**Princípios básicos do Microsoft Azure: descrever os principais serviços do Azure**

Depois de concluir este roteiro de aprendizagem, você poderá:

* Entender a variedade de serviços disponíveis no Azure, incluindo computação, rede, armazenamento e banco de dados
* Identificar serviços de virtualização, como Máquinas Virtuais do Azure, Instâncias de Contêiner do Azure, Serviço de Kubernetes do Azure e Área de Trabalho Virtual do Azure
* Comparar os serviços de banco de dados do Azure, como o Azure Cosmos DB, o SQL do Azure, o Banco de Dados do Azure para MySQL, o Banco de Dados do Azure para PostgreSQL e os serviços de Big Data e análise do Azure
* Examinar recursos de rede do Azure, como Redes Virtuais, Gateways de VPN e o ExpressRoute do Azure
* Resumir os serviços de armazenamento do Azure, como Armazenamento de Blobs do Azure, Armazenamento em Disco do Azure e Armazenamento de Arquivos do Azure

Aqui estão os roteiros de aprendizagem desta série:

# Introdução

Suponha que a sua empresa, Tailwind Traders, migrou alguns aplicativos para a nuvem e esteja criando novos. Os servidores que hospedam os dados de produtos e de clientes da Tailwind Traders são baseados no Vale do Silício. Sua empresa também tem várias filiais localizadas em regiões geográficas diferentes. Como parte da sua estratégia de migração, a empresa precisa ser capaz de determinar a abordagem correta para configurar a infraestrutura de rede.



Para ajudar a economizar custos, você convence a sua equipe a migrar o seu site e vários dos outros recursos de rede para a nuvem. Com isso em mente, você precisará fornecer acesso seguro aos dados privados da empresa para cada um de suas filiais. Você deseja saber como o Azure pode ajudar a gerenciar sua rede com mais eficiência. Acontece que gerenciar redes no Azure não é totalmente diferente do gerenciamento de redes locais.

Neste módulo, você saberá mais sobre as diferentes opções de rede do Azure e os cenários em que cada uma é apropriada.

## Objetivos de aprendizagem

Depois de concluir este módulo, você poderá:

* Descrever os principais recursos de rede que estão disponíveis no Azure.
* Descrever os benefícios e o uso da Rede Virtual do Azure, do Gateway de VPN do Azure e do Azure ExpressRoute.

## Pré-requisitos

* Você deve estar familiarizado com a terminologia e os conceitos básicos de rede.
* Ter familiaridade com a computação em nuvem é útil, mas não é necessário.

# Conceitos básicos da Rede Virtual do Azure

A Tailwind Traders tem um datacenter local que você planeja manter, mas deseja usar o Azure para reduzir o tráfego de pico usando VMs (máquinas virtuais) hospedadas no Azure. Você quer manter seu esquema de endereçamento IP e dispositivos de rede existentes, com a garantia de que a transferência de dados seja segura.

Usar a Rede Virtual do Azure para sua rede virtual pode ajudar você a alcançar suas metas.

## **O que é a rede virtual do Azure?**

As *redes virtuais do Azure* permitem que recursos do Azure, como VMs, aplicativos Web e bancos de dados, comuniquem-se uns com os outros, com usuários na Internet e com computadores cliente locais. Pense em uma rede do Azure como um conjunto de recursos que vincula outros recursos do Azure.

As redes virtuais do Azure oferecem as seguintes funcionalidades de rede essenciais:

* Isolamento e segmentação
* Comunicação pela Internet
* Comunicação entre recursos do Azure
* Comunicação com os recursos locais
* Rotear tráfego de rede
* Filtrar tráfego de rede
* Conectar redes virtuais

### **Isolamento e segmentação**

A Rede Virtual permite criar várias redes virtuais isoladas. Quando você configura uma rede virtual, define um espaço de endereço IP privado usando intervalos de endereços IP públicos ou privados. Você pode dividir esse espaço de endereços IP em sub-redes e alocar parte do espaço de endereço definido para cada sub-rede nomeada.

Para a resolução de nomes, é possível usar o serviço de resolução de nomes interno do Azure. Você também pode configurar a rede virtual para usar um servidor DNS interno ou externo.

