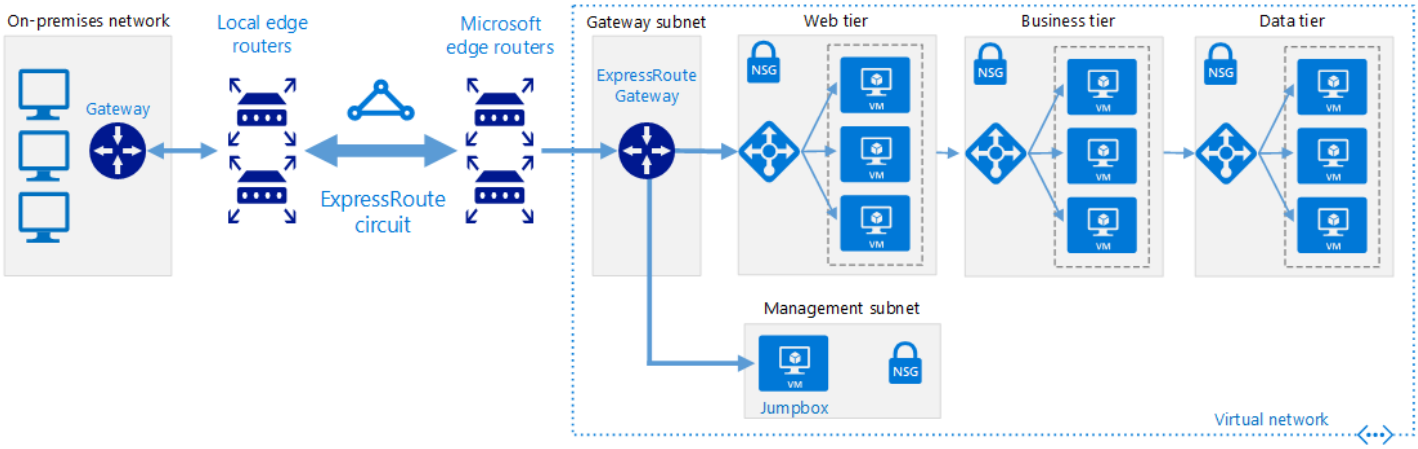
Connect an on-premises network to Azure using ExpressRoute

10/22/2017 • 12 minutes to read • Contributors all

In this article

This reference architecture shows how to connect an on-premises network to virtual networks on Azure, using Azure ExpressRoute. ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. The private connection extends your on-premises network into Azure. Deploy this solution.



Download a Visio file of this architecture.

Architecture

The architecture consists of the following components.

- **On-premises corporate network**. A private local-area network running within an organization.
- **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.
- **Local edge routers**. Routers that connect the on-premises network to the circuit managed by the provider. Depending on how your connection is provisioned, you may need to provide the public IP addresses used by the routers.
- **Microsoft edge routers**. Two routers in an active-active highly available configuration. These routers enable a connectivity provider to connect their circuits directly to their datacenter. Depending on how your connection is provisioned, you may need to provide the public IP addresses used by the routers.

- **Azure virtual networks (VNets)**. Each VNet resides in a single Azure region, and can host multiple application tiers. Application tiers can be segmented using subnets in each VNet.
- **Azure public services**. Azure services that can be used within a hybrid application. These services are also available over the Internet, but accessing them using an ExpressRoute circuit provides low latency and more predictable performance, because traffic does not go through the Internet. Connections are performed using public peering, with addresses that are either owned by your organization or supplied by your connectivity provider.
- **Office 365 services**. The publicly available Office 365 applications and services provided by Microsoft. Connections are performed using Microsoft peering, with addresses that are either owned by your organization or supplied by your connectivity provider. You can also connect directly to Microsoft CRM Online through Microsoft peering.
- **Connectivity providers** (not shown). Companies that provide a connection either using layer 2 or layer 3 connectivity between your datacenter and an Azure datacenter.

