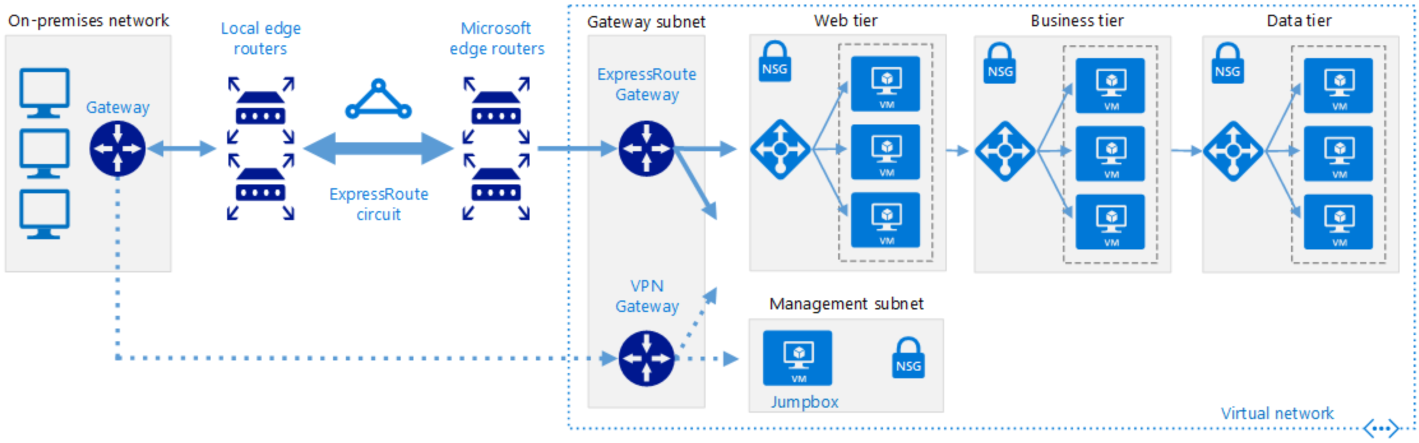
Connect an on-premises network to Azure using ExpressRoute with VPN failover

10/22/2017 • 4 minutes to read • Contributors all

In this article

This reference architecture shows how to connect an on-premises network to an Azure virtual network (VNet) using ExpressRoute, with a site-to-site virtual private network (VPN) as a failover connection. Traffic flows between the on-premises network and the Azure VNet through an ExpressRoute connection. If there is a loss of connectivity in the ExpressRoute circuit, traffic is routed through an IPSec VPN tunnel. **Deploy this solution**.

Note that if the ExpressRoute circuit is unavailable, the VPN route will only handle private peering connections. Public peering and Microsoft peering connections will pass over the Internet.



Download a Visio file of this architecture.

Architecture

The architecture consists of the following components.

- **On-premises network**. A private local-area network running within an organization.
- **VPN appliance**. A device or service that provides external connectivity to the on-premises network. The VPN appliance may be a hardware device, or it can be a software solution such as the Routing and Remote Access Service (RRAS) in Windows Server 2012. For a list of supported VPN appliances and information on configuring selected VPN appliances for connecting to Azure, see About VPN devices for Site-to-Site VPN Gateway connections.
- **ExpressRoute circuit**. A layer 2 or layer 3 circuit supplied by the connectivity provider that joins the on-premises network with Azure through the edge routers. The circuit uses the hardware infrastructure managed by the connectivity provider.
- **ExpressRoute virtual network gateway**. The ExpressRoute virtual network gateway enables the VNet to connect to the ExpressRoute circuit used for connectivity with your on-premises network.

- **VPN virtual network gateway**. The VPN virtual network gateway enables the VNet to connect to the VPN appliance in the on-premises network. The VPN virtual network gateway is configured to accept requests from the on-premises network only through the VPN appliance. For more information, see Connect an on-premises network to a Microsoft Azure virtual network.

- **VPN connection**. The connection has properties that specify the connection type (IPSec) and the key shared with the on-premises VPN appliance to encrypt traffic.

