

# Redes do Azure

# Livro de receitas

**Segunda edição**

---

Receitas práticas para uma infraestrutura de rede segura,  
entrega global de aplicações e conectividade acessível no Azure

Mustafa Toroman



# Redes do Azure Livro de receitas

*Segunda edição*

Receitas práticas para uma infraestrutura  
de rede segura, entrega global de aplicações  
e conectividade acessível no Azure

Mustafa Toroman

Packt›

## **Redes do Azure Livro de receitas, Segunda edição**

Copyright © 2020 Packt Publishing

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida sob qualquer forma ou por qualquer meio sem a permissão prévia por escrito da editora, exceto no caso de breves citações incorporadas em artigos críticos ou comentários.

Não se poupou esforços na preparação deste livro para garantir a precisão das informações apresentadas. No entanto, as informações contidas neste livro são vendidas sem garantia, expressa ou implícita. O autor, a Packt Publishing e seus revendedores e distribuidores não serão responsabilizados por quaisquer danos causados ou supostamente causados de forma direta ou indireta por este livro.

A Packt Publishing empenha-se em fornecer informações de marca registrada sobre todas as empresas e produtos mencionados neste livro pelo uso adequado de capitais. No entanto, a Packt Publishing não garante a precisão dessas informações.

Autor: Mustafa Toroman

Revisores técnicos: Kapil Bansal, Rithin Skaria

Editores de gerenciamento: Mamta Yadav, Siddhant Jain

Editores de aquisições: Ben Renow-Clarke e Divya Mudaliar

Editor de produção: Deepak Chavan

Conselho editorial: Alex Patterson, Arijit Sarkar, Ben Renow-Clarke, Dominic Shakeshaft, Edward Doxey, Joanne Lovell e Vishal Bodwani

Primeira publicação: março de 2019

Publicado pela segunda vez: outubro de 2020

Referência de produção: 1281020

ISBN: 978-1-80056-375-9

Publicado pela Packt Publishing Ltd.

Livery Place, 35 Livery Street

Birmingham B3 2PB, UK

# Table of Contents

Prefácio	i
<b>Capítulo 1: Rede Virtual do Azure</b>	<b>1</b>
Requisitos técnicos .....	1
Criar uma rede virtual no portal do Azure .....	2
Preparação .....	2
Como fazer isso... .....	2
Como funciona... .....	6
Criar uma rede virtual com o PowerShell .....	6
Preparação .....	6
Como fazer isso... .....	7
Como funciona... .....	7
Adicionar uma sub-rede no portal do Azure .....	8
Preparação .....	8
Como fazer isso... .....	8
Como funciona... .....	11
Adicionar uma sub-rede com o PowerShell .....	11
Preparação .....	11
Como fazer isso... .....	12
Como funciona... .....	12
E mais... .....	12
Alterar o tamanho do espaço de endereço .....	13
Preparação .....	13
Como fazer isso... .....	13
Como funciona... .....	14

Alterar o tamanho de uma sub-rede .....	14
Preparação .....	14
Como fazer isso... .....	14
Como funciona... .....	16
<b>Capítulo 2: Redes de máquinas virtuais</b>	<b>17</b>
Requisitos técnicos .....	17
Criar VMs do Azure .....	18
Preparação .....	18
Como fazer isso... .....	18
Como funciona... .....	24
E mais... .....	25
Exibir configurações de rede da VM .....	25
Preparação .....	25
Como fazer isso... .....	25
Como funciona... .....	26
Criar uma nova NIC .....	26
Preparação .....	26
Como fazer isso... .....	27
Como funciona... .....	27
Anexar uma NIC a uma VM .....	28
Preparação .....	28
Como fazer isso... .....	28
Como funciona... .....	28
Desanexar uma NIC de uma VM .....	29
Preparação .....	29
Como fazer isso... .....	29
Como funciona... .....	29

<b>Capítulo 3: Grupos de segurança de rede</b>	<b>31</b>
<b>Requisitos técnicos .....</b>	<b>32</b>
<b>Criar um novo NSG no portal do Azure .....</b>	<b>32</b>
<b>Preparação .....</b>	<b>32</b>
<b>Como fazer isso... .....</b>	<b>33</b>
<b>Como funciona... .....</b>	<b>33</b>
<b>Criar um novo NSG com o PowerShell .....</b>	<b>34</b>
<b>Preparação .....</b>	<b>34</b>
<b>Como fazer isso... .....</b>	<b>34</b>
<b>Como funciona... .....</b>	<b>34</b>
<b>Criar uma nova regra de permissão em um NSG .....</b>	<b>35</b>
<b>Preparação .....</b>	<b>35</b>
<b>Como fazer isso... .....</b>	<b>35</b>
<b>Como funciona... .....</b>	<b>37</b>
<b>Criar uma nova regra de negação em um NSG .....</b>	<b>37</b>
<b>Preparação .....</b>	<b>37</b>
<b>Como fazer isso... .....</b>	<b>37</b>
<b>Como funciona... .....</b>	<b>39</b>
<b>Criar uma nova regra de NSG com o PowerShell .....</b>	<b>39</b>
<b>Preparação .....</b>	<b>39</b>
<b>Como fazer isso... .....</b>	<b>39</b>
<b>Como funciona... .....</b>	<b>39</b>
<b>E mais... .....</b>	<b>40</b>
<b>Atribuir um NSG a uma sub-rede .....</b>	<b>40</b>
<b>Preparação .....</b>	<b>40</b>
<b>Como fazer isso... .....</b>	<b>40</b>
<b>Como funciona... .....</b>	<b>42</b>

Atribuir um NSG a uma interface de rede .....	42
Preparação .....	42
Como fazer isso... .....	42
Como funciona... .....	44
Atribuir um NSG a uma sub-rede com o PowerShell .....	44
Preparação .....	44
Como fazer isso... .....	44
Como funciona... .....	44
Criar um Grupo de segurança de aplicativos (ASG) .....	45
Preparação .....	45
Como fazer isso... .....	45
Como funciona... .....	46
Associar um ASG a uma VM .....	46
Preparação .....	46
Como fazer isso... .....	46
Como funciona... .....	48
Criar regras com um NSG e um ASG .....	48
Preparação .....	48
Como fazer isso... .....	48
Como funciona... .....	49
<b>Capítulo 4: Gerenciar endereços IP</b>	<b>51</b>
Requisitos técnicos .....	52
Criar um novo endereço IP público no portal do Azure .....	52
Preparação .....	52
Como fazer isso... .....	53
Como funciona... .....	54

Criar um novo endereço IP público com o PowerShell .....	54
Preparação .....	54
Como fazer isso... .....	54
Como funciona... .....	54
Atribuir um endereço IP público .....	55
Preparação .....	55
Como fazer isso... .....	55
Como funciona... .....	56
Cancelar a atribuição de um endereço IP público .....	57
Preparação .....	57
Como fazer isso... .....	57
Como funciona... .....	58
Criar uma reserva para um endereço IP público .....	58
Preparação .....	58
Como fazer isso... .....	59
Como funciona... .....	59
Remover uma reserva para um endereço IP público .....	60
Preparação .....	60
Como fazer isso... .....	60
Como funciona... .....	61
Criar uma reserva para um endereço IP privado .....	61
Preparação .....	61
Como fazer isso... .....	61
Como funciona... .....	62
Alterar uma reserva para um endereço IP privado .....	63
Preparação .....	63
Como fazer isso... .....	63
Como funciona... .....	64

Remover uma reserva para um endereço IP privado .....	65
Preparação .....	65
Como fazer isso... .....	65
Como funciona... .....	66
Adicionar vários endereços IP a uma NIC .....	67
Preparação .....	67
Como fazer isso... .....	67
Como funciona... .....	69
Criar um prefixo de IP público .....	70
Como fazer isso... .....	70
Como funciona... .....	71
<b>Capítulo 5: Gateways de rede local e virtual</b>	<b>73</b>
Requisitos técnicos .....	74
Criar um gateway de rede local no portal do Azure .....	74
Preparação .....	74
Como fazer isso... .....	74
Como funciona... .....	75
Criar um gateway de rede local com o PowerShell .....	76
Preparação .....	76
Como fazer isso... .....	76
Como funciona... .....	76
Criar um gateway de rede virtual no portal do Azure .....	76
Preparação .....	76
Como fazer isso... .....	77
Como funciona... .....	78

Criar um gateway de rede virtual com o PowerShell .....	79
Preparação .....	79
Como fazer isso... .....	79
Como funciona... .....	80
Modificar as configurações do gateway de rede local .....	80
Preparação .....	80
Como fazer isso... .....	80
Como funciona... .....	81
<b>Capítulo 6: DNS e roteamento</b>	<b>83</b>
Requisitos técnicos .....	84
Criar uma zona DNS do Azure .....	84
Preparação .....	84
Como fazer isso... .....	84
Como funciona... .....	85
Criar uma zona privada DNS do Azure .....	86
Preparação .....	86
Como fazer isso... .....	86
Como funciona... .....	87
Integrar uma rede virtual a uma zona privada DNS .....	87
Preparação .....	87
Como fazer isso... .....	87
Como funciona... .....	88
Criar um novo conjunto de registros no DNS do Azure .....	88
Preparação .....	89
Como fazer isso... .....	89
Como funciona... .....	91

Criar uma tabela de rotas .....	91
Preparação .....	92
Como fazer isso... .....	92
Como funciona... .....	92
Alterar uma tabela de rotas .....	93
Preparação .....	93
Como fazer isso... .....	93
Como funciona... .....	93
Associar uma tabela de rotas a uma sub-rede .....	94
Preparação .....	94
Como fazer isso... .....	94
Como funciona... .....	96
Dissociar uma tabela de rotas de uma sub-rede .....	97
Preparação .....	97
Como fazer isso... .....	97
Como funciona... .....	99
Criar uma nova rota .....	100
Preparação .....	100
Como fazer isso... .....	100
Como funciona... .....	102
Alterar uma rota .....	102
Preparação .....	102
Como fazer isso... .....	102
Como funciona... .....	103
Excluir uma rota .....	103
Preparação .....	103
Como fazer isso... .....	104
Como funciona... .....	105

Requisitos técnicos .....	108
Criar um novo firewall .....	108
Preparação .....	108
Como fazer isso... .....	110
Como funciona... .....	110
Criar um novo firewall com o PowerShell .....	111
Como fazer isso... .....	111
Como funciona... .....	112
Configurar uma nova regra de permissão .....	112
Preparação .....	112
Como fazer isso... .....	112
Como funciona... .....	112
Configurar uma nova regra de negação .....	113
Preparação .....	113
Como fazer isso... .....	113
Como funciona... .....	113
Configurar uma tabela de rotas .....	113
Preparação .....	113
Como fazer isso... .....	114
Como funciona... .....	114
Habilitar logs de diagnóstico para o Firewall do Azure .....	114
Preparação .....	114
Como fazer isso... .....	114
Como funciona... .....	116

Configurar o Firewall do Azure no modo de túnel forçado .....	116
Preparação .....	116
Como fazer isso... .....	116
Como funciona... .....	120
Criar um grupo de IP .....	120
Preparação .....	120
Como fazer isso... .....	120
Como funciona... .....	121
Definir configurações de DNS do Firewall do Azure .....	121
Preparação .....	121
Como fazer isso... .....	121
Como funciona... .....	122
<b>Capítulo 8: Criar conexões híbridas</b>	<b>123</b>
Requisitos técnicos .....	124
Criar uma conexão site a site .....	124
Preparação .....	125
Como fazer isso... .....	125
Como funciona... .....	128
Fazer o download da configuração do dispositivo VPN do Azure .....	128
Preparação .....	128
Como fazer isso... .....	128
Como funciona... .....	130
Criar uma conexão ponto a site .....	130
Preparação .....	130
Como fazer isso... .....	133
Como funciona... .....	136

Criar uma conexão VNet a VNet .....	136
Preparação .....	136
Como fazer isso... .....	136
Como funciona... .....	139
Conectar VNets usando emparelhamento de rede .....	139
Preparação .....	140
Como fazer isso... .....	140
Como funciona... .....	143
<b>Capítulo 9: Conectar a recursos com segurança</b>	<b>145</b>
Requisitos técnicos .....	146
Criar uma instância do Azure Bastion .....	146
Preparação .....	147
Como fazer isso... .....	149
Como funciona... .....	150
Conectar a uma máquina virtual com o Azure Bastion .....	150
Preparação .....	150
Como fazer isso... .....	150
Como funciona... .....	151
Criar uma WAN virtual .....	151
Preparação .....	151
Como fazer isso... .....	152
Como funciona... .....	152
Criar um hub (na WAN Virtual) .....	153
Preparação .....	153
Como fazer isso... .....	153
Como funciona... .....	158

Adicionar uma conexão site a site (em um hub virtual) .....	158
Preparação .....	158
Como fazer isso... .....	159
Como funciona... .....	163
Adicionar uma conexão de rede virtual (em um hub virtual) .....	163
Preparação .....	163
Como fazer isso... .....	164
Como funciona... .....	166
Criar um ponto de extremidade do Link Privado .....	166
Preparação .....	166
Como fazer isso... .....	168
Como funciona... .....	170
Criar um serviço do Link Privado .....	170
Preparação .....	171
Como fazer isso... .....	171
Como funciona... .....	173
<b>Capítulo 10: Balanceadores de carga</b>	<b>175</b>
Requisitos técnicos .....	176
Criar um balanceador de carga interno .....	176
Preparação .....	176
Como fazer isso... .....	176
Como funciona... .....	178
Criar um balanceador de carga público .....	178
Preparação .....	178
Como fazer isso... .....	178
Como funciona... .....	180

Criar um pool de back-end .....	180
Preparação .....	180
Como fazer isso... .....	181
Como funciona... .....	184
Consulte também .....	184
Criar investigações de integridade .....	184
Preparação .....	184
Como fazer isso... .....	184
Como funciona... .....	186
Criar regras de balanceador de carga .....	186
Preparação .....	186
Como fazer isso... .....	186
Como funciona... .....	188
Criar regras de NAT de entrada .....	188
Preparação .....	188
Como fazer isso... .....	188
Como funciona... .....	190
Criar regras de saída explícitas .....	190
Preparação .....	190
Como fazer isso... .....	191
Como funciona... .....	193
<b>Capítulo 11: Gerenciador de Tráfego</b>	<b>195</b>
Requisitos técnicos .....	196
Criar um novo perfil do Gerenciador de Tráfego .....	196
Preparação .....	196
Como fazer isso... .....	196
Como funciona... .....	197

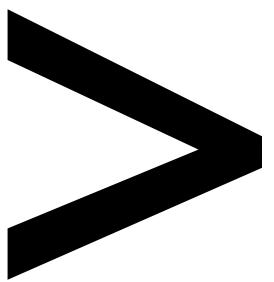
Adicionar um ponto de extremidade .....	197
Preparação .....	198
Como fazer isso... .....	198
Como funciona... .....	201
Configurar o tráfego distribuído .....	201
Preparação .....	201
Como fazer isso... .....	202
Como funciona... .....	203
Configurar o tráfego com base na prioridade .....	203
Preparação .....	203
Como fazer isso... .....	204
Como funciona... .....	204
Configurar o tráfego com base na localização geográfica .....	204
Preparação .....	205
Como fazer isso... .....	205
Como funciona... .....	205
Gerenciar pontos de extremidade .....	206
Preparação .....	206
Como fazer isso... .....	206
Como funciona... .....	207
Gerenciar perfis .....	207
Preparação .....	207
Como fazer isso... .....	208
Como funciona... .....	208
Configurar o Gerenciador de Tráfego com平衡adores de carga .....	209
Preparação .....	209
Como fazer isso... .....	209
Como funciona... .....	210

## **Capítulo 12: Gateway de aplicativo do Azure e WAF do Azure 211**

---

Requisitos técnicos .....	212
Criar um novo gateway de aplicativo .....	212
Preparação .....	212
Como fazer isso... .....	213
Como funciona... .....	221
Configurar os pools de back-end .....	221
Preparação .....	221
Como fazer isso... .....	222
Como funciona... .....	223
Configurar configurações de HTTP .....	224
Preparação .....	224
Como fazer isso... .....	224
Como funciona... .....	226
Configurar os ouvintes .....	226
Preparação .....	226
Como fazer isso... .....	226
Como funciona... .....	227
Regras de configuração .....	228
Preparação .....	228
Como fazer isso... .....	228
Como funciona... .....	229
Configurar investigações .....	230
Preparação .....	230
Como fazer isso... .....	230
Como funciona... .....	231

Configurar um Firewall de Aplicativo Web (WAF) .....	231
Preparação .....	232
Como fazer isso... .....	232
Como funciona... .....	234
Personalizar regras de WAF .....	234
Preparação .....	234
Como fazer isso... .....	234
Como funciona... .....	236
Criar uma política de WAF .....	236
Preparação .....	236
Como fazer isso... .....	236
Como funciona... .....	241
<b>Capítulo 13: Azure Front Door e CDN do Azure</b>	<b>243</b>
Requisitos técnicos .....	243
Criar uma instância do Azure Front Door .....	244
Preparação .....	244
Como fazer isso... .....	244
Como funciona... .....	252
Criar um perfil da CDN do Azure .....	254
Preparação .....	254
Como fazer isso... .....	254
Como funciona... .....	255
<b>Índice</b>	<b>257</b>



# Prefácio

## Sobre

Esta seção apresenta brevemente o autor e os revisores técnicos, a cobertura deste livro de receitas, as habilidades técnicas de que você precisará para começar e hardware e software necessários para completar todas as receitas.

## Sobre o livro de receitas Redes do Azure, Segunda edição

Os serviços de rede do Azure permitem que as organizações gerenciem as redes de forma eficaz. O Azure abre o caminho para uma empresa alcançar uma performance confiável e uma conectividade segura.

O livro *de receitas Redes do Azure, Segunda edição* começa com uma introdução às redes do Azure, abrangendo passos básicos, como criar redes virtuais do Azure, criar espaços de endereço e criar sub-redes. Você prosseguirá para aprender a criar e gerenciar grupos de segurança de rede, grupos de segurança de aplicativos e endereços IP no Azure.

À medida que você avançar, explorará vários aspectos, como conexões de rede a virtual, ponto a site e site a site, DNS e roteamento,平衡adores de carga e Gerenciador de Tráfego. Este livro de receitas abrange todos os aspectos e funções que você precisa conhecer, fornecendo receitas práticas para ajudá-lo a passar de uma compreensão básica das práticas de rede de nuvem para a capacidade de planejar, implementar e proteger sua infraestrutura de rede com o Azure.

Este livro de receitas não apenas ajudará você a escalar seu ambiente atual, como também fornecerá instruções sobre como monitorar, diagnosticar e garantir uma conectividade segura. Depois de aprender a criar um ambiente robusto, você obterá insights significativos de receitas sobre práticas recomendadas.

No final deste livro de receitas, você terá experiência prática suficiente para fornecer soluções econômicas para facilitar uma conectividade eficiente em sua organização.

## Sobre o autor

**Mustafa Toroman** é arquiteto de soluções da Authority Partners. Com anos de experiência na criação e no monitoramento de soluções de infraestrutura, ultimamente, ele se concentra em criar novas soluções na nuvem e migrar as soluções existentes para a nuvem. Com muito interesse em processos de DevOps, ele também é entusiasta de infraestrutura como código. Mustafa tem mais de 50 certificações da Microsoft e é um instrutor certificado pela Microsoft desde 2012. Ele faz palestras em conferências internacionais sobre tecnologias de nuvem com frequência e recebeu o prêmio de MVP do Azure nos últimos cinco anos seguidos.

Mustafa também é o autor de *Administração de nuvem prática no Azure* e co-autor de *Aprender Node.js com o Azure* e *Dominando a segurança do Azure*, todos publicados pela Packt.

## Sobre os revisores

**Kapil Bansal** é engenheiro de DevOps líder de inteligência de mercado global do S&P, na Índia. Ele tem mais de 12 anos de experiência na indústria de TI, trabalhou em computação na nuvem do Azure (PaaS, IaaS e SaaS), Azure Stack, DevSecOps, Kubernetes, Terraform, Office 365, SharePoint, gerenciamento de lançamento, gerenciamento de ciclo de vida de aplicações (ALM), biblioteca de infraestrutura de tecnologia da informação (ITIL) e Six Sigma. Ele trabalha com empresas como IBM India Pvt Ltd, HCL Technologies, NIIT Technologies, Encore Capital Group, e Xavient Software Solutions, Noida e atende clientes dos Estados Unidos, do Reino Unido e da África, como T-Mobile, World Bank Group, H&M, WBMI, Encore Capital e Bharti Airtel (Índia e África). Kapil também revisou o livro de receitas *Práticas do Kubernetes no Azure e redes do Azure* publicado pela Packt. Além disso, ele contribuiu em *IaaS prática do Microsoft Azure* e *Iniciando sites de comunicação do SharePoint* publicados pela Apress.

**Rithin Skaria** é um difusor de open source com mais de 7 anos de experiência no gerenciamento de workloads de Open Source no Azure, na AWS e no OpenStack. Atualmente, ele trabalha na Microsoft e faz parte de várias atividades da comunidade de Open Source realizadas na empresa. Ele é instrutor certificado da Microsoft, engenheiro e administrador da Linux Foundation, administrador e desenvolvedor de aplicações no Kubernetes e administrador certificado do OpenStack. Quando se trata do Azure, ele tem quatro certificações, incluindo para arquitetura de soluções, administração do Azure, DevOps e segurança, além de ser certificado em administração do Microsoft 365. Ele desempenhou uma função vital em várias implantações de Open Source e na administração e migração desses workloads para a nuvem. Ele é co-autor de *Administração do Linux no Azure e Azure para arquitetos – Terceira edição* publicados pela Packt.

## Objetivos de aprendizagem

Até o final deste livro de receitas, você será capaz de:

- Crie serviços de rede do Azure.
- Criar e trabalhar em conexões híbridas.
- Configurar e gerenciar os serviços de rede do Azure.
- Projetar soluções de rede de alta disponibilidade no Azure.
- Monitorar e solucionar recursos de rede do Azure.
- Usar diferentes métodos para conectar redes locais a redes virtuais do Azure.
- Usar diferentes métodos para proteger as redes.

## Público-alvo

Este livro de receitas destina-se a arquitetos de nuvem, provedores de soluções de nuvem ou quaisquer stakeholders lidando com redes do Azure. A familiaridade básica com o Azure será um diferencial.

## Abordagem

O livro de receitas *Redes do Azure, Segunda edição* consiste em uma combinação ideal entre teoria e treinamento prático para ajudá-lo a se preparar para os desafios de conectividade do mundo real que as empresas enfrentam.

## Aproveite ao máximo este livro

Este livro pressupõe que você tenha um nível básico de conhecimento sobre a computação na nuvem e o Azure. Para usar esse livro, tudo o que você precisa é de uma assinatura válida do Azure e conectividade com a Internet. Um computador Windows 10 com 4 GB de RAM é suficiente para usar o PowerShell.

## Requisitos de hardware

O portal do Azure é um console baseado na Web que funciona em todos os navegadores modernos para desktops, tablets e dispositivos móveis. Para usar o portal do Azure, você deve ter o JavaScript habilitado no seu navegador.

## Requisitos de software

Recomendamos usar o navegador mais recente que é compatível com seu sistema operacional. Os seguintes navegadores são compatíveis:

- Microsoft Edge (versão mais recente)
- Internet Explorer 11
- Safari (versão mais recente, somente Mac)
- Chrome (versão mais recente)
- Firefox (versão mais recente)

## Convenções

Palavras de código em textos, nomes de pastas, nomes de arquivos, extensões de arquivos, nomes de caminhos, simulações de URLs e entrada do usuário são mostrados da seguinte maneira:

"Além disso, podemos usar interruptores adicionais, como **-SKU** para selecionar **Básica** ou **Padrão**, **-IPAddressVersion** para escolher entre IPv4 e IPv6 e **-DomainNameLabel** para especificar o rótulo DNS."

Um bloco de código é definido da seguinte forma:

```
$VirtualNetwork = Get-AzVirtualNetwork -Name 'Packt-Script' '  
-ResourceGroupName 'Packt-Networking-Script'  
Add-AzVirtualNetworkSubnetConfig -Name BackEnd '  
-AddressPrefix 10.11.1.0/24 '  
-VirtualNetwork $VirtualNetwork  
$VirtualNetwork | Set-AzVirtualNetwork
```

## Fazer o download dos recursos

O pacote de código para este livro está hospedado no GitHub em <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition>. Você pode encontrar os arquivos usados neste livro, que são mencionados em instâncias relevantes. Também temos outros pacotes de código em nosso rico catálogo de manuais e vídeos disponíveis em <https://github.com/PacktPublishing/>. Dê uma olhada neles!



# 1

# Rede Virtual do Azure

Neste primeiro capítulo, aprenderemos sobre os fundamentos da rede do Azure, incluindo a criação de redes virtuais do Azure, a criação de espaços de endereço e sub-redes. Isso estabelecerá a base para todas as futuras receitas que abordaremos neste capítulo.

Abordaremos as seguintes receitas neste capítulo:

- Criar uma rede virtual no portal do Azure
- Criar uma rede virtual com o PowerShell
- Adicionar uma sub-rede no portal do Azure
- Adicionar uma sub-rede com o PowerShell
- Alterar o tamanho do espaço de endereço
- Alterar o tamanho de uma sub-rede

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Azure PowerShell

Os exemplos de código podem ser encontrados no

[https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/  
tree/master/Chapter01](https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter01).

## Criar uma rede virtual no portal do Azure

A Rede Virtual do Azure representa sua rede local na nuvem. Ela permite que outros recursos do Azure se comuniquem por meio de uma rede privada segura sem expor pontos de extremidade na Internet.

### Preparação

Antes de iniciar, abra um navegador da Web e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova rede virtual usando o portal do Azure, siga as seguintes etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Rede virtual** em **Rede** (ou pesquise **rede virtual** na barra de pesquisa). Um novo painel abrirá, onde precisamos fornecer informações para a rede virtual. Primeiro, selecione a opção **Assinatura** que queremos usar e a opção **Grupo de recursos** onde a rede virtual será implantada. Em seguida, inclua um nome e selecione uma região (do datacenter do Azure) onde a rede virtual será implantada. Um exemplo é mostrado na Figura 1.1:

### Create virtual network

The screenshot shows the 'Create virtual network' wizard in the Azure portal. The 'Basics' tab is active. In the 'Project details' section, the 'Subscription' dropdown is set to 'Microsoft Azure Sponsorship'. The 'Resource group' dropdown is set to '(New) Packt-Networking-Portal', with an option to 'Create new'. In the 'Instance details' section, the 'Name' field is filled with 'Packt-Portal' and has a green checkmark. The 'Region' dropdown is set to '((Europe) West Europe)'.

Figura 1.1: Criar uma rede virtual do Azure

2. No próximo painel, primeiro precisamos definir o espaço de endereço e definir os valores **Nome da sub-rede** e **Intervalo de endereços da sub-rede** para a primeira sub-rede. Depois que o espaço de endereço for definido, conforme mostrado na Figura 1.2, receberemos uma mensagem informando: **Esta rede virtual não tem nenhuma sub-rede**. Portanto, precisamos selecionar a opção **Adicionar sub-rede**:

## 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

10.10.0.0/16 10.10.0.0 - 10.10.255.255 (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  Remove subnet

Subnet name	Subnet address range
This virtual network doesn't have any subnets.	

 This virtual network doesn't have any subnets.

Figura 1.2: Configurar uma sub-rede e um espaço de endereço de rede virtual

3. No painel **Adicionar sub-rede**, precisamos definir **Nome da sub-rede** e **Intervalo de endereço da sub-rede**. Opcionalmente, podemos adicionar pontos de extremidade de serviço que desejamos conectar à rede virtual. Os pontos de extremidade de serviço permitem conectar aos serviços do Azure de forma segura, por meio da infraestrutura de backbone do Azure, sem precisar de um endereço IP público. Um exemplo é mostrado na Figura 1.3:

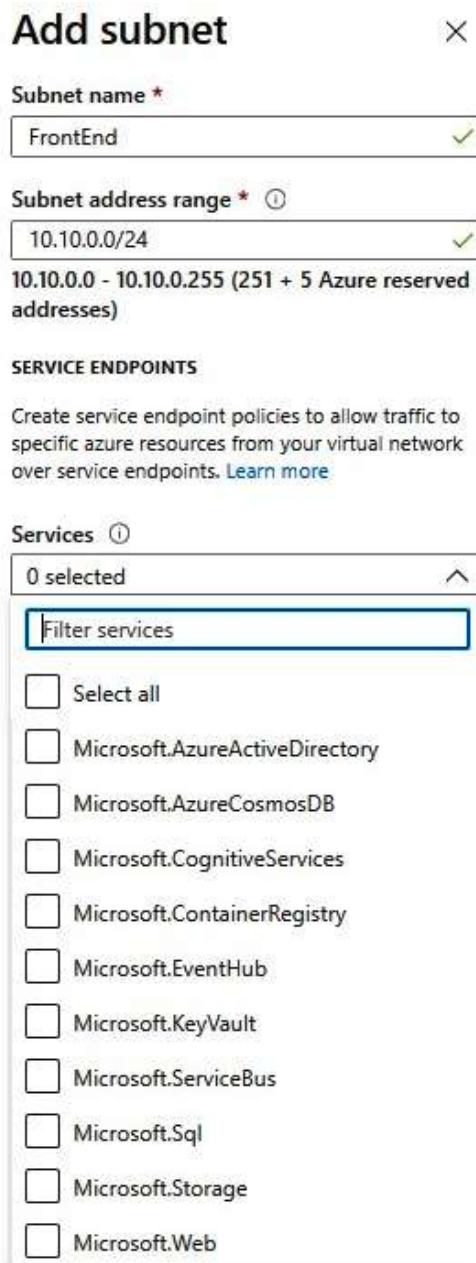


Figura 1.3: Adicionar uma sub-rede

4. Depois que adicionamos a primeira sub-rede, no nosso caso, o **Front-end**, podemos adicionar mais sub-redes à rede virtual ou seguir para a seção de **Segurança**, conforme mostrado na Figura 1.4:

## Create virtual network

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**

10.10.0.0/16 10.10.0.0 - 10.10.255.255 (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

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> FrontEnd	10.10.0.0/24

Figura 1.4: Adicionar a sub-rede de front-end

5. Na seção **Segurança**, podemos escolher se desejamos habilitar **Bastion host**, **Proteção contra DDoS** e **Firewall**. Se alguma dessas opções estiver habilitada, precisaremos fornecer informações adicionais para esse serviço. Depois, opcionalmente, podemos adicionar tags ou pular essa etapa e criar o serviço. Um exemplo é mostrado na Figura 1.5:

## Create virtual network

Basics IP Addresses Security Tags Review + create

BastionHost ⓘ  Enabled  Disabled

DDoS protection ⓘ  Standard  Basic

Firewall ⓘ  Enabled  Disabled

Figura 1.5: Alternar opções de segurança

6. A criação de uma rede virtual geralmente não leva muito tempo e deve ser concluída em menos de dois minutos. Após a conclusão da implantação, podemos começar a usar a rede virtual.

## Como funciona...

Implantamos redes virtuais no **Grupo de recursos em Assinatura** no datacenter do Azure que escolhermos. **Região** e **Assinatura** são parâmetros importantes. Só poderemos anexar recursos do Azure a essa rede virtual se eles estiverem na mesma assinatura e região que o datacenter do Azure. A opção Espaço de endereço define o número de endereços IP que estarão disponíveis para nossa rede. Ele usa o formato **Roteamento Entre Domínios Sem Classe (CIDR)** e o maior intervalo que podemos escolher é **/8**. No portal, é necessário criar uma sub-rede inicial e definir o intervalo de endereços da sub-rede. A menor sub-rede permitida é **/29** e a maior é **/8** (no entanto, não pode ser maior que o intervalo da rede virtual). Para referência, o intervalo **10.0.0.0/8** (em formato CIDR) criará o intervalo de endereços dos endereços IP **167772115** (de **10.0.0.0** a **10.255.255.255**) e **10.0.0.0/29** criará o intervalo de **8** endereços IP (de **10.0.0.0** a **10.0.0.7**).

## Criar uma rede virtual com o PowerShell

O PowerShell é um shell de linha de comando e uma linguagem de script baseada no .NET Framework. Ele é frequentemente usado por administradores de sistema para automatizar tarefas e gerenciar sistemas operacionais. O Azure PowerShell **Az** é um módulo do PowerShell que nos permite automatizar e gerenciar recursos do Azure. O **Az** também é frequentemente usado para automatizar tarefas de implantação e também pode ser usado para implantar uma nova rede virtual do Azure

## Preparação

Antes de começarmos, precisamos garantir que temos os módulos **Az** mais recentes instalados. Para instalar os módulos **Az**, precisamos executar este comando no console do PowerShell:

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

Para obter mais informações, você pode acessar <https://docs.microsoft.com/powershell/azure/install-az-ps?view=azps-4.5.0>.

Antes de começarmos, precisamos nos conectar à assinatura do Azure em um console do PowerShell. Este é o comando para se fazer isso:

```
Connect-AzAccount
```

Isso abrirá uma janela pop-up onde deveremos inserir as credenciais da assinatura do Azure.

Depois, deveremos criar um grupo de recursos onde nossa rede virtual será implantada:

```
New-AzResourceGroup -name 'Packt-Networking-Script' -Location 'westeurope'
```

A saída deve ser semelhante à mostrada na Figura 1.6:

```
ResourceGroupName : Packt-Networking-Script
Location         : westeurope
ProvisioningState : Succeeded
Tags             :
ResourceId       : /subscriptions/.../resourceGroups/Packt-Networking-Script
```

Figura 1.6: Conectar a uma assinatura do Azure no PowerShell

## Como fazer isso...

A implantação de uma rede virtual do Azure é feita em um único script. É necessário definir os parâmetros para o nome, grupo de recursos, o local e o intervalo de endereços. Veja um script de exemplo:

```
New-AzVirtualNetwork -ResourceGroupName 'Packt-Networking-Script' -Location
'westeurope' -Name 'Packt-Script' -AddressPrefix 10.11.0.0/16
```

Você deverá receber a seguinte saída:

```
Name          : Packt-Script
ResourceGroupName : Packt-Networking-Script
Location       : westeurope
Id            : /subscriptions/...
Etag          : W/"d0c9a5a2-d133-479e-a42d-5e53365d200b"
ResourceGuid   : 2f9b5c37 fcfc 4530 9f9c 9ff011d94f8d
ProvisioningState : Succeeded
Tags          :
AddressSpace  : {
    "AddressPrefixes": [
        "10.11.0.0/16"
    ]
}
DhcpOptions   : {}
Subnets       : []
VirtualNetworkPeerings : []
EnableDdosProtection : false
DdosProtectionPlan : null
```

Figura 1.7: Implantar uma rede virtual do Azure usando um script

## Como funciona...

A diferença entre implantar uma rede virtual no portal e usar o PowerShell é que não há necessidade de definir nenhuma sub-rede no PowerShell. A sub-rede é implantada em um comando separado que poderá ser executado quando você estiver implantando uma rede virtual ou posteriormente. Veremos esse comando na receita *Adicionar uma sub-rede com o PowerShell* mais adiante neste capítulo.

## Adicionar uma sub-rede no portal do Azure

Além de adicionar sub-redes ao criar uma rede virtual, podemos adicionar outras sub-redes à nossa rede a qualquer momento.

### Preparação

Antes de iniciar, abra um navegador da Web e accese o portal do Azure em <https://portal.azure.com>. Nele, localize a rede virtual criada anteriormente.

### Como fazer isso...

Para adicionar uma sub-rede a uma rede virtual usando o portal do Azure, devemos seguir estas etapas:

1. No painel **Rede virtual**, accese a seção **Sub-redes**.
2. Selecione a opção **Adicionar sub-rede**.
3. Um novo painel será aberto. Devemos fornecer as informações da sub-rede, incluindo o valor **Nome** e o valor **Intervalo de endereços** no formato CIDR. O valor **Intervalo de endereços** deve estar no limite de intervalos do intervalo de endereços da rede virtual e não pode sobrepor o intervalo de endereços de outras sub-redes na rede virtual. Opcionalmente, podemos adicionar informações para **Grupo de segurança**, **Tabela de rotas**, **Pontos de extremidade de serviço** e **Delegação de sub-rede**. Estas opções serão abordadas em receitas posteriores:

**Add subnet** X

Packt-Portal

**Name \***  
BackEnd ✓

**Address range (CIDR block) \***  ⓘ  
10.10.1.0/24 ✓  
10.10.1.0 - 10.10.1.255 (251 + 5 Azure reserved addresses)

**NAT gateway**  ⓘ  
None ▼

Add IPv6 address space

**Network security group**  
None ▼

**Route table**  
None ▼

**Service endpoints**

**Services**  ⓘ  
0 selected ▼

**Subnet delegation**

**Delegate subnet to a service**  ⓘ  
None ▼

Figura 1.8: Adicionar o intervalo de endereços

4. Também podemos adicionar uma sub-rede de gateway no mesmo painel. Para adicionar uma sub-rede de gateway, selecione a opção **Sub-rede de gateway**.

Para uma sub-rede de gateway, o único parâmetro que dever ser definido é **Intervalo de endereços**. As mesmas regras se aplicam à adição de uma sub-rede regular. Dessa vez, não é necessário fornecer um nome, pois ele já está definido. Você pode adicionar somente uma sub-rede de gateway por rede virtual. Pontos de extremidade de serviço não são permitidos na sub-rede de gateway:

**Add subnet** X

Packt-Portal

Name  
GatewaySubnet

Address range (CIDR block) \* ⓘ  
10.10.2.0/24 ✓  
10.10.2.0 - 10.10.2.255 (251 + 5 Azure reserved addresses)

NAT gateway ⓘ  
None ▼  
 Add IPv6 address space

Network security group  
None ▼

Route table  
None ▼

Service endpoints

Services ⓘ  
0 selected ▼

Subnet delegation

Delegate subnet to a service ⓘ  
None ▼

Figura 1.9: Adicionar uma sub-rede de gateway para uma rede virtual

5. Depois que as sub-redes forem adicionadas, poderemos ver as sub-redes recém-criadas no painel **Sub-redes** na rede virtual:

Name	IPv4
FrontEnd	10.10.0.0/24 (251 available)
BackEnd	10.10.1.0/24 (251 available)
GatewaySubnet	10.10.2.0/24 (251 available)

Figura 1.10: Exibir sub-redes recém-criadas no painel Sub-redes

## Como funciona...

Uma única rede virtual pode ter várias sub-redes definidas. As sub-redes não podem se sobrepor e devem estar no intervalo de endereços da rede virtual. Para cada sub-rede, quatro endereços IP são salvos para o gerenciamento do Azure e não podem ser usados. Dependendo das configurações de rede, podemos definir as regras de comunicação entre as sub-redes na rede virtual. Uma sub-rede de gateway é usada para conexões da **Rede Virtual Privada (VPN)**, e isso será abordado mais adiante no livro de receitas.

Agora, vamos aprender a adicionar uma sub-rede usando o PowerShell.

## Adicionar uma sub-rede com o PowerShell

Ao criar uma rede virtual do Azure com o PowerShell, uma sub-rede não é criada na mesma etapa e requer que um comando adicional seja executado separadamente.

### Preparação

Antes de criar uma sub-rede, precisamos coletar informações sobre a rede virtual à qual a nova sub-rede será associada. Os parâmetros que devem ser fornecidos são o nome da rede virtual e o grupo de recursos no qual a rede virtual está localizada:

```
$VirtualNetwork = Get-AzVirtualNetwork -Name 'Packt-Script'  
-ResourceGroupName 'Packt-Networking-Script'
```

## Como fazer isso...

1. Para adicionar uma sub-rede à rede virtual usando o PowerShell, precisamos executar um comando e fornecer o nome e o prefixo de endereço. Novamente, o prefixo de endereço deve estar no formato CIDR:

```
Add-AzVirtualNetworkSubnetConfig -Name FrontEnd -AddressPrefix 10.11.0.0/24  
-VirtualNetwork $VirtualNetwork
```

2. Devemos confirmar essas alterações executando o seguinte comando:

```
$VirtualNetwork | Set-AzVirtualNetwork
```

3. Podemos adicionar uma sub-rede adicional executando todos os comandos em uma única etapa, da seguinte maneira:

```
$VirtualNetwork = Get-AzVirtualNetwork -Name 'Packt-Script'  
-ResourceGroupName 'Packt-Networking-Script'  
Add-AzVirtualNetworkSubnetConfig -Name BackEnd -AddressPrefix 10.11.1.0/24  
-VirtualNetwork $VirtualNetwork  
$VirtualNetwork | Set-AzVirtualNetwork
```

## Como funciona...

A sub-rede é criada e adicionada à rede virtual, mas devemos confirmar as alterações para que possam entrar em vigor. Quando se trata de tamanho, todas as regras para criar ou adicionar um sub-rede usando o portal do Azure também se aplicam nesse caso. A sub-rede deve estar dentro do espaço de endereço da rede virtual e não pode sobrepor outras sub-redes na rede virtual. A menor sub-rede permitida é /29 e a maior é /8, contanto que o valor esteja no espaço de endereço da rede virtual. Por exemplo, se você estiver criando uma rede /16, o maior valor para a sub-rede será somente /16, pois não podemos incluir uma sub-rede /8 em um espaço de endereço /16.

## E mais...

Podemos criar e adicionar várias sub-redes com um único script, da seguinte forma:

```
$VirtualNetwork = Get-AzVirtualNetwork -Name 'Packt-Script'  
-ResourceGroupName 'Packt-Networking-Script'  
  
$FrontEnd = Add-AzVirtualNetworkSubnetConfig -Name FrontEnd -AddressPrefix  
10.11.0.0/24 -VirtualNetwork $VirtualNetwork  
  
$BackEnd = Add-AzVirtualNetworkSubnetConfig -Name BackEnd -AddressPrefix  
10.11.1.0/24 -VirtualNetwork $VirtualNetwork  
  
$VirtualNetwork | Set-AzVirtualNetwork
```

## Alterar o tamanho do espaço de endereço

Depois que o espaço de endereço inicial é definido durante a criação de uma rede virtual, ainda podemos alterar o tamanho do espaço de endereço, conforme necessário. Podemos aumentar ou diminuir o tamanho do espaço de endereço ou alterar totalmente o espaço de endereço usando um novo intervalo de endereços.

### Preparação

Antes de iniciar, abra um navegador da Web e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para alterar o tamanho do espaço de endereço para uma rede virtual usando o portal do Azure, devemos seguir as seguintes etapas:

1. No painel **Rede virtual**, localize **Espaço de endereço** em **Configurações**.
2. Depois disso, clique em **Espaço de endereço** e altere o valor para o intervalo desejado. Um exemplo é mostrado na Figura 1.11:

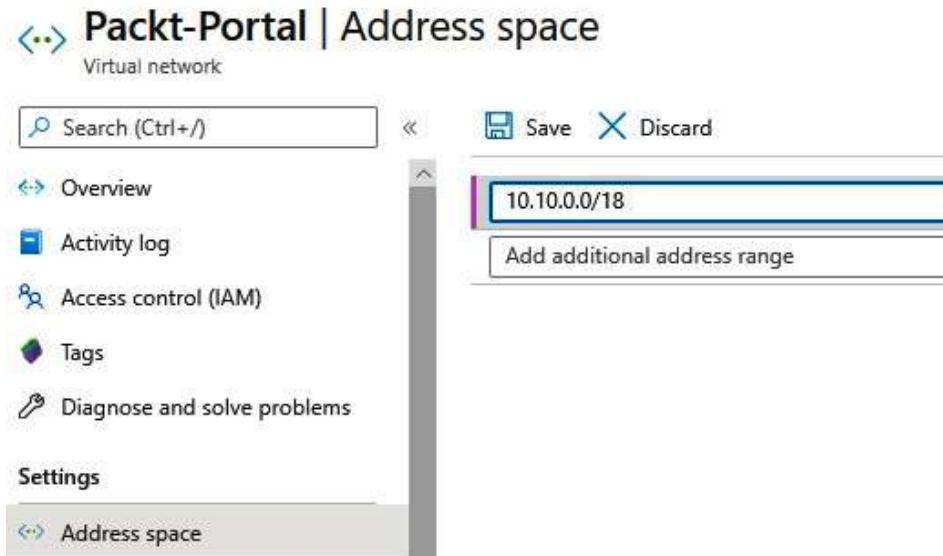


Figura 1.11: Alterar o intervalo do espaço de endereço

3. Depois de inserir um novo valor para o **Espaço de endereço**, clique em **Salvar** para aplicar as alterações.

## Como funciona...

Embora você possa alterar o espaço de endereço a qualquer momento, há algumas regras que determinam o que você pode fazer ou não. O espaço de endereço não poderá ser diminuído se você tiver sub-redes definidas no espaço de endereço que não seriam cobertas pelo novo espaço de endereço. Por exemplo, se o espaço de endereço estiver no intervalo de **10.0.0.0/16**, ele cobrirá endereços de **10.0.0.1** a **10.0.255.254**. Se uma das sub-redes for definida como **10.0.255.0/24**, não poderemos alterar a rede virtual para **10.0.0.0/17**, porque isso deixará a sub-rede fora do novo espaço.

O espaço de endereço não poderá ser alterado para um novo espaço de endereço se você tiver sub-redes definidas. Para mudar completamente o espaço de endereço, é necessário remover todas as sub-redes primeiro. Por exemplo, se tivermos o espaço de endereço definido como **10.0.0.0/16**, não poderemos alterá-lo para **10.1.0.0/16**, pois qualquer sub-rede que houvesse no espaço antigo a deixaria em um intervalo de endereços indefinido.

