



Virtual Networking - Caso de Estudo MS Azure

Tecnologias de Virtualização e Centros de Dados

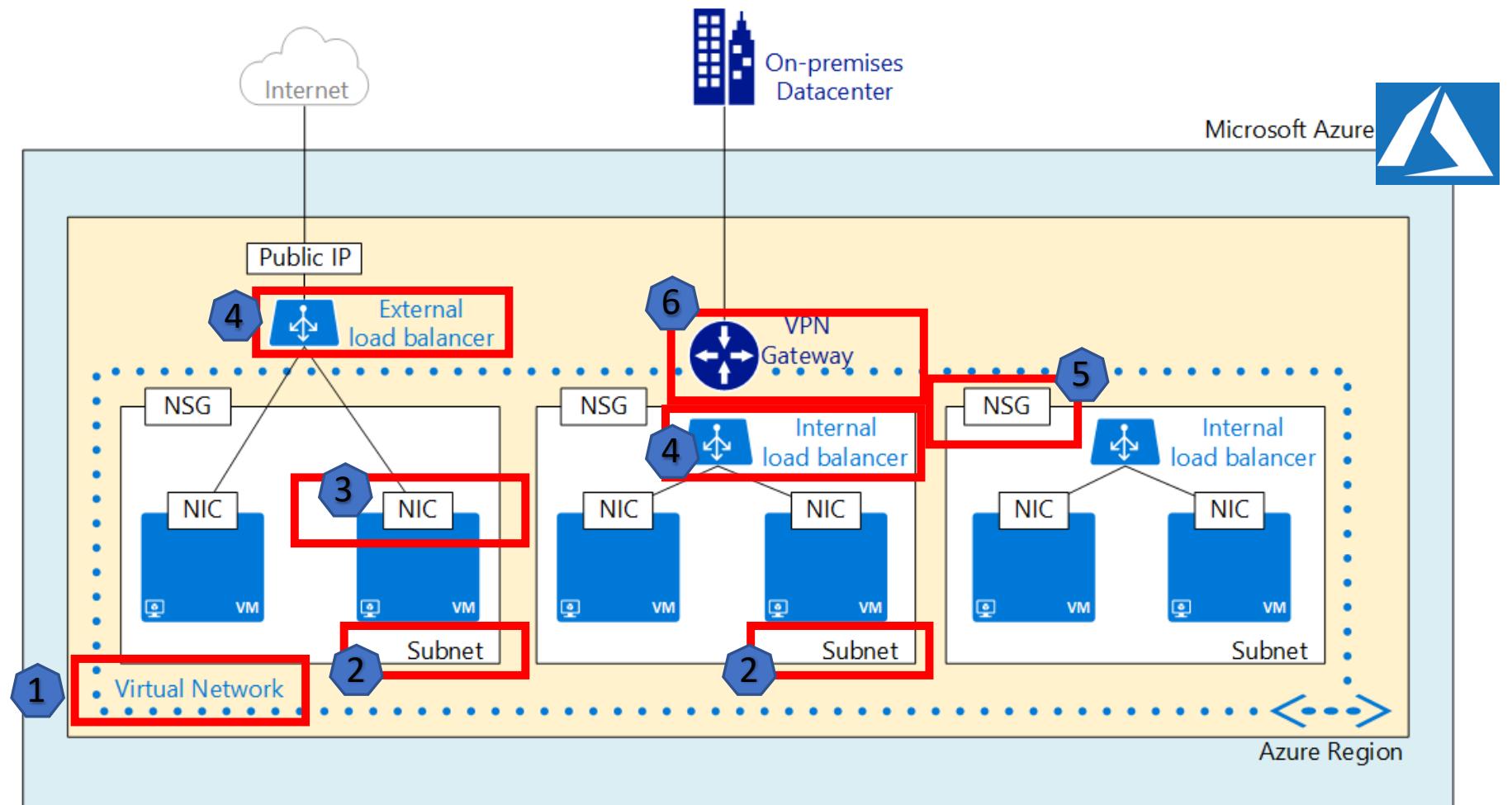
Mestrado em Engenharia Informática

Alexandre Fonte
alexandre.fonte@ubi.pt
(Professor Convidado)
Departamento de Informática
Ano Letivo 2023/2024

Sumário

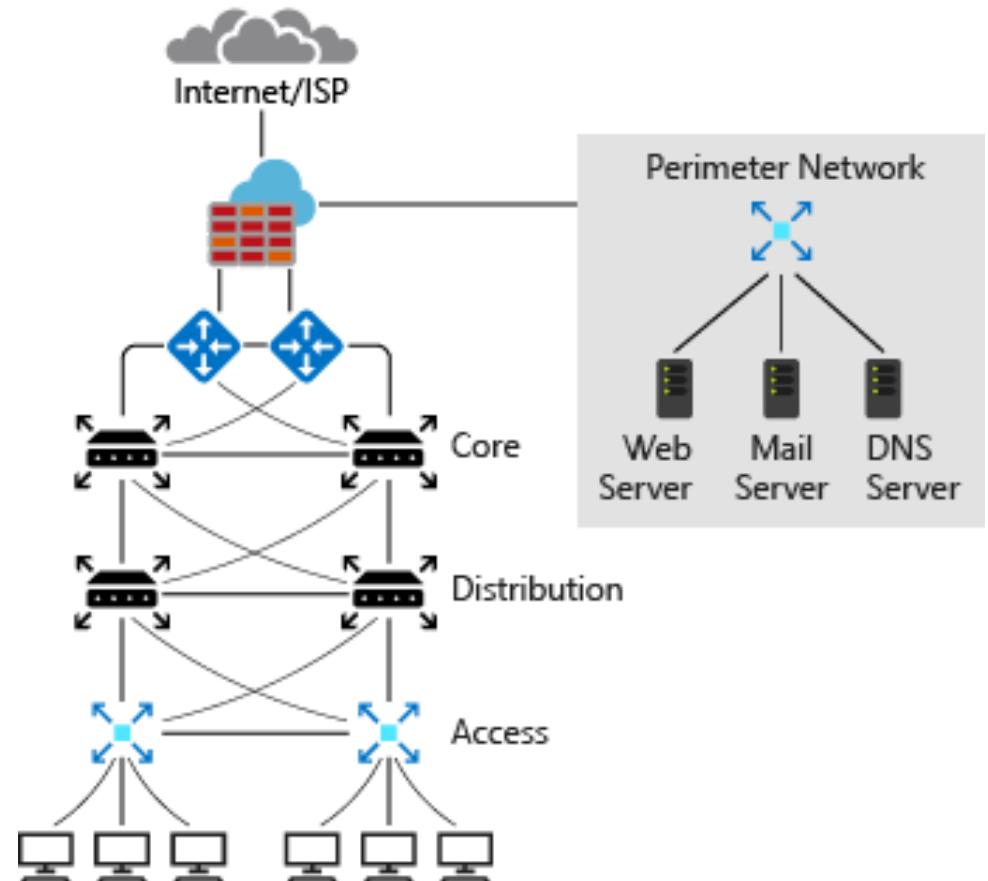
- Redes Virtuais - Caso de estudo Azure
 - VNets
 - Endereçamento IP
 - VNet Peering
 - Encaminhamento de tráfego no Azure
 - Balanceadores de carga
 - Ligações S2S e P2S

Redes Virtuais - Caso de estudo Azure



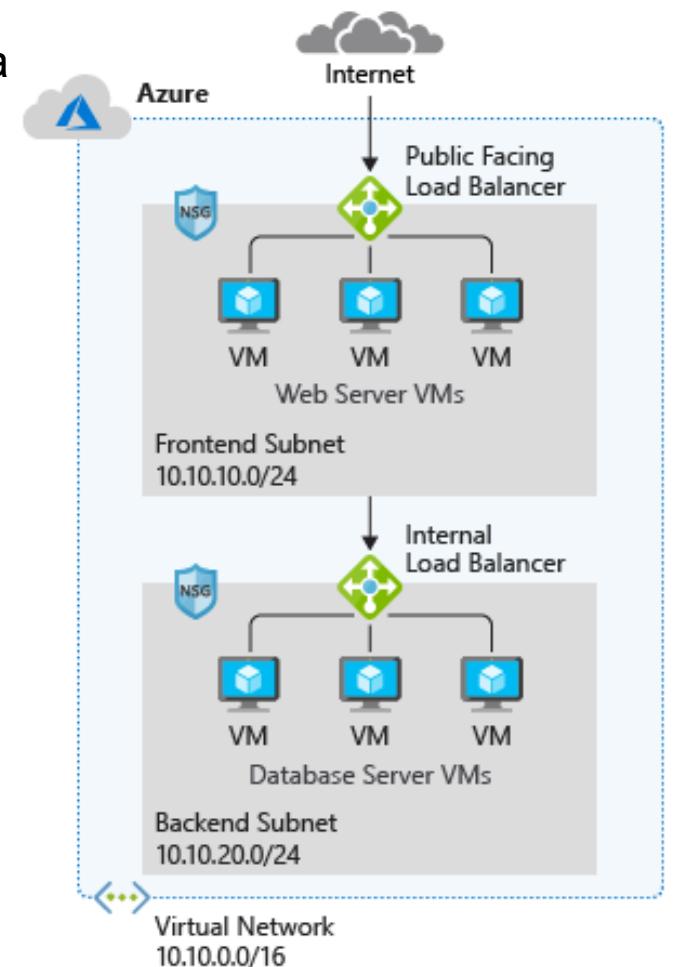
Modelo das Redes On-Premise (locais)

- Modelo Hierárquico organizados em 3 camadas
- Um esquema típico de rede local inclui os seguintes componentes:
 - Routers
 - Firewalls
 - Switches
 - VLANs (segmentação de rede)



Modelo das Redes Virtuais em Azure

- No Azure, o design de rede tem recursos e funções semelhantes a uma rede local, mas a estrutura da rede é diferente. A rede do Azure não segue o design de rede hierárquica local típico.
- Não há dispositivos de hardware, como routers ou switches. Toda a infraestrutura de rede é virtual.
- Os componentes típicos de uma rede Azure:
 - Virtual networks
 - Subnets
 - Network security groups
 - Firewalls
 - Load balancers
 - Gateways
- No Azure, normalmente implementa-se um grupo de segurança de rede e um firewall. Usa-se sub-redes para isolar serviços front-end, incluindo servidores da Web e DNS, e serviços back-end, como bases de dados e sistemas de armazenamento.
- Os grupos de segurança de rede filtram o tráfego interno e externo na camada de rede.
- Uma firewall possui recursos mais abrangentes para filtragem de camada de rede e filtragem de camada de aplicação. Ao implantar grupos de segurança de rede e um firewall, consegue-se obter um isolamento elevado dos recursos para uma arquitetura de rede segura.



Azure IP addressing: espaço de endereçamento e subredes

- As redes virtuais do Azure usam endereços IP privados. Tal como as redes locais, o administrador tem controle total sobre a gama, resolução de nome, configurações de segurança e regras de segurança numa rede virtual do Azure.
- Uma rede virtual também pode ser dividida em várias sub-redes. Cada sub-rede possui uma parte do espaço de endereçamento IP que é atribuído à rede virtual. Pode-se adicionar, remover, expandir ou reduzir uma sub-rede se não houver VMs ou serviços nela implantados.
- Por omissão, todas as sub-redes numa rede virtual do Azure podem comunicar entre si. No entanto, usando um grupo de segurança de rede pode-se negar a comunicação entre sub-redes.
- A menor sub-rede compatível usa uma máscara de sub-rede /29. A maior sub-rede com suporte usa uma máscara de sub-rede / 8.

Espaço de Endereçamento

Save Discard

10.0.0.0/16 ...

Add additional address range ...

Subnets
OpsLabRG-vnet

+ Subnet + Gateway subnet

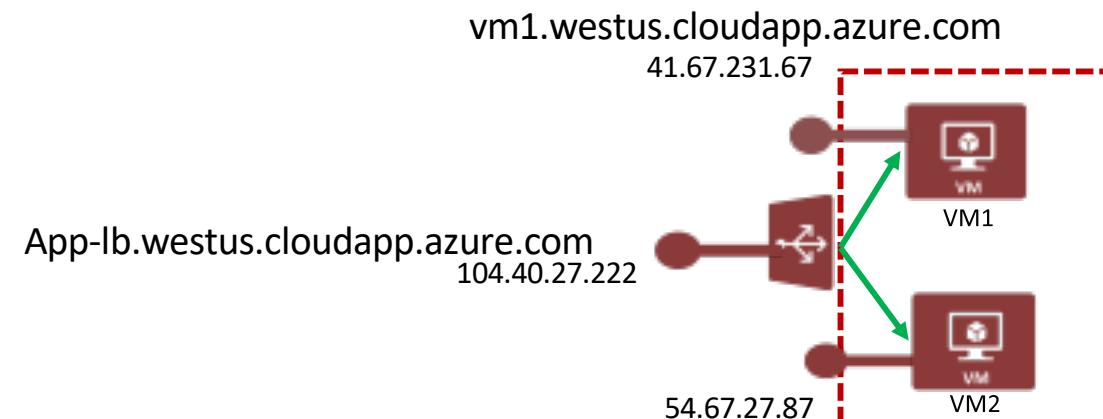
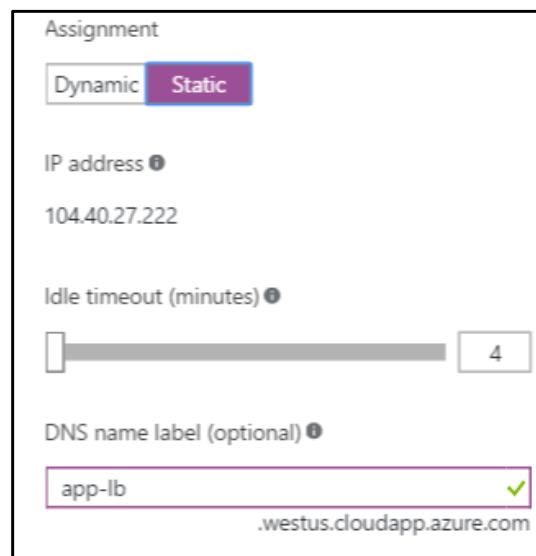
Search subnets

NAME	ADDRESS RANGE	AVAILABLE ADDR...	SECURITY GROUP
Apps	10.0.1.0/24	251	-
Data	10.0.2.0/24	251	-
Management	10.0.3.0/24	251	-
Identity	10.0.4.0/24	251	-

V 1.21.22 Key | Prof. Doutor Alexandre Fonte | TVC

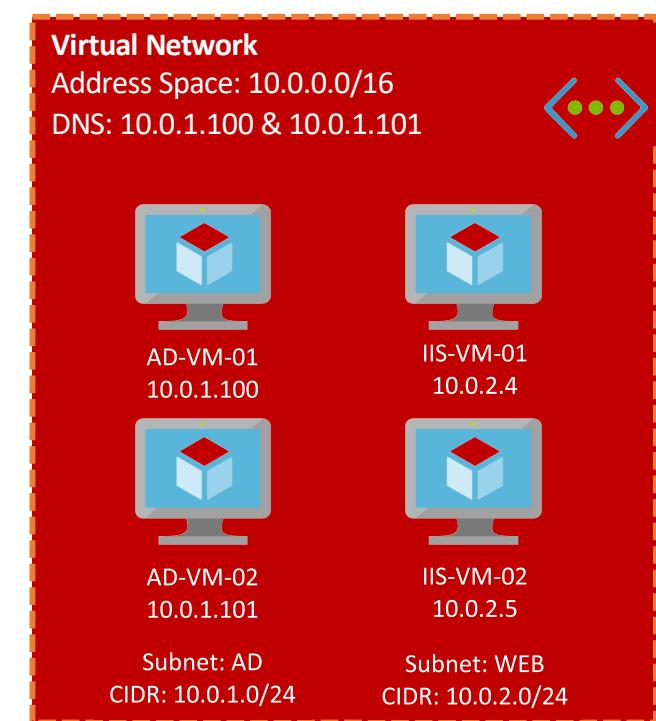
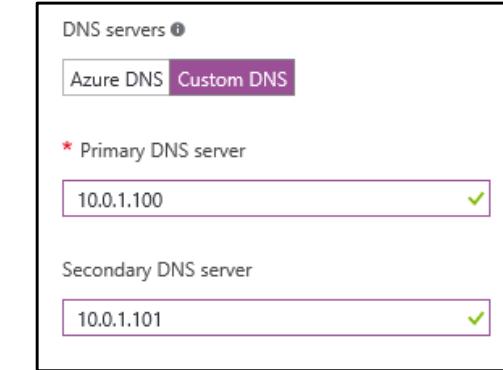
Azure IP addressing: Endereços Públicos

- Um endereço IP público pode ser atribuído diretamente a uma interface de rede ou a um平衡ador de carga
 - Suporta atribuição estática (reservada) ou dinâmica
 - Opcionalmente, suporta a especificação de um rótulo DNS
- Os 5 primeiros IPs estáticos são gratuitos



Azure DNS ou Próprio DNS

- Especificar servidores DNS no nível da rede virtual
 - Hospedado numa VM do Azure
 - Externo
 - No local (com conexão híbrida)
- As máquinas virtuais são atribuídas ao DNS especificado na inicialização
 - Se o DNS for adicionado depois que uma máquina virtual estiver em execução, uma reinicialização será necessária para a atribuição.



Demonstração Criação e Gestão de uma vNet no Microsoft Azure

Esta demonstração e seguintes sobre mecanismos existentes na cloud Azure pretendem ilustrar/demonstrar os conceitos para mais fácil compreensão ou apreensão.

Os seus detalhes não são alvo de avaliação.

Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 1. Indicação do Projecto
 - Subscrição e grupo de recursos
- 2. Detalhes da instância
 - Nome e Região

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar with the placeholder "Search resources, services, and docs (G+/" and a "Microsoft Azure" logo. Below the search bar, the breadcrumb navigation shows "Home > New > Virtual Network". The main title is "Virtual Network" by Microsoft. To the left is a blue icon with three dots and arrows. On the right, there's a "Create" button and a "Save for later" link. Below the main title, it says "Deploy with Resource Manager (change to Classic)". At the bottom, there are tabs for "Overview" (which is selected), "Plans", and "Usage Information + Support".

The screenshot shows the "Create virtual network" wizard in the Microsoft Azure portal. The top navigation bar includes "Microsoft Azure", a search bar, and a user profile for "adf@ipcb.pt" in "MICROSOFT LEARN SANDBOX". The breadcrumb navigation shows "Home > New > Virtual Network > Create virtual network". The main title is "Create virtual network". The "Basics" tab is selected. The "Project details" section shows "Subscription" set to "Concierge Subscription" and "Resource group" set to "learn-03328f81-2d40-4165-b3f9-6efbf594e784" (with a "Create new" link). The "Instance details" section shows "Name" set to "myVirtualNetwork" and "Region" set to "(Europe) West Europe". At the bottom, there are buttons for "Review + create", "< Previous" (disabled), "Next : IP Addresses >" (disabled), and "Download a template for automation".

Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 3. Especificação do Bloco de Endereçamento e da subrede
 - Nome: myVirtualNetwork ;
 - Endereço Base: 10.1.0.0/16
 - Subrede: myVirtualSubnet: 10.1.0.0/24

The screenshot shows the Microsoft Azure portal interface for creating a new virtual network. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information (adf@ipcb.pt, MICROSOFT LEARN SANDBOX). The main title is "Create virtual network". The breadcrumb navigation shows "Home > New > Virtual Network >". The current step is "IP Addresses", indicated by the blue underline. Below the step title, there is a note: "The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24)." Under the "IPv4 address space" section, the value "10.1.0.0/16" is listed, followed by the range "10.1.0.0 - 10.1.255.255 (65536 addresses)" and a delete icon. A checkbox for "Add IPv6 address space" is present. Below this, there is a note: "The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network." Under the "Subnet" section, there is a "+ Add subnet" button, a "Remove subnet" button, and two input fields: "Subnet name" (containing "myVirtualSubnet") and "Subnet address range" (containing "10.1.0.0/24").

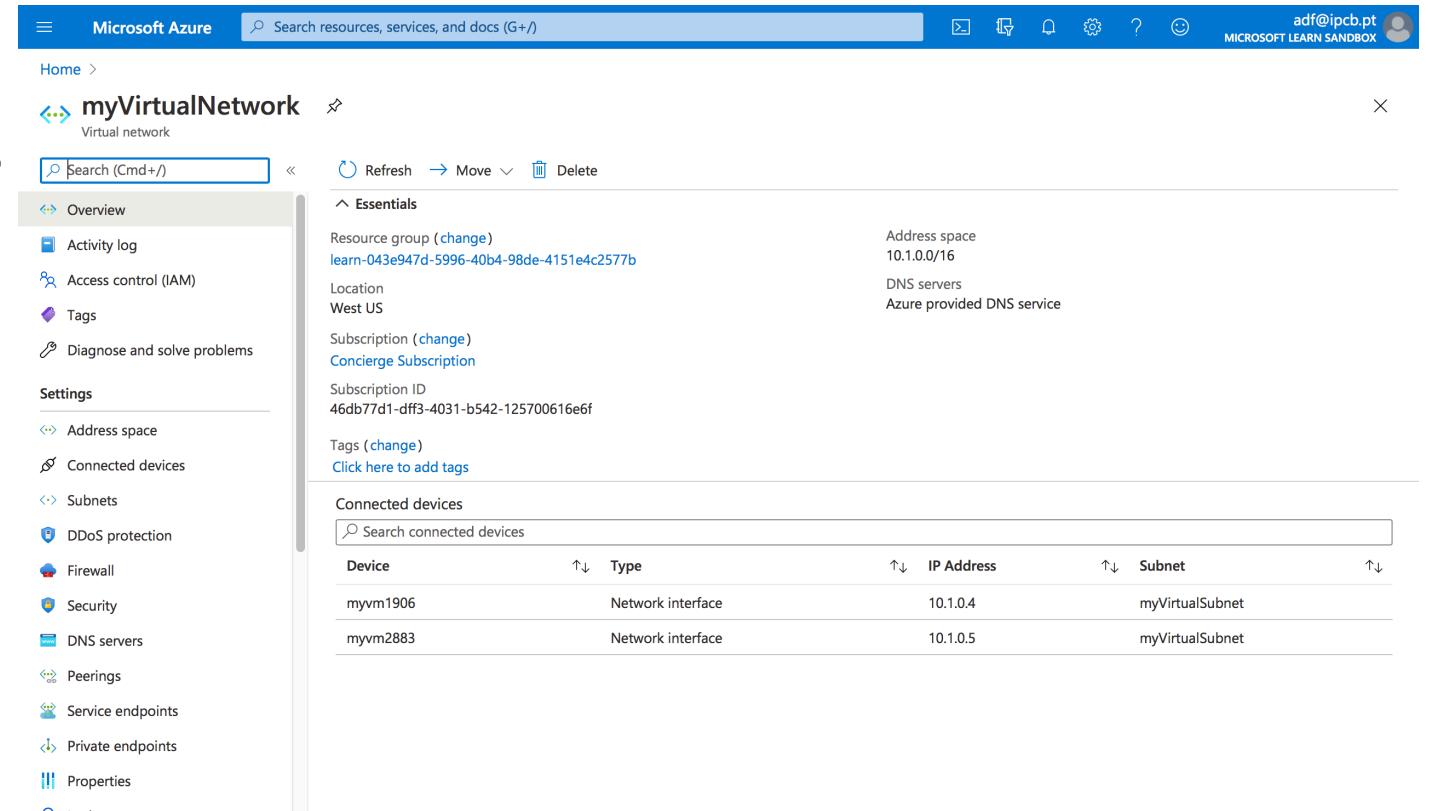
Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 4. Criação da VM e interfaces de rede, com indicação dos grupos de segurança e portas de entrada (inbound) autorizadas

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, and user information 'adf@ipcb.pt MICROSOFT LEARN SANDBOX'. The main page title is 'Create a virtual machine'. A sub-section title 'Network interface' is shown, with a note: 'Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.' Below this, there are dropdown menus for 'Virtual network' (set to 'myVirtualNetwork'), 'Subnet' (set to 'myVirtualSubnet (10.1.0.0/24)'), and 'Public IP' (set to '(new) myVm1-ip'). Under 'NIC network security group', the 'Basic' option is selected. A tooltip message states: 'The selected subnet 'myVirtualSubnet (10.1.0.0/24)' is already associated to a network security group 'NSG-westus'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.' At the bottom, 'Public inbound ports' is set to 'Allow selected ports'.

Configurações das vNets

- Espaço de Endereçamento
- Dispositivos ligados
- Subredes
- Servidores DNS
- Peerings
- Etc



The screenshot shows the Microsoft Azure portal interface for managing a virtual network named 'myVirtualNetwork'. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. The main content area displays the 'Overview' tab for the virtual network, showing details such as Resource group (learn-043e947d-5996-40b4-98de-4151e4c2577b), Location (West US), Subscription (Concierge Subscription), and Address space (10.1.0.0/16). It also lists DNS servers (Azure provided DNS service). The 'Connected devices' section shows two entries: 'myvm1906' and 'myvm2883', both listed as Network interface with IP addresses 10.1.0.4 and 10.1.0.5 respectively, and associated with the subnet 'myVirtualSubnet'. A sidebar on the left provides links to other settings like Address space, Subnets, DDoS protection, Firewall, Security, DNS servers, Peerings, Service endpoints, Private endpoints, and Properties.

Mais sobre Gestão de VNETs:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-virtual-network>

Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 5. Definição do Servidor DNS 8.8.8.8

The screenshot shows the Microsoft Azure portal interface for managing a virtual network. The URL in the address bar is `Home > learn-f2751b8c-af41-4335-9ced-1b2363a06bad > learn-f2751b8c-af41-4335-9ced-1b2363a06bad-vnet`. The main content area displays the configuration for the virtual network `learn-f2751b8c-af41-4335-9ced-1b2363a06bad-vnet`, specifically the DNS servers settings. A warning message states: "Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings." The DNS servers section shows that the "Custom" option is selected, with the IP address set to 8.8.8.8. An "Add DNS server" button is also present. On the left sidebar, under the "Settings" section, the "DNS servers" link is highlighted with a large orange arrow pointing towards it.

Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 6. Definição manual do endereço IP privado da interface de rede da VM myVM1
 - No portal Azure:
 - Aceder à VM1
 - Settings->Networking
 - Selecionar a placa de rede em **Network Interface: vm1983 ou outra designação**
 - Na placa de Rede->Settings->IP Configuration

Depois seleccione ipconfig1

Atribua de forma estática o endereço IP **10.1.0.101**

- Reinicie a VM e Teste a conectividade entre as VMs

VM1

Microsoft Azure | Search resources, services, and docs (G+)

Home > vm1

vm1 | Networking

Virtual machine

Search (Cmd + F)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Attach network interface Detach network interface

vm1983

IP configuration ipconfig1 (Primary)

Network Interface: vm1983 Effective security rules Topology

Virtual network/subnet: myVMNetwork/myVirtualSubnet NIC Public IP: 40.78.20.112 NIC Private IP: 10.1.0.4 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG-westus (attached to subnet: myVirtualSubnet)

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-VirtualHostIP-Inbound	Any	Any	168.63.129.16.169.25...	Any	AI
500	Allow-HTTP-Inbound	80,443,8080	Any	Any	Any	AI
501	Allow-SSH-Inbound	22	TCP	Any	Any	AI
502	Allow-RDP-Inbound	3389	TCP	Any	Any	AI
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	AI
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	AI
65500	DenyAllInbound	Any	Any	Any	Any	DI

Microsoft Azure | Search resources, services, and docs (G+)

Home > vm1

vm1983 Network interface

Search (Cmd + F)

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

Locks

Automation

Tasks

Export template

Support + troubleshooting

Effective security rules

Essentials

Resource group (change) learn-371c60ca-569f-46ab-b8ff-26316cbf338a

Location West US

Subscription (change) Concierge Subscription

Subscription ID db854904-5a16-4a0e-b2c0-8bb4b1a5c709

Private IP address 10.1.0.4

Public IP address 40.78.20.112 (vm1-ip)

Private IP address (IPv6) -

Public IP address (IPv6) -

Virtual network/subnet myVMNetwork/myVirtualSubnet

Network security group -

Attached to vm1

Criação e Gestão de vNet no Microsoft Azure e adição de uma VM

- 7. Criação de um endereço IP público e atribuição à VM
 - No portal Azure:

- Directamente na interface de rede.
- Pode criar a partir do MarketPlace onde deve procurar por **Public IP Address**

Crie um endereço IP publico chamado **vm1-ip-publico-extra**

Verifique o endereço publico atual e anote o endereço: _____

Regresse à interface de rede da myVM1 e altere o endereço público para o agora criado.

The screenshot shows the Microsoft Azure portal with the search bar at the top. Below it, the navigation bar includes 'Dashboard > New > Public IP address'. The main content area has a title 'Public IP address' with a 'Create' button. A detailed description explains what a Public IP address is and how it can be assigned to various Azure resources. Below this, there's a section titled 'More offers from Microsoft' with several service cards, including 'Workspace', 'Wire Data 2.0', 'Microsoft HPC Pack 2012 R2', and 'Windows Server 2019 Datacenter (zh-cn)'.

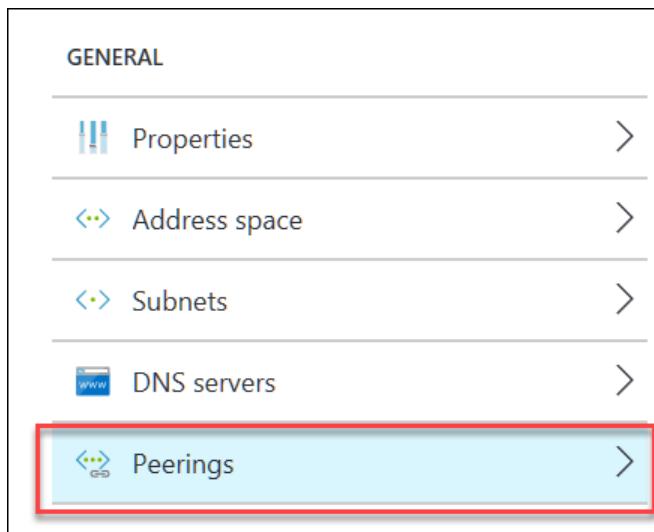
The screenshot shows the Microsoft Azure portal with the search bar at the top. Below it, the navigation bar includes 'Home > vm1983'. The main content area has a title 'ipconfig1' under 'vm1983'. It shows the 'Associate' tab selected for a 'Public IP address' named 'vm1-ip (40.78.20.112)'. A modal dialog box titled 'Add a public IP address' is open, prompting for a 'Name' (with a placeholder 'ipconfig1'), 'SKU' (set to 'Basic'), and 'Assignment' (set to 'Dynamic'). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Ligaçāo entre VNets



VNet Peering / Ligação entre VNets

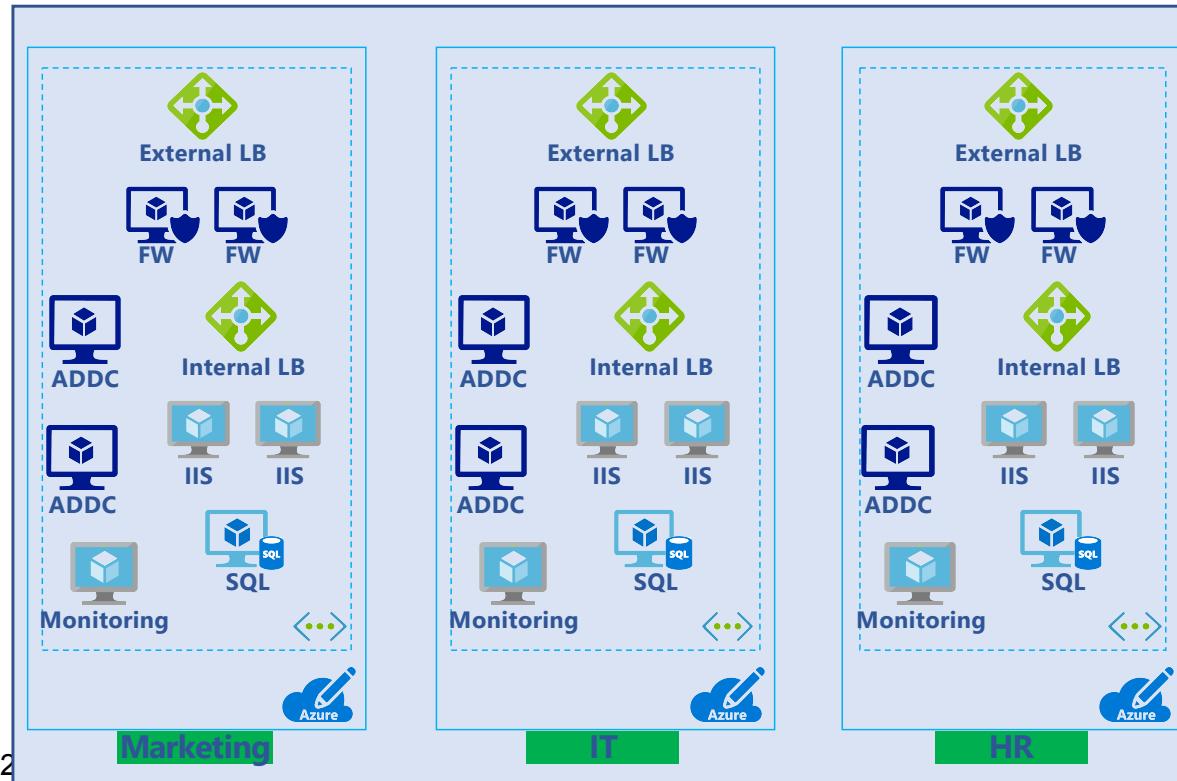
- Liga duas VNETs:
 - Regional VNet peering (VNet da mesma região)
 - Global VNet peering (VNets de regiões diferentes)
- Utiliza a rede Microsoft Backbone do Azure
- Apresenta-se como **uma rede para conectividade**
- Gerida como um recurso separado



As máquinas virtuais dispõem exatamente a mesma taxa de transferência para VNET ligada por peering como para a sua VNET.

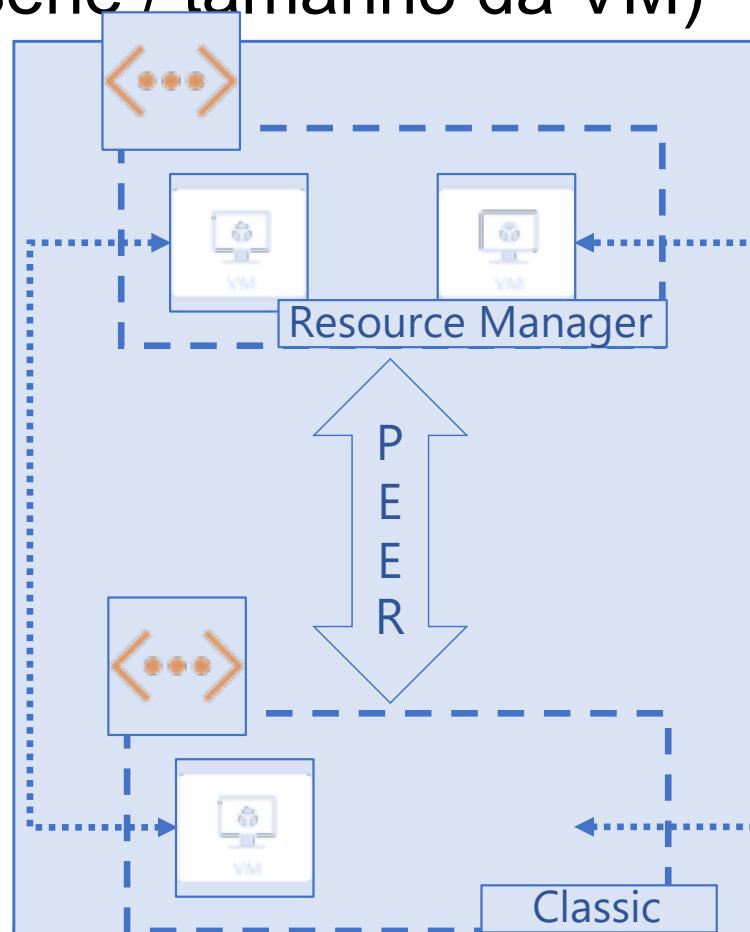
Razões para ter múltiplas VNets

- Mais comum em Enterprise Agreements com múltiplas assinaturas
 - Faturação
 - Administração
- Uma VNet não pode abranger várias assinaturas



Benefícios do VNet Peering

- Ligação de baixa latência e alta largura de banda entre recursos em diferentes VNets
- Nota: Sem restrição de largura de banda, além daquelas impostas na série / tamanho da VM)





Demonstração Criação e Gestão de uma ligação Regional VNET Peering

- Descrições em detalhe sobre a criação de uma ligação VNet peering: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#create-a-peering>

Criar uma Ligação VNet Peering usando o portal Azure

- 1. Criar um grupo de recursos
 - Nome: TVCD
 - Região: Europa Ocidental
- 2. Criar duas VNets, VNet1 e VNet2
 - VNET1, VNET2
 - Espaço de endereçamento: 10.1.0.0/16; 10.2.0.0/16
 - VNET1.Subnet1: 10.1.0.0/24; VNET2.Subnet2: 10.2.0.0/24

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.1.0.0/16 10.1.0.0 - 10.1.255.255 (65536 addresses)

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet

Subnet name	Subnet address range
<input type="checkbox"/> subnet1	10.1.0.0/24

Criar uma Ligação VNet Peering usando o portal Azure

- 3. Criar um VNet peering da VNET1 para a VNET2
 - Selecionar a VNET1 e clicar na opção “peerings”
 - Nome: VNET1-PARA-VNET2
 - Rede Virtual remota: VNET2

VNET1 | Peerings

Name	Peering status
Add a peering to get started	

Add peering

VNET1

Peering link name *

 ✓

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ
 Use this virtual network's gateway
 Use the remote virtual network's gateway
 None (default)

Remote virtual network

Peering link name *

 ✓

Virtual network deployment model ⓘ
 Resource manager
 Classic

Add peering

VNET1

Virtual network deployment model ⓘ
 Resource manager
 Classic

I know my resource ID ⓘ

Subscription * ⓘ

Virtual network * ⓘ
 ✓

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ
 Use this virtual network's gateway
 Use the remote virtual network's gateway
 None (default)

Add

Criar uma Ligação VNet Peering usando o portal Azure

- 4. Verificação do VNET Peering Status

The image shows two side-by-side Azure portal windows. Both windows have a blue header bar with the Microsoft Azure logo and a search bar. The left window is titled 'VNET1 | Peerings' and the right window is titled 'VNET2 | Peerings'. Both windows show a table with three columns: 'Name', 'Peering status', and 'Peer'. In the VNET1 window, there is one entry: 'VNET1-PARA-VNET2' with 'Connected' status and 'VNET2' as the peer. In the VNET2 window, there is one entry: 'VNET2-PARA-VNET1' with 'Connected' status and 'VNET1' as the peer. The tables also include a 'Search (Cmd+I)' field, an 'Add' button, and a 'Refresh' button. On the left side of each window, there is a sidebar with various settings like Overview, Activity log, Access control (IAM), Tags, and Peerings.

Name	Peering status	Peer
VNET1-PARA-VNET2	Connected	VNET2

Name	Peering status	Peer	Gateway transit
VNET2-PARA-VNET1	Connected	VNET1	Disabled

Criar uma Ligação VNet Peering usando o portal Azure

- 5. Ligar à myVm1 por RDP e colocar uma regra que permita a entrada de tráfego ICMP

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

- 6. Ligar à myVm2 por RDP e pingar a myVm1



Demonstração Criação e Gestão de um ligação global VNET Peering usando o Portal Azure

- Descrições em detalhe sobre a criação de uma ligação VNet peering: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#create-a-peering>

Demonstração Criação e Gestão de um ligação global VNET Peering

- 1. Criar um grupo de recursos
 - Nome: TVCD
 - Região: Alemanha
- 2. Criar uma terceira VNet na região da Alemanha ou outra
 - VNET3
 - Espaço de endereçamento: 10.3.0.0/16
 - VNET3.Subnet3: 10.3.0.0/24
- 3. Criar um VNet peering da VNET3 para a VNET1
 - Nome: VNET3-PARA-VNET1
 - Rede Virtual remota: VNET1
- 4. Verificação do VNET Peering Status
- 5. Consultar na VNET1 os dois peerings criados.

Name	Peering status	Peer
VNET1-PARA-VNET2	Connected	VNET2
VNET1-PARA-VNET3	Connected	VNET3

Demonstração Criação e Gestão de um ligação global VNET Peering

- 6. Criar a terceira VM por forma a pertencer à subrede3 da VNET3
- 7. Ligar por RDP à myVM3, abrir o command prompt e pingar a myVM1

Encaminhamento do Tráfego

Caso de Estudo Azure

Virtual network traffic routing

- Como é que o Azure encaminha o tráfego entre recursos Azure, on-premises, e na Internet?
- Azure automaticamente cria uma tabela de encaminhamento para cada subrede de uma rede virtual e adiciona um conjunto de rotas por pré-definidas (default).
- É possível contudo sobrepor-nos às rotas de sistema adicionando rotas *customizadas* às tabelas de encaminhamento das subredes.
- In a hybrid setup, Azure VNet may use any of the three route tables – **UDR, BGP (if ExpressRoute is used) and System routing tables.**
- Once an association is established, i.e. a UDR and/or a BGP route exists, routing is done based on Longest Prefix Match (LPM). In cases where there is more than one route with the same prefix length, a route is selected based on its origin in the following order:
 - User defined route, BGP route (when ExpressRoute is used) and System route.