- **Azure Virtual Network (VNet)**. Each VNet resides in a single Azure region, and can host multiple application tiers. Application tiers can be segmented using subnets in each VNet.

- **Gateway subnet**. The virtual network gateways are held in the same subnet.

- **Cloud application**. The application hosted in Azure. It might include multiple tiers, with multiple subnets connected through Azure load balancers. For more information about the application infrastructure, see Running Windows VM workloads and Running Linux VM workloads.

Recommendations

The following recommendations apply for most scenarios. Follow these recommendations unless you have a specific requirement that overrides them.

VNet and GatewaySubnet

Create the ExpressRoute virtual network gateway and the VPN virtual network gateway in the same VNet. This means that they should share the same subnet named *GatewaySubnet*.

If the VNet already includes a subnet named *GatewaySubnet*, ensure that it has a /27 or larger address space. If the existing subnet is too small, use the following PowerShell command to remove the subnet:

PowerShell Copy

```powershell
$vnet = Get-AzureRmVirtualNetworkGateway -Name <yourvnetname> -ResourceGroupName <yourresource-group>
Remove-AzureRmVirtualNetworkSubnetConfig -Name GatewaySubnet -VirtualNetwork $vnet
```

If the VNet does not contain a subnet named **GatewaySubnet**, create a new one using the following PowerShell command:

PowerShell Copy

```powershell
$vnet = Get-AzureRmVirtualNetworkGateway -Name <yourvnetname> -ResourceGroupName <yourresource-group>
Add-AzureRmVirtualNetworkSubnetConfig -Name "GatewaySubnet" -VirtualNetwork $vnet -AddressPrefix "10.200.255.224/27"
$vnet = Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
```

VPN and ExpressRoute gateways

Verify that your organization meets the ExpressRoute prerequisite requirements for connecting to Azure.

If you already have a VPN virtual network gateway in your Azure VNet, use the following PowerShell command to remove it:

PowerShell Copy

```
Remove-AzureRmVirtualNetworkGateway -Name <yourgatewayname> -ResourceGroupName
<yourresourcegroup>
```

Follow the instructions in Implementing a hybrid network architecture with Azure ExpressRoute to establish your ExpressRoute connection.

Follow the instructions in Implementing a hybrid network architecture with Azure and On-premises VPN to establish your VPN virtual network gateway connection.

After you have established the virtual network gateway connections, test the environment as follows:

1. Make sure you can connect from your on-premises network to your Azure VNet.
2. Contact your provider to stop ExpressRoute connectivity for testing.
3. Verify that you can still connect from your on-premises network to your Azure VNet using the VPN virtual network gateway connection.
4. Contact your provider to reestablish ExpressRoute connectivity.

Considerations

For ExpressRoute considerations, see the Implementing a Hybrid Network Architecture with Azure ExpressRoute guidance.

For site-to-site VPN considerations, see the Implementing a Hybrid Network Architecture with Azure and On-premises VPN guidance.

For general Azure security considerations, see Microsoft cloud services and network security.

Deploy the solution

Prerequisites. You must have an existing on-premises infrastructure already configured with a suitable network appliance.

To deploy the solution, perform the following steps.

1. Click the link below.

   Deploy to Azure

2. Wait for the link to open in the Azure portal, then follow these steps:

   - The **Resource group** name is already defined in the parameter file, so select **Create New** and enter `ra-hybrid-vpn-er-rg` in the text box.
   - Select the region from the **Location** drop down box.
   - Do not edit the **Template Root Uri** or the **Parameter Root Uri** text boxes.
   - Review the terms and conditions, then click the **I agree to the terms and conditions stated above** checkbox.
   - Click the **Purchase** button.

3. Wait for the deployment to complete.

4. Click the link below.

   Deploy to Azure

5. Wait for the link to open in the Azure portal, then enter then follow these steps:

- Select **Use existing** in the **Resource group** section and enter `ra-hybrid-vpn-er-rg` in the text box.
- Select the region from the **Location** drop down box.
- Do not edit the **Template Root Uri** or the **Parameter Root Uri** text boxes.
- Review the terms and conditions, then click the **I agree to the terms and conditions stated above** checkbox.
- Click the **Purchase** button.