### **Comunicações com a Internet**

Uma VM no Azure pode se conectar à Internet por padrão. É possível habilitar conexões de entrada da Internet definindo um endereço IP público ou um balanceador de carga público. Para o gerenciamento de VM, você pode se conectar por meio da CLI do Azure, do protocolo RDP ou do Secure Shell.

### **Comunicação entre recursos do Azure**

Convém habilitar recursos do Azure para que se comuniquem entre si com segurança. Você pode fazer isso de duas maneiras:

* **Redes virtuais** As redes virtuais podem conectar não apenas VMs, mas outros recursos do Azure, como o Ambiente do Serviço de Aplicativo para Power Apps, o Serviço de Kubernetes do Azure e os conjuntos de dimensionamento de máquinas virtuais do Azure.
* **Pontos de extremidade de serviço** Você pode usar pontos de extremidade de serviço para se conectar a outros tipos de recursos do Azure, como bancos de dados SQL do Azure e contas de armazenamento. Essa abordagem permite vincular vários recursos do Azure às redes virtuais para melhorar a segurança e fornecer o encaminhamento ideal entre recursos.

### Comunicação com os recursos locais

As redes virtuais do Azure permitem vincular recursos em seu ambiente local e na assinatura do Azure. Na verdade, você pode criar uma rede que abranja os ambientes locais e de nuvem. Há três mecanismos para você obter essa conectividade:

* **Redes virtuais privadas ponto a site** A abordagem típica de uma conexão de VPN (rede virtual privada) é de um computador fora da sua organização, de volta à sua rede corporativa. Nesse caso, o computador cliente inicia uma conexão VPN criptografada para conectar o computador à rede virtual do Azure.
* **Redes virtuais privadas site a site** Uma VPN site a site vincula seu dispositivo VPN ou gateway de VPN local ao Gateway de VPN do Azure em uma rede virtual. Na verdade, os dispositivos no Azure podem aparecer como estando na rede local. A conexão é criptografada e funciona pela Internet.
* **Azure ExpressRoute** No caso de ambientes em que você precisa de maior largura de banda e níveis de segurança ainda mais altos, o Azure ExpressRoute é a melhor abordagem. O ExpressRoute fornece conectividade privada dedicada para o Azure que não passa pela Internet. (Você aprenderá mais sobre o ExpressRoute em outra unidade posteriormente neste módulo.)

### Rotear tráfego de rede

Por padrão, o Azure faz o roteamento de tráfego entre sub-redes em redes virtuais conectadas, em redes locais e na Internet. Você também pode controlar o roteamento e substituir essas configurações da seguinte maneira:

* **Tabelas de rotas** Uma tabela de rotas permite definir regras sobre como o tráfego deve ser direcionado. Você pode criar tabelas de rotas personalizadas que controlam como os pacotes são encaminhados entre as sub-redes.
* **Border Gateway Protocol** O BGP (Border Gateway Protocol) funciona com Gateways de VPN do Azure ou ExpressRoute para propagar as rotas BGP locais para redes virtuais do Azure.

### Filtrar tráfego de rede

As redes virtuais do Azure permitem filtrar o tráfego entre sub-redes usando as seguintes abordagens:

* **Grupos de segurança de rede** Um grupo de segurança de rede é um recurso do Azure que pode conter várias regras de segurança de entrada e saída. Você pode definir essas regras para permitir ou bloquear tráfego com base em fatores como endereço IP de origem e de destino, porta e protocolo.
* **Soluções de virtualização de rede** Uma solução de virtualização de rede é uma VM especializada que pode ser comparada a um dispositivo de rede protegida. Uma solução de virtualização de rede realiza uma função de rede específica, como execução de um firewall ou otimização de WAN (rede de longa distância).

## Conectar redes virtuais

Você pode vincular redes virtuais usando o emparelhamento dessas redes. O emparelhamento permite que os recursos em cada rede virtual se comuniquem entre si. Essas redes virtuais podem estar em regiões separadas, o que permite criar uma rede global interconectada por meio do Azure.