Encaminhamento Azure - Rotas de Sistema

- São criadas automaticamente para permitir o fluxo do tráfego entre as VMs em diferentes subredes e espaços de endereçamento.
- Não é possível criarmos ou removermos as rotas de sistema.
- Tipos de rotas de sistema:
 - Encaminhamento dentro da própria subrede
 - Encaminhamento da subrede para outra subrede da mesma rede virtual
 - Encaminhamento para a Internet
 - Encaminhamento de uma VNet para outra VNet usando um VPN Gateway
 - Encaminhamento de uma VNet para a rede on-premises usando um VPN Gateway

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

Tráfego para
None é
descartado

Encaminhamento Azure - Rotas de Sistema

Estrutura das tabelas de encaminhamento Azure

- Cada entrada inclui (entre outros campos)
 - **Source:** fonte de informação da rota, isto é quem a inseriu na tabela de encaminhamento (sistema ou utilizador)
 - **Address prefix:** destino do tráfego
 - **Next hop type:** tipo de próximo salto
 - **Next hop IP:** IP do próximo salto
- O próximo salto representa como é que o Azure encaminha o tráfego para os prefixos destino indicados.
- Além das rotas para as subredes ou redes virtuais inclui rotas criadas automaticamente para três prefixos IP privados.
 - 10.0.0.0/8 and 192.168.0.0/16: Reserved for private use in RFC 1918.
 - 100.64.0.0/10: Reserved in RFC 6598.
 - Ver também: https://en.wikipedia.org/wiki/Reserved_IP_addresses

Encaminhamento Azure - Rotas de Sistema

Estrutura das tabelas de encaminhamento Azure

- Rota para a Internet (rota estática por omissão noutros contextos)
 - **Source:** origem da rota *default*
 - **Rede destino:** 0.0.0.0/0
 - Se não adicionarmos nenhuma rota, ou o tráfego não seja direcionado para nenhuma outra rota na tabela é usada esta rota.
 - Esta rota pode ser sobreposta com uma rota definida pelo utilizador
- Rotas default para IP reservados
 - ▶ Se eu criar uma rede virtual que utiliza as gamas das redes das rotas pré-definidas, o Azure automatically altera o próximo salto de NONE para VIRTUAL NETWORK
 - ▶ Se usarmos um espaço de endereçamento para a rede virtual que inclui parte dos endereços mas não todo o espaço, o Azure remove a rota e cria uma rota para o prefixo que definimos e coloca VIRTUAL NETWORK como próximo salto

Exemplo de Tabela de Encaminhamento

ID	Source	State	Address prefixes	Next hop type	Next hop IP address	User-defined route name
1	Default	Invalid	10.0.0.0/16	Virtual network		
2	User	Active	10.0.0.0/16	Virtual appliance	10.0.100.4	Within-VNet1
3	User	Active	10.0.0.0/24	Virtual network		Within-Subnet1
4	Default	Invalid	10.1.0.0/16	VNet peering		

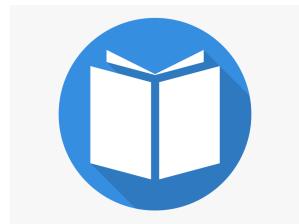
Tabelas de Encaminhamento: Tipos de Next hops para as diferentes ferramentas Azure

Next hop type	Azure CLI and PowerShell (Resource Manager)	Azure classic CLI and PowerShell (classic)
Virtual network gateway	VirtualNetworkGateway	VPNGateway
Virtual network	VNetLocal	VNETLocal (not available in the classic CLI in asm mode)
Internet	Internet	Internet (not available in the classic CLI in asm mode)
Virtual appliance	VirtualAppliance	VirtualAppliance
None	None	Null (not available in the classic CLI in asm mode)
Virtual network peering	VNet peering	Not applicable
Virtual network service endpoint	VirtualNetworkServiceEndpoint	Not applicable

Tráfego para
None é
descartado

Encaminhamento Azure - Rotas de Sistema *ROTAS DE SISTEMA OPCIONAIS*

- No caso de ativarmos certos mecanismos também são criadas automaticamente rotas dos seguintes tipos:
 - VNet Peering (quando ligamos duas VNets)
 - Virtual network gateway (quando adicionamos um VPN gateway ou um ExpressRoute gateway à rede virtual)
 - VirtualNetworkServiceEndpoint (rotas para certos serviços do Azure)



Demonstração Tabelas de Encaminhamento

Consulta Tabela de Encaminhamento numa VM Azure para diagnosticar problemas

- Regressando à atividade anterior, consulte as tabelas de encaminhamento nas myVM1, e myVM3, de acordo as seguintes instruções:
 - 1. Aceda às definições da VM
 - 2. Em networking consulte as informações da interface de rede
 - 3. Nas definições da interface, em support + troubleshooting consulte a opção **efective routes**

The screenshot shows two main windows from the Microsoft Azure portal:

- Left Window (myVM - Networking):** Shows the 'Networking' blade for the virtual machine 'myVM'. The 'Networking' tab is selected. It displays two network interfaces: 'myVMNic1' and 'myVMNic2'. The 'myVMNic1' card is expanded, showing details like 'Virtual network/subnet: myResourceGroup-vnet/default', 'NIC Public IP: 40.122.43.96', and 'NIC Private IP: 10.1.1.1'. It also shows 'Inbound port rules' and 'Outbound port rules'. A large orange arrow points from the bottom right of this window towards the 'Effective routes' table in the adjacent window.
- Right Window (myVMNic1 - Effective routes):** Shows the 'Effective routes' table for the network interface 'myVMNic1'. The table has columns: Source, State, Address Prefixes, Next Hop Type, and Next Hop. The data includes five default routes:

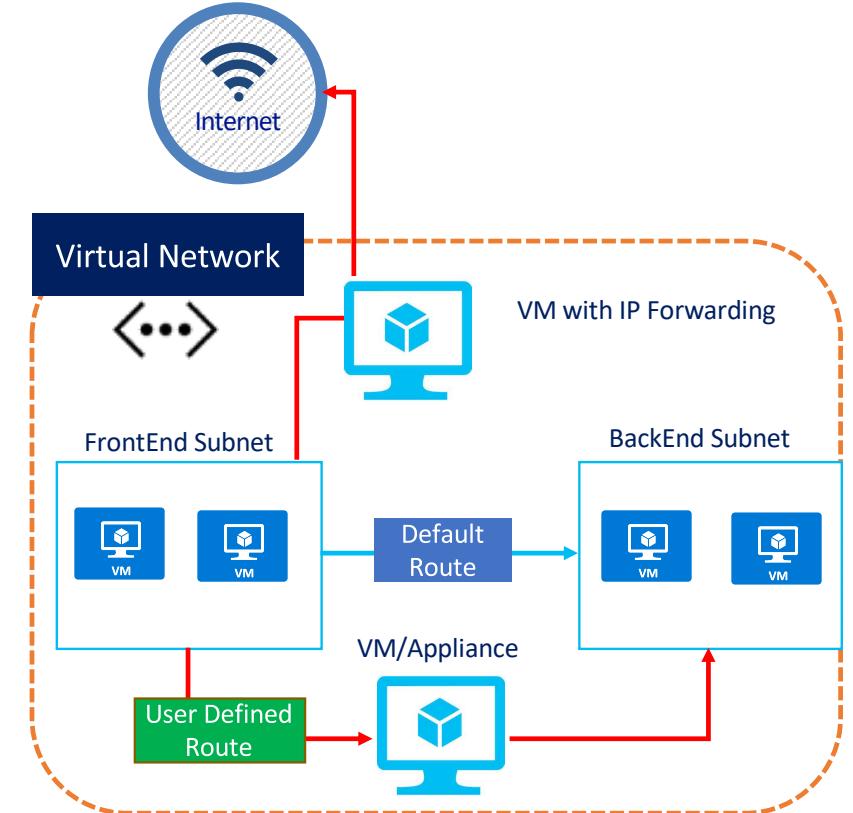
Source	State	Address Prefixes	Next Hop Type	Next Hop
Default	Active	10.1.1.0/24	Virtual network	-
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	192.168.0.0/16	None	-

Both windows have a red box highlighting the 'Networking' tab in the left sidebar and the 'Effective routes' link in the right sidebar.

Encaminhamento definido pelo Utilizador

User-Defined Routing /Rotas estáticas definidas pelo Utilizador

- Controlar o fluxo de tráfego com rotas personalizadas para:
 - Redes virtuais
 - Através de Virtual appliances
 - Através de Virtual network gateway
 - Internet: se tiver como next-hop type internet é faz o encaminhamento para esse endereço específico na Internet ou para o serviço Azure com um endereço IP público
- São inseridas nas tabelas de encaminhamento das subredes
- Especificam um Next-Hop para um prefixo de rede destino
- Permitem forçar que o tráfego seja encaminhado pelo túnel para as redes on-premises ou virtual network appliance (firewall ou outro dispositivo)



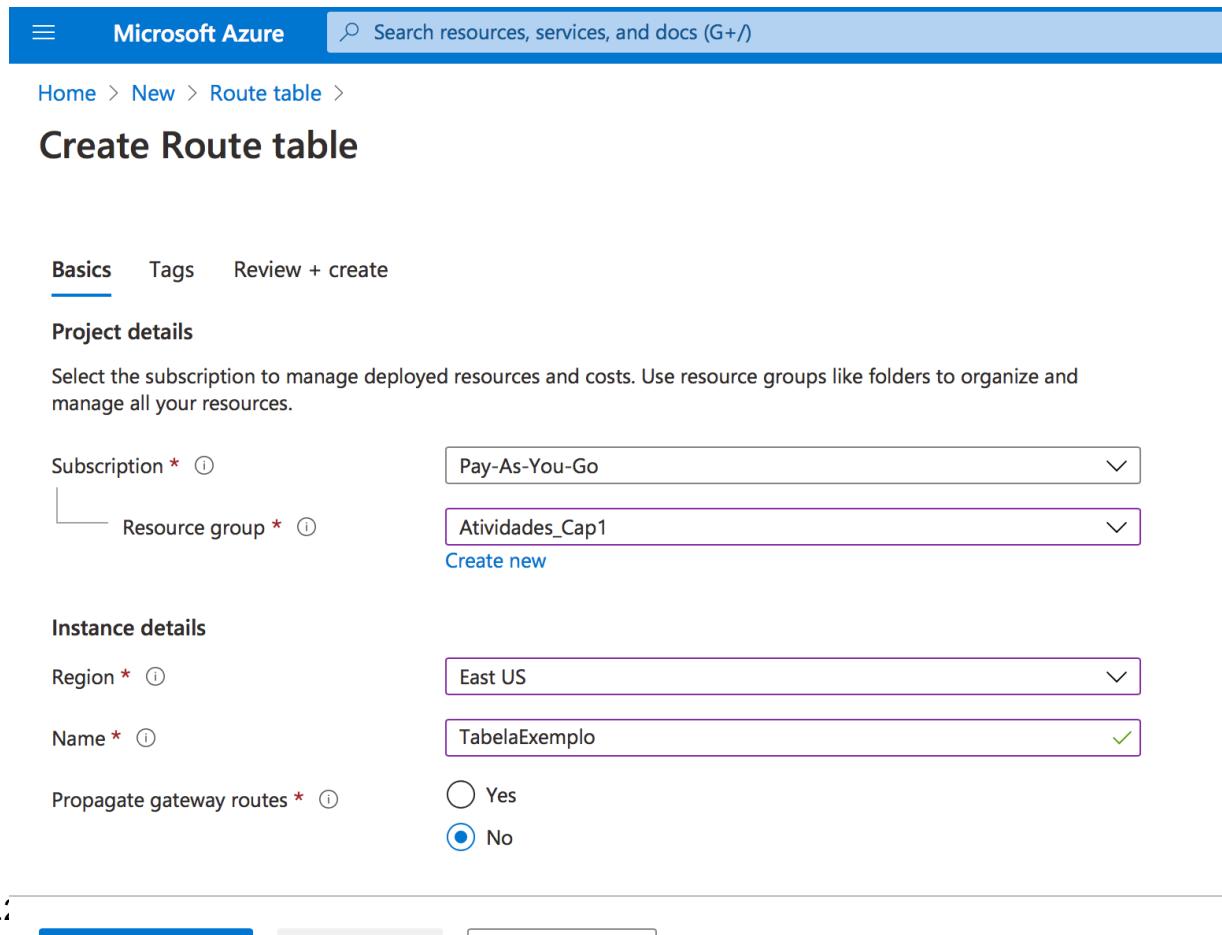


Demonstração Encaminhamento UDR

User-Defined Routing

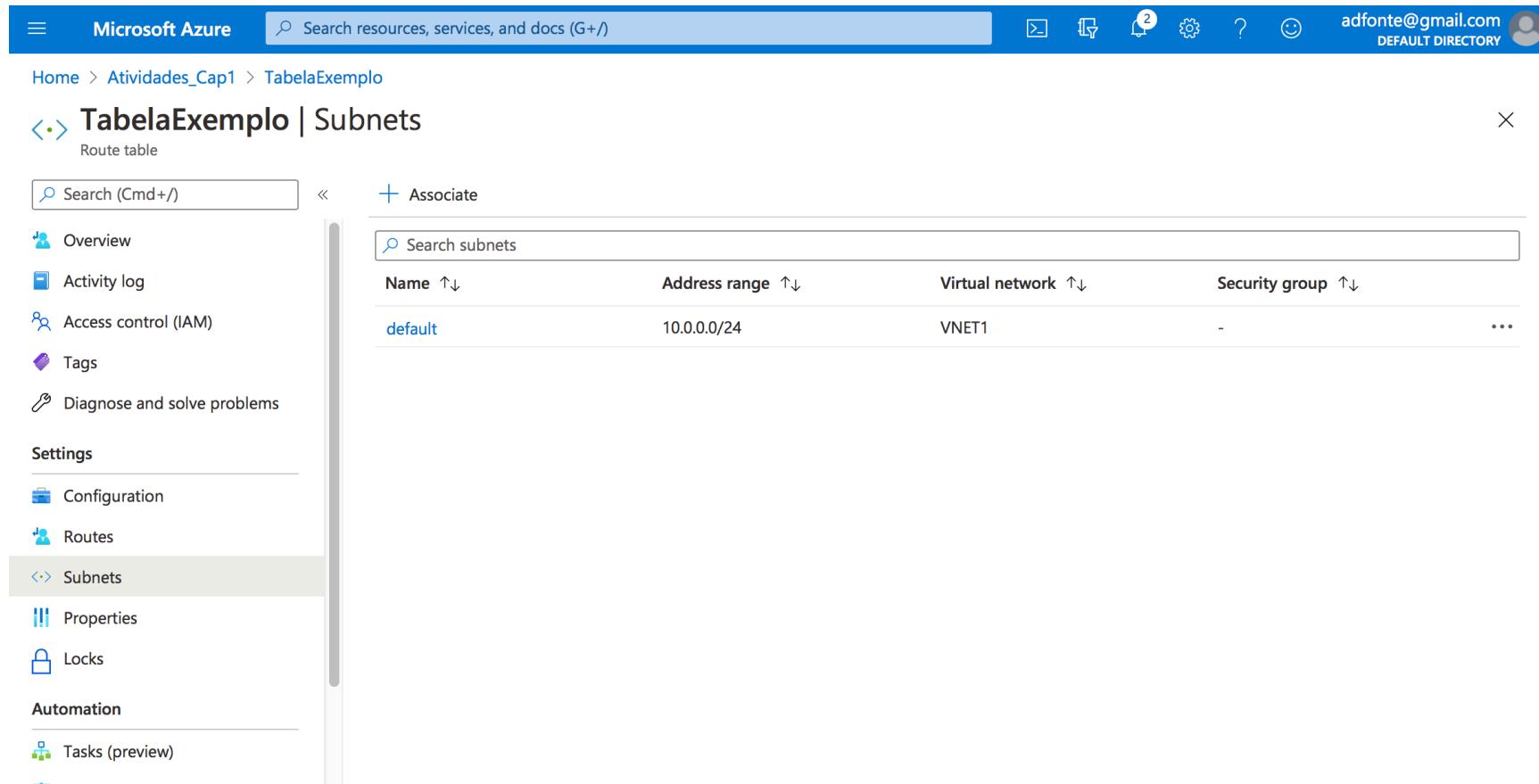


- Crie uma tabela de encaminhamento chamada TabelaExemplo
 - Associe a tabela à vnet1
 - Adicione uma rota por omissão direcionada para a internet



The screenshot shows the Microsoft Azure portal interface for creating a new route table. The top navigation bar includes the Microsoft Azure logo, a search bar, and a menu icon. Below the navigation, the breadcrumb trail shows 'Home > New > Route table >'. The main title is 'Create Route table'. The 'Basics' tab is selected, followed by 'Tags' and 'Review + create'. The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'Pay-As-You-Go'. The 'Resource group' dropdown is set to 'Atividades_Cap1', which is highlighted with a purple border. A 'Create new' link is visible below the dropdown. The 'Instance details' section includes fields for 'Region' (set to 'East US') and 'Name' (set to 'TabelaExemplo', also highlighted with a purple border). A 'Propagate gateway routes' section has two options: 'Yes' (unchecked) and 'No' (checked). At the bottom, there are 'Next Step' and 'Cancel' buttons.

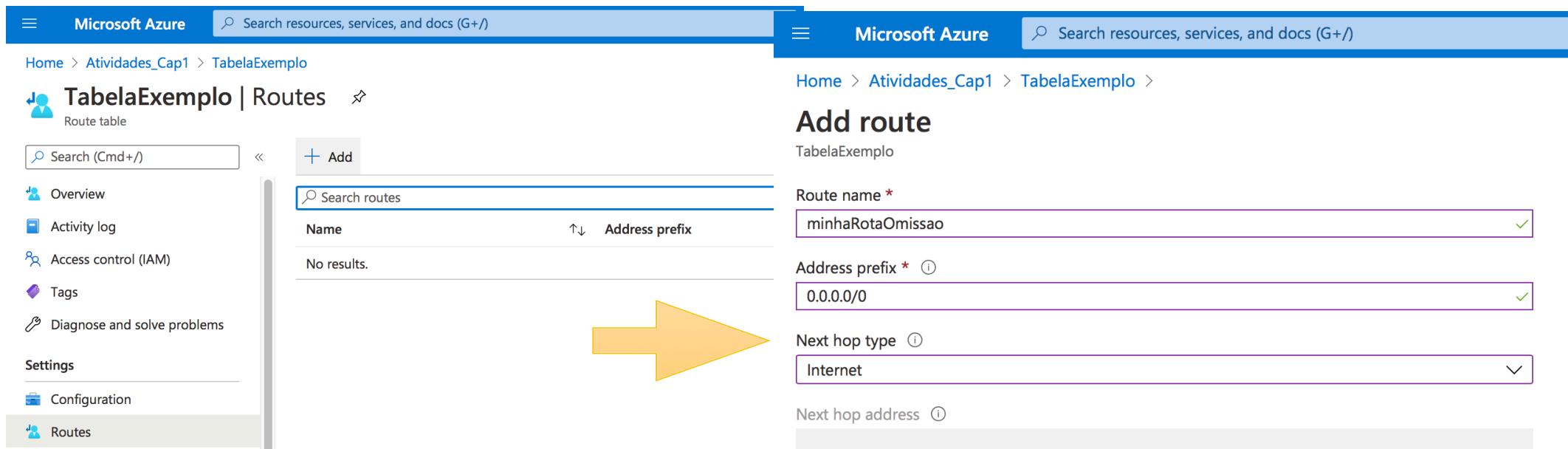
User-Defined Routing



The screenshot shows the Microsoft Azure portal interface for managing a route table named "TabelaExemplo". The left sidebar navigation includes "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (with "Configuration", "Routes", and "Subnets" selected), "Properties", "Locks", "Automation", and "Tasks (preview)". The main content area displays a table of subnets associated with the route table:

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓	...
default	10.0.0.0/24	VNET1	-	...

User-Defined Routing



The image shows two screenshots of the Microsoft Azure portal interface, illustrating the process of creating a user-defined route.

Screenshot 1: TabelaExemplo | Routes

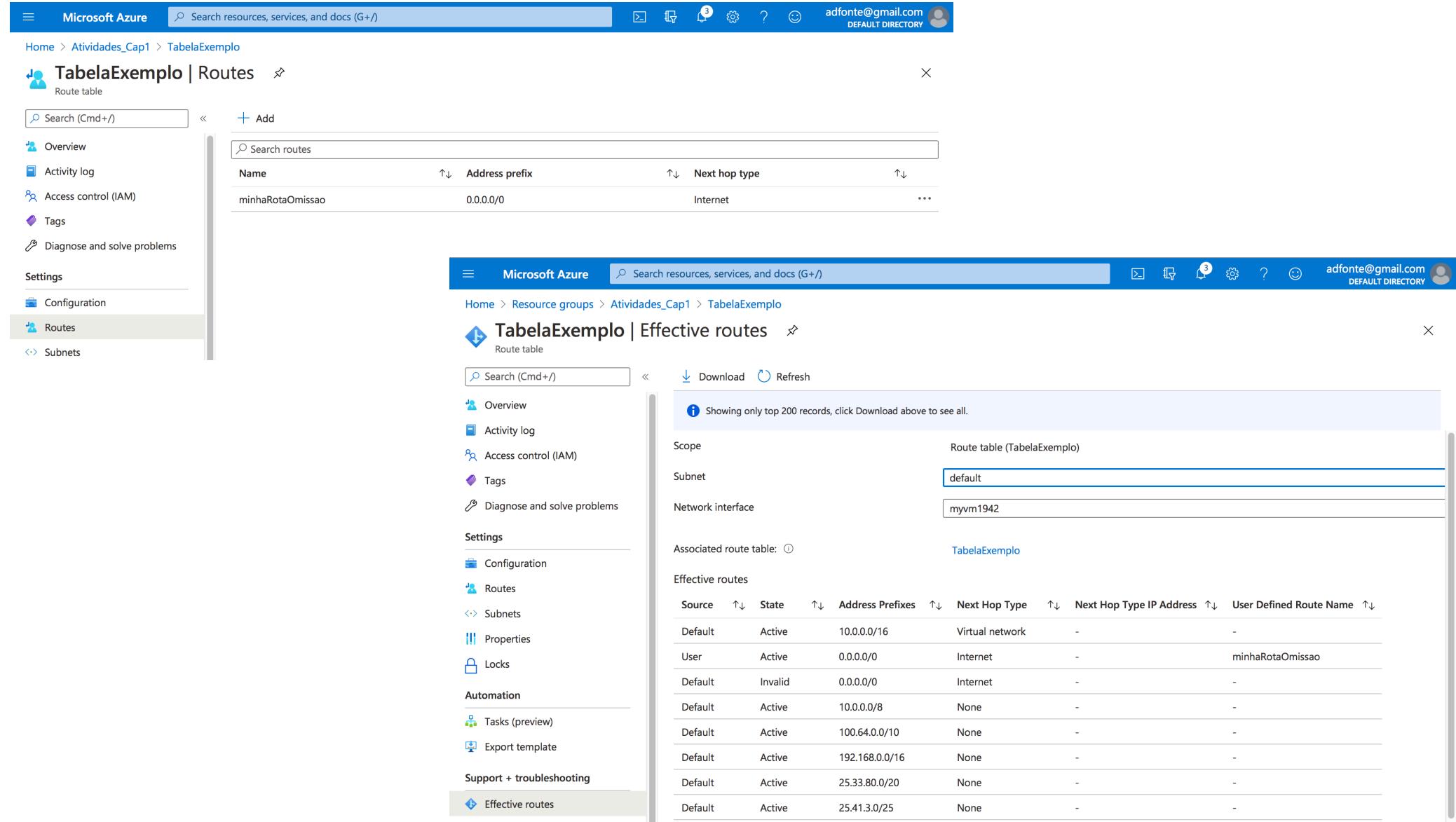
- Route table:** TabelaExemplo
- Search bar:** Search (Cmd+ /)
- Add button:** + Add
- Table header:** Search routes, Name, Address prefix
- Table body:** No results.
- Left sidebar:** Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Routes (selected).

Screenshot 2: Add route

- Route name:** minhaRotaOmissao
- Address prefix:** 0.0.0.0/0
- Next hop type:** Internet
- Next hop address:** (empty field)

A large orange arrow points from the 'Add' button in the first screenshot to the 'Route name' field in the second screenshot, indicating the flow of the process.

User-Defined Routing



The screenshot displays two Azure portal pages related to a user-defined route table named "TabelaExemplo".

Top Page: TabelaExemplo | Routes

- Route table:** minhaRotaOmissao
- Address prefix:** 0.0.0.0/0
- Next hop type:** Internet

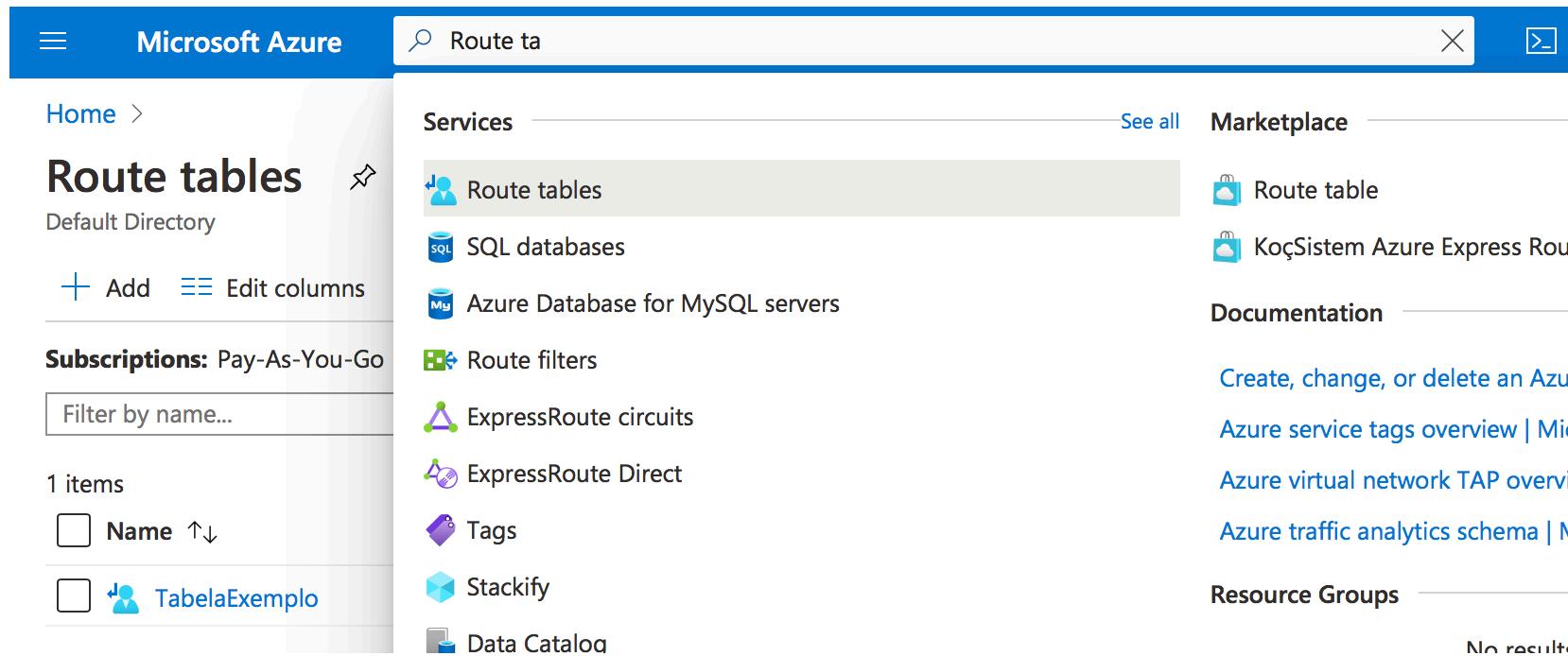
Bottom Page: TabelaExemplo | Effective routes

- Scope:** Route table (TabelaExemplo)
- Subnet:** default
- Network interface:** myvm1942
- Associated route table:** TabelaExemplo
- Effective routes:**

Source	State	Address Prefixes	Next Hop Type	Next Hop Type IP Address	User Defined Route Name
Default	Active	10.0.0.0/16	Virtual network	-	-
User	Active	0.0.0.0/0	Internet	-	minhaRotaOmissao
Default	Invalid	0.0.0.0/0	Internet	-	-
Default	Active	10.0.0.0/8	None	-	-
Default	Active	100.64.0.0/10	None	-	-
Default	Active	192.168.0.0/16	None	-	-
Default	Active	25.33.80.0/20	None	-	-
Default	Active	25.41.3.0/25	None	-	-

User-Defined Routing

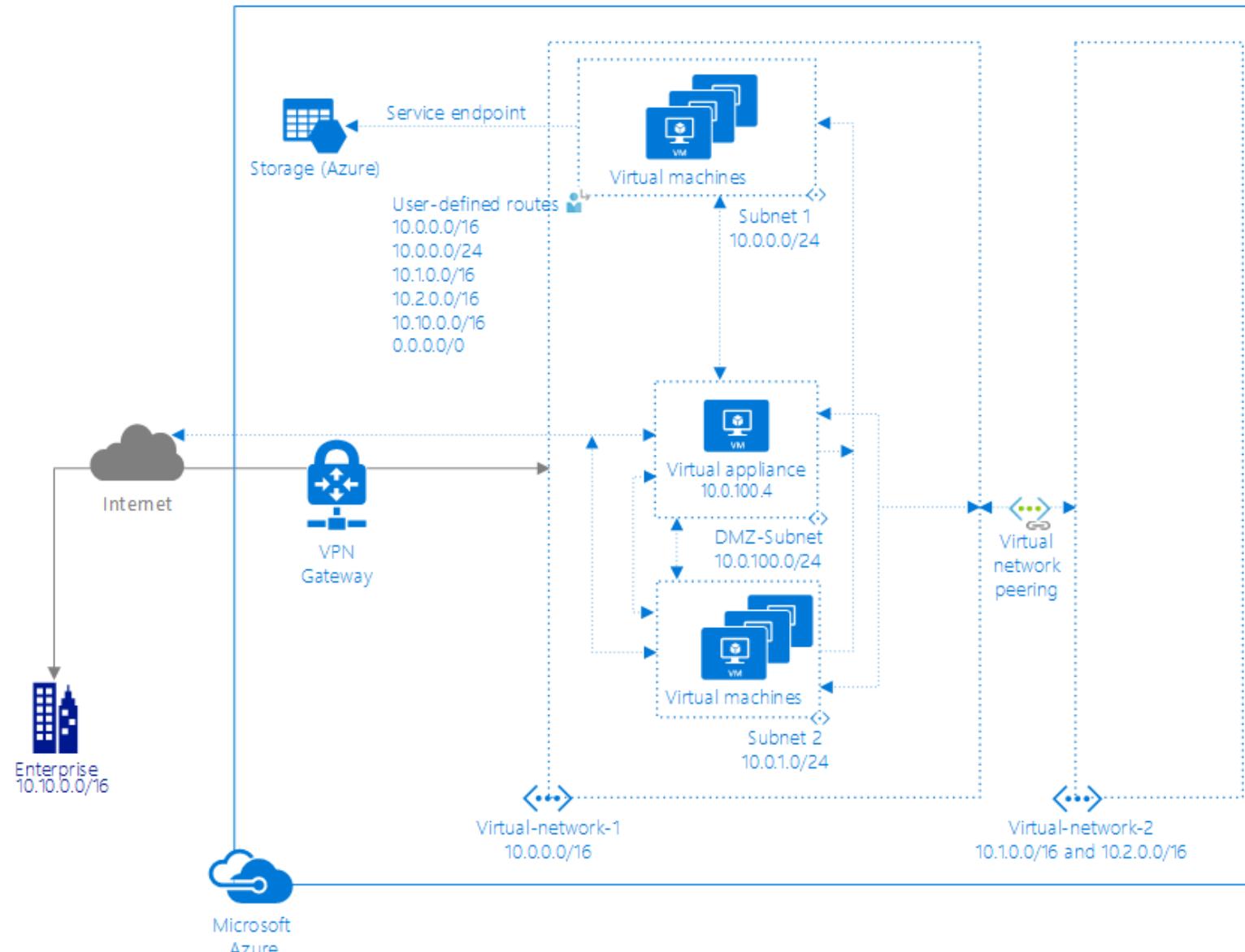
- Procura de uma tabela no Azure para modificar ou remover



The screenshot shows the Microsoft Azure portal interface. The top navigation bar is blue with the text "Microsoft Azure" and a search bar containing "Route ta". Below the navigation bar, the left sidebar shows the user is in the "Route tables" section under "Default Directory". The main content area displays a list of services. The "Route tables" service is highlighted with a gray background and a magnifying glass icon. Other listed services include "SQL databases", "Azure Database for MySQL servers", "Route filters", "ExpressRoute circuits", "ExpressRoute Direct", "Tags", "Stackify", and "Data Catalog". To the right, there are sections for "Marketplace", "Documentation", and "Resource Groups". The "Documentation" section contains links to "Create, change, or delete an Azure route table", "Azure service tags overview | Microsoft Docs", "Azure virtual network TAP overview | Microsoft Docs", and "Azure traffic analytics schema | Microsoft Docs". The "Resource Groups" section shows "No results".

Exemplo de Encaminhamento

<https://docs.microsoft.com/pt-pt/azure/virtual-network/virtual-networks-udr-overview>



Exemplo de Encaminhamento

Tabela de Encaminhamento da subrede1

ID	Source	State	Address prefixes	Next hop type	Next hop IP address	User-defined route name
1	Default	Invalid	10.0.0.0/16	Virtual network		
2	User	Active	10.0.0.0/16	Virtual appliance	10.0.100.4	Within-VNet1
3	User	Active	10.0.0.0/24	Virtual network		Within-Subnet1
4	Default	Invalid	10.1.0.0/16	VNet peering		
5	Default	Invalid	10.2.0.0/16	VNet peering		
6	User	Active	10.1.0.0/16	None		ToVNet2-1-Drop
7	User	Active	10.2.0.0/16	None		ToVNet2-2-Drop
8	Default	Invalid	10.10.0.0/16	Virtual network gateway	[X.X.X.X]	
9	User	Active	10.10.0.0/16	Virtual appliance	10.0.100.4	To-On-Prem
10	Default	Active	[X.X.X.X]	VirtualNetworkServiceEndpoint		
11	Default	Invalid	0.0.0.0/0	Internet		
12	User	Active	0.0.0.0/0	Virtual appliance	10.0.100.4	

Network Virtual Appliances

Network Virtual Appliances

Network virtual appliances (NVA): A network virtual appliance is a virtual machine running software that performs a network function, such as a firewall.

Network virtual appliances are also available that provide WAN optimization and other network traffic functions.

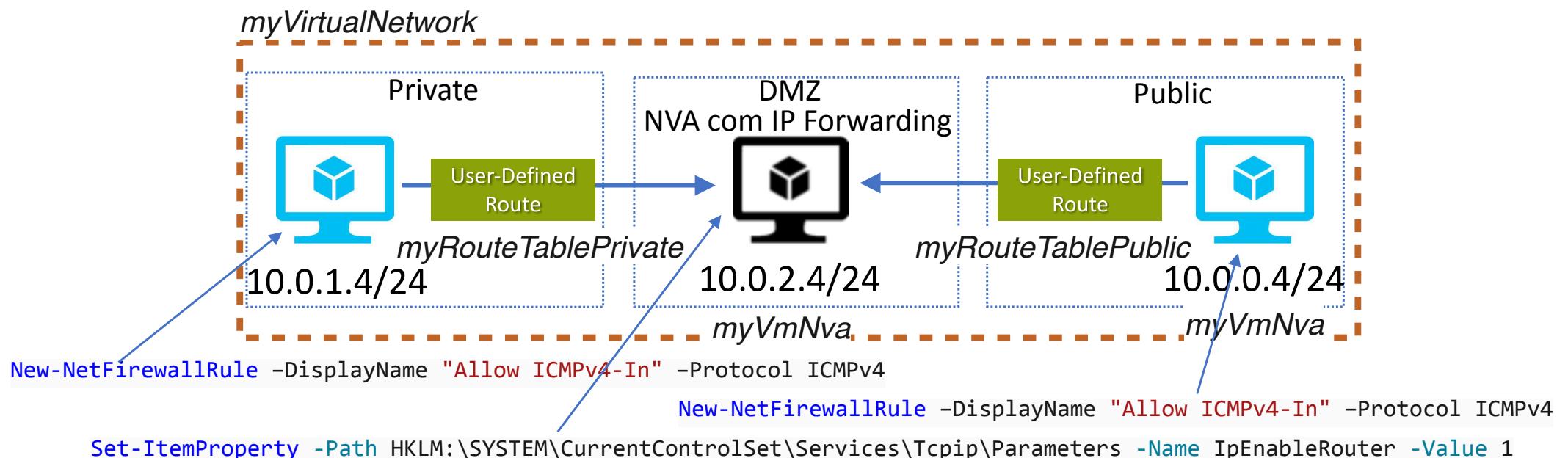
Network virtual appliances are typically used with user-defined or BGP routes.

You can also use a network virtual appliance to filter traffic between virtual networks.

User-Defined Routing - Encaminhamento através de uma NVA



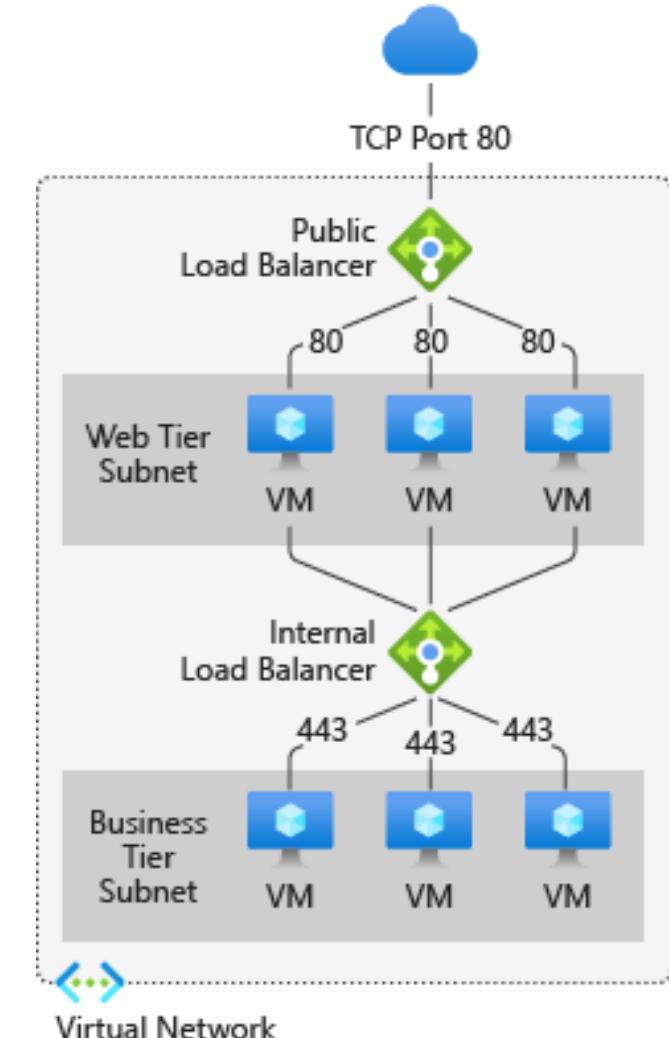
- Realizar o Laboratório disponível em:
<https://docs.microsoft.com/pt-pt/azure/virtual-network/tutorial-create-route-table-portal>



Introdução aos Balanceadores de Carga

Conceito e Motivação

- O **equilíbrio de carga** refere-se à distribuição uniforme da carga (tráfego de rede de entrada) através de um grupo de recursos ou servidores de *backend*.
- O Azure Load Balancer opera na camada de transporte do modelo Open Systems Interconnection (OSI).
- É o único ponto de contacto para os clientes. O Balanceador de Carga distribui os fluxos de entrada que chegam à parte frontal do Balanceador de carga pelas instâncias da *backend pool* de servidores.
- Estes fluxos são distribuídos de acordo com regras de equilíbrio de carga configuradas e as sondas sanitárias (healthy probes).
- As instâncias de backend pool podem ser Máquinas Virtuais Azure ou instâncias de um conjunto escalável de máquinas virtuais.
- Informações detalhadas em: <https://docs.microsoft.com/pt-pt/azure/load-balancer/>



Introdução aos Balanceadores de Carga

Conceito e Motivação

- A principal motivação de usar balanceadores de carga é permitir a escalabilidade de aplicações.
- Com o Balanceador de Carga, pode-se escalar as aplicações e criar serviços altamente disponíveis.
- O Balanceador de carga suporta cenários de entrada e saída. O balanceador de carga proporciona baixa latência, e escala até milhões de fluxos para todas as aplicações TCP e UDP.
- Os cenários-chave que pode realizar usando o Balancer de Carga Padrão incluem:
 - Equilibrar o tráfego interno e externo entre máquinas virtuais Azure.
 - Configurar a conectividade de saída para máquinas virtuais Azure.
 - Usar sondas sanitárias para monitorizar recursos equilibrados em carga.
 - Empregar o port forwarding para aceder a máquinas virtuais numa rede virtual por endereço IP público e porta.
 - Ativar o suporte para o equilíbrio de carga do IPv6.
 - Distribuir a carga dos serviços por várias portas, vários endereços IP, ou ambos.
- etc etc
- **Pricing and SLA**
 - For Standard Load Balancer pricing information, see Load Balancer pricing. Basic Load Balancer is offered at no charge. See SLA for Load Balancer. Basic Load Balancer has no SLA.