Vamos ver como alterar o tamanho das sub-redes recém-criadas.

## Alterar o tamanho de uma sub-rede

Semelhante ao espaço de endereço da rede virtual, podemos alterar o tamanho de uma sub-rede a qualquer momento.

### Preparação

Antes de iniciar, abra um navegador da Web e accesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para alterar o tamanho da sub-rede usando o portal do Azure, devemos seguir estas etapas:

1. No painel **Rede virtual**, selecione a opção **Sub-redes**.
2. Selecione a sub-rede que você deseja alterar. Na opção **Sub-redes**, insira um novo valor para o tamanho da sub-rede em **Intervalo de endereços**. Um exemplo de como fazer isso é mostrado na *Figura 1.12*:

 **FrontEnd**  
Packt-Portal

 Save  Discard  Delete  Refresh

---

**Address range (CIDR block) \*** ⓘ  
10.10.0.0/25 

10.10.0.0 - 10.10.0.127 (123 + 5 Azure reserved addresses)

---

**Available addresses** ⓘ  
251

**NAT gateway** ⓘ  
None

Add IPv6 address space

---

**Network security group**  
None

---

**Route table**  
None

---

**Users** >  
Manage users

---

**Service endpoints**

**Services** ⓘ  
0 selected

---

**Subnet delegation**

**Delegate subnet to a service** ⓘ  
None

Figura 1.12: Alterar o tamanho da sub-rede usando o portal do Azure

3. Depois de inserir um novo valor de intervalo de endereços, clique em **Salvar**.
4. Na lista de **Sub-redes**, podemos ver que as alterações foram aplicadas e que o espaço de endereço foi alterado, conforme mostrado na Figura 1.13:

Name	IPv4
BackEnd	10.10.1.0/24 (251 available)
GatewaySubnet	10.10.2.0/24 (251 available)
FrontEnd	10.10.0.0/25 (123 available)

Figura 1.13: Exibir as alterações feitas no intervalo de endereços da sub-rede

## Como funciona...

Ao alterar o tamanho da sub-rede, há algumas regras que devem ser seguidas. Não poderemos alterar o espaço de endereço se ele não estiver dentro do intervalo de espaço de endereço da rede virtual, e o intervalo da sub-rede não pode sobrepor outras sub-redes em uma rede virtual. Se os dispositivos forem atribuídos a essa sub-rede, poderemos alterar a sub-rede para excluir os endereços aos quais esses dispositivos já foram atribuídos.

# 2

# Redes de máquinas virtuais

Neste capítulo, abordaremos as **Máquinas Virtuais** do Azure (**VMs**) e a **interface de rede (NIC)** que é usada como uma interconexão entre as VMs do Azure e a Rede Virtual do Azure.

Abordaremos as seguintes receitas neste capítulo:

- Criar VMs do Azure
- Exibir configurações de rede da VM
- Criar uma nova NIC
- Anexar uma NIC a uma VM
- Desanexar uma NIC de uma VM

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure

## Criar VMs do Azure

As VMs do Azure dependem da rede virtual e, durante o processo de criação, precisamos definir as configurações de rede.

### Preparação

Antes de iniciarmos, abra um navegador da Web e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova VM usando o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha a VM do **Datacenter do Windows Server 2016** (ou pesquise qualquer imagem de VM pesquisando a **imagem** na barra de pesquisa **Pesquisar no Marketplace**).
2. No painel **Criar uma máquina virtual**, devemos fornecer informações para várias opções. Nem todas elas são relacionadas à rede. Primeiramente, devemos fornecer as informações sobre nossa **Assinatura** do Azure e sobre o **Grupo de recursos** (crie um novo grupo de recursos ou forneça um existente).
3. Em **Detalhes da instância**, precisamos fornecer informações nos campos **Nome da máquina virtual**, **Região**, **Opções de disponibilidade** e **Imagen** (no campo **Imagen**, deixe o padrão ou altere para uma imagem diferente no menu suspenso). Alguns exemplos configurações são mostrados na Figura 2.1:

The screenshot shows the 'Instance details' step of the Azure VM creation wizard. It includes fields for Subscription, Resource group, Virtual machine name, Region, Availability options, and Image.

Subscription *	Microsoft Azure Sponsorship
Resource group *	Packt-Networking-Portal
Virtual machine name *	Packt
Region *	(Europe) West Europe
Availability options	No infrastructure redundancy required
Image *	Windows Server 2016 Datacenter

**Subscription**: Microsoft Azure Sponsorship

**Resource group**: Packt-Networking-Portal

**Virtual machine name**: Packt

**Region**: (Europe) West Europe

**Availability options**: No infrastructure redundancy required

**Image**: Windows Server 2016 Datacenter

Figura 2.1: Fornecer informações para detalhes da instância

4. Em seguida, precisamos selecionar se desejamos usar a **Instância spot do Azure** (onde a VM é executada com a capacidade do datacenter não utilizada por um preço mais baixo, mas que pode ser desativada se os recursos forem necessários em outro lugar) e fornecer informações sobre o **Tamanho**, o **Nome de usuário** e a **Senha** de nossa VM. Observe que para o **Nome de usuário**, você não pode usar nomes como admin, administrador, sysadmin ou raiz. A senha deve ter pelo menos 12 caracteres e atender a três das quatro regras comuns (ou seja, ter letras maiúsculas, letras minúsculas, caracteres especiais e números). Um exemplo da tela preenchida é mostrado na Figura 2.2:

Azure Spot instance  Yes  No

Size \*  Standard\_B1ms - 1 vcpu, 2 GiB memory (\$17.05/month)

Administrator account

Username \*

Password \*

Confirm password \*

Figura 2.2: Configurar a instância spot do Azure

5. Em seguida, chegamos a uma opção relacionada à rede. É preciso definir se vamos permitir qualquer tipo de conexão por um endereço IP público. Podemos selecionar se queremos negar todo o acesso ou permitir uma porta específica. Opcionalmente, podemos usar o **Benefício Híbrido** para usar uma licença existente a fim de reduzir custos. No exemplo a seguir, vou escolher **RDP (3389)**, mas a lista suspensa também oferece opções para **SSH (22)**, **HTTP (80)** e **HTTPS (443)**:

#### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports \*

**⚠️** This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

#### Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Already have a Windows Server license? \*  Yes  No

Figura 2.3: Definir regras de porta de entrada

6. Na próxima seção, precisamos definir os discos. Podemos escolher entre **SSD Premium**, **SSD Standard** e **HDD Standard**. Um disco do sistema operacional é necessário e deve ser definido. É possível anexar discos de dados adicionais, conforme necessário. Os discos podem ser adicionados posteriormente também. A opção de criptografia padrão é usar chaves gerenciadas pela plataforma, mas podemos selecionar chaves gerenciadas pelo cliente, se necessário. Um exemplo de configurações de disco com somente o disco do sistema operacional é mostrado na Figura 2.4:

Basics    **Disks**    Networking    Management    Advanced    Tags    Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

#### Disk options

OS disk type \* ⓘ

Premium SSD



Encryption type \*

(Default) Encryption at-rest with a platform-managed key



Enable Ultra Disk compatibility ⓘ

Yes  No

Ultra disk is available only for Availability Zones in westeurope.

#### Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
<a href="#">Create and attach a new disk</a>		<a href="#">Attach an existing disk</a>		

Figura 2.4: Definir opções de armazenamento

7. Depois de definir os discos, chegamos às configurações de rede. Aqui, precisamos definir as opções de **Rede virtual** e **Sub-rede** que serão usadas pela VM. Essas duas opções são obrigatórias. Você pode optar por atribuir o endereço **IP público** à VM (você pode optar por desabilitar o endereço **IP público**, criar um novo ou atribuir um endereço IP existente). A última parte das configurações de rede está relacionada ao **Grupo de segurança de rede NIC**, onde devemos escolher se vamos usar um grupo de segurança de rede básico, avançado ou nenhum. Há também outra opção onde definiremos se permitiremos portas públicas. Também podemos configurar **Rede acelerada** ou **Balanceamento de carga** como opções adicionais. Um exemplo dessas configurações de rede da VM é mostrado na Figura 2.5:

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ	<input type="text" value="Packt-Portal"/> 
	<a href="#">Create new</a>
Subnet * ⓘ	<input type="text" value="FrontEnd (10.10.0.0/25)"/> 
	<a href="#">Manage subnet configuration</a>
Public IP ⓘ	<input type="text" value="(new) Packt-ip"/> 
	<a href="#">Create new</a>
NIC network security group ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports * ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="RDP (3389)"/> 
<div style="background-color: #ffffcc; padding: 10px;"><p> This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.</p></div>	

Accelerated networking ⓘ  On  Off

The selected VM size does not support accelerated networking.

### Load balancing

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

Place this virtual machine behind an existing load balancing solution?  Yes  No

Figura 2.5: Definir as opções da sub-rede e da rede virtual

8. Depois da seção de rede, devemos configurar **Gerenciamento** conforme mostrado na Figura 2.6:

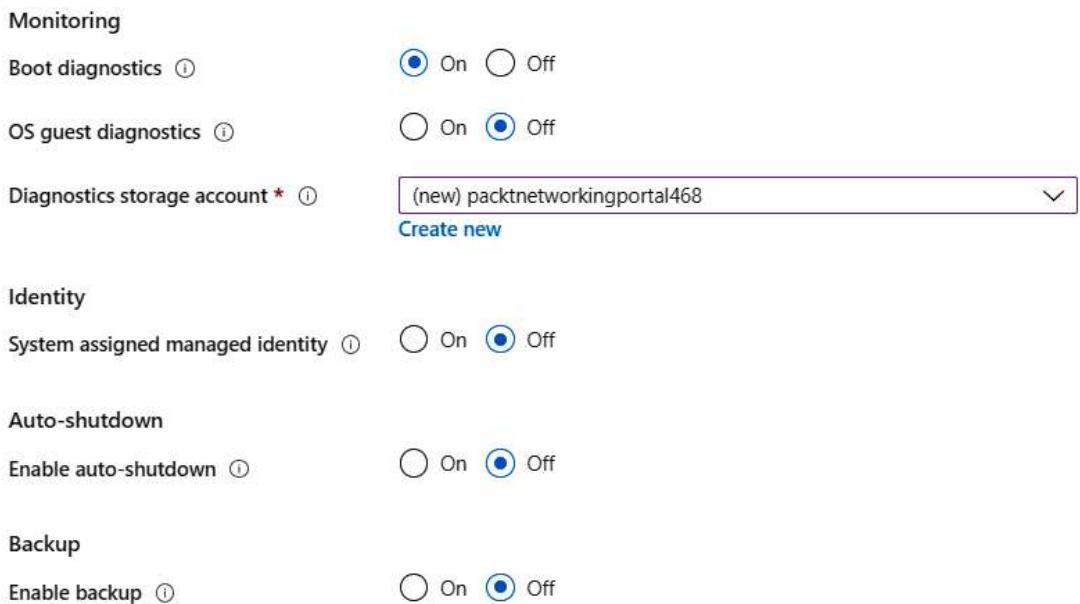


Figura 2.6: Habilitar recursos de gerenciamento

9. Em **Opções avançadas**, podemos definir as etapas de configuração pós-implantação adicionando instalações de software, scripts de configuração, dados personalizados e muito mais. A tela **Opções avançadas** é mostrada na Figura 2.7:

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

#### Extensions

Extensions provide post-deployment configuration and automation.

#### Extensions

Select an extension to install

#### Custom data

Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

#### Custom data



Custom data on the selected image will be processed by cloud-init. [Learn more about custom data and cloud init](#)

Figura 2.7: Definir a configuração pós-implantação

10. Na segunda parte das **Opções avançadas**, podemos selecionar uma configuração de **Grupo de host** (essa opção fornece um host dedicado que permite provisionar e gerenciar um servidor físico em um datacenter do Azure), um **Grupo de posicionamento por proximidade** (para agrupar servidores na mesma região) e se queremos usar VMs de **1ª geração** ou **2ª geração**. As opções padrão são mostradas na Figura 2.8:

**Host**

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

**Host group** No host group found

**Proximity placement group**

Proximity placement groups allow you to group Azure resources physically closer together in the same region. [Learn more](#)

**Proximity placement group** No proximity placement groups found

**VM generation**

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM).

**VM generation**  Gen 1  Gen 2

Generation 2 VMs do not yet support some Azure platform features, including Azure Disk Encryption.

Figura 2.8: Alocar um host dedicado para provisionar e gerenciar um servidor físico

11. As última configuração que podemos editar está relacionada às tags. As tags aplicam metadados adicionais aos recursos do Azure para organizá-los logicamente em uma taxonomia. A guia **Tags** é mostrada na Figura 2.9:

## Create a virtual machine

Basics Disks Networking Management Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
<input type="text"/>	<input type="text"/> :	<input type="button" value="12 selected"/>

Figura 2.9: Aplicar tags aos recursos do Azure

12. Depois que todas as configurações forem definidas, chegaremos à tela de validação, em que todas as nossas configurações são verificadas pela última vez. Após a aprovação da validação, confirmamos a criação de uma VM clicando no botão **Criar**, conforme mostrado na Figura 2.10:

## Create a virtual machine

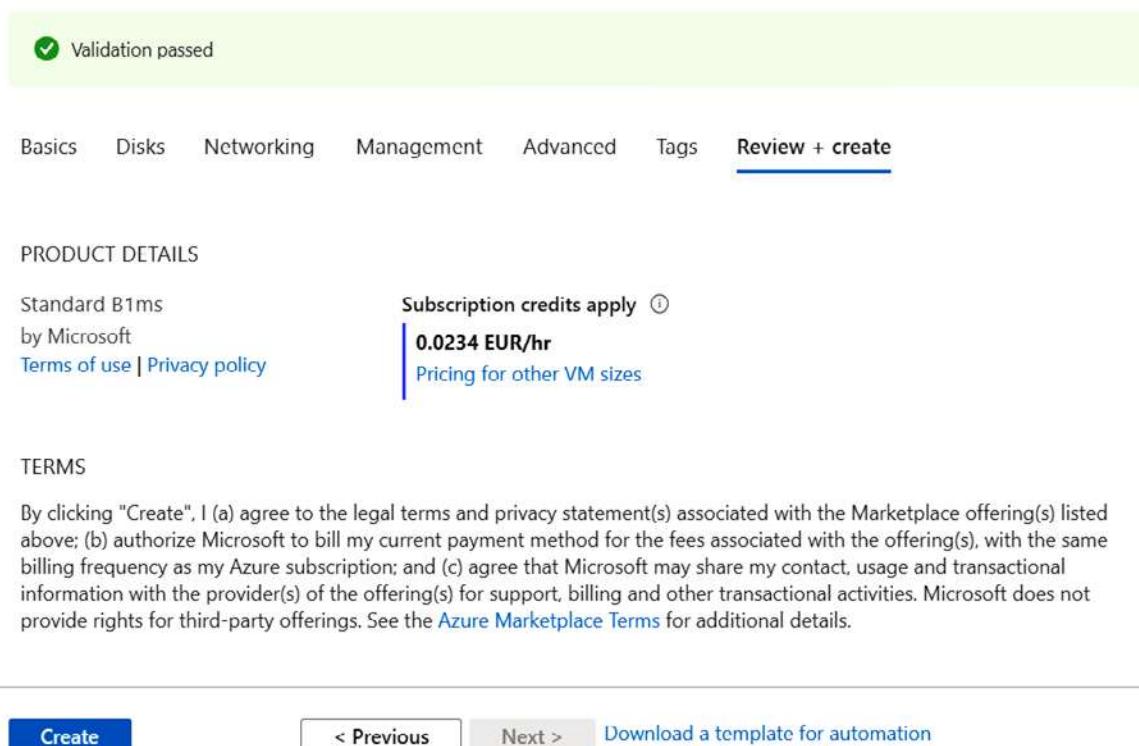


Figura 2.10: Criar uma VM

## Como funciona...

Quando uma VM é criada, uma NIC é criada no processo. Uma NIC é usada como uma espécie de interconexão entre a VM e a rede virtual. Uma NIC é atribuída um endereço IP privado pela rede. Como uma NIC é associada à VM e à rede virtual, o endereço IP é usado pela VM. Usando esse endereço IP, a VM pode se comunicar por meio de uma rede privada com outras VMs (ou outros recursos do Azure) na mesma rede. Além disso, as NICs e as VMs também podem ser atribuídas a endereços IP públicos. Um endereço público pode ser usado para a comunicação com a VM pela Internet, seja para acessar serviços ou para gerenciar a VM.

Agora que criamos uma VM do Azure e definimos as configurações de rede, na próxima seção, veremos como revisar essas configurações de rede.

## E mais...

Se estiver interessado em saber mais sobre as VMs do Azure, você poderá ler meu livro [Administração de nuvem prática no Azure](#), da Packt Publishing, em que as VMs são abordadas mais detalhadamente.

## Exibir configurações de rede da VM

Depois que uma VM do Azure é criada, podemos examinar as configurações de rede no painel da VM.

### Preparação

Antes de iniciar, abra um navegador da Web e accesse o portal do Azure em <https://portal.azure.com>. Nele, localize a VM criada anteriormente.

### Como fazer isso...

Para examinar as configurações de rede da VM, devemos seguir estas etapas:

1. No painel da VM, localize as configurações de **Rede**. Aqui, você pode ver a **Interface de rede**, os **Grupos de segurança de aplicativos** e o **Grupo de segurança de rede** associados à VM. Um exemplo disso é mostrado na Figura 2.11:

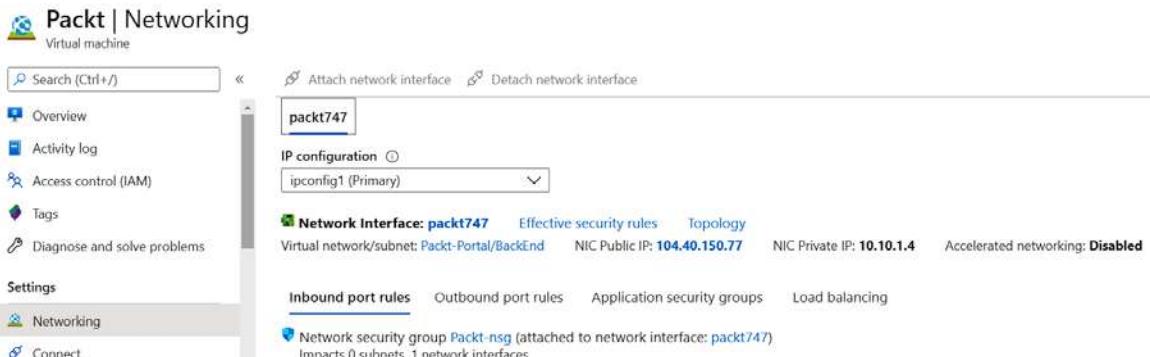


Figura 2.11: Configurações de rede de uma VM

2. Se selecionarmos qualquer um dos elementos de rede associados, poderemos descobrir mais detalhes. Por exemplo, se selecionarmos a opção de **Interface de rede** associada à VM, poderemos ver outras informações de rede, como **Endereço IP privado**, **Endereço IP público**, **Sub-rede/rede virtual**, **Grupo de segurança de rede**, **Configurações de IP**, **Servidores DNS** e muito mais. A exibição da NIC é mostrada na Figura 2.12:

Setting	Value
Resource group (change)	Packt-Networking-Portal
Location	West Europe
Subscription (change)	Microsoft Azure Sponsorship
Subscription ID	cb638267-a366-463c-bfe5-7a49311c27a8
Private IP address	10.10.1.8
Public IP address	13.95.110.109 (Packt-ip)
Private IP address (IPv6)	-
Public IP address (IPv6)	-
Virtual network/subnet	Packt-Portal/BackEnd
Network security group	Packt-nsg
Attached to	Packt

Figura 2.12: Exibir informações de rede da NIC

## Como funciona...

As informações de rede são exibidas em vários locais, inclusive nas configurações de rede da VM. Além disso, cada recurso do Azure tem um painel separado e existe como um recurso individual para que possamos exibir essas configurações em vários locais. No entanto, a imagem mais completa das configurações de rede da VM que podem ser encontradas no painel da VM e no painel da NIC.

## Criar uma nova NIC

Uma NIC geralmente é criada durante o processo de criação da VM, mas cada VM pode ter várias NICs. Com base nisso, podemos criar uma NIC como um recurso individual e anexá-la ou desanexá-la conforme necessário.

## Preparação

Antes de iniciar, abra um navegador da Web e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma nova NIC usando o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Interface de rede** em serviços de **Rede** (ou pesquise **interface de rede** na barra de pesquisa).
2. No painel de criação, devemos fornecer informações para os campos **Nome** e **Rede virtual**, bem como a sub-rede à qual a NIC será associada. Outras informações a serem fornecidas incluem o tipo de atribuição do endereço IP (**Dinâmico** ou **Estático**), se queremos que a NIC seja associada a um tipo de **Grupo de segurança de rede** e se queremos usar **IPv6**. Todos os recursos do Azure exigem informações sobre a **Assinatura**, o **Grupo de recursos** e a **Região**, e as NICs não são exceção. As informações necessárias para criar uma nova NIC são mostradas na Figura 2.13:

### Create network interface

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal

[Create new](#)

**Instance details**

Name \* NIC1

Region \* (Europe) West Europe

Virtual network ⓘ Packt-Portal

[Manage selected virtual network](#)

Subnet \* ⓘ FrontEnd (10.10.0.0/25)

Private IP address assignment **Dynamic** Static

Network security group ⓘ None

Private IP address (IPv6)

Figura 2.13: Criar uma NIC usando o portal do Azure

## Como funciona...

Uma NIC não pode existir sem uma associação de rede, e essa associação deve ser atribuída a uma rede virtual e a uma sub-rede. Isso é definido durante o processo de criação e não pode ser alterado posteriormente. Por outro lado, a associação a uma VM pode ser alterada e a NIC pode ser anexada ou desanexada de uma VM a qualquer momento.

## Anexar uma NIC a uma VM

Cada VM pode ter várias NICs. Por causa disso, podemos adicionar uma nova NIC a qualquer momento.

### Preparação

Antes de iniciar, abra um navegador da Web e acesse o portal do Azure em <https://portal.azure.com>. Aqui, localize a VM que criamos anteriormente neste capítulo.

### Como fazer isso...

Para anexar uma NIC a uma VM, devemos fazer o seguinte:

1. No painel da VM, certifique-se de que a VM esteja interrompida (ou seja, desalocada).
2. Localize as configurações de **Rede** no painel da VM.
3. Na parte superior da tela de configurações de **Rede** no painel da VM, selecione a opção **Anexar interface de rede**.
4. Uma nova opção será exibida, permitindo criar uma nova NIC ou selecionar uma NIC existente que não esteja associada à VM.
5. Clique em **OK** e, em alguns instantes, o processo será concluído e a NIC será associada à VM. Um exemplo disso é mostrado na Figura 2.14:

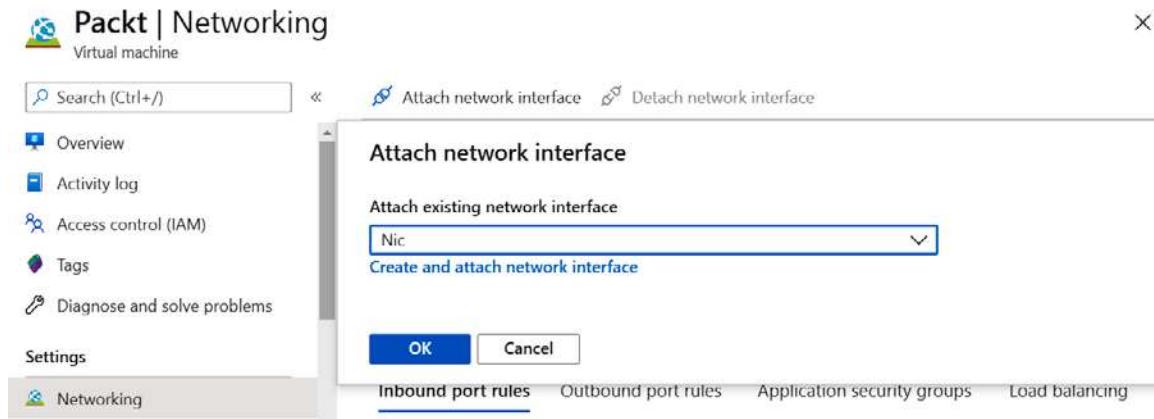


Figura 2.14: Anexar uma NIC

### Como funciona...

Cada VM pode ter várias NICs. O número de NICs que podem ser associadas a uma VM depende do tipo e do tamanho da VM. Para anexar uma NIC a uma VM, a VM deve estar interrompida (ou seja, desalocada). Você não pode adicionar outra NIC a uma VM em execução.

## Desanexar uma NIC de uma VM

Assim como com o processo para anexar uma NIC, podemos desanexar uma NIC a qualquer momento e anexá-la a outra VM.

### Preparação

Antes de iniciar, abra um navegador da Web e accese o portal do Azure em <https://portal.azure.com>. Nele, localize a VM criada anteriormente.

### Como fazer isso...

Para desanexar uma NIC de uma VM, devemos fazer o seguinte:

1. No painel da VM, certifique-se de que a VM esteja interrompida (ou seja, desalocada).
2. Localize as configurações de **Rede** no painel da VM.
3. Na parte superior da tela de configurações de **Rede** no painel da VM, selecione a opção **Desanexar interface de rede**.
4. Selecione a NIC que você deseja desanexar da VM.
5. Clique em **OK** e, em alguns instantes, o processo será concluído e a NIC será removida da VM. Um exemplo disso é mostrado na Figura 2.15:

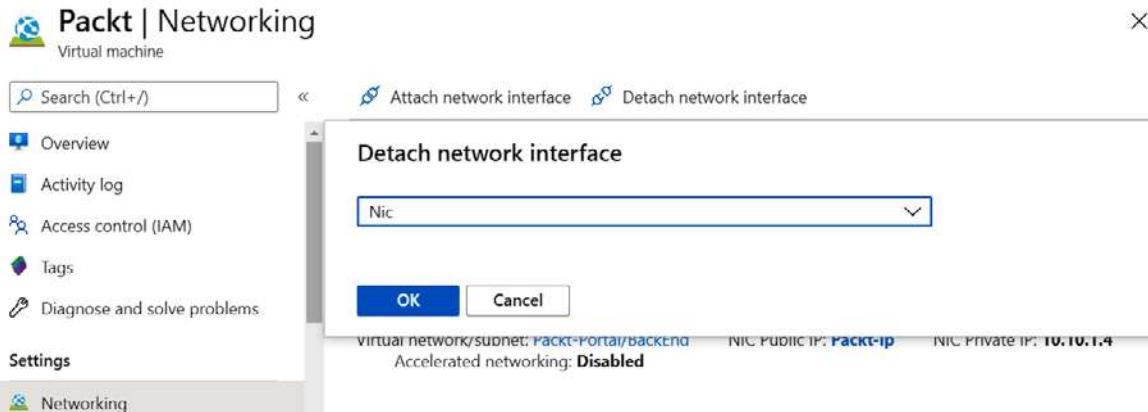


Figura 2.15: Desanexar uma NIC

### Como funciona...

Para desanexar uma NIC, a VM associada à NIC deve estar interrompida (ou seja, desalocada). Pelo menos uma NIC deve ser associada à VM. Portanto, você não pode remover a última NIC de uma VM. Todas as associações de rede ficam com a NIC. Elas são atribuídas à NIC, não à VM.



# 3

## Grupos de segurança de rede

**Os Grupos de segurança de rede (NSGs)** são ferramentas internas para controle de rede e permitem controlar o tráfego de entrada e de saída em uma interface de rede ou no nível da sub-rede. Eles contêm conjuntos de regras que permitem ou negam um tráfego específico a recursos ou sub-redes específicos no Azure. Um NSG pode ser associado a uma sub-rede (aplicando regras de segurança a todos os recursos associados à sub-rede) ou a uma **Placa de interface de rede (NIC)**, que é feito aplicando regras de segurança a todos os recursos associados à **Máquina virtual (VM)** associada à NIC.

Abordaremos as seguintes receitas neste capítulo:

- Criar um novo NSG no portal do Azure
- Criar um novo NSG com o PowerShell
- Criar uma nova regra de permissão em um NSG
- Criar uma nova regra de negação em um NSG
- Criar uma nova regra de NSG com o PowerShell
- Atribuir um NSG a uma sub-rede
- Atribuir um NSG a uma interface de rede
- Atribuir um NSG a uma sub-rede com o PowerShell
- Criar um **Grupo de segurança de aplicativos (ASG)**
- Associar um ASG a uma VM
- Criar regras com um NSG e um ASG

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Azure PowerShell

Os exemplos de código podem ser encontrados no

[https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/  
tree/master/Chapter03.](https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter03)

## Criar um novo NSG no portal do Azure

Como primeiro passo para controlar o tráfego de rede de forma mais eficiente, vamos criar um novo NSG.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em  
<https://portal.azure.com>.

## Como fazer isso...

Para criar um novo NSG usando o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Grupo de segurança de rede** em **Rede** (ou pesquise **grupo de segurança de rede** na barra de pesquisa).
2. Os parâmetros que precisamos definir para a implantação são **Assinatura**, **Grupo de recursos**, **Nome** e **Região**. Um exemplo dos parâmetros necessários é mostrado na Figura 3.1:

### Create network security group

Basics   Tags   Review + create

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal

Create new

**Instance details**

Name \* NSG1

Region \* (Europe) West Europe

Figura 3.1: Criar um novo NSG usando o portal do Azure

Depois que a implantação for validada e iniciada (são necessários alguns instantes para ser concluída), o NSG estará pronto para uso.

## Como funciona...

A implantação do NSG pode ser iniciada durante uma implantação da VM. Isso associará o NSG à NIC associada à VM implantada. Nesse caso, o NSG já está associado ao recurso, e as regras definidas no NSG serão aplicadas somente à VM associada.

Se o NSG for implantado separadamente, como visto nesta receita, ele não será associado, e as regras criadas nele não serão aplicadas até que uma associação seja criada com a NIC ou a sub-rede. Quando for associado a uma sub-rede, as regras de NSG se aplicarão a todos os recursos na sub-rede.

Vamos avançar para a próxima receita para entender como criar um novo NSG usando o PowerShell.

## Criar um novo NSG com o PowerShell

Como alternativa, podemos criar um NSG usando o PowerShell. A vantagem dessa abordagem é que podemos adicionar regras de NSG em um único script, criando regras personalizadas logo após a criação do NSG. Isso permite automatizar o processo de implantação e criar nossas próprias regras padrão logo após a criação do NSG.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure. Consulte o Capítulo 1, *Rede Virtual do Azure*, para um lembrete de como fazer isso.

### Como fazer isso...

Para implantar um novo NSG, execute o seguinte comando:

```
New-AzNetworkSecurityGroup -Name "nsg1" -ResourceGroupName "Packt-Networking-Script" -Location "westeurope"
```

### Como funciona...

O script está usando o **Grupo de recursos (GR)** que foi implantado no Capítulo 1, *Rede Virtual do Azure* (usaremos o mesmo GR para todas as implantações). Caso contrário, um novo GR precisará ser implantado antes da execução do script. O resultado final será o mesmo da criação de um novo NSG usando o portal do Azure: um novo NSG será criado com as regras padrão. Uma das vantagens de usar o PowerShell é que podemos adicionar mais regras durante a implantação que ajudará a automatizar o processo. Você verá um exemplo disso na receita *Criar uma nova regra de NSG com o PowerShell* mais adiante neste capítulo.

Nesta receita, você aprendeu a criar um novo NSG usando o PowerShell. Vamos avançar para a próxima receita para aprender a permitir regras no NSG usando o portal do Azure.

## Criar uma nova regra de permissão em um NSG

Quando um novo NSG for criado, apenas as regras padrão estarão presentes, o que permite todo o tráfego de saída e bloqueia todo o tráfego de entrada. Para alterá-las, regras adicionais precisam ser criadas. Primeiro, vamos mostrar como criar uma nova regra para permitir o tráfego de entrada.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Localize o NSG criado anteriormente.

### Como fazer isso...

Para criar uma nova regra de permissão de NSG usando o portal do Azure, devemos seguir estas etapas:

1. No painel NSG, localize a opção **Regras de segurança de entrada** em **Configurações**.
2. Clique no botão **Adicionar** na parte superior da página e aguarde até que o novo painel seja aberto:

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). The left sidebar shows options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area is titled "NSG1 | Inbound security rules" and shows a table of existing rules:

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

Figura 3.2: Criar uma nova regra de permissão do NDG usando o portal do Azure

3. No novo painel, precisamos fornecer informações para os campos **Origem** (intervalo de porta e local), **Destino** (intervalo de porta e local), **Protocolo**, **Ação**, **Prioridade**, **Nome** e **Descrição**. Se deseja permitir o tráfego, selecione **Permitir** em **Ação**. Um exemplo de como criar uma regra para permitir o tráfego pela porta **443** (permitindo, assim, o tráfego ao servidor Web) é mostrado na Figura 3.3:

 Add inbound security rule ×

NSG1

 Basic

**Source \*** ⓘ  
Any

**Source port ranges \*** ⓘ  
\*

**Destination \*** ⓘ  
Any

**Destination port ranges \*** ⓘ  
443 ✓

**Protocol \***  
 Any  TCP  UDP  ICMP

**Action \***  
 Allow  Deny

**Priority \*** ⓘ  
100

**Name \***  
Port\_443 ✓

**Description**  
Allow HTTPS ✓

**Add**

Figura 3.3: Criar uma regra para permitir o tráfego pela porta 443

## Como funciona...

Por padrão, todo o tráfego proveniente do Azure Load Balancer ou da Rede Virtual do Azure é permitido. Todo o tráfego proveniente da Internet é negado. Para alterar isso, precisamos criar regras adicionais. Certifique-se de definir a prioridade certa ao criar regras. As regras com prioridade mais alta (ou seja, aquelas com o número menor) são processadas primeiro. Portanto, se você tiver duas regras, com uma negando tráfego e outra permitindo-o, a regra com prioridade mais alta terá precedência, enquanto a com prioridade mais baixa será ignorada.

Nesta receita, você aprendeu a criar uma nova regra para permitir o tráfego de entrada. Na próxima receita, você aprenderá a criar uma nova regra no NSG para negar o tráfego.

## Criar uma nova regra de negação em um NSG

Quando um novo NSG for criado, somente as regras padrão estarão presentes. As regras padrão permitem todo o tráfego de saída e bloqueiam todo o tráfego de entrada. Para alterar isso, regras adicionais precisam ser criadas. Agora, vamos mostrar como criar uma nova regra de saída para negar o tráfego.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Localize o NSG criado anteriormente.

### Como fazer isso...

Para criar uma nova regra de negação de NSG usando o portal do Azure, devemos seguir estas etapas:

1. No painel NSG, localize a opção **Regras de segurança de saída** em **Configurações**.
2. Clique no botão **Adicionar** na parte superior da página e aguarde até que o novo painel seja aberto:

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	<input checked="" type="checkbox"/> Allow
65500	DenyAllOutBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny

Figura 3.4: Criar uma nova regra de negação do NSG usando o portal do Azure

3. Na novo painel, precisamos fornecer informações para os campos **Origem** (intervalo de porta e local), **Destino** (intervalo de porta e local), **Protocolo**, **Ação**, **Prioridade**, **Nome** e **Descrição**. Se deseja negar o tráfego, selecione **Negar** em **Ação**. Um exemplo de como criar uma regra para negar o tráfego pela porta 22 é mostrado na Figura 3.5:

 Add outbound security rule X

NSG1

 Basic

**Source \*** ⓘ  
Any

**Source port ranges \*** ⓘ  
\*

**Destination \*** ⓘ  
Any

**Destination port ranges \*** ⓘ  
22 ✓

**Protocol \***  
 Any  TCP  UDP  ICMP

**Action \***  
 Allow  Deny

**Priority \*** ⓘ  
100

**Name \***  
Port\_22 ✓

**Description**  
Deny SSH ✓

**Add**

Figura 3.5: Adicionar uma regra de segurança de saída

## Como funciona...

Todo o tráfego de saída é permitido por padrão, não importa para onde ele está indo. Se quisermos negar explicitamente o tráfego em uma porta específica, precisamos criar uma regra para fazer isso. Certifique-se de definir a prioridade certa ao criar regras. As regras com a prioridade a mais elevada (aqueles com os menores números) são processadas primeiro. Portanto, se você tiver duas regras, com uma negando tráfego e outra permitindo-o, a regra com prioridade mais alta será aplicada.

Vamos avançar para a próxima receita, onde você aprenderá a criar uma regra de NSG usando o PowerShell.

## Criar uma nova regra de NSG com o PowerShell

Como alternativa, podemos criar uma regra de NSG usando o PowerShell. Este comando pode ser executado diretamente após a criação do NSG, permitindo criar e configurar um NSG em um único script. Dessa forma, podemos padronizar a implantação e ter regras aplicadas sempre que um NSG for criado.

## Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

## Como fazer isso...

Para criar uma nova regra de NSG, execute o seguinte comando:

```
$nsg = Get-AzNetworkSecurityGroup -Name 'nsg1' -ResourceGroupName 'Packt-Networking-Script'  
$nsg | Add-AzNetworkSecurityRuleConfig -Name 'Allow_HTTPS' -Description 'Allow_HTTPS' -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 443 | Set-AzNetworkSecurityGroup
```

## Como funciona...

Usando um script, criar uma regra de NSG é apenas uma questão de parâmetros. O parâmetro **Acesso**, que pode ser **Permitir** ou **Negar**, determinará se queremos permitir o tráfego ou negá-lo. O parâmetro **Direção**, que pode ser **Entrada** ou **Saída**, determina se a regra é para o tráfego de entrada ou de saída. Todos os outros parâmetros são os mesmos, não importa o tipo de regra que queremos criar. Novamente, a prioridade desempenha um papel muito importante. Por isso, é importante verificar se ela foi escolhida corretamente.

## E mais...

Como mencionado na receita *Criar um novo NSG com o PowerShell*, podemos criar o NSG e as regras necessárias em um único script. O script a seguir é um exemplo disso:

```
$nsg = New-AzNetworkSecurityGroup -Name 'nsg1' -ResourceGroupName 'Packt-Networking-Script' -Location "westeurope"

$nsg | Add-AzNetworkSecurityRuleConfig -Name 'Allow_HTTPS' -Description 'Allow_HTTPS' -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 443 | Set-AzNetworkSecurityGroup
```

Esta receita explica como criar uma nova regra de NSG usando o PowerShell. Na próxima receita, você aprenderá a atribuir um NSG a uma sub-rede.

## Atribuir um NSG a uma sub-rede

O NSG e suas regras devem ser atribuídos a um recurso para causar um impacto. Aqui, você verá como associar um NSG a uma sub-rede.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Localize o NSG criado anteriormente.

### Como fazer isso...

Para atribuir um NSG a uma sub-rede, siga estas etapas:

1. No painel NSG, localize a opção **Sub-redes** em **Configurações**.
2. Clique no botão **Associar** na parte superior da página e aguarde até que o novo painel seja aberto:

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). The main title is 'NSG1 | Subnets'. On the left, there's a sidebar with several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules, Outbound security rules, Network interfaces, and Subnets. The 'Subnets' option is highlighted with a grey background. At the top right, there's a search bar with the placeholder 'Search (Ctrl+ /)'. To its right is a button labeled '+ Associate'. Below this is another search bar with the placeholder 'Search subnets'. Underneath is a table with a single row. The first column is 'Name' and the second column is 'No results.'

Figura 3.6: Atribuir um NSG a uma sub-rede

3. No novo painel, selecione primeiro a rede virtual que contém a sub-rede à qual você deseja associar o NSG e, em seguida, selecione a sub-rede, como visto na Figura 3.7:

This is a screenshot of a modal dialog titled 'Associate subnet'. At the top left is the text 'Associate subnet' and at the top right is a close button 'X'. Below that is the identifier 'NSG1'. The dialog contains two dropdown menus. The first dropdown is labeled 'Virtual network' and has the value 'Packt-Portal'. The second dropdown is labeled 'Subnet' and has the value 'FrontEnd'.

Figura 3.7: Associar o subconjunto ao NSG

4. Depois de enviar a alteração, a sub-rede será exibida em uma lista de sub-redes associadas:

Name	Address range	Virtual network
FrontEnd	10.10.0.0/25	Packt-Portal

Figura 3.8: Uma lista de sub-redes associadas

## Como funciona...

Quando um NSG é associado a uma sub-rede, as regras no NSG serão aplicadas a todos os recursos na sub-rede. Observe que a sub-rede pode ser associada a mais de um NSG e que as regras de todos os NSGs serão aplicadas nesse caso. A prioridade é o fator mais importante ao analisar um único NSG, mas quando as regras de mais NSGs são observadas, a regra **Negar** prevalecerá. Portanto, se tivermos dois NSGs em uma sub-rede, uma com **Permitir** na porta 443 e outra com a regra **Negar** na mesma porta, o tráfego nessa porta será negado.

Vamos avançar para a próxima receita e aprender a atribuir um NSG a uma interface de rede.

## Atribuir um NSG a uma interface de rede

Agora, vamos ampliar nosso escopo e mostrar como associar um NSG a uma interface de rede.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Localize o NSG criado anteriormente.

### Como fazer isso...

Para atribuir um NSG a uma interface de rede, siga estas etapas:

1. No painel NSG, localize a opção **Interfaces de rede** em **Configurações**.

2. Clique no botão **Associar** na parte superior da página e aguarde até que o novo painel seja aberto:

The screenshot shows the 'NSG1 | Network interfaces' page in the Azure portal. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, and Settings. Under Settings, there are sections for Inbound security rules, Outbound security rules, and Network interfaces. The 'Network interfaces' section is highlighted. On the right, there's a large 'Associate' button with a plus sign, a search bar for 'Search network interfaces', and a 'Name' input field which currently says 'No results.'

Figura 3.9: Atribuir o NSG a uma interface de rede

3. Selecione a NIC à qual deseja associar o NSG na lista das que estão disponíveis:

### Associate network interface

The screenshot shows the 'Associate network interface' dialog. At the top, there's a note: 'Choose a network interface to associate with this network security group'. Below it, another note says: 'These are the network interfaces in the selected subscription and location 'West Europe''. A list of network interfaces is shown: 'Nic' (Packt-Networking-Portal), 'rvsb329' (RedVSBlue), 'kali-vm382' (Security), and 'packt747' (Packt-Networking-Portal).

Figura 3.10: Associar à interface de rede

## Como funciona...

Quando um NSG for associado a uma NIC, as regras de NSG serão aplicadas somente a uma única NIC (ou uma VM associada à NIC). A NIC pode ser associada somente a um NSG diretamente, mas uma sub-rede associada a uma NIC pode ter uma associação a outro NSG (ou até mesmo a vários NSGs). Isso é semelhante a quando temos vários NSGs atribuídos a uma única sub-rede, e a regra **Negar** terá maior prioridade. Se um dos NSGs permitir o tráfego em uma porta, mas um outro NSG o bloquear, o tráfego será negado.

Nesta receita, você aprendeu a atribuir um NSG a uma interface de rede. Vamos avançar para a próxima receita, onde você aprenderá a atribuir um NSG usando o PowerShell.