UDR é o roteamento definido pelo usuário. O UDR é uma atualização significativa das Redes Virtuais do Azure, pois permite que os administradores de rede controlem as tabelas de roteamento entre as sub-redes de uma VNet, bem como entre VNets, possibilitando um maior controle sobre o fluxo de tráfego de rede.

Diagrama

Descrição gerada automaticamente

# Configurações de Rede Virtual do Azure

Você pode criar e configurar instâncias da Rede virtual do Azure no portal do Azure, no Azure PowerShell do computador local ou no Azure Cloud Shell.

### **Criar uma rede virtual**

Quando você cria uma Rede Virtual do Azure, pode configurar várias configurações básicas. Você também terá a opção de definir configurações avançadas, como várias sub-redes, proteção de DDoS (ataque de negação de serviço distribuído) e pontos de extremidade de serviço.

Você vai configurar as seguintes configurações para uma rede virtual básica:

* **Nome da rede** O nome da rede deve ser exclusivo em sua assinatura, mas não precisa ser globalmente exclusivo. Crie um nome descritivo que seja fácil de lembrar e de diferenciar de outras redes virtuais.
* **Espaço de endereço** Quando você configura uma rede virtual, define o espaço de endereço interno no formato CIDR (roteamento entre domínios). Esse espaço de endereço deve ser exclusivo dentro de sua assinatura e quaisquer redes às quais você deseje se conectar. Vamos supor que você escolha um espaço de endereço de 10.0.0.0/24 para sua primeira rede virtual. Os endereços definidos nesse espaço variam de 10.0.0.1 a 10.0.0.254. Em seguida, você criará uma segunda rede virtual e escolherá o espaço de endereço 10.0.0.0/8. Os endereços nesse espaço variam de 10.0.0.1 a 10.255.255.254. Alguns dos endereços se sobrepõem e não podem ser usados para as duas redes virtuais. Mas você pode usar 10.0.0.0/16, com endereços que variam de 10.0.0.1 a 10.0.255.254, e 10.1.0.0/16, com endereços que variam de 10.1.0.1 a 10.1.255.254. Você pode atribuir esses espaços de endereço às suas redes virtuais porque não há nenhuma sobreposição de endereços.
* **Assinatura** Só se aplica se você tem várias assinaturas para escolher.
* **Grupo de recursos** Como qualquer outro recurso do Azure, uma rede virtual precisa existir em um grupo de recursos. Você pode selecionar um grupo de recursos existente ou criar um novo.
* **Local** Selecione o local onde você deseja criar a rede virtual.
* **Sub-rede** Em cada intervalo de endereços de rede virtual, você pode criar uma ou mais sub-redes que particionam o espaço de endereço da rede virtual. O roteamento entre sub-redes dependerá das rotas padrão de tráfego. Você também pode definir rotas personalizadas. Como alternativa, você pode definir uma sub-rede que abrange todos os intervalos de endereços das redes virtuais.
* **Proteção contra DDoS** Você pode selecionar a proteção contra DDoS Básica ou Standard. A proteção contra DDoS do Standard é um serviço Premium. Para obter mais informações sobre a proteção contra DDoS do Standard, confira [Visão geral da proteção contra DDoS do Standard do Azure](https://docs.microsoft.com/pt-br/azure/virtual-network/ddos-protection-overview).
* **Pontos de extremidade de serviço** Aqui, você habilita os pontos de extremidade de serviço. Selecione na lista quais pontos de extremidade de serviço do Azure você deseja habilitar. As opções incluem o Azure Cosmos DB, o Barramento de Serviço do Azure, o Azure Key Vault e assim por diante.

### **Definir configurações adicionais**

Depois de criar uma rede virtual, você poderá definir outras configurações. Estão incluídos:

* **Grupo de segurança de rede** Os grupos de segurança de rede têm regras de segurança que permitem filtrar o tipo de tráfego de rede que pode entrar e sair das sub-redes da rede virtual e dos adaptadores de rede. Crie o grupo de segurança de rede separadamente. Associe-o à rede virtual.
* **Tabela do rotas** O Azure cria automaticamente uma tabela de rotas para cada sub-rede dentro de uma rede virtual do Azure e adiciona as rotas de sistema padrão à tabela. Você pode adicionar tabelas de rotas personalizadas para modificar o tráfego entre redes virtuais.