Introdução aos Balanceadores de Carga Componentes de um LB (FRONTEND)

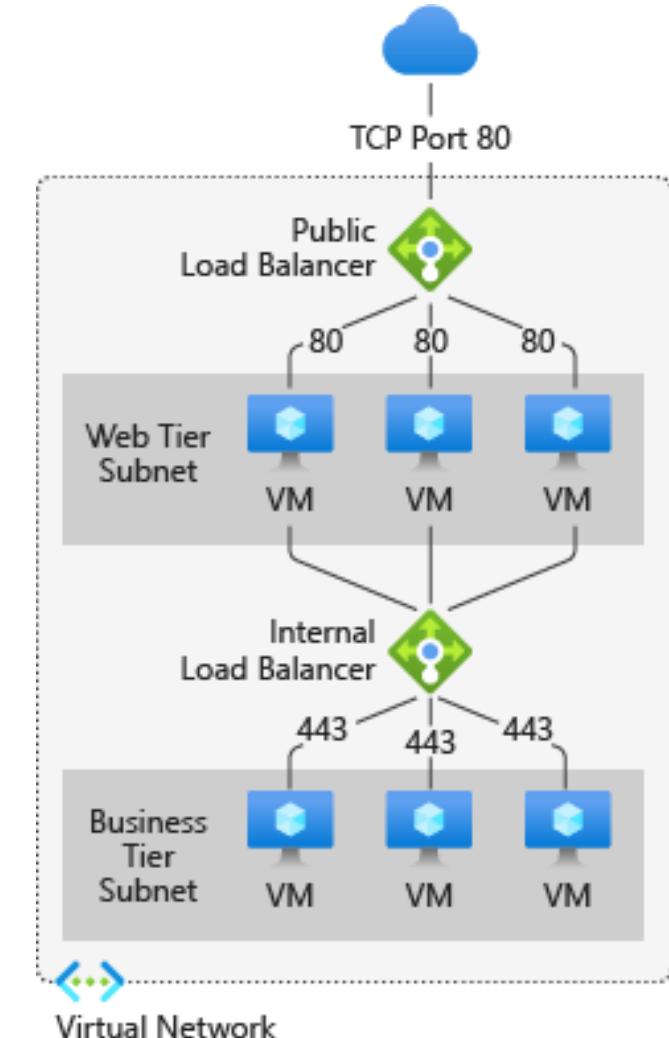
- Configuração IP do Frontend

-Trata-se do endereço IP do Azure Load Balancer. É o ponto de contacto para os clientes. Estes endereços IP podem ser:

- Endereços IP Públicos
- Endereços IP Privados

-A natureza do endereço IP determina o tipo de balanceado de carga criado.

- A selecção de um Endereço IP Privado cria um balanceado de carga interno.
- A selecção de um Endereço IP Público cria um balanceado de carga público.



Introdução aos Balanceadores de Carga Componentes de um LB (FRONTEND)

	Public Load Balancer	Internal Load Balancer
Frontend IP configuration	Public IP address	Private IP address
Description	A public load balancer maps the public IP and port of incoming traffic to the private IP and port of the VM. Load balancer maps traffic the other way around for the response traffic from the VM. You can distribute specific types of traffic across multiple VMs or services by applying load-balancing rules. For example, you can spread the load of web request traffic across multiple web servers.	An internal load balancer distributes traffic to resources that are inside a virtual network. Azure restricts access to the frontend IP addresses of a virtual network that are load balanced. Front-end IP addresses and virtual networks are never directly exposed to an internet endpoint. Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources.
SKUs supported	Basic, Standard	Basic, Standard

Introdução aos Balanceadores de Carga Componentes de um LB (BACKEND POOL)

- Backend pool
 - É o grupo de máquinas virtuais ou instâncias que pertence a conjunto escalável de máquina virtuais (virtual machine scale set) que atende os pedidos de entrada.
 - Para para atender a altos volumes de tráfego de entrada, as diretrizes de computação geralmente recomendam a adição de mais instâncias de VMs ao pool de back-end.
 - **O balanceador de carga reconfigura-se automaticamente quando se aumenta ou diminui o número de instâncias.** Adicionar ou remover VMs da pool de back-end reconfigura o balanceador de carga sem operações adicionais.

Introdução aos Balanceadores de Carga Componentes de um LB (BACKEND POOL)

- Backend pool
 - Em vez de criar uma VM de cada vez, por exemplo, VM1, VM2 e VM3 o melhor é criar um conjunto escalável de 3 VMs.
 - Alguns Benefícios
 - Criação, configuração simultânea das várias VMs
 - Manutenção de uma configuração consistente
 - Ler mais em:<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview>

Introdução aos Balanceadores de Carga

Componentes de um LB (Health probes)

- **Health probes** (sondas de saúde ou sondas sanitárias)
 - É possível definir limites (**unhealthy threshold**) a partir dos quais o LB considera que a instância não está saudável.
 - Uma proba falha quando não tem resposta num certo tempo limite, nesse caso o Load Balancer pára de enviar novas ligações para as instâncias “não saudáveis”. Contudo esta falha não afeta as ligações existentes. A ligação continua até a aplicação:
 - O fluxo de tráfego termina explicitamente (Ends the flow)
 - Fica inativa (Idle timeout occurs)
 - A VM foi/está desligada
 - O Load Balancer fornece diferentes tipos de *health probes* para verificar o estado das instâncias: TCP, HTTP, and HTTPS.
 - Um LB Básico (Basic Load Balancer) não suporta HTTPS probes.

	TCP	HTTP	HTTPS
SKU Standard	✓	✓	✓
SKU Básico	✓	✓	✗

Introdução aos Balanceadores de Carga

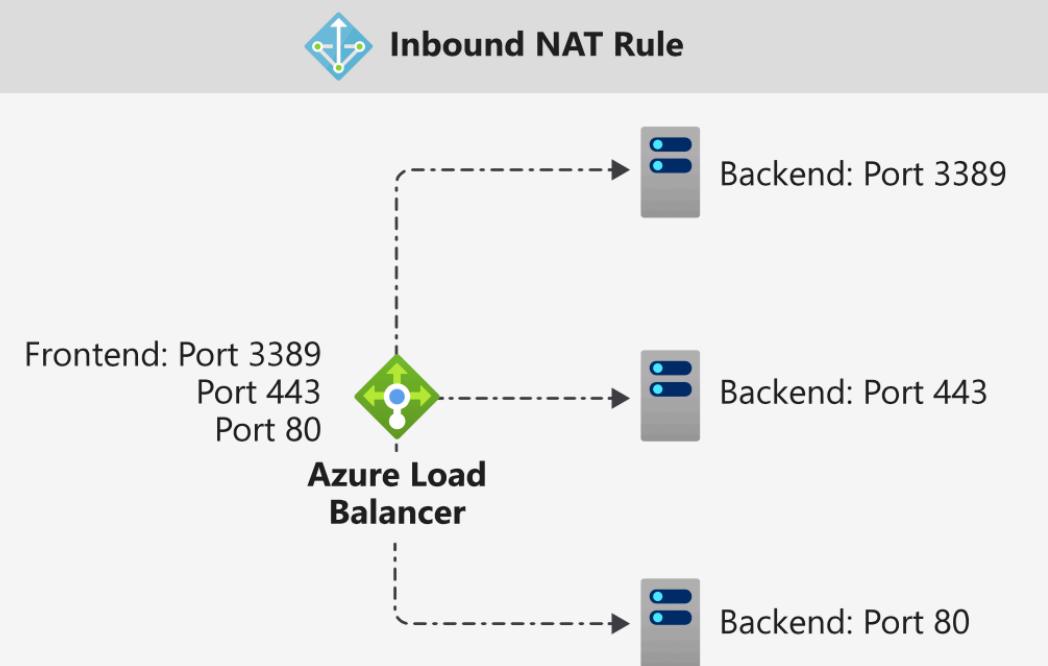
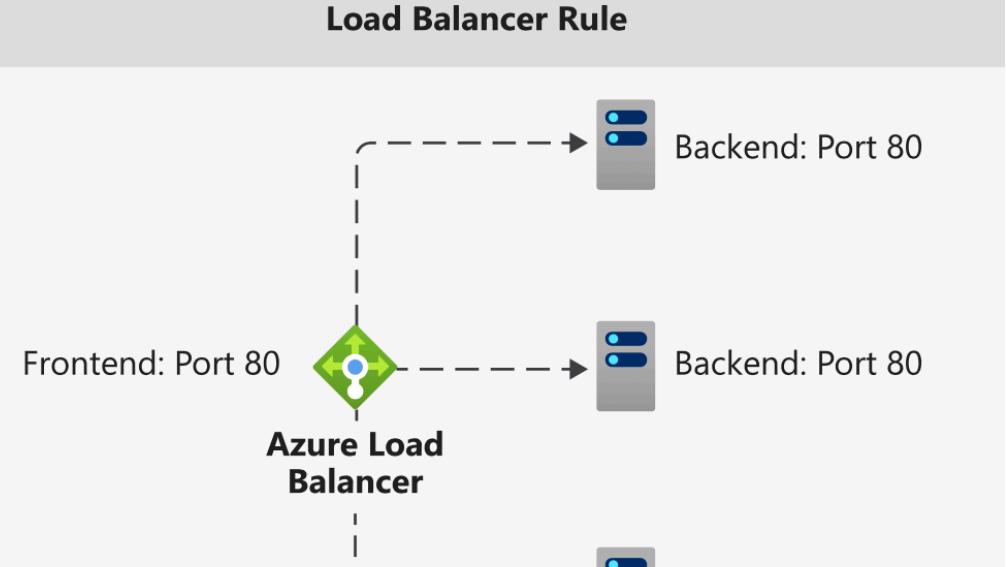
Regras de Balanceamento de Carga

- Load Balancing rules

- Uma regra de balanceador de carga é usada para definir como o tráfego de entrada é distribuído pelas as instâncias da pool de back-end.

- Uma regra de平衡amento de carga mapeia uma determinada configuração IP de front-end e porta em vários endereços IP e portas de back-end.

- Por exemplo, use uma regra de balanceamento de carga para a porta 80 para rotear o tráfego de seu IP de front-end para a porta 80 de suas instâncias de back-end





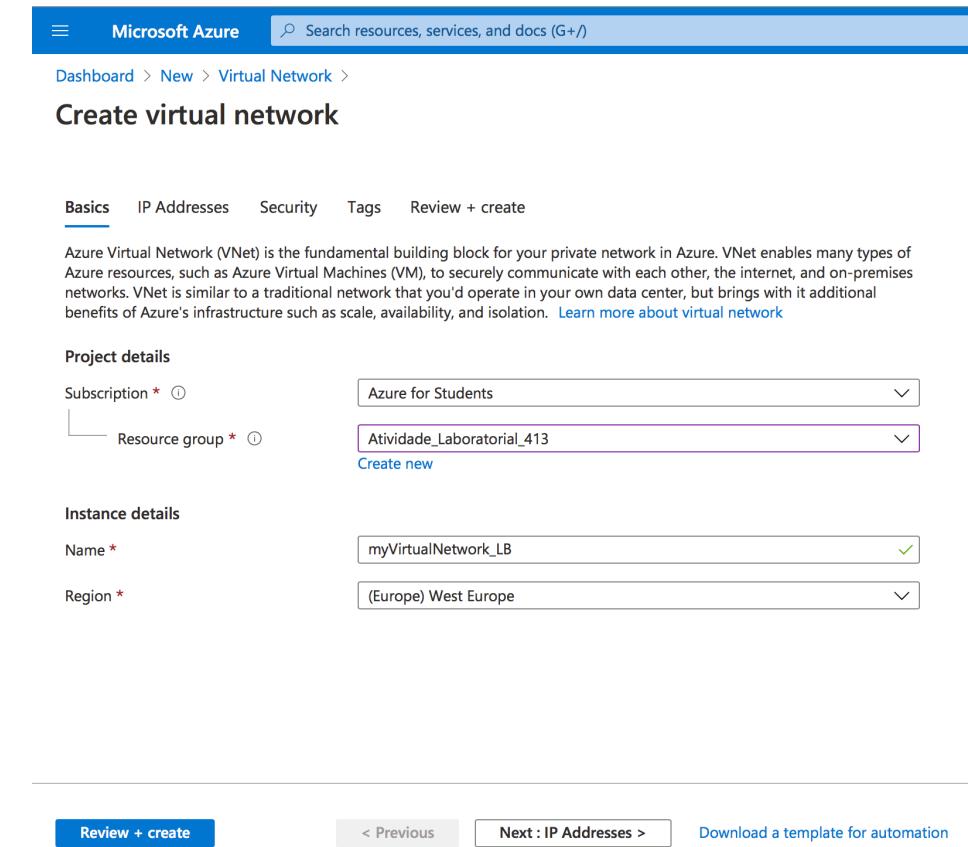
Demonstração Criação de um Balanceador de Carga

Introdução aos Balanceadores de Carga



Criar um Balanceador de Carga e um Conjunto de máquinas virtuais

- 1. Comece por criar um Grupo de Recursos chamado TVCD
- 2. Crie uma rede virtual e uma subrede de acordo com a seguinte especificação
 - **myVirtualNetwork_LB**
 - Espaço de endereçamento: 172.16.0.0/16
 - Subrede:
mySubnet
172.16.1.0/24



Microsoft Azure Search resources, services, and docs (G+)

Dashboard > New > Virtual Network >

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * Resource group * [Create new](#)

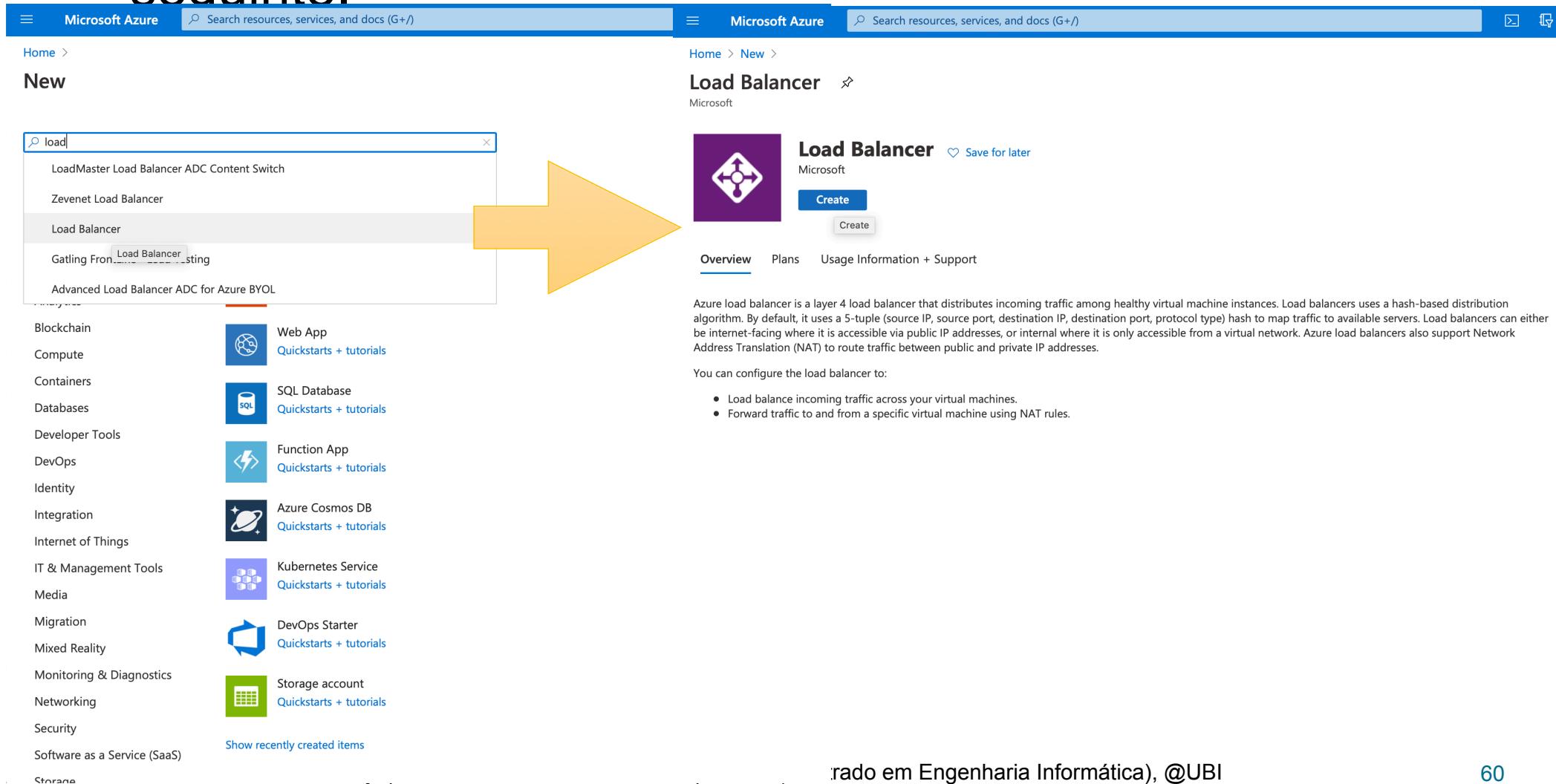
Instance details

Name * Region *

Review + create < Previous Next : IP Addresses > Download a template for automation

Introdução aos Balanceadores de Carga

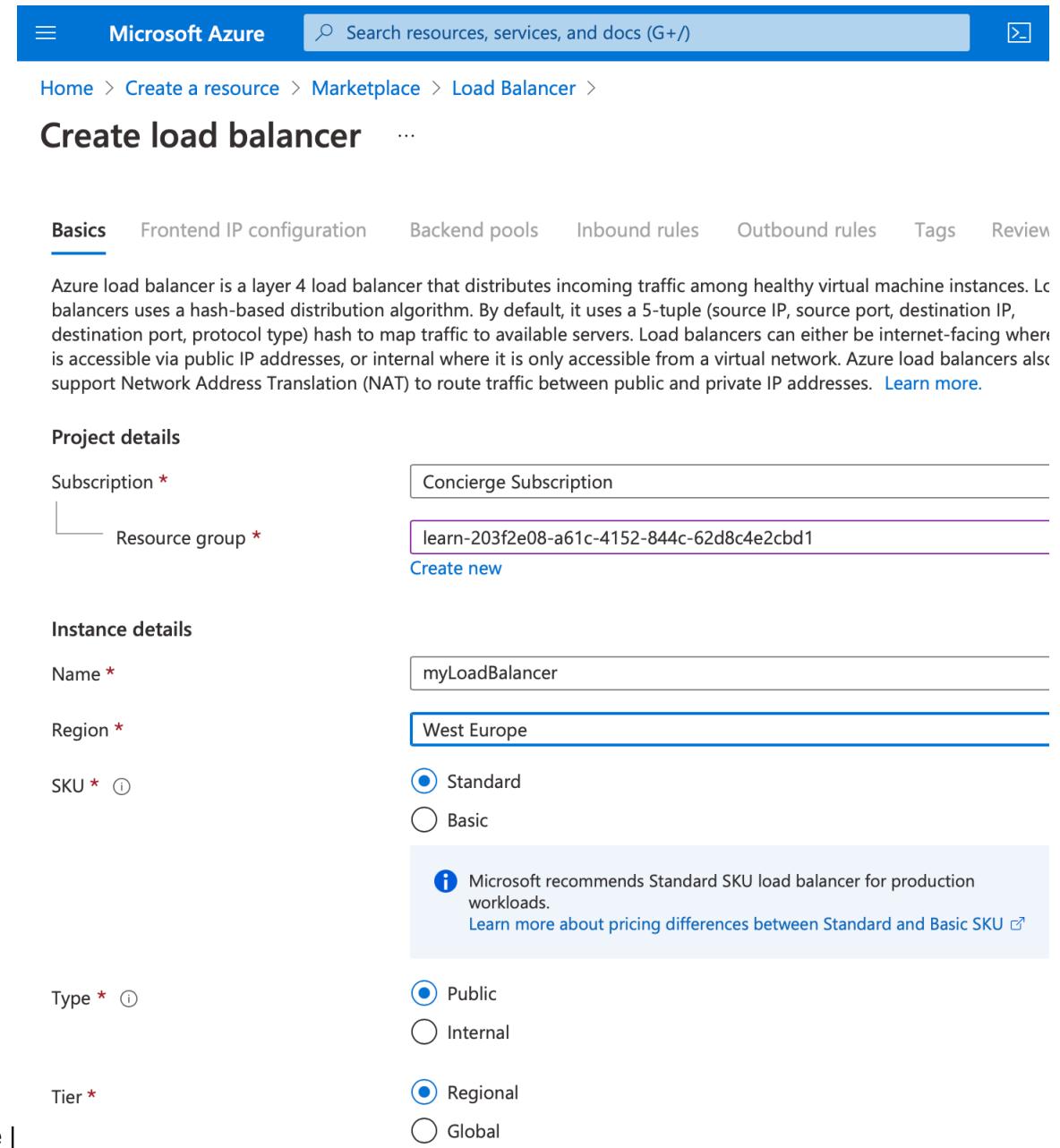
- 3. A partir do Azure marketplace, crie um balanceador de carga público, conforme o formulário do slide seguinte.



The image shows two screenshots of the Microsoft Azure Marketplace. On the left, a search bar contains the term "load". Below the search bar, a list of results includes "LoadMaster Load Balancer ADC Content Switch", "Zevenet Load Balancer", "Load Balancer" (which is highlighted with a red underline), "Gatling Frontend Load Balancing", and "Advanced Load Balancer ADC for Azure BYOL". On the right, the "Load Balancer" product page is displayed. It features a purple icon with four arrows pointing outwards, the title "Load Balancer" with a "Create" button, and a detailed description of the service. A large orange arrow points from the search result on the left to the product page on the right.

Introdução aos Balanceadores de Carga

- 3.1 Dados do novo balanceador de carga:
 - Nome: **myLoadBalancer**
 - Região: **West Europe**
 - SKU: **standard**
 - Tipo: **público**
 - Tier: **Regional**



The screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal, specifically the 'Basics' step. The page title is 'Create load balancer'. The 'Basics' tab is selected, while other tabs like 'Frontend IP configuration', 'Backend pools', 'Inbound rules', 'Outbound rules', 'Tags', and 'Review' are visible. The main content area describes an Azure load balancer as a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. It mentions the default hash-based distribution algorithm and supports internet-facing and internal access via public or private IP addresses, including Network Address Translation (NAT). A 'Learn more' link is provided.

Project details

Subscription *: Concierge Subscription

Resource group *: learn-203f2e08-a61c-4152-844c-62d8c4e2cbd1
Create new

Instance details

Name *: myLoadBalancer

Region *: West Europe

SKU *: Standard (selected)

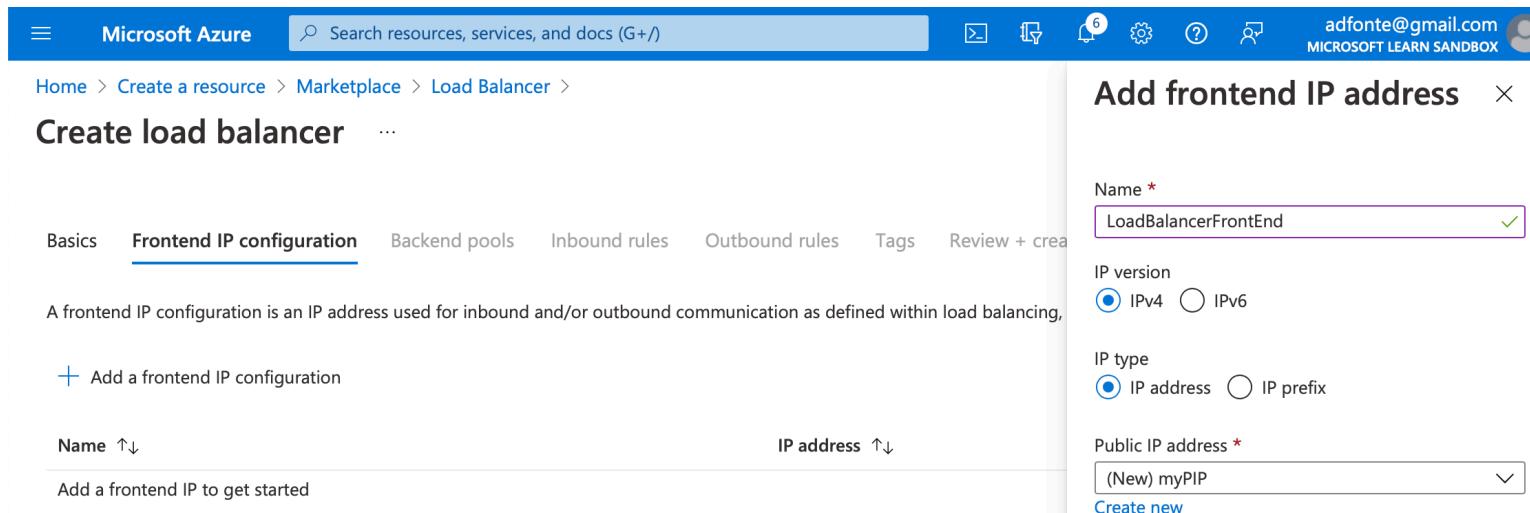
Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU ↗

Type *: Public (selected)

Tier *: Regional (selected)

Introdução aos Balanceadores de Carga

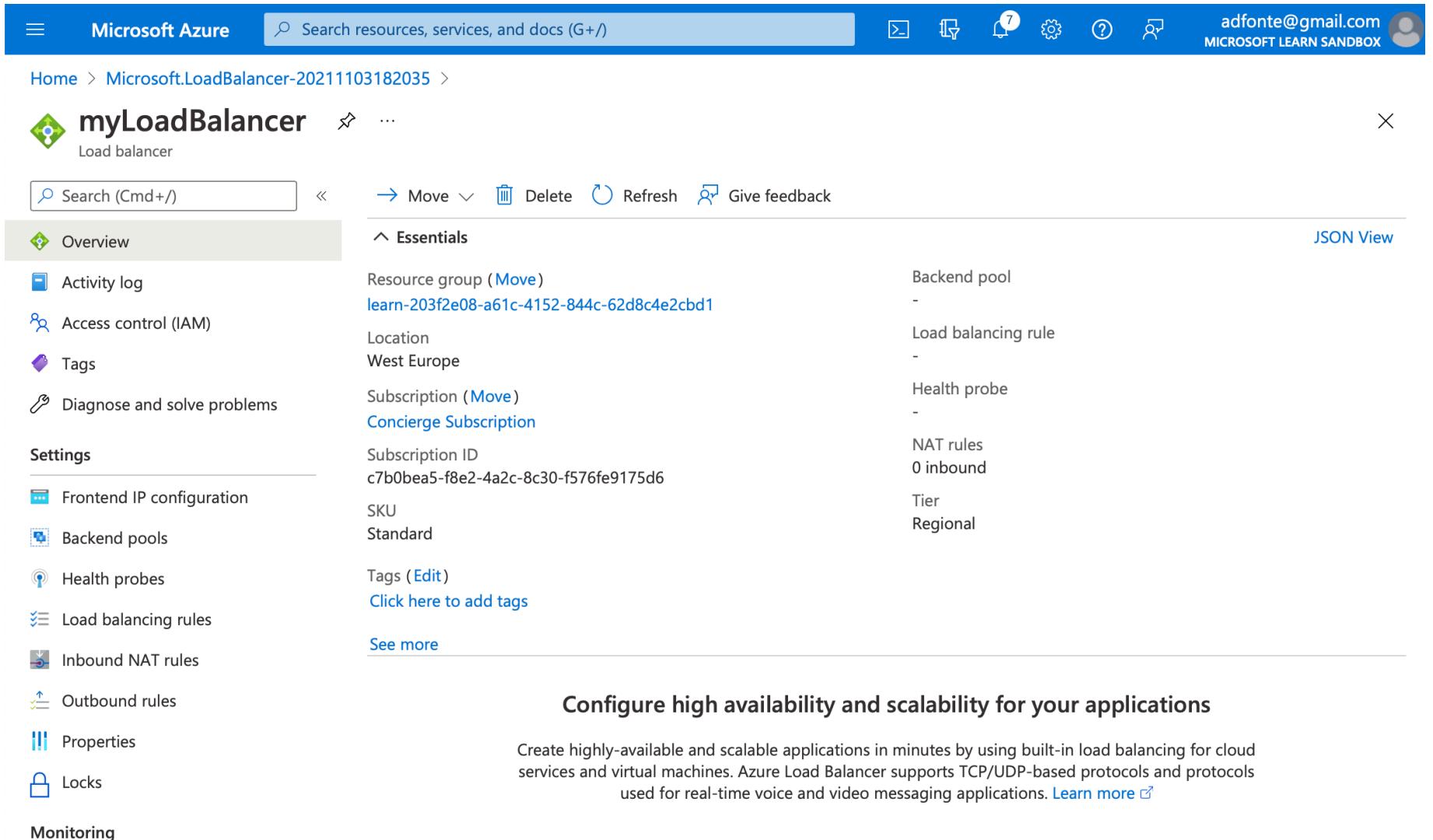
- 3.2 Dados do Front-End do LB:
 - Nome: LoadBalancerFrontEnd
 - Endereço IP Público: myPIP
- Nota: Após definir o Front-End já pode criar o Balanceador de carga, embora no novo portal do Azure pode ainda configurar a Backend Pool e a regras de LB.



The screenshot shows the Microsoft Azure portal interface for creating a load balancer. The main navigation bar includes 'Microsoft Azure', a search bar, and user information (adfonte@gmail.com, MICROSOFT LEARN SANDBOX). Below the navigation is a breadcrumb trail: Home > Create a resource > Marketplace > Load Balancer > Create load balancer. The current step is 'Frontend IP configuration'. A modal window titled 'Add frontend IP address' is open, prompting for a name (LoadBalancerFrontEnd), IP version (IPv4 selected), IP type (IP address selected), and a public IP address (New myPIP). Other tabs like Basics, Backend pools, and Inbound rules are visible at the top of the page.

Introdução aos Balanceadores de Carga

- 3.1 (Continuação) Visualização do recurso Load Balancer



The screenshot shows the Microsoft Azure portal interface for a 'myLoadBalancer' load balancer. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. The main content area displays the 'Overview' tab of the load balancer's configuration. Key details shown include:

- Resource group:** learn-203f2e08-a61c-4152-844c-62d8c4e2cbd1
- Location:** West Europe
- Subscription:** Concierge Subscription
- Backend pool:** -
- Load balancing rule:** -
- Health probe:** -
- NAT rules:** 0 inbound
- Tier:** Regional

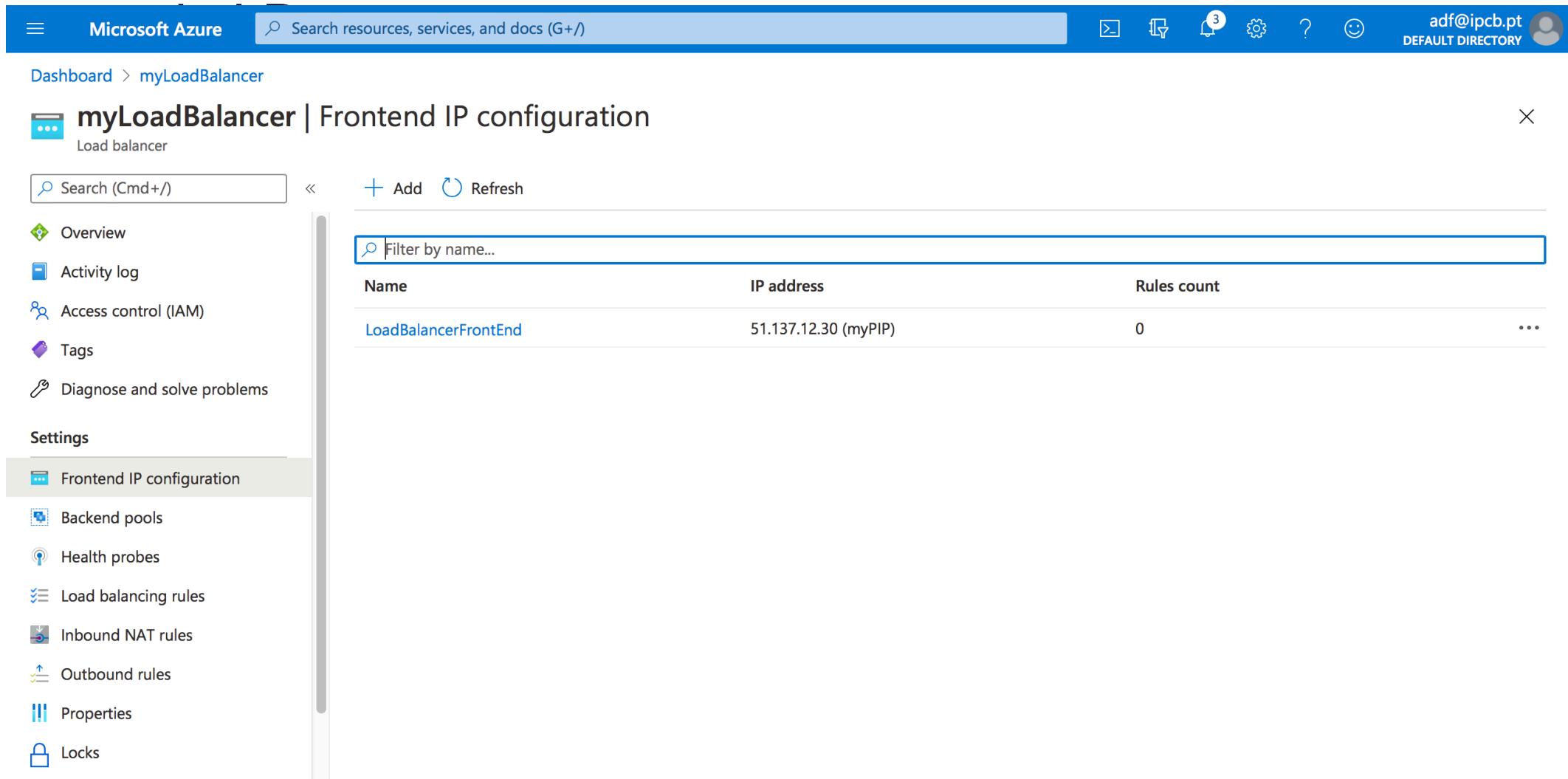
The left sidebar lists other configuration tabs: Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Frontend IP configuration, Backend pools, Health probes, Load balancing rules, Inbound NAT rules, Outbound rules, Properties, Locks), Monitoring, and JSON View.

Configure high availability and scalability for your applications

Create highly-available and scalable applications in minutes by using built-in load balancing for cloud services and virtual machines. Azure Load Balancer supports TCP/UDP-based protocols and protocols used for real-time voice and video messaging applications. [Learn more](#)

Introdução aos Balanceadores de Carga

- 3.1 (Cont.) Visualização da configuração do FrontEnd



The screenshot shows the Microsoft Azure portal interface for managing a Load Balancer named "myLoadBalancer". The left sidebar navigation bar is visible, showing the current section: "Frontend IP configuration". The main content area displays the "Frontend IP configuration" for the load balancer, listing one entry:

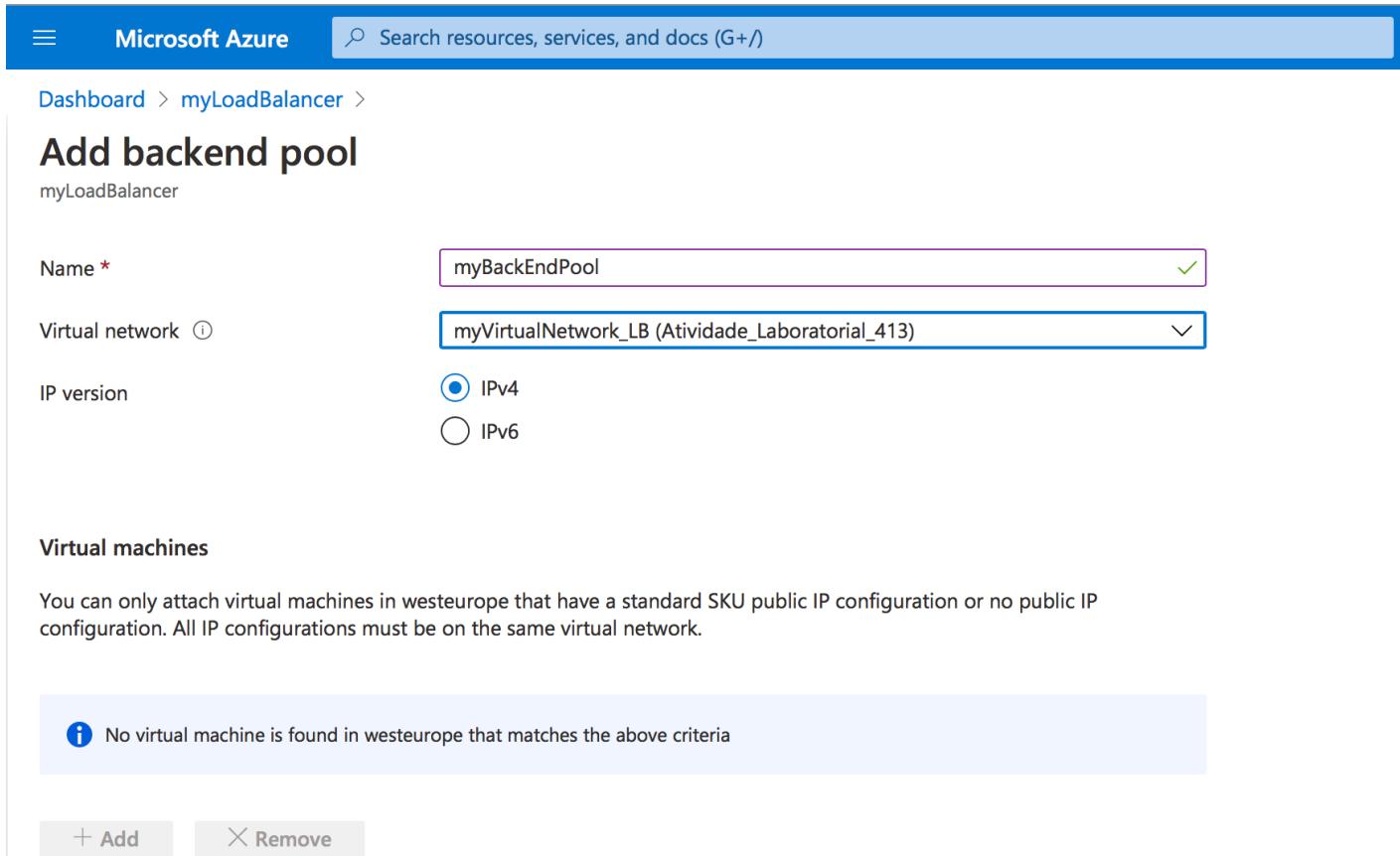
Name	IP address	Rules count
LoadBalancerFrontEnd	51.137.12.30 (myPIP)	0

Introdução aos Balanceadores de Carga

- 4. Criar/Configurar os recursos do Balanceador de Carga
 - Load balancer settings for a backend address pool.
 - Sondas sanitárias (health probes).
 - Regra de Balanceamento de Carga (load balancer rule).

Introdução aos Balanceadores de Carga

- 4.1 Criação da Backend pool de endereços de servidores
 - Em settings->Backend pools->Add
 - Nome: myBackEndPool



The screenshot shows the 'Add backend pool' configuration page in the Microsoft Azure portal. The page title is 'Add backend pool' under 'myLoadBalancer'. The 'Name' field is set to 'myBackEndPool'. The 'Virtual network' dropdown is set to 'myVirtualNetwork_LB (Atividade_Laboratorial_413)'. The 'IP version' radio button is selected for 'IPv4'. Below this, the 'Virtual machines' section notes that only virtual machines in 'westeurope' with standard SKU public IP configurations can be attached. A message indicates no matching virtual machines were found. At the bottom, there are '+ Add' and 'X Remove' buttons.

Introdução aos Balanceadores de Carga

- 4.2 Crie Duas Health Probes TCP para a portas 80 e 3389
 - Nomes: myHTTPProbe e myRDPPProbe
 - Intervalo de probing 5 segundos e 2 respostas falhas

Microsoft Azure Search resources, services, and docs (G+/)

Dashboard > myLoadBalancer >

Add health probe

myLoadBalancer

Name *

Protocol

TCP

Port *

80

Interval *

5 seconds

Unhealthy threshold *

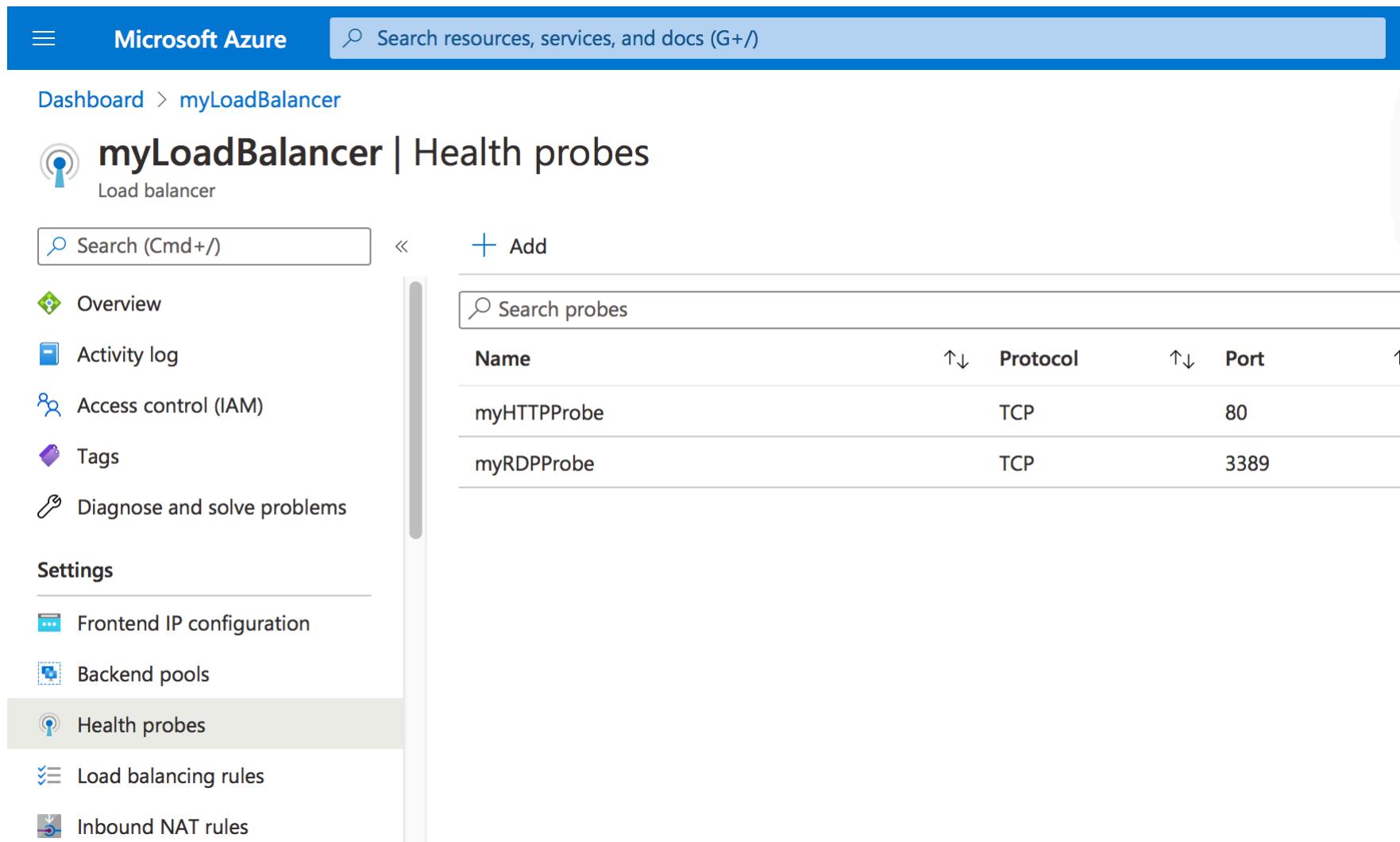
2 consecutive failures

OK

O intervalo mínimo da sonda é de 5 segundos e o número mínimo de respostas pouco saudáveis é 2. A duração total de todos os intervalos não pode exceder 120 segundos.

