Introduction

Azure Private Endpoint is the fundamental building block for Azure Private Link. Private endpoints enable Azure resources deployed in a virtual network to communicate privately with private link resources.

Private endpoints allow resources access to the private link service deployed in a virtual network. Access to the private endpoint through virtual network peering and on-premises network connections extend the connectivity.

Note

If you want to secure traffic to private endpoints in Azure Virtual WAN using secured virtual hub, see Secure traffic destined to private endpoints in Azure Virtual WAN.

You may need to inspect or block traffic from clients to the services exposed via private endpoints. Complete this inspection by using Azure Firewall or a third-party network virtual appliance.

The following limitations apply:

• Network security groups (NSG) are bypassed by traffic coming from private endpoints

• User-defined routes (UDR) are bypassed by traffic coming from private endpoints. User-defined routes can be used to override traffic destined for the private endpoint.

• A single route table can be attached to a subnet

• A route table supports up to 400 routes

Azure Firewall filters traffic using either:

• FQDN in network rules for TCP and UDP protocols

• FQDN in application rules for HTTP, HTTPS, and MSSQL.

Important

The use of application rules over network rules is recommended when inspecting traffic destined to private endpoints in order to maintain flow symmetry. If network rules are used, or an NVA is used instead of Azure Firewall, SNAT must be configured for traffic destined to private endpoints.

Note

SQL FQDN filtering is supported in proxy-mode only (port 1433). Proxy mode can result in more latency compared to redirect. If you want to continue using redirect mode, which is the default for clients connecting within Azure, you can filter access using FQDN in firewall network rules.

Scenario 1: Hub and spoke architecture - Dedicated virtual network for private endpoints

This scenario is the most expandable architecture to connect privately to multiple Azure services using private endpoints. A route pointing to the network address space where the private endpoints are deployed is created. This configuration reduces administrative overhead and prevents running into the limit of 400 routes.

Connections from a client virtual network to the Azure Firewall in a hub virtual network will incur charges if the virtual networks are peered. Connections from Azure Firewall in a hub virtual network to private endpoints in a peered virtual network are not charged.

For more information on charges related to connections with peered virtual networks, see the FAQ section of the pricing page.

Scenario 2: Hub and spoke architecture - Shared virtual network for private endpoints and virtual machines

This scenario is implemented when:

• It's not possible to have a dedicated virtual network for the private endpoints

• When only a few services are exposed in the virtual network using private endpoints

The virtual machines will have /32 system routes pointing to each private endpoint. One route per private endpoint is configured to route traffic through Azure Firewall.

The administrative overhead of maintaining the route table increases as services are exposed in the virtual network. The possibility of hitting the route limit also increases.

Depending on your overall architecture, it's possible to run into the 400 routes limit. It's recommended to use scenario 1 whenever possible.

Connections from a client virtual network to the Azure Firewall in a hub virtual network will incur charges if the virtual networks are peered. Connections from Azure Firewall in a hub virtual network to private endpoints in a peered virtual network are not charged.

For more information on charges related to connections with peered virtual networks, see the FAQ section of the pricing page.

Scenario 3: Single virtual network

Use this pattern when a migration to a hub and spoke architecture isn't possible. The same considerations as in scenario 2 apply. In this scenario, virtual network peering charges don't apply.

Scenario 4: On-premises traffic to private endpoints

This architecture can be implemented if you have configured connectivity with your on-premises network using either:

• ExpressRoute

• Site to Site VPN

If your security requirements require client traffic to services exposed via private endpoints to be routed through a security appliance, deploy this scenario.

The same considerations as in scenario 2 above apply. In this scenario, there aren't virtual network peering charges. For more information about how to configure your DNS servers to allow on-premises workloads to access private endpoints, see On-Premises workloads using a DNS forwarder.