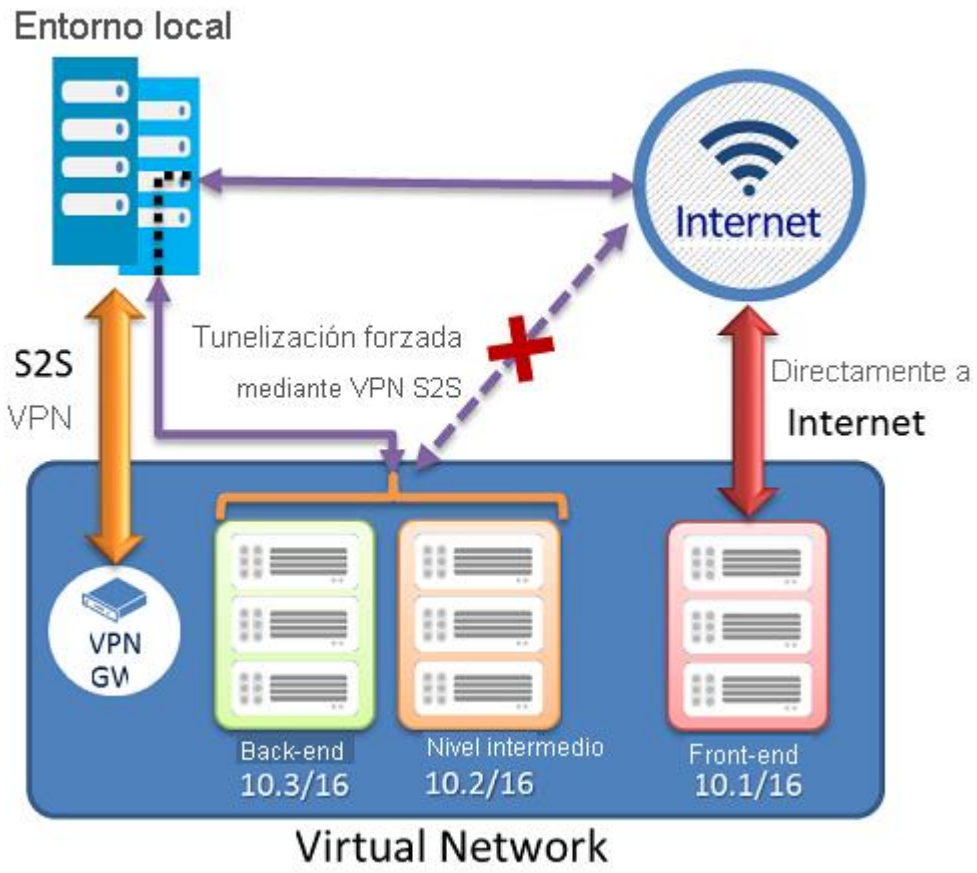
Configuración de la tunelización forzada de VPN

¿Por qué en algunos casos se requiere la tunelización forzada? - Una red privada virtual (VPN) consta de pares remotos que se envían datos privados entre sí de manera segura a través de una red no segura, como Internet. A esto se le denomina "tunelización de Internet". Las **VPN de sitio a sitio (S2S)** usan túneles para encapsular paquetes de datos dentro de paquetes IP normales para el reenvío a través de redes basadas en IP, mediante cifrado para garantizar la privacidad y autenticación para garantizar la integridad de los datos.

La tunelización forzada permite redirigir o "forzar" todo el tráfico vinculado a Internet de vuelta a la ubicación local mediante un túnel VPN de sitio a sitio para inspección y auditoría. Se trata de un requisito de seguridad crítico en la mayoría de las directivas de las empresas de TI. Sin la tunelización forzada, el tráfico enlazado a Internet desde las máquinas virtuales de Azure siempre atraviesa directamente de la infraestructura de red de Azure a Internet, sin la opción de permitirle inspeccionar o auditar el tráfico. El acceso no autorizado a Internet puede dar lugar a la divulgación de información u otros tipos de vulneraciones de seguridad.

