VNet Connectivity scenarios

Vnet connectivity scenarios

Azure Infrastructure

Virtual Network

Point to Site (P2S) VPN

Remote Users

VPN Gateway

Gateway Subnet

Peering — Virtual Network Same region

Global peering — Virtual Network Different region

Site to Site VPN — On-premise data centre

Express Route
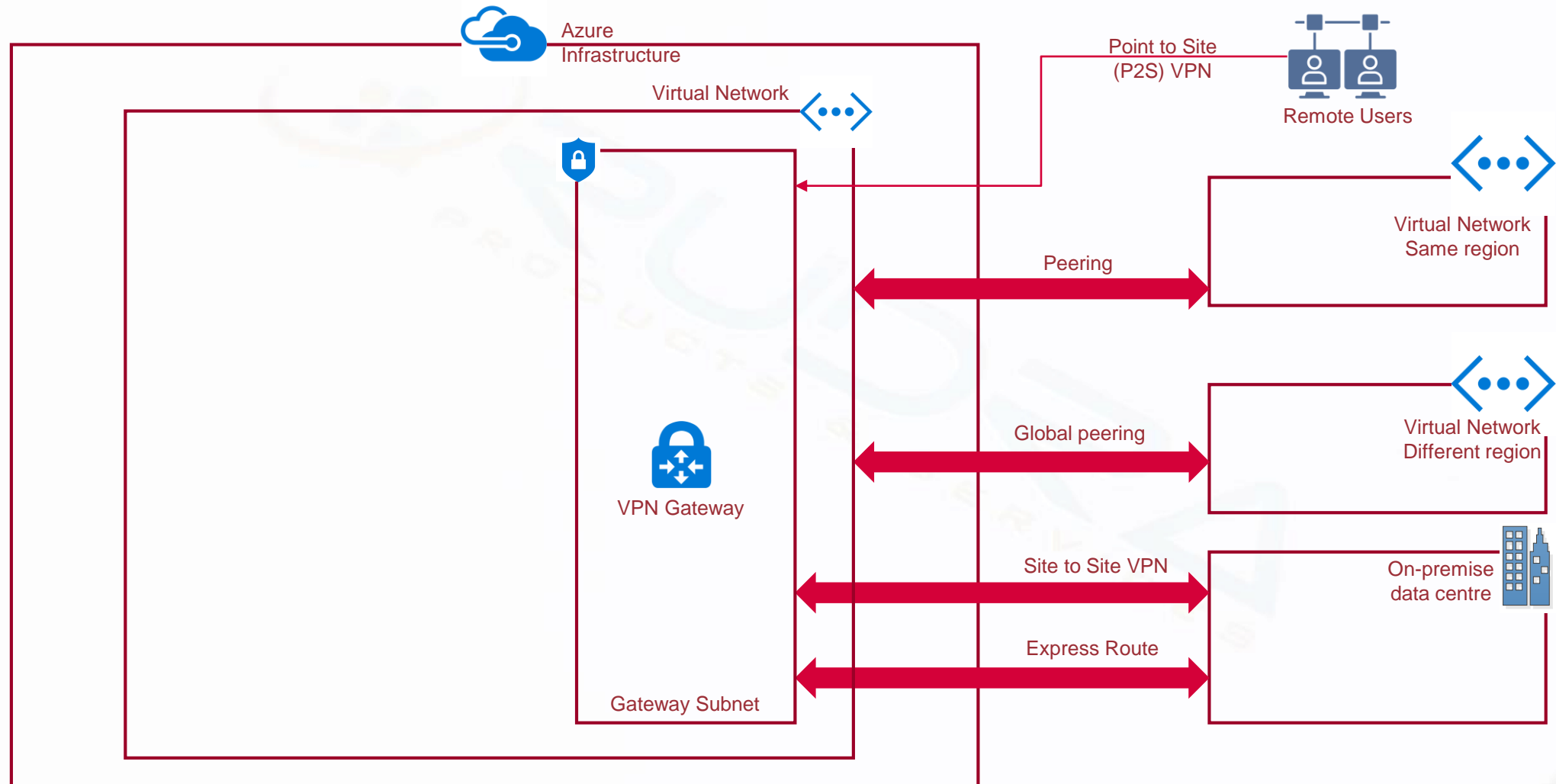
Peering

Virtual network peering enables you to connect two Vnets in the same (VNet peering) or across regions (Global VNet peering).
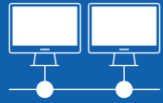
Connectivity

"Seamless connectivity"

› The traffic between virtual machines in peered virtual networks is routed directly through the Microsoft backbone infrastructure, not through a gateway or over the public Internet.

› Network security groups can be applied in either virtual network to block access to other virtual networks or subnets, if desired.

Service chaining

"Hub and spoke"

› You can deploy hub-and-spoke networks, where the hub virtual network can host infrastructure components such as a network virtual appliance or VPN gateway

› All the spoke virtual networks can then peer with the hub virtual network. Traffic can flow through network virtual appliances or VPN gateways in the hub virtual network.

Gateway and on-premise connectivity

"Gateway transit"

› When virtual networks are peered, you can also configure the gateway in the peered virtual network as a transit point to an on-premises network.

› Gateway transit is supported for both VNet Peering and Global VNet Peering.

Peering scenarios

- Peering between VNets in same subscription is allowed

- Peering between VNets in different subscriptions under the same AD tenant is allowed

- Peering between VNets in different subscription located in different AD tenants are also allowed