Também é possível corrigir os pontos de extremidade de serviço.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

### **Configurar redes virtuais**

Depois de criar uma rede virtual, você poderá alterar configurações adicionais no painel **Redes virtuais** no portal do Azure. Como alternativa, você pode usar comandos do PowerShell ou comandos no Cloud Shell para fazer alterações.

Você pode examinar e alterar as configurações nos subpainéis adicionais. Essas configurações incluem:

* **Espaços de endereço**: você pode adicionar mais espaços de endereço à definição inicial.
* **Dispositivos conectados**: use a rede virtual para conectar computadores.
* **Sub-redes**: você pode adicionar outras sub-redes.
* **Emparelhamentos**: vincule redes virtuais nas disposições de emparelhamento.

Você também pode monitorar e solucionar problemas de redes virtuais. Ou pode criar um script de automação para gerar a rede virtual atual.

Redes virtuais são mecanismos avançados e altamente configuráveis para conectar entidades no Azure. Você pode conectar recursos do Azure entre si ou aos recursos existentes no local. Você pode isolar, filtrar e rotear o tráfego de rede. O Azure permite que você aumente a segurança onde achar necessário.

# Conceitos básicos do Gateway de VPN do Azure

VPNs usam um túnel criptografado dentro de outra rede. Normalmente, elas são implantadas para conectar duas ou mais redes privadas confiáveis entre si em uma rede não confiável (normalmente a Internet pública). O tráfego é criptografado ao viajar pela rede não confiável para evitar interceptação ou outros ataques.

Para nosso cenário da Tailwind Traders, as VPNs podem permitir que as filiais compartilhem informações confidenciais entre localizações. Por exemplo, digamos que os escritórios na região da Costa Leste da América do Norte precisam acessar os dados particulares do cliente da sua empresa, que estão armazenados em servidores localizados fisicamente na região da Costa Oeste. Uma VPN que conecta os seus escritórios da Costa Leste aos servidores da Costa Oeste permite que a empresa acesse os dados particulares do cliente com segurança.

## **Gateways VPN**

Um gateway de VPN é um tipo de gateway de rede virtual. As instâncias do Gateway de VPN do Azure são implantadas em instâncias da Rede Virtual do Azure e permitem a seguinte conectividade:

* Conecte datacenters locais a redes virtuais por meio de uma conexão *site a site*.
* Conecte dispositivos individuais a redes virtuais por meio de uma conexão *ponto a site*.
* Conecte redes virtuais a outras redes virtuais por meio de uma conexão *rede a rede*.

Diagrama

Descrição gerada automaticamente

Todos os dados transferidos são criptografados em um túnel privado à medida que atravessam a Internet. Você só poderá implantar um gateway de VPN em cada rede virtual, mas poderá usar um gateway para se conectar a vários locais, incluindo outras redes virtuais ou datacenters locais.

Ao implantar um gateway de VPN, você especifica o tipo de VPN: *baseada em política* ou *baseada em rota*. A principal diferença entre esses dois tipos de VPN é como o tráfego a ser criptografado é especificado. No Azure, ambos os tipos de gateways de VPN usam uma chave pré-compartilhada como o único método de autenticação. Ambos os tipos também dependem do protocolo IKE na versão 1 ou na versão 2 e do protocolo IPsec. O IKE é usado para configurar uma associação de segurança (um contrato da criptografia) entre dois pontos de extremidade. Essa associação é passada para o conjunto do IPsec, que criptografa e descriptografa os pacotes de dados encapsulados no túnel VPN.

### **VPNs baseadas em política**

Gateways de VPN baseados em política especificam estaticamente o endereço IP dos pacotes que devem ser criptografados por meio de cada túnel. Esse tipo de dispositivo avalia cada pacote de dados em relação a esses conjuntos de endereços IP para escolher o túnel para o qual o pacote será enviado.