Introdução aos Balanceadores de Carga

- 4.2 (Cont.) Duas Health Probes TCP para a portas 80 e 3389



The screenshot shows the Microsoft Azure portal interface for managing a load balancer named "myLoadBalancer". The left sidebar navigation bar is visible, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools, Health probes (which is currently selected and highlighted in grey), Load balancing rules, and Inbound NAT rules. The main content area displays the "Health probes" section for "myLoadBalancer". It includes a search bar labeled "Search probes", a "Add" button, and a table listing two health probes:

Name	Protocol	Port
myHTTPProbe	TCP	80
myRDPProbe	TCP	3389

Introdução aos Balanceadores de Carga

- 4.3. Adição de uma regra de balanceamento de carga

-Uma regra LB define como o tráfego é distribuído pelas VMs.

-Na configuração é preciso definir a configuração IP do frontend para o tráfego de entrada e a backend pool para receber o tráfego. As portas de origem e destino são definidas na regra de balanceamento de carga:

- Uma regra chamada myHTTPRule.

Porta 80 a escutar

Direccionar o tráfego load balanced traffic para o backend com o nome myBackendPool na porta Porta 80.

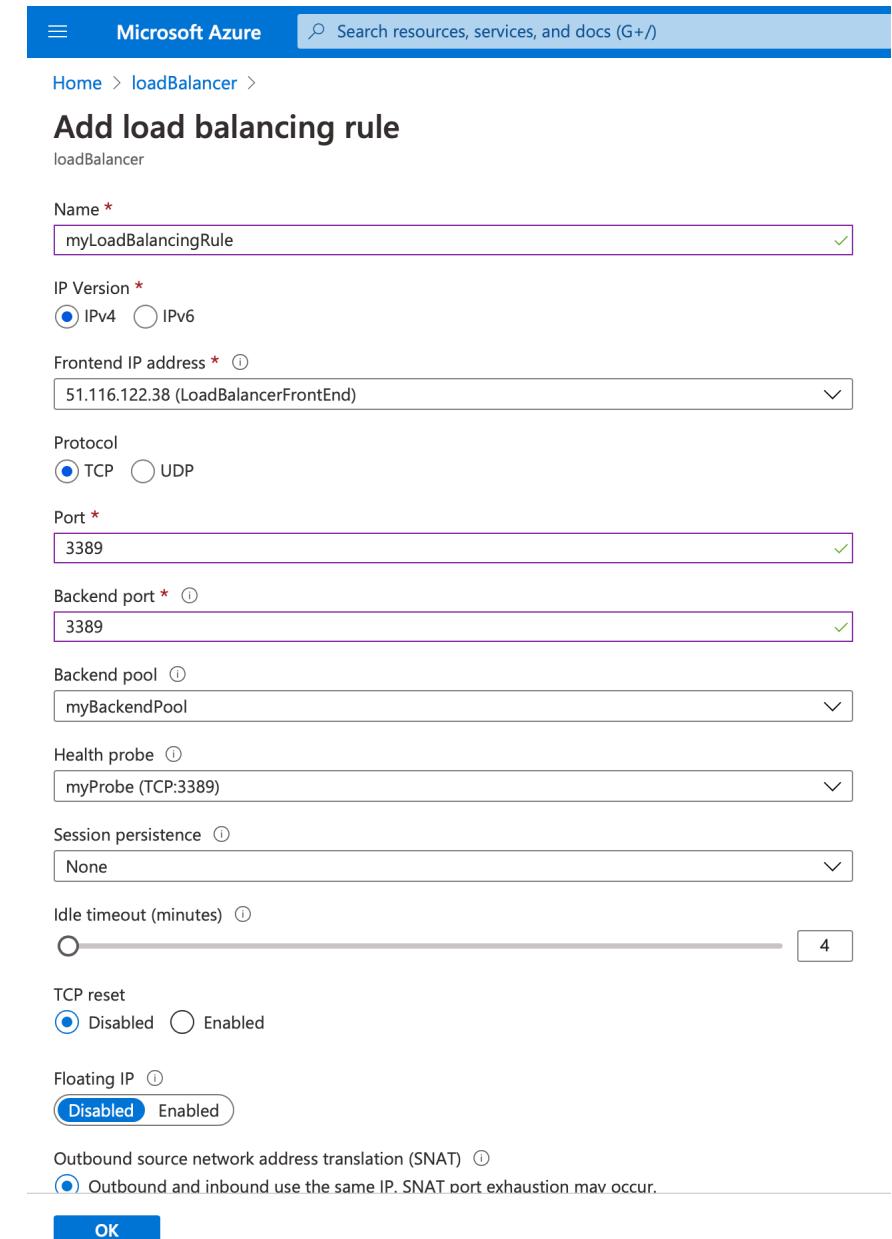
Sonda sanitária: **myHttpProbe**

- Outra regra chamada myRDPRule

Porta 3389 a escutar

Porta Backend: 80, na myBackendPool

Sonda sanitária: **myRDPProbe**



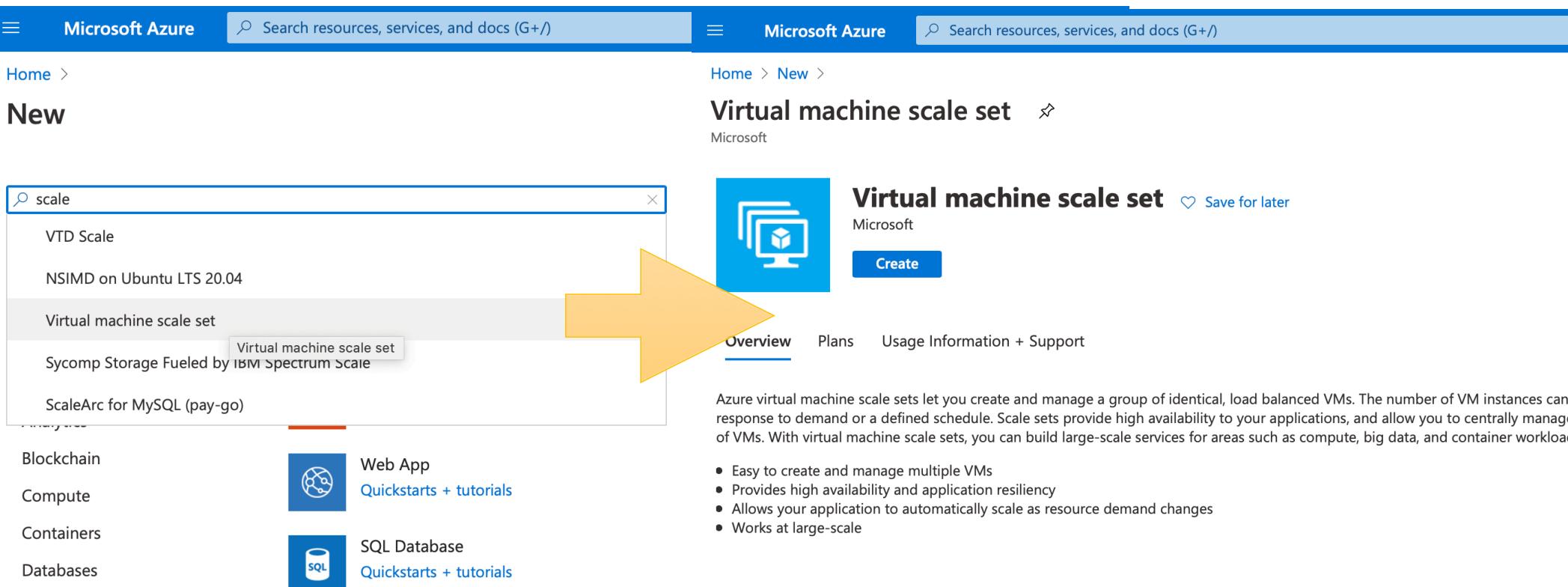
The screenshot shows the 'Add load balancing rule' configuration page in the Microsoft Azure portal. The form fields are as follows:

- Name ***: myLoadBalancingRule
- IP Version ***: IPv4 (selected)
- Frontend IP address ***: 51.116.122.38 (LoadBalancerFrontEnd)
- Protocol**: TCP (selected)
- Port ***: 3389
- Backend port ***: 3389
- Backend pool**: myBackendPool
- Health probe**: myProbe (TCP:3389)
- Session persistence**: None
- Idle timeout (minutes)**: 4
- TCP reset**: Disabled (selected)
- Floating IP**: Disabled (selected)
- Outbound source network address translation (SNAT)**: Outbound and inbound use the same IP. SNAT port exhaustion may occur.

At the bottom right is an 'OK' button.

Introdução aos Balanceadores de Carga

- 5. A partir do Azure marketplace, crie um conjunto de Máquinas Virtuais



The screenshot shows two side-by-side views of the Microsoft Azure Marketplace.

Left View (Search Results): A search bar at the top contains the text "scale". Below it, a list of items includes:

- VTD Scale
- NSIMD on Ubuntu LTS 20.04
- Virtual machine scale set** (highlighted with a red box)
- Sycomp Storage Fueled by IBM Spectrum Scale
- ScaleArc for MySQL (pay-go)

Right View (Product Detail Page): The page title is "Virtual machine scale set" by Microsoft. It features a "Create" button and tabs for "Overview", "Plans", and "Usage Information + Support". The "Overview" tab is selected. The page describes how Virtual machine scale sets let you create and manage a group of identical, load balanced VMs. It lists several benefits:

- Easy to create and manage multiple VMs
- Provides high availability and application resiliency
- Allows your application to automatically scale as resource demand changes
- Works at large-scale

Universidade da Beira Interior

Introdução aos Balanceadores de Carga

- 5.1 A partir do Azure marketplace, crie um conjunto de Máquinas Virtuais (formulário):
 - Nome: **myVMsScaleSet**
 - Indique a rede virtual para o conjunto de máquinas
 - Indique que precisa de usar um平衡ador de carga, e escolha o balanceador de carga já criado
 - Escolha a Backend Pool. Caso não exista uma backend pool pode criá-la agora (no nosso caso já foi criada)

Microsoft Azure Show portal menu Search resources, services, and docs (G+)

Dashboard > New > Virtual machine scale set >

Create a virtual machine scale set

Basics Disks Networking Scaling Management Health Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more about VMSS networking](#)

Virtual network configuration

Azure Virtual Network (VNet) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. [Learn more about VNets](#)

Virtual network * ⓘ myVirtualNetwork_LB

Create virtual network Manage selected virtual network

Network interface

A network interface enables an Azure virtual machine to communicate with internet, Azure, and on-premises resources. A VM can have one or more network interfaces.

+ Create new nic Delete

NAME	CREATE PUBLI...	SUBNET	NETWORK SECURIT...	ACCELERATED N...
myVirtualNetwork_LB...	No	mySubNet (172.16.1.0...)	Basic	Off

Load balancing

You can place this virtual machine scale set in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Use a load balancer Yes No

Review + create < Previous Next : Scaling >

Load balancing

You can place this virtual machine scale set in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Use a load balancer Yes No

Load balancing settings

- Application Gateway is an HTTP/HTTPS web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. [Learn more about Application Gateway](#)
- Azure Load Balancer supports all TCP/UDP network traffic, port-forwarding, and outbound flows. [Learn more about Azure Load Balancer](#)

Load balancing options * ⓘ Azure load balancer

Select a load balancer * ⓘ myLoadBalancer

Create new

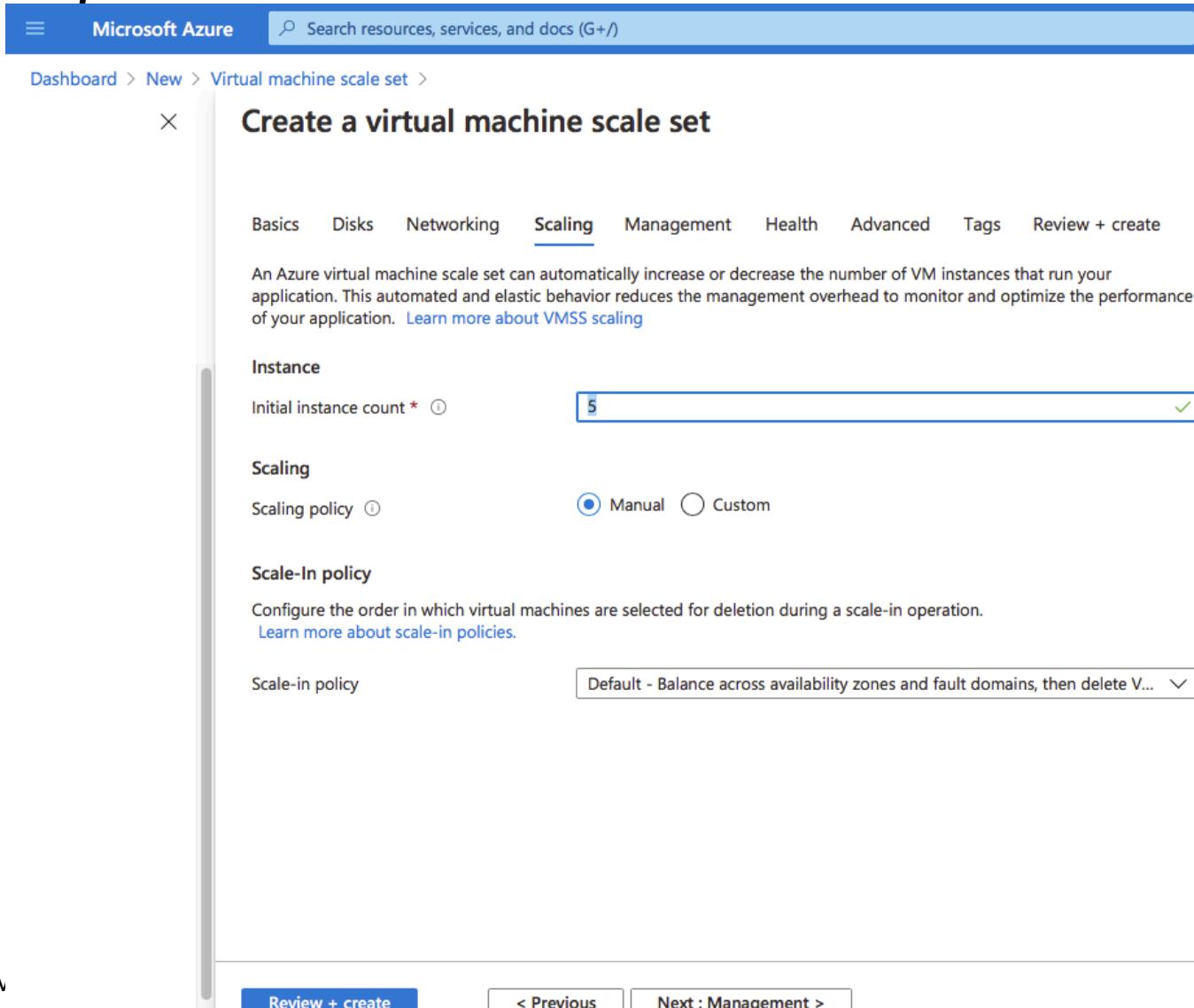
Select a backend pool * ⓘ myBackEndPool

Create new

Review + create < Previous Next : Scaling >

Introdução aos Balanceadores de Carga

- 5.1 (cont.) No tabulador Scaling defina que pretende um conjunto de 2 VMs.



The screenshot shows the 'Create a virtual machine scale set' wizard in the Microsoft Azure portal. The 'Scaling' tab is selected. The 'Initial instance count' field contains the value '5'. The 'Scaling policy' section shows 'Manual' selected. Under 'Scale-In policy', it says 'Default - Balance across availability zones and fault domains, then delete V...'. Navigation links at the bottom include 'Review + create', '< Previous', and 'Next : Management >'.

Microsoft Azure Search resources, services, and docs (G+)

Dashboard > New > Virtual machine scale set >

Create a virtual machine scale set

Scaling

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Instance

Initial instance count * ⓘ 5 ✓

Scaling

Scaling policy ⓘ Manual Custom

Scale-In policy

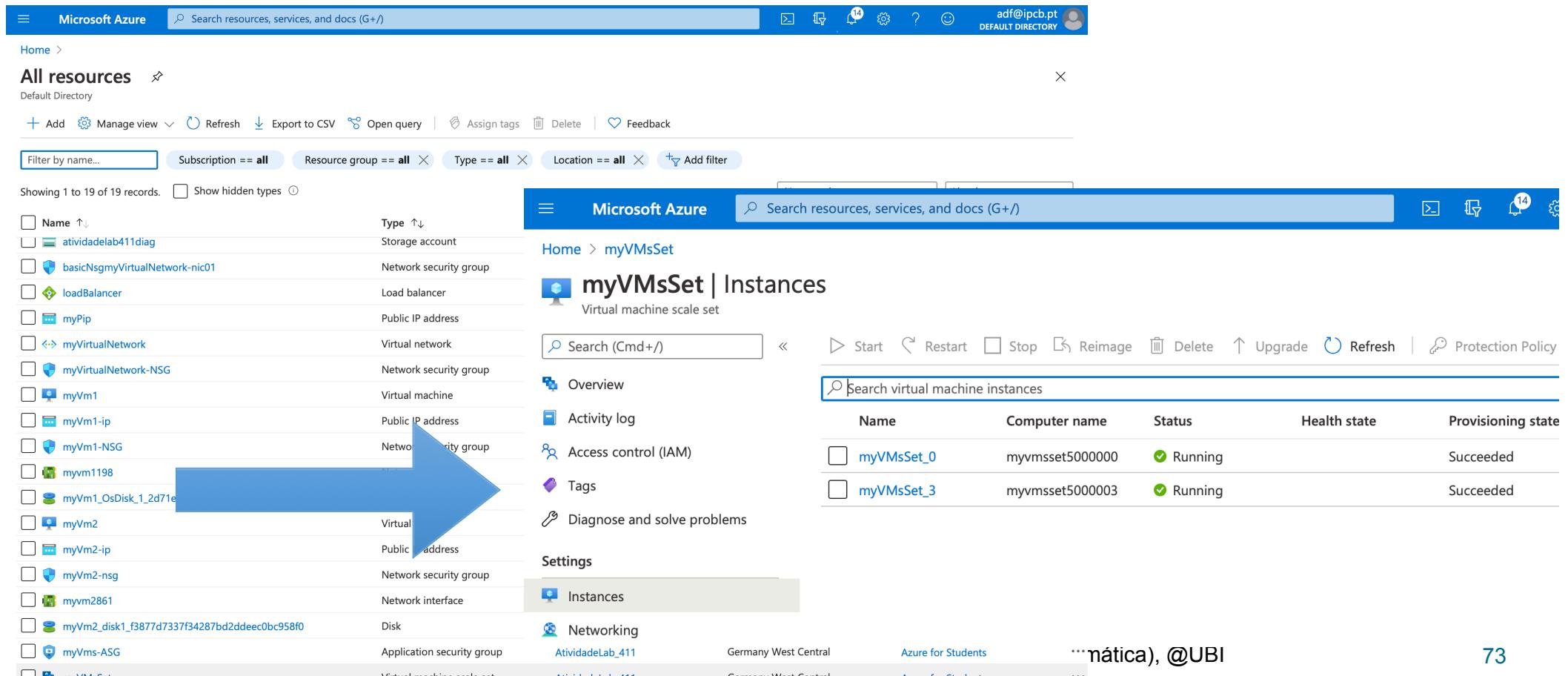
Configure the order in which virtual machines are selected for deletion during a scale-in operation. [Learn more about scale-in policies](#).

Scale-in policy Default - Balance across availability zones and fault domains, then delete V...

Review + create < Previous Next : Management >

Introdução aos Balanceadores de Carga

- 5.1 (cont.) A partir de home->All Resources aceda ao conjunto de VMs do backend pool do Balanceador de carga e verifique o “status” da VMs
- Como verá as VMs não dispõem de endereço IP público

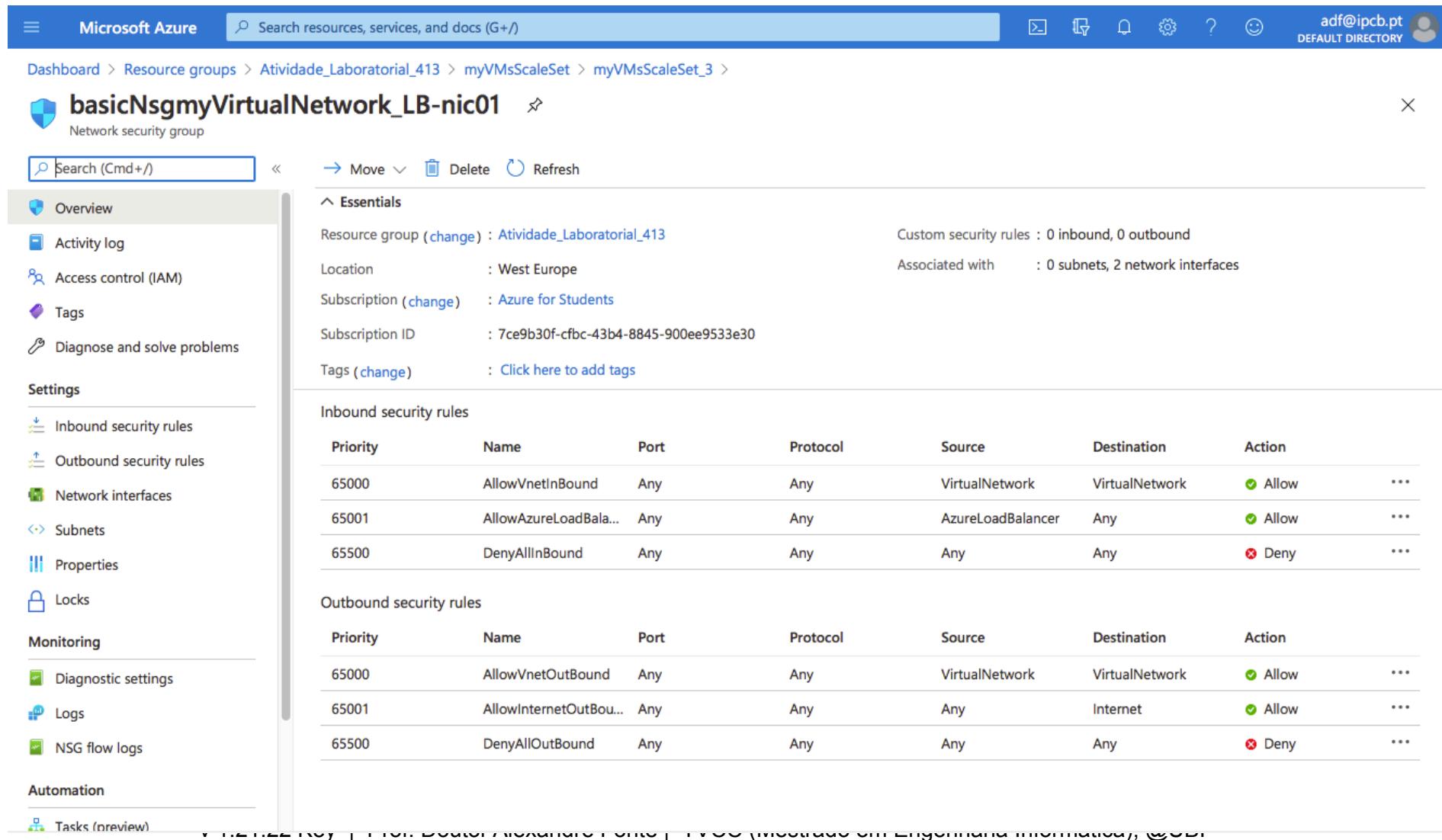


The image shows two screenshots of the Microsoft Azure portal. The left screenshot displays the 'All resources' view, listing various Azure resources such as storage accounts, network security groups, load balancers, public IP addresses, virtual networks, and virtual machines. A blue arrow points from the 'Virtual machine' section of the left sidebar to the 'Instances' section of the right sidebar. The right screenshot shows the detailed view for a 'Virtual machine scale set' named 'myVMsSet'. It lists three instances: 'myVMsSet_0' and 'myVMsSet_3' are running (Status: Running, Provisioning state: Succeeded), while 'myVMsSet_1' is not visible in the list. The 'Instances' section is highlighted with a blue box.

Name	Computer name	Status	Health state	Provisioning state
myVMsSet_0	myvmsset5000000	Running	Normal	Succeeded
myVMsSet_3	myvmsset5000003	Running	Normal	Succeeded

Introdução aos Balanceadores de Carga

- 5.1 (cont.) Podemos observar que é criado 1 NSG aplicado a duas interfaces de rede os quais estão aplicados a cada VM do Backend, contudo é preciso abrir as portas RDP e Web



The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The top navigation bar includes 'Microsoft Azure', a search bar, and user information ('adf@ipcb.pt DEFAULT DIRECTORY'). Below the header, the breadcrumb navigation shows: Dashboard > Resource groups > Atividade_Laboratorial_413 > myVMsScaleSet > myVMsScaleSet_3 > basicNsgmyVirtualNetwork_LB-nic01.

The main content area displays the 'basicNsgmyVirtualNetwork_LB-nic01' NSG details. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks), Monitoring (Diagnostic settings, Logs, NSG flow logs), and Automation (Tasks (review)).

The 'Essentials' section provides summary information: Resource group (Atividade_Laboratorial_413), Location (West Europe), Subscription (Azure for Students), Subscription ID (7ce9b30f-cfbc-43b4-8845-900ee9533e30), and Tags (Click here to add tags). It also shows Custom security rules: 0 inbound, 0 outbound, and Associated with: 0 subnets, 2 network interfaces.

The 'Inbound security rules' table lists three rules:

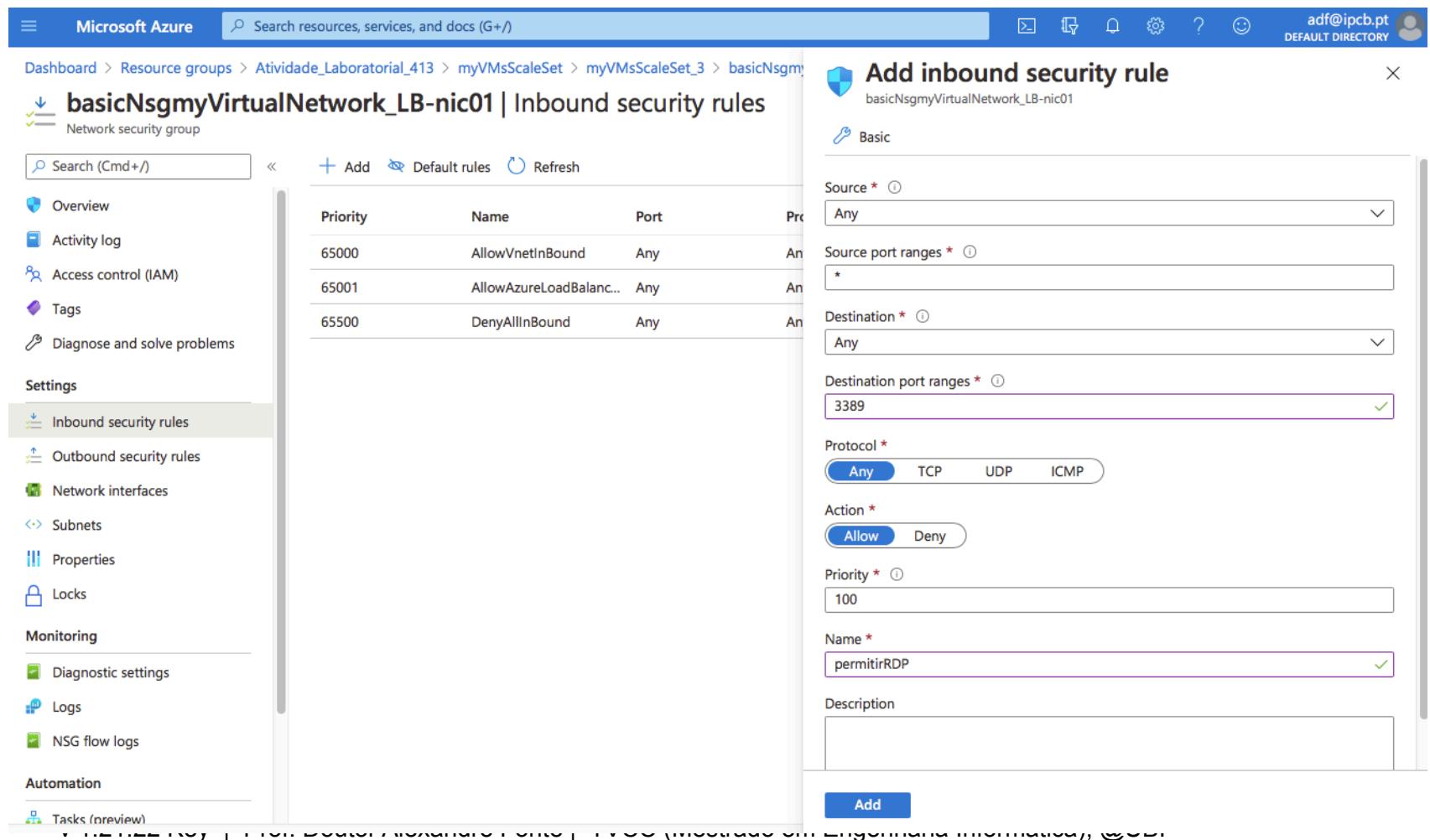
Priority	Name	Port	Protocol	Source	Destination	Action	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBal...	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

The 'Outbound security rules' table lists three rules:

Priority	Name	Port	Protocol	Source	Destination	Action	...
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	...

Introdução aos Balanceadores de Carga

- 5.2 (cont.) Adicionar duas regras de segurança para permitir o tráfego de entrada RDP e Web
 - permitirRDP, porta 3389
 - permitirHTTP, porta 80



The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). On the left, a sidebar menu is visible with options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, Inbound security rules is selected. The main pane displays the 'basicNsgmyVirtualNetwork_LB-nic01 | Inbound security rules' page, showing a table of existing rules:

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

To the right, a modal window titled 'Add inbound security rule' is open, allowing the creation of a new rule. The configuration fields are as follows:

- Source: Any
- Source port ranges: *
- Destination: Any
- Destination port ranges: 3389
- Protocol: Any (selected)
- Action: Allow
- Priority: 100
- Name: permitirRDP
- Description: (empty)

At the bottom of the modal is a blue 'Add' button.

Introdução aos Balanceadores de Carga

- 5.3 (cont.) Finalmente:
 - Ligar-se às VMs por RDP
 - Instalar o servidor Web IIS.
 - Aceder ao servidor Web usando um browser

Instalação do IIS via Powershell
Windows Administrative Tools > Windows PowerShell.

```
# Install IIS server role
```

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

```
# Remove default htm file
```

```
Remove-Item C:\inetpub\wwwroot\iisstart.htm
```

```
# Add a new htm file that displays server name
```

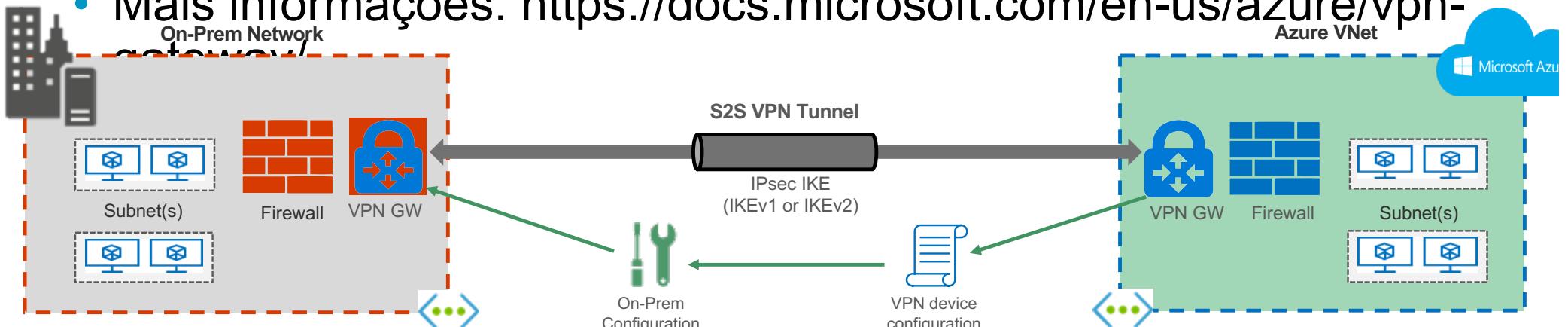
```
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $($("Hello World from " +  
$env:computername))
```

Sumário

- Redes Virtuais
 - Ligações VNET-TO-VNET com VPN Gateways
 - Ligações Site-to-Site
 - Ligações Point-to-Site (Opcional)

Azure VPN Gateway

- Gateway VPN é um gateway de rede virtual seguro que envia tráfego cifrado através da rede da Microsoft permitindo:
 - Ligação VNet-to-VNet
 - Ligação On-premises to Azure
- Um Gateway VPN no máximo por VNet
 - Suporta múltiplas ligações
 - Todos os túneis VPN partilham a largura de banda atribuída ao gateway
- Mais informações: <https://docs.microsoft.com/en-us/azure/vpn-gateway/>



Azure VPN Gateway (Cont.)

- Um gateway virtual é composto por duas ou mais VMs, criadas aquando da criação do gateway virtual, implantadas numa rede específica, chamada de **gateway subnet**
 - /27 (até 27 dispositivos) ou /28 (até 11 dispositivos)
- As Virtual Network Gateway VMs contêm tabelas de encaminhamento e executam os serviços específicos de gateway.
- Não é possível configurar as VMs à parte do gateway
- Aquando da configuração do gateway escolhe-se o tipo de gateway a criar:
 - Gateway do tipo “vpn” é um VPN Gateway
 - Gateway do tipo “ExpressRoute”
- Uma rede pode ter no máximo um VPN Gateway e no máximo um ExpressRoute, no caso de coexistirem estas configurações

Azure VPN Gateway (Cont.)

- A configuração de um vpn gateway pode levar até 45 minutos
- Após isso pode-se criar um túnel IP Sec IKEv2:
 - **VNET-TO-VNET**: Pode ser um túnel IPsec/IKE entre dois VPN gateways
 - **SITE-TO-SITE**: Ou um túnel IPsec/IKE entre um VPN gateway e um dispositivo VPN on-premise
 - **Point-to-site VPN**: Ou uma ligação Point-to-site VPN sobre OpenVPN, IKEv2 ou SSTP (Secure Socket Tunneling Protocol), entre uma localização remota e a rede virtual Azure

Azure VPN Gateway (Cont.)

- Tipos de VPN Gateways:
- <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwtype>

SKUs

Basic

Vpngw1

Vpngw2

Vpngpw3

Azure VPN Gateway (Cont.)

- Preços VPN Gateways

<https://azure.microsoft.com/en-us/pricing/details/vpn-gateway/>

VPN Gateways

Setting up a virtual network is free of charge. However, we do charge for the VPN gateway that connects to on-premises and other virtual networks in Azure. This charge is based on the amount of time that gateway is provisioned and available.

VPN Gateway Type	Price	Bandwidth	S2S Tunnels	P2S Tunnels
Basic	€0.04/hour	100 Mbps	Max 10 1-10: Included	Max 128 1-128: Included
VpnGw1	€0.1603/hour	650 Mbps	Max 30 1-10: Included 11-30: €0.013/hour per tunnel	Max 250 1-128: Included 129-250: €0.009/hour per connection
VpnGw2	€0.4133/hour	1 Gbps	Max 30 1-10: Included 11-30: €0.013/hour per tunnel	Max 500 1-128: Included 129-500: €0.009/hour per connection
VpnGw3	€1.0542/hour	1.25 Gbps	Max 30 1-10: Included 11-30: €0.013/hour per tunnel	Max 1000 1-128: Included 129-1000: €0.009/hour per connection
VpnGw4	€1.7710/hour	5 Gbps	Max 30 1-10: Included 11-30: €0.013/hour per tunnel	Max 5000 1-128: Included 129-5000: €0.009/hour per connection
VpnGw5	€3.0781/hour	10 Gbps	Max 30 1-10: Included 11-30: €0.013/hour per tunnel	Max 10000 1-128: Included 129-10000: €0.009/hour per connection

Monthly price estimates are based on 730 hours of usage per month.

Azure VPN Gateway (Cont.)

- Terminologia

- Azure VPN gateway:** É o serviço de gateway VPN que permite a ligação de uma VNet à rede local por meio de um dispositivo VPN (VPN appliance).
- Virtual network gateway:** É um recurso que fornece um dispositivo VPN virtual (VPN appliance) para a VNet. É responsável por encaminhar o tráfego da rede on-premises para a VNet.
- Local network gateway:** É uma abstração de um dispositivo VPN on-premises. O tráfego de rede a partir da nuvem para a rede local é encaminhamento por meio deste gateway.
- Connection:** Uma ligação tem propriedades que especificam o tipo de ligação (IPSec) e a chave partilhada com o dispositivo VPN on-premises para criptografar o tráfego.
- Gateway subnet:** Rede virtual do gateway.

Azure VPN Gateway (Cont.)

- Terminologia (continuação)

-Componentes outside VNet

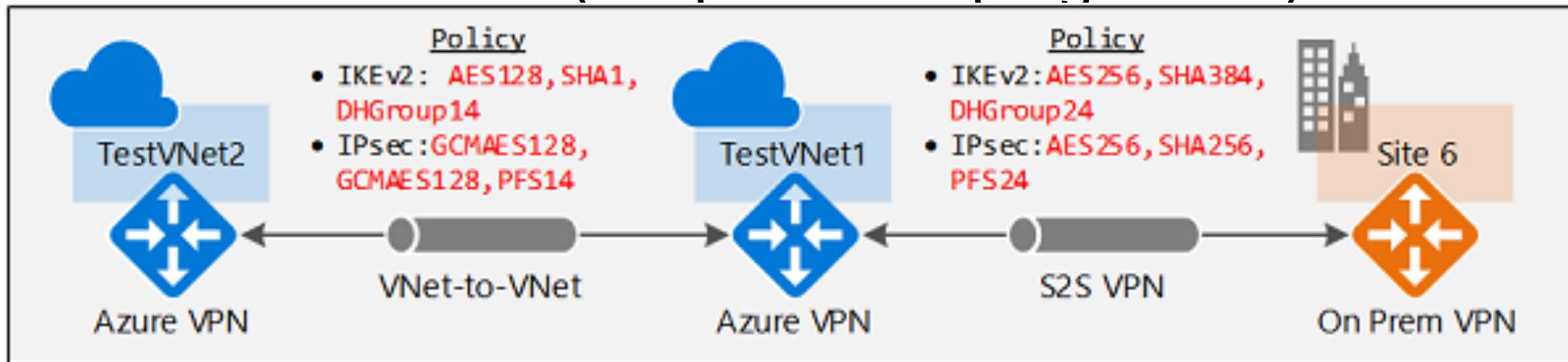
- **On-premises network.** Rede local privada dentro de uma organização
- **VPN appliance.** Dispositivo ou serviço que fornece ligação externa à rede On-premises.
- Uma VPN appliance pode ser um dispositivo de hardware (e.g. router cisco ISR o Firewall Cisco ASA), ou pode ser uma solução de software como o serviço ***Routing and Remote Access Service (RRAS)*** do Windows.

Azure VPN Gateway (Cont.)

- Dispositivos validados (VPN Appliances)
 - <https://docs.microsoft.com/pt-pt/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

Azure VPN Gateway (Cont.)

