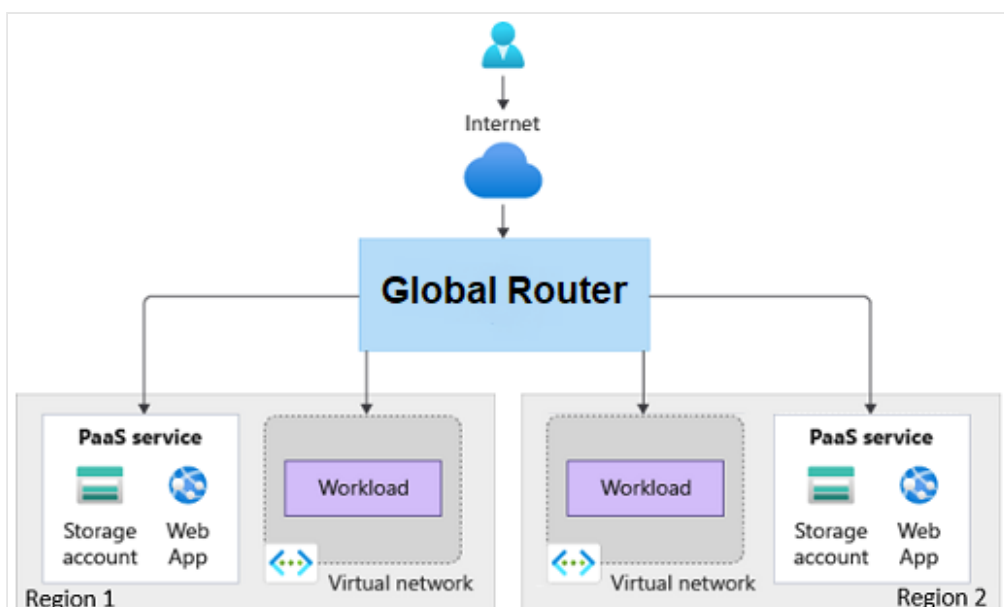
<https://learn-video.azurefd.net/vod/player?id=163c161c-0f7e-4fea-b126-c8f540fc84e0&embedUrl=%2Fazure%2Farchitecture%2Fpattern-implementations%2Fnetwork-secure-ingress&locale=en-us>

## Pattern requirements

This article describes three requirements that the pattern implementation for network secure ingress focuses on: global routing, low-latency failover, and mitigating attacks at the edge.

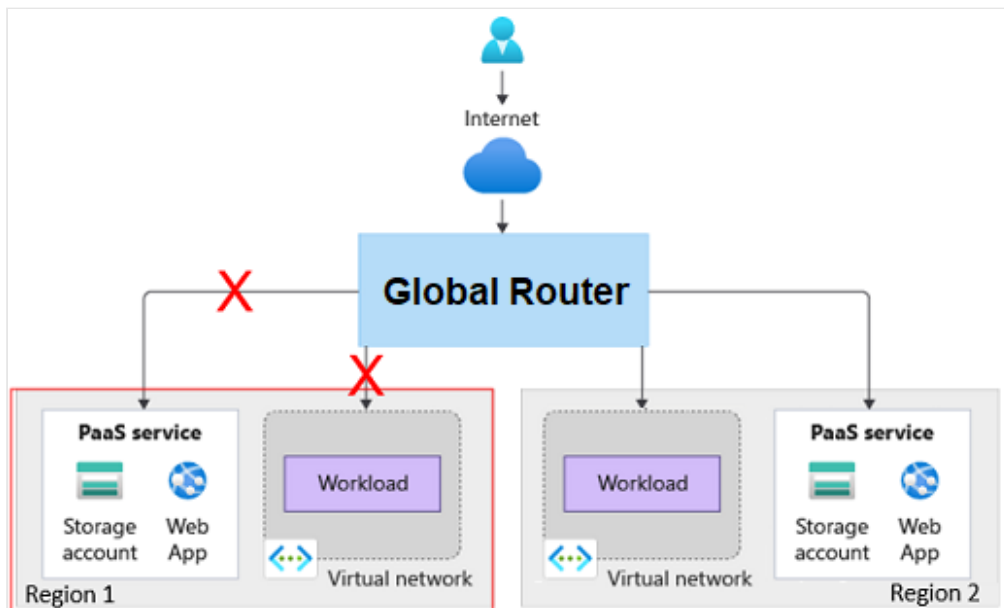
## Global routing

The network secure ingress pattern encapsulates the global routing pattern. As such, the implementation can route requests to workloads in different regions.