## Atribuir um NSG a uma sub-rede com o PowerShell

Como alternativa, podemos associar um NSG usando o Azure PowerShell. Nesta receita, vamos mostrar como associar um NSG a uma sub-rede.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

### Como fazer isso...

Para associar um NSG a uma sub-rede, execute o seguinte comando:

```
$vnet = Get-AzVirtualNetwork -Name 'Packt-Script' -ResourceGroupName 'Packt-Networking-Script'  
$subnet = Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name BackEnd  
  
$nsg = Get-AzNetworkSecurityGroup -ResourceGroupName 'Packt-Networking-Script' -Name 'nsg1'  
$subnet.NetworkSecurityGroup = $nsg  
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

## Como funciona...

Para atribuir um NSG usando o PowerShell, precisamos coletar informações sobre a rede virtual, a sub-rede e o NSG. Quando todas as informações forem coletadas, poderemos fazer a associação usando o comando **Set-AzVirtualNetwork** e aplicar as alterações.

Vamos avançar para a próxima receita e criar um ASG usando o portal do Azure.

## Criar um Grupo de segurança de aplicativos (ASG)

ASGs são uma extensão de NSGs, permitindo criar regras adicionais e ter melhor controle do tráfego. Usar somente NSGs permite criar regras que permitirão ou negarão o tráfego somente para uma origem, um endereço IP ou uma sub-rede específica. ASGs permitem criar uma filtragem melhor e criar verificações adicionais em que o tráfego é permitido com base em ASGs. Por exemplo, com NSGs, podemos criar uma regra em que a sub-rede A pode se comunicar com a sub-rede B. Se tivermos a estrutura da aplicação para ela e um ASG associado, podemos adicionar recursos em grupos de aplicações. Ao adicionar esse elemento, podemos criar uma regra que permitirá a comunicação entre a sub-rede A e a sub-rede B, mas somente se os recursos pertencerem à mesma aplicação.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar um ASG usando o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Grupo de segurança de aplicativos** em **Rede** (ou pesquise **grupo de segurança de aplicativos** na barra de pesquisa).
2. Os parâmetros que precisamos definir para a implantação são **Assinatura**, **Grupo de recursos**, **Nome** e **Região**. Um exemplo dos parâmetros necessários é mostrado na Figura 3.11:

### Create an application security group

**Basics** Tags Review + create

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal [Create new](#)

**Instance details**

Name \* ASG1

Region \* (Europe) West Europe

Figura 3.11: Criar um ASG usando o portal do Azure

## Como funciona...

ASGs não fazem muita diferença isoladamente e devem ser combinados com NSGs para criar regras de NSG que proporcionarão melhor controle do tráfego, aplicando verificações adicionais antes que o fluxo de tráfego seja permitido.

Agora que criamos um ASG, vamos avançar para uma nova receita, onde associaremos o ASG a uma VM.

## Associar um ASG a uma VM

Depois de criar um ASG, devemos associá-lo a uma VM. Depois de fazer isso, podemos criar regras com o NSG e o ASG para o controle de tráfego.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>. Localize a VM criada anteriormente.

### Como fazer isso...

Para associar um ASG a uma VM, devemos seguir estas etapas:

1. No painel da VM, localize as configurações de **Rede**.
2. Nas configurações de **Rede**, selecione a guia **Grupos de segurança de aplicativos**, conforme mostrado na Figura 3.12:

Priority	Name	Port	Protocol	Source	Destination	Action	...
300	<span style="color: orange;">⚠️</span> RDP	3389	TCP	Any	Any	<span style="color: green;">Allow</span>	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<span style="color: green;">Allow</span>	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<span style="color: green;">Allow</span>	...
65500	DenyAllInBound	Any	Any	Any	Any	<span style="color: red;">✖️ Deny</span>	...

Figura 3.12: Associar um ASG a uma VM

3. Nas configurações de **Grupos de segurança de aplicativos**, selecione **Configurar os grupos de segurança de aplicativos**, conforme mostrado na Figura 3.13:

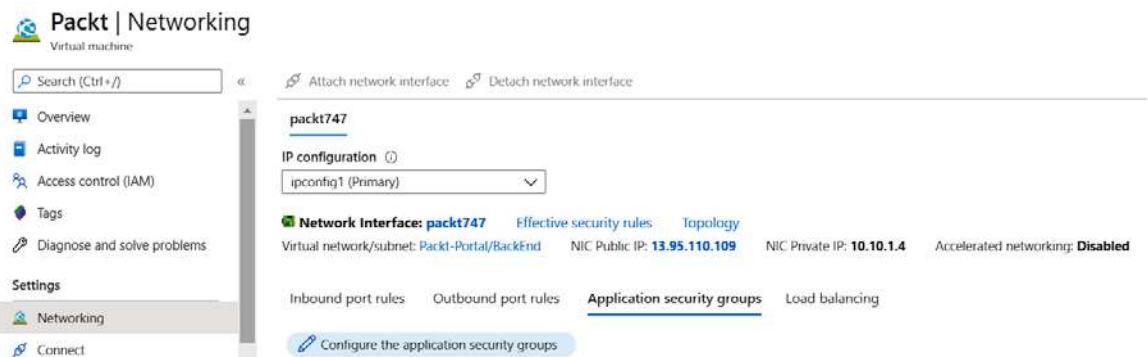


Figura 3.13: Configurar ASGs

4. No novo painel da lista de ASGs disponíveis, selecione o ASG ao qual você deseja associar a VM:

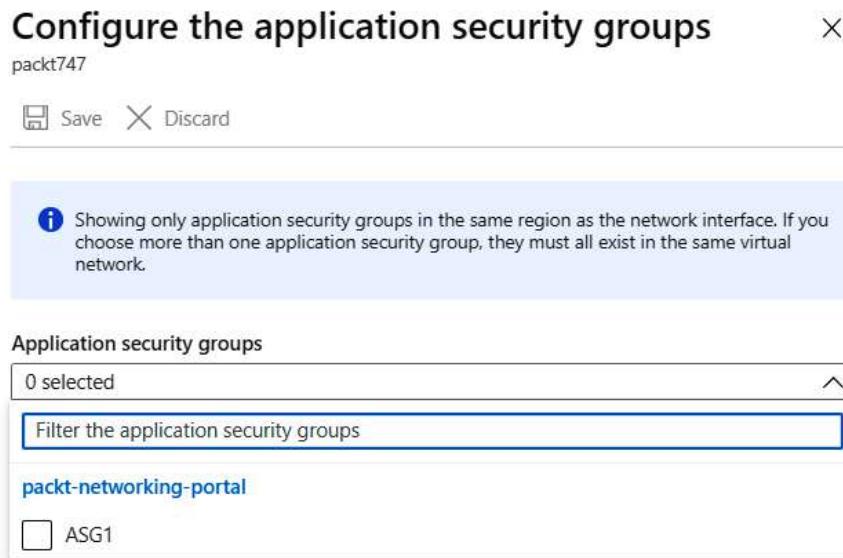


Figura 3.14: Associar um ASG a uma VM

5. Depois de clicar em **Salvar**, levará alguns segundos para aplicar as alterações e, depois disso, a VM será associada ao ASG.

## Como funciona...

A VM deve ser associada ao ASG. Podemos associar mais de uma VM a cada ASG. Em seguida, o ASG é usado em combinação com o NSG para criar novas regras de NSG.

Na próxima receita, criaremos novas regras usando um NSG e um ASG.

## Criar regras com um NSG e um ASG

Como última etapa, podemos usar NSGs e ASGs para criar novas regras com melhor controle. Essa abordagem permite ter melhor controle de tráfego, limitando o tráfego de entrada não apenas a uma sub-rede específica, mas também apenas com base em se o recurso faz parte ou não do ASG.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Localize o NSG criado anteriormente.

### Como fazer isso...

Para criar uma regra usando um ASG e um NSG, devemos seguir estas etapas:

1. No painel NSG, localize **Regras de segurança de entrada**. Selecione **Adicionar** para adicionar uma nova regra.
2. Para a origem, selecione **Grupo de segurança de aplicativos** e selecione o ASG que você deseja usar como origem. Também precisamos fornecer parâmetros para **Origem, Intervalos de porta de origem, Destino, Intervalos de porta de destino, Protocolo, Ação, Prioridade, Nome e Descrição**. Um exemplo é mostrado na Figura 3.15:

Add inbound security rule

Packt-nsg

Basic

Source application security group \*

Source port ranges \*

Destination \*

Destination port ranges \*

Protocol \*  Any  TCP  UDP  ICMP

Action \*  Allow  Deny

Priority \*

Name \*

Description

Add

Figura 3.15: Adicionar uma regra de segurança de entrada

## Como funciona...

Usando apenas NSGs para criar regras, podemos criar permitir ou negar o tráfego somente para um intervalo ou endereço IP específico. Com um ASG, podemos ampliar ou restringir isso conforme necessário. Por exemplo, podemos criar uma regra para permitir VMs de uma sub-rede de front-end, mas somente se essas VMs estiverem em um ASG específico. Como alternativa, podemos permitir o acesso a várias VMs de diferentes redes virtuais e sub-redes, mas somente se elas pertencerem a um ASG específico.



# 4

## Gerenciar endereços IP

No Azure, podemos ter dois tipos de endereços IP: públicos e privados. Os endereços públicos podem ser acessados pela Internet. Os endereços privados são do espaço de endereço da Rede Virtual do Azure e são usados para comunicação privada em redes privadas. Os endereços podem ser atribuídos a um recurso ou podem existir como um recurso separado.

Abordaremos as seguintes receitas neste capítulo:

- Criar um novo endereço IP público no portal do Azure
- Criar um novo endereço IP público com o PowerShell
- Atribuir um endereço IP público
- Cancelar a atribuição de um endereço IP público
- Criar uma reserva para um endereço IP público
- Remover uma reserva para um endereço IP público
- Criar uma reserva para um endereço IP privado
- Alterar uma reserva para um endereço IP privado
- Remover uma reserva para um endereço IP privado
- Adicionar vários endereços a uma NIC
- Criar um prefixo de IP público

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Azure PowerShell

Os exemplos de código podem ser encontrados no

[https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/  
tree/master/Chapter04](https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter04).

## Criar um novo endereço IP público no portal do Azure

Endereços IP públicos podem ser criados como um recurso separado ou criados durante a criação de alguns outros recursos (por exemplo, uma **máquina virtual (VM)**). Portanto, um IP público pode existir como parte de um recurso ou como um recurso autônomo. Primeiro, vamos mostrar como criar um novo endereço IP público.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em  
<https://portal.azure.com>.

## Como fazer isso...

Para criar um novo endereço IP público, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Endereço IP público** nos serviços de **Rede** (ou pesquise **endereço IP público** na barra de pesquisa).
2. Os parâmetros que precisamos definir para a implantação são **Versão IP**, **SKU**, **Nome**, **Atribuição de endereço IP**, **Rótulo de nome DNS**, **Assinatura**, **Grupo de recursos** e **Local**. O tempo limite de inatividade (período em que a conexão permanecerá aberta sem nenhuma atividade) é definido como padrão para 4 minutos, mas pode ser aumentado para 30 minutos no máximo. Um exemplo dos parâmetros necessários é mostrado na Figura 4.1:

### Create public IP address

IP Version \* ⓘ  
 IPv4  IPv6  Both

SKU \* ⓘ  
 Basic  Standard

**IPv4 IP Address Configuration**

Name \*  
 ✓

IP address assignment \*  
 Dynamic  Static

Idle timeout (minutes) \* ⓘ  
 4

DNS name label ⓘ

Subscription \*  
 ✓

Resource group \*  
 ✓  
[Create new](#)

Location \*  
 ✓

Create [Automation options](#)

Figura 4.1: Criar um novo endereço IP público usando o portal do Azure

## Como funciona...

A **unidade de estocagem (SKU)** pode ser **Básica** ou **Padrão**. As diferenças principais são que **Padrão** é fechada ao tráfego de entrada por padrão (o tráfego de entrada deve ser permitido em **Grupos de segurança de rede (NSGs)**) e **Padrão** com redundância de zona. Outra diferença é que um endereço IP público de SKU **Padrão** tem uma atribuição estática, enquanto uma SKU **Básica** pode ser estática ou dinâmica.

Você pode escolher a versão **IPv4** ou **IPv6** para o endereço IP, mas escolher **IPv6** limitará a uma atribuição dinâmica para a SKU **Básica** e uma atribuição estática para a SKU **Padrão**.

O **rótulo de nome DNS** é opcional. Ele poderá ser usado para resolver o ponto de extremidade se uma atribuição dinâmica for selecionada. Caso contrário, não há utilidade na criação de um rótulo DNS, pois um endereço IP sempre poderá ser usado para resolver o ponto de extremidade se uma atribuição estática for selecionada.

## Criar um novo endereço IP público com o PowerShell

Como alternativa, podemos criar um endereço IP público usando o Azure PowerShell. Novamente, essa abordagem é melhor quando queremos automatizar o processo. Embora um endereço IP público possa existir por conta própria, ele geralmente é associado a outros recursos e para ser usado como um ponto de extremidade. Ao usar o PowerShell para criar um recurso, podemos seguir para a próxima etapa e associá-lo a um recurso em um único script.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

## Como fazer isso...

Para implantar um novo endereço IP público, execute o seguinte comando:

```
New-AzPublicIpAddress -Name 'ip-public-script' -ResourceGroupName 'Packt-Networking-Script' -AllocationMethod Dynamic -Location 'westeurope'
```

## Como funciona...

Como resultado, um novo endereço IP público será criado. Nesse caso, as configurações serão uma atribuição dinâmica de SKU básica, versão IPv4 e sem nenhum rótulo DNS. Além disso, podemos usar interruptores adicionais, como **-SKU** para selecionar **Básica** ou **Padrão**, **-IPAddressVersion** para escolher entre **IPv4** e **IPv6** ou **-DomainNameLabel** para especificar o rótulo DNS. Esses são parâmetros opcionais. Se eles não forem especificados, o Azure criará o IP público com os valores padrão mencionados acima.

## Atribuir um endereço IP público

Um endereço IP público pode ser criado como um recurso separado ou desassociado de outro recurso e existir por conta própria. Em seguida, esse endereço IP pode ser atribuído a um novo recurso ou outro já existente. Se o recurso não estiver mais em uso ou foi migrado, ainda poderemos usar o mesmo endereço IP público. Nesse caso, o ponto de extremidade público usado para acessar um serviço pode permanecer inalterado. Isso pode ser útil quando uma aplicação ou um serviço disponível ao público geral é migrado ou atualizado, pois podemos continuar usando o mesmo ponto de extremidade, e os usuários não precisam tomar conhecimento de nenhuma alteração.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para atribuir um endereço IP público, devemos fazer o seguinte:

1. Localize a **interface de rede (NIC)** à qual você deseja que o endereço IP seja atribuído. Isto pode ser feito diretamente ao localizar a NIC ou por meio do painel da VM à qual a NIC está atribuída.
2. No painel **Interface de rede**, acesse **Configurações de IP** em **Configurações** e selecione a configuração mostrada na Figura 4.2:

The screenshot shows the 'Nic | IP configurations' page for a specific network interface. The left sidebar lists options: Overview, Activity log, Access control (IAM), Tags, Settings (selected), IP configurations (selected), DNS servers, Network security group, and Properties. The main area displays the following information:

- IP forwarding settings:** IP forwarding is set to **Disabled** (Enabled is also shown).
- Virtual network:** Packt-Portal
- IP configurations:** Subnet \* FrontEnd (10.10.0.0/25) is selected.
- Search IP configurations:** ipconfig1
- Table:** Shows a single row for ipconfig1 with columns: Name, IP Version, Type, Private IP address, and Public IP address. The values are: ipconfig1, IPv4, Primary, 10.10.0.4 (Dynamic), and -.

Figura 4.2: Exibir as configurações de IP no painel da NIC

3. No novo painel, selecione **Associar** em **Endereço IP público** e selecione o **Endereço IP público** que você deseja atribuir no menu suspenso. Somente os endereços IP não atribuídos na mesma região serão mostrados na lista. Um exemplo disso é mostrado na Figura 4.3:

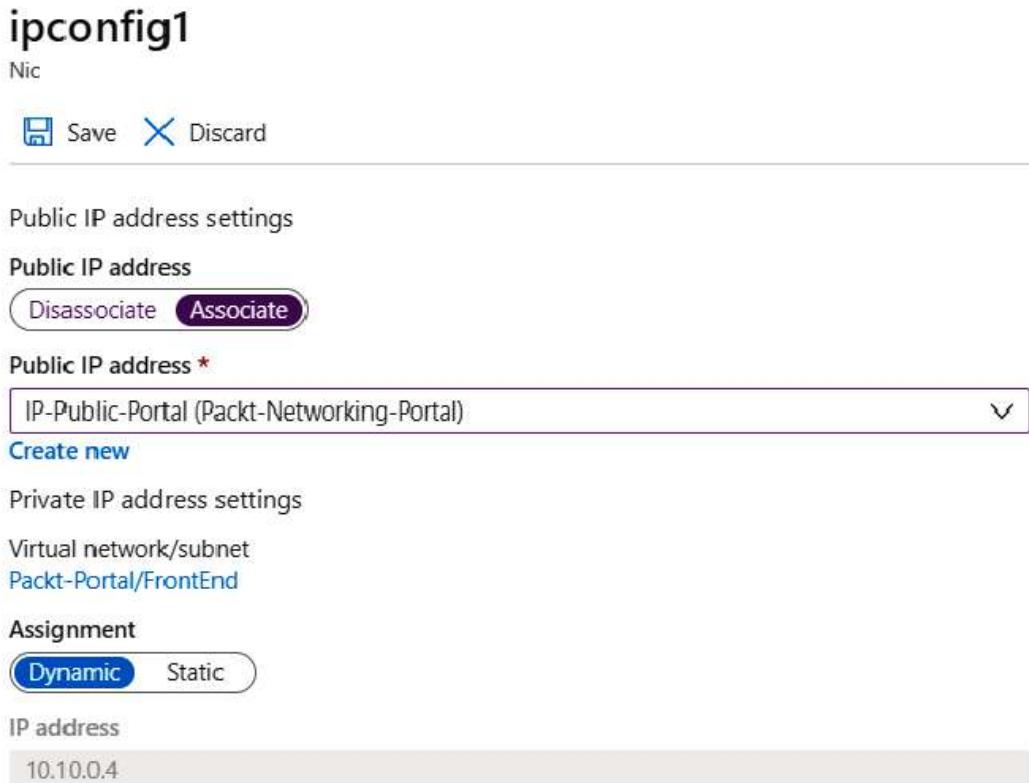


Figura 4.3: Atribuir um endereço IP público

4. Depois que o endereço IP público for selecionado, clique em **Salvar** para aplicar as configurações.

## Como funciona...

Um endereço IP público existe como um recurso separado e pode ser atribuído a um recurso a qualquer momento. Quando um endereço IP público é atribuído, você pode usar esse endereço IP para acessar serviços em execução em um recurso ao qual o endereço IP é atribuído (lembre-se de que um NSG apropriado deve ser aplicado). Também podemos remover um endereço IP de um recurso e atribuí-lo a um novo recurso. Por exemplo, se quisermos migrar serviços para uma nova VM, o endereço IP poderá ser removido da VM antiga e atribuído à nova. Dessa forma, os pontos de extremidade de serviço em execução na VM não serão alterados. Isso será útil principalmente quando endereços IP estáticos forem usados.

## Cancelar a atribuição de um endereço IP público

Um endereço IP público pode deixar de ser atribuído a um recurso a fim de ser salvo para uso posterior ou atribuído a outro recurso. Quando um recurso é excluído ou desativado, ainda podemos usar o endereço IP público e atribuí-lo ao próximo recurso.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>. Certifique-se de que a VM que está usando um endereço IP público não esteja em execução.

### Como fazer isso...

Para cancelar a atribuição de um endereço IP público, devemos fazer o seguinte:

1. Localize a NIC à qual o endereço IP público está associado.
2. No painel **Interface de rede**, accese **Configurações de IP** em **Configurações** e selecione a **Configuração de IP**:

Name	IP Version	Type	Private IP address	Public IP address	Actions
ipconfig1	IPv4	Primary	10.10.0.4 (Dynamic)	Unassigned (IP-Public-Portal)	...

Figura 4.4: Configurações de IP no painel da NIC

3. No novo painel, altere a configuração de **Endereço IP público** para **Desassociar**:

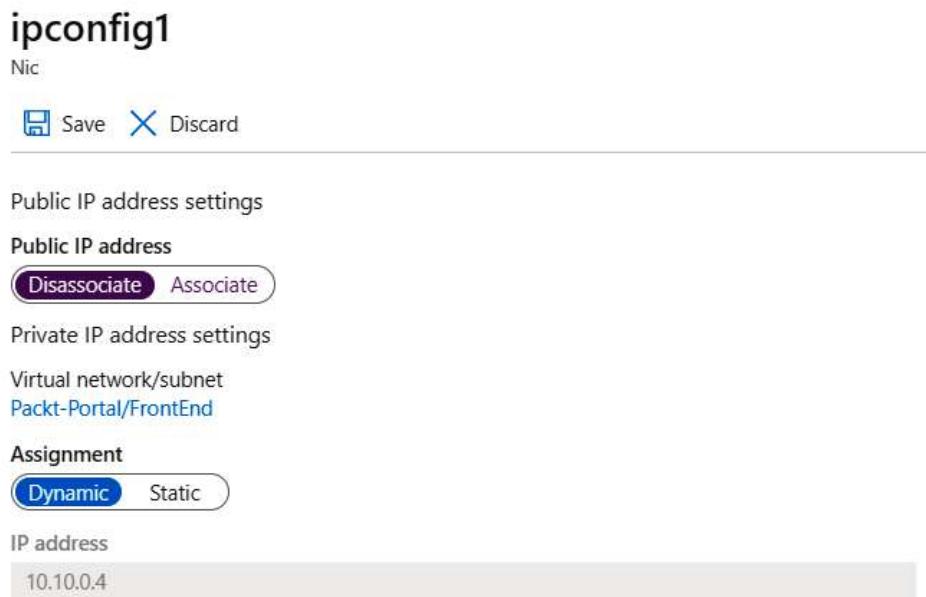


Figura 4.5: Cancelar a atribuição do endereço IP público

4. Depois que as alterações forem feitas, clique em **Salvar** para aplicar a nova configuração.

## Como funciona...

Um endereço IP público pode ser atribuído ou deixar de ser atribuído a um recurso a fim de salvá-lo para uso futuro ou para transferi-lo para um novo recurso. Para removê-lo, basta desabilitar o endereço IP público na configuração de IP na NIC à qual o endereço IP é atribuído. Isso removerá a associação, mas manterá o endereço IP como um recurso separado.

## Criar uma reserva para um endereço IP público

A opção padrão para um endereço IP público é a atribuição dinâmica de IP. Isso pode ser alterado durante a criação do endereço IP público ou posteriormente. Se for alterado da atribuição dinâmica de IP, o endereço IP público se tornará reservado (ou estático).

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma reserva para um endereço IP público, devemos seguir estas etapas:

1. Localize o endereço IP público no portal do Azure. Isso pode ser feito localizando o endereço IP diretamente ou por meio do recurso ao qual ele é atribuído (a NIC ou a VM).
2. No painel **Endereço IP público**, acesse **Configuração** em **Configurações**. Altere a **Atribuição de Dinâmica** para **Estática**, conforme mostrado na Figura 4.6:

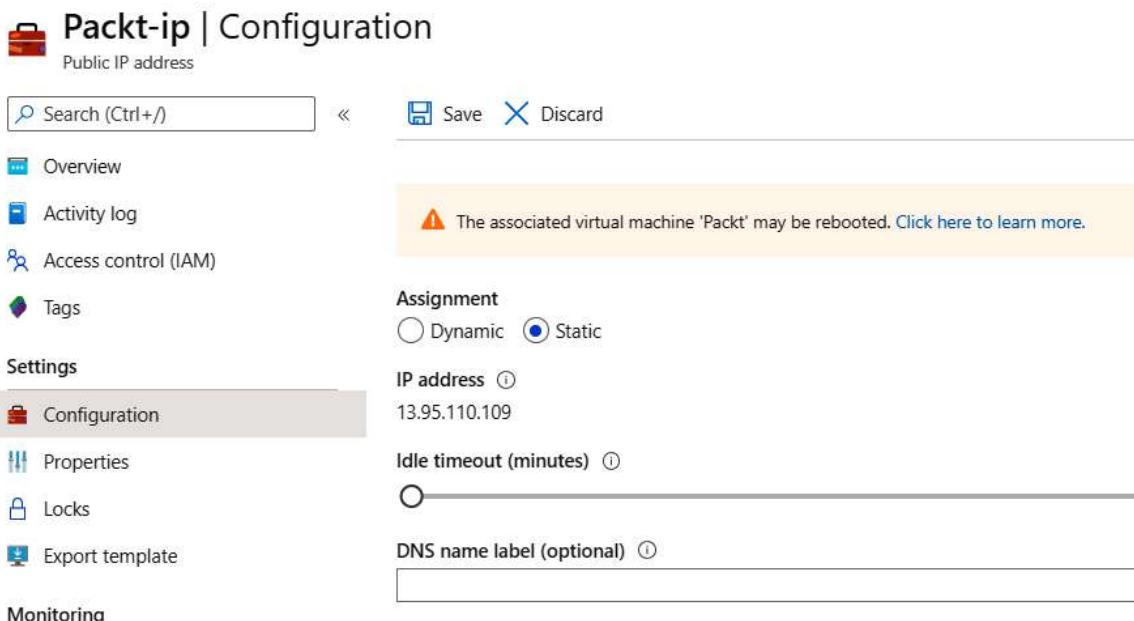


Figura 4.6: Alterar a atribuição do endereço IP público para Estática

3. Depois de fazer essa alteração, clique em **Salvar** para aplicar as novas configurações.

## Como funciona...

Um endereço IP público é definido como dinâmico por padrão. Isso significa que um endereço IP pode mudar com o tempo. Por exemplo, se uma VM à qual um endereço IP é atribuído for desativada ou reinicializada, haverá uma possibilidade de que o endereço IP seja alterado após a VM estar em execução novamente. Isso pode causar problemas se os serviços que estão sendo executados na VM forem acessados por meio do endereço IP público ou se houver um registro DNS associado ao endereço IP público.

Criamos uma reserva de IP e definimos a atribuição como estática para evitar esse cenário e manter o endereço IP reservado para nossos serviços.

## Remover uma reserva para um endereço IP público

Se o endereço IP público estiver definido como estático, poderemos remover uma reserva e definir a atribuição do endereço IP como dinâmica. Isso não é feito com frequência porque geralmente há uma razão pela qual a reserva está definida desde o início. Mas, como a reserva para o endereço IP público tem um custo adicional, às vezes há a necessidade de remover a reserva, se não for necessária.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>. Certifique-se de que o endereço IP não esteja associado a nenhum recurso.

### Como fazer isso...

Para remover uma reserva para um endereço IP público, devemos seguir estas etapas:

1. Localize o endereço IP público no portal do Azure.
2. No painel **Endereço IP público**, acesse **Configuração** em **Configurações** e defina a **Atribuição** como **Dinâmica**:

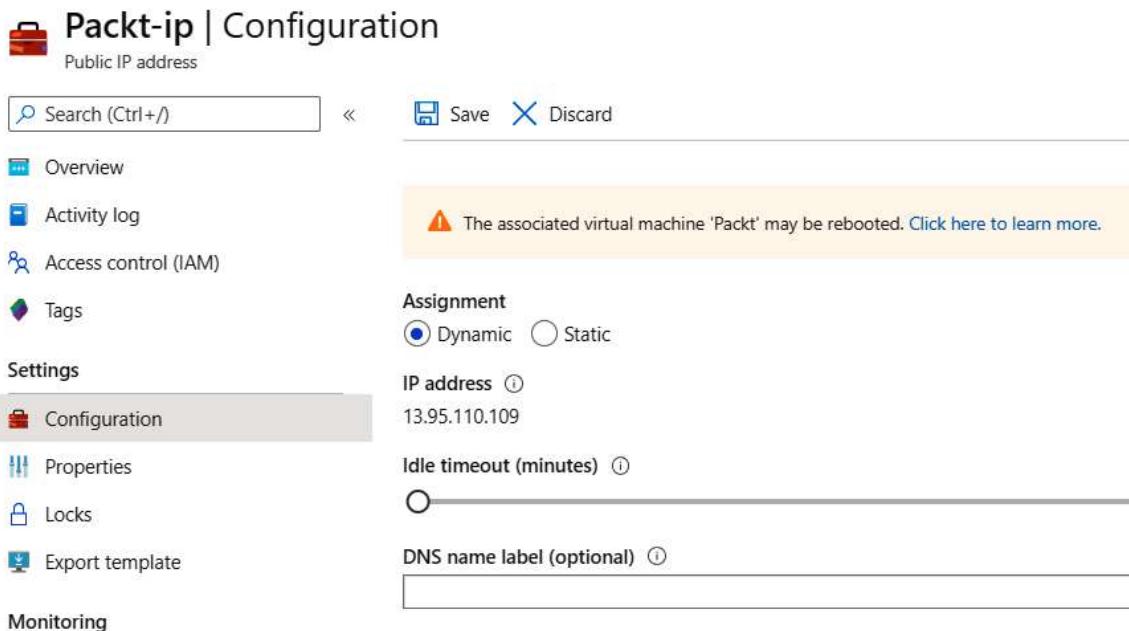


Figura 4.7: Alterar a atribuição do endereço IP público para Dinâmica

3. Depois que essas alterações forem feitas, clique em **Salvar** para aplicar a nova configuração.

## Como funciona...

Para remover uma reserva de IP de um endereço IP público, o endereço IP público não deve ser associado a um recurso. Podemos remover a reserva definindo a atribuição de endereço IP como dinâmica.

A principal razão para isso é o preço. No Azure, as cinco primeiras reservas de IP público são gratuitas. Após as cinco iniciais, cada nova reserva é cobrada. Para evitar pagamentos por recursos desnecessários, podemos remover uma reserva quando não for necessária ou quando o endereço IP público não estiver sendo usado.

## Criar uma reserva para um endereço IP privado

De forma semelhante aos endereços IP públicos, podemos fazer uma reserva para endereços IP privados. Isso geralmente é feito para garantir a comunicação entre servidores na mesma rede virtual e permitir o uso de endereços IP em cadeias de conexão.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma reserva para um endereço IP privado, devemos seguir estas etapas:

1. No portal do Azure, localize a NIC para a qual deseja fazer a reserva.
2. No painel **Interface de rede**, accese **Configurações de IP** em **Configurações** e selecione a configuração de IP:

The screenshot shows the Azure portal interface for managing network interfaces. The main title is "packt747 | IP configurations". On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Settings, IP configurations (which is selected and highlighted in grey), DNS servers, Network security group, and Properties. The main content area has tabs for Overview, IP forwarding settings, IP forwarding (with a switch set to Enabled), Virtual network (set to Packt-Portal), and IP configurations. Under IP configurations, there's a table with columns: Name, IP Version, Type, Private IP address, and Public IP address. One row is visible: ipconfig1, IPv4, Primary, 10.10.1.4 (Dynamic), 13.95.110.109 (Packt-ip). There's also a "..." button at the end of the table row.

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.10.1.4 (Dynamic)	13.95.110.109 (Packt-ip) ...

Figura 4.8: Exibir as configurações de IP no painel da NIC

3. Na novo painel, nas configurações de **Endereço IP privado**, defina a **Atribuição** como **Estática**. O valor do endereço IP atual será definido automaticamente. Se necessário, você pode alterar esse valor para outro, mas ele deve estar no espaço de endereço da sub-rede associada à NIC:



Figura 4.9: Atribuição de endereço IP privado definida como Estática

4. Depois que essas alterações forem feitas, clique em **Salvar** para aplicar a nova configuração.

## Como funciona...

Uma reserva pode ser feita para endereços IP privados. A diferença é que um endereço IP privado não existe como um recurso separado, mas é atribuído a uma NIC.

Outra diferença é que você pode selecionar um valor para um endereço IP privado. Um endereço IP público é atribuído aleatoriamente e pode ser reservado, mas você não pode escolher qual valor será. Para endereços IP privados, você pode selecionar o valor para o IP, mas ele deve ser um IP não utilizado da sub-rede associada à NIC.

## Alterar uma reserva para um endereço IP privado

Para endereços IP privados, você pode alterar o endereço IP a qualquer momento para outro valor. Com endereços IP públicos, esse não é o caso, pois você obter o endereço IP aleatoriamente de um grupo e não pode alterar o valor. Com um endereço IP privado, você pode alterar o valor para outro endereço IP do espaço de endereço.

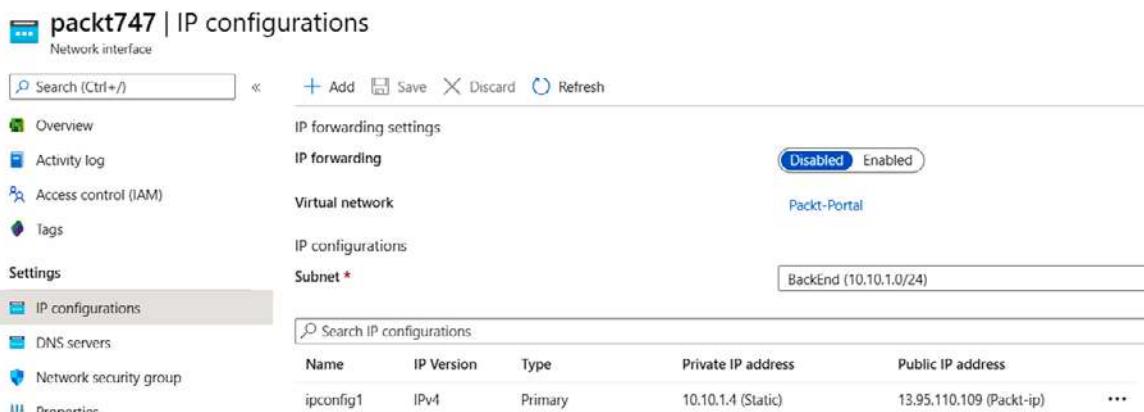
### Preparação

Antes de iniciar, abra seu navegador e accesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para alterar uma reserva para um endereço IP privado, devemos seguir estas etapas:

1. No portal do Azure, localize a NIC para a qual deseja fazer alterações.
2. No painel **Interface de rede**, accese **Configurações de IP** em **Configurações** e selecione a configuração de IP:



The screenshot shows the Azure portal interface for a network interface named 'packt747'. The left sidebar has 'IP configurations' selected under 'Settings'. The main area shows the 'IP configurations' section with a table. The table has columns: Name, IP Version, Type, Private IP address, and Public IP address. One row is visible: ipconfig1, IPv4, Primary, 10.10.1.4 (Static), and 13.95.110.109 (Packt-ip). There is also a 'Subnet' dropdown set to 'BackEnd (10.10.1.0/24)' and a 'Virtual network' dropdown set to 'Packt-Portal'. On the top right, there are buttons for 'Add', 'Save', 'Discard', and 'Refresh', and a toggle switch for 'IP forwarding' which is currently set to 'Disabled'.

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.10.1.4 (Static)	13.95.110.109 (Packt-ip)

Figura 4.10: Localizar a configuração de IP no painel Interface de rede

3. Em **Configurações de endereço IP privado**, insira um novo valor para o **Endereço IP**:

**ipconfig1**

packt747

Save Discard

**⚠** The virtual machine associated with this network interface will be restarted to utilize the new private IP address. The network interface will be re-provisioned and network configuration settings, including secondary IP addresses, subnet masks, and default gateway, will need to be manually reconfigured within the virtual machine. [Learn more](#)

Public IP address settings

Public IP address

[Disassociate](#) [Associate](#)

Public IP address \*

Packt-ip (13.95.110.109)

[Create new](#)

Private IP address settings

Virtual network/subnet

[Packt-Portal/BackEnd](#)

Assignment

[Dynamic](#) [Static](#)

IP address \*

10.10.1.8



Figura 4.11: Atribuir um novo valor para o endereço IP privado

4. Depois que essas alterações forem feitas, clique em **Salvar** para aplicar a nova configuração.

## Como funciona...

Uma reserva para um endereço IP privado pode ser alterada. Novamente, o valor deve ser um endereço IP não utilizado de uma sub-rede associada à NIC. Se a VM associada à NIC estiver desativada, o novo endereço IP será atribuído em sua próxima inicialização. Se a VM estiver em execução, ela será reiniciada para aplicar as novas alterações.

## Remover uma reserva para um endereço IP privado

De forma semelhante aos endereços IP públicos, podemos remover uma reserva para um endereço IP privado a qualquer momento. Um endereço IP privado é gratuito, portanto, os custos adicionais não são um fator nesse caso. Mas há cenários em que uma atribuição dinâmica é necessária, e podemos defini-la a qualquer momento.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para remover uma reserva para um endereço IP privado, devemos seguir estas etapas:

1. No portal do Azure, localize a NIC para a qual deseja fazer alterações.
2. No painel **Interface de rede**, accese **Configurações de IP** em **Configurações** e selecione a configuração de IP:

The screenshot shows the Azure portal interface for managing network interfaces. The main title is "packt747 | IP configurations". On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Settings, IP configurations (which is selected and highlighted in grey), DNS servers, Network security group, and Properties. The main content area has tabs for Overview, IP forwarding settings, IP forwarding, Virtual network, and IP configurations. Under IP configurations, it shows a table with one row for "ipconfig1". The table columns are Name, IP Version, Type, Private IP address, and Public IP address. The row data is: ipconfig1, IPv4, Primary, 10.10.1.8 (Static), 13.95.110.109 (Packt ip). There are also "Add", "Save", "Discard", and "Refresh" buttons at the top of the IP configurations section. A "Disabled" button is shown next to the IP forwarding settings tab, which is currently active.

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.10.1.8 (Static)	13.95.110.109 (Packt ip)

Figura 4.12: Selecionar a configuração de IP no painel Interface de rede

- No novo painel, em **Configurações de endereço IP privado**, altere **Atribuição** para **Dinâmica**:

The screenshot shows the 'ipconfig1' configuration interface. At the top, there are 'Save' and 'Discard' buttons. A warning message states: 'The virtual machine associated with this network interface will be restarted to utilize the new private IP address. The network interface will be re-provisioned and network configuration settings, including secondary IP addresses, subnet masks, and default gateway, will need to be manually reconfigured within the virtual machine.' Below this, under 'Public IP address settings', the 'Associate' button is highlighted. The 'Public IP address \*' dropdown contains 'Packt-ip (13.95.110.109)'. There is a 'Create new' link. Under 'Private IP address settings', the 'Virtual network/subnet' is set to 'Packt-Portal/BackEnd'. The 'Assignment' section has 'Dynamic' selected. The 'IP address' dropdown is set to 'Unassigned'.

Figura 4.13: Atribuição de endereço IP privado definida como Dinâmica

- Depois que essas alterações forem feitas, clique em **Salvar** para aplicar a nova configuração.

## Como funciona...

Podemos remover uma reserva de endereço IP privada a qualquer momento, mudando a **Atribuição** para **Dinâmica**. Quando essa alteração for feita, a VM associada à NIC será reiniciada para aplicar as novas alterações. Depois que uma alteração for feita, um endereço IP privado poderá ser alterado após a VM ser reiniciada ou desativada.

## Adicionar vários endereços IP a uma NIC

Em várias situações, talvez seja necessário ter vários endereços IP associados a uma única NIC. No Azure, isso é possível para endereços IP públicos e privados.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

1. No portal do Azure, localize a NIC para a qual deseja fazer alterações.
2. No painel **Interface de rede**, acesse **Configurações de IP** em **Configurações** e clique em **Adicionar**:

The screenshot shows the 'Nic | IP configurations' page in the Azure portal. The left sidebar has 'IP configurations' selected under 'Settings'. The main area shows an 'Overview' card with 'IP forwarding settings' (Enabled), 'Activity log', 'Access control (IAM)', and 'Tags'. Below it is a 'Virtual network' card with 'Subnet \*' set to 'FrontEnd (10.10.0.0/25)'. A 'Packt-Portal' tag is also present. On the right, there's a table titled 'IP configurations' with one row:

Name	IP Version	Type	Private IP address	Public IP address	⋮
ipconfig1	IPv4	Primary	10.10.0.4 (Dynamic)	Unassigned (IP-Public-Portal)	⋮

Figura 4.14: O painel Interface de rede

3. Um novo painel para configuração de IP será exibido. Precisamos fornecer valores para os campos **Nome** e **Tipo** (**Tipo** estará acinzentado se outra configuração de IP já existir) e precisamos selecionar algumas configurações de endereço IP. Se somente um endereço IP privado for necessário, basta selecionar a **Alocação** do endereço privado e clicar em **Criar**:

**Add IP configuration** X

Nic

Name **\***  
 ✓

Type  
 Primary  Secondary

**Info:** Primary IP configuration already exists

Private IP address settings

Allocation  
 Dynamic  Static

Public IP address  
 Disassociate  Associate

Figura 4.15: Adicionar a configuração de IP à NIC

4. Se um endereço IP público adicional for necessário, precisaremos selecionar **Associar** em **Endereço IP público**. Devemos fornecer informações adicionais para **Nome**, **SKU** e o tipo **Atribuição**:

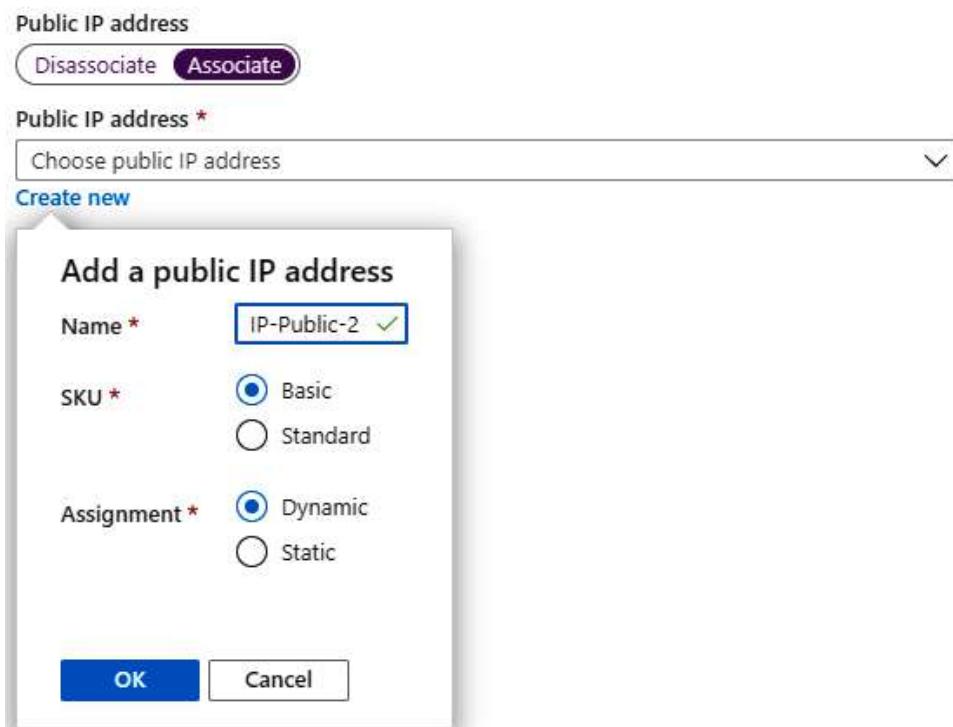


Figura 4.16: Adicionar o novo endereço IP público

## Como funciona...

Cada NIC pode ter várias configurações de IP atribuídas. Cada configuração de IP deve ter um endereço IP privado e pode ter um endereço IP público. Assim, é possível adicionar um endereço IP privado sem um endereço IP público, mas não o contrário. Isso fornece diferentes opções de roteamento e a capacidade de se comunicar com diferentes aplicações e serviços em diferentes endereços IP. O roteamento será explicado mais detalhadamente no Capítulo 6: DNS e roteamento.

## Criar um prefixo de IP público

A criação de novos recursos geralmente está associada à criação de novos endereços IP. Pode haver problemas quando os endereços IP públicos precisam ser associados a regras de firewall ou configurações de aplicativos. Para superar isso, podemos criar um prefixo IP público e reservar uma grande variedade de endereços IP que serão atribuídos aos nossos recursos.

### Como fazer isso...

Para criar um novo prefixo de IP público, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Prefixo de IP público** nos serviços de **Rede** (ou pesquise **prefixo de IP público** na barra de pesquisa).
2. Precisamos fornecer informações para **Assinatura**, **Grupo de recursos**, **Nome**, **Região** e **Versão IP**. **SKU** não é selecionável e é definido como **Padrão**. Para o **Tamanho do prefixo**, definimos quantos endereços IP desejamos reservar:

### Create a public IP prefix

**Basics** Tags Review + create

A Public IP prefix is a range of contiguous static public IP addresses. Azure allocates a static range of addresses to your subscription based on how many you specify. This allows you to associate public IP addresses to virtual machines, load balancers, or other resources from a predictable range that will not change when moved or dissociated from the resource. [Learn more.](#)

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal [Create new](#)

**Instance details**

Name \* IP-prefix

Region \* (Europe) West Europe

SKU Standard

IP version IPv4 IPv6

Prefix size \* /28 (16 addresses)

- /28 (16 addresses)
- /29 (8 addresses)
- /30 (4 addresses)
- /31 (2 addresses)

Figura 4.17: Criar um prefixo de IP público

## Como funciona...

Quando criamos um prefixo de IP público, a associação de endereços IP públicos não é feita aleatoriamente, mas sim com base em um conjunto de endereços reservados para nós. Em muitos aspectos, isso age de forma semelhante à criação de uma rede virtual e à definição de um espaço de endereço IP privado, somente com endereços IP públicos. Isso pode ser muito útil quando precisamos obter endereços com antecedência. Por exemplo, digamos que precisamos criar uma regra de firewall para cada serviço que criamos. Isso exigiria que esperássemos que cada serviço fosse implantado e obtivesse um endereço IP público depois que ele foi criado. Com um prefixo de IP público, os endereços IP são obtidos antecipadamente e podemos definir uma regra para uma grande variedade de endereços IP, em vez de fazê-lo para cada IP.



# 5

## Gateways de rede local e virtual

Os gateways de rede local e virtual são gateways de **rede privada virtual (VPN)** que são usados para se conectarem a redes na infraestrutura local e criptografarem todo o tráfego entre a **Rede Virtual do Azure (VNet)** e uma rede local. Cada rede virtual pode ter apenas um gateway de rede virtual, mas ele pode ser usado para configurar várias conexões VPN.

Abordaremos as seguintes receitas neste capítulo:

- Criar um gateway de rede local no portal do Azure
- Criar um gateway de rede local com o PowerShell
- Criar um gateway de rede virtual no portal do Azure
- Criar um gateway de rede virtual com o PowerShell
- Modificar as configurações do gateway de rede local

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Azure PowerShell

Os exemplos de código podem ser encontrados no

[https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/  
tree/master/Chapter05](https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter05).

## Criar um gateway de rede local no portal do Azure

Quando uma conexão site a site é criada, temos que fornecer a configuração para ambos os lados da conexão, ou seja, o Azure e a infraestrutura local.

Embora um gateway de rede local seja criado no Azure, ele representa a rede local (na infraestrutura local) e contém informações de configuração nas definições de rede local. É um componente essencial para criar a conexão VPN necessária para criar uma conexão site a site entre a rede virtual e a rede local.

## Preparação

Antes de iniciar, abra um navegador da Web e accesse o portal do Azure em  
<https://portal.azure.com>.

## Como fazer isso...

Para criar um novo gateway de rede local, as seguintes etapas são necessárias:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Gateway de rede local** nos serviços de **Rede** (ou pesquise **gateway de rede local** na barra de pesquisa).
2. Os parâmetros que precisamos fornecer são **Nome**, **Endereço IP** (ou seja, o endereço IP público do firewall local), **Espaço de endereço** (o espaço de endereço local ao qual você deseja se conectar), **Assinatura**, **Grupo de recursos** e **Local**. Opcionalmente, podemos definir as configurações de **Border Gateway Protocol (BGP)**:

## Create local network gateway

Name \*

 ✓

IP address \* ⓘ

 ✓

Address space ⓘ

192.168.1.0/24 ...  
Add additional address range ...

Configure BGP settings

Subscription \*

 ▼

Resource group \* ⓘ

 ▼

[Create new](#)

Location \*

 ▼

Figura 5.1: Criar um novo gateway de rede local

### Como funciona...

O gateway de rede local é usado para conectar um gateway de rede virtual a uma rede na infraestrutura local. O gateway de rede virtual é diretamente conectado à rede virtual e tem todas as informações relevantes da VNet do Azure necessárias para criar uma conexão VPN. Por outro lado, um gateway de rede local contém todas as informações de rede local necessárias para criar uma conexão VPN.

Nesta receita, criamos um gateway de rede local no portal do Azure. Na próxima receita, aprenderemos a fazer o mesmo usando o PowerShell.

## Criar um gateway de rede local com o PowerShell

Conforme mencionado na receita anterior, o gateway de rede local contém informações sobre a rede local que queremos conectar a uma VNet do Azure. Além de criar um gateway de rede local por meio do portal do Azure, podemos criá-lo com o Azure PowerShell.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

### Como fazer isso...

Para criar um novo gateway de rede local, execute o seguinte comando:

```
New-AzLocalNetworkGateway -Name packt-lng-script -ResourceGroupName 'Packt-Networking-Script' -Location 'westeurope' -GatewayIpAddress '195.222.10.20' -AddressPrefix '192.168.1.0/24'
```

### Como funciona...

Para implantar um novo gateway de rede local, precisamos fornecer parâmetros para o nome, o grupo de recursos, o local, o endereço IP do gateway e o prefixo de endereço que queremos. O endereço IP do gateway é o endereço IP público do firewall local ao qual você está tentando se conectar. O prefixo do endereço é o prefixo de sub-rede da rede local à qual você está tentando se conectar. Esse endereço deve ser associado a um endereço de firewall fornecido como um endereço IP de gateway.

Nesta receita, criamos um gateway de rede local com o Azure PowerShell.

Vamos avançar para a próxima receita e aprender a criar um gateway de rede virtual no portal do Azure.

## Criar um gateway de rede virtual no portal do Azure

Depois que um gateway de rede local for criado, precisaremos criar um gateway de rede virtual para criar uma conexão VPN entre as redes locais e do Azure. Como um gateway de rede local contém informações sobre a rede local, o gateway de rede virtual contém informações para a VNet do Azure à qual estamos tentando nos conectar.

### Preparação

Antes de iniciar, abra um navegador da Web e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar um novo gateway de rede virtual, as seguintes etapas são necessárias:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Gateway de rede virtual** nos serviços de **Rede** (ou pesquise **gateway de rede virtual** na barra de pesquisa).
2. Tudo é feito em um único painel, mas com a finalidade de obter uma melhor visibilidade, vamos dividir em duas seções. Na primeira seção, precisamos fornecer **Assinatura**, **Nome**, **Região**, **Tipo de gateway**, **Tipo de VPN**, **SKU** e **Geração**, (a opção **Geração** depende da SKU; nem todas as SKUs são compatíveis com a **Geração 2**) e precisamos selecionar a **Rede virtual** que será usada na conexão. Observe que a sub-rede do gateway deve ser criada antes disso, e somente as redes virtuais com uma sub-rede de gateway estarão disponíveis para seleção. Um exemplo é mostrado em Figura 5.2:

### Create virtual network gateway

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Microsoft Azure Sponsorship	▼
Resource group ⓘ	Packt-Networking-Portal (derived from virtual network's resource group)	

**Instance details**

Name *	packt-vng-portal	✓
Region *	(Europe) West Europe	
Gateway type * ⓘ	<input checked="" type="radio"/> VPN	<input type="radio"/> ExpressRoute
VPN type * ⓘ	<input checked="" type="radio"/> Route-based	<input type="radio"/> Policy-based
SKU * ⓘ	VpnGw1	
Generation ⓘ	Generation1	
Virtual network * ⓘ	Packt-Portal	
<a href="#">Create virtual network</a>		
Subnet ⓘ	GatewaySubnet (10.10.2.0/24)	

**💡** Only virtual networks in the currently selected subscription and region are listed.

Figura 5.2: Criar um novo gateway de rede virtual

3. Na segunda seção, precisamos definir as opções de **Endereço IP público** (selecione um endereço IP existente ou crie um novo) e, opcionalmente, podemos definir **Ativar modo ativo-ativo** e **Número do sistema autônomo do Border Gateway Protocol (ASN do BGP)**:

**Public IP address**

Public IP address \*  Create new  Use existing

Public IP address name \*

Public IP address SKU Basic

Assignment  Dynamic  Static

Enable active-active mode \*  Enabled  Disabled

Configure BGP ASN \*  Enabled  Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

Figura 5.3: Definir as opções de endereço IP público

4. Após a validação, podemos clicar em **Criar** e iniciar a implantação. Observe que a criação do gateway de rede virtual demora mais do que a maioria dos outros recursos do Azure. A implantação pode demorar de 45 a 90 minutos.

## Como funciona...

O gateway de rede virtual é a segunda parte necessária para estabelecer a conexão com a VNet do Azure. Ele é diretamente conectado à rede virtual e é necessário para criar conexões site a site e ponto a site. Precisaremos definir o tipo de VPN, que precisa corresponder ao tipo de dispositivo VPN local quando uma conexão site a site for criada.

O modo ativo-ativo fornece alta disponibilidade associando dois endereços IP com configurações de gateway separadas para garantir o tempo de atividade.

O Border Gateway Protocol é um protocolo padrão para a troca de informações de roteamento e acessibilidade entre diferentes **sistemas autônomos (ASes)**. Cada sistema recebe um **número de sistema autônomo (ASN)**.

Nesta receita, criamos um gateway de rede virtual no portal do Azure. Vamos avançar para a próxima receita.

## Criar um gateway de rede virtual com o PowerShell

É possível criar um gateway de rede virtual com o PowerShell. Novamente, isso ajuda a automatizar processos. Por exemplo, se começarmos a criar um gateway de rede virtual usando um portal e percebermos que nossa rede virtual não está listada, provavelmente é porque está faltando uma sub-rede de gateway. Por isso, devemos abandonar o processo, voltar, criar a sub-rede do gateway e começar a criar o gateway de rede virtual. Usando o PowerShell, podemos garantir que todos os recursos necessários estejam presentes antes de iniciar e prosseguir com a criação do gateway de rede virtual.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

### Como fazer isso...

Para criar um novo gateway de rede virtual, execute o seguinte script:

```
$vnet = Get-AzVirtualNetwork -ResourceGroupName 'Packt-Networking-Script'  
-Name 'Packt-Script'  
  
Add-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -AddressPrefix  
10.11.2.0/27 -VirtualNetwork $vnet  
  
$vnet | Set-AzVirtualNetwork  
  
$gwpip = New-AzPublicIpAddress -Name VNet1GWIP -ResourceGroupName 'Packt-  
Networking-Script' -Location 'westeurope' -AllocationMethod Dynamic  
  
  
$vnet = Get-AzVirtualNetwork -ResourceGroupName 'Packt-Networking-Script'  
-Name 'Packt-Script'  
  
$subnet = Get-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet'  
-VirtualNetwork $vnet  
  
$gwipconfig = New-AzVirtualNetworkGatewayIpConfig -Name gwipconfig1 -SubnetId  
$subnet.Id -PublicIpAddressId $gwpip.Id  
  
New-AzVirtualNetworkGateway -Name VNet1GW -ResourceGroupName 'Packt-  
Networking-Script' -Location 'westeurope' -IpConfigurations $gwipconfig  
-GatewayType Vpn -VpnType RouteBased -GatewaySku VpnGw1
```

## Como funciona...

O script executa algumas operações diferentes a fim de garantir que todos os requisitos sejam atendidos para que possamos criar um gateway de rede virtual. A primeira etapa é coletar informações sobre a rede virtual que vamos usar. Em seguida, adicionamos a sub-rede do gateway à VNet do Azure e criamos um endereço IP público que será usado pelo gateway de rede virtual. Coletamos todas as informações, garantimos que todos os recursos necessários estejam presentes e, por fim, criamos um novo gateway de rede virtual.

Nesta receita, aprendemos a criar um gateway de rede virtual com o Azure PowerShell. Na próxima receita, aprenderemos a modificar as configurações do gateway de rede local.

## Modificar as configurações do gateway de rede local

As configurações de rede podem mudar com o tempo, e talvez seja necessário abordar essas alterações no Azure também. Por exemplo, o endereço IP público de um firewall local pode mudar e, por isso, precisaremos reconfigurar o gateway de rede local, ou uma rede local pode ser reconfigurada e o espaço de endereço ou a sub-rede mudou e, por isso, precisaremos reconfigurar o gateway de rede local mais uma vez.

### Preparação

Antes de iniciar, abra um navegador da Web e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para modificar as configurações do gateway de rede local, devemos fazer o seguinte:

1. Localize o gateway de rede local no portal do Azure e accese **Configuração**.
2. Na **Configuração**, podemos editar o **Endereço IP** ou o **Espaço de endereço**. Também poderemos adicionar espaços de endereço adicionais se quisermos conectar várias sub-redes locais à VNet do Azure:

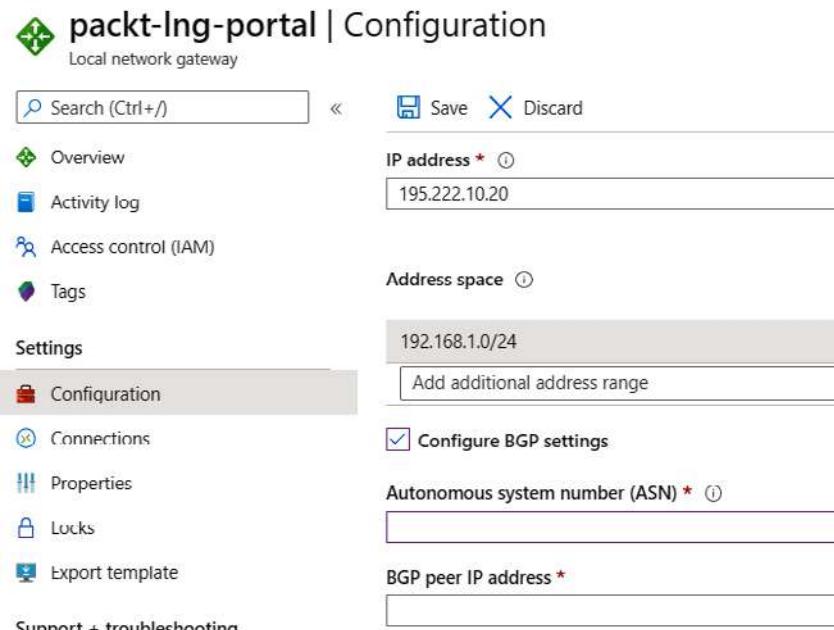


Figura 5.4: Modificar as configurações do gateway de rede local

## Como funciona...

O gateway de rede local contém as informações da rede local necessárias para criar uma conexão site a site entre as redes locais e do Azure. Se essas informações forem alteradas, poderemos editá-las nas definições de **Configuração**. As alterações que podem ser feitas são o endereço IP (ou seja, o endereço IP público do firewall local) e o espaço de endereço ao qual estamos nos conectando. Além disso, poderemos adicionar ou remover espaços de endereço se quisermos adicionar ou remover sub-redes que podem se conectar à VNet do Azure. Se a configuração no gateway de rede local não for mais válida, ainda poderemos usá-la para criar uma conexão completamente nova com uma nova rede local, se necessário.



# 6

# DNS e roteamento

O DNS do Azure permite hospedar domínios do **Sistema de Nomes de Domínio (DNS)** no Azure. Ao usar o DNS do Azure, usamos a infraestrutura da Microsoft para a resolução de nomes, o que resulta em consultas DNS rápidas e confiáveis. A infraestrutura de DNS do Azure usa um grande número de servidores para fornecer ótima confiabilidade e disponibilidade de serviço. Usando a rede Anycast, cada consulta DNS é atendida pelo servidor DNS mais próximo disponível para fornecer uma resposta rápida.

Abordaremos as seguintes receitas neste capítulo:

- Criar uma zona DNS do Azure
- Criar uma zona privada DNS do Azure
- Integrar uma rede virtual a uma zona privada DNS
- Criar um novo conjunto de registros no DNS do Azure
- Criar uma tabela de rotas
- Alterar uma tabela de rotas
- Associar uma tabela de rotas a uma sub-rede
- Dissociar uma tabela de rotas de uma sub-rede
- Criar uma nova rota
- Alterar uma rota
- Excluir uma rota

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure

## Criar uma zona DNS do Azure

Para começar a usar o DNS do Azure, primeiro devemos criar uma zona DNS. Uma zona DNS contém um registro DNS para um domínio específico e pode conter registros para um único domínio por vez. Uma zona DNS conterá registros DNS para esse domínio e possíveis subdomínios. Os servidores de nomes DNS são configurados para responder a qualquer consulta em um domínio registrado e apontam para um destino.

### Preparação

Antes de iniciar, abra seu navegador e accesse o portal do Azure em  
<https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova zona DNS do Azure com o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Zona DNS** em serviços de **Rede** (ou pesquise **Zona DNS** na barra de pesquisa).
2. No novo painel, devemos inserir informações para os campos **Assinatura, Grupo de recursos** e **Nome**. Se selecionarmos um grupo de recursos existente, a região será automaticamente a mesma que aquele do grupo de recursos selecionado. Opcionalmente, poderemos marcar essa zona se o filho de uma zona existente estiver hospedado no DNS do Azure. O nome deve ser um **Nome de Domínio Totalmente Qualificado (FQDN)**:

## Create DNS zone

**Basics** Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more](#).

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal [Create new](#)

**Instance details**

This zone is a child of an existing zone already hosted in Azure DNS [ⓘ](#)

Name \* toroman.cloud ✓

Resource group location ⓘ West Europe

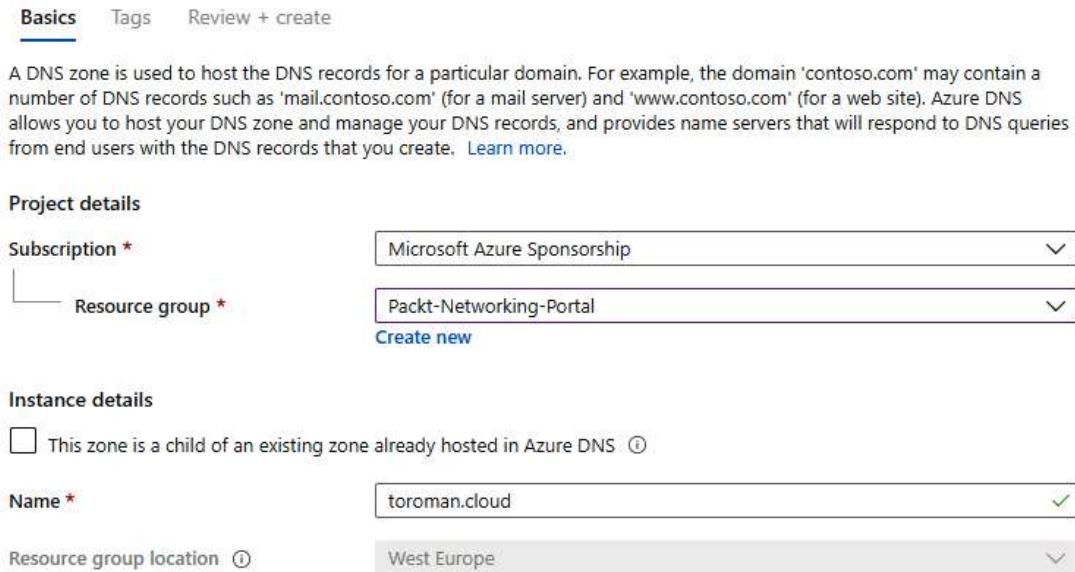


Figura 6.1: Criar uma nova zona DNS do Azure com o portal do Azure

## Como funciona...

Uma zona DNS é necessária para começar a usar o DNS do Azure. Uma nova zona DNS é necessária para cada domínio que queremos hospedar com o DNS do Azure, pois uma única zona DNS pode conter informações para um único domínio. Depois de criar uma zona DNS, podemos adicionar registros, conjuntos de registros e tabelas de rotas a um domínio hospedado com o DNS do Azure. Usando-os, podemos rotear o tráfego e definir destinos usando um FQDN para recursos do Azure (e outros recursos também). Mostraremos como criá-los e gerenciá-los nas próximas receitas deste capítulo.

Vamos avançar para a próxima receita para aprender a criar uma zona privada DNS.

## Criar uma zona privada DNS do Azure

Uma zona privada DNS do Azure funciona de forma semelhante a uma zona DNS. No entanto, em vez de funcionar em registros públicos, ela funciona dentro de uma rede virtual. Ela é usada para resolver nomes e domínios personalizados dentro de sua rede virtual do Azure.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova zona DNS do Azure com o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Zona privada DNS** em serviços de **Rede** (ou pesquise **Zona privada DNS** na barra de pesquisa).
2. No novo painel, devemos inserir informações para os campos **Assinatura**, **Grupo de recursos** e **Nome**. Se selecionarmos um grupo de recursos existente, a região será automaticamente a mesma que aquele do grupo de recursos selecionado. O nome deve ser um FQDN:

### Create DNS zone

**Basics** Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more](#).

**Project details**

**Subscription \*** Microsoft Azure Sponsorship

**Resource group \*** Packt-Networking-Portal [Create new](#)

**Instance details**

This zone is a child of an existing zone already hosted in Azure DNS [①](#)

**Name \*** toroman.cloud ✓

**Resource group location** [①](#) West Europe

Figura 6.2: Criar uma nova zona privada DNS do Azure com o portal do Azure

## Como funciona...

Quando uma rede virtual for criada, uma zona DNS padrão será disponibilizada. A zona DNS padrão usa nomes fornecidos pelo Azure, e devemos usar uma zona privada DNS para usar nomes personalizados. Uma zona privada DNS também é necessária para a resolução de nomes em todas as redes virtuais, pois o DNS padrão não oferece suporte a essa opção.

Vamos avançar para a próxima receita para aprender a integrar uma rede virtual a uma zona privada DNS.

## Integrar uma rede virtual a uma zona privada DNS

Quando uma zona privada DNS é criada, é um serviço autônomo que não tem muitas funções por conta própria. Devemos integrá-la a uma rede virtual para começar a usá-la. Depois de integrada, fornecerá o DNS dentro da rede virtual.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para adicionar um novo registro à zona DNS, devemos usar as seguintes etapas:

1. No portal do Azure, localize a **Zona privada DNS**.
2. Na **Zona privada DNS**, selecione **Links de rede virtual** e clique em **Adicionar**:

The screenshot shows the Azure portal interface for managing a Private DNS zone named 'toroman.cloud'. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Below the sidebar, 'Virtual network links' is selected. At the top right, there are 'Search (Ctrl+ /)', 'Add', and 'Refresh' buttons. The main area displays a table with one row: 'Link Name' (empty) and 'No results.' below it. The 'Add' button is highlighted with a blue border.

Figura 6.3: Adicionar um link de rede virtual

3. No novo painel, preencha o **Nome do link** e selecione valores para os campos **Assinatura** e **Rede virtual** (somente as redes virtuais na assinatura selecionada estarão disponíveis). Como alternativa, podemos fornecer a ID do recurso de nossa rede virtual, em vez de selecionar opções no menu suspenso:

The screenshot shows the 'Add virtual network link' configuration page. At the top, it says 'Link name \*' with 'Link1' entered. Below that is a note: 'Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.' Under 'Subscription \*', 'Microsoft Azure Sponsorship' is selected. Under 'Virtual network \*', 'packtdemoVM-Vnet (packt-demo)' is selected. In the 'Configuration' section, 'Enable auto registration' is checked. There are also 'Link properties' and 'Next Step' buttons at the bottom.

Link name \*

Link1

Virtual network details

Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.

I know the resource ID of virtual network

Subscription \*

Microsoft Azure Sponsorship

Virtual network \*

packtdemoVM-Vnet (packt-demo)

Configuration

Enable auto registration

Figura 6.4: Adicionar um link de rede virtual

## Como funciona...

Depois que a rede virtual estiver vinculada à zona privada DNS, a zona poderá ser usada para a resolução de nomes dentro da rede virtual conectada. Para a resolução de nomes em várias redes virtuais conectadas, devemos usar uma zona privada DNS, pois o DNS padrão não oferece suporte à resolução em todas as redes. O mesmo se aplica se a rede estiver conectada a uma rede na infraestrutura local.

Se habilitamos o registro automático em **Configuração**, as máquinas virtuais recém-criadas serão automaticamente registradas na zona privada DNS. Caso contrário, devemos adicionar cada novo recurso manualmente.

Vamos avançar para a próxima receita para aprender a criar um novo registro definido no DNS do Azure.

## Criar um novo conjunto de registros no DNS do Azure

Ao criar uma zona DNS, definimos o domínio para o qual vamos armazenar registros. Uma zona DNS é criada para um domínio **raiz** definido com um FQDN. Podemos adicionar subdomínios adicionais e adicionar registros para armazenar informações sobre outros recursos no mesmo domínio.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar um novo registro à zona DNS, devemos usar as seguintes etapas:

1. No portal do Azure, localize a **Zona DNS**.
2. Em **Visão geral**, selecione a opção para adicionar um conjunto de registros:

Figura 6.5: Adicionar um conjunto de registros na zona DNS

3. Um novo painel será aberto. Insira o nome do subdomínio ao qual você deseja adicionar um registro:

Name	demo
Type	A
Alias record set	<input type="radio"/> Yes <input checked="" type="radio"/> No
TTL *	1
TTL unit	Hours
IP address	0.0.0.0 ...

Figura 6.6: Adicionar um subdomínio para o registro

4. Precisamos selecionar o tipo de registro que queremos adicionar. As opções são **A**, **AAAA**, **CNAME**, **MX**, **NS**, **SRV**, **TXT** e **PTR**. O tipo de registro mais comum é **A**, por isso, vamos selecioná-lo:

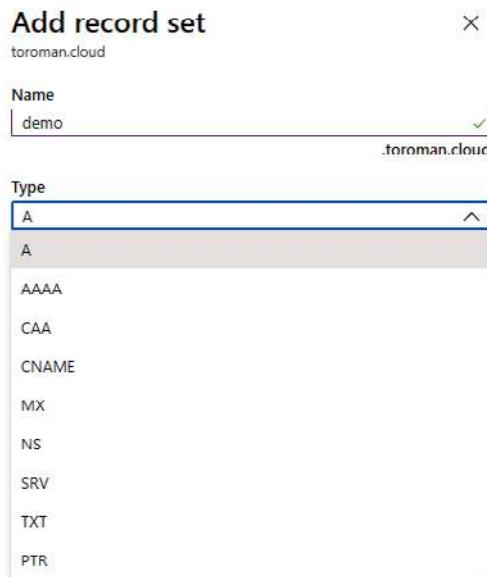


Figura 6.7: Selecionar o tipo de registro

5. Depois que selecionarmos o tipo de registro, precisaremos selecionar um alias (aliases estão disponíveis somente para os tipos **A**, **AAAA** e **CNAME**) e a opção **TTL (Time-To-Live)**. Por fim, adicionamos um destino de registro. Isso depende do tipo de registro e, no caso do registro **A**, será um endereço IP:

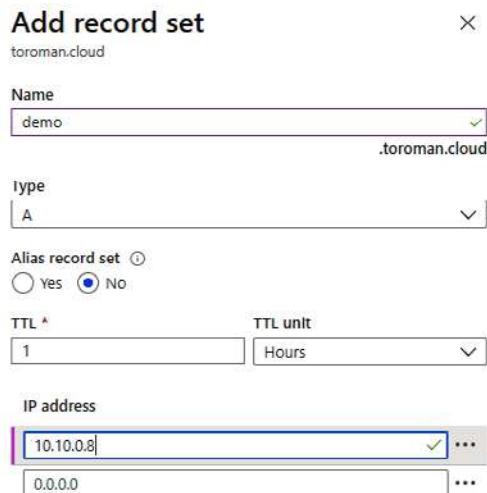


Figura 6.8: Adicionar um alias, TTL e destino de registro

6. Se escolhermos **CNAME** como tipo de registro, não estaremos inserindo um endereço IP, mas sim um alias. Quando uma consulta for feita para o registro, em vez de um endereço IP, uma URL será retornada e o cliente será direcionado para esse registro:

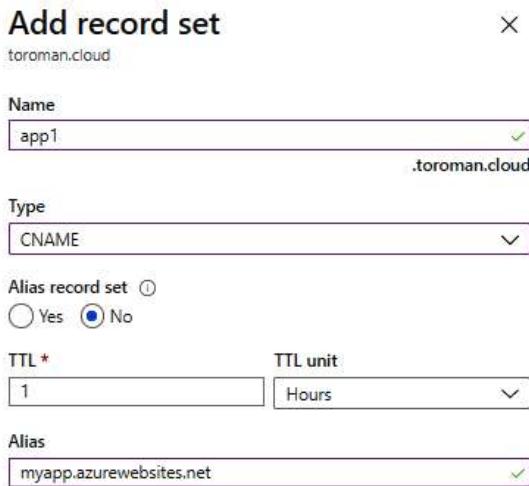


Figura 6.9: Adicionar um registro CNAME

7. Adicionar uma única entrada ao nosso registro cria um novo conjunto de registros e um novo registro. Podemos adicionar mais registros ao conjunto de registros, adicionando mais endereços IP (nesse caso).

## Como funciona...

Um conjunto de registros DNS contém informações sobre o subdomínio no domínio hospedado com a zona DNS. Nesse caso, o domínio seria **toroman.cloud**, e o subdomínio seria **test**. Isso forma um FQDN, **demo.toroman.cloud**, e o registro aponta esse domínio para o endereço IP que definimos. O conjunto de registros pode conter vários registros para um único subdomínio, geralmente usado para redundância e disponibilidade.

O uso de um **CNAME** e/ou um alias pode ser feito com o Gerenciador de Tráfego do Azure. Dessa forma, os nomes de domínio personalizados podem ser usados para a resolução de nomes, em vez dos nomes padrão fornecidos pelo Azure.

Nesta receita, você aprender a criar um novo registro no DNS do Azure. Vamos avançar para a próxima receita para aprender a criar uma tabela de rotas.

## Criar uma tabela de rotas

O Azure roteia o tráfego de rede em sub-redes por padrão. No entanto, queremos usar rotas de tráfego personalizadas para definir onde e como o tráfego flui. Nesses casos, usamos **tabelas de rotas**. Uma tabela de rotas define o próximo salto para o tráfego e determina onde o tráfego de rede precisa ir.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar um novo registro à zona DNS, devemos usar as seguintes etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Tabela de rotas** em serviços de **Rede** (ou pesquise **tabela de rotas** na barra de pesquisa).
2. No novo painel, precisamos selecionar opções para **Assinatura**, **Grupo de recursos** e **Região** e fornecer o nome da tabela de rotas. Opcionalmente, podemos definir se queremos permitir a propagação de rotas do gateway (que é habilitada por padrão):

### Create Route table

**Basics** Tags Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Microsoft Azure Sponsorship

Resource group \* Packt-Networking-Portal

Create new

**Instance details**

Region \* West Europe

Name \* Routetable-Portal

Propagate gateway routes \* Yes

Figura 6.10: Criar uma tabela de rotas

## Como funciona...

O roteamento de rede na Rede Virtual do Azure é feito automaticamente, mas podemos usar o roteamento personalizado com tabelas de rotas. As tabelas de rotas usam regras e associações de sub-rede para definir o fluxo de tráfego na Rede Virtual. Quando uma nova tabela de rotas é criada, nenhuma configuração é criada, apenas um recurso vazio. Depois que o recurso for criado, precisaremos definir regras e sub-redes a fim usar uma tabela de rotas para o fluxo de tráfego. Mostraremos nas próximas receitas deste capítulo como criamos e aplicamos regras em tabelas de rotas.

## Alterar uma tabela de rotas

Como mencionado na receita anterior, criar uma nova tabela de rotas resultará em um recurso vazio. Depois que um recurso for criado, poderemos alterar as configurações conforme necessário. Antes de configurarmos as rotas e sub-redes associadas à tabela de rotas, a única configuração que podemos alterar é a propagação de rotas **Border Gateway Protocol (BGP)**. Também podemos alterar outras configurações após a criação.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para alterar uma tabela de rotas, devemos fazer o seguinte:

1. No portal do Azure, localize a **Tabela de rotas**.
2. Em **Configurações**, podemos alterar as configurações de **Propagar de rotas de gateway** no painel **Configuração** a qualquer momento:

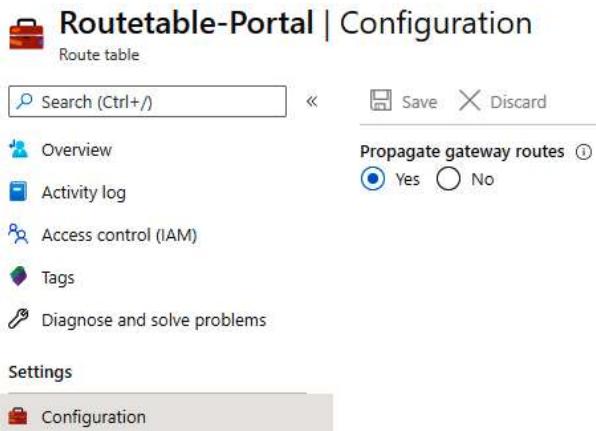


Figura 6.11: Opção para alterar as configurações de Propagar rotas de gateway

### Como funciona...

Nas configurações da tabela de rotas, podemos desabilitar ou habilitar a propagação de rotas de gateway a qualquer momento. Se desabilitada, essa opção impede que as rotas na infraestrutura local sejam propagadas via BGP para as interfaces de rede em uma sub-rede de rede virtual. Nas configurações, podemos criar, excluir ou alterar rotas e sub-redes. Essas opções serão abordadas nas próximas receitas deste capítulo.

Vamos avançar para a próxima receita, onde você aprenderá a associar uma tabela de rotas a uma sub-rede.

## Associar uma tabela de rotas a uma sub-rede

Quando uma tabela de rotas for criada, ela não terá nenhum efeito até que seja configurada corretamente. Há duas coisas que precisamos abordar: os recursos que são afetados e como. Para definir os recursos que são afetados, devemos fazer uma associação entre uma sub-rede e uma tabela de rotas.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para associar uma sub-rede a uma tabela de rotas, devemos fazer o seguinte:

1. No portal do Azure, localize a **Tabela de rotas**.
2. Em **Configurações**, selecione a opção **Sub-redes**. No painel **Sub-redes**, selecione a opção **Associar** para criar uma nova associação:



Figura 6.12: Criar uma nova associação

3. Um novo painel será aberto. Há duas opções disponíveis: selecionar uma rede virtual e escolher a sub-rede à qual queremos associar a tabela de rotas. Primeiro, devemos selecionar **Rede virtual**. Selecionar essa opção listará todas as redes virtuais disponíveis. Selecione a que você deseja associar nesta lista:

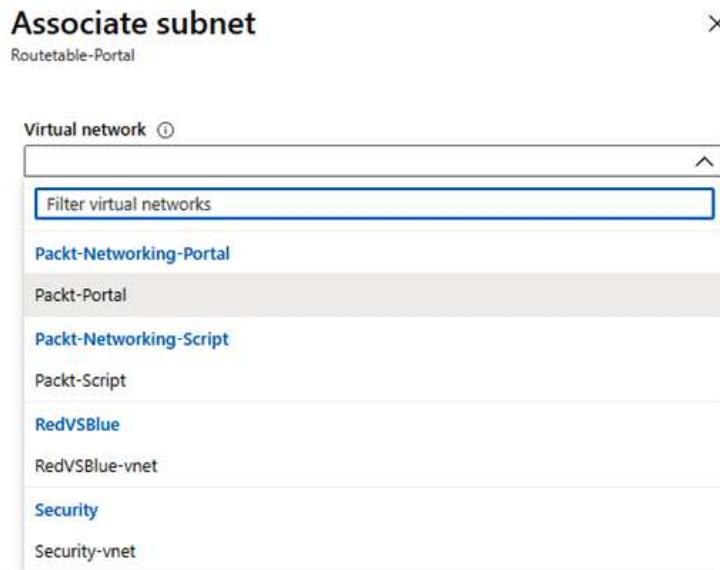


Figura 6.13: Selecionar a rede virtual

4. Depois que uma rede virtual for selecionada, poderemos prosseguir para selecionar uma sub-rede. A opção **Sub-rede** listará todas as sub-redes da rede virtual que selecionamos na etapa anterior. Escolha a sub-rede que você deseja associar nesta lista:

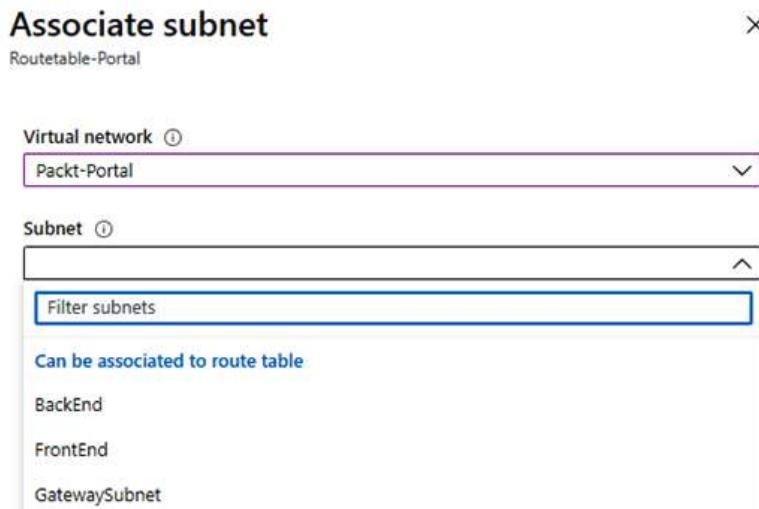


Figura 6.14: Selecionar a sub-rede

5. Depois que as duas opções forem selecionadas, poderemos prosseguir para criar uma associação:

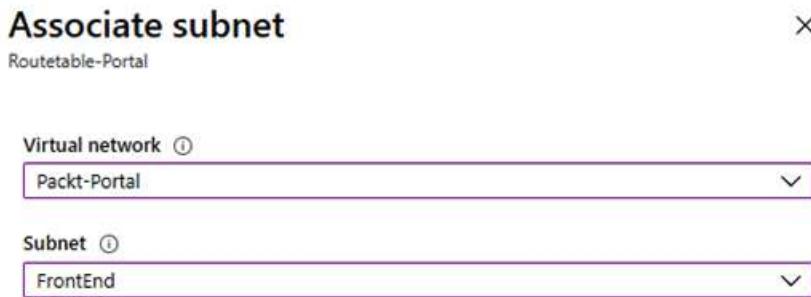


Figura 6.15: Rede virtual e sub-rede selecionadas

6. Depois que uma sub-rede for associada, ela será exibida em uma lista de sub-redes na tabela de rotas:

Routetable-Portal   Subnets				
	Name	Address range	Virtual network	Security group
FrontEnd	FrontEnd	10.0.0.0/24	Packt-Portal	testS2

Figura 6.16: Lista de sub-redes associadas

## Como funciona...

Para ser eficaz, a tabela de rotas deve ter duas partes definidas: *o que* e *como*. Definimos o que será afetado pela tabela de rotas com uma associação de sub-rede. Essa é apenas uma das partes da configuração, pois apenas associar uma sub-rede a uma tabela de rotas não terá efeito. Devemos criar regras que se aplicarão a essa associação. Vamos explicar as regras nas receitas a seguir deste capítulo.

Vamos avançar para uma nova receita e aprender a dissociar uma tabela de rotas de uma sub-rede.

## Dissociar uma tabela de rotas de uma sub-rede

Depois que criarmos uma associação e regras, essas regras serão aplicadas a todos os recursos na sub-rede associada. Se quisermos que as regras não se apliquem mais a uma sub-rede específica, poderemos remover a associação.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para remover a associação entre a sub-rede e a tabela de rotas, devemos fazer o seguinte:

1. No portal do Azure, localize a **Tabela de rotas**.
2. Em **Configurações**, selecione a opção **Sub-redes** e selecione a sub-rede que você deseja remover:



Figura 6.17: Selecionar uma sub-rede para remoção

3. O painel de configuração da sub-rede será aberto. Selecione a opção **Tabela de rotas**. Observe que isso abrirá uma configuração da sub-rede. É um erro comum confundir esse painel com a associação e escolher a opção **Excluir**. Isso não só removerá a associação, como também removerá a sub-rede:

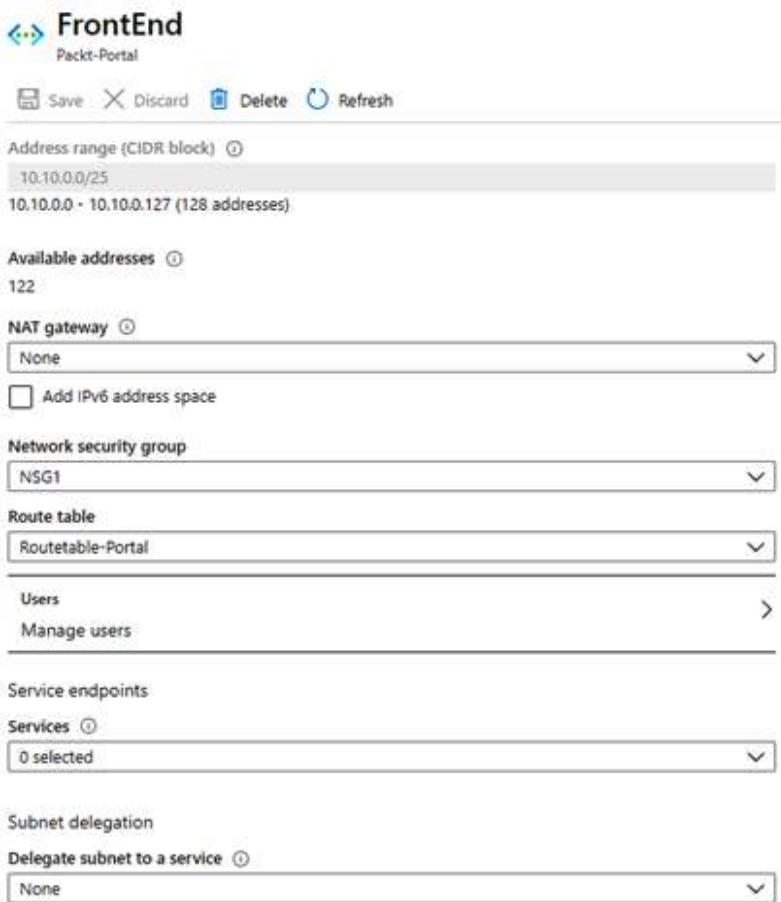


Figure 6.18: Painel de configuração da sub-rede

4. O portal do Azure mostrará uma lista das tabelas de rotas disponíveis para uma sub-rede específica. Escolha **Nenhum**:



Figura 6.19: Lista de tabelas de rotas disponíveis para uma sub-rede

5. Depois de selecionar **Nenhum**, clique no botão **Salvar** para aplicar as novas configurações. A associação de tabela de rotas é removida da sub-rede:

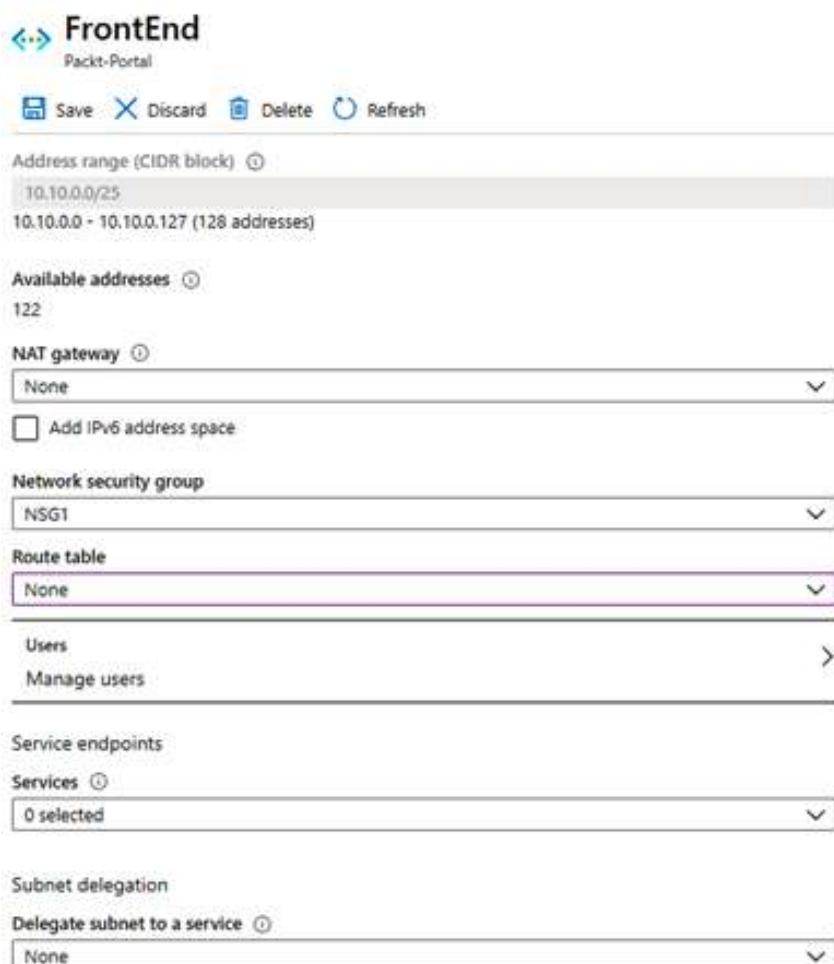


Figura 6.20: Remover uma associação de tabela de rotas da sub-rede

## Como funciona...

Em algum momento, talvez criamos regras em uma tabela de rotas que se aplicam a várias sub-redes. Se não quisermos mais aplicar uma ou mais regras a uma sub-rede específica, poderemos remover a associação. Depois que a associação for removida, as regras não serão mais aplicadas à sub-rede. Todas as regras serão aplicadas a todas as sub-redes associadas. Se precisarmos fazer com que uma única regra não se aplique mais a uma sub-rede específica, deveremos remover a associação.

Nesta receita, aprendemos a dissociar uma tabela de rotas. Vamos avançar para a próxima receita e aprender a criar uma nova rota.

## Criar uma nova rota

Depois de criarmos uma tabela de rotas e as sub-redes associadas, ainda há uma parte faltando. Definimos a tabela de rotas que será afetada com a associação de sub-rede, mas está faltando a parte que define como ela será afetada. Definimos como as sub-redes associadas são afetadas usando regras chamadas **rotas**. As rotas definem rotas de tráfego, informando onde o tráfego específico precisa ir. Se a rota padrão para o tráfego específico for a Internet, poderemos alterar isso e redirecionar o tráfego para um IP ou uma sub-rede específica.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova rota, devemos fazer o seguinte:

1. No portal do Azure, localize a **Tabela de rotas**.
2. No painel **Tabela de rotas**, em **Configurações**, selecione **Rotas**. Selecione **Adicionar** para adicionar uma nova rota:



Figura 6.21: Adicionar uma nova rota

3. No novo painel, precisamos definir valores para os campos **Nome da rota** e **Prefixo de endereço** (no formato CIDR) para o intervalo de endereços IP de destino e selecionar uma opção para **Tipo do próximo salto**. As opções para isso incluem **Gateway de rede virtual**, **Rede virtual**, **Internet**, **Dispositivo virtual** e **Nenhum**:

**Add route**

Routetable-Portal

Route name \*

Address prefix \* ⓘ

Next hop type ⓘ

Internet

Virtual network gateway

Virtual network

Internet

Virtual appliance

None

Figura 6.22: Adicionar detalhes da rota

4. A última opção, **Endereço do próximo salto**, está ativa somente quando um dispositivo virtual é usado. Nesse caso, precisamos fornecer o endereço IP do dispositivo virtual nesse campo, e todo o tráfego percorrerá o dispositivo virtual: Vamos escolher **Internet** e fornecer um endereço IP público no campo **Prefixo de endereço** (a opção **Prefixo de endereço** sempre depende da opção **Tipo do próximo salto**):

**Add route**

Routetable-Portal

Route name \*

Address prefix \* ⓘ

Next hop type ⓘ

Internet

Next hop address ⓘ

Figura 6.23: Selecionar Internet para Tipo do próximo salto

## Como funciona...

A rota define o fluxo do tráfego. Todo o tráfego da sub-rede associada seguirá a rota definida por essas regras. Se definirmos que o tráfego irá para a Internet, todo o tráfego irá para fora da rede para um intervalo de endereços IP definido com um prefixo de endereço IP. Se escolhermos que o tráfego irá para uma rede virtual, ele irá para uma sub-rede definida pelo prefixo de endereço IP. Se esse gateway de rede virtual for usado, todo o tráfego percorrerá o gateway de rede virtual e chegará à sua conexão no outro lado: uma outra rede virtual ou nossa rede local. A opção **Dispositivo virtual** enviará todo o tráfego para o dispositivo virtual, que, com seu próprio conjunto de regras, definirá para onde o tráfego irá em seguida.

Vamos avançar para a próxima receita e aprender a alterar uma rota.

## Alterar uma rota

Os requisitos de rotas podem ser alterados ao longo do tempo. Nesses casos, podemos remover a rota ou editá-la, dependendo de nossas necessidades. Se um trajeto precisar ser ajustado, poderemos selecionar a opção para alterar a rota e aplicar o novo fluxo do tráfego a qualquer momento.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para alterar a rota existente, precisamos fazer o seguinte:

1. No portal do Azure, localize a **Tabela de rotas**.
2. Em **Configurações**, selecione **Rotas** e selecione a rota que deseja alterar na lista de rotas disponíveis:



Figura 6.24: Alterar uma rota disponível

3. Um novo painel será aberto. Podemos alterar o **Prefixo de endereço** (para o intervalo de IP de destino) e as configurações de **Tipo do próximo salto**. Se a opção **Tipo do próximo salto** for um dispositivo virtual, uma opção para **Endereço do próximo salto** estará disponível:

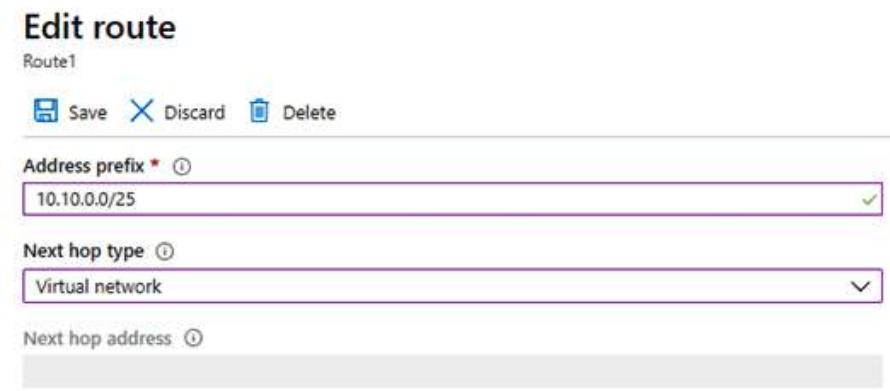


Figura 6.25: Opção para Endereço do próximo salto

## Como funciona...

Os requisitos para uma rota podem ser alterados ao longo do tempo. Podemos alterar uma rota e ajustá-la para se adaptar aos novos requisitos, conforme necessário. Os cenários mais comuns são que o tráfego precisa chegar a um serviço específico quando o IP do serviço é alterado ao longo do tempo. Por exemplo, talvez seja necessário rotear todo o tráfego por meio de um dispositivo virtual, mas o endereço IP do dispositivo virtual é alterado ao longo do tempo. Podemos alterar a rota na tabela de rotas para refletir essa alteração e forçar o fluxo do tráfego por meio do dispositivo virtual. Outro exemplo é quando o tráfego precisa chegar à nossa rede local por meio de um gateway de rede virtual. O intervalo de endereços IP de destino pode ser alterado ao longo do tempo, e precisamos refletir essas alterações na rota novamente.

Nesta receita, aprenderemos a alterar uma rota. Na próxima receita, aprenderemos a excluir uma rota.

## Excluir uma rota

Conforme já mencionado, os requisitos de rotas podem ser alterados ao longo do tempo. Em alguns casos, as regras não são mais aplicáveis, e devemos removê-las. Nesses casos, alterar a rota não concluirá a tarefa, e precisaremos remover completamente a rota. Essa tarefa pode ser concluída ao excluir a rota.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para excluir uma rota, devemos fazer o seguinte:

1. No portal do Azure, localize o link da **Tabela de rotas**.
2. Em **Configurações**, selecione **Rotas** e, em seguida, selecione a rota que você deseja excluir:

The screenshot shows the 'Routes' section of the Azure Route Table configuration. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Keys, and Diagnosis and solve problems. The 'Routes' link is highlighted. The main area has a search bar and a 'Create' button. A table lists one route: 'Route1' with address prefix '10.10.0.0/25' and next hop type 'Virtual network'. There are 'Edit' and 'Delete' buttons for each row.

Figura 6.26: Excluir uma rota existente

3. Um novo painel será aberto. Selecione a opção **Excluir** e confirme sua ação:

The screenshot shows the 'Edit route' dialog for 'Route1'. It includes fields for 'Address prefix' (10.10.0.0/25) and 'Next hop type' (Virtual network). At the top, there are 'Save', 'Discard', and 'Delete' buttons, with 'Delete' being the active one. Below the form is a large grayed-out area.

Figura 6.27: Selecionar a opção Excluir

4. Depois que essa ação for confirmada, você retornará ao painel anterior, e a rota excluída não estará mais listada:

The screenshot shows the 'Routes' section again, but now it's empty. The table header is visible, but there are no rows below it. The sidebar and other interface elements remain the same as in the previous screenshot.

Figura 6.28: A exclusão bem-sucedida de uma rota

## Como funciona...

À medida que nossas necessidades mudam, precisamos atender aos novos requisitos em nossas tabelas de rotas. Podemos editar rotas ou removê-las para atender a esses novos requisitos. Quando várias rotas são usadas em uma única tabela de rotas, uma das rotas pode se tornar obsoleta ou até mesmo bloquear novos requisitos. Nesses casos, convém excluir uma rota para resolver os problemas.



# 7

## Firewall do Azure

A maioria dos componentes de rede do Azure usados para segurança estão disponíveis para impedir o tráfego de entrada indesejado. Não importa se usamos grupos de segurança de rede, grupos de segurança de aplicativos ou um **Firewall de Aplicativo Web (WAF)**, todos eles têm uma única finalidade: impedir o tráfego indesejado de chegar aos nossos serviços. O Firewall do Azure tem funcionalidade semelhante, incluindo uma extensão que podemos usar para impedir que o tráfego de saída saia da rede virtual.

Abordaremos as seguintes receitas neste capítulo:

- Criar um novo firewall
- Criar um novo firewall com o PowerShell
- Configurar uma nova regra de permissão
- Configurar uma nova regra de negação
- Configurar uma tabela de rotas
- Habilitar logs de diagnóstico para o Firewall do Azure
- Configurar o Firewall do Azure no modo de túnel forçado
- Criar um grupo de IP
- Definir configurações de DNS do Firewall do Azure

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Azure PowerShell

Os exemplos de código podem ser encontrados no <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter07>.

## Criar um novo firewall

O Firewall do Azure proporciona controle total sobre nosso tráfego. Além de controlar o tráfego de entrada, com o Firewall do Azure, podemos controlar o tráfego de saída também.

### Preparação

Para que possamos criar uma instância do Firewall do Azure, devemos primeiro preparar uma sub-rede.

Para criar uma nova sub-rede para o Firewall do Azure, devemos fazer o seguinte:

1. Localize a rede virtual que será associada ao nosso Firewall do Azure.
2. Selecione a opção **Sub-redes** em **Configurações** e clique em **Sub-rede** para adicionar uma nova sub-rede, conforme mostrado na Figura 7.1:

Name ↑↓	IPv4 ↑↓
BackEnd	10.10.1.0/24 (250 available)
GatewaySubnet	10.10.2.0/24 (250 available)
FrontEnd	10.10.0.0/25 (112 available)

Figura 7.1: Adicionar uma nova sub-rede

3. No novo painel, devemos fornecer os valores para os campos **Nome** e o **Intervalo de endereços**. É muito importante que a sub-rede seja chamada **AzureFirewallSubnet**:

**Add subnet** X

Packt-Portal

**Name \***  
AzureFirewallSubnet ✓

**Address range (CIDR block) \*** ⓘ  
10.10.3.0/24 ✓  
10.10.3.0 - 10.10.3.255 (251 + 5 Azure reserved addresses)

**NAT gateway** ⓘ  
None ▼  
 Add IPv6 address space

**Network security group**  
None ▼

**Route table**  
None ▼

**Service endpoints**

**Services** ⓘ  
0 selected ▼

**Subnet delegation**

**Delegate subnet to a service** ⓘ  
None ▼

Figura 7.2: Fornecer o nome e o intervalo de endereços da sub-rede

## Como fazer isso...

Para criar uma nova instância do Firewall do Azure usando o portal do Azure, siga estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Firewall do Azure** em serviços de **Rede** (ou pesquise **Firewall do Azure** na barra de pesquisa).
2. No novo painel, devemos fornecer primeiro os valores para os menus suspensos de **Assinatura** e **Grupo de recursos**. Precisamos preencher os campos **Nome** e **Região** para o Firewall do Azure e, opcionalmente, selecionar uma opção de **Zona de disponibilidade**. Em seguida, prosseguiremos para a seleção da rede virtual. As redes virtuais estão disponíveis somente na região onde a instância do Firewall do Azure será criada. Além disso, a rede virtual selecionada deve conter a sub-rede **AzureFirewallSubnet** que criamos anteriormente. Por fim, definimos um endereço IP público (podemos escolher um existente ou criar um novo). Opcionalmente, podemos habilitar **Túnel forçado**:

The screenshot shows the 'Project details' and 'Instance details' sections of the Azure Firewall creation interface.

**Project details:**

- Subscription \***: Microsoft Azure Sponsorship
- Resource group \***: Packt-Networking-Portal (with a 'Create new' link)

**Instance details:**

- Name \***: Packt-Firewall
- Region \***: West Europe
- Availability zone**: None
- Choose a virtual network**: Create new (radio button selected) / Use existing (radio button selected)
- Virtual network**: Packt-Portal (Packt-Networking-Portal)
- Public IP address \***: (New) packt-Firewall-IP (with an 'Add new' link)
- Forced tunneling**: Disabled (switch off)

Figura 7.3: Adicionar detalhes do Firewall do Azure

## Como funciona...

O Firewall do Azure usa um conjunto de regras para controlar o tráfego de saída. Podemos bloquear tudo por padrão e permitir apenas o tráfego permitido ou podemos permitir tudo e bloquear apenas o tráfego proibido. Essencialmente, é o ponto central onde podemos definir políticas de rede, aplicar essas políticas e monitorar o tráfego de rede em redes virtuais ou até mesmo assinaturas. Como firewall como serviço, o Firewall do Azure é um serviço gerenciado com alta disponibilidade e escalabilidade incorporadas.

## Criar um novo firewall com o PowerShell

Como alternativa, podemos implantar o Firewall do Azure usando o PowerShell. Esse método é útil principalmente quando os serviços fazem parte de uma grande implantação ou de qualquer implantação que precisa ser automatizada.

### Como fazer isso...

Há várias etapas que precisam ser realizadas para criar um novo firewall com o Azure PowerShell:

1. Primeiro, definimos os parâmetros:

```
$RG="Packt-Networking-Script"  
$Location="West Europe"  
$VNetName = "Packt-Script"  
$AzFwIpName = "AzFW-Public-IP"  
$AzFwname = "AzFw-Script"
```

2. Em seguida, precisamos criar uma sub-rede separada para o Firewall do Azure:

```
$vnet = Get-AzVirtualNetwork -ResourceGroupName $RG '  
-Name $VnetName  
Add-AzVirtualNetworkSubnetConfig -Name AzureFirewallSubnet '  
-VirtualNetwork $vnet '  
-AddressPrefix 10.11.3.0/24  
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

3. Em seguida, precisamos criar um endereço IP público para o Firewall do Azure:

```
$AzFwIp = New-AzPublicIpAddress -Name $AzFwIpName '  
-ResourceGroupName $RG '  
-Location $Location '  
-AllocationMethod Static '  
-Sku Standard
```

4. Por fim, temos todos os componentes implantados e podemos prosseguir para criar o firewall:

```
$Azfw = New-AzFirewall -Name $AzFwname '  
-ResourceGroupName $RG '  
-Location $Location '  
-VirtualNetworkName $vnet.Name '  
-PublicIpName $AzFwIp.Name
```

## Como funciona...

O firewall exige uma sub-rede separada que é chamada **AzureFirewallSubnet**. Então, precisamos criar uma sub-rede na rede virtual que pretendemos usar. Outro requisito é um endereço IP público. Por fim, estamos prontos para a implantação e podemos criar uma nova instância do Firewall do Azure.

Mas a implantação do Firewall do Azure é apenas o começo. Precisamos configurar nosso firewall criando regras e rotas. Vamos seguir para a próxima receita e ver como as regras são criadas.

## Configurar uma nova regra de permissão

Se quisermos permitir um tráfego específico, devemos criar uma regra de permissão. As regras são aplicadas com base no nível de prioridade. Por isso, uma regra será aplicada somente quando não houver outra regra com prioridade mais alta.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

### Como fazer isso...

Para criar uma nova regra de permissão no Firewall do Azure, execute o seguinte comando:

```
$RG="Packt-Networking-Script"  
$Location="West Europe"  
$Azfw = Get-AzFirewall -ResourceGroupName $RG  
$Rule = New-AzFirewallApplicationRule -Name Rule1 -Protocol  
"http:80","https:443" -TargetFqdn "*packt.com"  
$RuleCollection = New-AzFirewallApplicationRuleCollection -Name  
RuleCollection1 -Priority 100 -Rule $Rule -ActionType "Allow"  
$Azfw.ApplicationRuleCollections = $RuleCollection  
Set-AzFirewall -AzureFirewall $Azfw
```

## Como funciona...

Uma regra de permissão no Firewall do Azure permitirá um tráfego específico. Se houver uma regra que também bloqueia esse tráfego, a regra de prioridade mais alta será aplicada.

Também podemos criar regras de negação. Vamos ver como podemos fazer isso na próxima receita.

## Configurar uma nova regra de negação

Se quisermos negar um tráfego específico, devemos criar uma regra de negação. As regras são aplicadas por prioridade. Por isso, essa regra será aplicada somente se não houver uma regra de prioridade mais alta em vigor.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

### Como fazer isso...

Para criar uma nova regra de negação no Firewall do Azure, execute o seguinte comando:

```
$RG="Packt-Networking-Script"  
$Location="West Europe"  
$Azfw = Get-AzFirewall -ResourceGroupName $RG  
$Rule = New-AzFirewallApplicationRule -Name Rule1 -Protocol  
"http:80", "https:443" -TargetFqdn "*google.com"  
$RuleCollection = New-AzFirewallApplicationRuleCollection -Name  
RuleCollection1 -Priority 100 -Rule $Rule -ActionType "Deny"  
$Azfw.ApplicationRuleCollections = $RuleCollection  
Set-AzFirewall -AzureFirewall $Azfw
```

### Como funciona...

A regra de negação é a opção mais usada com o Firewall do Azure. Uma abordagem em que você bloqueia tudo e permite que apenas o tráfego na lista de permissões não é muito prática, pois poderemos acabar adicionando muitas regras de permissão. Portanto, a abordagem mais comum é usar regras de negação para bloquear um determinado tráfego que queremos impedir.

## Configurar uma tabela de rotas

As tabelas de rotas geralmente são usadas com o Firewall do Azure quando há conectividade cruzada. A conectividade cruzada pode ser com outras redes virtuais do Azure ou com redes na infraestrutura local. Nesses casos, o Firewall do Azure usa tabelas de rotas para encaminhar o tráfego com base nas regras especificadas nas tabelas de rotas.

### Preparação

Abra o console do PowerShell e verifique se você está conectado à sua assinatura do Azure.

## Como fazer isso...

Para criar uma nova tabela de rotas no Firewall do Azure, execute o seguinte comando:

```
$RG="Packt-Networking-Script"
$Location="West Europe"
$Azfw = Get-AzFirewall -ResourceGroupName $RG
$config = $Azfw.IpConfigurations[0].PrivateIPAddress
$Route = New-AzRouteConfig -Name 'Route1' -AddressPrefix 0.0.0.0/0 -NextHopType
VirtualAppliance -NextHopIpAddress $config
$routeTable = New-AzRouteTable -Name 'RouteTable1' -ResourceGroupName $RG
-location $Location -Route $Route
```

## Como funciona...

Usando tabelas de rotas associadas ao Firewall do Azure, podemos definir como o tráfego entre redes é tratado e como roteamos o tráfego de uma rede para outra. Em um ambiente de várias redes, especialmente em uma rede híbrida em que conectamos uma rede virtual do Azure a uma rede na infraestrutura local, essa opção é muito importante. Isso permite determinar qual tipo de tráfego pode fluir, onde e como.

## Habilitar logs de diagnóstico para o Firewall do Azure

Os diagnósticos são uma parte muito importante de qualquer sistema de TI, e a rede não é exceção a isso. As configurações de diagnóstico no Firewall do Azure permitem coletar várias informações que podem ser usadas para solução de problemas ou auditoria.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para habilitar o diagnóstico no Firewall do Azure, devemos seguir estas etapas:

1. No painel Firewall do Azure, localize **Configurações de diagnóstico** em **Monitoramento**.
2. Selecione a opção **Adicionar configuração de diagnóstico**, conforme mostrado na Figura 7.4:

Packt-Firewall | Diagnostic settings

Firewall

Search (Ctrl+ /) Refresh Provide feedback

- Overview
- Activity log
- Access control (IAM)
- Tags

**Settings**

- DNS (preview)
- Rules
- Public IP configuration
- Threat intelligence
- Firewall Manager
- Properties
- Locks
- Export template

**Monitoring**

- Metrics
- Diagnostic settings

Figura 7.4: Adicionar uma configuração de diagnóstico

- No novo painel, preencha o campo de nome e especifique onde os logs serão armazenados. Escolha a conta de armazenamento onde os logs serão armazenados e especifique o período de retenção e quais logs serão armazenados, conforme mostrado na Figura 7.5:

Diagnostic setting name \*

Packt-Firewall

**Category details**

**log**

<input checked="" type="checkbox"/> AzureFirewallApplicationRule	Retention (days) 90
<input checked="" type="checkbox"/> AzureFirewallNetworkRule	Retention (days) 90
<input checked="" type="checkbox"/> AzureFirewallDnsProxy	Retention (days) 90

**metric**

<input checked="" type="checkbox"/> AllMetrics	Retention (days) 90
--	------------------------

Retention only applies to storage account. Retention policy ranges from 1 to 365 days. If you do not want to apply any retention policy and retain data forever, set retention (days) to 0.

**Destination details**

Send to Log Analytics

Archive to a storage account

You'll be charged normal data rates for storage and transactions when you send diagnostics to a storage account.

Showing all storage accounts including classic storage accounts

**Location**  
West Europe

**Subscription**  
Microsoft Azure Sponsorship

**Storage account \***  
packtnetworkingportal251

Stream to an event hub

Figura 7.5: Adicionar detalhes de log

## Como funciona...

O diagnóstico tem dois objetivos: auditoria e solução de problemas. Com base no tráfego e nas configurações, esses logs podem aumentar ao longo do tempo. Portanto, é importante considerar o objetivo principal de habilitar o diagnóstico desde o início. Se os diagnósticos estiverem habilitados para auditoria, convém escolher um máximo de 365 dias de retenção. Se o objetivo principal for a solução de problemas, o período de retenção poderá ser mantido em 7 dias ou um período ainda mais curto. Definir a política de retenção como **0** armazenará logs sem removê-los após um período. Isso pode gerar custos adicionais, e talvez seja necessário configurar um procedimento diferente para remover logs.

Se não quisermos armazenar logs de diagnóstico em uma conta de armazenamento, podemos escolher o Log Analytics ou os Hubs de Eventos. Nesse caso, o processo não inclui a configuração de períodos de retenção, pois essas configurações são mantidas no lado do destino.

## Configurar o Firewall do Azure no modo de túnel forçado

O túnel forçado nos permite forçar todo o tráfego que irá à Internet a um firewall na infraestrutura local para inspeção ou auditoria. Devido a diferentes dependências do Azure, isso não é habilitado por padrão e requer rotas definidas pelo usuário (USRs) para permitir o túnel forçado. Isso também não é possível usando **AzureFirewallSubnet**, e precisamos adicionar uma sub-rede adicional chamada **AzureFirewallManagementSubnet**. Observe que isso precisa ser feito antes da implantação do Firewall do Azure e não funcionará se a sub-rede for adicionada posteriormente.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar **AzureFirewallManagementSubnet** para túnel forçado, precisamos fazer o seguinte:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Tabela de rotas** em serviços de **Rede** (ou pesquise **Tabela de rotas** na barra de pesquisa).

2. No novo painel, devemos fornecer informações para os campos **Assinatura, Grupo de recursos, Região e Nome** para a tabela de rotas. Selecione **Não** para **Propagar rotas de gateway**:

## Create Route table

Basics Tags Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Microsoft Azure Sponsorship
Resource group *	Packt-Portal
	<a href="#">Create new</a>

**Instance details**

Region *	West Europe
Name *	RouteTable1
Propagate gateway routes *	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figura 7.6: Criar uma tabela de rotas usando o portal do Azure

3. Depois que a tabela de rotas for criada, precisaremos definir uma rota de Internet padrão. Acesse a tabela de rotas que acabamos de criar e, em **Rotas** na seção **Configurações**, selecione **Adicionar**:

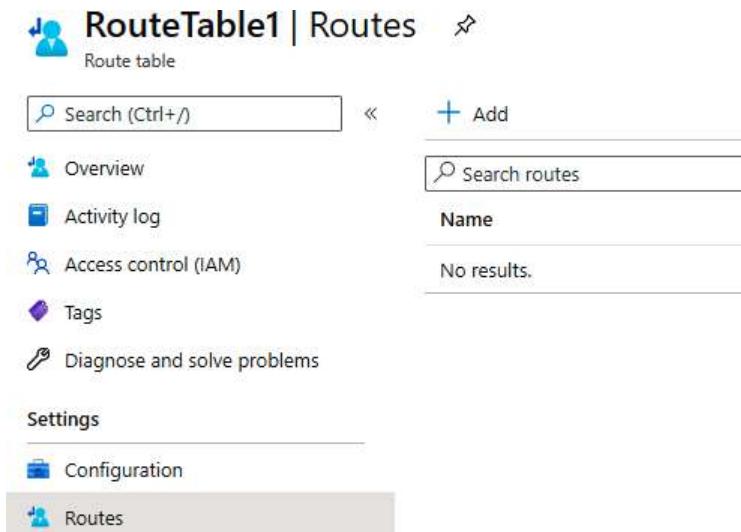


Figura 7.7: Adicionar uma rota padrão da Internet para a tabela de rotas

4. No novo painel, precisamos fornecer um nome para a rota. Também devemos colocar **0.0.0.0/0** em **Prefixo de endereço** e **Internet** em **Tipo do próximo salto**:

## Add route

RouteTable1

Route name \*

Internet	<input checked="" type="checkbox"/>
----------	-------------------------------------

Address prefix \* ⓘ

0.0.0.0/0	<input checked="" type="checkbox"/>
-----------	-------------------------------------

Next hop type ⓘ

Internet	<input checked="" type="checkbox"/>
----------	-------------------------------------

Next hop address ⓘ

	<input type="text"/>
--	----------------------

Figura 7.8: Configurar a rota padrão da Internet para a tabela de rotas

5. Agora, acesse a rede virtual onde você planeja implantar o Firewall do Azure. Em **Sub-redes**, adicione uma nova sub-rede. Observe que **AzureFirewallSubnet** ainda precisa ser adicionada, bem como:

## Packt-Portal | Subnets

Virtual network

Name ↑↓	IPv4 ↑↓
FrontEnd	10.10.0.0/25 (123 available)
BackEnd	10.10.1.0/24 (251 available)
GatewaySubnet	10.10.2.0/24 (251 available)
AzureFirewallSubnet	10.10.3.0/24 (251 available)

Figura 7.9: Adicionar uma nova sub-rede no painel de rede virtual

6. No novo painel, defina o nome para **AzureFirewallManagementSubnet**, forneça um valor para o campo **Intervalo de endereços de sub-rede** (um tamanho mínimo de sub-rede de /26 é necessário) e selecione a tabela de rotas que criamos no campo **Tabela de rotas**:

The screenshot shows the 'Add subnet' dialog with the following fields:

- Name \***: AzureFirewallManagementSubnet
- Subnet address range \***: 10.10.4.0/24 (10.10.4.0 - 10.10.4.255 (251 + 5 Azure reserved addresses))
- Add IPv6 address space**: Unchecked
- NAT gateway**: None
- Network security group**: None
- Route table**: RouteTable1

**SERVICE ENDPOINTS**

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

**Services**: 0 selected

**SUBNET DELEGATION**

Delegate subnet to a service

None

Figura 7.10: Configurar as configurações da sub-rede no novo painel

7. Agora, podemos prosseguir com a implantação do Firewall do Azure. Veja a receita *Criar um novo firewall*.

## Como funciona...

Para oferecer suporte ao túnel forçado, o tráfego associado ao gerenciamento de serviços é separado do restante do tráfego. Uma sub-rede adicional é necessária com um tamanho mínimo de /26, juntamente com um endereço IP público associado. Uma tabela de rotas é necessária com uma única rota definindo a rota para a Internet, e a **Propagação de rotas BGP (propagar rotas de gateway)** deve ser desabilitada. Agora, podemos incluir rotas e definir onde exatamente o tráfego precisa ir (um dispositivo de rede virtual ou firewall na infraestrutura local) para ser inspecionado ou auditado antes de chegar à Internet.

## Criar um grupo de IP

Os grupos de IP são recursos do Azure que ajudam a agrupar endereços IP para facilitar o gerenciamento. Dessa forma, podemos aplicar regras do Firewall do Azure com mais facilidade e com melhor visibilidade.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar um novo grupo de IP, precisamos fazer o seguintes:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Grupo de IP** em serviços de **Rede** (ou pesquise **grupo de IP** na barra de pesquisa).
2. No novo painel, forneça informações para **Assinatura**, **Grupo de recursos**, **Nome** e **Região**:

**Create an IP Group**

**Basics**   IP addresses   Tags   Review + create

An IP group is a user-defined collection of static IP addresses, ranges, and subnets. It can be used with Azure Firewall for network, application, and network address translation (NAT) rules.

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Subscription \***: Microsoft Azure Sponsorship

**Resource group \***: Packt Portal

**IP Group details**

**Name \***: IPGroup01

**Region \***: West Europe

IP Groups are global and can be used across regions regardless where they are stored.

Figura 7.11: Criar um novo grupo de IP usando o portal do Azure

3. Em **Endereços IP**, precisamos fornecer algo para o campo **Endereço IP, intervalo ou sub-rede**. Neste exemplo, estamos adicionando uma sub-rede:

### Create an IP Group

The screenshot shows a user interface for creating an IP group. At the top, there are tabs: Basics, IP addresses (which is the active tab), Tags, and Review + create. Below the tabs are two buttons: Import from File and Delete. A section titled 'IP address, range or subnet' contains a checkbox and an input field. The input field contains '10.1.0.0/24' and has a green checkmark next to it, indicating it is valid. Below this is a placeholder text: 'Enter a single IP address, multiple IP addresses, or ranges...'. At the bottom, there are navigation controls: '< Previous', 'Page 1 of 1', and 'Next >'.

Figura 7.12: Adicionar uma sub-rede no campo de endereços IP, intervalo ou sub-rede

4. Agora, podemos continuar e implantar o grupo de IP.

## Como funciona...

Os grupos de IP permitem associar vários endereços IP a um único recurso para facilitar o gerenciamento. Podemos associar qualquer número de endereços IP individuais (em **Formato 10.10.10.10**), intervalos de IP (em formato **10.10.10.10-10.10.10.20**) ou sub-redes (em formato **10.10.10.0/24**). Em seguida, as regras de firewall podem ser associadas a grupos de IP e a todos os endereços IP em um grupo de IP definido. Em vez de criar uma regra separada para cada endereço IP, intervalo ou sub-rede, agora podemos ter uma única regra para um intervalo de IP único. Isso significa gerenciamento e manutenção mais fáceis do Firewall do Azure, juntamente com uma melhor visibilidade das regras eficazes.

## Definir configurações de DNS do Firewall do Azure

Podemos usar um servidor DNS personalizado com nossa instância do Firewall do Azure. Isso nos permite resolver nomes personalizados e aplicar filtragem com base no **Nome de Domínio Totalmente Qualificado (FQDN)**.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para configurar configurações de DNS personalizadas no Firewall do Azure, precisamos fazer o seguinte:

- No painel Firewall do Azure, localize **DNS** em **Configurações**. Precisamos defini-lo como **Habilitado**. Selecione o tipo de DNS (padrão ou personalizado) e se queremos usar um proxy de DNS:

The screenshot shows the 'DNS (preview)' settings page for an Azure Firewall named 'Packt-Firewall'. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Tags, and Settings. Under Settings, 'DNS (preview)' is selected. The main area has two radio button options: 'Disabled' (unchecked) and 'Enabled' (checked). Below 'Enabled', it says 'DNS settings will be applied on the firewall'. There are two sections for 'DNS Servers': 'Default (Azure provided)' (radio button unchecked) and 'Custom' (radio button checked). Under 'Custom', there's a 'Custom DNS servers' section with two input fields containing '10.0.0.6' and '168.63.129.16', each with a delete icon. Below these is an 'Add Existing' link. At the bottom, there's a 'DNS Proxy' section with a note: 'If enabled, the firewall will listen on port 53 and will forward DNS requests to the DNS server specified above.' It has two radio buttons: 'Disabled' (unchecked) and 'Enabled' (checked).

Figura 7.13: Definir configurações de DNS do Firewall do Azure usando o portal do Azure

- Depois que todas as configurações necessárias forem disponibilizadas, selecione **Salvar** para aplicá-las. Leva até 30 minutos para propagar corretamente as rotas e para que elas tenham efeito completo.

## Como funciona...

Para usar a filtragem do FQDN, o Firewall do Azure precisa ser capaz de resolver o FQDN em questão. Isso pode ser feito ao habilitar as configurações de DNS no Firewall do Azure. Quando habilitado, podemos escolher entre o DNS fornecido pelo Azure ou o DNS personalizado. O DNS personalizado pode ser uma zona DNS do Azure ou um servidor DNS em execução em uma rede virtual.

# 8

## Criar conexões híbridas

As conexões híbridas permitem criar conexões seguras com **Redes virtuais do Azure (VNets)**. Essas conexões podem ser na infraestrutura local ou em outras VNets do Azure. Estabelecer conexões com VNets do Azure permite a troca de tráfego de rede seguro com outros serviços que estão localizados em diferentes VNets do Azure, assinaturas ou serviços fora do Azure (em nuvens ou infraestruturas locais diferentes). O uso de conexões seguras elimina a necessidade de pontos de extremidade expostos ao público geral que representam um possível risco de segurança. Isso é especialmente importante quando consideramos o gerenciamento, em que a abertura de pontos de extremidade públicos cria um risco de segurança e apresenta um problema importante. Por exemplo, se considerarmos o gerenciamento de máquinas virtuais, é uma prática comum usar o **Remote Desktop Protocol (RDP)** ou o PowerShell para gerenciamento. Expor essas portas ao acesso público representa um grande risco. Uma prática recomendada é desabilitar qualquer tipo de acesso público a essas portas e usar somente o acesso de uma rede interna para gerenciamento. Nesse caso, usamos uma conexão site a site ou ponto a site para proporcionar o gerenciamento seguro.

Em outro cenário, talvez precisemos acessar um serviço ou um banco de dados em outra rede, na infraestrutura local ou por meio de outra VNet do Azure. Novamente, a exposição desses serviços pode representar um risco e usamos o emparelhamento site a site, VNet a VNet ou VNet para proporcionar essa conexão de forma segura.

Abordaremos as seguintes receitas neste capítulo:

- Criar uma conexão site a site
- Fazer download da configuração do dispositivo de VPN do Azure
- Criar uma conexão ponto a site
- Criar uma conexão VNet a VNet
- Conectar VNets usando emparelhamento de rede

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure
- Windows PowerShell

Os exemplos de código podem ser encontrados no <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter08>.

## Criar uma conexão site a site

Uma conexão site a site é usada para criar uma conexão segura entre uma rede na infraestrutura local e uma VNet do Azure. Essa conexão é usada para executar várias tarefas diferentes, como habilitar conexões híbridas ou gerenciamento seguro. Em uma conexão híbrida, permitimos que um serviço em um ambiente se conecte a um serviço em outro ambiente. Por exemplo, poderíamos ter um aplicativo no Azure que use um banco de dados localizado em um ambiente na infraestrutura local. O gerenciamento seguro permite limitar as operações de gerenciamento a serem permitidas somente quando provenientes de um ambiente seguro e controlado, como a nossa rede local.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma nova conexão site a site, devemos seguir estas etapas:

1. Localize o gateway de rede virtual (aquele que criamos no Capítulo 5, Gateways de rede local e virtual) e selecione **Conexões**.
2. Em **Conexões**, selecione a opção **Adicionar** para adicionar uma nova conexão:

The screenshot shows the 'Connections' blade in the Azure portal for a 'Virtual network gateway' named 'packt-vng-portal'. At the top, there's a search bar labeled 'Search (Ctrl+ /)' and buttons for 'Add' and 'Refresh'. On the left, a sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. Below the sidebar is a 'Settings' section with 'Configuration' and 'Connections' selected. A 'User VPN configuration' link is also visible. The main area displays a search bar for 'Search connections' and a table with one row: 'Name' (No results). The 'Add' button is highlighted with a light gray background.

Figura 8.1: O painel Conexões no portal do Azure

3. No novo painel, precisamos inserir algumas informações para o nome da conexão e selecionar **Site a site (IPsec)** para **Tipo de conexão**:

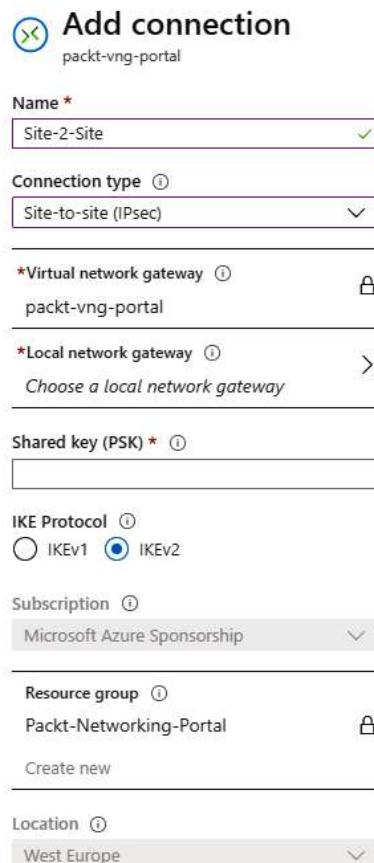


Figura 8.2: Adicionar atributos de conexão

4. Em **Gateway de rede local**, precisamos selecionar um gateway de rede local na lista (criamos um gateway de rede local no Capítulo 5, *Gateways de rede local e virtual*):

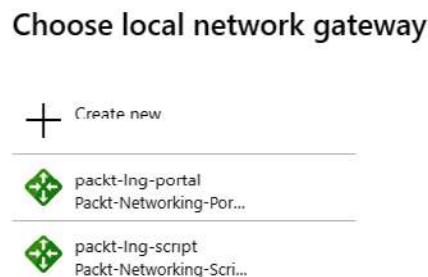


Figura 8.3: Selecionar um gateway de rede local

5. Precisamos fornecer uma chave compartilhada no campo **Chave compartilhada (PSK)** que será usada para a conexão IPSec. Também precisamos definir o **Protocolo IKE** que será usado para a associação de segurança. Podemos escolher entre **IKEv1** e **IKEv2**. Observe que as opções para **Assinatura**, **Grupo de recursos** e **Local** estão bloqueadas e serão as mesmas que são para o gateway de rede virtual:

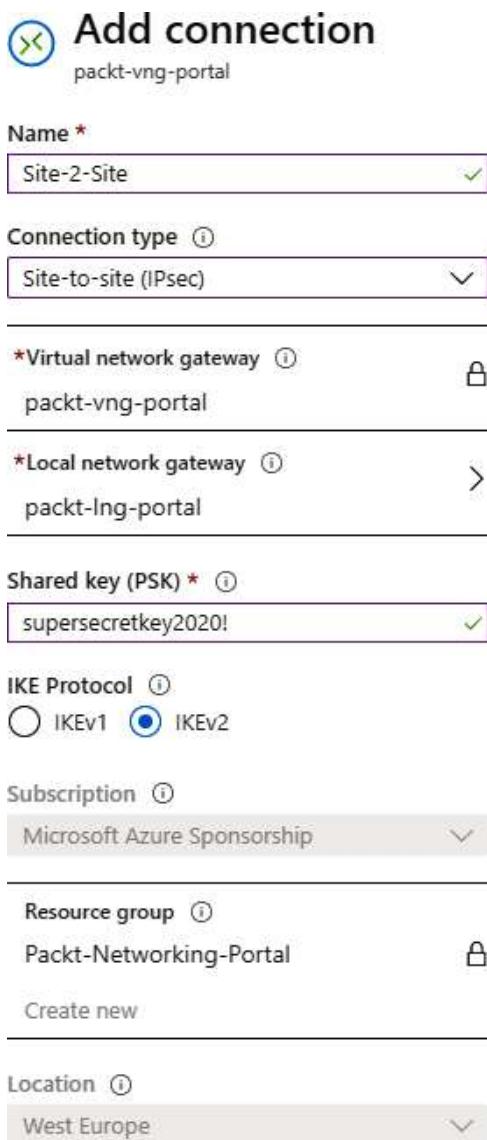


Figura 8.4: Adicionar uma nova conexão

6. Por fim, selecionamos **Criar**, e a implantação será iniciada.

## Como funciona...

Usando o gateway de rede virtual, definimos o lado do Azure do túnel IPsec. O gateway de rede local fornece informações sobre a rede local, definindo o lado local do túnel com o endereço IP público e as informações da sub-rede local. Dessa forma, o lado do túnel do Azure tem todas as informações relevantes necessárias para formar uma conexão bem-sucedida com uma rede na infraestrutura local. No entanto, isso conclui apenas metade do trabalho, pois o lado oposto da conexão também deve ser configurado. Essa parte do trabalho depende muito do dispositivo VPN usado localmente, e cada dispositivo tem etapas de configuração exclusivas. Depois que os dois lados do túnel forem configurados, o resultado será uma conexão VPN segura e criptografada entre redes.

Vamos conferir como configurar nosso dispositivo VPN local.

## Fazer o download da configuração do dispositivo VPN do Azure

Depois de criar o lado do Azure da conexão site a site, ainda precisamos configurar o dispositivo VPN local. A configuração depende do fornecedor e do tipo de dispositivo. Você pode ver todos os dispositivos compatíveis em <https://docs.microsoft.com/azure/vpn-gateway/vpn-gateway-about-vpn-devices>. Em alguns casos, há uma opção para fazer o download da configuração de um dispositivo VPN diretamente no portal do Azure.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para fazer o download da configuração do dispositivo VPN, devemos seguir estas etapas:

1. Localize a conexão **site a site** no portal do Azure. O painel **Visão geral** será aberto por padrão.
2. Selecione a opção **Fazer o download da configuração** na parte superior do painel:

Resource group (change) : Packt-Networking-Portal	
Status	: Unknown
Location	: West Europe

Figura 8.5: Visão geral da conexão site a site no portal do Azure

3. Um novo painel será aberto, e você verá que todas as opções no painel estão predefinidas:

Download configuration

Download customer VPN device configuration template

**Device vendor \***

Choose a device vendor

**Device family \***

Waiting on device vendor selection

**Firmware version \***

Waiting on device family selection

Figura 8.6: Escolher a configuração do dispositivo VPN

4. Selecione as opções relevantes para os campos **Fornecedor do dispositivo**, **Família de dispositivos** e **Versão de firmware**. Observe que apenas algumas opções estão disponíveis e que nem todos os dispositivos compatíveis têm essas opções. Depois que todas essas opções forem selecionadas, faça o download do arquivo de configuração. O arquivo de exemplo ([Site-2-Site.txt](#) na pasta **Capítulo 8**) pode ser encontrado no repositório do GitHub associado a este livro:

Download configuration

Download customer VPN device configuration template

**Device vendor \***

Cisco

**Device family \***

ASA (Adaptive Security Appliance)

**Firmware version \***

Cisco ASA [9.8+\_ONLY]\_RouteBased(IKEv2+VTI+BGP)

Figura 8.7: Fazer o download do arquivo de configuração

5. Depois de usar o arquivo de configuração do dispositivo VPN local, os dois lados do túnel IPsec serão configurados. O valor **Status** na conexão **site a site** será alterado para **Conectado**:

The screenshot shows the Azure portal interface for a 'Site-2-Site' connection. At the top, there's a search bar labeled 'Search (Ctrl+ /)' and some action buttons: 'Move', 'Download configuration', and 'Delete'. Below this, the connection name 'Site-2-Site' is displayed along with its resource group ('Packt-Networking-Portal'). The 'Overview' tab is selected, showing the current status as 'Connected' and the location as 'West Europe'. There's also an 'Activity log' section.

Resource group (change) : Packt-Networking-Portal	
Status	: Connected
Location	: West Europe

Figura 8.8: Verificar o status da conexão site a site

Agora, vamos conferir como essa conexão funciona em detalhes.

### Como funciona...

Depois de configurar o lado do Azure do túnel IPsec, precisamos configurar o outro lado, bem como o dispositivo VPN local. As etapas e a configuração são diferentes para cada dispositivo. Em alguns casos, podemos fazer download do arquivo de configuração diretamente no portal do Azure. Após a configuração do dispositivo VPN, tudo está configurado, e podemos usar o túnel para uma comunicação segura entre a rede local e a VNet.

## Criar uma conexão ponto a site

O acesso a recursos de forma segura é importante, e isso deve ser realizado com segurança. Nem sempre é possível fazer isso usando uma conexão site a site, principalmente quando temos que realizar algo fora do horário de trabalho. Nesse caso, podemos usar ponto a site para criar uma conexão segura que pode ser estabelecida em qualquer lugar.

### Preparação

Para criar uma conexão ponto a site, precisaremos gerar um certificado que será usado para a conexão. Para criar um certificado, devemos seguir estas etapas:

1. Execute o seguinte script do PowerShell para gerar um certificado:

```
$cert = New-SelfSignedCertificate -Type Custom '
-KeySpec Signature '
-Subject "CN=P2SRootCert" '
-KeyExportPolicy Exportable '
-HashAlgorithm sha256 -KeyLength 2048 '
-CertStoreLocation "Cert:\CurrentUser\My" '
```

```

-KeyUsageProperty Sign '
-KeyUsage CertSign

New-SelfSignedCertificate -Type Custom '
-DnsName P2SChildCert '
-KeySpec Signature '
-Subject "CN=P2SChildCert" '
-KeyExportPolicy Exportable '
-HashAlgorithm sha256 -KeyLength 2048 '
-CertStoreLocation "Cert:\CurrentUser\My" '
-Signer $cert '
-TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

```

2. Em seguida, precisamos exportar o certificado. Abra **certmgr**, acesse **Pessoal>Certificados**, selecione **P2SRootCert** e escolha a opção **Exportar...**:

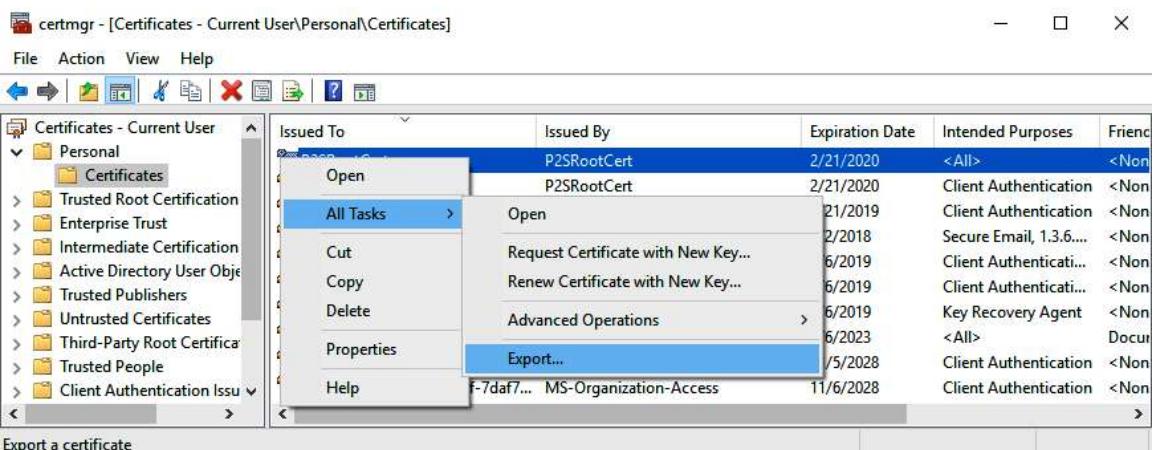


Figura 8.9: Exportar o certificado usando certmgr

3. Isso iniciará o **Assistente para Exportação de Certificados**. Clique em **Avançar**.

4. Selecione a opção **Não, não exportar a chave privada** e clique em **Avançar**:



Figura 8.10: Assistente para Exportação de Certificados

5. Selecione o formato **X.509 (.CER) codificado em Base-64** e clique em **Avançar**:



Figura 8.11: Selecionar o formato de exportação

6. Selecione o local em que você deseja salvar o certificado e clique em **Avançar**.
7. Por fim, temos a opção de revisar todas as informações. Depois de clicar em **Concluir**, a exportação será concluída:



Figura 8.12: Concluir o Assistente para Exportação de Certificados

Agora, vamos ver as etapas para criar uma conexão ponto a site.