- Túneis IPsec/IKE (Requisitos criptográficos)

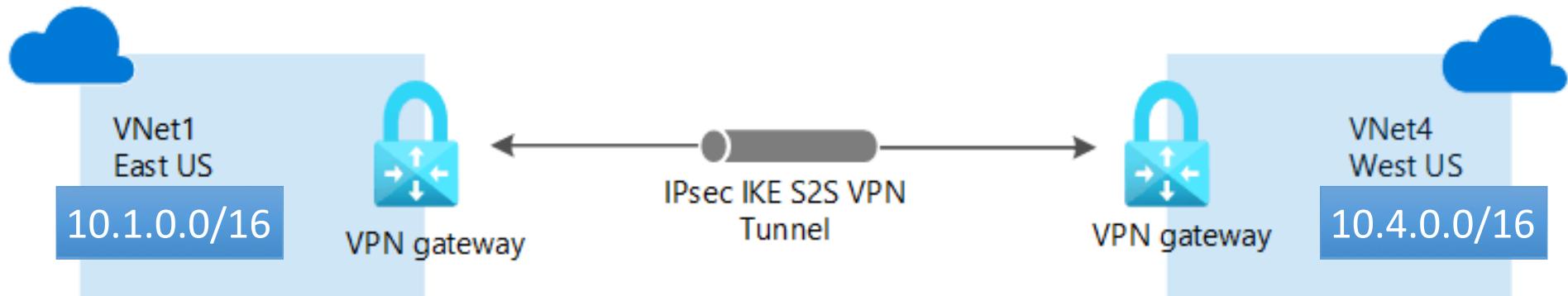


Opções de Configuração disponíveis para as políticas IPsec/IKE a aplicar à ligação VNET-to-NET ou S2S a criar.	
<u>IPsec/IKEv2*</u>	Options
IKEv2 Encryption	AES256, AES192, AES128, DES3, DES
IKEv2 Integrity	SHA384, SHA256, SHA1, MD5
DH Group	DHGroup24, ECP384, ECP256, DHGroup14 (DHGroup2048), DHGroup2, DHGroup1, None
IPsec Encryption	GCMAES256, GCMAES192, GCMAES128, AES256, AES192, AES128, DES3, DES, None
IPsec Integrity	GCMAES256, GCMAES192, GCMAES128, SHA256, SHA1, MD5
PFS Group	PFS24, ECP384, ECP256, PFS2048, PFS2, PFS1, None
QM SA Lifetime	Seconds (integer; min. 300 /default 27000 seconds) KBytes (integer; min. 1024 /default 102400000 KBytes)
Traffic Selector	UsePolicyBasedTrafficSelectors (\$True/\$False; default \$False)

Azure VPN Gateway (Cont.)

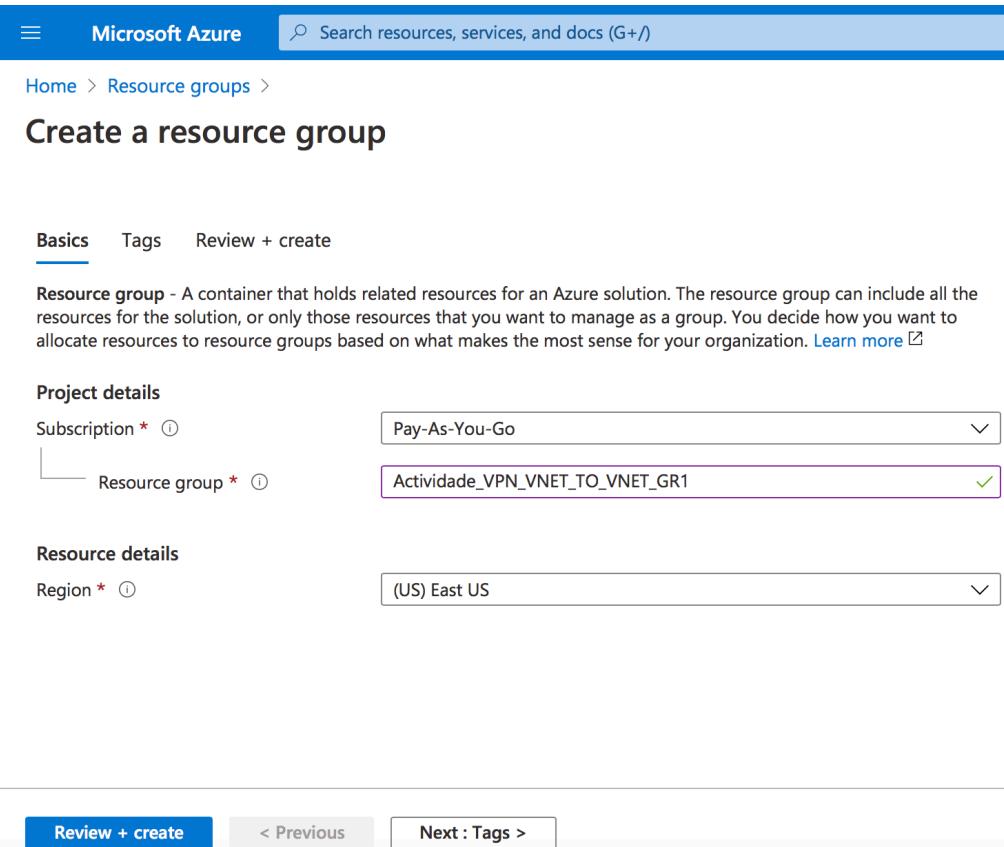


**Configurar uma ligação VNET-to-VNET
usando VPN Gateways**

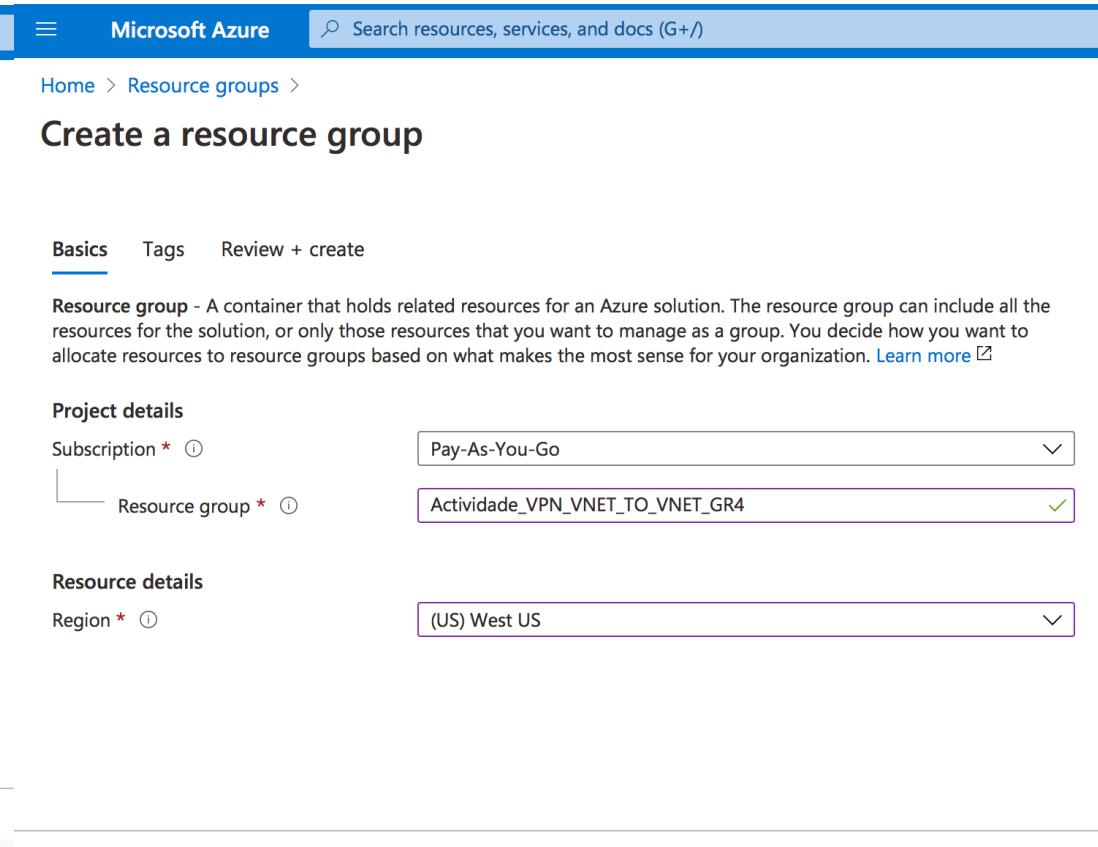


Azure VPN Gateway (Cont.)

- 1. Crie dois grupos de recursos
 - **Actividade_VPN_VNET_TO_VNET_GR1**, região East US



The screenshot shows the 'Create a resource group' page for 'Actividade_VPN_VNET_TO_VNET_GR1'. It includes fields for Project details (Subscription: Pay-As-You-Go, Resource group: Actividade_VPN_VNET_TO_VNET_GR1), Resource details (Region: (US) East US), and navigation buttons (Review + create, < Previous, Next : Tags >).



The screenshot shows the 'Create a resource group' page for 'Actividade_VPN_VNET_TO_VNET_GR4'. It includes fields for Project details (Subscription: Pay-As-You-Go, Resource group: Actividade_VPN_VNET_TO_VNET_GR4), Resource details (Region: (US) West US), and navigation buttons (Review + create, < Previous, Next : Tags >).

Azure VPN Gateway (Cont.)

- 2. Crie e configure em cada região uma VNET
 - VNET1 (10.1.0.0/16)
 - Subrede: FrontEnd (10.1.0.0/24)
 - VNET4 (10.4.0.0/16)



Microsoft Azure Search resources, services, and docs (G+/)

Home > New > Virtual Network >

Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables your Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, or premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual networks](#)

Project details

Subscription * [\(i\)](#)

Pay-As-You-Go

Resource group * [\(i\)](#)

Actividade_VPN_VNET_TO_VNET_GR1

[Create new](#)

Instance details

Name * [\(i\)](#)

VNET1

Region * [\(i\)](#)

(US) East US



Microsoft Azure Search resources, services, and docs (G+/)

Home > New > Virtual Network >

Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.1.0.0/16 10.1.0.0 - 10.1.255.255 (65536 addresses)

Add IPv6 address space [\(i\)](#)

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+ Add subnet](#) Remove subnet

Subnet name

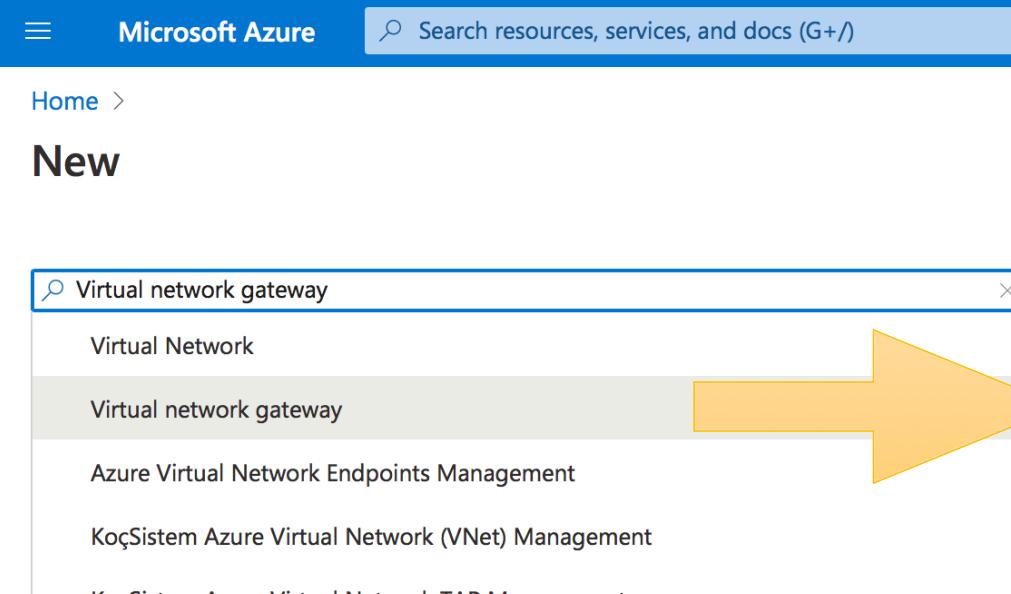
Subnet address range

FrontEnd

10.1.0.0/24

Azure VPN Gateway (Cont.)

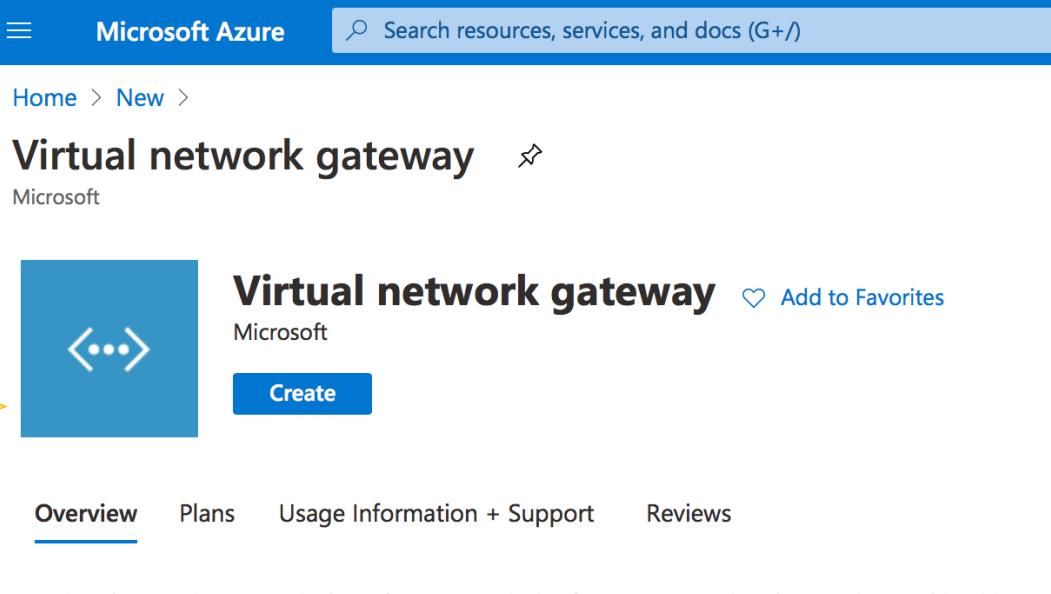
- 3. Crie o Gateway VPN da VNET1



A yellow arrow points from the search result to the 'Create' button on the right.

Virtual Network
Virtual network gateway
Azure Virtual Network Endpoints Management
KoçSistem Azure Virtual Network (VNet) Management
KoçSistem Azure Virtual Network TAP Management

Blockchain
Compute
Containers
Databases
Developer Tools
DevOps
Identity
Integration
Internet of Things



Virtual network gateway Microsoft

Create

[Overview](#) [Plans](#) [Usage Information + Support](#) [Reviews](#)

A virtual network gateway is the software VPN device for your Azure virtual network. Use this with a co... virtual network and your local network, or a VNet-to-VNet VPN connection between two Azure virtual ... ExpressRoute circuit.

Microsoft Azure provides a [99.9% uptime SLA](#) for virtual network gateways.

More offers from Microsoft

 Web App Quickstarts + tutorials
 SQL Database Quickstarts + tutorials
 Function App Quickstarts + tutorials
 Azure Cosmos DB Quickstarts + tutorials
 Workspace Microsoft
 Wire Data 2.0 Microsoft
 Microsoft HPC Pack 2 Microsoft
 Virtual Machine Azure Service

Azure VPN Gateway (Cont.)

- Crie o Gateway VPN da VNET1, considerando as seguintes configurações:



The screenshot shows the 'Create virtual network gateway' wizard in the Microsoft Azure portal. The 'Review + create' step is selected. A validation message 'Validation passed' is displayed. The configuration details are summarized in the following table.

Nome:	VNet1GW
Região:	East US
Geração:	Generation 1
Tipo de Gateway:	VPN.
Tipo de VPN:	Route*based.
SKU:	VpnGw1
Rede Virtual:	VNET1
Subrede:	GatewaySubnet (10.1.255.0/27)
Endereço IP Público IP:	VNet1GWpip

Basics

Subscription	Pay-As-You-Go
Resource group	Actividade_VPN_VNET_TO_VNET_GR1
Name	VNet1GW
Region	East US
SKU	VpnGw1
Generation	Generation1
Virtual network	VNET1
Subnet	GatewaySubnet (10.1.255.0/27)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	VNet1GWpip

Tags

None

Azure VPN Gateway (Cont.)

- 4. Crie o Gateway VPN da VNET4, considerando as seguintes configurações:



The screenshot shows the 'Create virtual network gateway' wizard in the Microsoft Azure portal. The 'Review + create' step is selected. A validation message 'Validation passed' is displayed. The configuration details are as follows:

Nome:	VNet4GW
Região:	West US
Geração:	Generation 1
Tipo de Gateway:	VPN.
Tipo de VPN:	Route*based.
SKU:	VpnGw1
Rede Virtual:	VNET4
Subrede:	GatewaySubnet (10.4.255.0/27)
Endereço IP Público IP:	VNet4GWpip

Basics

Subscription	Pay-As-You-Go
Resource group	Actividade_VPN_VNET_TO_VNET_GR4
Name	VNet4GW
Region	West US
SKU	VpnGw1
Generation	Generation1
Virtual network	VNET4
Subnet	GatewaySubnet (10.4.255.0/27)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	VNet4GWpip

Tags

Create **Previous** **Next** Download a template for automation

Azure VPN Gateway (Cont.)

- 5. Enquanto espera pela Implantação dos Gateways

-Crie duas VMs Windows

- myVM1 (VNET1)

Tamanho Standard B1

SSD Standard

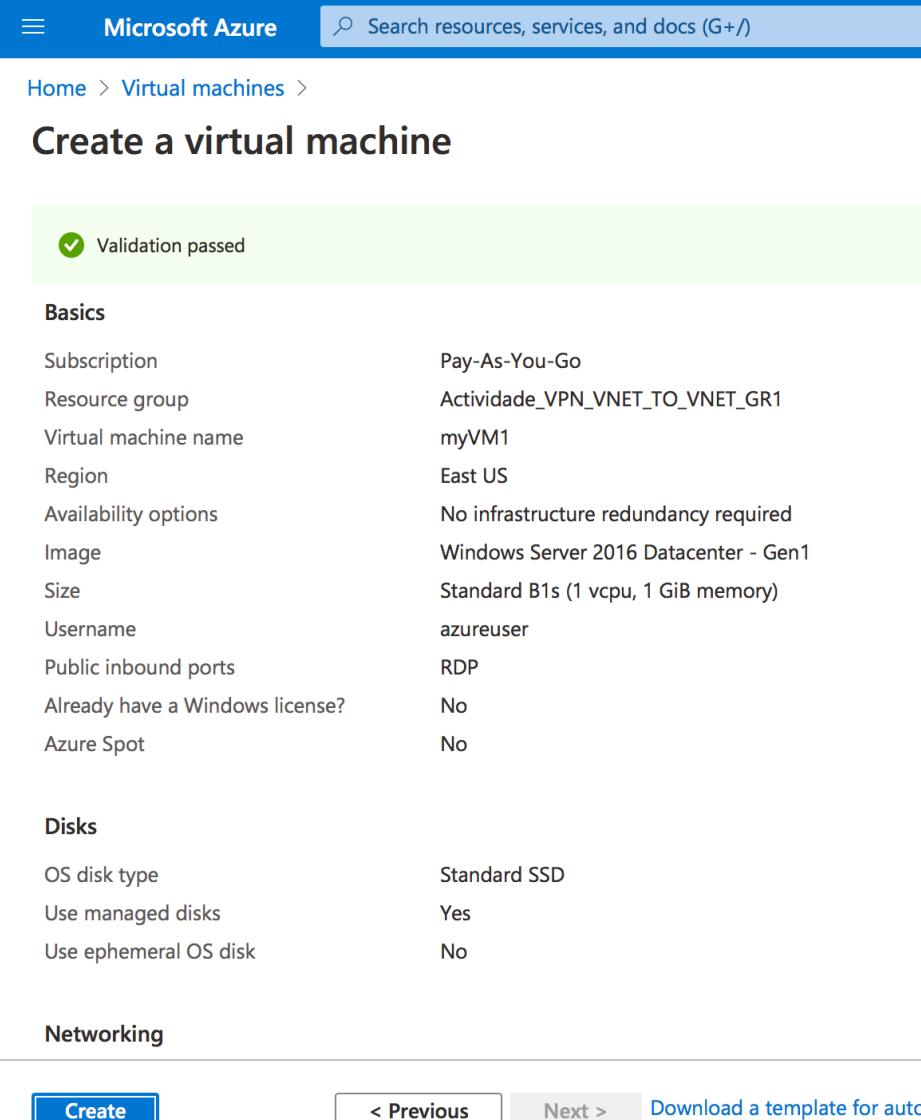
- myVM4 (VNET4)

Tamanho Standard B1

SSD Standard

Azure VPN Gateway (Cont.)

- 5.1. Configurações: myVM1 (VNET1)



Basics

Subscription	Pay-As-You-Go
Resource group	Actividade_VPN_VNET_TO_VNET_GR1
Virtual machine name	myVM1
Region	East US
Availability options	No infrastructure redundancy required
Image	Windows Server 2016 Datacenter - Gen1
Size	Standard B1s (1 vcpu, 1 GiB memory)
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Standard SSD
Use managed disks	Yes
Use ephemeral OS disk	No

Networking

Virtual network	VNET1
Subnet	FrontEnd (10.1.0.0/24)
Public IP	(new) myVM1-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

Management

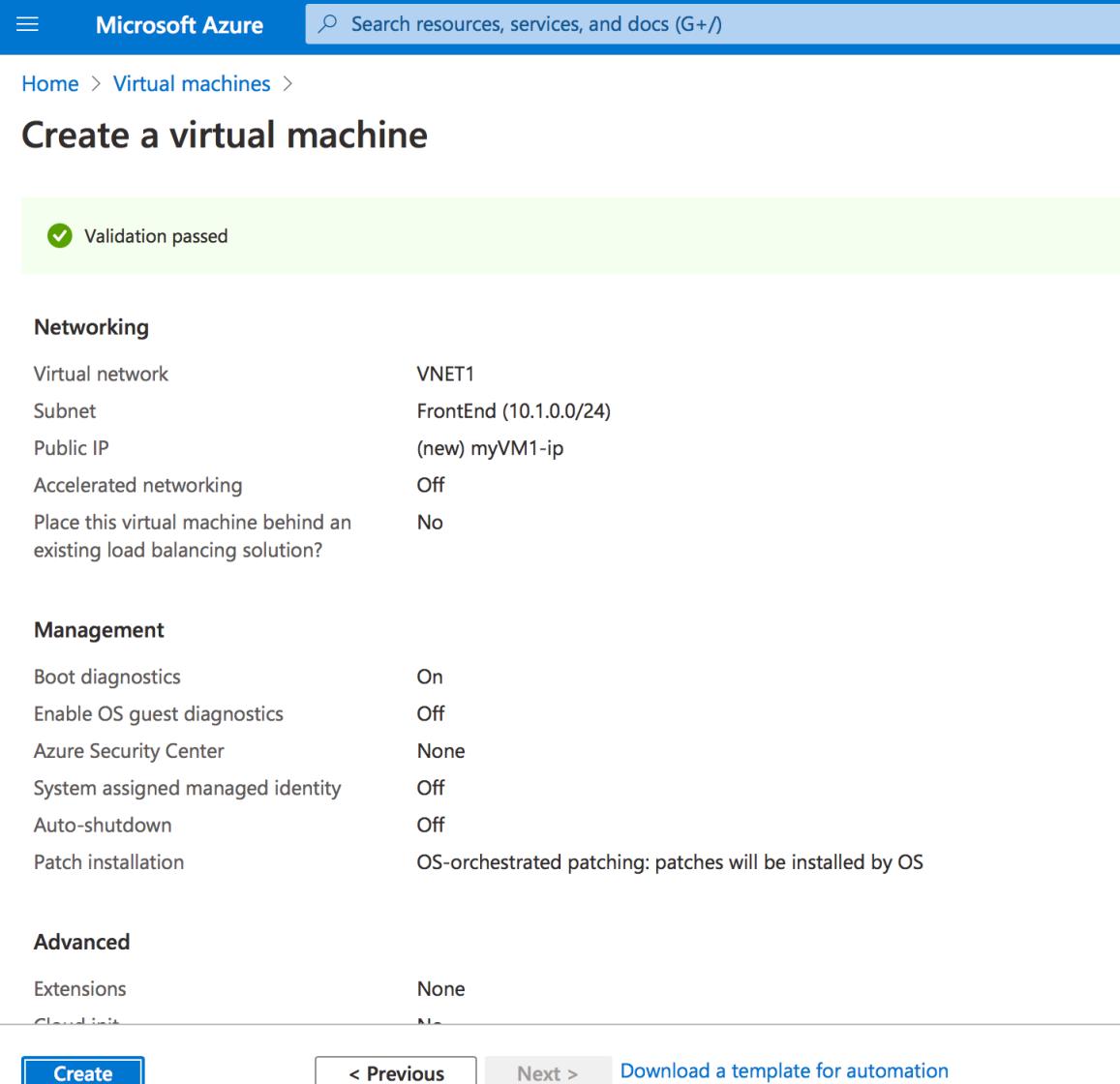
Boot diagnostics	On
Enable OS guest diagnostics	Off
Azure Security Center	None
System assigned managed identity	Off
Auto-shutdown	Off
Patch installation	OS-orchestrated patching: patches will be installed by OS

Advanced

Extensions	None
------------	------

Actions

[Create](#) | [< Previous](#) | [Next >](#) | [Download a template for automation](#)



Networking

Virtual network	VNET1
Subnet	FrontEnd (10.1.0.0/24)
Public IP	(new) myVM1-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

Management

Boot diagnostics	On
Enable OS guest diagnostics	Off
Azure Security Center	None
System assigned managed identity	Off
Auto-shutdown	Off
Patch installation	OS-orchestrated patching: patches will be installed by OS

Advanced

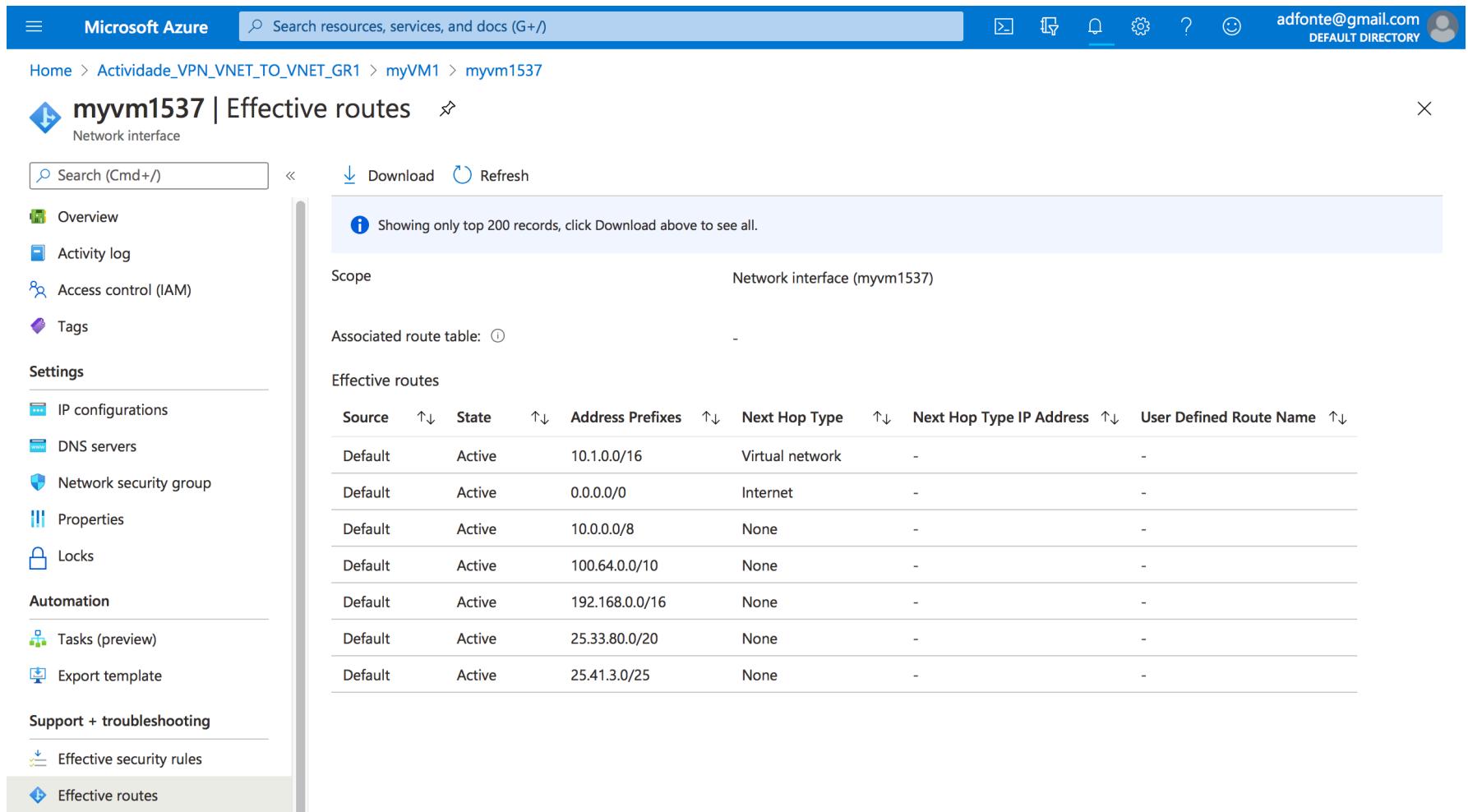
Extensions	None
------------	------

Actions

[Create](#) | [< Previous](#) | [Next >](#) | [Download a template for automation](#)

Azure VPN Gateway (Cont.)

- 5.2. Consulte a tabela de Encaminhamento da myVM1 da VNET1
 - Acha que é possível atingir a VNET4?



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (adfente@gmail.com, DEFAULT DIRECTORY). Below the navigation bar, the URL path is displayed: Home > Actividade_VPN_VNET_TO_VNET_GR1 > myVM1 > myvm1537. The main content area is titled "myvm1537 | Effective routes" and shows the "Network interface" details. On the left, there is a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Settings (IP configurations, DNS servers, Network security group, Properties, Locks), Automation (Tasks (preview), Export template), and Support + troubleshooting (Effective security rules, Effective routes). The "Effective routes" link is currently selected and highlighted in grey. The main content area displays the "Effective routes" table with the following data:

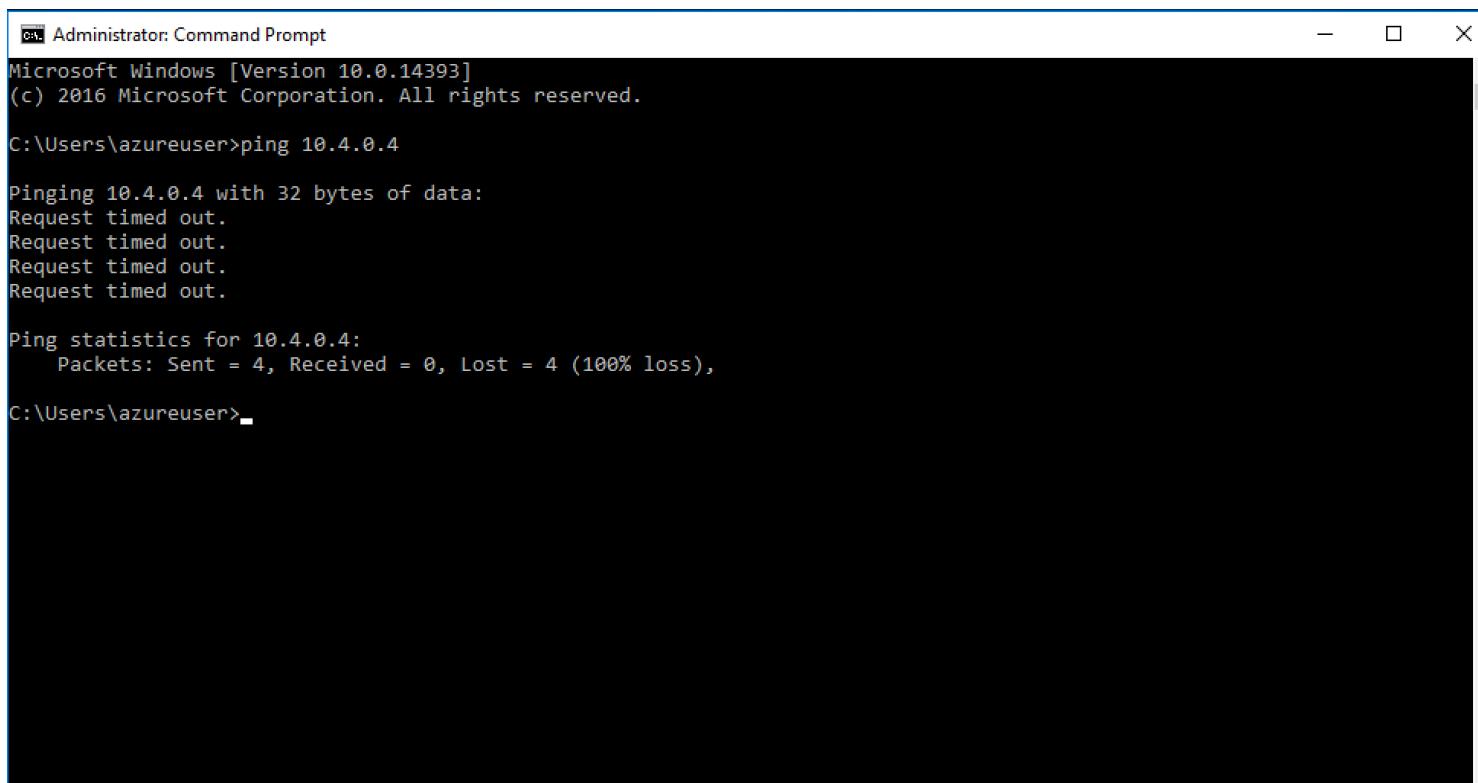
Source	State	Address Prefixes	Next Hop Type	User Defined Route Name
Default	Active	10.1.0.0/16	Virtual network	-
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	192.168.0.0/16	None	-
Default	Active	25.33.80.0/20	None	-
Default	Active	25.41.3.0/25	None	-

Azure VPN Gateway (Cont.)

- 5.3. Ligue-se à myVM4 e coloque a uma regra na firewall que permita se pingada

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

- De seguida, ligue-se à myVM1 e pingue a myVM4
 - Consegue indicar porque ainda não é possível?



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the following output:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