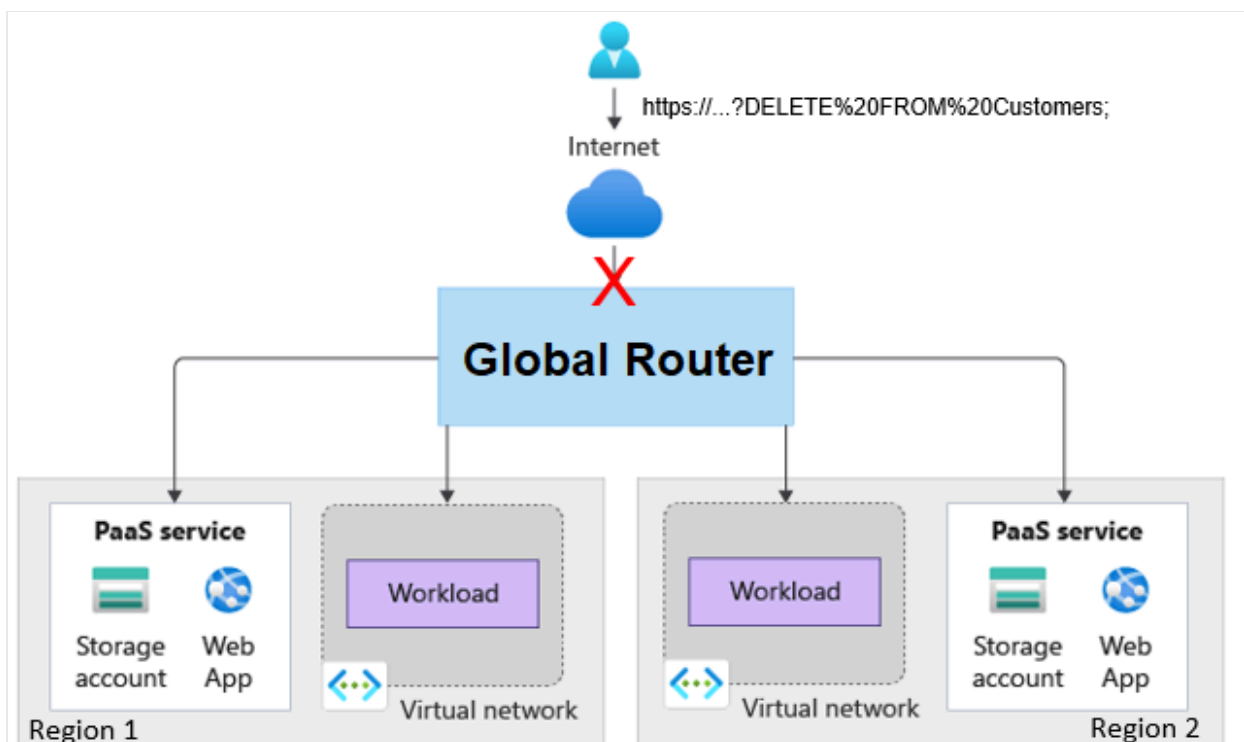
## Low-latency failover

The implementation must be able to identify healthy and unhealthy workloads and adjust the routing accordingly in a time-sensitive way. The latency should be able to support adjusting the routing in a matter of minutes.



## Mitigating attacks at the edge

Mitigating attacks at the edge necessitates the "network secure" part of the implementation. The workloads or platform as a service (PaaS) services shouldn't be accessible via the internet. Internet traffic should only be able to route through the gateway. The gateway should have the ability to mitigate exploits.