Como ya se indicó, Azure actualmente funciona con dos modelos de implementación: el modelo de Resource Manager y el de implementación clásica. Los dos modelos no son totalmente compatibles entre sí. El ejercicio siguiente pasa por la configuración de la tunelización para redes virtuales que se crearon a través del modelo de implementación de Resource Manager.

En la ilustración siguiente se muestra el funcionamiento de la tunelización forzada.



En la ilustración anterior, la subred de front-end no usa la tunelización forzada. Las cargas de trabajo de la subred de front-end pueden seguir aceptando y respondiendo las solicitudes de los clientes que proceden directamente de Internet. Las subredes de nivel medio y back-end usan la tunelización forzada. Las conexiones salientes de estas dos subredes a Internet se fuerzan de vuelta a un sitio local a través de uno de los túneles VPN S2S.

Esto permite restringir e inspeccionar el acceso a Internet desde sus VM o servicios en la nube en Azure, mientras se sigue habilitando la arquitectura de servicio de varios niveles. Si no existen cargas de trabajo orientadas a Internet en las máquinas virtuales, también puede aplicar la tunelización forzada a toda la red virtual.

La tunelización forzada se configura en Azure a través de rutas definidas por el usuario (UDR) de la red virtual. Redirigir el tráfico a un sitio local se expresa como una ruta predeterminada a la puerta de enlace VPN de Azure. En este ejemplo se usan UDR para crear una tabla de enrutamiento a fin de agregar primero una ruta predeterminada y, a continuación, asociar la tabla de enrutamiento a las subredes de red virtual para habilitar la tunelización forzada en esas subredes.

Requisitos previos

Antes de comenzar con la configuración, verifique que dispone de los elementos siguientes:

- Suscripción a Azure. Si todavía no la tiene, puede activar sus ventajas como suscriptor de MSDN o registrarse para obtener una cuenta gratuita.
- Una red virtual configurada.
- Cuando se trabaja con el modelo de implementación clásica, no se puede usar Azure Cloud Shell. En su lugar, debe instalar la versión más reciente de los cmdlets de PowerShell para Azure Service Management (SM) en el equipo. Estos cmdlets son diferentes de los de AzureRM o Az. Para instalar los cmdlets de SM, consulte Instalación de cmdlets de Service Management. Para más información sobre Azure PowerShell en general, consulte la documentación de Azure PowerShell.

Configuración de la tunelización forzada

El siguiente procedimiento lo ayudará a especificar la tunelización forzada en una red virtual. Los pasos de configuración corresponden al archivo de configuración de red virtual. En este ejemplo, la red virtual "MultiTier-VNet" tiene tres subredes: las subredes "Frontend", "Midtier" y "Backend", con cuatro conexiones entre locales: "DefaultSiteHQ" y tres ramas.

XML

```xml
<VirtualNetworkSite name="MultiTier-VNet" Location="North Europe">
     <AddressSpace>
      <AddressPrefix>10.1.0.0/16</AddressPrefix>
        </AddressSpace>
        <Subnets>
          <Subnet name="Frontend">
            <AddressPrefix>10.1.0.0/24</AddressPrefix>
          </Subnet>
          <Subnet name="Midtier">
            <AddressPrefix>10.1.1.0/24</AddressPrefix>
          </Subnet>
          <Subnet name="Backend">
            <AddressPrefix>10.1.2.0/23</AddressPrefix>
          </Subnet>
          <Subnet name="GatewaySubnet">
            <AddressPrefix>10.1.200.0/28</AddressPrefix>
          </Subnet>
        </Subnets>
        <Gateway>
          <ConnectionsToLocalNetwork>
            <LocalNetworkSiteRef name="DefaultSiteHQ">
              <Connection type="IPsec" />
            </LocalNetworkSiteRef>
            <LocalNetworkSiteRef name="Branch1">
              <Connection type="IPsec" />
            </LocalNetworkSiteRef>
            <LocalNetworkSiteRef name="Branch2">
              <Connection type="IPsec" />
            </LocalNetworkSiteRef>
            <LocalNetworkSiteRef name="Branch3">
              <Connection type="IPsec" />
            </LocalNetworkSiteRef>
        </Gateway>
      </VirtualNetworkSite>
    </VirtualNetworkSite>
```

Los siguientes pasos establecerán "DefaultSiteHQ" como la conexión de sitio predeterminada para la tunelización forzada y configurarán las subredes Midtier y Backend para que usen dicha tunelización.