Os principais recursos dos gateways de VPN baseados em políticas no Azure incluem:

* Suporte apenas para IKEv1.
* O uso do *roteamento estático*, em que as combinações de prefixos de endereço de ambas as redes controlam o modo como o tráfego é criptografado e descriptografado por meio do túnel VPN. A origem e o destino das redes por túnel são declarados na política e não precisam ser declarados em tabelas de roteamento.
* As VPNs baseadas em política devem ser usadas em cenários específicos que as exigem, por exemplo, para compatibilidade com os dispositivos VPN locais herdados.

### **VPNs baseadas em rota**

Caso seja muito complicado definir quais endereços IP estão por trás de cada túnel, será possível usar gateways baseados em rota. Com gateways baseados em rota, os túneis IPSec são modelados como uma interface de rede ou uma interface de túnel virtual. O roteamento de IP (protocolos de roteamento dinâmico ou rotas estáticas) decide qual dessas interfaces de túnel usar ao enviar cada pacote. VPNs baseadas em rota são o método preferido para conectar dispositivos locais. Elas são mais resilientes a alterações de topologia, como a criação de novas sub-redes.

Use um gateway de VPN baseado em rota se precisar de qualquer um dos seguintes tipos de conectividade:

* Conexões entre redes virtuais
* Conexões ponto a site
* Conexões multissite
* Coexistência com um gateway do Azure ExpressRoute

Os principais recursos de gateways de VPN baseados em rota no Azure incluem:

* Dá suporte ao IKEv2
* Usa seletores de tráfego any-to-any (curinga)
* Pode usar protocolos de roteamento dinâmico, em que as tabelas de roteamento/encaminhamento direcionam o tráfego para túneis IPsec diferentes. Nesse caso, as redes de origem e de destino não são definidas estaticamente, pois estão em VPNs baseadas em políticas ou mesmo em VPNs baseadas em rota com roteamento estático. Em vez disso, os pacotes de dados são criptografados com base em tabelas de roteamento de rede que são criadas dinamicamente usando protocolos de roteamento como o BGP (Border Gateway Protocol).

## Tamanhos do gateway de VPN

As funcionalidades do seu gateway de VPN são determinadas pelo SKU ou tamanho implantado. Esta tabela mostra as principais funcionalidades de cada SKU disponível.

| **SKU** | **Túneis de site a site/rede a rede** | **Parâmetro de comparação de taxa de transferência agregada** | **Suporte ao BGP (Border Gateway Protocol)** |
| --- | --- | --- | --- |
| Básico [Veja a Observação] | Máximo: 10 | 100 Mbps | Sem suporte |
| VpnGw1/Az | Máximo: 30 | 650 Mbps | Com suporte |
| VpnGw2/Az | Máximo: 30 | 1 Gbps | Com suporte |
| VpnGw3/Az | Máximo: 30 | 1,25 Gbps | Com suporte |

**Observação**

Um Gateway de VPN Básico deve ser usado apenas para cargas de trabalho de Desenvolvimento/Teste. Além disso, não há suporte para migrar do Básico para os SKUs VpnGW1/2/3/Az posteriormente sem precisar remover e reimplantar o gateway

## **Implantar gateways de VPN**

Antes de implantar um gateway de VPN, serão necessários alguns recursos locais e do Azure.

### **Recursos do Azure necessários**

Serão necessários os seguintes recursos do Azure antes que você possa implantar um gateway de VPN operacional:

* **Rede virtual**. Implante uma rede virtual com espaço de endereço suficiente para a sub-rede adicional que será necessária para o gateway de VPN. O espaço de endereço dessa rede virtual não pode se sobrepor à rede local à qual você se conectará. Só é possível implantar um único gateway de VPN em uma rede virtual.
* **GatewaySubnet**. Implante uma sub-rede chamada GatewaySubnet para o gateway de VPN. Use uma máscara de endereço de pelo menos **/27** para garantir que você tenha endereços IP suficientes na sub-rede para crescimento futuro. Não é possível usar essa sub-rede para nenhum outro serviço.
* **Endereço IP público**. Crie um endereço IP público dinâmico do SKU Básico se você estiver usando um gateway sem reconhecimento de zona. Esse endereço fornece um endereço IP roteável público como o destino do dispositivo VPN local. Embora esse endereço IP seja dinâmico, ele não será alterado a menos que você exclua e recrie o gateway de VPN.
* **Gateway de rede local**. Crie um gateway de rede local para definir a configuração da rede local, como onde o gateway de VPN se conectará e a que ele se conectará. Essa configuração inclui o endereço IPv4 público do dispositivo VPN local e as redes roteáveis locais. Essas informações são usadas pelo gateway de VPN para rotear, por meio do túnel IPsec, pacotes destinados a redes locais.
* **Gateway de rede virtual**. Crie o gateway de rede virtual para rotear tráfego entre a rede virtual e o datacenter local ou outras redes virtuais. O gateway de rede virtual pode ser um gateway de VPN ou ExpressRoute, mas esta unidade lida apenas com gateways de rede virtual de VPN. (Você aprenderá mais sobre o ExpressRoute em outra unidade posteriormente neste módulo.)
* **Conexão**. Crie um recurso de conexão para criar uma conexão lógica entre o gateway de VPN e o gateway de rede local.
  + A conexão é realizada com o endereço IPv4 do dispositivo VPN local conforme definido pelo gateway de rede local.
  + A conexão é realizada do gateway de rede virtual e seu endereço IP público associado.

É possível criar várias conexões.

O diagrama a seguir mostra essa combinação de recursos e suas relações para ajudar você a entender melhor o que é necessário para implantar um gateway de VPN.

Interface gráfica do usuário, Diagrama

Descrição gerada automaticamente

### **Recursos locais necessários**

Para conectar seu datacenter a um gateway de VPN, serão necessários os seguintes recursos locais:

* Um dispositivo VPN que dá suporte a gateways de VPN baseada em política ou em rota
* Um endereço IPv4 (roteável pela Internet) voltado para o público

## **Cenários de alta disponibilidade**

Há várias maneiras de verificar se você tem uma configuração tolerante a falhas

### **Ativo/em espera**

Por padrão, gateways de VPN são implantados como duas instâncias em uma configuração ativa/em espera, mesmo se você vê apenas um recurso de gateway de VPN no Azure. Quando a manutenção planejada ou a interrupção não planejada afeta a instância ativa, a instância de modo de espera assume automaticamente a responsabilidade pelas conexões sem nenhuma intervenção do usuário. Durante esse failover, as conexões são interrompidas, mas normalmente são restauradas em alguns segundos para manutenção planejada e dentro de 90 segundos em caso de interrupções não planejadas

Diagrama

Descrição gerada automaticamente

### **Ativo/ativo**

Com a introdução da compatibilidade com o protocolo de roteamento BGP, você também pode implantar os gateways de VPN em uma configuração ativo/ativo. Nessa configuração, você atribui um endereço IP público exclusivo a cada instância. Em seguida, cria túneis do dispositivo local para cada endereço IP. É possível estender a alta disponibilidade implantando um dispositivo VPN local adicional.

### **Failover do ExpressRoute**

Outra opção de alta disponibilidade é configurar um gateway de VPN como um caminho de failover seguro para conexões ExpressRoute. Os circuitos ExpressRoute têm resiliência integrada. Mas não são imunes a problemas físicos que afetam os cabos que fornecem conectividade nem a interrupções que afetam toda a localização do ExpressRoute. Em cenários de alta disponibilidade, nos quais há risco associado a uma interrupção de um circuito do ExpressRoute, você também pode provisionar um gateway de VPN que usa a Internet como um método alternativo de conectividade. Dessa forma, você pode garantir que sempre haja uma conexão com as redes virtuais.

### **Gateways com redundância de zona**

Nas regiões que dão suporte a zonas de disponibilidade, os gateways de VPN e os gateways de ExpressRoute podem ser implantados em uma configuração com redundância de zona. Essa configuração oferece resiliência, escalabilidade e maior disponibilidade para os gateways de rede virtual. A implantação de gateways em zonas de disponibilidade do Azure separa de forma física e lógica os gateways em uma região, enquanto protege a conectividade de rede local com o Azure contra falhas no nível da zona. Esses gateways exigem SKUs de gateway diferentes e usam os endereços IP públicos Standard em vez dos Básicos.