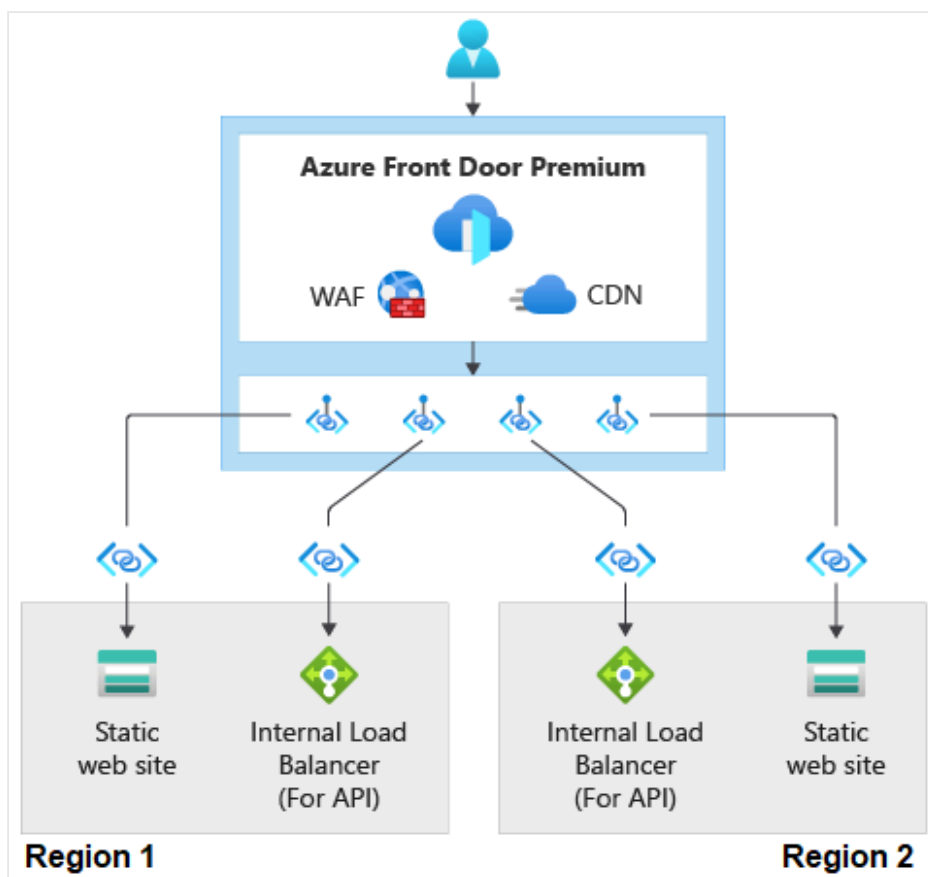


# Patterns

This solution implements the following design patterns:

- [Gateway routing pattern](#): Route requests to multiple services or service instances that can reside in different regions.
- [Gateway offloading pattern](#): Offload functionality, such as mitigating attacks, to a gateway proxy.
- [Health endpoint monitoring pattern](#): Expose endpoints that validate the health of the workload.

## Design



This implementation includes the following details:

- It uses Azure Blob Storage accounts to simulate static web workloads running in two regions. This implementation doesn't include any workloads running behind an internal load balancer (ILB). The diagram shows an ILB to illustrate that this implementation would work for private workloads running behind an ILB.
- It uses Azure Front Door Premium tier as the global gateway.
- The Azure Front Door instance has a global web application firewall (WAF) policy configured with managed rules that help protect against common exploits.
- The storage accounts aren't exposed over the internet.

- The Azure Front Door Premium tier accesses the storage accounts via Azure Private Link.
- The Azure Front Door instance has the following high-level configuration:
  - An endpoint with a single route that points to a single origin group. An origin group is a collection of origins or back ends.
  - The origin group has an origin configured to point to each storage account.
  - Each origin requests Private Link access to the storage account.
  - The origin group has health probes configured to access an HTML page in the storage accounts. The HTML page is acting as the health endpoint for the static workloads. If the probes can successfully access the origin in three out of the last four attempts, the origin is deemed healthy.

## Components

### Web request

- [Azure Web Application Firewall](#): The Premium tier of Web Application Firewall supports Microsoft-managed rules that help protect against common exploits.
- [Azure Private Link](#): Private endpoints in Azure Private Link expose an Azure PaaS service to a private IP address in a virtual network. This exposure allows the communication to flow across the Microsoft backbone network and not on the public internet.
- [Azure Front Door Premium tier](#): Azure Front Door provides Layer 7 global load balancing. Azure Front Door has integration with Web Application Firewall. The Premium tier supports:
  - [Azure Private Link](#): Private Link support allows Azure Front Door to communicate with PaaS services or workloads running in a private virtual network over the Microsoft backbone network.
  - [Microsoft-managed rule sets](#): The premium tier of Azure Front Door supports the premium tier of Web Application Firewall, which supports the managed rule set in the WAF.
- [Azure Storage](#): This implementation uses Blob Storage accounts to represent a static website or workload.
- [Internal load balancer](#): This implementation doesn't use the internal load balancer. It's pictured to represent a private workload running behind that load balancer. The routing to the storage account is the same as it would be to load balancers.