## Como fazer isso...

Para criar uma conexão ponto a site, precisamos fazer o seguinte:

1. No portal do Azure, localize o gateway de rede local e **Configuração de VPN do usuário**. Selecione **Configurar agora**:

The screenshot shows the 'User VPN configuration' page in the Azure portal. The 'User VPN configuration' section is highlighted. It displays the following information:

- Status: Point-to-site is not configured
- Action: Configure now
- Other sections: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems

Figura 8.13: Configurar conexão ponto a site

2. Precisamos definir o **Pool de endereços**. O pool de endereços aqui não pode sobrepor o pool de endereços da VNet associada ao gateway de rede virtual:

Figura 8.14: Adicionar o pool de endereços

3. Em seguida, precisamos selecionar a opção **Tipo de túnel** na lista de opções predefinidas. Nesta receita, vamos selecionar **OpenVPN (SSL)**, mas qualquer opção é válida:

Figura 8.15: Selecionar Tipo de túnel no menu suspenso

4. Localize o certificado exportado (na seção Preparação) e abra-o no Bloco de notas (ou qualquer outro editor de texto). Selecione o valor do certificado e copie-o da seguinte forma:

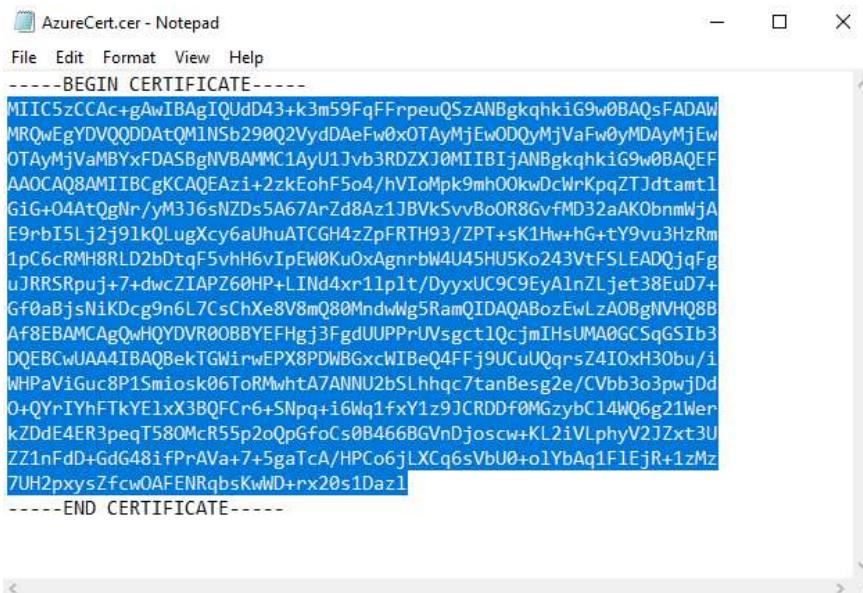


Figura 8.16: Abrir o certificado no Bloco de notas

5. No portal do Azure, precisamos definir o certificado raiz. Insira o nome do certificado e cole o valor do certificado (da etapa anterior) no campo **Dados do certificado público**:

packt-vng-portal | User VPN configuration

Virtual network gateway

Search (Ctrl+ /) < Save Discard Download VPN client

Address pool \*

10.20.3.0/24

Tunnel type

OpenVPN (SSL)

Authentication type

Azure certificate  RADIUS authentication  Azure Active Directory

Root certificates

Name	Public certificate data
Point2Site	6BGVnDjoscw+KL2iVLphyV2JZxt3...

Settings

- Configuration
- Connections
- User VPN configuration
- Properties
- Locks
- Export template

Figura 8.17: Definir o certificado raiz

- Depois de clicar em **Salvar** para a configuração ponto a site, uma nova opção será disponibilizada: **Fazer o download do cliente VPN**. Podemos fazer o download da configuração e começar a usar esta conexão:



Figura 8.18: Fazer o download da configuração

Agora, vamos ver como funciona.

## Como funciona...

Ponto a site permite acessar as VNets do Azure de forma segura. O acesso a uma conexão site a site é restrito à nossa rede local, mas ponto a site permite conectar em qualquer lugar. A autenticação baseada em certificado é usada, que usa o mesmo certificado no servidor (Azure) e no cliente (o cliente VPN) para verificar a conexão e permitir o acesso. Isso permite acessar as VNets do Azure em qualquer lugar e a qualquer momento. Esse tipo de conexão geralmente é usado para tarefas de gerenciamento e manutenção, pois é uma conexão sob demanda. Se uma conexão constante for necessária, você precisará considerar uma conexão site a site.

## Criar uma conexão VNet a VNet

De forma semelhante à necessidade de conectar a VNets do Azure aos recursos em uma rede local, talvez seja necessário conectar-se a recursos em outra VNet do Azure. Nesses casos, podemos criar uma conexão VNet a VNet que permitirá usar serviços e pontos de extremidade em outra VNet. Esse processo é muito semelhante à criação de uma conexão site a site. A diferença é que não exigimos um gateway de rede local. Em vez disso, usamos dois gateways de rede virtual, um para cada VNet.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma nova conexão VNet a VNet, devemos seguir estas etapas:

- No portal do Azure, localize um dos gateways de rede virtual (associado a uma das VNets às quais você está tentando se conectar).
- No painel **Gateway de rede virtual**, selecione **Conexões** e **Adicionar** para adicionar uma nova conexão:

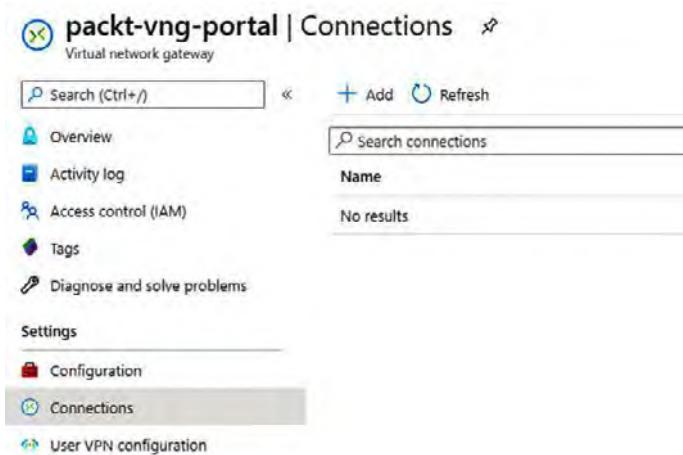


Figura 8.19: Adicionar uma nova conexão

3. No novo painel, insira um valor **Nome** para uma nova conexão e selecione **VNet a VNet** em **Tipo de conexão**:

**Name \***  
VNet-2-VNet

**Connection type** ⓘ  
VNet-to-VNet

**\*First virtual network gateway** ⓘ  
packt-vng-portal

**\*Second virtual network gateway** ⓘ  
Choose another virtual network gateway

**Shared key (PSK) \*** ⓘ

**IKE Protocol** ⓘ  
 IKEv1  IKEv2

**Subscription** ⓘ  
Microsoft Azure Sponsorship

**Resource group** ⓘ  
Packt-Networking-Portal

**Create new**

**Location** ⓘ  
West Europe

Figura 8.20: Configurar a nova conexão

4. O primeiro gateway de rede virtual será realçado automaticamente. Precisamos selecionar o segundo gateway de rede virtual:

### Choose virtual network gateway

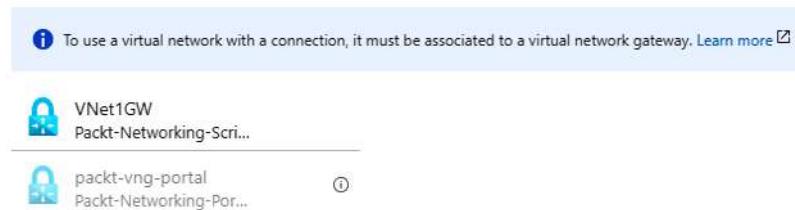


Figura 8.21: Escolher o gateway de rede virtual

5. Precisamos fornecer uma chave compartilhada para a conexão antes de selecionarmos **Criar** e iniciarmos a implantação. Observe que as opções **Assinatura**, **Grupo de recursos** e **Local** estão bloqueadas e que os valores para o primeiro gateway de rede virtual serão usados aqui:

**Add connection**

Name \*  
VNet-2-VNet

Connection type ⓘ  
VNet-to-VNet

\*First virtual network gateway ⓘ  
packt-vng-portal

\*Second virtual network gateway ⓘ  
VNet1GW

Shared key (PSK) \* ⓘ  
supersecretkey2020!

IKE Protocol ⓘ  
 IKEv1  IKEv2

Subscription ⓘ  
Microsoft Azure Sponsorship

Resource group ⓘ  
Packt-Networking-Portal

Create new

Location ⓘ  
West Europe

Figura 8.22: Fornecer uma chave compartilhada para a conexão

6. A implantação de VNet a VNet não demora muito e deve ser realizada em poucos minutos. No entanto, leva algum tempo para estabelecer conexões. Por isso, você pode ver o status **Desconhecido** por até 15 minutos até que seja alterado para **Conectado**:

Name	Status	Connection type	Peer
VNet-2-VNet	Unknown	VNet-to-VNet	VNet1GW

Figura 8.23: Status de implantação de VNet a VNet

Agora, vamos ver seu funcionamento em detalhes.

## Como funciona...

Uma conexão VNet a VNet funciona de forma muito semelhante a uma conexão site a site. A diferença é que o Azure usa um gateway de rede local para obter informações sobre a rede local. Nesse caso, não precisamos dessas informações. Usamos dois gateways de rede virtual para conexão. Cada gateway de rede virtual fornece informações de rede para a VNet à qual está associado. Isso resulta em conexões VPN seguras e criptografadas entre duas VNets do Azure que podem ser usadas para estabelecer conexões entre os recursos do Azure nas duas VNets.

Agora, vamos aprender sobre o uso do emparelhamento de rede para conectar VNets.

## Conectar VNets usando emparelhamento de rede

Outra forma de conectar duas VNets do Azure é usar o **emparelhamento de rede**. Essa abordagem não requer o uso de um gateway de rede virtual, portanto, é mais econômico usar se o único requisito é estabelecer uma conexão entre VNets do Azure. O emparelhamento de rede usa a infraestrutura de backbone da Microsoft para estabelecer uma conexão entre duas VNets, e o tráfego é roteado somente por endereços IP privados. No entanto, esse tráfego não é criptografado. É o tráfego privado que permanece na rede da Microsoft, de forma semelhante ao que acontece com o tráfego na mesma VNet do Azure.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar emparelhamento de rede, devemos seguir estas etapas:

1. No portal do Azure, localize uma das VNets à qual você deseja se conectar.
2. No painel **Rede virtual**, selecione a opção **Emparelhamentos** e selecione **Adicionar** para adicionar uma nova conexão:

The screenshot shows the 'Packt-Portal | Peerings' section of the Azure Portal. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Address space, Connected devices, Subnets, DDoS protection, Firewall, Security, and DNS servers. The 'Peerings' option is highlighted at the bottom of the sidebar. On the right, there's a main content area with a search bar, an 'Add' button, a refresh button, and a 'Filter by name...' dropdown. Below these are sections for 'Name' and 'No results.'

Figura 8.24: Adicionar uma nova conexão de emparelhamento de rede

3. No novo painel, devemos inserir o nome da conexão, selecionar uma opção de **Modelo de implantação de rede virtual** (**Gerenciador de recursos** ou **Clássico**) e selecione a VNet à qual estamos nos conectando. Essas informações podem ser fornecidas ao fornecer uma ID de recurso ou selecionar as opções **Assinatura** e **Rede virtual** no menu suspenso. Há algumas configurações adicionais que são opcionais, mas fornecem melhor controle de tráfego:

## Add peering

Packt-Portal

- For peering to work, a peering link must be created from Packt-Portal to Packt-Script as well as from Packt-Script to Packt-Portal.

Name of the peering from Packt-Portal to Packt-Script \*

Peering



Peer details

Virtual network deployment model ⓘ

Resource manager  Classic

I know my resource ID ⓘ

Subscription \* ⓘ

Microsoft Azure Sponsorship



Virtual network \*

Packt-Script (Packt-Networking-Script)



Name of the peering from Packt-Script to Packt-Portal \*

Peering



Configuration

Configure virtual network access settings

Allow virtual network access from Packt-Portal to Packt-Script ⓘ

Disabled  Enabled

Allow virtual network access from Packt-Script to Packt-Portal ⓘ

Disabled  Enabled

Configure forwarded traffic settings

Allow forwarded traffic from Packt-Script to Packt-Portal ⓘ

Disabled  Enabled

Allow forwarded traffic from Packt-Portal to Packt-Script ⓘ

Disabled  Enabled

Configure gateway transit settings

Allow gateway transit ⓘ

Figura 8.25: Configurar detalhes do emparelhamento de uma nova conexão

4. Depois que uma conexão for criada, poderemos ver as informações e o status do emparelhamento. Também podemos alterar as opções de **Configuração** a qualquer momento:

## Peering

Packt-Portal

Save Discard Delete

Name of the peering from Packt-Portal to Packt-Script

Peering

Peering status

Connected

Provisioning state

Succeeded

Peer details

Address space

10.11.0.0/16

Remote Vnet Id

/subscriptions/cb638267-a366-463c-bfe5-7a49311c27a8/resourceGroups/Packt-Networking-Scri...

Virtual network

Packt-Script

Configuration

Configure virtual network access settings

Allow virtual network access from Packt-Portal to Packt-Script

Disabled  Enabled

Configure forwarded traffic settings

Allow forwarded traffic from Packt-Script to Packt-Portal

Disabled  Enabled

Configure gateway transit settings

Allow gateway transit

Configure Remote Gateways settings

Use remote gateways

Figura 8.26: Revisar as informações de emparelhamento e o status de uma nova conexão

Agora, vejamos seu funcionamento em detalhes.

## Como funciona...

O emparelhamento de rede permite estabelecer uma conexão entre duas VNets Azure no mesmo locatário do Azure. O emparelhamento usa uma rede de backbone da Microsoft para rotear o tráfego privado entre recursos na mesma rede, usando somente endereços IP privados. Não há necessidade de gateways de rede virtual (que criam custos adicionais), pois um "gateway remoto" virtual é criado para estabelecer uma conexão. A desvantagem dessa abordagem é que a mesma VNet não pode usar emparelhamento e um gateway de rede virtual ao mesmo tempo. Se houver necessidade de conectar uma VNet à rede local e a outra VNet, devemos ter uma abordagem diferente e usar um gateway de rede virtual, que permitirá criar uma conexão site a site com uma rede local e uma conexão VNet a VNet com outra VNet.

Quando se trata de configurações de acesso à rede, temos várias opções para controlar o fluxo de tráfego de rede. Por exemplo, podemos afirmar que o tráfego é permitido da VNet A à VNet B, mas negado da VNet B à VNet A. Obviamente, podemos configurá-lo de forma oposta ou torná-lo bidirecional.

Também podemos controlar o tráfego em trânsito quando uma rede adicional está envolvida. Se a VNet A estiver conectada à VNet B e, além disso, a VNet A estiver conectada à VNet C, poderemos controlar se o tráfego é permitido entre a VNet B e a VNet C como tráfego de trânsito por meio da VNet A.

No entanto, isso só funcionará se o trânsito não for feito por meio de emparelhamento. Se todas as redes forem VNets do Azure, a VNet A estiver conectada à VNet B por meio de emparelhamento e a VNet B estiver conectada à VNet C por meio de emparelhamento, a conexão entre a VNet A e a VNet C não será possível por meio do trânsito entre VNets. Isso ocorre porque o emparelhamento é uma relação não transitiva entre duas VNets. Se a VNet B estiver conectada à VNet C por meio de VNet a VNet (ou a uma rede na infraestrutura local por meio de site a site), o trânsito será possível entre a VNet A e a VNet, em vez da VNet B.



# 9

## Conectar a recursos com segurança

Expor pontos de extremidade de gerenciamento (RDP, SSH, HTTP e outros) por um endereço IP público não é uma boa ideia. Qualquer tipo de acesso de gerenciamento deve ser controlado e permitido somente por uma conexão segura. Normalmente, isso é feito ao conectar a uma rede privada (por meio de S2S ou P2S) e acessar recursos por endereços IP privados. Em algumas situações, isso não é uma tarefa fácil. A causa disso pode ser a infraestrutura local insuficiente ou, em alguns casos, o cenário pode ser muito complexo. Felizmente, há outras maneiras de atingir o mesmo objetivo. Podemos nos conectar com segurança aos nossos recursos usando o Azure Bastion, a WAN Virtual do Azure e o Link Privado do Azure.

Abordaremos as seguintes receitas neste capítulo:

- Criar uma instância do Azure Bastion
- Conectar a uma máquina virtual com o Azure Bastion
- Criar uma WAN virtual
- Criar um hub (na WAN virtual)
- Adicionar uma conexão site a site (em um hub virtual)
- Adicionar uma conexão de rede virtual (em um hub virtual)
- Criar um ponto de extremidade do Link Privado
- Criar um serviço do Link Privado

## Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure

## Criar uma instância do Azure Bastion

O Azure Bastion permite conectar com segurança aos nossos recursos do Azure sem infraestrutura adicional. Só precisamos de um navegador. Basicamente, é um serviço PaaS provisionado em nossa rede virtual que fornece uma conexão RDP/SSH segura para Máquinas Virtuais do Azure. A conexão é feita diretamente no portal do Azure por **Transport Layer Security (TLS)**.

## Preparação

Para que possamos criar uma instância do Azure Bastion, devemos preparar a sub-rede.

Para criar uma nova sub-rede para o Azure Bastion, devemos fazer o seguinte:

1. Localize a rede virtual que será associada à nossa instância do Azure Bastion.
2. Selecione a opção **Sub-redes** em **Configurações** e selecione a opção para adicionar uma nova sub-rede, conforme mostrado na Figura 9.1:

Name ↑↓	IPv4 ↑↓
BackEnd	10.10.1.0/24 (250 available)
GatewaySubnet	10.10.2.0/24 (250 available)
FrontEnd	10.10.0.0/25 (122 available)
AzureFirewallSubnet	10.10.3.0/24 (251 available)

Figura 9.1: Criar uma nova sub-rede para o Azure Bastion

3. No novo painel, devemos preencher os campos **Nome** e **Intervalo de endereços**. É muito importante que a sub-rede seja chamada **AzureBastionSubnet** e que a sub-rede use um prefixo de pelo menos /27 (este é um requisito de serviço, e não poderemos continuar de outra forma). As opções para o **Gateway NAT** e o **Grupo de segurança de rede (NSG)** podem ser adicionadas, se necessário (por exemplo, uma regra que força o tráfego por meio da **conversão de endereços de rede (NAT)**). Os campos **Pontos de extremidade de serviço** e **Delegação de sub-rede** não são necessários, e como essa sub-rede deve ser dedicada apenas ao Azure Bastion, não é recomendável usá-los:

**Add subnet**

Packt-Portal

Name \*

 ✓

Address range (CIDR block) \* ⓘ

10.10.4.0/27 ✓  
10.10.4.0 - 10.10.4.31 (27 + 5 Azure reserved addresses)

NAT gateway ⓘ

None ✓

Add IPv6 address space

Network security group

None ✓

Route table

None ✓

Service endpoints

Services ⓘ

0 selected ✓

Subnet delegation

Delegate subnet to a service ⓘ

None ✓

Figura 9.2: Preencher Nome e Intervalo de endereços da sub-rede

## Como fazer isso...

Para criar uma nova instância do Azure Bastion, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Azure Bastion** em **Rede** (ou pesquise **Azure Bastion** na barra de pesquisa).
2. No novo painel, devemos fornecer informações para os campos **Assinatura**, **Grupo de recursos**, **Nome** e **Região**. Em seguida, devemos fazer uma seleção para **Rede virtual** (somente as redes na mesma região estarão disponíveis) e **Sub-rede** (a que criamos anteriormente) e fornecer informações para **Endereço IP público** (selecione um existente ou crie um novo):

### Create a Bastion

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

**Project details**

Subscription *	Microsoft Azure Sponsorship
Resource group *	Packt-Networking-Portal
	<a href="#">Create new</a>

**Instance details**

Name *	Packt-Bastion
Region *	West Europe

**Configure virtual networks**

Virtual network * ⓘ	Packt-Portal
	<a href="#">Create new</a>
Subnet *	AzureBastionSubnet (10.10.4.0/27)
	<a href="#">Manage subnet configuration</a>

**Public IP address**

Public IP address * ⓘ	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing
Public IP address name *	Packt-Bastion-IP
Public IP address SKU	Standard
Assignment	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static

Figura 9.3: Detalhes de configuração de uma instância do Bastion

## Como funciona...

O Azure Bastion é provisionado dentro de nossa rede virtual, o que permite a comunicação com todos os recursos nessa rede. Usando o TLS, ele fornece uma conexão RDP e SSH segura a todos os recursos nessa rede. A conexão é realizada por meio de uma sessão de navegador, e nenhum endereço IP público é necessário. Isso significa que não precisamos expor nenhuma das portas de gerenciamento em um endereço IP público.

Depois de criar a instância do Azure Bastion, vamos avançar para a próxima receita, onde aprenderemos a conectar a uma máquina virtual com o Azure Bastion.

## Conectar a uma máquina virtual com o Azure Bastion

Com o Azure Bastion, podemos nos conectar a uma máquina virtual por meio do navegador sem um endereço IP público e sem expô-la publicamente.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para conectar a uma máquina virtual com o Azure Bastion, devemos seguir estas etapas:

1. No portal do Azure, encontre a máquina virtual à qual você deseja se conectar. A máquina virtual precisa estar na mesma rede virtual em que o Azure Bastion está implantado.
2. No painel **Máquina virtual**, selecione a opção **Conectar** em **Configurações**. Selecione a guia **BASTION** e, nessa guia, selecione **Usar o Bastion**:

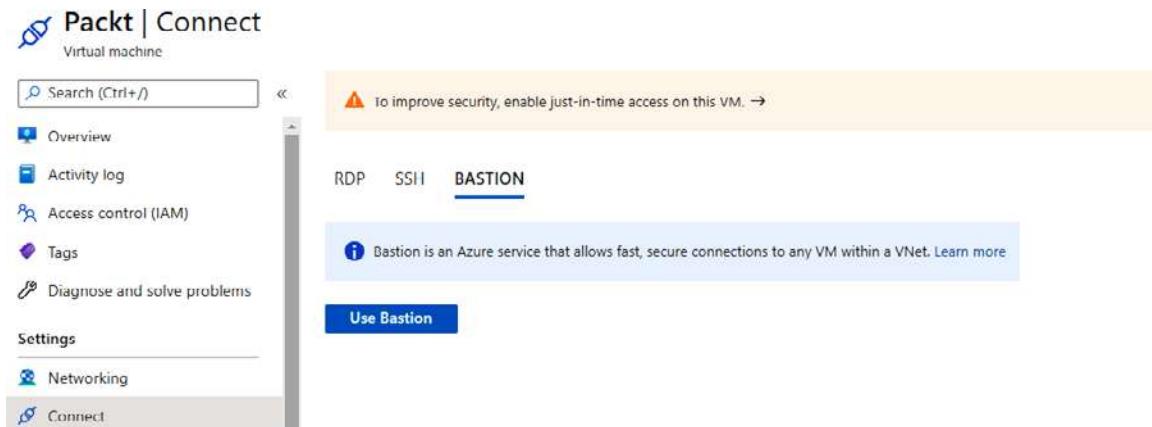
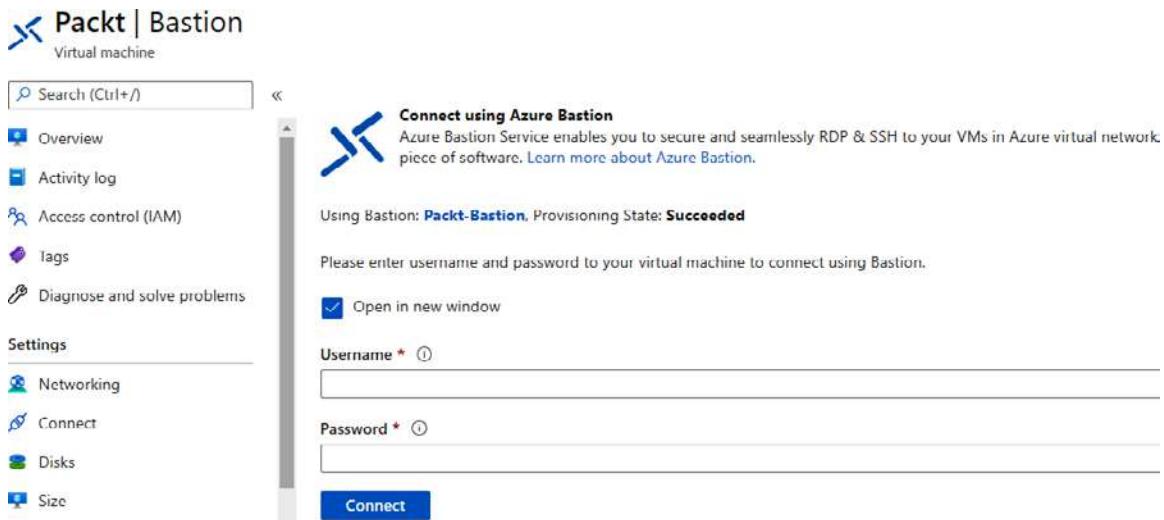


Figura 9.4: Conectar a uma máquina virtual com o Azure Bastion

- Selecione a opção **Abrir em uma nova janela** e preencha **Nome de usuário** e **Senha**:



**Figura 9.5:** Adicionar um nome de usuário e uma senha para a máquina virtual

A conexão abrirá em uma nova janela, permitindo gerenciar totalmente sua máquina virtual. A interface depende da porta de gerenciamento padrão, RDP ou SSH.

## Como funciona...

O Azure Bastion usa uma sub-rede na rede virtual para conectar a máquinas virtuais nessa rede específica. Ele fornece uma conexão segura por TLS e permite uma conexão com uma máquina virtual sem expô-la por um endereço IP público.

Nesta receita, aprendemos a conectar uma máquina virtual ao Azure Bastion. Na próxima receita, aprenderemos como criar uma WAN virtual.

## Criar uma WAN virtual

Em muitas situações, a topologia de rede pode ficar muito complexa. Pode ser difícil acompanhar todas as conexões de rede, gateways e processos de emparelhamento. A WAN Virtual do Azure fornece uma única interface para gerenciar todos esses pontos.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

1. No portal do Azure, selecione **Criar um recurso** e escolha **WAN Virtual** em **Rede** (ou pesquise **WAN Virtual** na barra de pesquisa).
2. No novo painel, devemos fornecer informações para os campos **Assinatura**, **Grupo de recursos**, **Local do grupo de recursos**, **Nome** e **Tipo**:

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)

**Project details**

**Subscription \*** Microsoft Azure Sponsorship

**Resource group \*** Packt-Networking-Portal

**Virtual WAN details**

**Resource group location \*** West Europe

**Name \*** Packt-WAN

**Type** Standard

Figura 9.6: Informações para o recurso de WAN virtual

A WAN Virtual do Azure está pronta para implantação e, geralmente, leva apenas alguns minutos para ser concluída.

## Como funciona...

A WAN Virtual do Azure traz vários serviços de rede para um único ponto. A partir daqui, podemos configurar, controlar e monitorar conexões, como site a site, ponto a site, ExpressRoute ou uma conexão entre redes virtuais. Quando temos várias conexões site a site ou várias redes virtuais conectadas ao emparelhamento, pode ser difícil acompanhar todos esses recursos. A WAN Virtual permite fazer isso com um único serviço.

Isso é feito com hubs e, na próxima receita, veremos como configurar um hub.

## Criar um hub (na WAN Virtual)

Os hubs são usados como pontos de conexão regionais. Eles contêm vários pontos de extremidade de serviço que permitem a conectividade entre diferentes redes e serviços. Eles são o núcleo da rede para cada região.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

1. No portal do Azure, localize a WAN virtual criada anteriormente.
2. No painel **WAN virtual**, selecione **Hubs** na seção **Conectividade**. Selecione a opção para adicionar um novo hub:

The screenshot shows the Azure Portal interface for managing a 'Virtual WAN'. The main title is 'Packt-WAN | Hubs'. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Settings (Configuration, Export template, Properties, Locks), and Connectivity (Hubs). The 'Hubs' link is highlighted with a grey background. The main content area has a search bar at the top labeled 'Search (Ctrl+ /)' and a 'New Hub' button. Below that is another search bar labeled 'Search for hubs by name' and a 'Clear all filters' link. There's also an 'Add filter' button. A table below lists 'Hub', 'Hub status', and 'Region', with a single row 'No results'.

Hub	Hub status	Region
No results		

Figura 9.7: Adicionar um novo hub

3. No novo painel, precisamos fornecer informações nos campos **Região**, **Nome** (para o novo hub) e **Espaço de endereço privado do hub**. **Assinatura** e **Grupo de recursos** estão acinzentados, pois usam as mesmas opções que a WAN Virtual:

## Create virtual hub

The screenshot shows the 'Create virtual hub' wizard. At the top, there are tabs: Basics (selected), Site to site, Point to site, ExpressRoute, Tags, Review + create. Below the tabs, a descriptive text states: "A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). The hub is the core of your network in a region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub VNet and a virtual hub vpngateway. [Learn more](#)".

**Project details**

The hub will be created under the same subscription and resource group as the vWAN.

Subscription	Microsoft Azure Sponsorship
Resource group	Packt-Networking-Portal

**Virtual Hub Details**

Region *	West Europe
Name *	Hub1
Hub private address space * ⓘ	192.168.0.0/16

Figura 9.8: Informações para o novo hub virtual

4. As próximas três etapas são opcionais, e podemos escolher qualquer uma ou todas elas. A primeira etapa é configurar um gateway site a site. Se habilitarmos essa opção, precisaremos selecionar uma opção para **Unidades de escala de gateway** (ou SKU). Um número de sistema autônomo (**Número de AS**) é fornecido para ser usado, se necessário (para configuração de VPN posteriormente):

## Create virtual hub

The screenshot shows the 'Create virtual hub' wizard with the 'Site to site' tab selected. Below the tabs, a note says: "You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)".

Do you want to create a Site to site (VPN gateway)?  Yes  No

AS Number ⓘ	65515
*Gateway scale units ⓘ	1 scale unit - 500 Mbps x 2

Figura 9.9: Configurar um gateway site a site

5. A próxima configuração opcional é **Ponto a site**. Se optarmos por habilitá-lo, precisaremos selecionar uma opção para **Unidades de escala de gateway** e **Configuração de ponto a site**. Clique em **Criar novo** para adicionar uma nova configuração:

## Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site gateway before connecting end-user devices. You can do this after hub creation, but doing now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Point to site (User VPN gateway)?  Yes  No

\*Gateway scale units ⓘ

Point to site configuration \* ⓘ  [Create new](#)

Client address pool

i.e. 10.0.0.0/24

Custom DNS Servers

 At the most 5 custom DNS servers can be provided

Figura 9.10: Configurar um gateway ponto a site

6. No novo painel, precisamos fornecer informações para **Nome da configuração**, **Tipo de túnel** e **Método de autenticação**. Se o **certificado do Azure** for usado, precisaremos fornecer informações de certificado (para obter mais informações sobre certificados, consulte a receita *Criar uma conexão ponto a site no Capítulo 8, Criar conexões híbridas*):

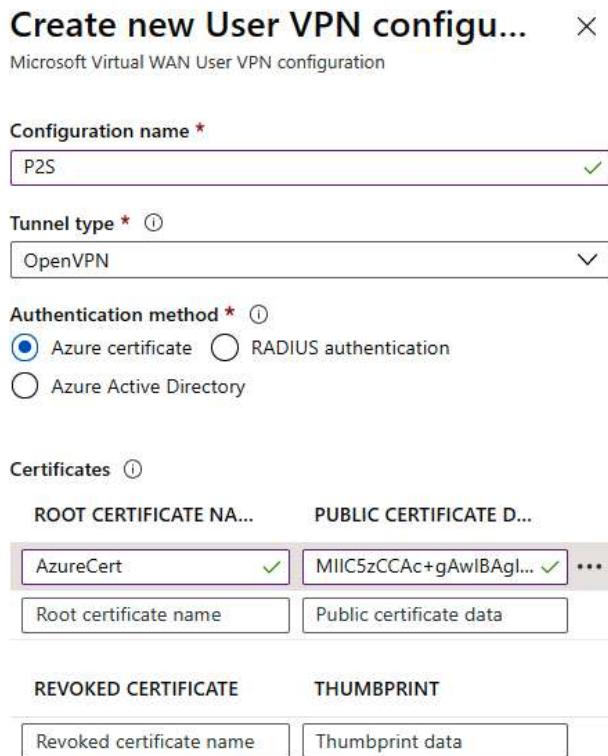


Figura 9.11: Criar uma nova configuração de VPN

7. Depois que a configuração de ponto a site for adicionada, retornaremos ao painel anterior. Precisamos preencher o campo **Pool de endereços do cliente** e, opcionalmente, **Servidores DNS personalizados**:

## Create virtual hub

Basics Site to site **Point to site** ExpressRoute Tags Review + create

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site gateway before connecting end-user devices. You can do this after hub creation, but doing now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Point to site (User VPN gateway)? **Yes** No

\*Gateway scale units ⓘ **1 scale unit - 500 Mbps x 2, supports 500 clients** ▾  
 Point to site configuration \* ⓘ **P2S** ▾  
[Create new](#)

Client address pool

**172.0.0.0/24** ✓

i.e. 10.0.0.0/24

Custom DNS Servers

ⓘ At the most 5 custom DNS servers can be provided

Figura 9.12: Adicionar informações de servidores DNS personalizados e pool de endereços do cliente

8. A terceira configuração opcional é **ExpressRoute**. Se escolhermos habilitá-lo, precisaremos selecionar uma opção para **Unidades de escala de gateway**:

## Create virtual hub

Basics Site to site Point to site **ExpressRoute** Tags Review + create

If you plan to use this hub with ExpressRoutes, you will need to enable an ExpressRoute gateway before connecting to ExpressRoute circuits. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create an ExpressRoute gateway? ⓘ **Yes** No

\*Gateway scale units **1 scale unit - 2 Gbps** ▾

Figura 9.13: Configurar ExpressRoute

9. Opcionalmente, podemos adicionar tags e, em seguida, prosseguir com a criação do hub virtual. Pode levar até 30 minutos para concluir a implantação.

## Como funciona...

Os hubs virtuais representam pontos de controle dentro de uma região. A partir daí, podemos definir todas as conexões com redes virtuais dentro da região. Isso se aplica a site a site, ponto a site e ExpressRoute. Cada seção é opcional, e podemos criar um hub sem configurações para tipos de conexão. Se escolhermos criá-los neste momento, precisaremos fornecer uma SKU para cada tipo. Uma conexão ponto a site também exige que a configuração de VPN do usuário seja disponibilizada. Cada tipo de conexão pode ser adicionado posteriormente também.

Nesta receita, aprendemos a criar um hub virtual. Vamos avançar para a próxima receita e aprender a adicionar uma conexão site a site em um hub virtual.

## Adicionar uma conexão site a site (em um hub virtual)

Depois que um hub virtual for criado e a SKU site a site for definida dentro do hub, podemos prosseguir com a criação de uma conexão site a site. Para isso, precisamos aplicar as configurações de conexão adequadas e fornecer detalhes de configuração.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma conexão site a site em um hub virtual (em uma WAN virtual), devemos seguir as seguintes etapas:

1. Encontre a WAN virtual e localize o hub virtual criado anteriormente em **Hubs** na seção **Conectividade**. Selecione esse hub:

The screenshot shows the Azure portal interface for managing a Virtual WAN. The title bar says "Packt-WAN | Hubs". On the left, there's a sidebar with sections: Overview, Activity log, Access control (IAM), Tags, Settings (Configuration, Export template, Properties, Locks), and Connectivity (Hubs). The "Hubs" item is highlighted with a gray background. The main content area has a search bar "Search (Ctrl+ /)" and a "New Hub" button. Below that is another search bar "Search for hubs by name" and a "Clear all filters" link. A "Hub status" table lists one hub: "Hub1" with a green checkmark and the status "Succeeded".

Figura 9.14: Selecionar o hub criado anteriormente na seção Conectividade

2. No painel **Hub virtual**, acesse as configurações de VPN (**site a site**) em **Conectividade**. Selecione a opção **Criar novo site de VPN**:

**Hub1 | VPN (Site to site)**

Virtual HUB

Search (Ctrl+ /) Download VPN Config Delete gateway Reset gateway

Overview Essentials

ASN : 65515

Gateway scale units : 1 scale unit - 500 Mbps x 2

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Search this page Clear all filters

Hub association : Connected to this hub

VPN Sites

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

Site name Location

No results

Figura 9.15: Selecionar a opção Criar novo site de VPN no painel Hub virtual

3. Um novo painel será exibido. **Assinatura e Grupo de recursos** estão acinzentados, pois o site de VPN é um recurso filho na WAN virtual e deve usar as mesmas opções que a WAN virtual. Precisamos fornecer informações nos campos **Região, Nome** (do site de VPN) e **Fornecedor de dispositivo**. Temos a opção de habilitar ou desabilitar o **Border Gateway Protocol (BGP)**. Se o BGP não estiver configurado, precisaremos fornecer pelo menos um espaço de endereço privado. Também precisamos definir um hub (ou mais deles) que será usado na conexão:

## Create VPN site

**Project details**

Subscription	Microsoft Azure Sponsorship
Resource group	Packt-Networking-Portal

**Instance details**

Region *	West Europe
Name *	VPN1
Device vendor *	Palo Alto
Border Gateway Protocol	<input type="button" value="Enable"/> <input type="button" value="Disable"/>

**Private address space**

At least one address space is required if BGP isn't configured

**Connect to**

Hubs (1)

Hub1	<input type="button" value="Delete"/>
<input type="button" value="Add"/>	

Figura 9.16: Criar um site de VPN

- Na seção **Links** do site de VPN, precisamos fornecer informações para **Nome do link**, **Nome do provedor**, **Velocidade** (em Mbps), **Endereço IP/FQDN** (do dispositivo VPN ao qual desejamos conectar), **Endereço BGP** e **ASN**, conforme mostrado na Figura 9.17:

Basics    **Links**    Review + create

Link Details (1)   

<input type="checkbox"/>	Link name * <small>(1)</small>	Link1	Provider name * <small>(1)</small>	Logosoft
Speed * <small>(1)</small>	100	IP address / FQDN * <small>(1)</small>	217.75.192.10	
BGP address *	192.168.150.5	ASN *	64512	

Figura 9.17: Fornecer detalhes do link no painel Links

5. Depois que o site de VPN for criado, poderemos fazer o download da configuração de VPN para o dispositivo VPN. Depois que o dispositivo VPN estiver configurado, poderemos selecionar o site de VPN e iniciar a conexão com a opção **Conectar sites de VPN**:

**Hub1 | VPN (Site to site)**

**Virtual HUB**

**Overview**

**Connectivity**

**VPN (Site to site)** (selected)

**ExpressRoute**

**User VPN (Point to site)**

**Routing**

**Security**

**Convert to secure hub**

**VPN Sites**

+ Create new VPN site    ⚙ Connect VPN sites    ⚡ Disconnect VPN sites    ⏪ Refresh

Page: 1

Site name	Location	Connection status
VPN1	westeurope	Not connected

Figura 9.18: Clicar na opção Conectar sites de VPN para iniciar a conexão

6. Isso abrirá um novo painel. Devemos fornecer informações para **Chave pré-compartilhada (PSK)**, **Protocolo** e **IPSec** e escolher opções para **Propagar rota padrão** e **Usar política baseada em seletor de tráfego**:

**Connect sites**

**Virtual HUB**

**Security settings**

**Pre-shared key (PSK)**: VerySecureKey2020!

**Protocol**: IKEv2

**IPSec**: Default

**Propagate Default Route**: Disable

**Use policy based traffic selector**: Disable

These sites will be connected to the [Hub1] hub.

Site name	Region
VPN1	westeurope

Figura 9.19: Fornecer informações no painel Conectar sites

## Como funciona...

Adicionar uma conexão site a site ao nosso hub virtual permite conectar a um hub virtual em uma região específica de nossa rede na infraestrutura local (ou outras redes usando o **Dispositivo virtual**). Para fazer isso, devemos fornecer informações sobre a conexão VPN no hub virtual e configurar o dispositivo de VPN que será usado para conectar.

No entanto, isso permite apenas conectar ao hub. Precisamos conectar redes virtuais para acessar os recursos do Azure. Na próxima receita, veremos como adicionar uma conexão de rede virtual ao hub virtual.

## Adicionar uma conexão de rede virtual (em um hub virtual)

Um hub virtual representa um ponto central em uma região do Azure. Mas, para realmente usar esse ponto, precisamos conectar redes virtuais a um hub virtual. Em seguida, podemos usar o hub virtual como pretendido.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar uma conexão de rede virtual em um hub virtual (em uma WAN virtual), devemos seguir estas etapas:

1. Encontre a WAN virtual e localize o hub virtual criado anteriormente em **Coneções de rede virtual** na seção **Conectividade**. Selecione a opção **Adicionar conexão**:

The screenshot shows the 'Virtual network connections' blade in the Azure portal. The title bar says 'Packt-WAN | Virtual network connections'. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Settings (Configuration, Export template, Properties, Locks), Connectivity (Hubs, VPN sites, User VPN configurations, ExpressRoute circuits), and Virtual network connections (which is highlighted with a grey background). At the top right, there's a search bar, an 'Add connection' button, and a 'Refresh' button. The main area displays a table with one row:

Hub	Hub region	Virtual network
Hub1	West Europe	Virtual networks (0)

Figura 9.20: Adicionar um hub virtual criado anteriormente

2. No novo painel, precisamos fornecer informações nos campos **Nome da conexão**, **Hubs**, **Assinatura**, **Grupo de recursos** e **Rede virtual**. Em seguida, precisamos fornecer informações de **Configuração de roteamento**. Podemos selecionar **Sim** para **Propagar para nenhuma**. Se selecionarmos **Não**, precisamos fornecer informações para **Associar tabela de rotas**, **Propagar para tabelas de rotas** e **Propagar para rótulos**. **Rotas estáticas** é uma configuração opcional:

**Add connection** X

**Connection name \***  
Packt-Portal

**Hubs \* (i)**  
Hub1

**Subscription \***  
Microsoft Azure Sponsorship

**Resource group \***  
Packt-Networking-Portal

**Virtual network \***  
Packt-Portal

**Routing configuration (i)**

Propagate to none  
 Yes  No

**Associate Route Table**  
Default

**Propagate to Route Tables**  
Default (Hub1)

**Propagate to labels (i)**  
default

**Static routes (i)**

Route name	Destination prefix	Next hop IP
<input type="text"/>	<input type="text"/>	<input type="text"/>

Figura 9.21: Configurar os detalhes do hub virtual

## Como funciona...

Conectar uma rede virtual a um hub virtual permitirá acessar recursos quando conectados ao mesmo hub. Uma conexão pode ser feita por meio de uma conexão site a site, uma conexão ponto a site ou outra rede virtual (conectado ao mesmo hub). Ao criar uma conexão, precisamos fornecer regras de roteamento e propagação para definir o fluxo de rede. Também podemos definir uma rota estática. Uma rota estática forçará todo o tráfego a percorrer um único endereço IP, geralmente por meio de um firewall ou dispositivo virtual de rede.

Vamos avançar para a próxima receita e aprender a criar um ponto de extremidade do Link Privado.

## Criar um ponto de extremidade do Link Privado

O Link Privado permite conectar aos serviços PaaS por meio de uma rede segura. Como esses serviços geralmente são expostos pela Internet, isso nos oferece um método de acesso mais seguro. Há dois componentes disponíveis para fazer uma conexão segura: um ponto de extremidade do Link Privado e um serviço do Link Privado. Vamos começar criando ponto de extremidade do Link Privado primeiro.

### Preparação

Precisamos criar um serviço que será associado ao Ponto de extremidade do Link Privado:

1. Abra o navegador e acesse o portal do Azure em <https://portal.azure.com>. Selecione a opção para criar um novo serviço. Pesquisa **SQL Server** (servidor lógico) e selecione a opção **Criar novo**.
2. No novo painel, devemos fornecer informações nos campos **Assinatura**, **Grupo de recursos**, **Nome do servidor** (deve ser um FQDN exclusivo) e **Local**. Por fim, devemos fornecer credenciais para o login do administrador antes de selecionar **Revisar + criar**:

## Create SQL Database Server

Microsoft

Basics Networking Additional settings Tags Review + create

SQL database server is a logical container for managing databases and elastic pools. Complete the Basic tab, then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Microsoft Azure Sponsorship"/>
Resource group *	<input type="text" value="Packt-Networking-Portal"/> <a href="#">Create new</a>

### Server details

Enter required settings for this server, including providing a name and location.