# Conceitos básicos do ExpressRoute do Azure

O ExpressRoute permite que você estenda suas redes locais para a nuvem da Microsoft em uma conexão privada com a ajuda de um provedor de conectividade. Com o ExpressRoute, você pode estabelecer conexões com os serviços em nuvem da Microsoft, como o Microsoft Azure e o Microsoft 365.

A conectividade pode ocorrer de uma rede any-to-any (VPN de IP), uma rede Ethernet ponto a ponto ou uma conexão cruzada virtual por meio de um provedor de conectividade em uma colocação. As conexões do ExpressRoute não passam pela Internet pública. Isso permite que as conexões de ExpressRoute ofereçam mais confiabilidade, mais velocidade, latências consistentes e muito mais segurança do que as conexões típicas pela Internet. Para saber mais sobre como conectar sua rede à Microsoft usando ExpressRoute, veja Modelos de conectividade do ExpressRoute.

Diagrama

Descrição gerada automaticamente

Como parte do seu trabalho para a Tailwind Traders, você deve entender o que é o Azure ExpressRoute e como ele se integra com redes locais e do Azure. Nesta unidade, você conhecerá os benefícios que o ExpressRoute oferece em comparação com outras opções de conectividade site a site. Como resultado, saberá se o ExpressRoute pode fornecer à sua empresa o melhor desempenho de rede possível.

Nesta unidade, nós nos concentraremos em duas camadas diferentes do modelo de OSI (Open Systems Interconnection):

* **Camada 2 (L2)**: essa é a Camada de Vínculo de Dados, que fornece comunicação de nó para nó entre dois nós na mesma rede.
* **Camada 3 (L3)**: essa é a Camada de Rede, que fornece endereçamento e roteamento entre nós em uma rede de vários nós.

## **Recursos e benefícios do ExpressRoute**

Há vários benefícios de usar o ExpressRoute como o serviço de conexão entre o Azure e as redes locais.

* Conectividade de Camada 3 entre sua rede local e a Microsoft Cloud por meio de um provedor de conectividade. A conectividade pode ocorrer de uma rede “qualquer para qualquer” (IPVPN), de uma conexão Ethernet ponto a ponto ou por meio de uma conexão cruzada virtual via troca Ethernet.
* Conectividade com os serviços de nuvem da Microsoft em todas as regiões da região geopolítica.
* Conectividade global com os serviços da Microsoft em todas as regiões com o complemento premium do ExpressRoute.
* Roteamento dinâmico entre sua rede e a Microsoft por meio do BGP.
* Redundância interna em cada local de emparelhamento para proporcionar maior confiabilidade.
* SLAdo tempo de atividade da conexão.
* Suporte a QoS para Skype for Business.

### **Conectividade de Camada 3**

O ExpressRoute oferece conectividade de Camada 3 (nível do endereço) entre sua rede local e a nuvem da Microsoft é fornecida por meio de parceiros de conectividade. Essas conexões podem ser de uma rede ponto a ponto ou any-to-any. Elas também podem ser conexões cruzadas virtuais por meio de uma troca.

### **Redundância interna**

Cada provedor de conectividade usa dispositivos redundantes para verificar se as conexões estabelecidas com a Microsoft estão altamente disponíveis. É possível configurar vários circuitos para complementar esse recurso. Todas as conexões redundantes são configuradas com conectividade de Camada 3 para atender aos contratos de nível de serviço.

### **Conectividade com serviços em nuvem da Microsoft**

O ExpressRoute permite acesso direto aos seguintes serviços em todas as regiões:

* Microsoft Office 365
* Microsoft Dynamics 365
* Serviços de computação do Azure, como as Máquinas Virtuais do Azure
* Serviços de Nuvem do Azure, como o Azure Cosmos DB e o Armazenamento do Azure

O Office 365 foi criado para ser acessado de modo seguro e confiável pela Internet. Por isso, recomendamos o uso do ExpressRoute para cenários específicos. A seção “Saiba mais” no fim deste módulo inclui um link sobre como usar o ExpressRoute para acessar o Office 365.