### Operations

Securing resources from a network perspective helps protect against exploits, but it also isolates the resources from processes or administrators who might need to access those

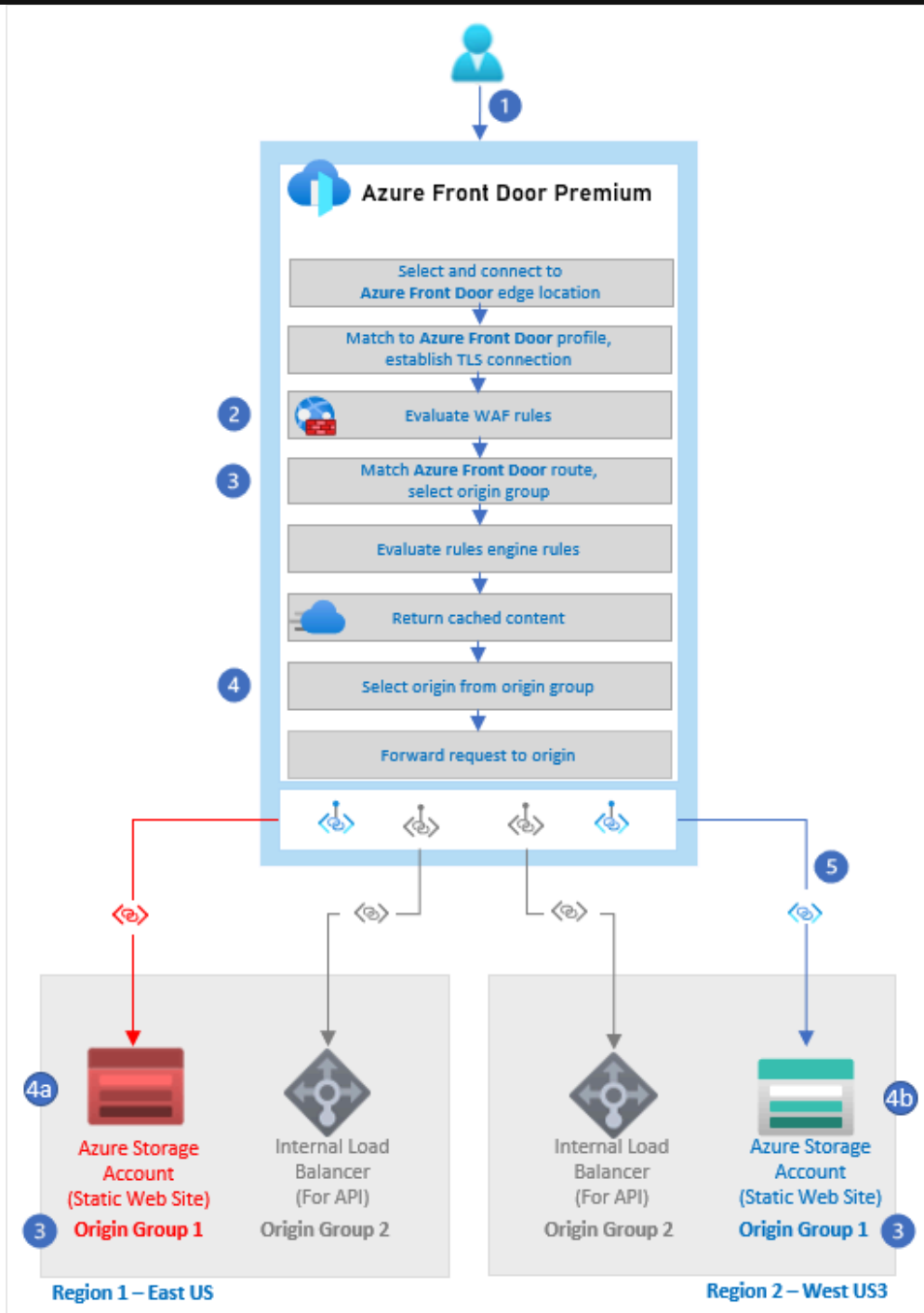
resources. For example, a build agent in a DevOps pipeline might need to access the storage account in order to deploy an update to the web application. Also, an administrator might need to access the resource for troubleshooting purposes.

To illustrate providing access to network secure access for operational purposes, this implementation deploys a virtual machine (VM) in a virtual network that has Private Link access to the storage accounts. This implementation deploys Azure Bastion, which the administrator can use to connect to the VM. For the deployment scenario, a private build agent could be deployed to the virtual network, similar to how the VM was.