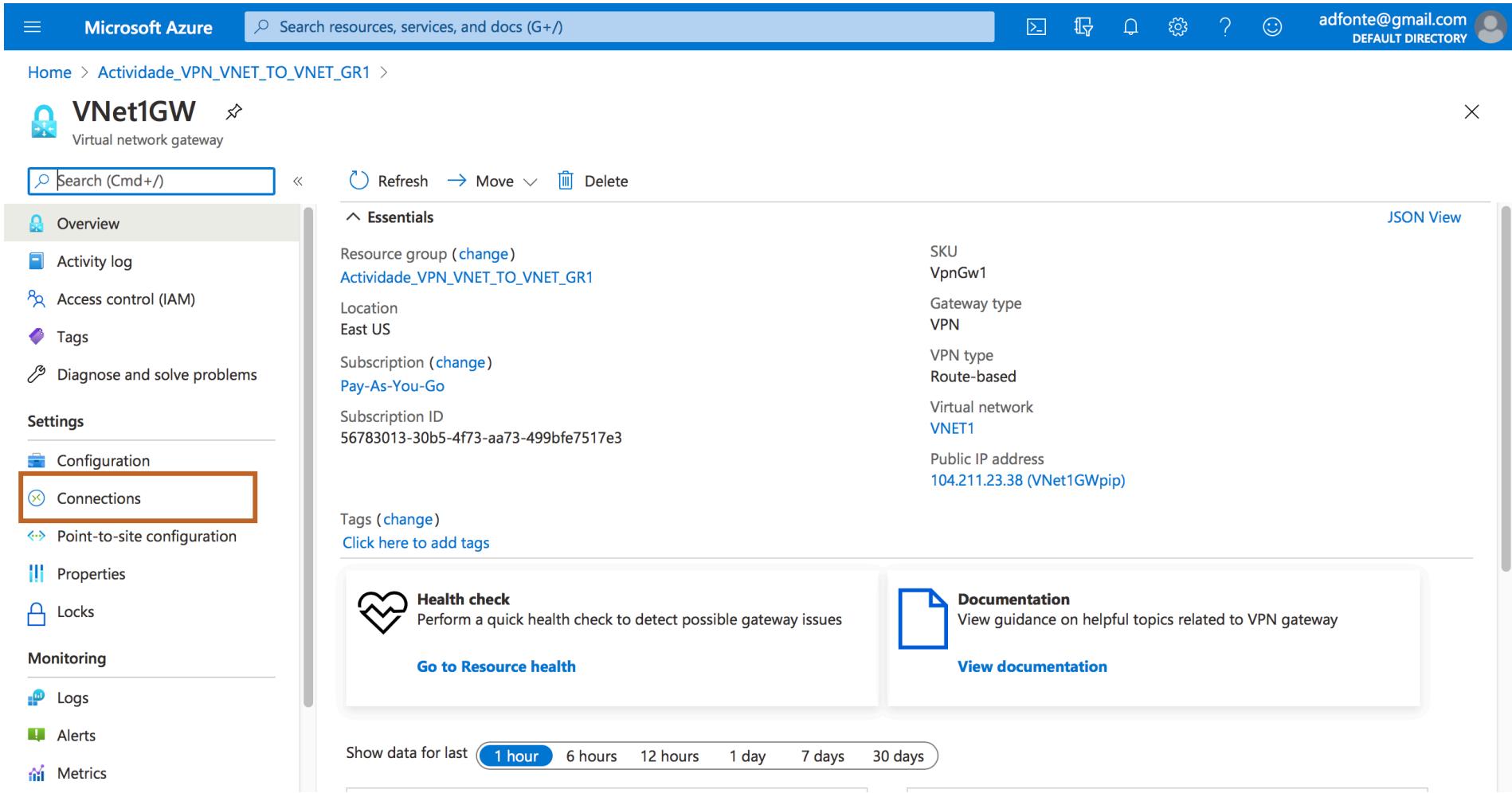
C:\Users\azureuser>ping 10.4.0.4

Pinging 10.4.0.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.4.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\azureuser>
```

Azure VPN Gateway (Cont.)

- 6.1. Aceda ao VNET1GW e configure a ligação à VNET4



The screenshot shows the Microsoft Azure portal interface for managing a Virtual Network Gateway (VNet1GW). The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (adfente@gmail.com, DEFAULT DIRECTORY). The main title is "VNet1GW" under the "Virtual network gateway" category. The left sidebar menu lists several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Connections (which is highlighted with a red box), Point-to-site configuration, Properties, Locks, Monitoring, Logs, Alerts, and Metrics. The "Connections" section is expanded, showing a "Tags (change)" section with a link to "Click here to add tags". The "Essentials" section displays resource details: Resource group (Actividade_VPN_VNET_TO_VNET_GR1), Location (East US), Subscription (Pay-As-You-Go), Subscription ID (56783013-30b5-4f73-aa73-499bfe7517e3), SKU (VpnGw1), Gateway type (VPN), VPN type (Route-based), Virtual network (VNET1), and Public IP address (104.211.23.38 (VNet1GWpip)). Below these details are two callout boxes: "Health check" (with a heart icon) and "Documentation" (with a document icon). The "Health check" box contains the text "Perform a quick health check to detect possible gateway issues" and a "Go to Resource health" button. The "Documentation" box contains the text "View guidance on helpful topics related to VPN gateway" and a "View documentation" button. At the bottom, there is a "Show data for last" dropdown menu with options: 1 hour, 6 hours, 12 hours, 1 day, 7 days, and 30 days.

Azure VPN Gateway (Cont.)

- 6.1. Aceda ao VNET1GW e configure a ligação à VNET4 (Cont.)
 - Defina como Pre-Shared Key: c3iaas, e use o protocolo IKEv2. Na ligação reversa deve definir a mesma chave.

Add connection

VNet1GW

Name *

VNET1-VNET4

Connection type ⓘ

VNet-to-VNet

*First virtual network gateway ⓘ

VNet1GW

*Second virtual network gateway ⓘ

Choose another virtual network gateway...

Shared key (PSK) *

c3iaas

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ

IKEv1 IKEv2

Subscription ⓘ

Microsoft Azure Search resources, services, and docs (G+/)

Home > Actividade_VPN_VNET_TO_VNET_GR1 > VNet1GW >

Add connection

Microsoft Azure Search resources, services, and docs (G+/)

Home > Actividade_VPN_VNET_TO_VNET_GR1 > VNet1GW > Add connection >

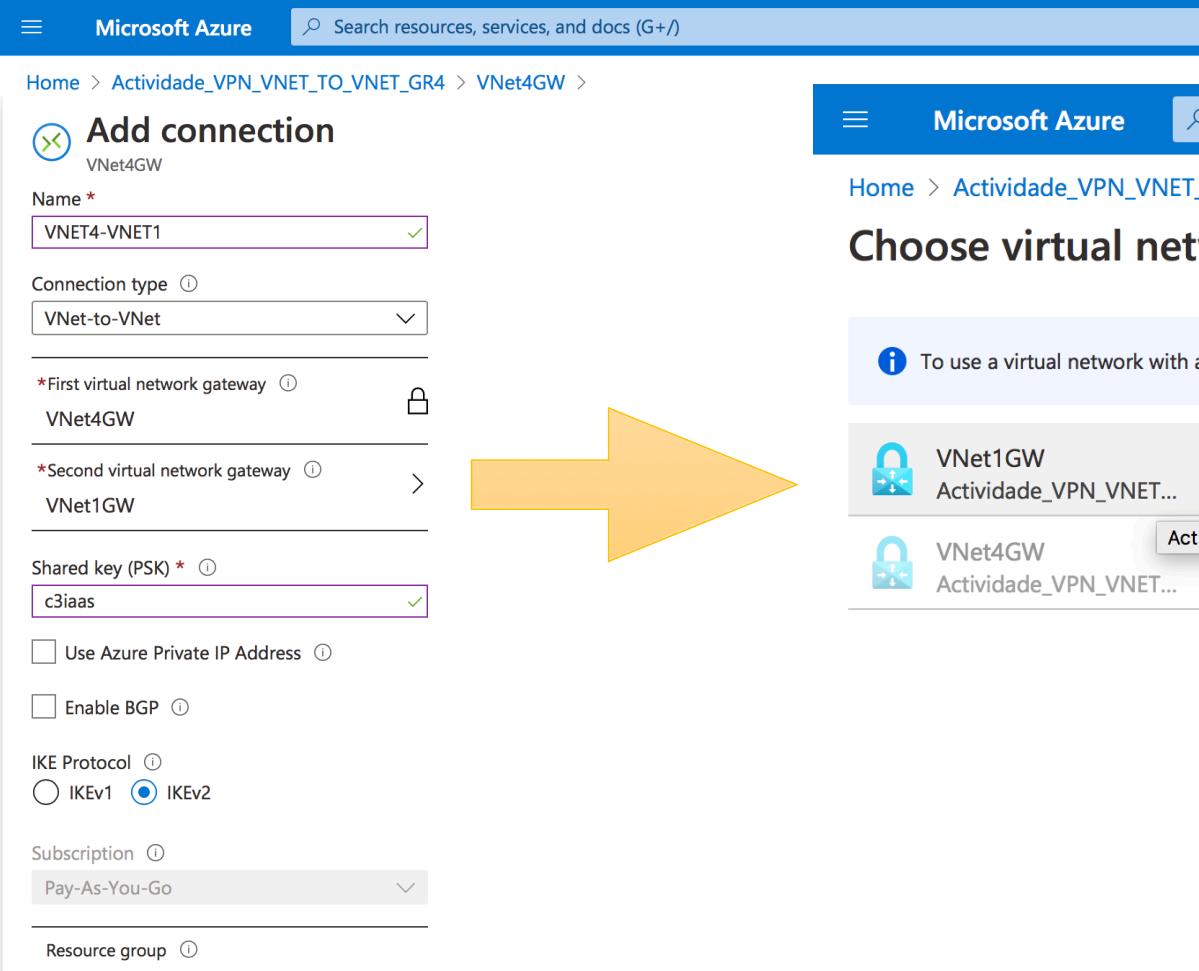
Choose virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway. [Learn more](#)

Virtual Network Gateway	Description
VNet4GW	Actividade_VPN_VNET...
VNet1GW	Actividade_VPN_VNET...

Azure VPN Gateway (Cont.)

- 6.2. Aceda ao VNET4GW e configure a ligação reversa à VNET1
 - Defina como Pre-Shared Key: c3iaas, e use o protocolo IKE2. Na ligação reversa deve definir a mesma chave.



Add connection

VNet4GW

Name *

Connection type ⓘ

*First virtual network gateway ⓘ

Second virtual network gateway ⓘ

Shared key (PSK) *

Use Azure Private IP Address ⓘ

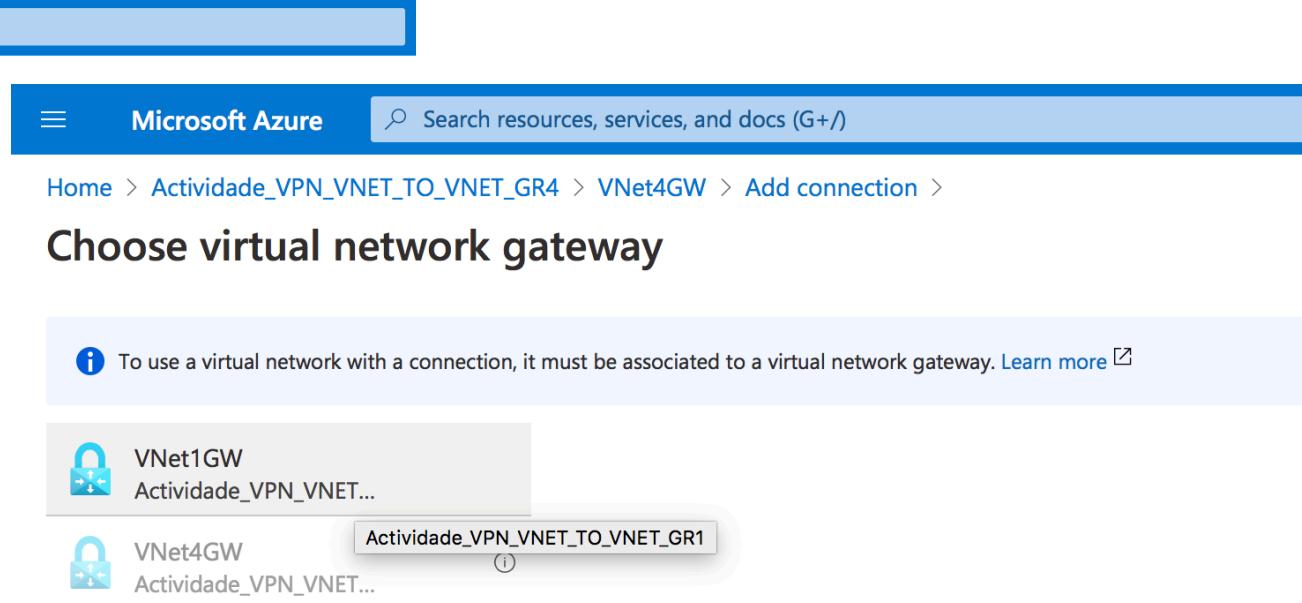
Enable BGP ⓘ

IKE Protocol ⓘ

IKEv1 IKEv2

Subscription ⓘ

Resource group ⓘ



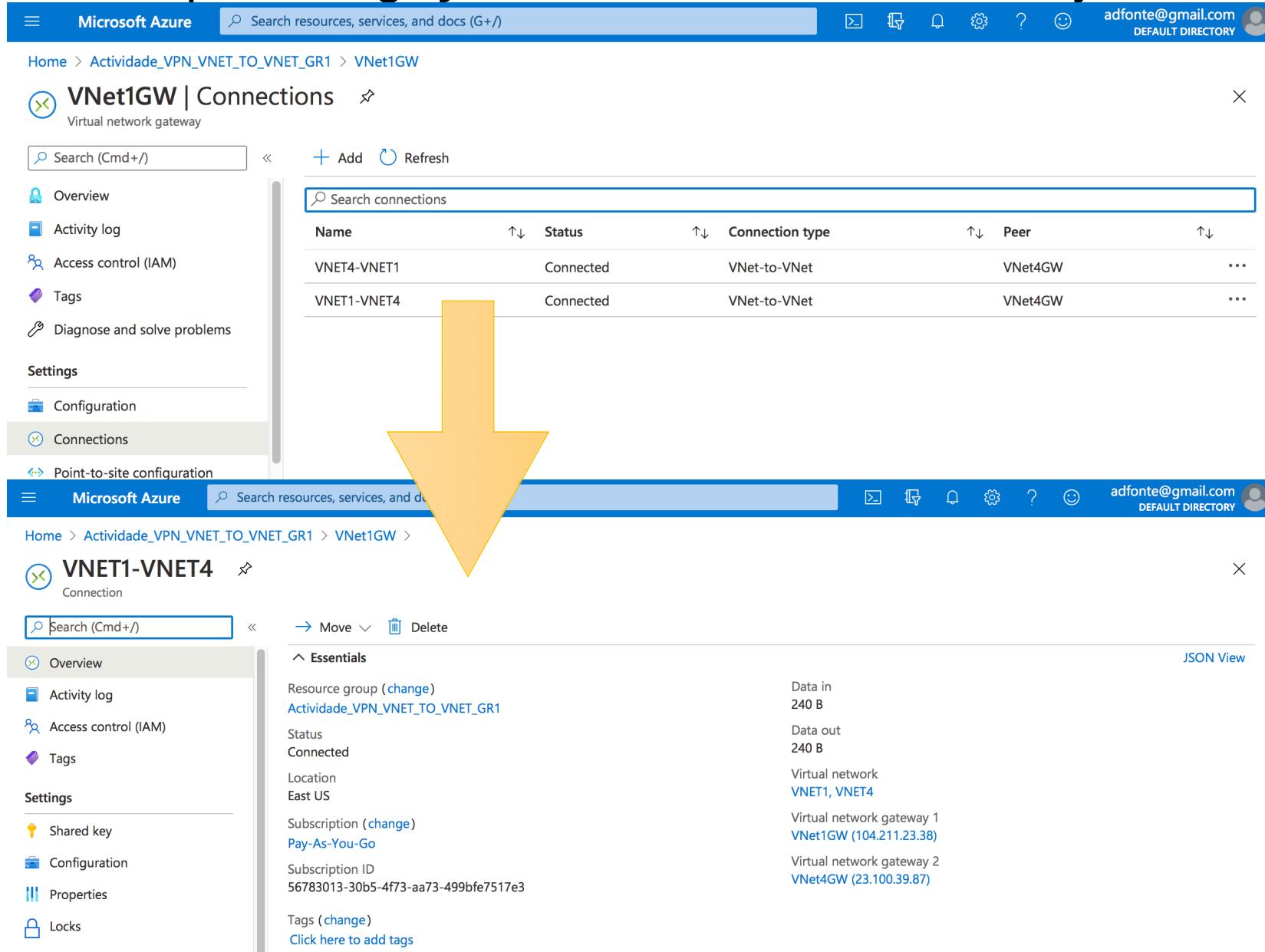
Choose virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway. [Learn more](#)

 VNet1GW Actividade_VPN_VNET...	 Actividade_VPN_VNET_TO_VNET_GR1 Actividade_VPN_VNET...
---	---

Azure VPN Gateway (Cont.)

- 7. Verifique as Ligações entre os VPNs Gateways



The screenshot displays two pages from the Microsoft Azure portal related to Virtual Network Gateways.

Top Page: The title is "VNet1GW | Connections". The left sidebar shows "Connections" is selected. The main area lists connections:

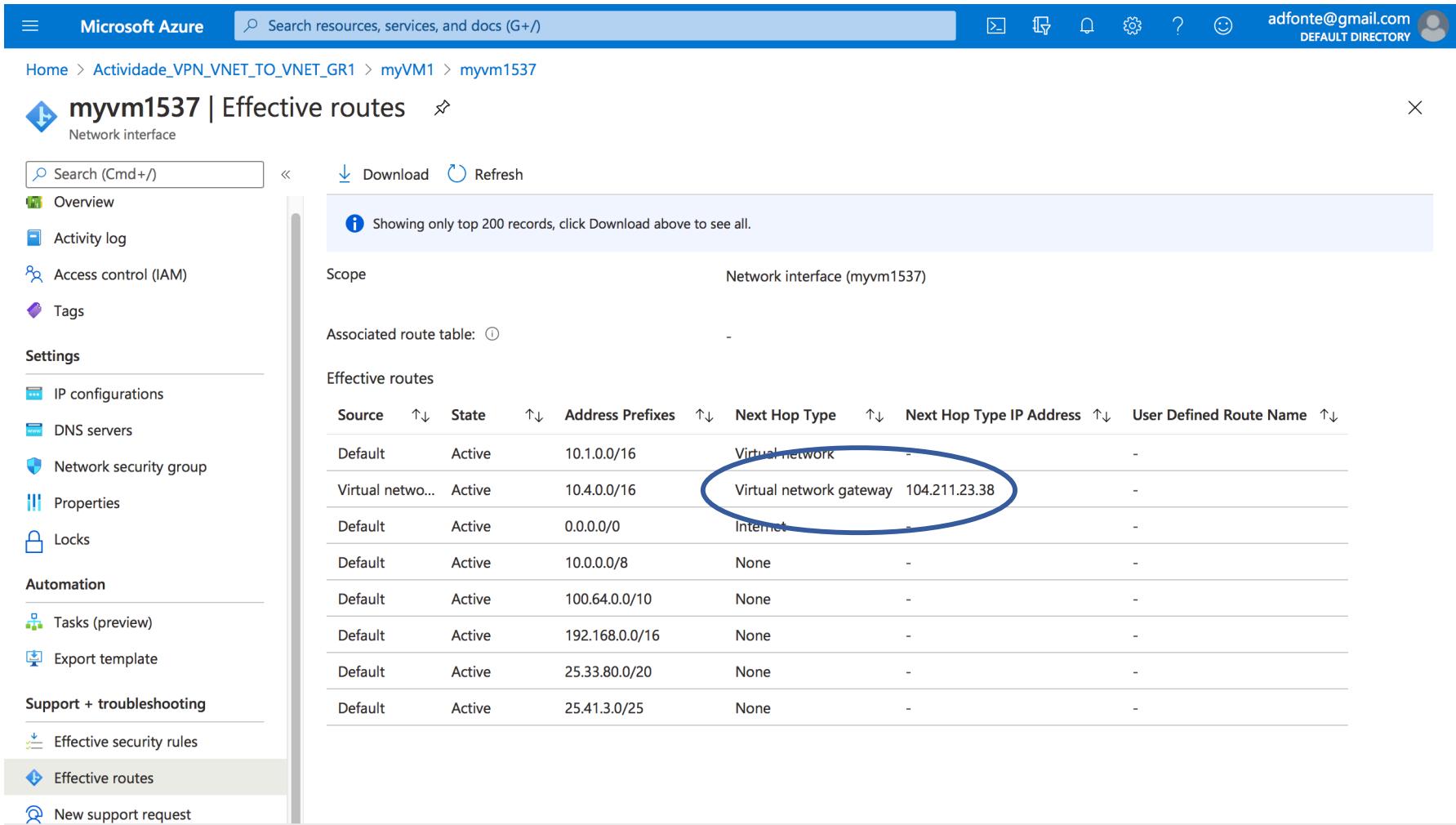
Name	Status	Connection type	Peer
VNET4-VNET1	Connected	VNet-to-VNet	VNet4GW
VNET1-VNET4	Connected	VNet-to-VNet	VNet4GW

Bottom Page: The title is "VNET1-VNET4 | Connection". The left sidebar shows "Connections" is selected. The main area shows the connection details:

Essentials		JSON View
Resource group	(change) Actividade_VPN_VNET_TO_VNET_GR1	Data in 240 B
Status	Connected	Data out 240 B
Location	East US	Virtual network VNET1, VNET4
Subscription	(change) Pay-As-You-Go	Virtual network gateway 1 VNet1GW (104.211.23.38)
Subscription ID	56783013-30b5-4f73-aa73-499bfe7517e3	Virtual network gateway 2 VNet4GW (23.100.39.87)
Tags	(change) Click here to add tags	

Azure VPN Gateway (Cont.)

- 7. Verificação da Tabela de Encaminhamento de myVM1 da VNET1 e Teste de Conectividade final



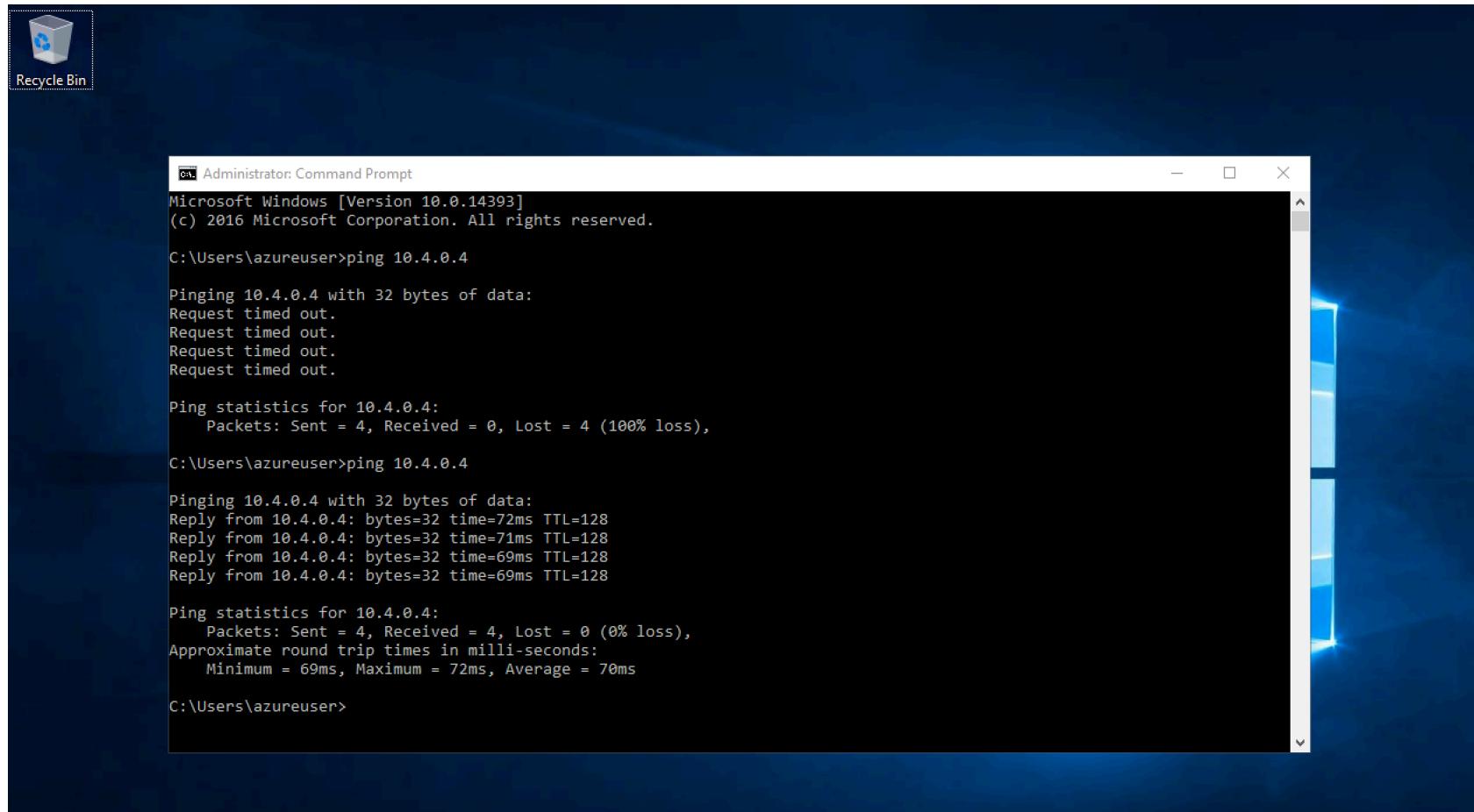
The screenshot shows the Microsoft Azure portal interface for managing a network interface named 'myvm1537'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Settings (IP configurations, DNS servers, Network security group, Properties, Locks), Automation (Tasks (preview), Export template), Support + troubleshooting (Effective security rules, Effective routes, New support request), and Effective routes (which is currently selected).

The main content area displays the 'Effective routes' table. The table has columns for Source, State, Address Prefixes, Next Hop Type, IP Address, and User Defined Route Name. The table shows several routes, including a default route to 10.1.0.0/16 via a virtual network, a route to 10.4.0.0/16 via a virtual network gateway (IP address 104.211.23.38), and other default routes to various address ranges via the Internet.

Source	State	Address Prefixes	Next Hop Type	IP Address	User Defined Route Name
Default	Active	10.1.0.0/16	Virtual network	-	-
Virtual netwo...	Active	10.4.0.0/16	Virtual network gateway	104.211.23.38	-
Default	Active	0.0.0.0/0	Internet	-	-
Default	Active	10.0.0.0/8	None	-	-
Default	Active	100.64.0.0/10	None	-	-
Default	Active	192.168.0.0/16	None	-	-
Default	Active	25.33.80.0/20	None	-	-
Default	Active	25.41.3.0/25	None	-	-

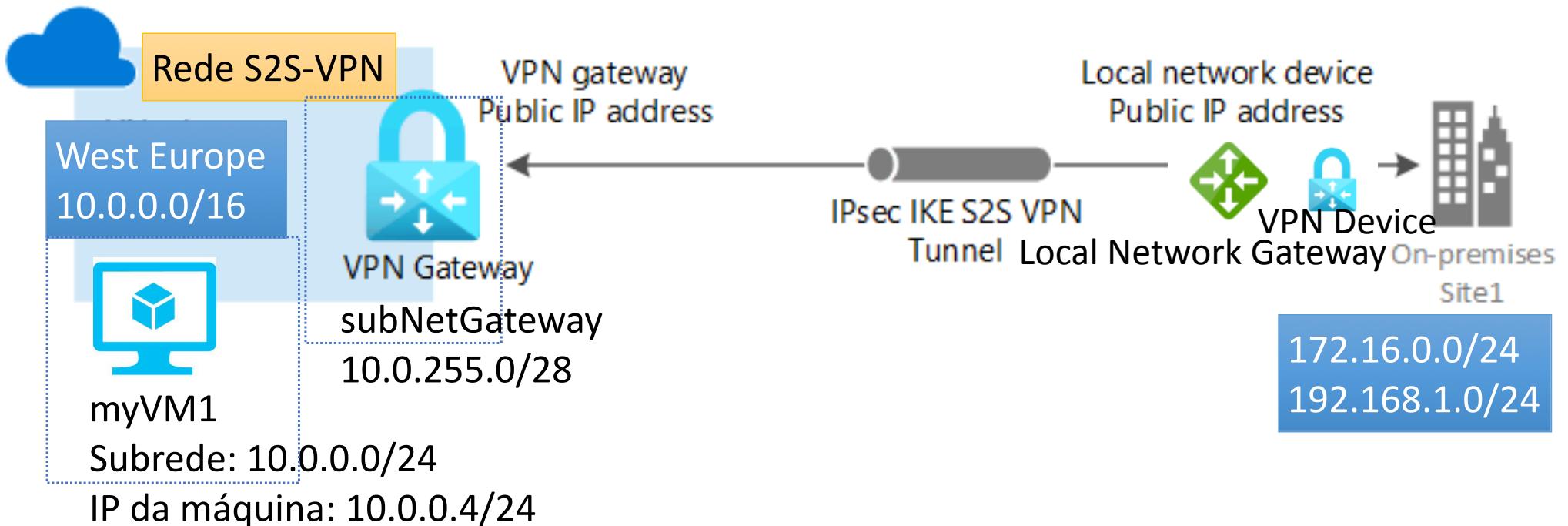
Azure VPN Gateway (Cont.)

- Teste final
 - Finalmente, a partir da myVM1 já poderemos pingar a myVM4





Configurar uma ligação Site-to-Site (S2S) usando VPN Gateways



Azure VPN Gateway (Cont.)



Configurar uma ligação Site-to-Site (S2S) usando VPN Gateways

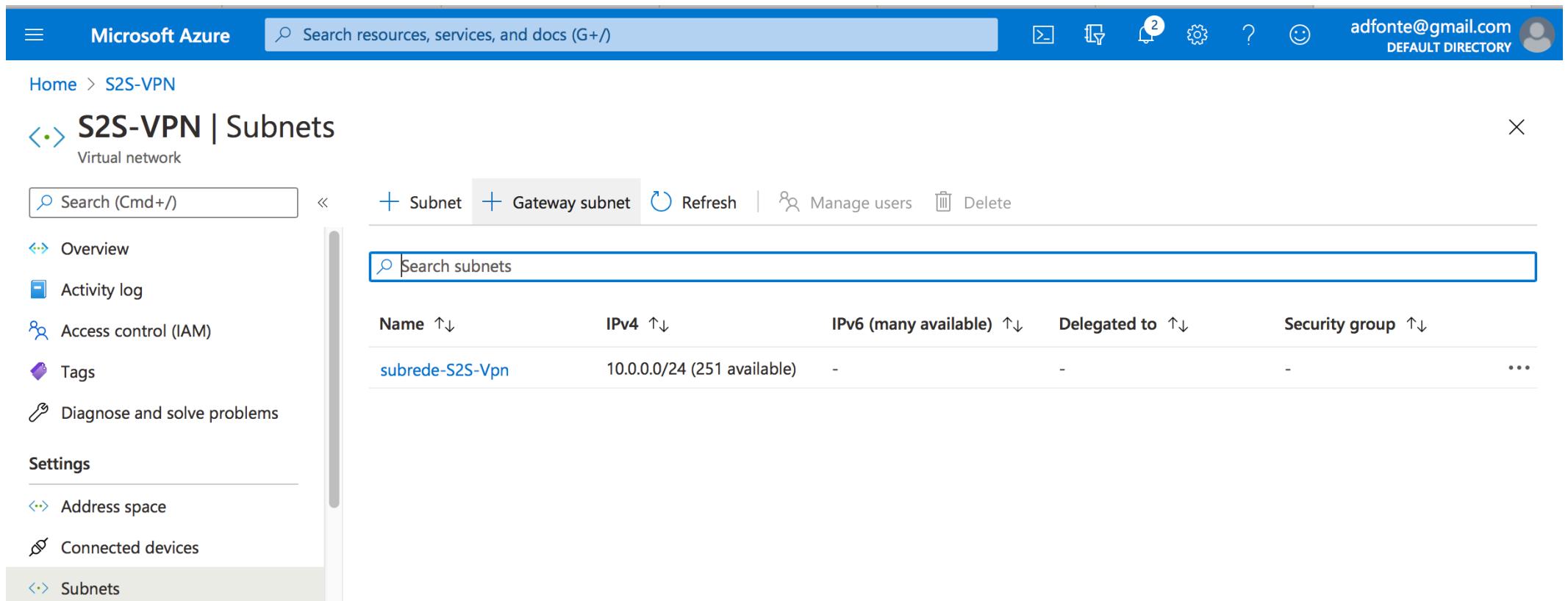
- Esta atividade será realizada em 10 passos:
 - #1: Criar o grupo de recursos
 - #2: Criar a rede virtual
 - #3: Criar o **Local Network Gateway**
 - #4: Criar um endereço Público para o Gateway VPN
 - #5: Criar o Gateway VPN da Rede Virtual Azure
 - #6: Criar a Ligação VPN
 - #7: Criar a máquina virtual na rede virtual
 - #8: Configurar o VPN Device da rede On-Premises
 - #9: Configuração de uma rota estática no Servidor local para desviar o tráfego para a rede 10.0.0.0 através da VPN