### Conectividade local com Alcance Global do ExpressRoute

Você pode habilitar o Alcance Global do ExpressRoute para trocar dados entre sites locais conectando seus circuitos do ExpressRoute. Por exemplo, suponha que você tenha um datacenter privado na Califórnia conectado ao ExpressRoute no Vale do Silício. Você tem outro datacenter privado no Texas conectado ao ExpressRoute em Dallas. Com o Alcance Global do ExpressRoute, você pode conectar seus datacenters privados por meio de dois circuitos do ExpressRoute. Seu tráfego entre datacenters percorrerá a rede da Microsoft.

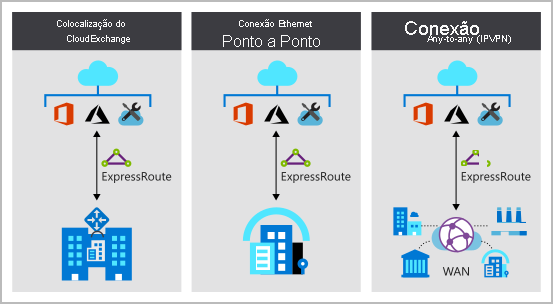
### Roteamento dinâmico

O ExpressRoute usa o protocolo de roteamento BGP (Border Gateway Protocol). O BGP é usado para trocar rotas entre as redes locais e os recursos em execução no Azure. Esse protocolo permite o roteamento dinâmico entre a rede local e os serviços em execução na nuvem da Microsoft.

## Modelos de conectividade do ExpressRoute

O ExpressRoute dá suporte a três modelos que podem ser usados para conectar a rede local à nuvem da Microsoft:

* Colocação do CloudExchange
* Conexão Ethernet ponto a ponto
* Conexão qualquer para qualquer



### **Colocalização em um compartilhamento de nuvem**

Normalmente, provedores colocalizados podem oferecer conexões de Camada 2 e Camada 3 entre sua infraestrutura, que podem estar localizadas nas instalações de colocalização e na nuvem da Microsoft. Por exemplo, se o seu datacenter estiver colocalizado em uma troca de nuvem, como um ISP, você poderá solicitar uma conexão cruzada virtual com a nuvem da Microsoft.

### **Conexão Ethernet ponto a ponto**

Conexões ponto a ponto fornecem conectividade de Camada 2 e Camada 3 entre o local e o Azure. Você pode conectar seus escritórios ou data centers ao Azure usando links ponto a ponto. Por exemplo, se tiver um datacenter local, você poderá usar um link Ethernet ponto a ponto para se conectar à Microsoft.

### **Redes qualquer para qualquer**

Com a conectividade any-to-any, você pode integrar sua WAN (rede de longa distância) ao Azure fornecendo conexões aos seus escritórios e datacenters. O Azure é integrado à sua conexão WAN para fornecer uma conexão, da mesma forma que você teria entre o datacenter e as filiais.

Com conexões qualquer para qualquer, todos os provedores de WAN oferecem conectividade de Camada 3. Por exemplo, caso você já use Multiprotocol Label Switching para se conectar às suas filiais ou a outras unidades de sua organização, uma conexão do ExpressRoute com a Microsoft se comporta como qualquer outra localização de sua WAN privada.

## **Considerações sobre segurança**

Com o ExpressRoute, os seus dados não passam pela Internet pública e, portanto, não são expostos aos riscos potenciais associados às comunicações da Internet. O ExpressRoute é uma conexão particular de sua infraestrutura local com a infraestrutura do Azure. Mesmo que você tenha uma conexão do ExpressRoute, consultas DNS, verificações de listas de certificados revogados e solicitações da Rede de Distribuição de Conteúdo do Azure ainda serão enviadas pela Internet pública.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

# Resumo

Neste módulo, você usou o cenário da Tailwind Traders para saber mais sobre os principais recursos de rede que estão disponíveis no Azure. Você conheceu os benefícios e o uso da Rede Virtual do Azure, do Gateway de VPN do Azure e do Azure ExpressRoute. Agora você pode aplicar essas informações para ajudar sua empresa a usar os recursos de rede do Azure para configurar a infraestrutura de rede.