Recommendations

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

Connectivity providers

Select a suitable ExpressRoute connectivity provider for your location. To get a list of connectivity providers available at your location, use the following Azure PowerShell command:

PowerShell Copy

```
Get-AzureRmExpressRouteServiceProvider
```

ExpressRoute connectivity providers connect your datacenter to Microsoft in the following ways:

- **Co-located at a cloud exchange**. If you're co-located in a facility with a cloud exchange, you can order virtual cross-connections to Azure through the co-location provider's Ethernet exchange. Co-location providers can offer either layer 2 cross-connections, or managed layer 3 cross-connections between your infrastructure in the co-location facility and Azure.
- **Point-to-point Ethernet connections**. You can connect your on-premises datacenters/offices to Azure through point-to-point Ethernet links. Point-to-point Ethernet providers can offer layer 2 connections, or managed layer 3 connections between your site and Azure.
- **Any-to-any (IPVPN) networks**. You can integrate your wide area network (WAN) with Azure. Internet protocol virtual private network (IPVPN) providers (typically a multiprotocol label switching VPN) offer any-to-any connectivity between your branch offices and datacenters. Azure can be interconnected to your WAN to make it look just like any other branch office. WAN providers typically offer managed layer 3 connectivity.

For more information about connectivity providers, see the ExpressRoute introduction.

ExpressRoute circuit

Ensure that your organization has met the ExpressRoute prerequisite requirements for connecting to Azure.

If you haven't already done so, add a subnet named `GatewaySubnet` to your Azure VNet and create an ExpressRoute virtual network gateway using the Azure VPN gateway service. For more information about this process, see ExpressRoute workflows for circuit provisioning and circuit states.

Create an ExpressRoute circuit as follows:

1. Run the following PowerShell command:

```
PowerShell
New-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>> -Location <<location>> -SkuTier <<sku-tier>> -SkuFamily <<sku-family>> -ServiceProviderName <<service-provider-name>> -PeeringLocation <<peering-location>> -BandwidthInMbps <<bandwidth-in-mbps>>
```

2. Send the `ServiceKey` for the new circuit to the service provider.

3. Wait for the provider to provision the circuit. To verify the provisioning state of a circuit, run the following PowerShell command:

```
PowerShell
Get-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>>
```

   The `Provisioning state` field in the `Service Provider` section of the output will change from `NotProvisioned` to `Provisioned` when the circuit is ready.

   > **Note**
   >
   > If you're using a layer 3 connection, the provider should configure and manage routing for you. You provide the information necessary to enable the provider to implement the appropriate routes.

4. If you're using a layer 2 connection:

   a. Reserve two /30 subnets composed of valid public IP addresses for each type of peering you want to implement. These /30 subnets will be used to provide IP addresses for the routers used for the circuit. If you are implementing private, public, and Microsoft peering, you'll need 6 /30 subnets with valid public IP addresses.

   b. Configure routing for the ExpressRoute circuit. Run the following PowerShell commands for each type of peering you want to configure (private, public, and Microsoft). For more information, see Create and modify routing for an ExpressRoute circuit.

```
PowerShell
Set-AzureRmExpressRouteCircuitPeeringConfig -Name <<peering-name>> -Circuit <<circuit-name>> -PeeringType <<peering-type>> -PeerASN <<peer-asn>> -PrimaryPeerAddressPrefix <<primary-peer-address-prefix>> -SecondaryPeerAddressPrefix <<secondary-peer-address-prefix>> -VlanId <<vlan-id>>

Set-AzureRmExpressRouteCircuit -ExpressRouteCircuit <<circuit-name>>
```

   c. Reserve another pool of valid public IP addresses to use for network address translation (NAT) for public and Microsoft peering. It is recommended to have a different pool for each peering. Specify the pool to your connectivity provider, so they can configure border gateway protocol (BGP) advertisements for those ranges.