 - #10: Realizar uma ligação RDP à VM de teste

Azure VPN Gateway (Cont.)

- #1 Criar o grupo de recursos
 - Nome: Atividade_S2S_VPN
 - Região: (Europe) West Europe
- #2 Criar a Rede Virtual, a subrede para a VM myVM1 e a subrede para o Gateway VPN
- #2.1: Rede virtual + Subnet subrede-S2S-Vpn
 - Nome: S2S-VPN
 - Region: West Europe
 - Espaço de endereçamento: 10.0.0.0/16
 - Subnet: subrede-S2S-Vpn (10.0.0.0/24)

Azure VPN Gateway (Cont.)

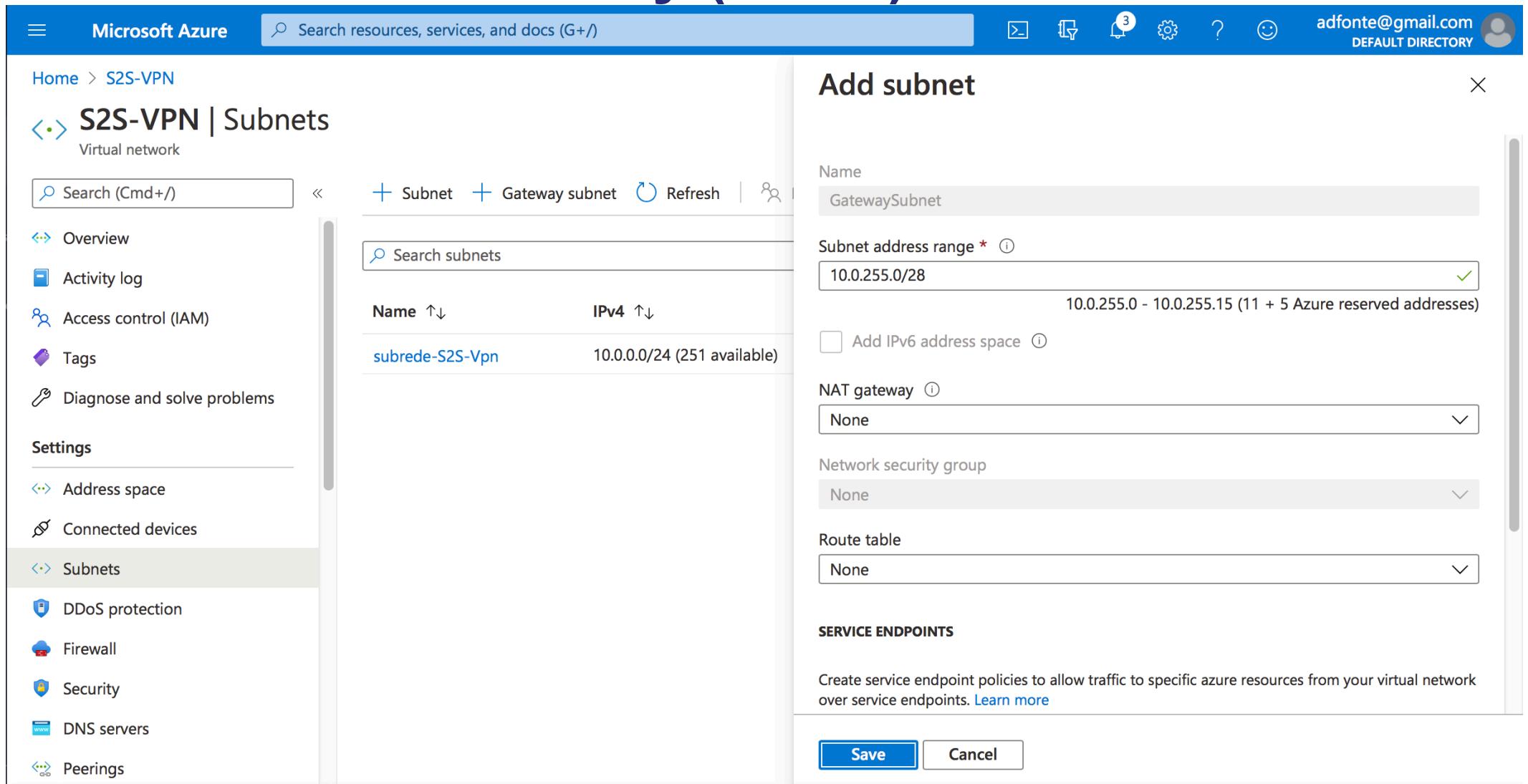
- #2.2: Subnet subrede-Gateway-Vpn



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (adfente@gmail.com, DEFAULT DIRECTORY). Below the navigation bar, the breadcrumb navigation shows 'Home > S2S-VPN'. The main title is 'S2S-VPN | Subnets' under the 'Virtual network' section. On the left, there is a sidebar with links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Address space, Connected devices, and Subnets selected), and a search bar. The main content area has a header with buttons for '+ Subnet', '+ Gateway subnet', 'Refresh', 'Manage users', and 'Delete'. A search bar labeled 'Search subnets' is present. The table lists one subnet: 'subrede-S2S-Vpn' with IPv4 range '10.0.0.0/24 (251 available)' and no delegation or security group assigned.

Name	IPv4	IPv6 (many available)	Delegated to	Security group
subrede-S2S-Vpn	10.0.0.0/24 (251 available)	-	-	-

Azure VPN Gateway (Cont.)



The screenshot shows the Microsoft Azure portal interface for managing a Virtual Network (S2S-VPN). On the left, the navigation menu includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. Under Settings, Subnets is selected. The main pane displays the 'S2S-VPN | Subnets' page, showing a table with one existing subnet named 'subrede-S2S-Vpn' with an IPv4 range of 10.0.0.0/24 (251 available). A search bar at the top right is set to 'Search resources, services, and docs (G+)'. A modal window titled 'Add subnet' is open on the right, prompting for configuration details:

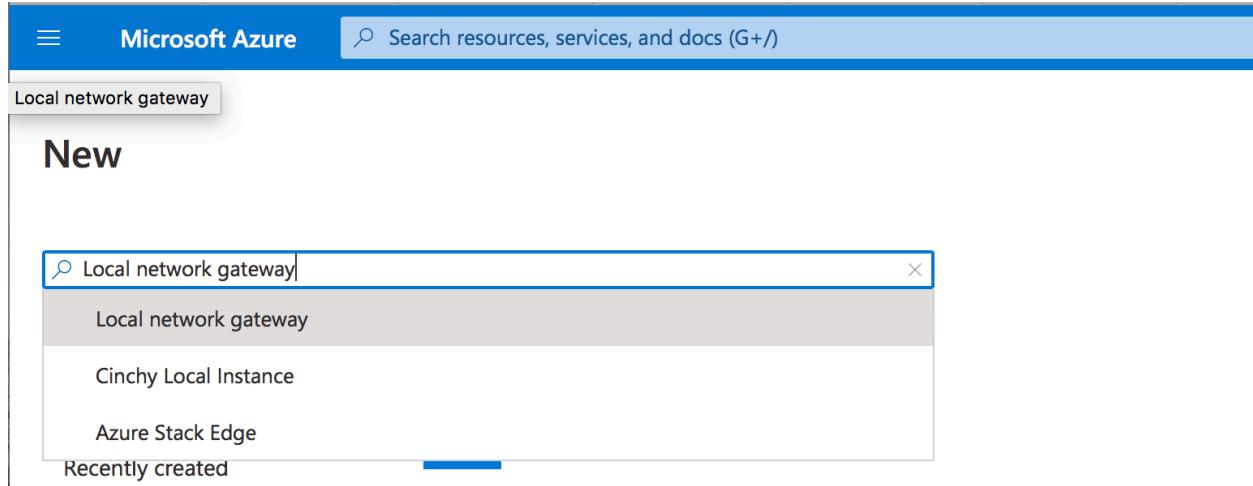
- Name:** GatewaySubnet
- Subnet address range ***: 10.0.255.0/28 (10.0.255.0 - 10.0.255.15 (11 + 5 Azure reserved addresses))
- Add IPv6 address space**: Unchecked
- NAT gateway**: None
- Network security group**: None
- Route table**: None

SERVICE ENDPOINTS section: Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

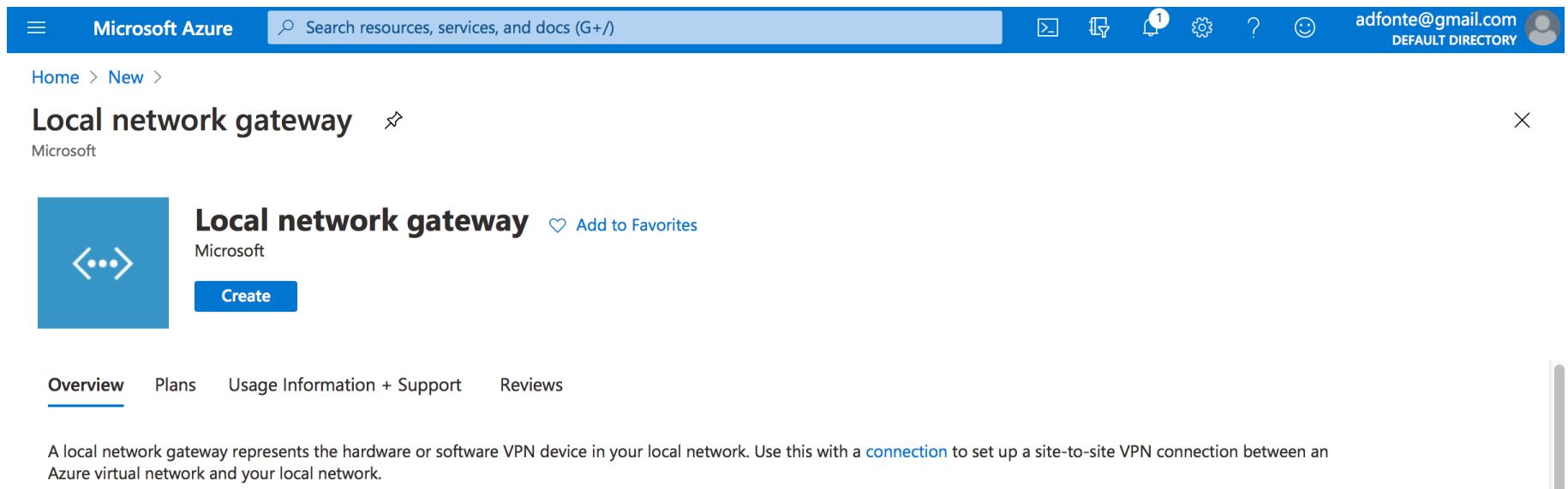
At the bottom of the modal are 'Save' and 'Cancel' buttons.

Azure VPN Gateway (Cont.)

- #3: Criar o Local Network Gateway



The screenshot shows the Microsoft Azure search interface. The search bar at the top contains the text "Local network gateway". Below the search bar is a dropdown menu with three items: "Local network gateway", "Cinchy Local Instance", and "Azure Stack Edge". The "Local network gateway" item is highlighted.

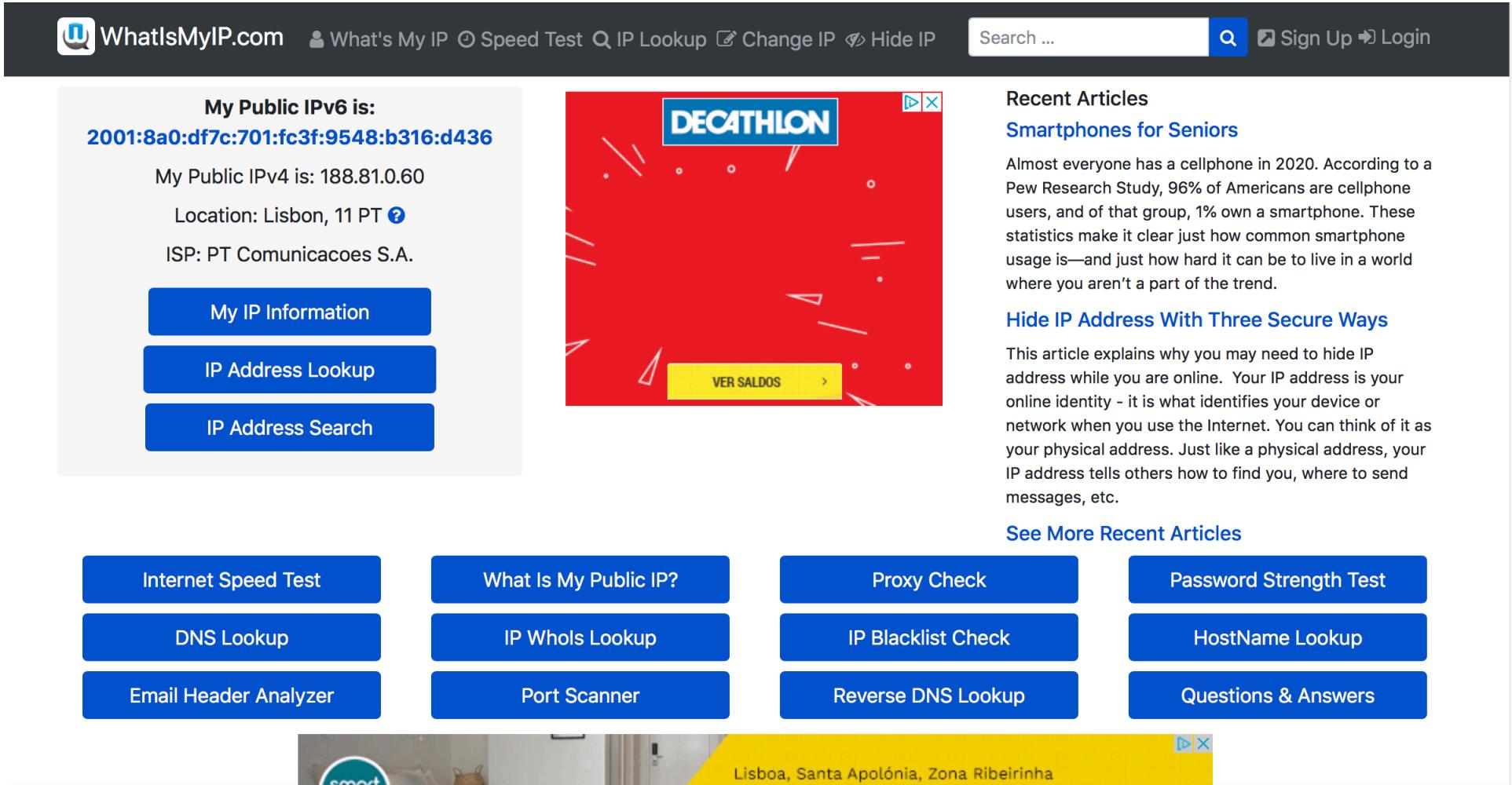


The screenshot shows the Microsoft Azure marketplace search results for "Local network gateway". The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (adfonte@gmail.com, DEFAULT DIRECTORY). The search results page shows a single result: "Local network gateway" by Microsoft. The product card features a blue icon with a double-headed arrow, the product name, the Microsoft logo, and a "Create" button. Below the card, there are navigation links: "Overview" (underlined), "Plans", "Usage Information + Support", and "Reviews". A descriptive text at the bottom explains what a local network gateway is: "A local network gateway represents the hardware or software VPN device in your local network. Use this with a [connection](#) to set up a site-to-site VPN connection between an Azure virtual network and your local network."

Azure VPN Gateway (Cont.)

• #3: Criar o Local Network Gateway

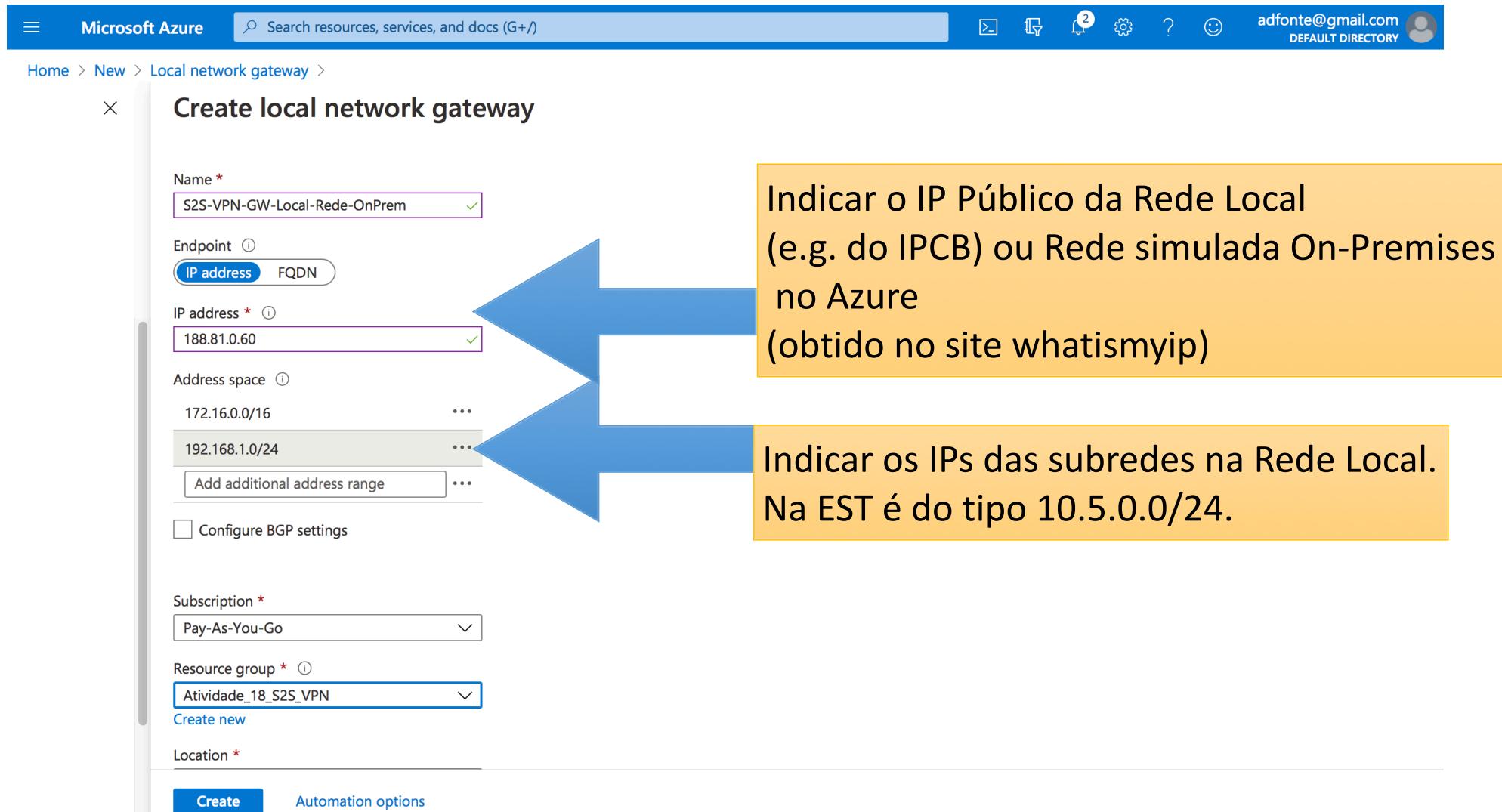
-Consultar o nosso IP público: www.whatismyip.com



The screenshot shows the homepage of WhatIsMyIP.com. On the left, a sidebar displays the user's public IP addresses: IPv6 (2001:8a0:df7c:701:fc3f:9548:b316:d436) and IPv4 (188.81.0.60), along with location (Lisbon, 11 PT) and ISP (PT Comunicacoes S.A.). Below these are three blue buttons: "My IP Information", "IP Address Lookup", and "IP Address Search". The main content area features a large red banner with the Decathlon logo and a yellow button labeled "VER SALDOS". To the right, there's a "Recent Articles" section with a link to "Smartphones for Seniors" and a paragraph about smartphone usage. Further down is another article titled "Hide IP Address With Three Secure Ways" with a detailed explanation. At the bottom, there are two rows of blue buttons for various services: Internet Speed Test, What Is My Public IP?, Proxy Check, Password Strength Test; DNS Lookup, IP Whois Lookup, IP Blacklist Check, HostName Lookup; Email Header Analyzer, Port Scanner, Reverse DNS Lookup, Questions & Answers. A footer banner at the bottom indicates the location as Lisboa, Santa Apolónia, Zona Ribeirinha.

Azure VPN Gateway (Cont.)

- #3: Criar o Local Network Gateway (Cont.)



The screenshot shows the 'Create local network gateway' wizard in the Microsoft Azure portal. The form includes fields for Name, Endpoint, IP address, Address space, Subscription, Resource group, and Location. Two large blue arrows point from callout boxes to specific fields: one arrow points to the 'IP address' field, and another points to the 'Address space' section.

Name *
S2S-VPN-GW-Local-Rede-OnPrem

Endpoint
 IP address FQDN

IP address *
188.81.0.60

Address space
172.16.0.0/16
192.168.1.0/24
Add additional address range

Configure BGP settings

Subscription *
Pay-As-You-Go

Resource group *
Atividade_18_S2S_VPN
Create new

Location *

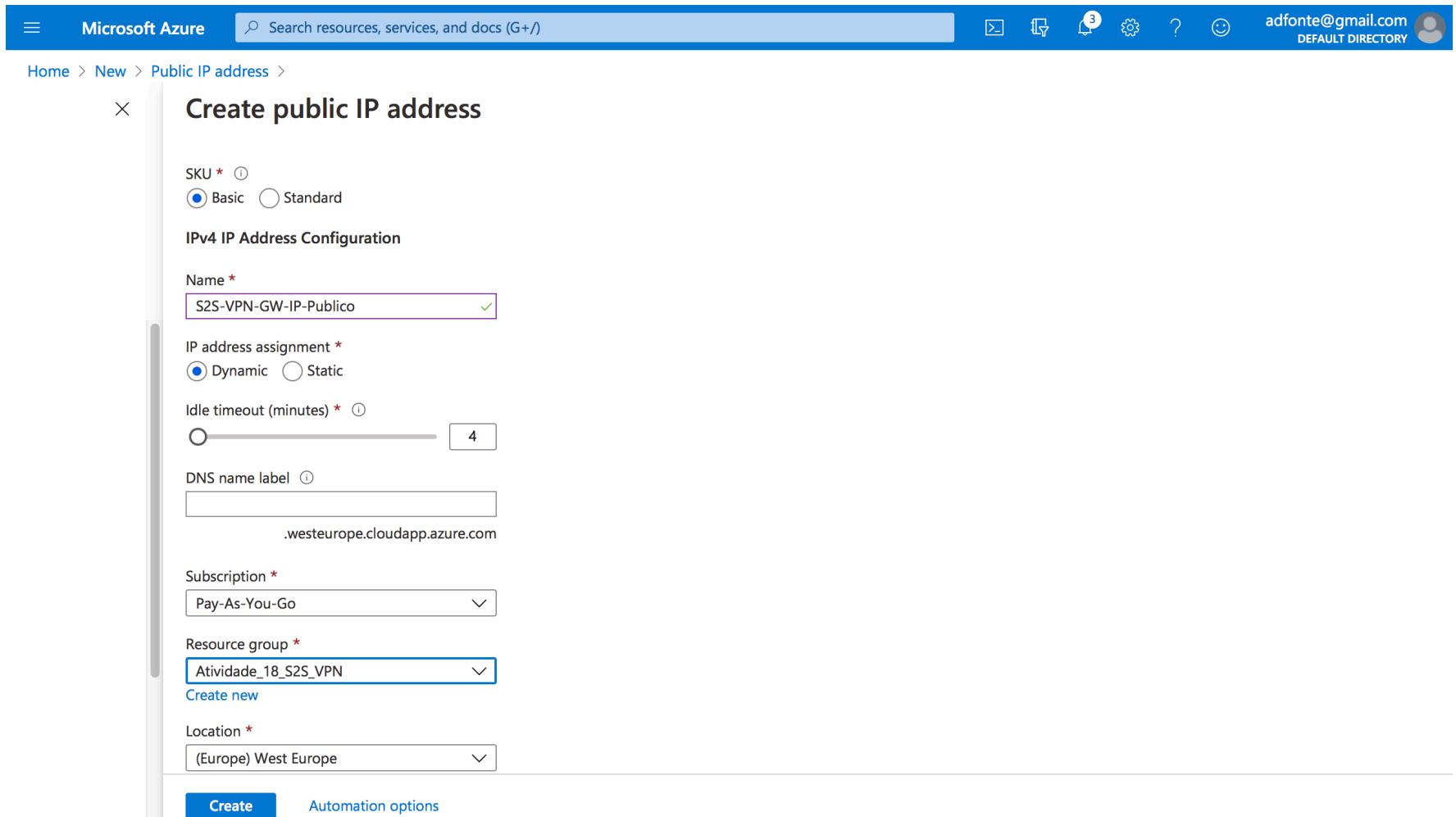
Create Automation options

Indicar o IP Público da Rede Local (e.g. do IPCB) ou Rede simulada On-Premises no Azure (obtido no site whatismyip)

Indicar os IPs das subredes na Rede Local. Na EST é do tipo 10.5.0.0/24.

Azure VPN Gateway (Cont.)

- #4: Criar um endereço Público para o Gateway VPN
-Nome: S2S-VPN-GW-IP-Publico



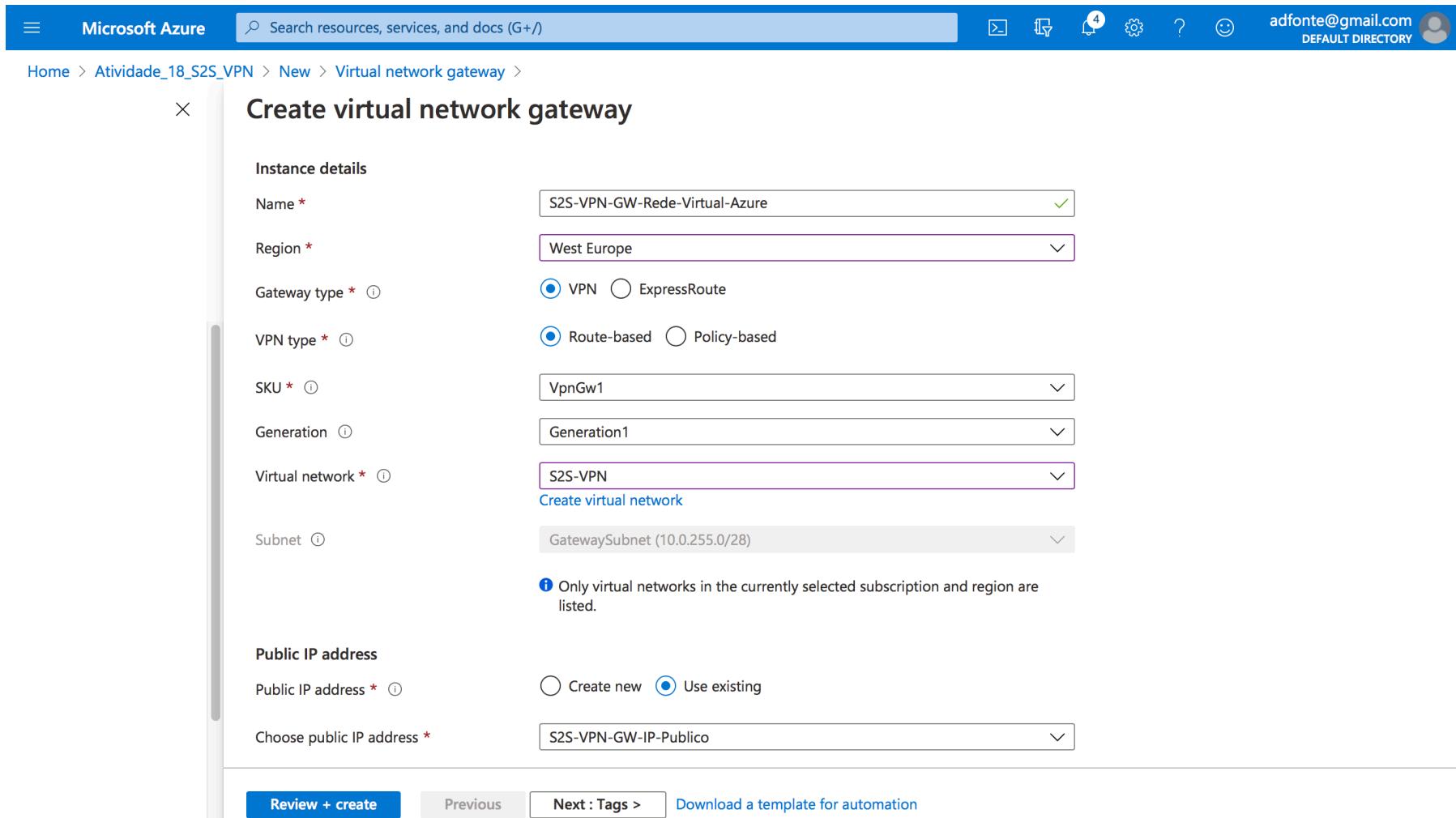
The screenshot shows the 'Create public IP address' wizard in the Microsoft Azure portal. The steps are as follows:

- SKU ***: Basic (selected)
- IPv4 IP Address Configuration**
 - Name ***: S2S-VPN-GW-IP-Publico
 - IP address assignment ***: Dynamic (selected)
 - Idle timeout (minutes) ***: 4
 - DNS name label**: .westeurope.cloudapp.azure.com
- Subscription ***: Pay-As-You-Go
- Resource group ***: Atividade_18_S2S_VPN
- Location ***: (Europe) West Europe

At the bottom, there are two buttons: **Create** (highlighted in blue) and **Automation options**.

Azure VPN Gateway (Cont.)

- #5: Criar o Gateway VPN da Rede Virtual Azure
 - Nome: S2S-VPN-GW-Rede-Virtual-Azure
 - Rede Virtual: S2S-VPN e GatewaySubnet



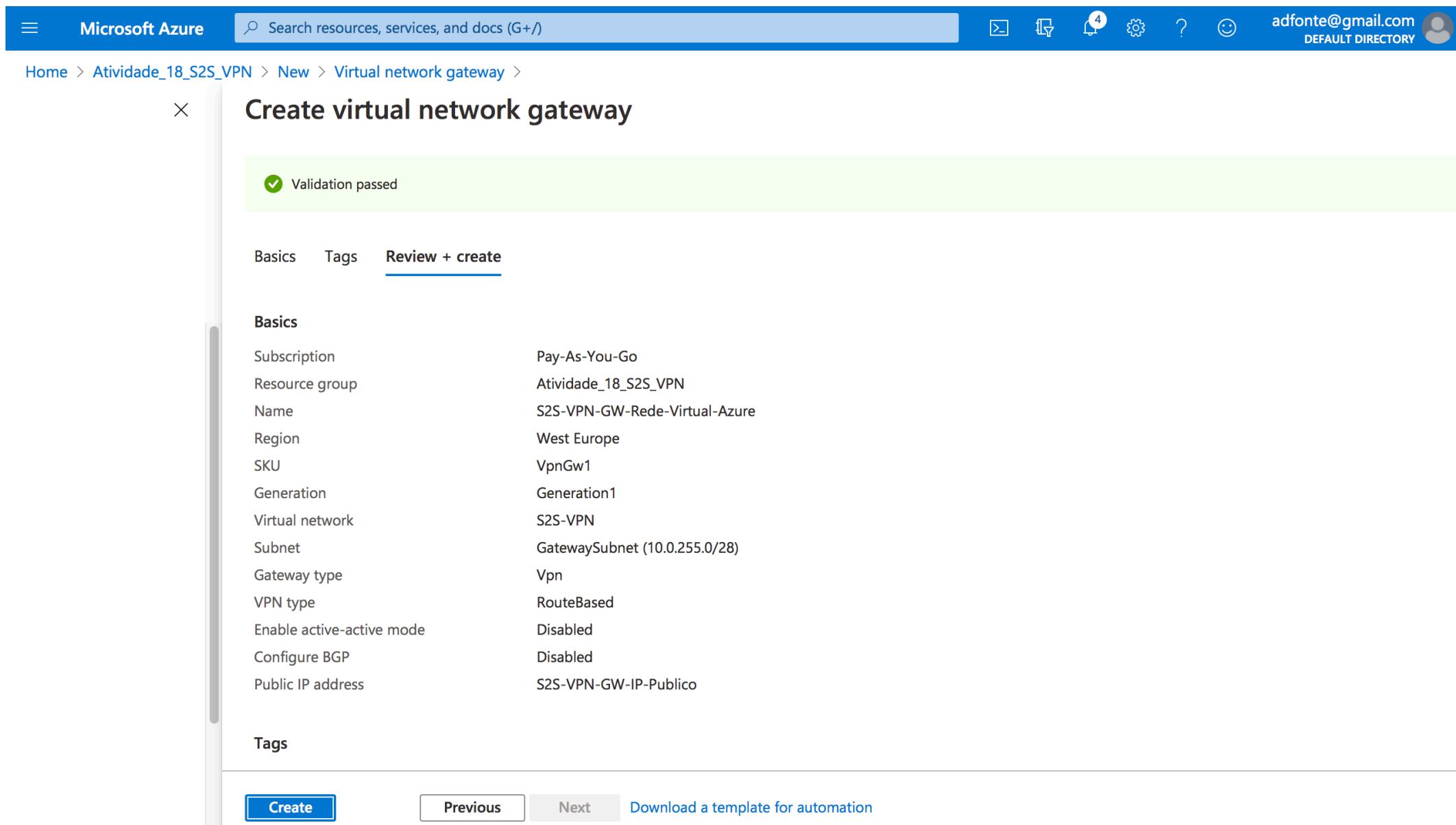
