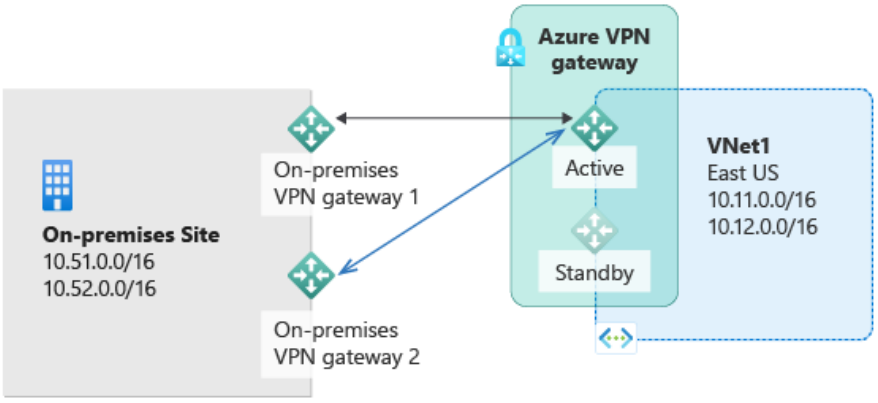
Redundancy of Gateways

Index

Highly Available cross-premises

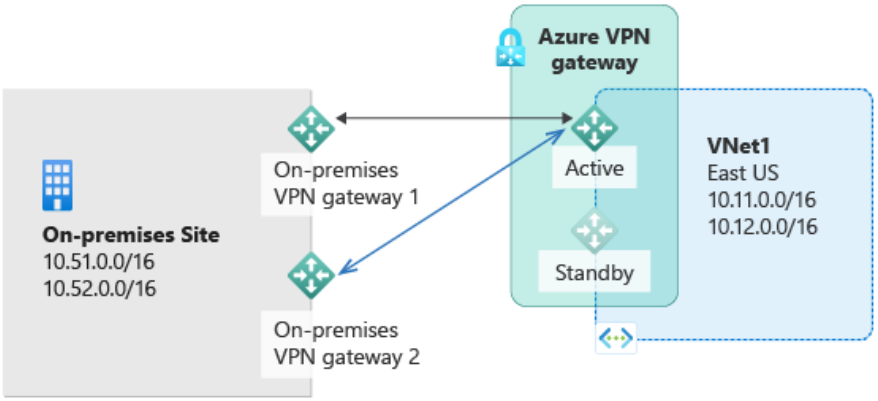
- To provide better availability for your `#VPN_gateway/cross-premises-connections`, there are a few options available:
  - Multiple on-premises VPN devices
  - Active-active Azure VPN gateway
  - Combination of both

Multiple on-premises VPN devices



- You can use multiple VPN devices from your on-premises network to connect to your Azure VPN gateway.
- This configuration provides multiple active tunnels from the same Azure VPN gateway to your on-premises devices in the same location.
  1. You need to create multiple S2S VPN connections from your VPN devices to Azure. When you connect multiple VPN devices from the same on-premises network to Azure, you need to create one local network gateway for each VPN device, and one connection from your Azure VPN gateway to each local network gateway.
  2. The local network gateways corresponding to your VPN devices must have unique public IP addresses in the "GatewayIpAddress" property.
  3. BGP is required for this configuration. Each local network gateway representing a VPN device must have a unique BGP peer IP address specified in the "BgpPeerIpAddress" property.
  4. You should use BGP to advertise the same prefixes of the same on-premises network prefixes to your Azure VPN gateway, and the traffic will be forwarded through these tunnels simultaneously.
  5. You must use Equal-cost multi-path routing (ECMP).
  6. Each connection is counted against the maximum number of tunnels for your Azure VPN gateway. See the VPN Gateway settings page for the latest information about tunnels, connections, and throughput.

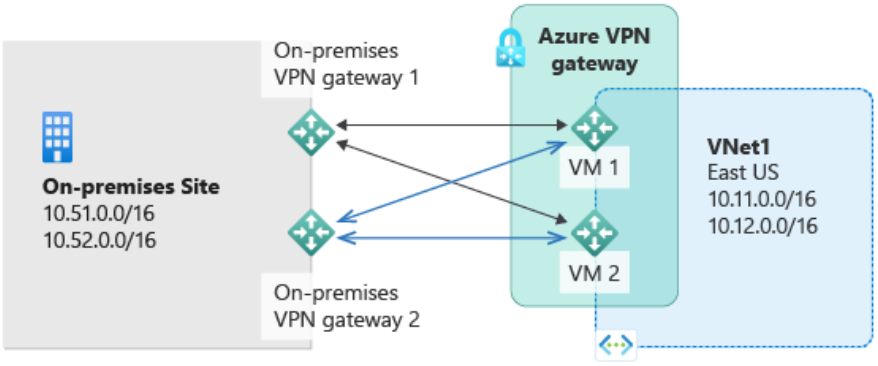
Active-active VPN gateways



- each Azure gateway instance has a unique public IP address.
- each will establish an IPsec/IKE S2S VPN tunnel to your on-premises VPN device specified in your local network gateway and connection.
- Note that both VPN tunnels are actually part of the same connection.
- You'll still need to configure your on-premises VPN device to accept or establish two S2S VPN tunnels to those two Azure VPN gateway public IP addresses.

- Because the Azure gateway instances are in active-active configuration, the traffic from your Azure virtual network to your on-premises network will be routed through both tunnels simultaneously.
- even if your on-premises VPN device may favor one tunnel over the other. For a single TCP or UDP flow, Azure attempts to use the same tunnel when sending packets to your on-premises network. However, your on-premises network could use a different tunnel to send packets to Azure.

Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks



- The most reliable option is to combine the active-active gateways on both your network and Azure.
- Here you create and set up the Azure VPN gateway in an active-active configuration.
- create two local network gateways and two connections for your two on-premises VPN devices.
- The result is a full **mesh connectivity** of 4 IPsec tunnels between your Azure virtual network and your on-premises network.

- All gateways and tunnels are active from the Azure side, so the traffic is spread among all 4 tunnels simultaneously
- The primary goal of this configuration is for **high availability**

- This topology requires two local network gateways and two connections to support the pair of on-premises VPN devices.
- BGP is required to allow the two connections to the same on-premises network.