5. Run the following PowerShell commands to link your private VNet(s) to the ExpressRoute circuit. For more information,see Link a virtual network to an ExpressRoute circuit.

```
PowerShell
```

```
$circuit = Get-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<re-
source-group>>
$gw = Get-AzureRmVirtualNetworkGateway -Name <<gateway-name>> -ResourceGroupName <<re-
source-group>>
New-AzureRmVirtualNetworkGatewayConnection -Name <<connection-name>> -ResourceGroupName
<<resource-group>> -Location <<location> -VirtualNetworkGateway1 $gw -PeerId $circuit.Id -
ConnectionType ExpressRoute
```

You can connect multiple VNets located in different regions to the same ExpressRoute circuit, as long as all VNets and the ExpressRoute circuit are located within the same geopolitical region.

Troubleshooting

If a previously functioning ExpressRoute circuit now fails to connect, in the absence of any configuration changes on-premises or within your private VNet, you may need to contact the connectivity provider and work with them to correct the issue. Use the following PowerShell commands to verify that the ExpressRoute circuit has been provisioned:

PowerShell Copy

```
Get-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>>
```

The output of this command shows several properties for your circuit, including `ProvisioningState`, `CircuitProvisioningState`, and `ServiceProviderProvisioningState` as shown below.

PowerShell Copy

```
ProvisioningState                : Succeeded
Sku                              : {
                                     "Name": "Standard_MeteredData",
                                     "Tier": "Standard",
                                     "Family": "MeteredData"
                                   }
CircuitProvisioningState         : Enabled
ServiceProviderProvisioningState : NotProvisioned
```

If the `ProvisioningState` is not set to `Succeeded` after you tried to create a new circuit, remove the circuit by using the command below and try to create it again.

PowerShell Copy

```
Remove-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>>
```

If your provider had already provisioned the circuit, and the `ProvisioningState` is set to `Failed`, or the `CircuitProvisioningState` is not `Enabled`, contact your provider for further assistance.

Scalability considerations

ExpressRoute circuits provide a high bandwidth path between networks. Generally, the higher the bandwidth the greater the cost.

ExpressRoute offers two pricing plans to customers, a metered plan and an unlimited data plan. Charges vary according to circuit bandwidth. Available bandwidth will likely vary from provider to provider. Use the `Get-AzureRmExpressRouteServiceProvider` cmdlet to see the providers available in your region and the bandwidths that they offer.

A single ExpressRoute circuit can support a certain number of peerings and VNet links. See ExpressRoute limits for more information.

For an extra charge, the ExpressRoute Premium add-on provides some additional capability:

- Increased route limits for public and private peering.
- Increased number of VNet links per ExpressRoute circuit.
- Global connectivity for services.

See ExpressRoute pricing for details.

ExpressRoute circuits are designed to allow temporary network bursts up to two times the bandwidth limit that you procured for no additional cost. This is achieved by using redundant links. However, not all connectivity providers support this feature. Verify that your connectivity provider enables this feature before depending on it.

Although some providers allow you to change your bandwidth, make sure you pick an initial bandwidth that surpasses your needs and provides room for growth. If you need to increase bandwidth in the future, you are left with two options:

- Increase the bandwidth. You should avoid this option as much as possible, and not all providers allow you to increase bandwidth dynamically. But if a bandwidth increase is needed, check with your provider to verify they support changing ExpressRoute bandwidth properties via PowerShell commands. If they do, run the commands below.

  PowerShell Copy

  ```
  $ckt = Get-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>>
  $ckt.ServiceProviderProperties.BandwidthInMbps = <<bandwidth-in-mbps>>
  Set-AzureRmExpressRouteCircuit -ExpressRouteCircuit $ckt
  ```

  You can increase the bandwidth without loss of connectivity. Downgrading the bandwidth will result in disruption in connectivity, because you must delete the circuit and recreate it with the new configuration.