Server name *	<input type="text" value="packt"/> .database.windows.net
Location *	<input type="text" value="(Europe) West Europe"/>

### Administrator account

Server admin login *	<input type="text" value="packt"/>
Password *	<input type="password" value="*****"/>
Confirm password *	<input type="password" value="*****"/>

Figura 9.22: Associar um novo serviço a um ponto de extremidade do Link Privado

## Como fazer isso...

Para implantar um novo ponto de extremidade do Link Privado, devemos seguir estas etapas:

1. Acesse o portal do Azure e selecione a opção para criar um novo serviço. Pesquise **Link Privado** e selecione a opção **Criar novo**.
2. No novo painel, **Centro de Link Privado**, selecione **Criar ponto de extremidade privado**:

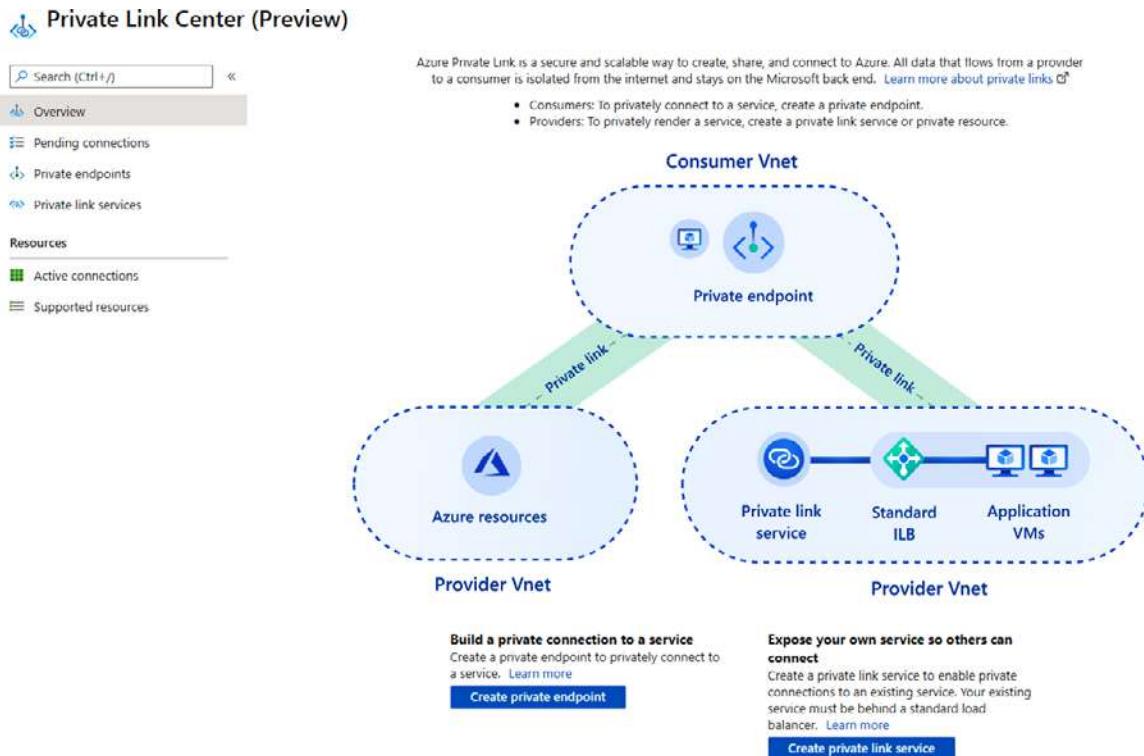


Figura 9.23: Criar um novo ponto de extremidade do Link Privado

3. No novo painel, na seção **Básico**, forneça informações para **Assinatura, Grupo de recursos, Nome e Região**:

## Create a private endpoint

**Basics**    **Resource**    **Configuration**    **Tags**    **Review + create**

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \* ⓘ Microsoft Azure Sponsorship

Resource group \* ⓘ Packt-Networking-Portal

Create new

**Instance details**

Name \* Endpoint1

Region \* (Europe) West Europe

Figura 9.24: Informações básicas para o ponto de extremidade do Link Privado

4. Na seção **Recurso**, devemos selecionar uma opção para **Assinatura, Tipo de recurso** (no nosso caso, **Microsoft.Sql/servers**), **Recurso** (somente recursos do tipo de recurso selecionado estarão disponíveis) e **Sub-recursos de destino**:

## Create a private endpoint

**✓ Basics**    **Resource**    **Configuration**    **Tags**    **Review + create**

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

**Connection method** ⓘ  Connect to an Azure resource in my directory.  Connect to an Azure resource by resource ID or alias.

Subscription \* ⓘ Microsoft Azure Sponsorship

Resource type \* ⓘ Microsoft.Sql/servers

Resource \* ⓘ packt

Target sub-resource \* ⓘ sqlServer

Figura 9.25: Configurar os recursos para o ponto de extremidade do Link Privado

5. No painel **Configuração**, devemos fornecer configurações de **Rede** e selecionar a rede virtual e a sub-rede que serão associadas. Opcionalmente, podemos adicionar a integração com um DNS privado. Se escolhermos adicionar a integração de DNS, devemos fornecer informações para **Assinatura** e **Zonas privadas DNS**:

## Create a private endpoint

✓ Basics   ✓ Resource   3 Configuration   4 Tags   5 Review + create

**Networking**

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network \* ⓘ Packt-Portal

Subnet \* ⓘ BackEnd (10.10.1.0/24)

If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

**Private DNS integration**

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone  Yes  No

Configuration name	Subscription	Private DNS zones
privatelink-database-...	Microsoft Azure Sponsorship	(New) privatelink.database.windows.net

Figura 9.26: Configurar a configuração de rede

## Como funciona...

O ponto de extremidade do Link Privado associa o recurso PaaS selecionado à sub-rede na rede virtual. Ao fazer isso, temos a opção de acessar o recurso PaaS por meio de uma conexão segura. Opcionalmente, podemos integrar uma zona privada DNS e usar a resolução de DNS, em vez de endereços IP.

Um ponto de extremidade do Link Privado permite vincular serviços diretamente, mas somente serviços individuais e somente diretamente. Se precisarmos adicionar平衡adores de carga implantados, podemos usar um serviço do Link Privado.

## Criar um serviço do Link Privado

Um serviço do Link Privado permite configurar uma conexão segura com os recursos associados ao balanceador de carga padrão. Para isso, precisamos preparar a infraestrutura antes da implantação do serviço do Link Privado.

## Preparação

Devemos criar uma máquina virtual primeiro. Confira a receita *Criar de máquinas virtuais do Azure* no Capítulo 2, *Rede de máquinas virtuais*. Observe que, na seção **Rede**, convém selecionar a mesma rede virtual que foi usada para conectar o SQL Server na receita anterior.

Um serviço do Link Privado também exige o balanceador de carga padrão. Veja as receitas *Criar um平衡ador de carga público*, *Criar um pool de back-end*, *Criar investigações de integridade* e *Criar regras de平衡ador de carga* no Capítulo 10, *Balanceadores de carga*. Observe que, no destino de back-end, precisamos selecionar a máquina virtual que acabamos de criar.

Agora, abra o navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para implantar o novo serviço do Link Privado, devemos seguir estas etapas:

1. No portal do Azure, selecione a opção para criar um novo serviço. Pesquise **Link Privado** e selecione a opção **Criar novo**.
2. No novo painel, **Centro de Link Privado**, selecione **Criar serviço do Link Privado**:

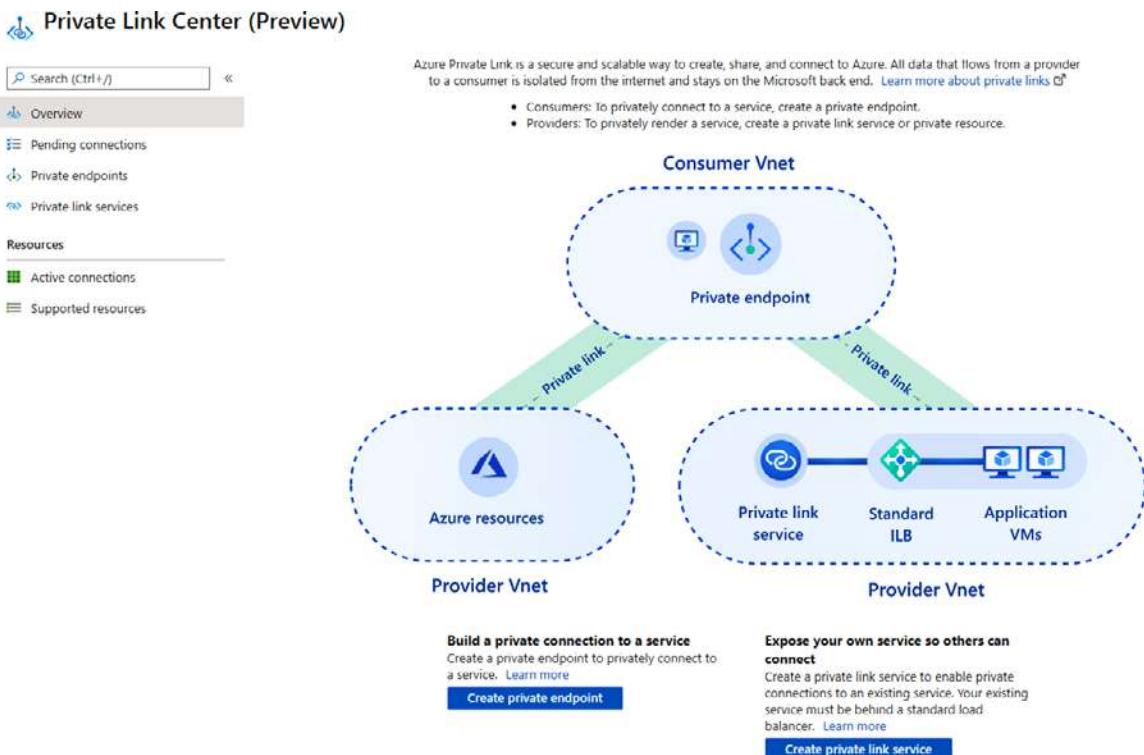


Figura 9.27: Criar um novo serviço do Link Privado

3. Em **Básico**, precisamos fornecer informações para **Assinatura**, **Grupo de recursos**, **Nome** e **Região**:

### Create private link service

**Basics**    ② Outbound settings    ③ Access security    ④ Tags    ⑤ Review + create

Use private endpoints to privately connect to your service or resource. The private link resource can be in any region, regardless of the location of your virtual network. [Learn more](#)

**Project details**

Subscription \* ① Microsoft Azure Sponsorship

Resource group \* ① packt-demo

Create new

**Instance details**

Name \* ① Service1

Region \* ① (Europe) West Europe

Figura 9.28: Informações sobre o novo serviço do Link Privado

4. Em **Configurações de saída**, devemos selecionar opções para **Balanceador de carga**, **Endereço IP de front-end do balanceador de carga** e **Sub-rede NAT de origem**. **Rede virtual NAT de origem** é selecionada e acinzentada automaticamente. Também podemos selecionar **Sim** ou **Não** para **Habilitar proxy TCP V2** e se o endereço IP privado será dinâmico ou estático:

### Create private link service

**Basics**    **Outbound settings**    ③ Access security    ④ Tags    ⑤ Review + create

A private link service enables private connections to a standard load balancer and the virtual machines behind it. Select the standard load balancer, the virtual network, and subnet containing the virtual machines. Private IP addresses will be allocated from the selected subnet. [Learn more](#)

Load balancer \* ① LB1

Load balancer frontend IP address \* ① 51.105.145.61 (LB1-IP)

Source NAT Virtual network ① Packt-Portal (required)

Source NAT subnet \* ① BackEnd (10.10.1.0/24)

Enable TCP proxy V2  Yes  No

**Private IP address settings**

Configure the allocation method and IP address for each NAT IP. Increase the number of NAT IPs to compensate for higher outbound traffic. You can have up to 8 NAT IPs. Dynamic allocation will manage the allocation process for you. Static allocation will require you to specify a public IP address. [Learn more](#)

Allocation	Private IP address	Primary
<input checked="" type="radio"/> Dynamic <input type="radio"/> Static	Yes	
<input type="radio"/> Dynamic <input checked="" type="radio"/> Static	<input type="checkbox"/>	

Figura 9.29: Definir configurações de saída

5. Em **Segurança de acesso**, podemos selecionar quem pode solicitar acesso ao nosso serviço. As opções são **Somente controle de acesso baseado em função (RBAC)**, **Restrito por assinatura** e **Qualquer pessoa com seu alias**. A opção padrão e recomendada é usar o RBAC como controle de acesso nativo no Azure:

## Create private link service

Basics     Outbound settings     Access security     Tags     Review + create

Determine how your private link service will be consumed by consumers without existing permissions. You can expose it using a short friendly name, and auto-approve connections from trusted subscribers. If you already have permissions to the subscription that hosts this private link service, no action is required on this page. [Learn more](#)

### Visibility

The visibility setting determines who can request access to your private link service.

- **Role-based access control only:** This private link service will only be available to individuals with role-based access control permissions within your directory. (Most restrictive)
- **Restricted by subscription:** Any user with access to specific subscriptions (that you'll add below) can request access to your service, even across directories,
- **Anyone with your alias:** Anyone with your private link service alias can request access to your service. (Least restrictive)

Who can request access to your service?  Role-based access control only  
 Restricted by subscription  
 Anyone with your alias

Figura 9.30: O painel Segurança de acesso

## Como funciona...

Um serviço do Link Privado é um ponto de extremidade do Link Privado funcionam de forma semelhante, permitindo conectar a serviços (que são publicamente acessíveis por padrão) por uma rede privada. A principal diferença é que, com um ponto de extremidade do Link Privado, vinculamos os serviços PaaS e, com um serviço do Link Privado, criamos um serviço personalizado por trás do balanceador de carga padrão.



# 10

## Balanceadores de carga

Os **balanceadores de carga** são usados para oferecer suporte à escalabilidade e à alta disponibilidade para aplicações e serviços. Um balanceador de carga é composto principalmente por três componentes: um front-end, um back-end e regras de roteamento. As solicitações que vêm para o frontend de um balanceador de carga são distribuídas com base em regras de roteamento para o back-end, onde podemos colocar várias instâncias de um serviço. Isso pode ser usado por motivos relacionados à performance, em que gostaríamos de distribuir o tráfego igualmente entre pontos de extremidade no back-end ou para alta disponibilidade, em que várias instâncias de serviços são usadas para aumentar as chances de que pelo menos um ponto de extremidade esteja disponível o tempo todo.

Abordaremos as seguintes receitas neste capítulo:

- Criar um balanceador de carga interno
- Criar um balanceador de carga público
- Criar um pool de back-end
- Criar investigações de integridade
- Criar regras de balanceador de carga
- Criar regras de NAT de entrada
- Criar regras de saída explícitas

## Requisitos técnicos

Para este capítulo, é necessária uma assinatura do Azure.

Os exemplos de código podem ser encontrados no <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter10>.

## Criar um balanceador de carga interno

O Microsoft Azure oferece suporte a dois tipos de balanceadores: **internos** e **públicos**. Um balanceador de carga interno recebe um endereço IP privado (do intervalo de endereços de sub-redes na rede virtual) para um endereço IP de front-end e destina-se aos endereços IP privados dos nossos serviços (normalmente, uma **máquina virtual** do Azure (**VM**)) no back-end. Um balanceador de carga interno geralmente é usado por serviços que não são voltados para a Internet e são acessados somente de dentro da nossa rede virtual.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar um novo balanceador de carga interno com o portal do Azure, devemos usar as seguintes etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Balanceador de carga** em **Rede** (ou pesquise **Balanceador de carga** na barra de pesquisa).
2. No novo painel, devemos selecionar uma opção de **Assinatura** e uma opção de **Grupo de recursos** para onde o balanceador de carga deve ser criado. Em seguida, devemos fornecer informações para as opções **Nome**, **Região**, **Tipo** e **SKU**. Nesse caso, selecionamos **Interno** como **Tipo** para implantar um balanceador de carga interno e definimos **SKU** como **Padrão**. Por fim, devemos selecionar a **Rede virtual** e a **Sub-rede** à qual o balanceador de carga será associado, juntamente com as informações da **Atribuição de endereço IP**, que pode ser **Estática** ou **Dinâmica**:

**Project details**

Subscription \* Microsoft Azure Sponsorship

Resource group \* packt-demo [Create new](#)

**Instance details**

Name \* Packt-LoadBalancer-Internal

Region \* (Europe) West Europe

Type \*  Internal  Public

SKU \*  Basic  Standard

**Configure virtual network.**

Virtual network \* packtdemoVM-Vnet

Subnet \* packtdemoVM-subnet (192.168.1.0/24) [Manage subnet configuration](#)

IP address assignment \*  Static  Dynamic

Availability zone \*  Zone-redundant

Figura 10.1: Criar um novo balanceador de carga interno

- Depois que todas as informações forem inseridas, selecionaremos a opção **Revisar + criar** para validar as informações e iniciar a implantação do balanceador de carga.

## Como funciona...

Um balanceador de carga interno é atribuído a um endereço IP privado, e todas as solicitações que chegam ao front-end de um balanceador de carga interno devem chegar a esse endereço privado. Isso limita o tráfego que chega ao balanceador de carga a ser de dentro da rede virtual associada ao balanceador de carga. O tráfego pode vir de outras redes (outras redes virtuais ou redes locais) se houver algum tipo de **rede privada virtual (VPN)** implementada. O tráfego que chega ao front-end do balanceador de carga interno será distribuído entre os pontos de extremidade no back-end do balanceador de carga. Os balanceadores de carga internos geralmente são usados para serviços que não foram colocados em uma **zona desmilitarizada (DMZ)** (e, portanto, não são acessíveis pela Internet), mas sim em serviços de camada intermediária ou inferior em um arquitetura de aplicação de várias camadas.

Também precisamos ter em mente as diferenças entre as SKUs **Básica** e **Padrão**. A principal diferença está na performance (melhor na SKU padrão) e SLA (a padrão tem um SLA garantindo 99,99% de disponibilidade, enquanto a básica não tem SLA). Além disso, observe que a SKU padrão exige um **Grupo de segurança de rede (NSG)**. Se um NSG não estiver presente na sub-rede ou na **Interface de rede**, ou NIC (da VM no back-end), o tráfego não será autorizado a chegar ao seu destino. Para obter mais informações sobre SKUs do balanceador de carga, consulte <https://docs.microsoft.com/azure/load-balancer/skus>.

## Criar um balanceador de carga público

O segundo tipo de balanceador de carga no Azure é um **balanceador de carga público**. A principal diferença é que um balanceador de carga público é atribuído um endereço IP público no front-end, e todas as solicitações chegam por meio da Internet. As solicitações são distribuídas para os pontos de extremidade no back-end.

## Preparação

Antes de iniciar, abra seu navegador e accesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar um novo balanceador de carga público com o portal do Azure, devemos seguir estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Balanceador de carga** em **Rede** (ou pesquise **Balanceador de carga** na barra de pesquisa).

2. No novo painel, devemos selecionar uma opção de **Assinatura** e uma opção de **Grupo de recursos** para onde o balanceador de carga deve ser criado. Em seguida, devemos fornecer informações para **Nome**, **Região**, **Tipo** e **SKU**. Nesse caso, selecionamos **Público** como **Tipo** para implantar um balanceador de carga público e definimos **SKU** como **Padrão**. Selecionar **Público** como o tipo do balanceador de carga alterará um pouco o painel. Não teremos mais a opção de selecionar a rede virtual e a sub-rede, como fizemos para o balanceador de carga interno. Em vez disso, podemos escolher opções para **Endereço IP público** (novo ou existente), **SKU de endereço IP público**, uma atribuição de endereço IP e se queremos usar IPv6. Observe que a SKU de endereço IP público depende diretamente da SKU do balanceador de carga. Por isso, a SKU selecionada para o balanceador de carga será transferida automaticamente para o endereço IP:

## Create load balancer

**Subscription \*** Microsoft Azure Sponsorship

**Resource group \*** packt-demo [Create new](#)

**Instance details**

**Name \*** Packt-LoadBalancer-Public

**Region \*** (Europe) West Europe

**Type \***  Public  Internal

**SKU \***  Basic  Standard

**Public IP address**

**Public IP address \***  Create new  Use existing

**Public IP address name \*** Packt-LoadBalancer-PublicIP

**Public IP address SKU** Standard

**Assignment**  Dynamic  Static

**Availability zone \*** Zone-redundant

Add a public IPv6 address  No  Yes

Figura 10.2: Criar um novo balanceador de carga público

3. Depois que todas as informações forem inseridas, selecione a opção **Revisar + criar** para validar as informações e iniciar a implantação do balanceador de carga.

## Como funciona...

O balanceador de carga público é atribuído um endereço IP público no front-end. Portanto, todas as solicitações que chegam ao balanceador de carga público virão por meio da Internet, direcionadas ao endereço IP público do balanceador de carga. As solicitações são distribuídas para os pontos de extremidade no back-end do balanceador de carga. O que é interessante é que o balanceador de carga público não é direcionado aos endereços IP públicos no back-end, mas aos endereços IP privados. Por exemplo, vamos supor que temos um balanceador de carga público com duas VMs do Azure no back-end. O tráfego que chega ao endereço IP público do balanceador de carga será distribuído para VMs, mas será direcionado aos endereços IP privados das VMs.

Os balanceadores de carga públicos são usados para serviços voltados ao público, mais comumente para servidores Web.

## Criar um pool de back-end

Depois que o balanceador de carga for criado, internamente ou publicamente, precisaremos configurá-lo ainda mais para começar a usá-lo. Durante o processo de criação, definimos o front-end do balanceador de carga e sabemos onde o tráfego precisa ir para chegar ao balanceador de carga. Mas, para definir onde esse tráfego precisa de ir após chegar ao balanceador de carga, primeiro devemos definir um pool de back-end.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar o pool de back-end, devemos fazer o seguinte:

1. No portal do Azure, localize o平衡ador de carga criado anteriormente (interno ou público).
2. No painel **Balanceador de carga**, em **Configurações**, selecione **Pools de back-end**. Selecione **Adicionar** para adicionar o novo pool de back-end:

The screenshot shows the Azure portal interface for managing a load balancer. The title bar reads "Packt-LoadBalancer-Internal | Backend pools". Below the title, it says "Load balancer". On the left, there's a sidebar with icons for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The "Backend pools" option is highlighted with a grey background. At the top right, there are "Add" and "Refresh" buttons. The main content area has two columns: "Backend pool" and "Virtual machine". A message "No results" is displayed under both columns.

Figura 10.3: Adicionar um novo pool de back-end

3. No novo painel, devemos fornecer um **Nome** e especificar ao que o balanceador de carga está associado. As associações podem ser criadas para VMs ou conjuntos de escalas de VM. Neste exemplo, usaremos **Máquinas virtuais**. Com base nesta seleção, você será oferecido mais opções para adicionar VMs ao pool de back-end:

### Add backend pool

Packt-LoadBalancer-Public

Name *	BackendPool1
Virtual network ⓘ	packtdemoVM-Vnet (packt-demo)
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Associated to ⓘ	Virtual machines

**Virtual machines**

You can only attach virtual machines in westeurope that have a basic SKU public IP configuration or no public IP configuration. All virtual machines must be in the same availability set and all IP configurations must be on the same virtual network.

+ Add    X Remove

Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓
No virtual machines selected		

Figura 10.4: Informações adicionais para adicionar o pool de back-end

4. Clique em **Adicionar**, e um novo painel será aberto. Aqui, podemos adicionar as VMs que queremos associar ao pool de back-end. Observe que as VMs devem estar na mesma rede virtual que o balanceador de carga e no mesmo conjunto de disponibilidade. Selecione as VMs que você deseja adicionar ao pool de back-end:

### Add virtual machines to backend pool

! You can only attach virtual machines that are in the same location and on the same virtual network as the loadbalancer. Virtual machines must have a basic SKU public IP or no public IP. All virtual machines must be in the same availability set.

Filter by name...

Location == westeurope	Virtual network == packtdemoVM-Vnet	Resource group == all	Availability set == all
<input checked="" type="checkbox"/> Virtual machine ↑↓	Resource group ↑↓	IP Configuration ↑↓	Availability set ↑↓
<input checked="" type="checkbox"/> packtdemovm-02	packt-demo	packtdemoVM-02 (19... PACKTDEMOVMSSET1	-
<input checked="" type="checkbox"/> packtdemovm-01	packt-demo	packtdemoVM-01 (19... PACKTDEMOVMSSET1	-

Figura 10.5: Adicionar VMs ao pool de back-end

5. Depois que as VMs forem selecionadas, elas serão exibidas na lista de **Máquinas virtuais** para criar o pool. Clique em **Adicionar** para criar o pool de back-end com as VMs associadas:

## Add backend pool

Packt-LoadBalancer-Public

Name *	BackendPool1										
Virtual network	packtdemoVM-Vnet (packt-demo)										
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6										
Associated to	Virtual machines										
<b>Virtual machines</b>											
<a href="#">+ Add</a> <a href="#">X Remove</a>											
<table border="1"> <thead> <tr> <th>Virtual machine ↑↓</th> <th>IP Configuration ↑↓</th> <th>Availability set ↑↓</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> packtdemoVM-01</td> <td>packtdemoVM-01 (192.168.1.4)</td> <td>packtdemoVMset1</td> </tr> <tr> <td><input checked="" type="checkbox"/> packtdemoVM-02</td> <td>packtdemoVM-02 (192.168.1.5)</td> <td>packtdemoVMset1</td> </tr> </tbody> </table>			Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓	<input checked="" type="checkbox"/> packtdemoVM-01	packtdemoVM-01 (192.168.1.4)	packtdemoVMset1	<input checked="" type="checkbox"/> packtdemoVM-02	packtdemoVM-02 (192.168.1.5)	packtdemoVMset1
Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓									
<input checked="" type="checkbox"/> packtdemoVM-01	packtdemoVM-01 (192.168.1.4)	packtdemoVMset1									
<input checked="" type="checkbox"/> packtdemoVM-02	packtdemoVM-02 (192.168.1.5)	packtdemoVMset1									

Figura 10.6: Lista de VMs para a criação de um pool de back-end

6. Depois que a configuração for inserida, reserve alguns minutos para criar o pool de back-end. Depois disso, os recursos associados serão exibidos na lista de pools de back-end:

Packt-LoadBalancer-Internal   Backend pools			
Load balancer		Backend pool	
		Virtual machine	Virtual machine status
Overview			
Activity log		Backend pool	
Access control (IAM)		BackendPool1 (2 virtual machines)	
Tags		packtdemoVM-01	Running
Diagnose and solve problems		packtdemoVM-02	Running
Settings			
Frontend IP configuration			
Backend pools			

Figura 10.7: A lista de pools de back-end

## Como funciona...

Os dois componentes principais de qualquer balanceador de carga são o frontend e o back-end. O front-end define o ponto de extremidade do balanceador de carga, e o back-end define onde o tráfego precisa ir depois de chegar ao balanceador de carga. Como as informações de front-end são criadas juntamente com o balanceador de carga, devemos definir o back-end por conta própria, após o qual o tráfego será distribuído uniformemente em todos os pontos de extremidade no back-end. As opções disponíveis para o pool de back-end são VMs e conjuntos de escalas de VM.

## Consulte também

Mais informações sobre VMs, conjuntos de disponibilidade e conjunto de escalas de VMs estão disponíveis em meu livro *Administração de nuvem prática no Azure*, publicado pela Packt em <https://www.packtpub.com/virtualization-and-cloud/hands-cloud-administration-azure>.

## Criar investigações de integridade

Depois que o front-end e o back-end do balanceador de carga forem definidos, o tráfego é distribuído uniformemente entre os pontos de extremidade no back-end. Mas e se um dos pontos de extremidade não estiver disponível? Nesse caso, algumas das solicitações falharão até detectarmos o problema ou até mesmo falharão indefinidamente caso o problema permaneça não detectado. O balanceador de carga enviará uma solicitação para todos os pontos de extremidade definidos no pool de back-end, e a solicitação falhará quando direcionada para um servidor não disponível.

É por isso que apresentamos os próximos dois componentes no balanceador de carga: **investigações de integridade e regras**. Esses componentes são usados para detectar problemas e definir o que fazer quando problemas são detectados.

As investigações de integridade monitoram constantemente todos os pontos de extremidade definidos no pool de back-end e detectam se algum deles não está disponível. Elas fazem isso enviando uma investigação no protocolo configurado e escutando uma resposta. Se uma investigação HTTP estiver configurada, uma resposta HTTP 200 OK será necessária para ser considerada bem-sucedida.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma nova investigação de integridade no balanceador de carga, devemos fazer o seguinte:

1. No portal do Azure, localize o balanceador de carga criado anteriormente (interno ou público).

2. No painel **Balanceador de carga**, em **Configurações**, selecione **Investigações de integridade**. Selecione **Adicionar** para adicionar uma nova investigação de integridade:

The screenshot shows the AWS Lambda console interface. On the left, there's a sidebar with links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Frontend IP configuration, Backend pools, and Health probes (which is highlighted with a grey background). The main content area is titled 'Packt-LoadBalancer-Internal | Health probes'. It has a search bar labeled 'Search (Ctrl+ /)' and a '+' Add button. Below that is a table with columns: Name, Protocol, Port, and Used By. A message 'No results.' is displayed.

Figura 10.8: Adicionar uma nova investigação de integridade

3. No novo painel, precisamos fornecer informações sobre o **Nome** e a versão IP ou o **Protocolo** da investigação de integridade que queremos usar, bem como configurar as opções **Porta**, **Intervalo** e **Limite não íntegro**, conforme mostrado na Figura 10.9:

The screenshot shows the 'Add health probe' dialog. It has a title 'Add health probe' and a subtitle 'Packt-LoadBalancer-Internal'. There are several input fields: 'Name \*' with value 'HTTPS', 'Protocol \*' with value 'TCP', 'Port \*' with value '443', 'Interval \*' with value '5' followed by 'seconds', and 'Unhealthy threshold \*' with value '2' followed by 'consecutive failures'.

Figura 10.9: Fornecer informações sobre a investigação de integridade

4. Depois de selecionar **OK**, a nova investigação de integridade será criada e exibida na lista de investigações de integridade disponíveis associadas ao balanceador de carga.

## Como funciona...

Depois que definirmos a investigação de integridade, ela será usada para monitorar os pontos de extremidade no pool de back-end. Definimos o protocolo e a porta como informações úteis que fornecerão informações sobre se o serviço que estamos usando está disponível ou não. O monitoramento do estado do servidor não será suficiente, pois pode estar equivocado. Por exemplo, o servidor pode estar em execução e disponível, mas o servidor IIS ou SQL que usamos pode não estar disponível. Assim, o protocolo e a porta detectarão as alterações no serviço em que estamos interessados, e não somente se o servidor está em execução. O intervalo define a frequência com que uma verificação é executada, e o limite não íntegro define depois de quantas falhas consecutivas o ponto de extremidade é declarado como não disponível.

## Criar regras de balanceador de carga

A última peça do quebra-cabeça ao falar sobre balanceadores de carga do Azure refere-se à **regra**. Por fim, as regras interligam tudo e definem qual investigação de integridade (pode haver mais de uma) monitorará qual pool de back-end (mais de um pode estar disponível). Além disso, as regras permitem o mapeamento de porta do front-end de um balanceador de carga para o pool de back-end, definindo como as portas se relacionam e como o tráfego de entrada é encaminhado para o back-end.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma regra de balanceador de carga, devemos fazer o seguinte:

1. No portal do Azure, localize o balanceador de carga criado anteriormente (interno ou público).
2. No painel **Balanceador de carga**, em **Configurações**, selecione **Regras de balanceamento de carga**. Selecione **Adicionar** para adicionar uma regra de balanceamento de carga:

The screenshot shows the Azure portal interface for managing a load balancer named 'Packt-LoadBalancer-Internal'. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools, Health probes, and Load balancing rules. The 'Load balancing rules' option is currently selected. The main content area has a search bar at the top and a table below it. The table has columns for 'Name', 'Load balancing rule', 'Backend pool', and 'Health probe'. A note says 'No results.' The table is currently empty.

Figura 10.10: Adicionar regras de平衡amento de carga

3. No novo painel, devemos fornecer informações para o **Nome** e a **Versão IP** que vamos usar, qual **Endereço IP de front-end** que vamos usar (pois um balanceador de carga pode ter mais de um), o **Protocolo** e o mapeamento de **Porta** (o tráfego da porta de entrada será encaminhado para a porta de back-end). Se habilitarmos as portas de alta disponibilidade (disponíveis somente em平衡adores de carga internos), isso removerá as opções de protocolo e habilitará o平衡amento de carga em todas as portas para protocolos TCP e UDP. Além disso, precisamos fornecer informações para as configurações **Porta de back-end**, **Pool de back-end**, **Investigação de integridade**, **Persistência de sessão** e **Tempo ocioso (minutos)**, e decidir se queremos usar um IP flutuante: **IP flutuante**. Por fim, temos a opção de criar uma regra de saída implícita:

**Add load balancing rule**

Packt-LoadBalancer-Public

Name **\***  
Rule1

IP Version **\***  
 IPv4  IPv6

Frontend IP address **\*** ⓘ  
192.168.1.6 (LoadBalancerFrontEnd)

HA Ports ⓘ

Protocol  
 TCP  UDP

Port **\***  
443

Backend port **\*** ⓘ  
443

Backend pool ⓘ  
BackendPool1 (2 virtual machines)

Health probe ⓘ  
HTTPS (TCP:443)

Session persistence ⓘ  
None

Idle timeout (minutes) ⓘ  
4

TCP reset  
 Disabled  Enabled

Floating IP (direct server return) ⓘ  
 Disabled  Enabled

Create implicit outbound rules ⓘ  
 Yes  No

Figura 10.11: Configurar regras de平衡amento de carga

4. Depois de selecionarmos **OK**, uma nova regra será criada, que será exibida na lista de regras de平衡amento de carga disponíveis.

## Como funciona...

A regra do balanceador de carga é a última peça que interliga todos os componentes. Definimos qual endereço IP de front-end é usado e para qual back-end o tráfego do pool será encaminhado. A investigação de integridade é atribuída para monitorar os pontos de extremidade no pool de back-end e para controlar se há pontos de extremidade não responsivos. Também criamos um mapeamento de porta que determinará qual protocolo e porta o balanceador de carga escutará e, quando o tráfego chegar, para onde esse tráfego será encaminhado.

Como modo de distribuição padrão, o Azure Load Balancer usa um hash de cinco tuplas (IP de origem, porta de origem, IP de destino, porta de destino e tipo de protocolo). Se alterarmos a persistência da sessão para o **IP do cliente**, a distribuição será de duas tuplas (as solicitações do mesmo endereço IP do cliente serão tratadas pela mesma VM). Alterar a persistência da sessão para **Protocolo e IP do cliente** alterará a distribuição para três tuplas (as solicitações da mesma combinação de protocolo e endereço IP do cliente serão tratadas pela mesma VM).

## Criar regras de NAT de entrada

As regras de **Conversão de Endereço de Rede (NAT)** de entrada são uma configuração opcional do Azure Load Balancer. Basicamente, essas regras criam outro mapeamento de porta do front-end para o back-end, encaminhando o tráfego de uma porta específica no front-end para uma porta específica no back-end. A diferença entre as regras de NAT de entrada e o mapeamento de porta nas regras do balanceador de carga é que as regras de NAT de entrada se aplicam ao encaminhamento direto a uma VM, enquanto o balanceador de carga encaminha o tráfego a um pool de back-end.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma nova regra de NAT de entrada, devemos fazer o seguinte:

1. No portal do Azure, localize o balanceador de carga criado anteriormente (interno ou público).
2. No painel **Balanceador de carga**, em **Configurações**, selecione **Regras de NAT de entrada**. Selecione **Adicionar** para adicionar uma nova regra de NAT de entrada:

Packt-LoadBalancer-Internal | Inbound NAT rules

Search (Ctrl + /)  Add Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Frontend IP configuration Backend pools Health probes Load balancing rules Inbound NAT rules

Add a rule to get started

Name	IP Version	Destination	Target	Service

Figura 10.12: Adicionar uma regra de NAT de entrada para um平衡ador de carga existente

3. No novo painel, devemos fornecer detalhes para os campos **Nome**, **IP de front-end endereço**, **Versão IP** (definido com base no endereço IP de front-end), **Serviço**, **Protocolo** e **Porta**. Também podemos editar o **Tempo limite de inatividade**, que é definido como 4 minutos por padrão. Selecione **Máquina virtual de destino** e **Configuração IP de rede** para a mesma máquina (se a VM tiver mais de uma configuração de IP). Por fim, você pode selecionar o mapeamento de porta padrão ou use um personalizado:

### Add inbound NAT rule

Packt-LoadBalancer-Internal

i An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.

Name *	<input type="text" value="NATRule01"/>	<span style="color: #0070C0;">✓</span>
Frontend IP address *	<input type="text" value="LoadBalancerFrontEnd (192.168.1.6)"/>	
IP Version	IPv4	
Service *	<input type="text" value="MS SQL"/>	
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP
Idle timeout (minutes)	<input type="range" value="4"/>	4 Max: 30
Port *	<input type="text" value="1433"/>	
Target virtual machine	<input type="text" value="packtdemoVM-01 (packt-demo)"/>	
Network IP configuration	<input type="text" value="packtdemoVM-01 (192.168.1.4)"/>	
Port mapping	<input checked="" type="radio"/> Default <input type="radio"/> Custom	

Figura 10.13: Definir configurações de regra de NAT de entrada

4. Depois de selecionar **OK**, uma nova regra de NAT de entrada será criada.

## Como funciona...

As regras de NAT de entrada permitem usar o IP público do balanceador de carga para conectar diretamente a uma instância de back-end específica. Elas criam um mapeamento de porta semelhante ao mapeamento de porta criado pelas regras do balanceador de carga, mas para uma instância de back-end específica. Uma regra do balanceador de carga cria configurações adicionais, como a investigação de integridade ou a persistência da sessão. As regras de NAT de entrada excluem essas configurações e criam um mapeamento incondicional do front-end para o back-end. Com uma regra de NAT de entrada, o tráfego encaminhado sempre chegará ao único servidor no back-end, enquanto um balanceador de carga encaminhará o tráfego para o pool de back-end e usará um algoritmo pseudo-round-robin para rotear o tráfego para qualquer um dos servidores íntegros no pool de back-end.

## Criar regras de saída explícitas

Ao criar regras de平衡amento de carga, podemos criar regras de saída implícitas. Isso habilitará **Conversão de Endereços de Rede de Origem (SNAT)** para VMs no pool de back-end e permitirá que eles acessem a Internet pelo IP público do balanceador de carga (especificado na regra). Mas, em alguns cenários, as regras implícitas não são suficientes e precisamos criar regras de saída explícitas. As regras de saída explícitas (e SNAT em geral) estão disponíveis apenas para平衡adores de carga públicos com a SKU padrão.

## Preparação

Antes de começar, certifique-se de que as regras de saída implícitas estejam desabilitadas nas regras de平衡amento de carga:

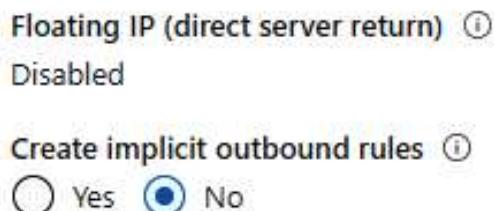


Figura 10.14: Desabilitar regras de saída implícitas

Agora, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar uma regra de balanceador de carga, devemos fazer o seguinte:

1. No portal do Azure, localize o平衡ador de carga público criado anteriormente.
2. No painel **Balanceador de carga**, em **Configurações**, selecione **Regras de saída**.  
Selecione **Adicionar** para adicionar a regra de balanceamento de carga:

The screenshot shows the Azure portal interface for managing a load balancer named 'Pack-Loadbalancer-Public'. The left sidebar lists various configuration options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools, Health probes, Load balancing rules, Inbound NAT rules, and Outbound rules. The 'Outbound rules' option is highlighted with a gray selection bar at the bottom. The main content area is titled 'Outbound rules' and contains a search bar ('Search (Ctrl+ /)'), a 'Add' button, and a 'Refresh' button. A descriptive text block explains that outbound rules are used to configure the outbound network pool and that at least one public IP address is required. Below this is a 'Filter by name...' search bar, a 'Name' input field, and a placeholder text 'Add a rule to get started'.

Figura 10.15: Adicionar regras de saída

3. No painel **Regras de saída**, devemos fornecer o nome da regra e selecionar opções para os campos **Endereço IP de front-end**, **Protocolo** (Todos, TCP ou UDP), **Tempo limite de inatividade**, **Redefinição de TCP** e **Pool de back-end**. Na seção **Alocação de porta**, **Portas de saída**, **Portas por instância** (desabilitado quando o número máximo de instâncias de back-end é selecionado) e **Número máximo de instâncias de back-end**:

## Add outbound rule

Pack-Loadbalancer-Public

Name *	<input type="text" value="OutRule1"/> <span style="color: green;">✓</span>
Frontend IP address * ⓘ	<input type="text" value="1 selected"/> <span style="color: green;">✓</span> <a href="#">Create new</a>
Protocol	<input checked="" type="radio"/> All <input type="radio"/> TCP <input type="radio"/> UDP
Idle timeout (minutes) ⓘ	<input type="range" value="4"/> <span style="border: 1px solid #ccc; padding: 2px;">4</span> Max: 30
TCP Reset ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Backend pool * ⓘ	<input type="text" value="BackendPool1 (2 instances)"/> <span style="color: green;">✓</span> <a href="#">Create new</a>

### Port allocation

Azure automatically assigns the number of outbound ports to use for source network address translation (SNAT) based on the number of frontend IP addresses and backend pool instances. [Learn more about outbound connectivity](#) ↗

Port allocation ⓘ	<input type="text" value="Manually choose number of outbound ports"/> <span style="color: green;">✓</span>
Outbound ports	
Choose by *	<input type="text" value="Maximum number of backend instances"/> <span style="color: green;">✓</span>
Ports per instance ⓘ	0
Frontend IPs	1
Maximum number of backend instances ⓘ	<input type="text" value="2"/> <span style="color: green;">✓</span>

Figura 10.16: O painel de regras de saída

## Como funciona...

As regras de saída dependem de três itens: endereços IP de front-end, instâncias no pool de back-end e conexões. Cada endereço IP de front-end tem um número limitado de portas para conexões. Quanto mais endereços IP forem atribuídos ao front-end, mais conexões serão permitidas. Por outro lado, o número de conexões permitidas (por instância de back-end) diminui com o número de instâncias no back-end.

Se definimos o número padrão de portas de saída, a alocação é feita automaticamente e sem controle. Se tivermos um conjunto de escalas de VM definido com o número padrão de instâncias, a alocação de porta será feita automaticamente para cada VM no conjunto de escalas. Se o número de instâncias em um conjunto de escalas aumentar, isso significará que o número de portas alocadas para cada VM diminuirá.

Para evitar isso, podemos definir a alocação de porta para manual e limitar o número de instâncias que são permitidas ou limitar o número de portas por instância. Isso garantirá que cada VM tenha um determinado número de portas dedicadas e que as conexões não serão descartadas.



# 11

## Gerenciador de Tráfego

O Azure Load Balancer é limitado a fornecer alta disponibilidade e escalabilidade apenas para **máquinas virtuais do Azure (VMs)**. Além disso, um único balanceador de carga é limitado a VMs em uma única região do Azure. Se quisermos fornecer alta disponibilidade e escalabilidade a outros serviços do Azure distribuídos globalmente, deveremos apresentar um novo componente: o **Gerenciador de Tráfego do Azure**.

O Gerenciador de Tráfego do Azure é baseado em DNS e fornece a capacidade de distribuir o tráfego por meio de serviços e distribuir o tráfego entre regiões do Azure. Mas o Gerenciador de Tráfego não é limitado somente aos serviços do Azure. Também podemos adicionar pontos de extremidade externos.

Abordaremos as seguintes receitas neste capítulo:

- Criar um novo perfil do Gerenciador de Tráfego
- Adicionar um ponto de extremidade
- Configurar o tráfego distribuído
- Configurar o tráfego com base na prioridade
- Configurar o tráfego com base na localização geográfica
- Gerenciar pontos de extremidade
- Gerenciar perfis
- Configurar o Gerenciador de Tráfego com平衡adores de carga

## Requisitos técnicos

Para este capítulo, é necessária uma assinatura do Azure.

Os exemplos de código podem ser encontrados no <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter11>.

## Criar um novo perfil do Gerenciador de Tráfego

O Gerenciador de Tráfego fornece balanceamento de carga para serviços, mas o tráfego é roteado e direcionado usando entradas de DNS. O front-end é um **Nome de Domínio Totalmente Qualificado (FQDN)** atribuído durante a criação, e todo o tráfego que chega ao Gerenciador de Tráfego é distribuído aos pontos de extremidade no back-end. Nesta receita, criaremos um novo perfil do Gerenciador de Tráfego.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar um novo perfil do Gerenciador de Tráfego, devemos fazer o seguinte:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Perfil do Gerenciador de Tráfego** nos serviços de **Rede** (ou pesquise **Perfil do Gerenciador de Tráfego** na barra de pesquisa).
2. No novo painel, devemos fornecer informações para os campos **Nome**, **Método de roteamento**, **Assinatura** e **Grupo de recursos**:

### Create Traffic Manager profile

The screenshot shows the 'Create Traffic Manager profile' wizard. The first step, 'Set profile details', is displayed. The 'Name \*' field contains 'packt-demo'. Below it, a tooltip shows '.trafficmanager.net'. The 'Routing method' dropdown is set to 'Performance'. The 'Subscription \*' dropdown shows 'Microsoft Azure Sponsorship'. The 'Resource group \*' dropdown shows 'packt-demo-webapp', with a 'Create new' link below it. The 'Resource group location' dropdown is set to 'West Europe'.