The screenshot shows the 'Create virtual network gateway' wizard in the Microsoft Azure portal. The page is titled 'Create virtual network gateway'. It contains several configuration sections:

- Instance details**:
 - Name: S2S-VPN-GW-Rede-Virtual-Azure
 - Region: West Europe
 - Gateway type: VPN (selected)
 - VPN type: Route-based (selected)
 - SKU: VpnGw1
 - Generation: Generation1
 - Virtual network: S2S-VPN (selected)
 - Subnet: GatewaySubnet (10.0.255.0/28)
- Public IP address**:
 - Public IP address: S2S-VPN-GW-IP-Publico
 - Options: Create new (radio button) or Use existing (radio button selected)

At the bottom, there are navigation buttons: 'Review + create', 'Previous', 'Next : Tags >', and 'Download a template for automation'. The status bar at the bottom right shows '112'.

Azure VPN Gateway (Cont.)

- #5: Criar o Gateway VPN da Rede Virtual Azure (Cont.)



Microsoft Azure Search resources, services, and docs (G+) 4 ? DEFAULT DIRECTORY

Home > Atividade_18_S2S_VPN > New > Virtual network gateway >

Create virtual network gateway

Validation passed

Basics Tags Review + create

Basics

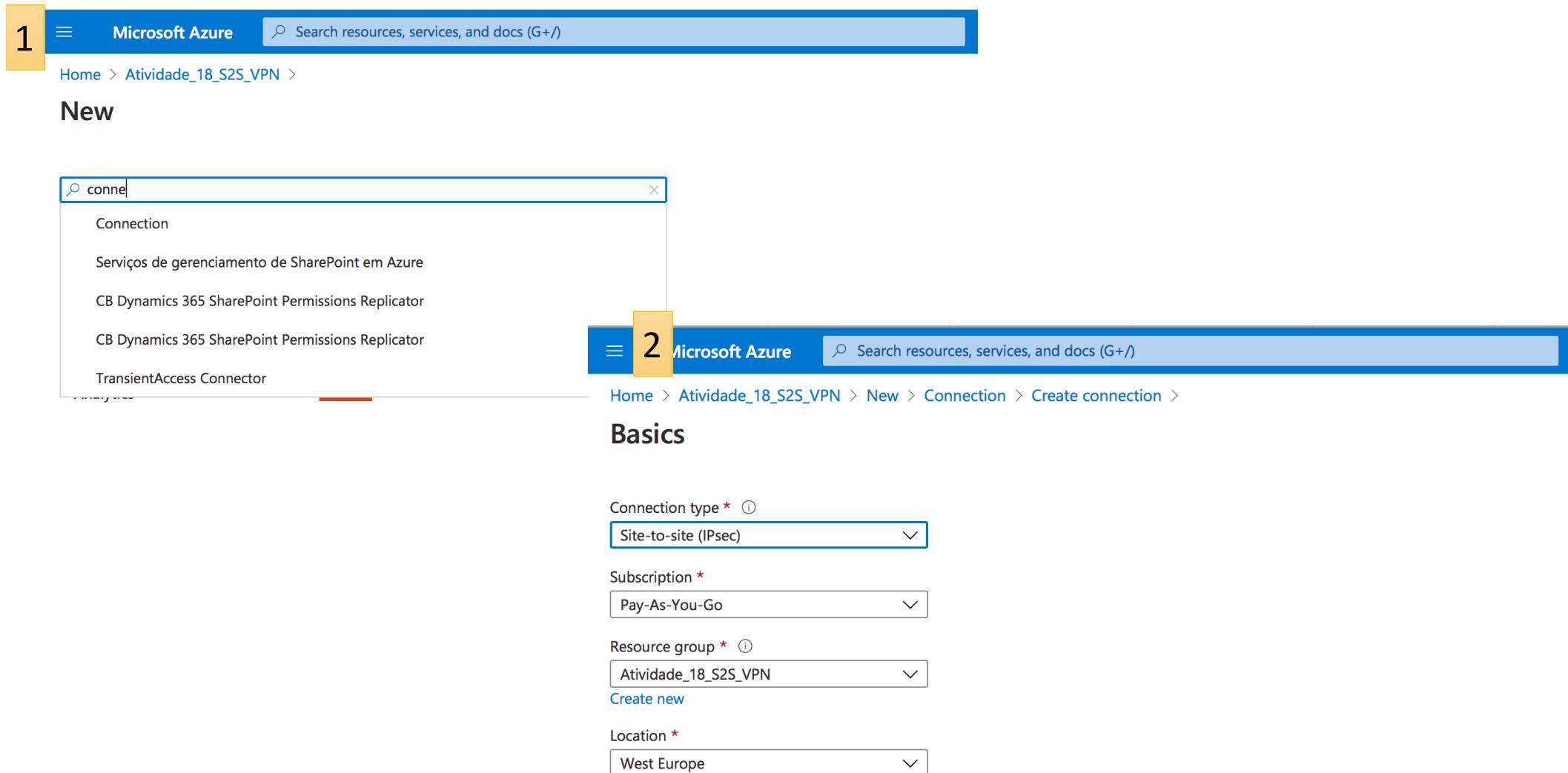
Subscription	Pay-As-You-Go
Resource group	Atividade_18_S2S_VPN
Name	S2S-VPN-GW-Rede-Virtual-Azure
Region	West Europe
SKU	VpnGw1
Generation	Generation1
Virtual network	S2S-VPN
Subnet	GatewaySubnet (10.0.255.0/28)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	S2S-VPN-GW-IP-Publico

Tags

Create Previous Next Download a template for automation

Azure VPN Gateway (Cont.)

- #6: Criar a Ligação VPN



The screenshot illustrates the process of creating a Site-to-Site (S2S) VPN connection in the Microsoft Azure portal.

Panel 1: A search bar at the top left contains the text "conne". Below it is a list of search results:

- Connection
- Serviços de gerenciamento de SharePoint em Azure
- CB Dynamics 365 SharePoint Permissions Replicator
- CB Dynamics 365 SharePoint Permissions Replicator
- TransientAccess Connector

Panel 2: The main Azure portal interface shows the following navigation path: Home > Atividade_18_S2S_VPN > New > Connection > Create connection. The current step is labeled "Basics". The configuration fields are:

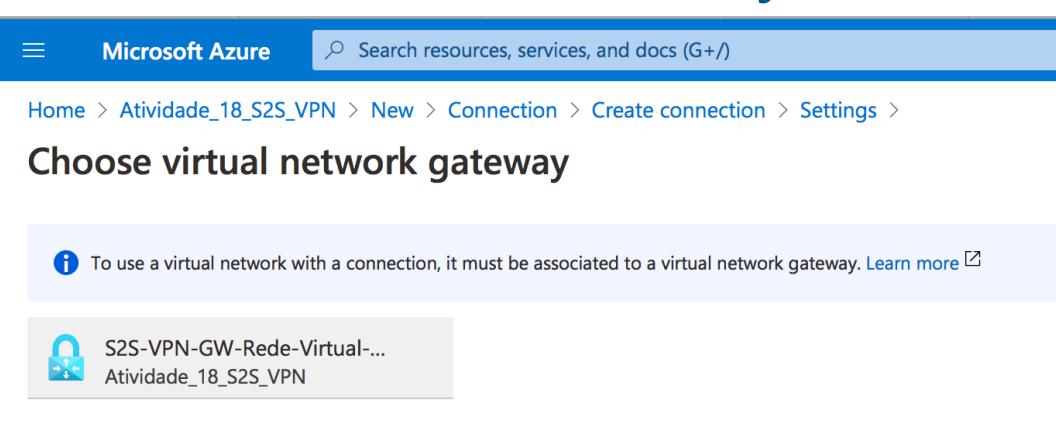
- Connection type ***: Site-to-site (IPsec)
- Subscription ***: Pay-As-You-Go
- Resource group ***: Atividade_18_S2S_VPN
- Create new** (link)
- Location ***: West Europe

Azure VPN Gateway (Cont.)

- #6: Criar a Ligação VPN

- A ligação VPN tem com extremidades do túnel VPN o VPN Gateway e o Local Network Gateway

3



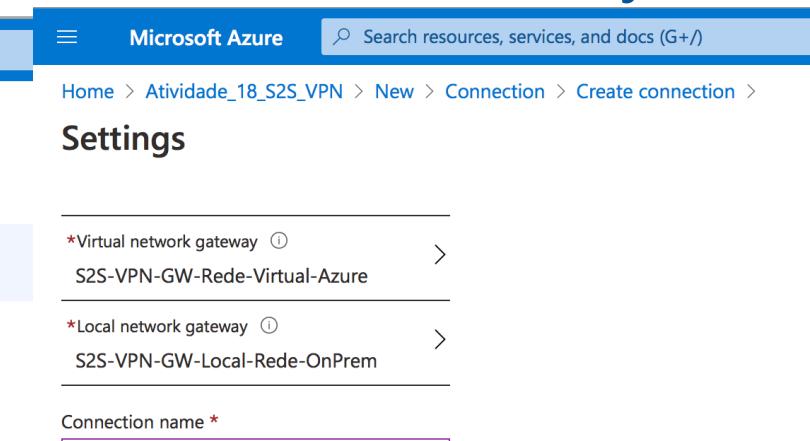
To use a virtual network with a connection, it must be associated to a virtual network gateway. [Learn more](#)

 S2S-VPN-GW-Rede-Virtual-...
Atividade_18_S2S_VPN

4



5



Virtual network gateway S2S-VPN-GW-Rede-Virtual-Azure

Local network gateway S2S-VPN-GW-Local-Rede-OnPrem

Connection name *

Shared key (PSK) *

IKE Protocol IKEv1 IKEv2

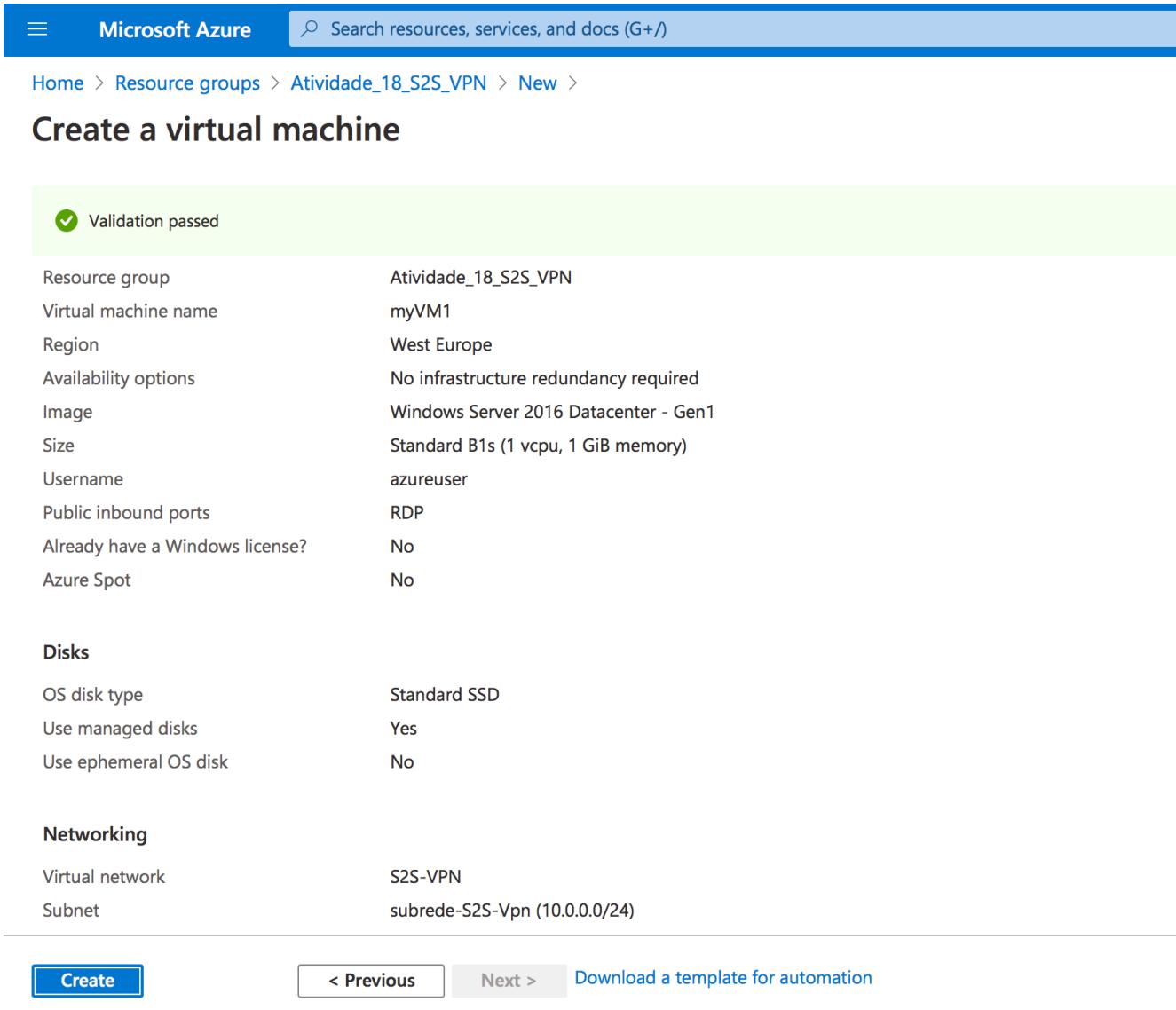
Use Azure Private IP Address

Enable BGP

A definição da chave partilhada e a escolha do protocolo IKEv2 são aspectos importantes

Azure VPN Gateway (Cont.)

- #7: Criar a máquina virtual de teste: myVM1 pertencente à Rede Virtual Azure



The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The configuration details are as follows:

Validation passed	
Resource group	Atividade_18_S2S_VPN
Virtual machine name	myVM1
Region	West Europe
Availability options	No infrastructure redundancy required
Image	Windows Server 2016 Datacenter - Gen1
Size	Standard B1s (1 vcpu, 1 GiB memory)
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Standard SSD
Use managed disks	Yes
Use ephemeral OS disk	No

Networking

Virtual network	S2S-VPN
Subnet	subrede-S2S-Vpn (10.0.0.0/24)

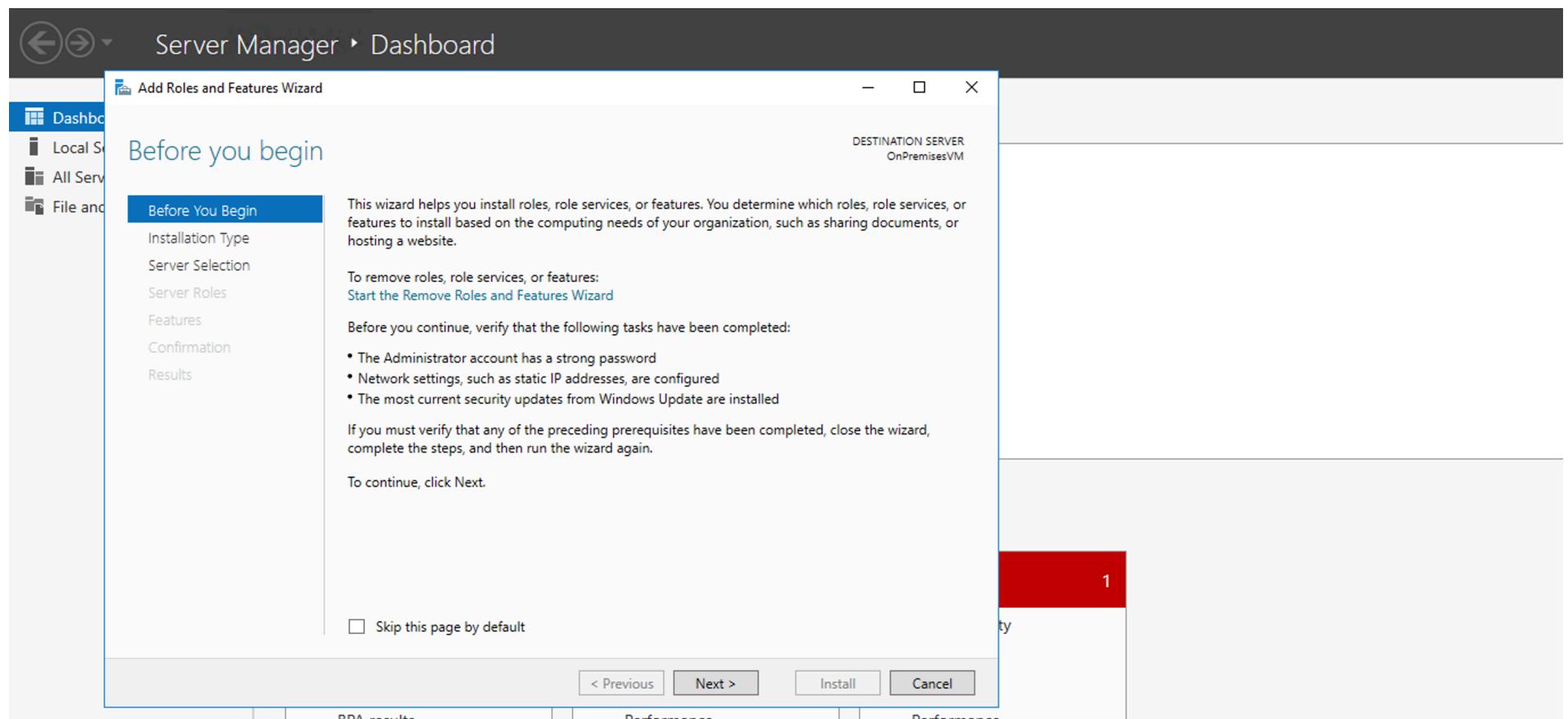
Buttons at the bottom: Create, < Previous, Next >, Download a template for automation.

Azure VPN Gateway (Cont.)

- #8: Configurar o VPN Device da rede On-Premises
 - Usar o serviço RRAS num servidor Windows Server local *
 - Nota: A melhor solução, contudo, seria estabelecer o túnel entre a firewall ou router de acesso e o VPN Gateway da rede virtual Azure
 - * *Como não dispomos de um servidor local Windows Datacenter ou outro da linha Server, vamos simular a rede On-Premise no Azure.*

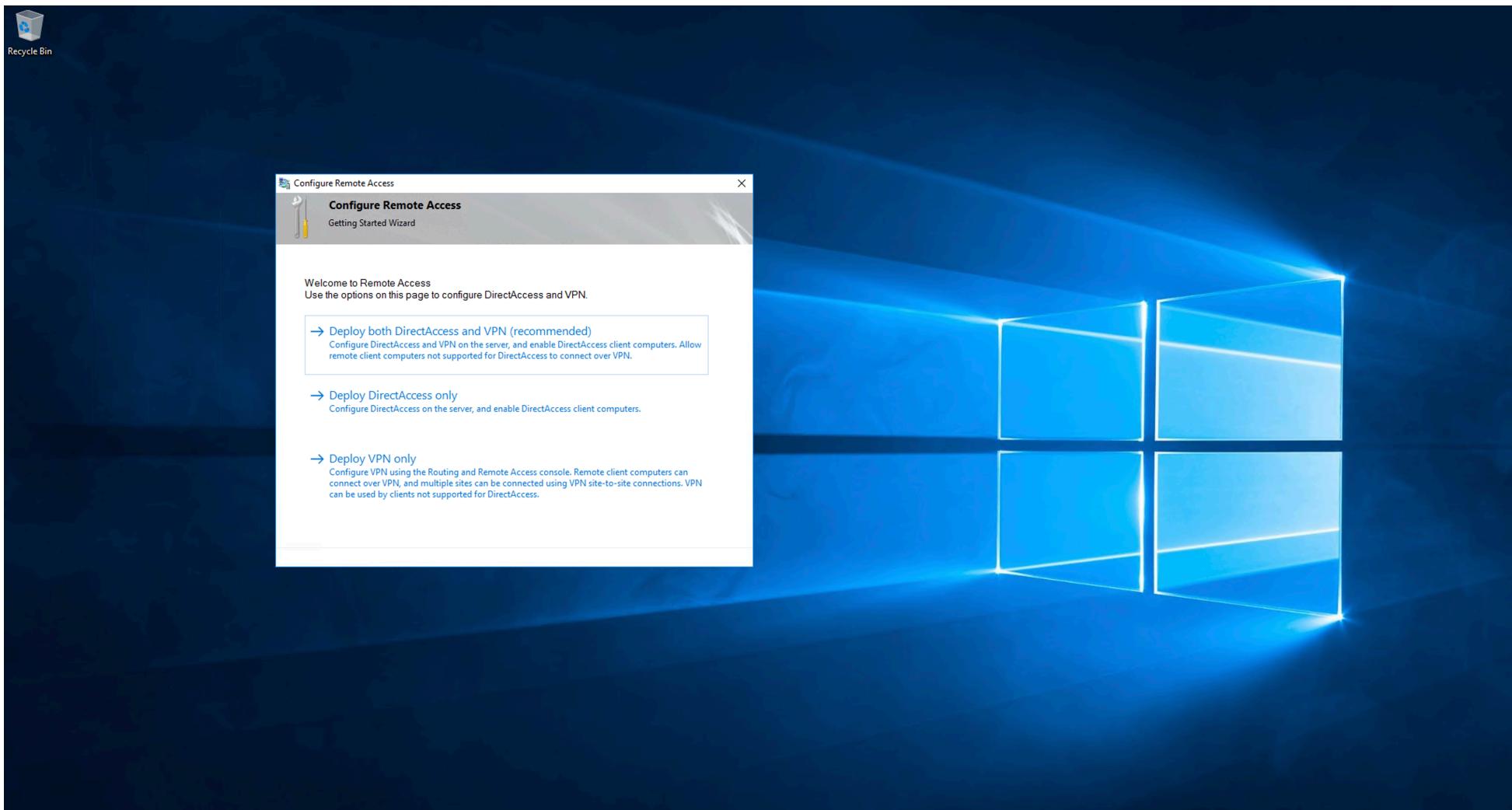
Azure VPN Gateway (Cont.)

- #8.1: Instalar o serviço **Routing and Remote Access**
 - Entrar no Server Manager do Servidor e clicar em Add Role and Features.
 - Adicionar o Server Role: Remote Access
 - Serviços de Remote Access: Direct Access e VPN e Routing



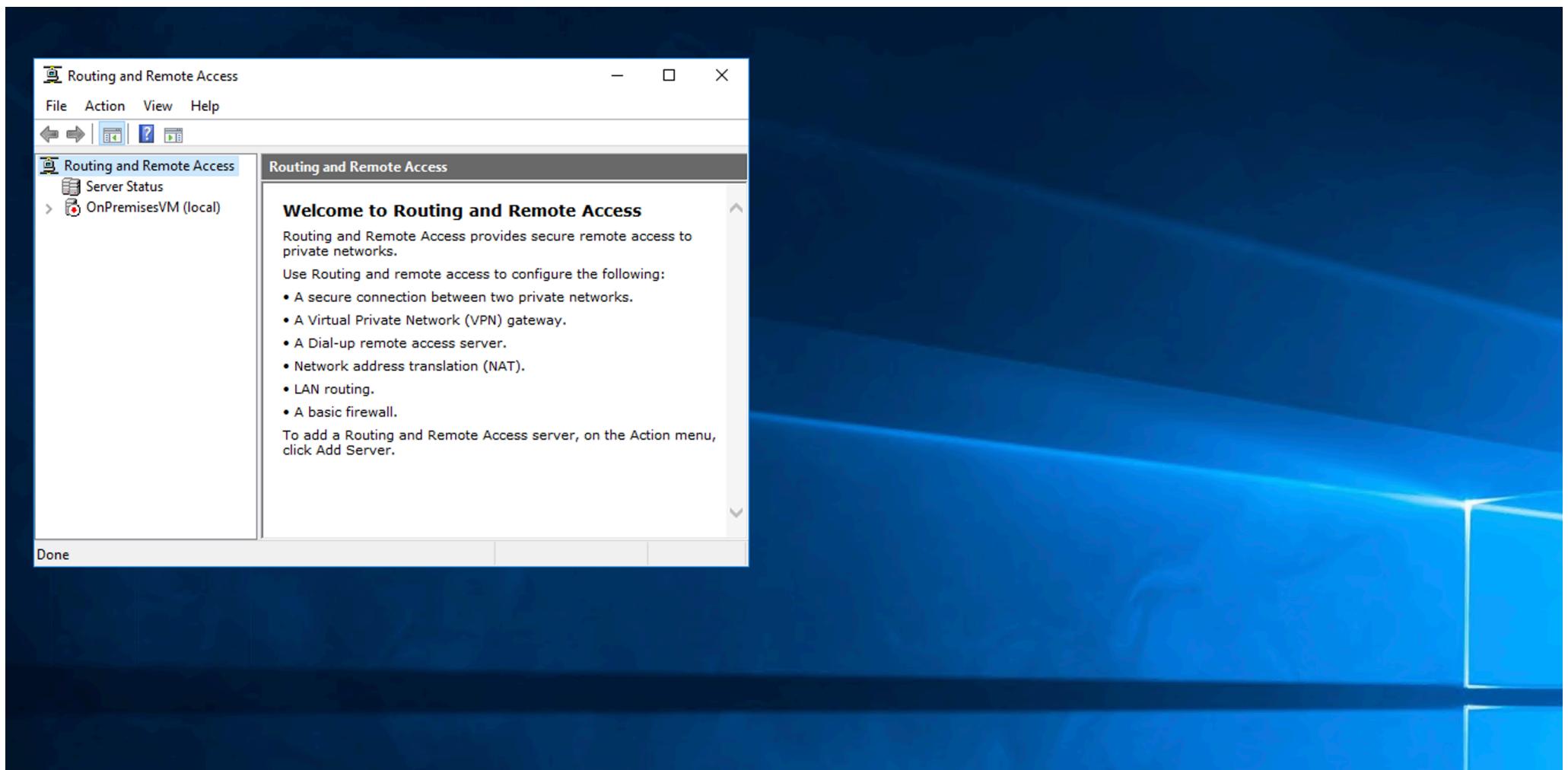
Azure VPN Gateway (Cont.)

- #8.1: Instalar o serviço **Routing and Remote Access** (Cont.)
 - Escolher a opção **Deploy VPN only**



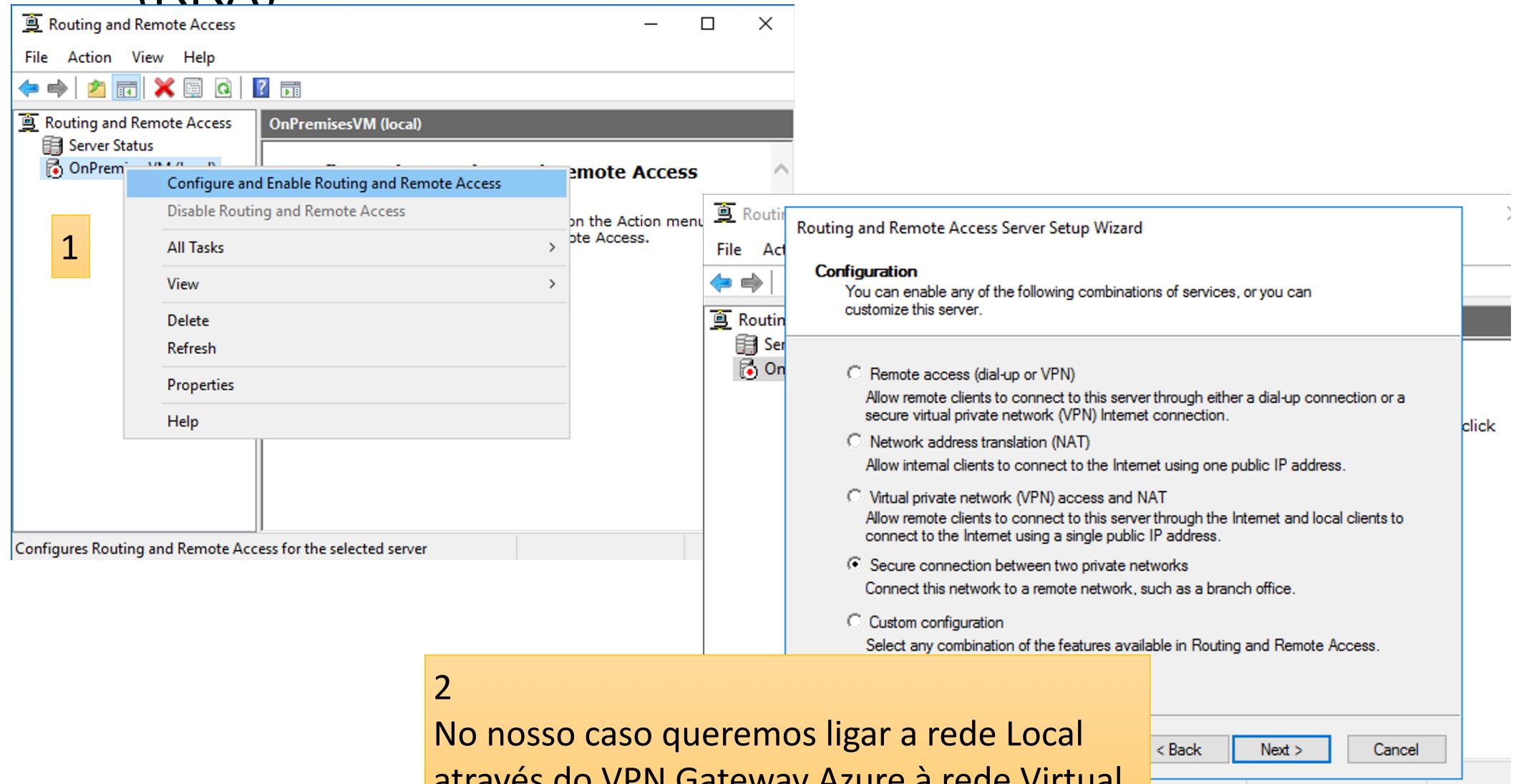
Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routing e Remote Access (RRA)
 - Seleccionar o Servidor local (OnPremisesVM)



Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routing e Remote Access (RRA)



2

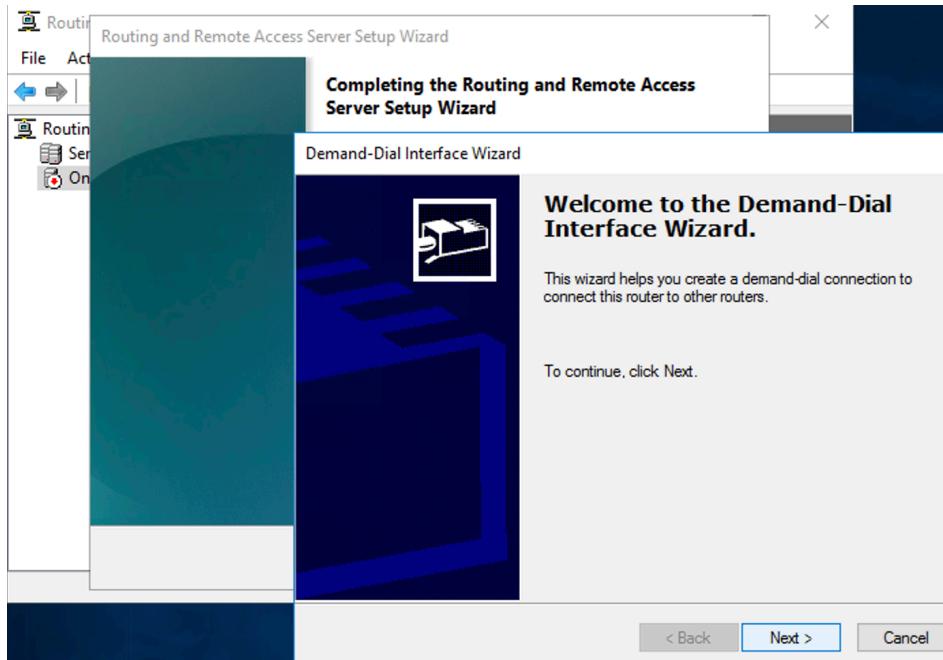
No nosso caso queremos ligar a rede Local através do VPN Gateway Azure à rede Virtual

Azure VPN Gateway (Cont.)

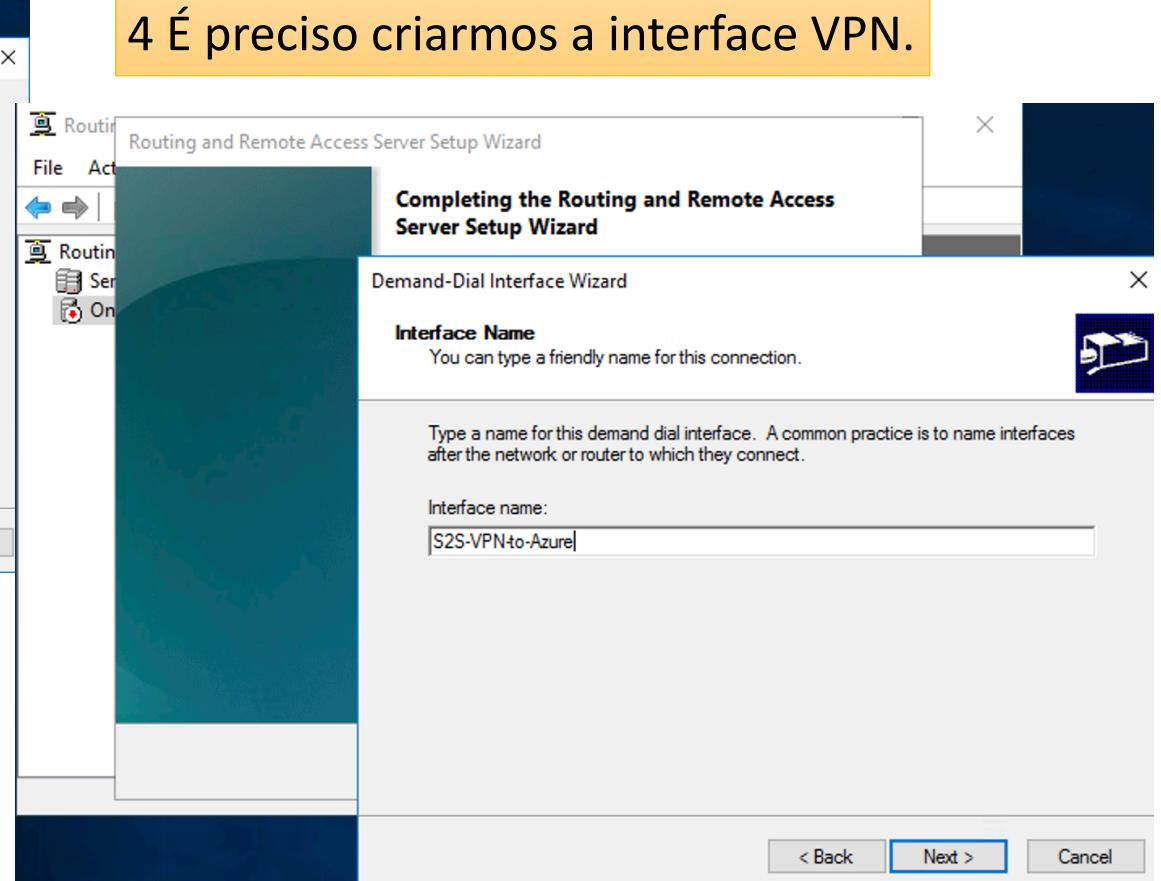
- #8.2: Realizar as configurações Routing e Remote Access (RRA)

3

-Cria a interface: S2S-VPN-to-Azure

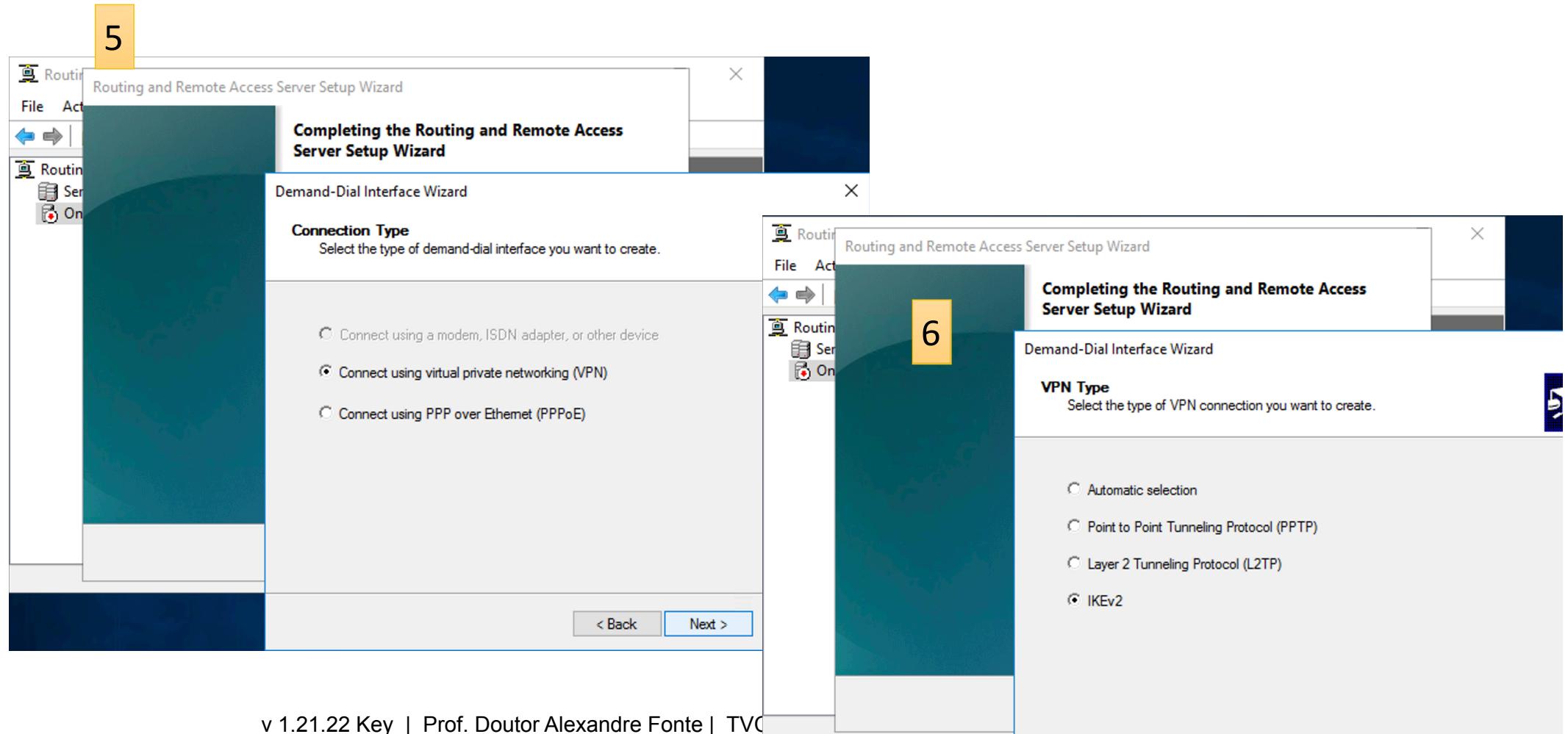


4 É preciso criarmos a interface VPN.



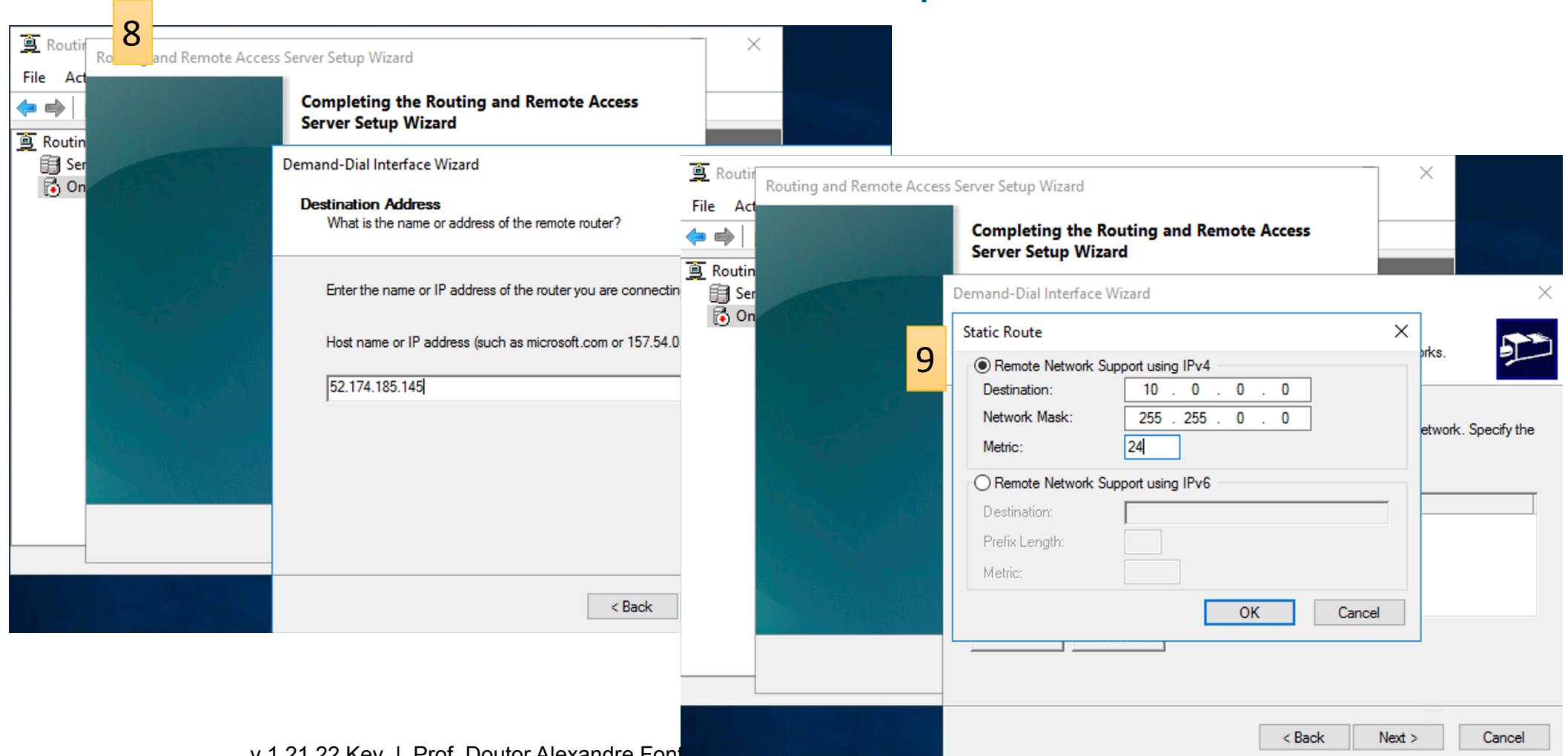
Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routing e Remote Access (RRA)
 - Indicar que a ligação é do tipo VPN e é usado o protocolo IKEv2



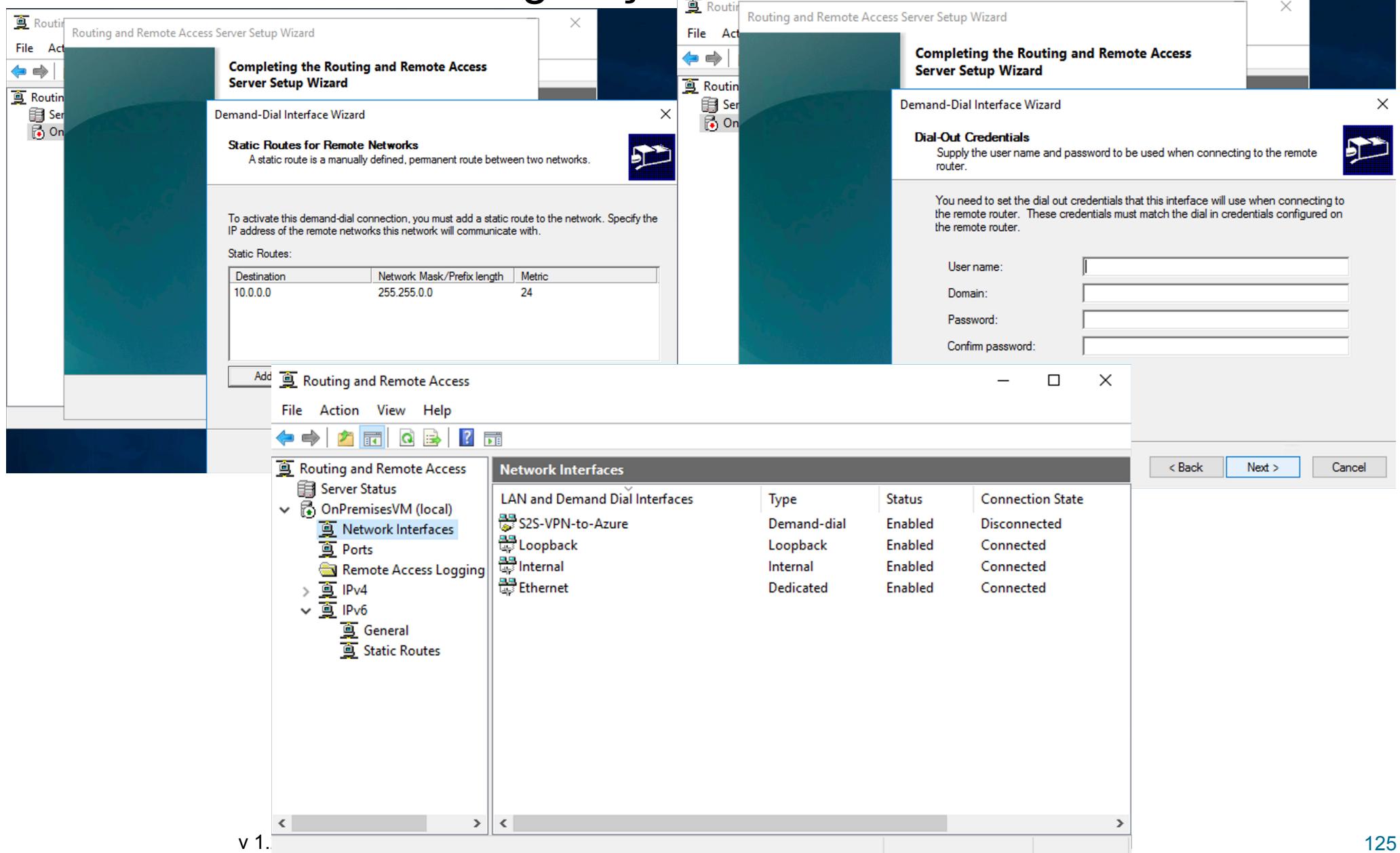
Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routing e Remote Access (RRA)
 - Indicar o IP público do VPN Gateway Azure e adicionar uma rota estática direcionada para a rede virtual Azure



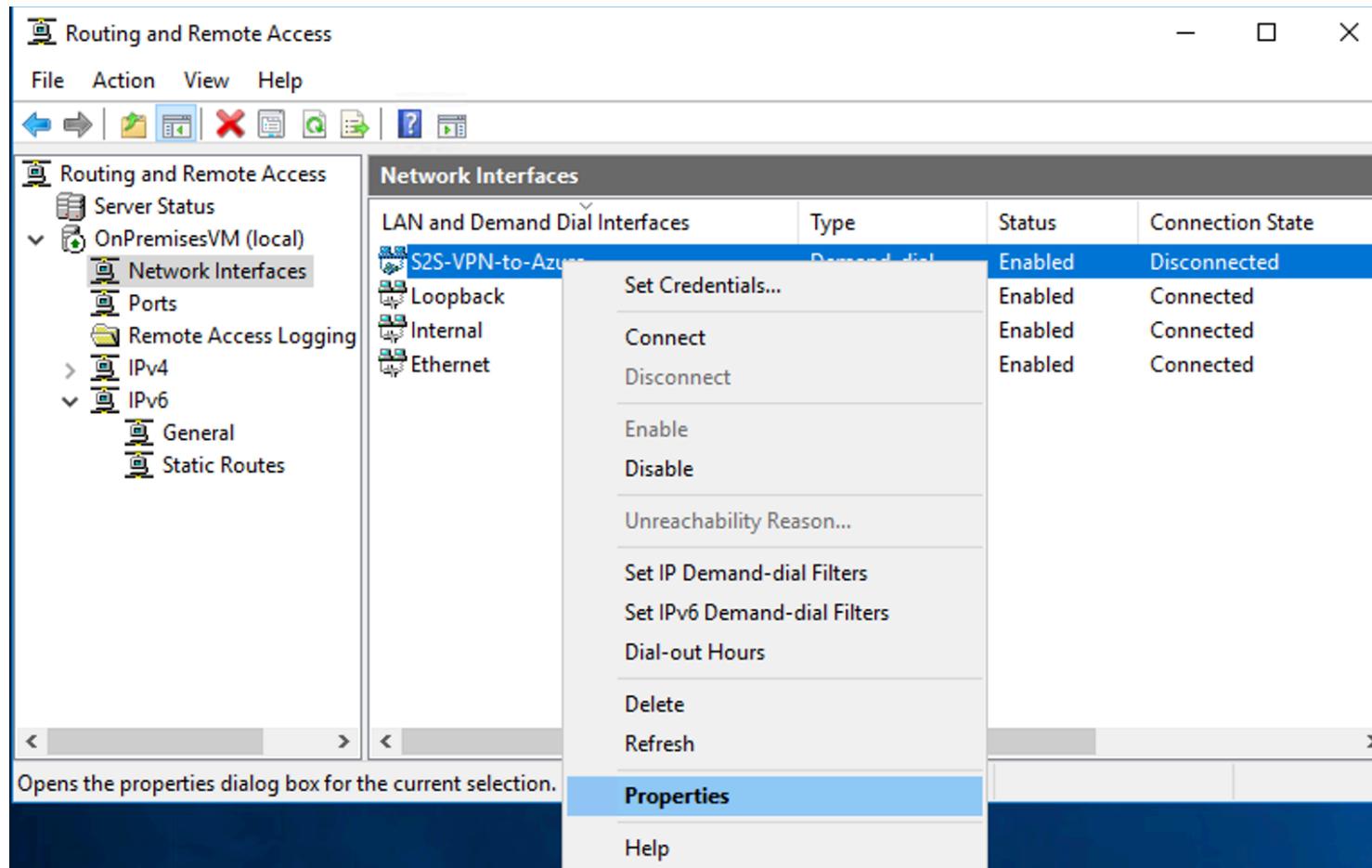
Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routina e Remote Access (RRA)



Azure VPN Gateway (Cont.)

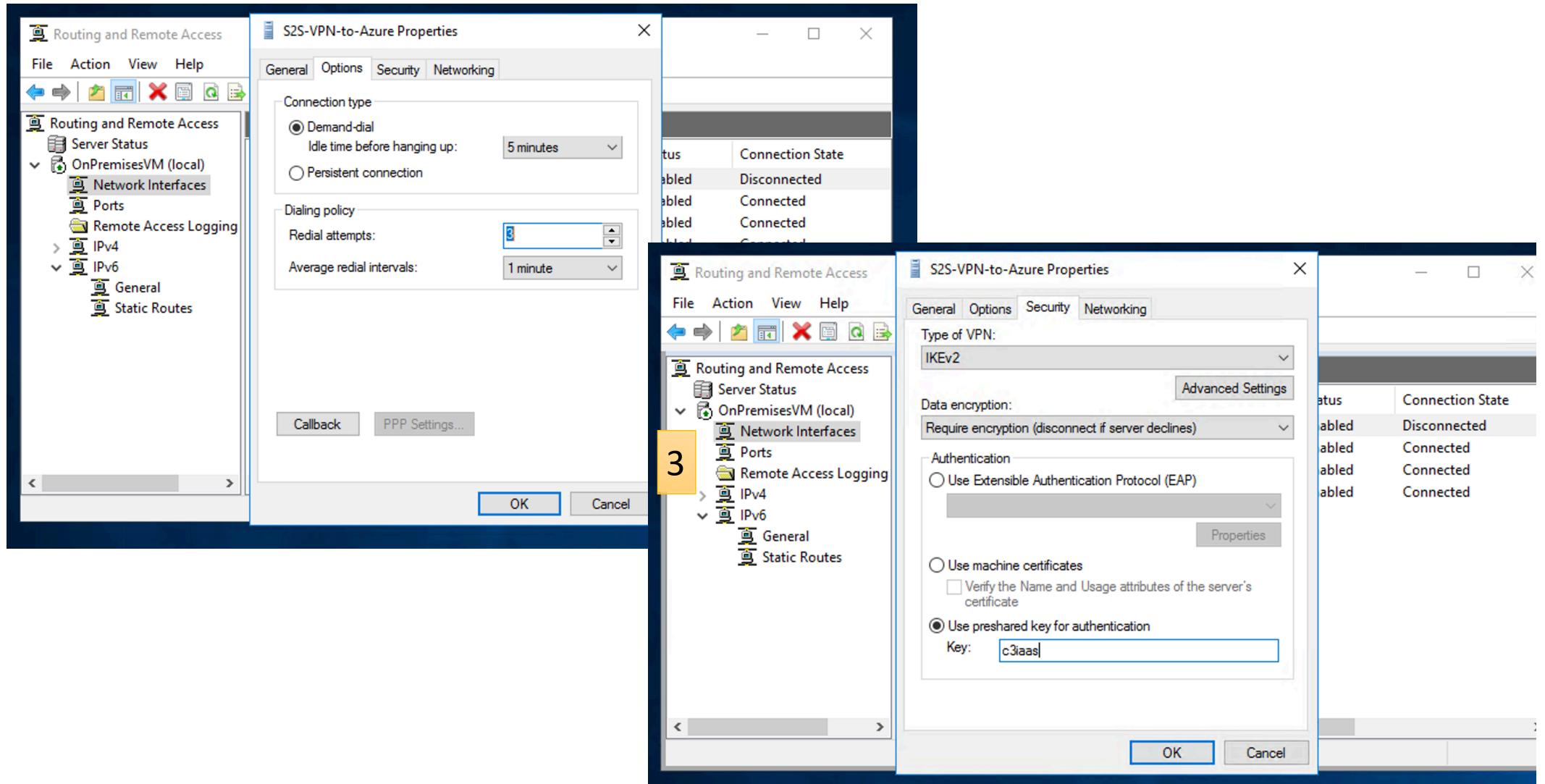
- #8.2: Realizar as configurações Routing e Remote Access (RRA)
 - Nas propriedade da interface, introduzir as credenciais de autenticação: c3iaas



Azure VPN Gateway (Cont.)

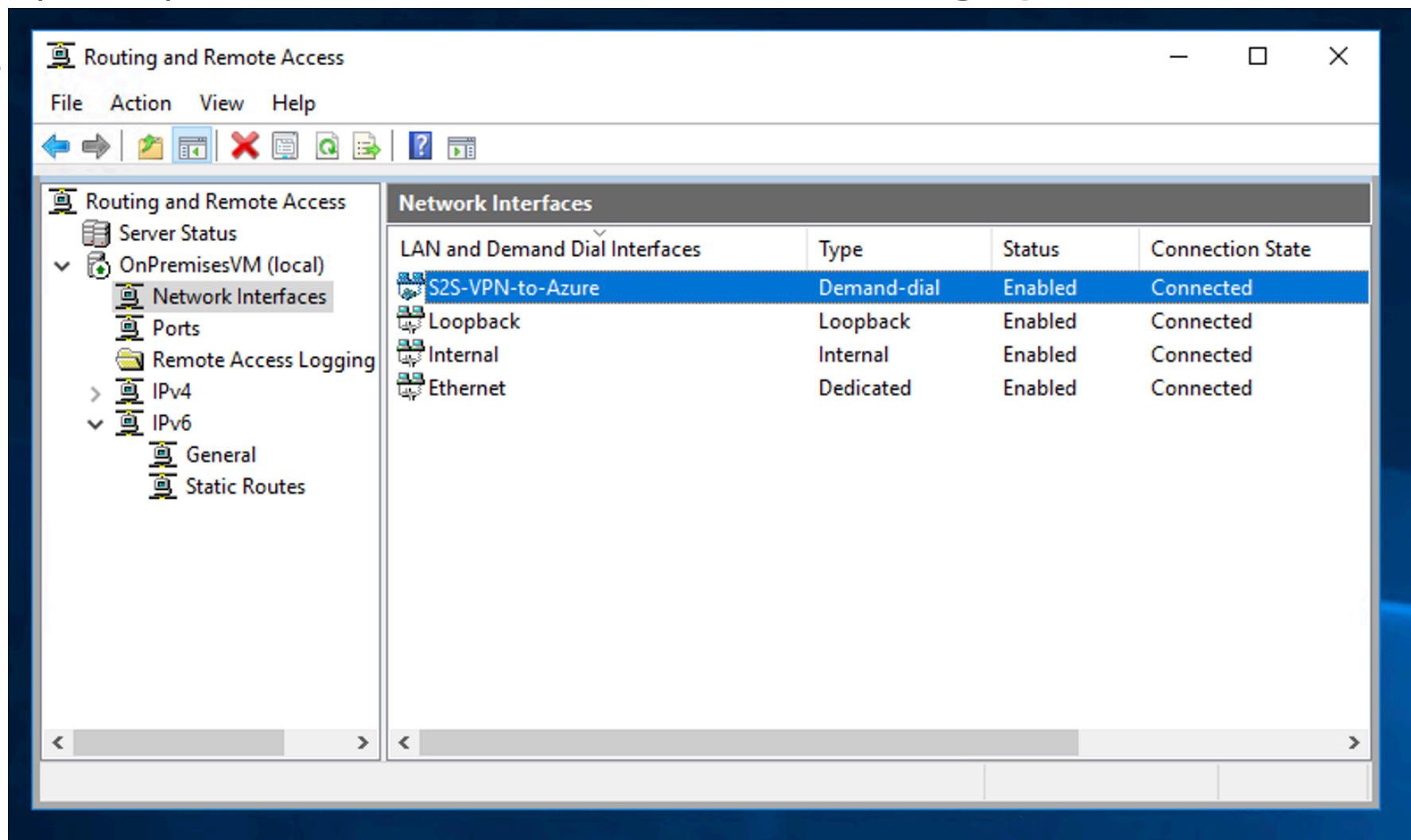
- #8.2: Realizar as configurações Routing e Remote Access (RRA)

2



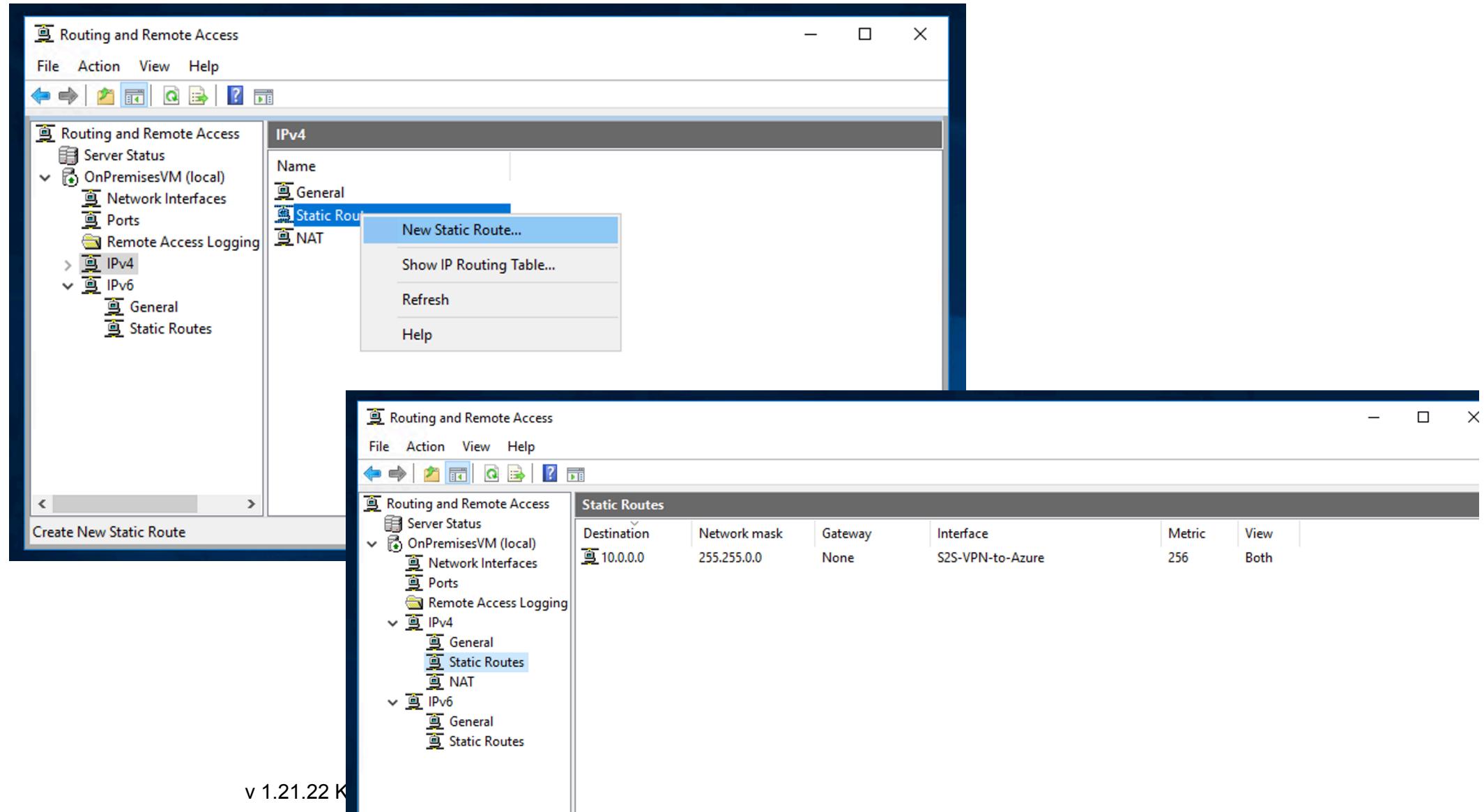
Azure VPN Gateway (Cont.)

- #8.2: Realizar as configurações Routing e Remote Access (RRA) - **Finalmente estabelecer a ligação S2S**



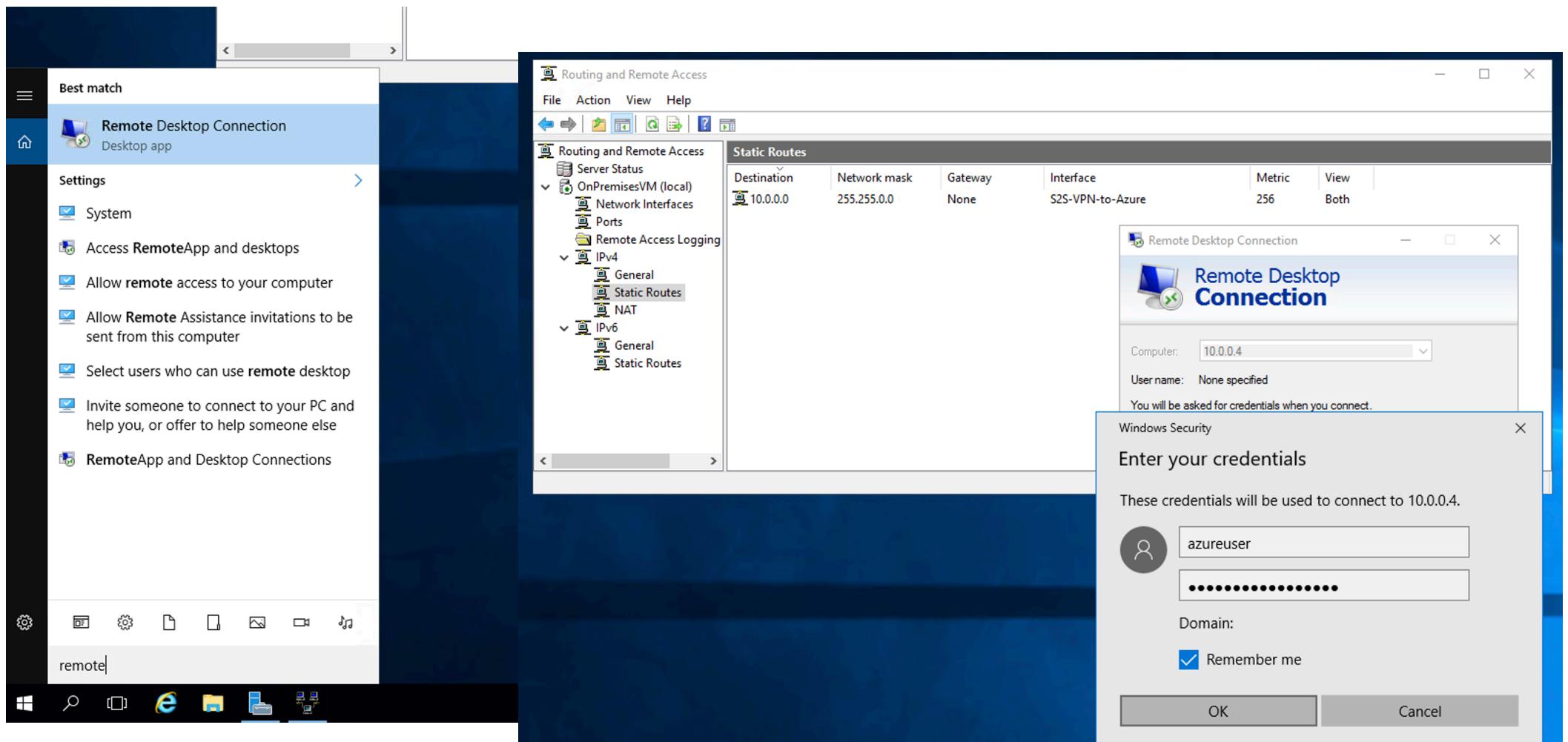
Azure VPN Gateway (Cont.)

- #9: Configuração de uma rota estática no Servidor para desviar o tráfego para a rede 10.0.0.0 através da VPN



Azure VPN Gateway (Cont.)

- #10: Realizar uma ligação RDP à myVM1 a partir do Servidor local (OnPremises)



Questões