- Change your pricing plan and/or upgrade to Premium. To do so, run the following commands. The `Sku.Tier` property can be `Standard` or `Premium`; the `Sku.Name` property can be `MeteredData` or `UnlimitedData`.

  PowerShell Copy

  ```
  $ckt = Get-AzureRmExpressRouteCircuit -Name <<circuit-name>> -ResourceGroupName <<resource-group>>

  $ckt.Sku.Tier = "Premium"
  $ckt.Sku.Family = "MeteredData"
  $ckt.Sku.Name = "Premium_MeteredData"

  Set-AzureRmExpressRouteCircuit -ExpressRouteCircuit $ckt
  ```

  Important

  Make sure the `Sku.Name` property matches the `Sku.Tier` and `Sku.Family`. If you change the family and tier, but not the name, your connection will be disabled.

  You can upgrade the SKU without disruption, but you cannot switch from the unlimited pricing plan to metered. When downgrading the SKU, your bandwidth consumption must remain within the default limit of the standard SKU.

Availability considerations

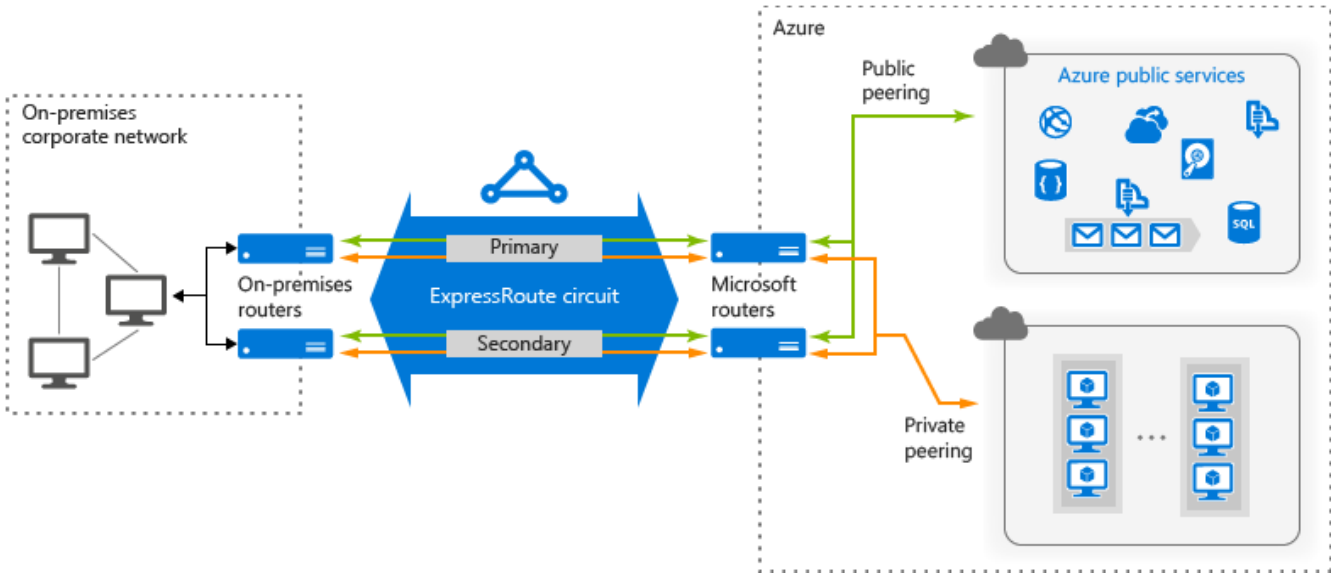
ExpressRoute does not support router redundancy protocols such as hot standby routing protocol (HSRP) and virtual router redundancy protocol (VRRP) to implement high availability. Instead, it uses a redundant pair of BGP sessions per peering. To facilitate highly-available connections to your network, Azure provisions you with two redundant ports on two routers (part of the Microsoft edge) in an active-active configuration.