Here are details about the components for operations:

- [Azure Virtual Network](#): This implementation uses the virtual network to contain the components required for an administrator to securely communicate with the storage account over the private Microsoft backbone network.
- [Azure Virtual Machines](#): This implementation uses a VM as a jumpbox for administrators to connect to. The VM is deployed in the private virtual network.
- [Azure Bastion](#): Azure Bastion allows the administrator to securely connect to the jumpbox VM over Secure Shell (SSH) without requiring the VM to have a public IP address.
- [Private Link endpoint](#): The private endpoint is assigned a private IP address from the virtual network and connects to the storage account PaaS service. This connection allows resources in the private virtual network to communicate with the storage account over the private IP address.
- [Private Azure DNS zone](#): The private Azure DNS zone is a DNS service that's used to resolve the Azure storage account's Private Link host name to the private endpoint's private IP address.

## Web request flow



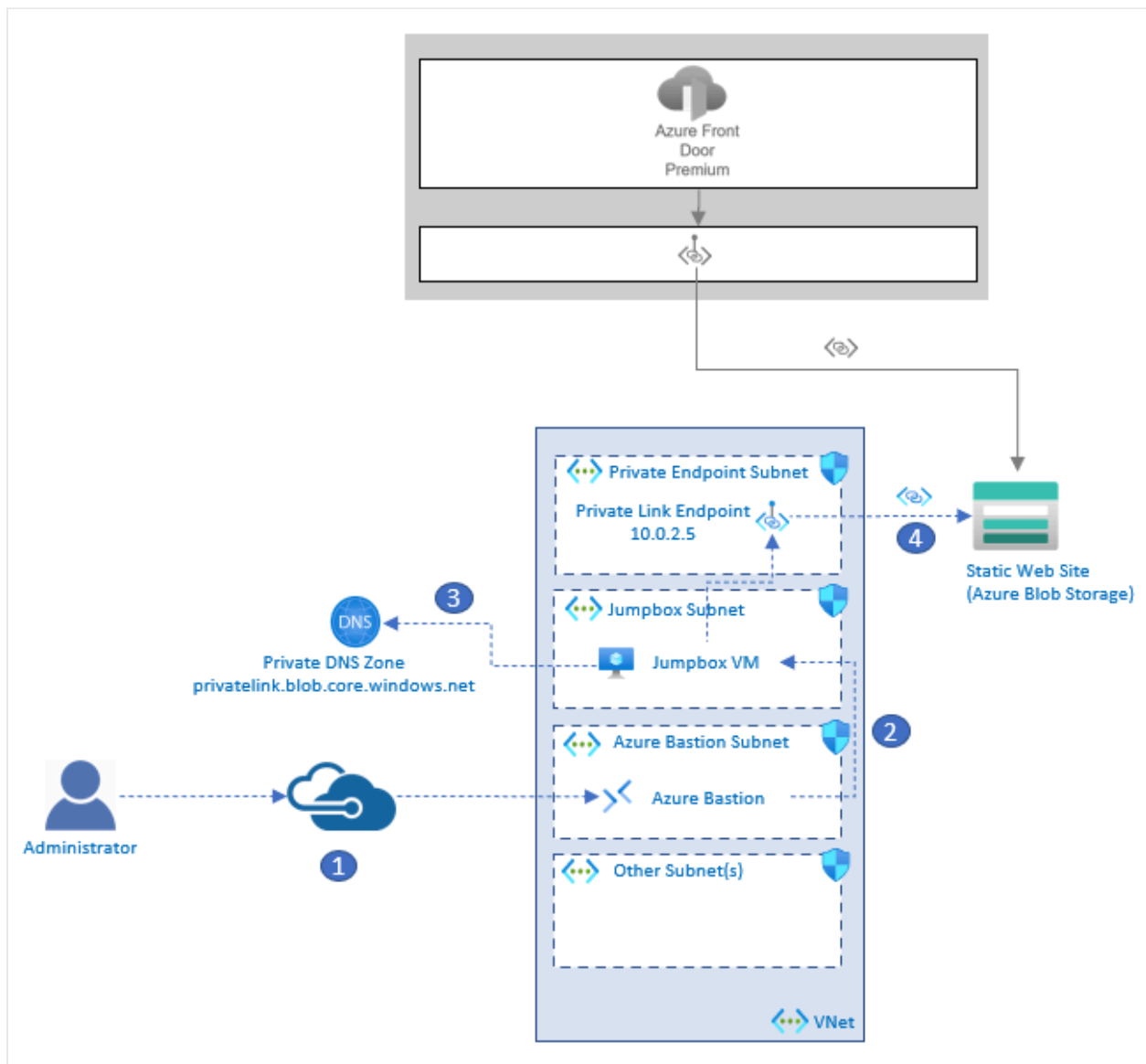
1. The user issues an HTTP or HTTPS request to an Azure Front Door endpoint.
2. The WAF rules are evaluated. Rules that match are always logged. If the Azure Front Door WAF policy mode is set to *prevention* and the matching rule has an action set to *block on anomaly*, the request is blocked. Otherwise, the request continues or is redirected, or the subsequent rules are evaluated.
3. The route configured in Azure Front Door is matched and the correct origin group is selected. In this example, the path was to the static content in the website.
4. The origin is selected from the origin group.
  - a. In this example, the health probes deemed the website unhealthy, so it's eliminated from the possible origins.