1. Abra la consola de PowerShell con privilegios elevados. Conéctese a su cuenta mediante el ejemplo siguiente:

Add-AzureAccount

Cree una tabla de enrutamiento. Use el siguiente cmdlet para crear la tabla de enrutamiento.

New-AzureRouteTable –Name "MyRouteTable" –Label "Routing Table for Forced Tunneling" –Location "North Europe"

Agregue una ruta predeterminada a la tabla de enrutamiento.

El siguiente ejemplo agrega una ruta predeterminada a la tabla de enrutamiento que creó en el paso 1. Tenga en cuenta que la única ruta admitida es el prefijo de destino de 0.0.0.0/0 para el próximo salto VPNGateway.

Get-AzureRouteTable -Name "MyRouteTable" | Set-AzureRoute –RouteTable "MyRouteTable" –RouteName "DefaultRoute" –AddressPrefix "0.0.0.0/0" –NextHopType VPNGateway

Asocie la tabla de enrutamiento a las subredes.

Una vez creada una tabla de enrutamiento y agregada una ruta, use el ejemplo siguiente para agregar o asociar la tabla de enrutamiento a una subred de la red virtual. Los siguientes ejemplos agregan la tabla de enrutamiento MyRouteTable a las subredes Midtier y Backend de VNet MultiTier-VNet.

Set-AzureSubnetRouteTable -VirtualNetworkName "MultiTier-VNet" -SubnetName "Midtier" -RouteTableName "MyRouteTable"

Set-AzureSubnetRouteTable -VirtualNetworkName "MultiTier-VNet" -SubnetName "Backend" -RouteTableName "MyRouteTable"

Asigne un sitio predeterminado para la tunelización forzada.

En el paso anterior, los scripts del cmdlet de ejemplo crean la tabla de enrutamiento y la tabla de enrutamiento asociada a dos de las subredes de la red virtual. El paso restante consiste en seleccionar un sitio local entre las conexiones de varios sitios de la red virtual como el sitio predeterminado o túnel.

$DefaultSite = @("DefaultSiteHQ")

Set-AzureVNetGatewayDefaultSite –VNetName "MultiTier-VNet" –DefaultSite "DefaultSiteHQ"

Asigne un sitio predeterminado para la tunelización forzada.

En el paso anterior, los scripts del cmdlet de ejemplo crean la tabla de enrutamiento y la tabla de enrutamiento asociada a dos de las subredes de la red virtual. El paso restante consiste en seleccionar un sitio local entre las conexiones de varios sitios de la red virtual como el sitio predeterminado o túnel

$DefaultSite = @("DefaultSiteHQ")

Set-AzureVNetGatewayDefaultSite –VNetName "MultiTier-VNet" –DefaultSite "DefaultSiteHQ"

Para eliminar una tabla de enrutamiento

```
Remove-AzureRouteTable -Name <routeTableName>
```

Para mostrar una tabla de enrutamiento

```
Get-AzureRouteTable [-Name <routeTableName> [-DetailLevel <detailLevel>]]
```

Para eliminar una ruta de una tabla de enrutamiento

```
Remove-AzureRouteTable –Name <routeTableName>
```

Para quitar una ruta de una subred

```
Remove-AzureSubnetRouteTable –VirtualNetworkName <virtualNetworkName> -
SubnetName <subnetName>
```

Para mostrar la tabla de enrutamiento asociada a una subred

```
Get-AzureSubnetRouteTable -VirtualNetworkName <virtualNetworkName> -SubnetName
<subnetName>
```

Para quitar un sitio predeterminado de una puerta de enlace de VPN de VNet

```
Remove-AzureVnetGatewayDefaultSite -VNetName <virtualNetworkName>
```