By default, BGP sessions use an idle timeout value of 60 seconds. If a session times out three times (180 seconds total), the router is marked as unavailable, and all traffic is redirected to the remaining router. This 180-second timeout might be too long for critical applications. If so, you can change your BGP time-out settings on the on-premises router to a smaller value.

You can configure high availability for your Azure connection in different ways, depending on the type of provider you use, and the number of ExpressRoute circuits and virtual network gateway connections you're willing to configure. The following summarizes your availability options:

- If you're using a layer 2 connection, deploy redundant routers in your on-premises network in an active-active configuration. Connect the primary circuit to one router, and the secondary circuit to the other. This will give you a highly available connection at both ends of the connection. This is necessary if you require the ExpressRoute service level agreement (SLA). See SLA for Azure ExpressRoute for details.

  The following diagram shows a configuration with redundant on-premises routers connected to the primary and secondary circuits. Each circuit handles the traffic for a public peering and a private peering (each peering is designated a pair of /30 address spaces, as described in the previous section).



- If you're using a layer 3 connection, verify that it provides redundant BGP sessions that handle availability for you.
- Connect the VNet to multiple ExpressRoute circuits, supplied by different service providers. This strategy provides additional high-availability and disaster recovery capabilities.
- Configure a site-to-site VPN as a failover path for ExpressRoute. For more about this option, see Connect an on-premises network to Azure using ExpressRoute with VPN failover. This option only applies to private peering. For Azure and Office 365 services, the Internet is the only failover path.

Manageability considerations

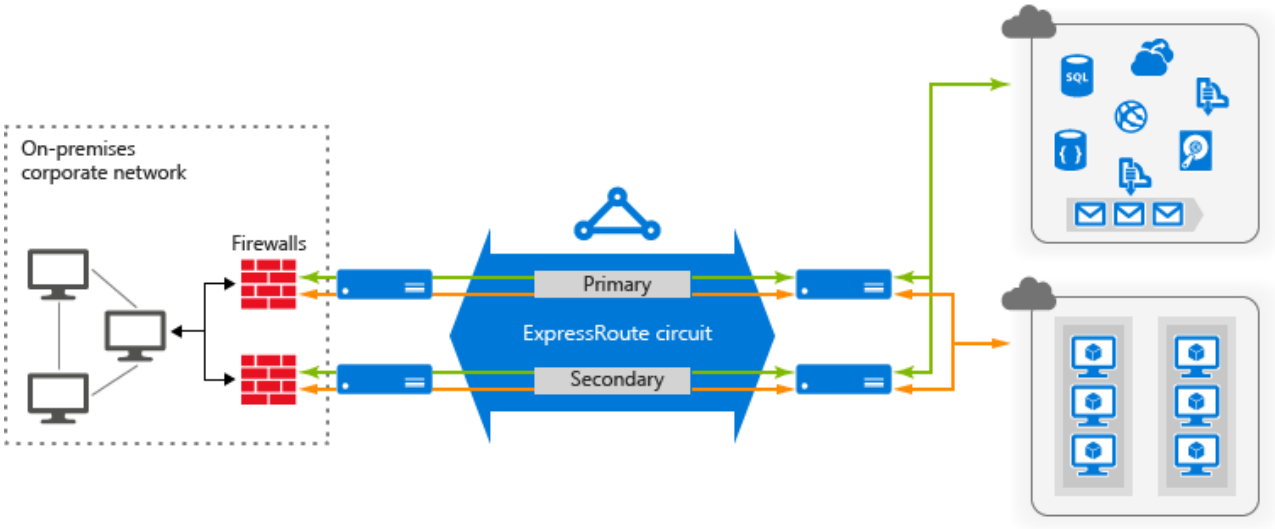
You can use the Azure Connectivity Toolkit (AzureCT) to monitor connectivity between your on-premises datacenter and Azure.