b. This website is selected.

- The request is routed to the Azure storage account via Private Link over the Microsoft backbone network.

For more information about the Azure Front Door routing architecture, see [Routing architecture overview](#).

## Operational flow



- An administrator connects to the Azure Bastion instance that's deployed in the virtual network.
- Azure Bastion provides SSH connectivity to the jumpbox VM.
- The administrator on the jumpbox tries to access the storage account via the Azure CLI. The jumpbox queries DNS for the public Azure Blob Storage account endpoint: `storageaccountname.blob.core.windows.net`.

Private DNS ultimately resolves to

`storageaccountname.privatelink.blob.core.windows.net`. It returns the private IP address of the Private Link endpoint, which is 10.0.2.5 in this example.

4. A private connection to the storage account is established through the Private Link endpoint.

## Considerations

Keep the following points in mind when you use this solution.

### Reliability

Reliability ensures that your application can meet the commitments that you make to your customers. For more information, see [Overview of the reliability pillar](#).

This scenario addresses the following key points about reliability:

- Global routing with low latency, through the use of health probes, enables reliability by insulating the application against regional outages.
- [Web Application Firewall on Azure Front Door](#) provides centralized protection for HTTP and HTTPS requests.

### Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see [Overview of the security pillar](#).

This scenario addresses the following key points about security:




- [Private Link support in Azure Front Door Premium](#) eliminates the need to expose your internal or PaaS services over the internet. Private Link allows Azure Front Door to communicate to your private services or PaaS services over the Microsoft backbone network.
- [Web Application Firewall on Azure Front Door](#) provides centralized protection for HTTP and HTTPS requests.
- [Managed rules in Web Application Firewall Premium](#) are Microsoft-managed rules that help protect you against a common set of security threats.

### Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).



Although both Azure Front Door Premium and Web Application Firewall Premium provide advanced security features over the Standard tier, there's additional cost to both. Review the following resources to learn more about pricing for Azure Front Door and Web Application Firewall:

- [Azure Front Door pricing](#) 
- [Web Application Firewall pricing](#) 
- [Azure pricing calculator](#) 


## Operational excellence

Operational excellence covers the operations processes that deploy an application and keep it running in production. For more information, see [Overview of the operational excellence pillar](#).

Implementing network security boundaries adds complexity to operations and deployment. Keep these points in mind:

- The [IP ranges for Microsoft-hosted agents vary over time](#). Consider implementing self-hosted agents in your virtual network.
- Implement [Azure Bastion](#) for scenarios where operations teams need to access network secure resources.
- The use of [Web Application Firewall on Azure Front Door](#) to provide centralized protection for HTTP and HTTPS requests is an example of the gateway offloading pattern. The responsibility of examining requests for exploits is offloaded to Web Application Firewall in Azure Front Door. The benefit from an operational excellence perspective is that you need to manage the rules in only one place.

### Important


The [network secure ingress sample](#)  allows you to deploy all of the resources required for you to connect to a jumpbox through Azure Bastion and connect to a network secure VM.

## Performance efficiency

Performance efficiency is the ability of your workload to scale to meet the demands that users place on it. For more information, see [Overview of the performance efficiency pillar](#).

Global routing enables horizontal scaling through the deployment of more resources in the same region or different regions.

## Next steps

- Deploy this implementation by following the steps outlined in the [network secured ingress sample](#) .

---

## Feedback

Was this page helpful?

 Yes

 No