Security considerations

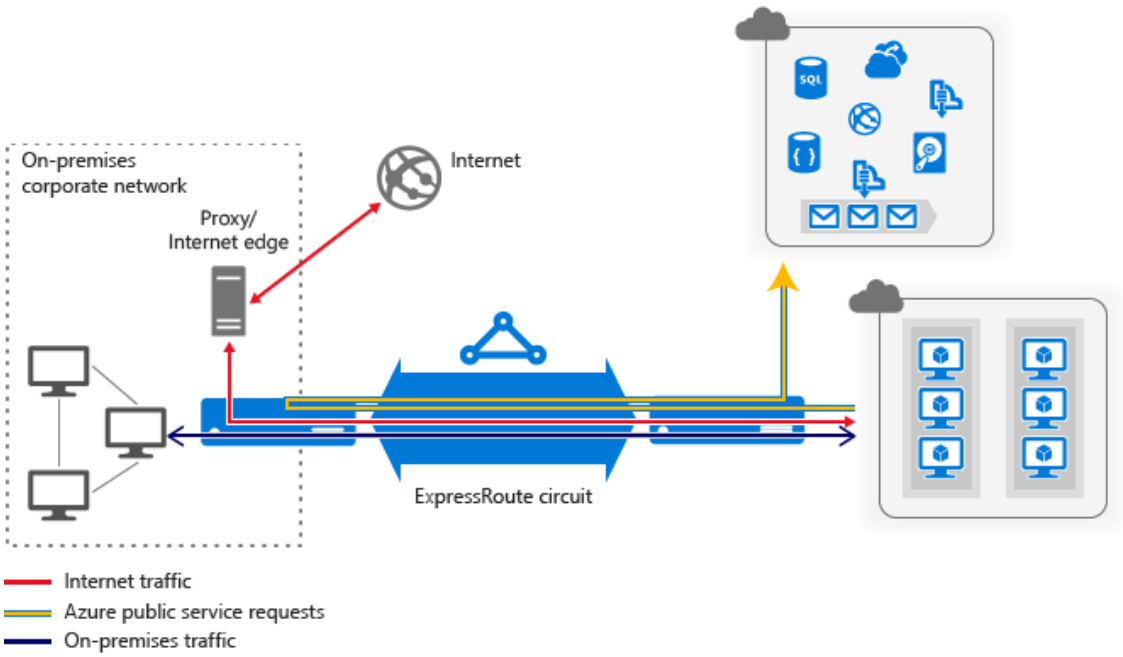
You can configure security options for your Azure connection in different ways, depending on your security concerns and compliance needs.

ExpressRoute operates in layer 3. Threats in the application layer can be prevented by using a network security appliance that restricts traffic to legitimate resources. Additionally, ExpressRoute connections using public peering can only be initiated from on-premises. This prevents a rogue service from accessing and compromising on-premises data from the Internet.

To maximize security, add network security appliances between the on-premises network and the provider edge routers. This will help to restrict the inflow of unauthorized traffic from the VNet:



For auditing or compliance purposes, it may be necessary to prohibit direct access from components running in the VNet to the Internet and implement forced tunneling. In this situation, Internet traffic should be redirected back through a proxy running on-premises where it can be audited. The proxy can be configured to block unauthorized traffic flowing out, and filter potentially malicious inbound traffic.



To maximize security, do not enable a public IP address for your VMs, and use NSGs to ensure that these VMs aren't publicly accessible. VMs should only be available using the internal IP address. These addresses can be made accessible through the ExpressRoute network, enabling on-premises DevOps staff to perform configuration or maintenance.

If you must expose management endpoints for VMs to an external network, use NSGs or access control lists to restrict the visibility of these ports to an allowed list of IP addresses or networks.

> **Note**

By default, Azure VMs deployed through the Azure portal include a public IP address that provides login access.

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.

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-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.

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

   - Select **Use existing** in the **Resource group** section and enter `ra-hybrid-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.

6. Wait for the deployment to complete.