Figura 11.1: Fornecer informações para um novo perfil do Gerenciador de tráfego

3. Observe que, nos métodos de roteamento, temos várias opções para escolher: **Performance, Ponderado, Prioridade, Geográfico, Vários valores e Sub-rede**. Para esta receita, vamos deixar a opção padrão (**Performance**), mas vamos abordar o restante dos métodos de roteamento em outras receitas deste capítulo:

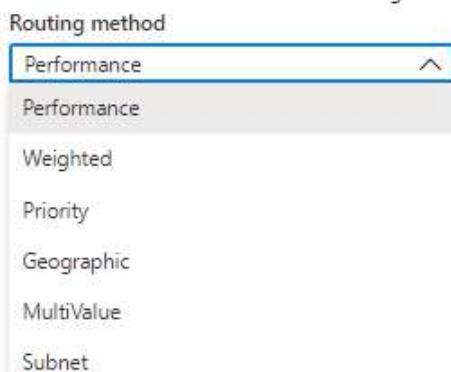


Figura 11.2: Selecionar o método de roteamento

## Como funciona...

O Gerenciador de Tráfego é atribuído um ponto de extremidade público que deve ser um FQDN. Todo o tráfego que chega nesse ponto de extremidade será distribuído aos ponto de extremidade no back-end, usando o método de roteamento selecionado. O método de roteamento padrão é **Performance**. O método de performance distribuirá o tráfego com base na melhor performance possível disponível. Por exemplo, se tivermos mais de um ponto de extremidade de back-end na mesma região, o tráfego será distribuído uniformemente. Se os pontos de extremidade estiverem localizados em regiões diferentes, o Gerenciador de Tráfego direcionará o tráfego para o ponto de extremidade mais próximo do tráfego de entrada em termos de localização geográfica e latência de rede mínima.

Vamos passar para a próxima receita e adicionar um ponto de extremidade ao Gerenciador de tráfego.

## Adicionar um ponto de extremidade

Depois que um perfil do Gerenciador de Tráfego for criado, temos o ponto de extremidade do front-end e o método de roteamento definidos. Mas ainda precisamos definir onde o tráfego precisa ir depois que chegar ao Gerenciador de Tráfego. Precisamos adicionar pontos de extremidade ao back-end e definir onde o tráfego é direcionado. Nesta receita, adicionaremos um novo ponto de extremidade ao Gerenciador de Tráfego.

## Preparação

Antes de podermos adicionar pontos de extremidade ao Gerenciador de tráfego, precisamos criá-los. A execução do script a seguir no PowerShell pode ajudá-lo a criar dois aplicativos Web rapidamente:

```
$ResourceGroupName = "packt-demo-webapp"  
$webappname="packt-demo-webapp"  
$location1="West Europe"  
$NumberOfWebApps= 2  
  
New-AzResourceGroup -Name $ResourceGroupName '  
-Location $location  
$i=1  
Do  
{  
New-AzWebApp -Name $webappname'-0'$i '  
-Location $location '  
-AppServicePlan $webappname '  
-ResourceGroupName $ResourceGroupName  
} While (($i=$I+1) -le $NumberOfWebApps)
```

O script pode ser editado para implantar mais de dois aplicativos Web, se necessário. No entanto, para aproveitar ao máximo o Gerenciador de tráfego, é melhor ter aplicativos Web em diferentes regiões.

Depois que o script for concluído, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar pontos de extremidade ao Gerenciador de Tráfego, devemos fazer o seguinte:

1. No portal do Azure, localize o perfil do Gerenciador de Tráfego criado anteriormente.
2. No painel **Perfil do Gerenciador de Tráfego**, em **Configurações**, selecione **Pontos de extremidade**. Selecione **Adicionar** para adicionar um novo ponto de extremidade.

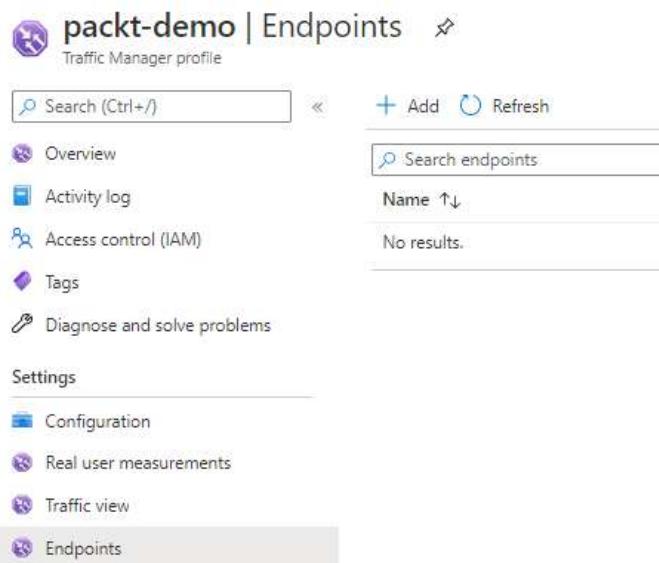


Figura 11.3: Adicionar um novo ponto de extremidade

3. No novo painel, precisamos fornecer informações para os campos **Tipo** (do ponto de extremidade que estamos adicionando) e **Nome**. Para **Tipo**, podemos escolher entre **Azure**, **Externo** e **Aninhado**. Se **Azure** for selecionado, poderemos selecionar determinados tipos de recursos de destino (**Serviços de nuvem**, **Serviço de aplicativo** ou **slot**, and **Endereço IP público**) e, com base na seleção de tipo de recurso de destino, poderemos selecionar recursos que sejam adequados ao tipo de recurso de destino selecionado. Aqui, selecionamos **packt-demo-webapp01**, que criamos anteriormente:

Type *	<input type="text" value="Azure endpoint"/>
Name *	<input type="text" value="packt1"/>
Target resource type	<input type="text" value="App Service"/>
Target resource *	<input type="text" value="packt-demo-webapp-01 (West Europe)"/>
Custom Header settings	<input type="text"/>
<input type="checkbox"/> Add as disabled	

Figura 11.4: Configurar o tipo de ponto de extremidade

4. Adicionar um único ponto de extremidade só funcionará como um redirecionamento de um FQDN para outro. Precisamos repetir o processo pelo menos mais uma vez e adicionar pelo menos mais um ponto de extremidade:

Type \* ⓘ  
Azure endpoint

Name \*  
packt2

Target resource type  
App Service

Target resource \*  
packt-demo-webapp-2 (West US)

Custom Header settings ⓘ

Add as disabled

Figura 11.5: Adicionar um ponto de extremidade secundário

5. Todos os pontos de extremidade adicionados serão exibidos na seção **Ponto de extremidade** na opção **Configurações** do Gerenciador de Tráfego:

Name	Status	Monitor status	Type	Location
packt1	Enabled	Online	Azure endpoint	West Europe
packt2	Enabled	Online	Azure endpoint	West US

Figura 11.6: Uma lista de pontos de extremidade

## Como funciona...

As solicitações de entrada chegam ao Gerenciador de Tráfego atingindo o ponto de extremidade de front-end do Gerenciador de Tráfego. Com base nas regras (principalmente o método de roteamento), o tráfego é encaminhado para os pontos de extremidade de back-end. O balanceador de carga funciona encaminhando o tráfego para endereços IP privados. Por outro lado, o Gerenciador de Tráfego usa pontos de extremidade públicos no back-end. Os tipos de ponto de extremidade compatíveis são externos, aninhados e do Azure. Com base no tipo de ponto de extremidade, podemos adicionar pontos de extremidade externos ou do Azure. Pontos de extremidade podem ser FQDNs (públicos) ou endereços IP públicos. Os pontos de extremidade aninhados permitem adicionar outros perfis do Gerenciador de Tráfego ao back-end do Gerenciador de Tráfego.

As configurações personalizadas de cabeçalho adicionam cabeçalhos HTTP específicos às verificações de integridade que o Gerenciador de Tráfego envia aos pontos de extremidade em um perfil. Elas podem ser definidas no nível do perfil (e aplicadas a todos os pontos de extremidade do perfil) ou para cada ponto de extremidade individual. Ele vem no formato **header:value** podemos adicionar até 8 pares (**header1:value1, header2:value2, header3:value3...**)

Depois de adicionar pontos de extremidade ao Gerenciador de tráfego, vamos avançar para a próxima receita e aprender a configurar o tráfego distribuído.

## Configurar o tráfego distribuído

O método de roteamento padrão para o Gerenciador de Tráfego é performance. O método de performance distribuirá o tráfego com base na melhor performance possível disponível. Esse método só terá efeito completo se tivermos várias instâncias de um serviço em várias regiões. Como isso geralmente não é o caso, outros métodos estão disponíveis, como o tráfego distribuído (também conhecido como método de roteamento ponderado). Nesta receita, configuraremos o Gerenciador de Tráfego para funcionar no modo distribuído.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para definir o tráfego distribuído, devemos fazer o seguinte:

1. No portal do Azure, localize o perfil do Gerenciador de Tráfego criado anteriormente.
2. Em **Configurações**, selecione a opção **Configuração**. Aqui, temos várias opções que podemos alterar, como o **DNS time to live (TTL)**, protocolos e configurações de failover:

**packt-demo | Configuration**  
Traffic Manager profile

Search (Ctrl+ /) Save Discard

**Overview** Routing method: Performance

**Activity log**

**Access control (IAM)** DNS time to live (TTL): 60 seconds

**Tags**

**Diagnose and solve problems**

**Settings**

- Configuration** (selected)
- Real user measurements
- Traffic view
- Endpoints
- Properties
- Locks
- Export template

**Monitoring**

- Alerts
- Metrics
- Diagnostic settings
- Logs

**Support + troubleshooting**

**Resource health**

**Routing method**: Performance

**DNS time to live (TTL)**: 60 seconds

**Protocol**: HTTP

**Port**: 80

**Path**: /

**Custom Header settings**

**Expected Status Code Ranges (default: 200)**

**Fast endpoint failover settings**

**Probing interval**: 30 seconds

**Tolerated number of failures**: 3

**Probe timeout**: 10 seconds

Figura 11.7: O painel Configuração do Gerenciador de tráfego

3. Altere o **Método de roteamento** para **Ponderado**, conforme mostrado na Figura 11.8. Além disso, podemos configurar as definições de peso, se necessário:

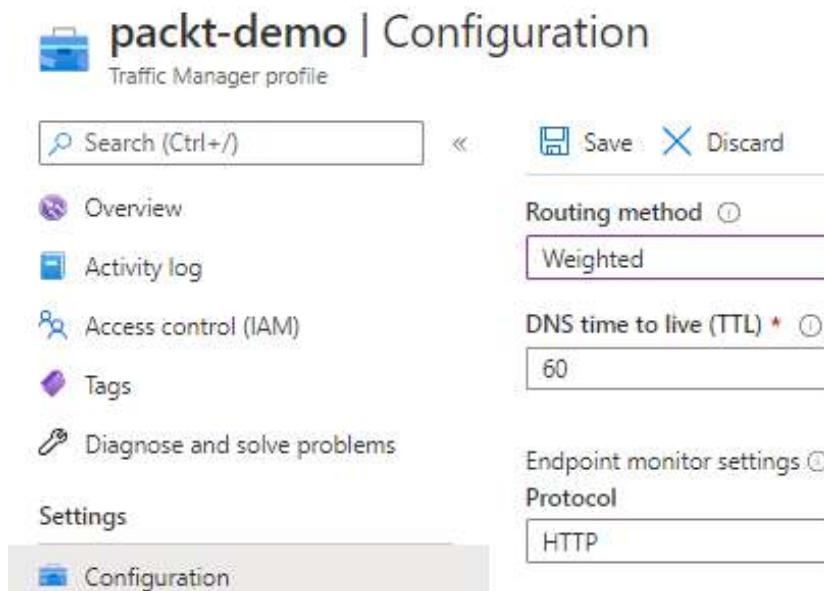


Figura 11.8: Alterar o método de roteamento para Ponderado

## Como funciona...

O método de roteamento ponderado distribuirá o tráfego uniformemente em todos os pontos de extremidade no back-end. Podemos configurar mais definições de peso para oferecer uma vantagem a um determinado ponto de extremidade e definir que alguns pontos de extremidade receberão uma porcentagem maior ou menor do tráfego. Esse método geralmente é usado quando temos várias instâncias de uma aplicação na mesma região ou para escalar horizontalmente para aumentar a performance.

Nesta receita, aprendemos a distribuir o tráfego uniformemente em todos os pontos de extremidade. Na próxima receita, aprenderemos a configurar o tráfego com base na prioridade.

## Configurar o tráfego com base na prioridade

Outro método de roteamento disponível é prioridade. Prioridade, como o nome sugere, dá prioridade a alguns pontos de extremidade, enquanto alguns pontos de extremidade são mantidos como backups. Os pontos de extremidade de backup serão usados somente se os pontos de extremidade com prioridade não estiverem disponíveis. Nesta receita, configuraremos o Gerenciador de Tráfego para rotear o tráfego com base na prioridade.

## Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para definir o método de roteamento como **Prioridade**, devemos fazer o seguinte:

1. No portal do Azure, localize o **perfil do Gerenciador de Tráfego** criado anteriormente.
2. Em **Configurações**, selecione a opção **Configuração**.
3. Altere o **Método de roteamento** para **Prioridade**, conforme mostrado na Figura 11.9:

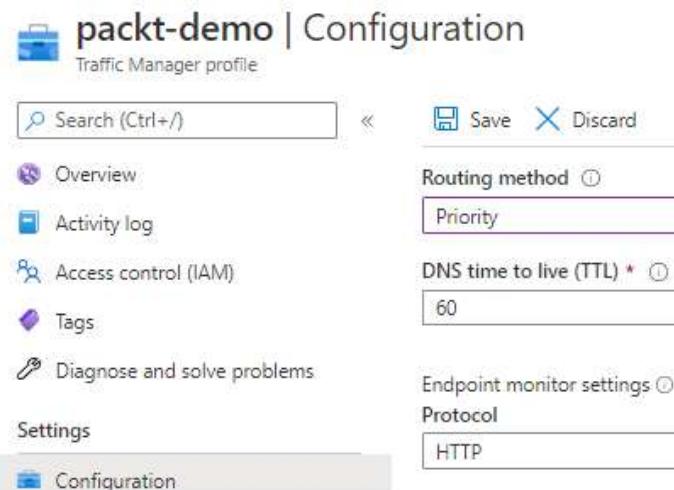


Figura 11.9: Alterar o método de roteamento para Prioridade

## Como funciona...

**Prioridade** define uma ordem de prioridade para pontos de extremidade. Todo o tráfego irá primeiro para os pontos de extremidade com a prioridade mais alta. Outros pontos de extremidade (com prioridade mais baixa) são copiados, e o tráfego será roteado para esses pontos de extremidade somente quando pontos de extremidade de prioridade mais alta ficarem indisponíveis. A ordem de prioridade padrão é a ordem de adição de pontos de extremidade ao Gerenciador de Tráfego, onde o ponto de extremidade adicionado primeiro se torna aquele com a prioridade mais alta, e o ponto de extremidade adicionado por último se torna o ponto de extremidade com a prioridade mais baixa. Prioridade pode ser alterada nas configurações de ponto de extremidade.

Na próxima receita, aprenderemos a configurar o tráfego com base na localização geográfica.

## Configurar o tráfego com base na localização geográfica

A localização geográfica é outro método de roteamento no Gerenciador de Tráfego. Esse método é baseado na latência da rede e direciona uma solicitação com base na localização geográfica da origem e do ponto de extremidade. Quando uma solicitação chega ao Gerenciador de Tráfego, com base na origem da solicitação, ela é roteada para o ponto de extremidade mais próximo em termos de região. Dessa forma, ele fornece a menor latência de rede possível. Nesta receita, configuraremos o Gerenciador de Tráfego para rotear o tráfego com base na localização geográfica.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para definir o método de roteamento com base na localização geográfica, devemos fazer o seguinte:

1. No portal do Azure, localize o perfil do Gerenciador de Tráfego criado anteriormente.
2. Em **Configurações**, selecione a opção **Configuração**.
3. Altere o método de roteamento para **Geográfico**, conforme mostrado na Figura 11.10:

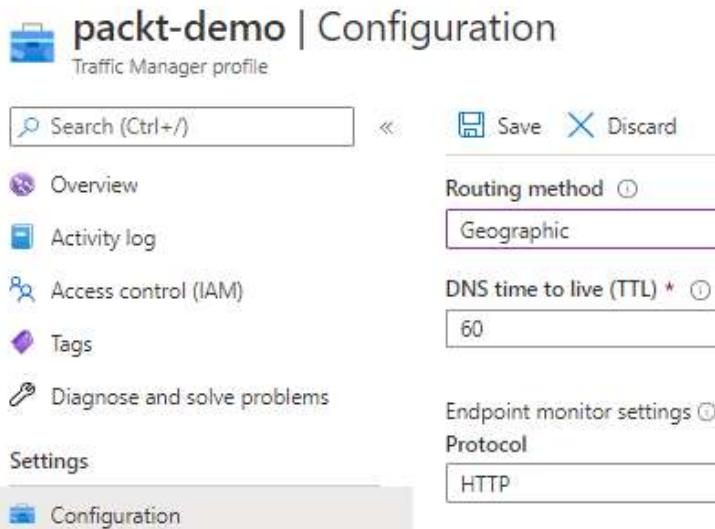


Figura 11.10: Alterar o método de roteamento para Geográfico

## Como funciona...

O método de roteamento geográfico corresponde à origem da solicitação com o ponto de extremidade mais próximo em termos de localização geográfica.

Por exemplo, vamos supor que temos vários pontos de extremidade, cada um em um continente diferente. Se uma solicitação vier da Europa, não faria sentido encaminhá-la para a Ásia ou para a América do Norte. O método de encaminhamento geográfico se certificará de que a solicitação proveniente da Europa seja direcionada para o ponto de extremidade localizado na Europa.

Vamos avançar para a próxima receita e aprender a gerenciar pontos de extremidade.

## Gerenciar pontos de extremidade

Depois de adicionarmos pontos de extremidade ao Gerenciador de Tráfego, talvez tenhamos que fazer alterações ao longo do tempo. Isso pode ser para fazer ajustes ou para remover completamente os pontos de extremidade. Nesta receita, vamos editar os pontos de extremidade existentes do Gerenciador de Tráfego.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para fazer alterações nos pontos de extremidade no Gerenciador de Tráfego, devemos fazer o seguinte:

1. No portal do Azure, localize o Gerenciador de Tráfego criado anteriormente.
2. Em **Configurações**, selecione **Pontos de extremidade**. Na lista exibida, selecione o ponto de extremidade que você deseja alterar:

The screenshot shows the Azure Traffic Manager Endpoints page for a profile named 'packt-demo'. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, and Diagnosis and solve problems. The 'Endpoints' link under Settings is highlighted. The main area shows a table of endpoints with columns: Name, Status, Monitor status, Type, and Location. Two entries are listed: 'packt1' (Enabled, Online, Azure endpoint, West Europe) and 'packt2' (Enabled, Online, Azure endpoint, West US). There are 'Add' and 'Refresh' buttons at the top of the table.

Name	Status	Monitor status	Type	Location
packt1	Enabled	Online	Azure endpoint	West Europe
packt2	Enabled	Online	Azure endpoint	West US

Figura 11.11: Alterar pontos de extremidade no Gerenciador de Tráfego

- No novo painel, podemos excluir, desabilitar ou fazer ajustes no ponto de extremidade:

The screenshot shows the Azure Traffic Manager endpoint configuration for a profile named 'packt1'. At the top, there are buttons for Save, Discard, and Delete. Below that, the 'Status' section has 'Enabled' selected. The 'Monitor status' is set to 'Online'. The 'Type' is 'Azure endpoint'. Under 'Target resource type', 'App Service' is chosen. A target resource named 'packt-demo-webapp-01' is listed. There is also a section for 'Custom Header settings'.

Figura 11.12: Painel para fazer ajustes no ponto de extremidade

## Como funciona...

O ponto de extremidade existente no back-end do Gerenciador de Tráfego pode ser alterado. Podemos excluir o ponto de extremidade para removê-lo completamente do Gerenciador de Tráfego ou podemos desabilitá-lo para removê-lo temporariamente do back-end. Também podemos alterar completamente o ponto de extremidade, para direcionar para outro serviço ou um tipo completamente diferente.

Nesta receita, aprenderemos a gerenciar pontos de extremidade. Na próxima receita, aprenderemos a gerenciar e ajustar perfis.

## Gerenciar perfis

O perfil do Gerenciador de Tráfego é outra configuração que podemos gerenciar e ajustar. Embora tenha opções muito limitadas, onde só podemos desabilitar e habilitar o Gerenciador de Tráfego, gerenciar a configuração do perfil pode ser muito útil para fins de manutenção. Nesta receita, gerenciaremos nosso perfil do Gerenciador de Tráfego.

## Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para fazer alterações no perfil do Gerenciador de Tráfego, devemos fazer o seguinte:

1. No portal do Azure, localize o perfil do Gerenciador de Tráfego criado anteriormente.
2. Em **Visão geral**, selecione a opção **Desabilitar perfil** e confirme clicando no botão **Sim**:

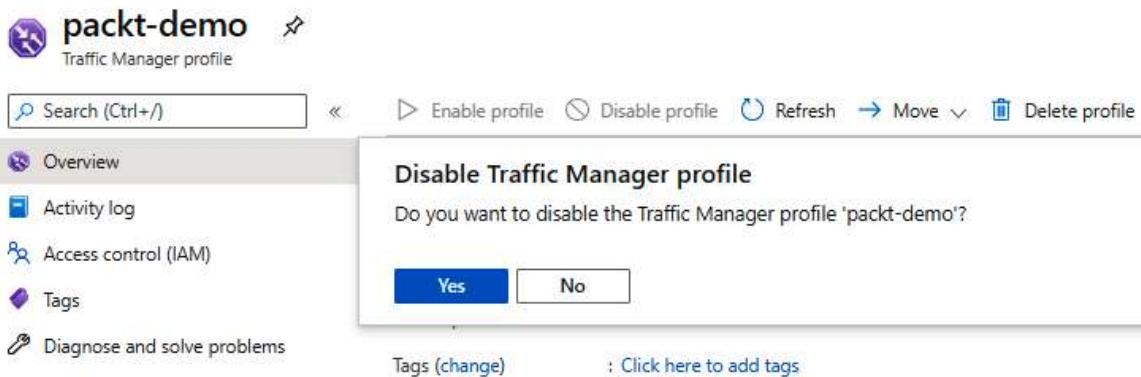


Figura 11.13: Desabilitar um perfil

3. Depois que o perfil for desabilitado, ele poderá ser habilitado novamente com a opção **Habilitar perfil**:

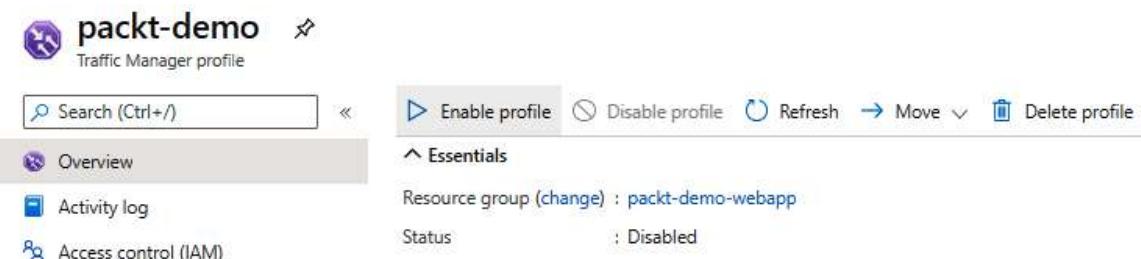


Figura 11.14: Habilitar um perfil

## Como funciona...

Gerenciar o perfil do Gerenciador de Tráfego com as opções de desabilitar e habilitar deixará o front-end do Gerenciador de Tráfego disponível ou indisponível (com base na opção selecionada). Isso pode ser muito útil para fins de manutenção. Se for necessário aplicar alterações em todos os pontos de extremidade, e as alterações precisarem ser aplicadas a todos os pontos de extremidade ao mesmo tempo, poderemos desabilitar o perfil do Gerenciador de Tráfego temporariamente. Depois que as alterações forem aplicadas a todos os pontos de extremidade, poderemos tornar o Gerenciador de Tráfego disponível novamente ao habilitar o perfil.

Vamos avançar para a próxima receita e aprender a configurar o Gerenciador de Tráfego com平衡adores de carga.

## Configurar o Gerenciador de Tráfego com平衡adores de carga

A combinação do Gerenciador de Tráfego com平衡adores de carga geralmente é feita para fornecer a máxima disponibilidade. Os平衡adores de carga são limitados a fornecer alta disponibilidade a um conjunto de recursos localizados na mesma região. Isso oferece uma vantagem se um único recurso falhar, pois temos várias instâncias de um recurso. Mas e se toda uma região falhar? Os平衡adores de carga não podem lidar com recursos em várias regiões, mas podemos combinar平衡adores de carga com o Gerenciador de Tráfego para fornecer disponibilidade ainda melhor com recursos em regiões do Azure. Nesta receita, configuraremos o Gerenciador de Tráfego para funcionar com平衡adores de carga.

### Preparação

Antes de iniciar, abra seu navegador e accese o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para configurar o Gerenciador de Tráfego com um平衡ador de carga, devemos fazer o seguinte:

1. No portal do Azure, localize o平衡ador de carga e verifique se ele tem o endereço IP atribuído conforme abordado no Capítulo 8, Balanceadores de carga. Somente os endereços IP públicos podem ser usados:

The screenshot shows the Azure portal interface for managing a load balancer. The top navigation bar includes 'Load balancer' and 'Frontend IP configuration'. The main area has a search bar, an 'Add' button, and a 'Refresh' button. On the left, there's a sidebar with links for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The 'Frontend IP configuration' link is highlighted. The main content area displays a table with one row of data:

Name	IP address
LoadBalancerFrontEnd	52.142.216.49 (Packt-LoadBalancer-PublicIP)

Figura 11.15: Verificar o endereço IP atribuído de um平衡ador de carga

2. Acesse o Gerenciador de Tráfego e selecione **Adicionar** para adicionar um novo ponto de extremidade. Selecione **Ponto de extremidade do Azure** para **Tipo**, forneça um nome para o ponto de extremidade e selecione **Endereço IP público** como o tipo de recurso de destino. Com base no tipo selecionado, uma nova opção será exibida, permitindo selecionar os recursos que correspondem ao tipo selecionado. No nosso caso, a opção de selecionar **Endereço IP público** está disponível:

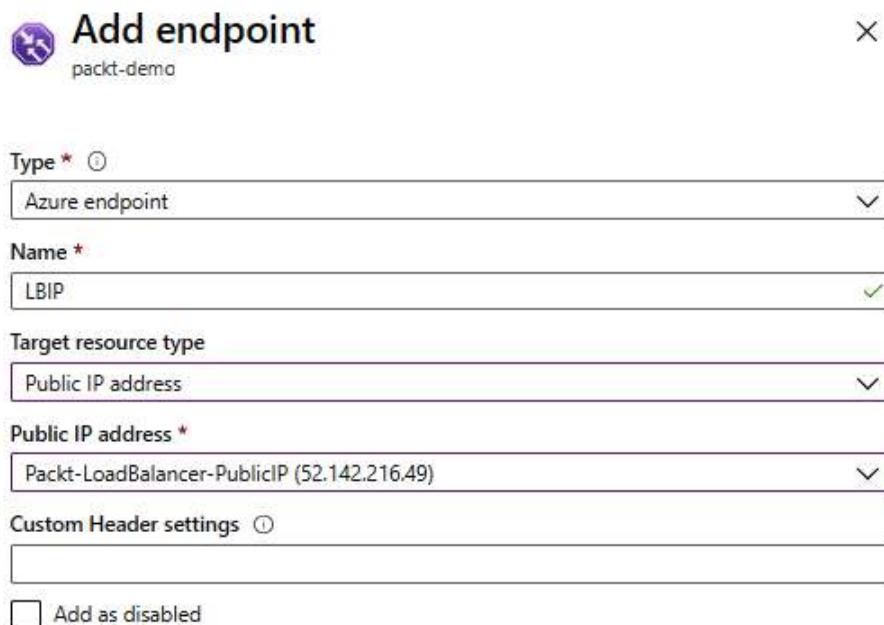


Figura 11.16: Configurar um novo ponto de extremidade no Gerenciador de Tráfego

3. Repita o processo e adicione outro balanceador de carga (de outra região) como o segundo ponto de extremidade do Gerenciador de Tráfego.

## Como funciona...

Os平衡adores de carga fornecem melhor disponibilidade, mantendo um serviço ativo mesmo se um dos serviços no pool do back-end falhar. Se uma região falhar, os平衡adores de carga não poderão fornecer ajuda porque são limitados a uma única região. Devemos fornecer outro conjunto de recursos em outra região para realmente aumentar a disponibilidade, mas esses conjuntos serão completamente independentes e não fornecerão failover, a não ser se incluirmos o Gerenciador de Tráfego.

O Gerenciador de Tráfego se tornará o front-end e adicionaremos平衡adores de carga como os pontos de extremidade do back-end do Gerenciador de Tráfego. Todas as solicitações chegarão ao Gerenciador de Tráfego primeiro e, em seguida, serão roteadas para o平衡ador de carga apropriado no back-end. O Gerenciador de Tráfego monitorará a integridade dos平衡adores de carga, e, se um deles não estiver disponível, o tráfego será redirecionado para um平衡ador de carga ativo.

# 12

## Gateway de aplicativo do Azure e WAF do Azure

**Basicamente, o Gateway de Aplicativo do Azure** é um balanceador de carga para tráfego da Web, mas também fornece melhor controle de tráfego. Os平衡adores de carga tradicionais operam na camada de transporte e permitem rotear o tráfego com base no protocolo (TCP ou UDP) e endereço IP, mapeando endereços IP e protocolos no front-end para endereços IP e protocolos no back-end. Esse modo de operação "clássico" é muitas vezes chamado de camada 4. O gateway de aplicativo expande isso e permite usar nomes de host e caminhos para determinar para onde o tráfego deve ir, tornando-o um balanceador de carga de camada 7. Por exemplo, podemos ter vários servidores que são otimizados para coisas diferentes. Se um dos nossos servidores for otimizado para vídeos, todas as solicitações de vídeo deverão ser roteadas para esse servidor específico com base na solicitação de URL de entrada.

Abordaremos as seguintes receitas neste capítulo:

- Criar um novo gateway de aplicativo
- Configurar os pools de back-end
- Configurar configurações de HTTP
- Configurar os ouvintes
- Regras de configuração
- Configurar investigações
- Configurar um **Firewall de Aplicativo Web (WAF)**
- Personalizar regras de WAF
- Criar uma política de WAF

## Requisitos técnicos

Para este capítulo, é necessária uma assinatura do Azure.

## Criar um novo gateway de aplicativo

O Gateway de Aplicativo do Azure pode ser usado como um balanceador de carga simples para executar a distribuição de tráfego do front-end para o back-end com base em protocolos e portas. Mas também pode expandir isso e executar roteamento adicional com base em nomes de host e caminhos. Isso permite ter pools de recursos com base em regras e também otimizar a performance. Usar essas opções e executar o roteamento com base no contexto aumentará a performance da aplicação, juntamente com o fornecimento de alta disponibilidade. Obviamente, nesse caso, precisamos ter vários recursos para cada tipo de performance em cada pool de back-end (cada tipo de performance solicita um pool de back-end separado).

## Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar um novo gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Gateway de aplicativo** em **Rede** (ou pesquise **gateway de aplicativo** na barra de pesquisa).
2. No novo painel, devemos fornecer informações para **Assinatura**, **Grupo de recursos**, **Nome**, **Região**, **Camada**, **Dimensionamento automático**, **Contagem de instâncias**, **Zona de disponibilidade** e **HTTP2**. Também devemos selecionar a **Rede virtual** e a **Sub-rede** que será associada ao nosso gateway de aplicativo. Você será limitado a redes virtuais localizadas na região selecionada para o gateway de aplicativo:

### Create application gateway

The screenshot shows the 'Create application gateway' wizard in the Azure portal. The 'Basics' tab is selected. The 'Project details' section includes a subscription dropdown set to 'Microsoft Azure Sponsorship' and a resource group dropdown set to 'packt-demo'. The 'Instance details' section includes an application gateway name 'packt-appgateway', region 'West Europe', tier 'Standard V2', and enable autoscaling (Yes). The 'Configure virtual network' section includes a virtual network 'packtdemoVM-Vnet' and a subnet 'AppGateway (192.168.2.0/24)'. Other fields like minimum and maximum scale units, availability zone, and HTTP2 settings are also visible.

Figura 12.1: Configurar detalhes do projeto para o gateway de aplicativo

3. Agora, preenchemos a guia **Front-ends**. Aqui, precisamos selecionar o tipo de endereço IP que o front-end usará (**Público**, **Privado** ou **Ambos**) e fornecer um IP (selecione um existente ou crie um novo):

## Create application gateway

The screenshot shows the 'Frontends' step of the 'Create application gateway' wizard. At the top, there are tabs: Basics (with a checkmark), Frontends (which is selected and highlighted in blue), Backends, Configuration, Tags, and Review + create. Below the tabs, a note says: 'Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.' Under 'Frontend IP address type', there are three radio buttons: 'Public' (selected), 'Private', and 'Both'. A dropdown menu labeled '(New) AppGateway-IP' is open, showing the option 'Add new'. There is also a small downward arrow icon next to the dropdown.

Figura 12.2: Selecionar o tipo de endereço IP de front-end

4. Em seguida, temos a guia **Back-ends**. Precisamos selecionar **Adicionar um novo pool de back-end**:

## Create application gateway

The screenshot shows the 'Backends' step of the 'Create application gateway' wizard. At the top, there are tabs: Basics, Frontends, Backends (selected and highlighted in blue), Configuration, Tags, and Review + create. Below the tabs, a note says: 'A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN).'. A button 'Add a backend pool' is visible. Below it, there is a table with two columns: 'Backend pool' and 'Targets'. The table has a single row with the text 'No results'.

Figura 12.3: Definir back-ends para o gateway de aplicativo

5. Neste momento, um novo painel será aberto. Precisamos fornecer informações para **Nome** e escolher se queremos adicionar um pool de back-end com ou sem destinos. Se escolhermos adicionar destinos nesta fase, primeiro, precisamos selecionar o **Tipo de destino**. Os tipos disponíveis são máquinas virtuais, conjuntos de escalas de máquinas virtuais, serviços de aplicativo e endereços IP/FQDNs. Com base no tipo escolhido, você pode adicionar destinos apropriados:

## Add a backend pool.

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name *	BackendPool	
Add backend pool without targets	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Backend targets	2 items	
Target type	Target	
Virtual machine	packtdemoVM-01	...
Virtual machine	packtdemoVM-02 (192.168.1.5)	...
IP address or FQDN		

Figura 12.4: Adicionar um pool de back-end

6. Depois de adicionar um pool de back-end, podemos ver informações relacionadas e continuar. Observe que podemos adicionar mais de um pool de back-end:

## Create application gateway

The screenshot shows the 'Create application gateway' wizard at the 'Backends' step (step 3). The top navigation bar includes 'Basics', 'Frontends', 'Backends' (which is underlined), 'Configuration', 'Tags', and 'Review + create'. Below the navigation, a note states: 'A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN)'. The main area shows a table titled 'Add a backend pool' with two columns: 'Backend pool' and 'Targets'. One row is visible, showing 'BackendPool' as the name, '2 targets' as the count, and two entries: 'packtdemoVM-01' and 'packtdemoVM-02', each with a three-dot menu icon.

Backend pool	Targets
BackendPool	▼ 2 targets
	packtdemoVM-01
	packtdemoVM-02

Figura 12.5: Revisar a configuração para o pool de back-end

7. No painel **Configuração**, podemos ver que os pools de front-end e back-end estão implementados, mas está faltando uma regra de roteamento. Ela é obrigatória para continuar. Por isso, devemos criar uma selecionando **Adicionar uma regra de roteamento**:

## Create application gateway

The screenshot shows the 'Create application gateway' wizard at the 'Configuration' step (step 4). The top navigation bar includes 'Basics', 'Frontends', 'Backends', 'Configuration' (which is underlined), 'Tags', and 'Review + create'. Below the navigation, a note says: 'Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.' The main area has three sections: 'Frontends' (with a 'Public: (new) AppGateway-IP' entry and a plus icon), 'Routing rules' (with a large plus icon labeled 'Add a routing rule'), and 'Backend pools' (with a plus icon labeled '+ Add a backend pool').

Figura 12.6: Criar uma regra de roteamento

8. No novo painel, primeiro devemos definir um ouvinte. Para o ouvinte, devemos fornecer um nome, selecionar a configuração do **IP de front-end** e fornecer uma **Porta** e um **Protocolo** que serão monitorados. Também podemos alterar o botão de opção **Tipo de ouvinte** e adicionar uma página de URL de redirecionamento para erros (pode ser somente uma URL da conta de armazenamento do Azure):

**Add a routing rule** X

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

**Rule name \***  ✓

**\* Listener** **\* Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

**Listener name \***  ✓

**Frontend IP \***  ▼

**Protocol**  HTTP  HTTPS

**Port \***  ✓

**Additional settings**

**Listener type**  Basic  Multi site

**Error page url**  Yes  No

**Figura 12.7: Definir as configurações do ouvinte para a regra de roteamento**

9. Para a regra de roteamento, precisamos configurar os **Destinos de back-end** também. Nesta seção, precisamos definir o **Tipo de destino**, o **Destino de back-end** e as **Configurações de HTTP**. Nesta fase, ainda falta uma configuração de HTTP. Por isso, precisamos selecionar **Adicionar novo** no campo **Configurações de HTTP**:

**Add a routing rule**

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name \*  ✓

\* Listener  Backend targets \*

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type  Backend pool  Redirection

Backend target \*  BackendPool ✓  
 Add new

HTTP settings \*  Add new  
✖ The value must not be empty.

#### Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

#### Path based rules

Path	Target name	HTTP setting name	Backend pool
No additional targets to display			

[Add multiple targets to create a path-based rule](#)

Figura 12.8: Configurar destinos de back-end para a regra de roteamento

10. No novo painel, primeiro precisamos fornecer nossa configuração de HTTP com um nome e adicionar detalhes para o **Protocolo de back-end** e a **Porta de back-end**. Também devemos habilitar ou desabilitar **Afinidade baseada em cookies** e **Descarga de conexão** antes de especificar o **Limite de tempo de solicitação (segundos)**. Podemos habilitar ou desabilitar as configurações **Criar investigações personalizadas** e **Substituir com novo nome do host**:

## Add a HTTP setting

[← Discard changes and go back to routing rules](#)

HTTP settings name *	<input type="text" value="HTTP"/>
Backend protocol	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
Backend port *	<input type="text" value="80"/>
<b>Additional settings</b>	
Cookie-based affinity	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection draining	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Request time-out (seconds) *	<input type="text" value="20"/>
Override backend path	<input type="text"/>
<b>Host name</b>	
By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.	
Override with new host name	<input type="radio"/> Yes <input checked="" type="radio"/> No
Host name override	<input type="radio"/> Pick host name from backend target <input checked="" type="radio"/> Override with specific domain name
<input type="text" value="e.g. contoso.com"/>	
Create custom probes	<input type="radio"/> Yes <input type="radio"/> No

Figura 12.9: Adicionar um configuração de HTTP

11. Depois que a configuração de HTTP for criada, ela será adicionada automaticamente à nossa regra de roteamento, que agora podemos concluir:

### Add a routing rule

X

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name *	HTTP	<input checked="" type="checkbox"/>		
*Listener	<u>Backend targets</u>			
Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.				
Target type	<input checked="" type="radio"/> Backend pool	<input type="radio"/> Redirection		
Backend target *	BackendPool			
	<a href="#">Add new</a>			
HTTP settings *	HTTP			
	<a href="#">Add new</a>			
<b>Path-based routing</b>				
You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.				
<table border="1"> <thead> <tr> <th>Path based rules</th> </tr> </thead> <tbody> <tr> <td>No additional targets to display</td> </tr> </tbody> </table>			Path based rules	No additional targets to display
Path based rules				
No additional targets to display				
<a href="#">Add multiple targets to create a path-based rule</a>				

Figura 12.10: Configuração final para adicionar uma regra de roteamento

12. A configuração agora está concluída, e podemos avançar e implantar nosso gateway de aplicativo:

### Create application gateway

✓ Basics ✓ Frontends ✓ Backends Configuration Tags Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

<b>Frontends</b> + Add a frontend IP	<b>Routing rules</b> + Add a routing rule	<b>Backend pools</b> + Add a backend pool
Public: (new) AppGateway-IP	HTTP	BackendPool

Figura 12.11: Implantar nosso gateway de aplicativo

## Como funciona...

O Gateway de Aplicativo do Azure é muito semelhante ao Azure Load Balancer, com algumas opções adicionais. Ele roteará o tráfego chegando ao front-end do gateway de aplicativo para um back-end definido, com base nas regras que definimos. Além do roteamento com base nos protocolos e nas portas, o gateway de aplicativo também permite o roteamento definido com base nos caminhos e protocolos. Usando essas regras adicionais, podemos rotear solicitações de entrada para pontos de extremidade que são otimizados para determinadas funções. Por exemplo, podemos ter vários pools de back-end com configurações diferentes que são otimizadas para executar apenas tarefas específicas. Com base na natureza das solicitações de entrada, o gateway de aplicativo roteará as solicitações para o pool de back-end apropriado. Essa abordagem, juntamente com a alta disponibilidade, fornecerá melhor performance roteando cada solicitação para um pool de back-end que processará a solicitação de forma mais otimizada.

Podemos configurar o dimensionamento automático para gateway de aplicativo (disponível somente para V2) com informações adicionais para o número mínimo e máximo de unidades. Dessa forma, o gateway de aplicativo será escalado com base na demanda e garantirá que a performance não seja afetada, mesmo com o número máximo de solicitações.

## Configurar os pools de back-end

Depois que o gateway de aplicativo for criado, deveremos definir os pools de back-end. O tráfego que chega ao front-end do gateway de aplicativo será encaminhado para os pools de back-end. Pools de back-end em gateways de aplicativo são os mesmos que pools de back-end em平衡adores de carga e são definidos como possíveis destinos para onde o tráfego será roteado com base em outras configurações que serão adicionadas em receitas futuras deste capítulo.

## Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para adicionar pools de back-end ao nosso gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, localize o gateway de aplicativo criado anteriormente.
2. No painel **Gateway de aplicativo**, em **Configurações**, selecione **Pools de back-end**. Selecione **Adicionar** para adicionar um novo pool de back-end ou selecione um existente para editar:

The screenshot shows the 'Backend pools' section of the Azure Application Gateway configuration. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Web application firewall, and Backend pools (which is highlighted). The main area has a search bar at the top. Below it, there are two buttons: 'Add' and 'Refresh'. A table lists existing backend pools. The table has columns for Name, Rules associated, and Targets. One row is shown: 'BackendPool' with 1 rule and 2 targets.

Name	Rules associated	Targets
BackendPool	1	2

Figura 12.12: Adicionar um pool de back-end ao nosso gateway de aplicativo

3. No novo painel, a única diferença entre pools novos e existentes é o nome. Para um novo pool, devemos fornecer o nome do pool de back-end e, para pools existentes, essa opção está acinzentada e não pode ser editada. Para pools novos e existentes, devemos fornecer o tipo de destino. Os tipos disponíveis são máquinas virtuais, conjuntos de escalas de máquinas virtuais, serviços de aplicativo e endereços IP/FQDNs. Com base no tipo escolhido, você pode adicionar destinos apropriados:

## Edit backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, domain names, or an App Service.

Name  
BackendPool

Add backend pool without targets

Backend targets  
2 items

Target type	Target	⋮
Virtual machine	packtdemoVM-01	
Virtual machine	packtdemoVM-02	
IP address or FQDN	<input type="text"/>	⋮

Associated rule

[HTTP](#)

Figura 12.13: Fornecer o tipo de destino para o pool de back-end

## Como funciona...

Com pools de back-end, definimos os destinos para os quais o tráfego será encaminhado. Como o gateway de aplicativo permite definir o roteamento para cada solicitação, é melhor ter destinos com base na performance e tipos agrupados da mesma maneira. Por exemplo, se tivermos vários servidores Web, eles devem ser colocados no mesmo pool de back-end. Os servidores usados para processamento de dados devem ser colocados em um pool separado e os servidores usados para vídeo em outro pool separado. Dessa forma, podemos separar pools com base em tipos de performance e rotear o tráfego com base em operações que precisam ser concluídas.

Isso aumentará a performance da nossa aplicação, pois cada solicitação será processada pelo recurso mais adequado para uma tarefa específica. Para obter alta disponibilidade, devemos adicionar mais servidores a cada pool de back-end.

## Configurar configurações de HTTP

As configurações de HTTP em gateways de aplicativo são usadas para validação e várias configurações de tráfego. O principal objetivo é garantir que as solicitações sejam direcionadas para o pool de back-end apropriado. Algumas outras configurações de HTTP também são incluídas, como afinidade ou descarga de conexão. As configurações de substituição também fazem parte das configurações de HTTP. Elas permitirão o redirecionamento se uma solicitação incorreta for enviada.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para adicionar configurações de HTTP ao nosso gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, localize o gateway de aplicativo criado anteriormente.
2. No novo do **Gateway de aplicativo**, em **Configurações**, selecione **Configurações de HTTP**. Selecione **Adicionar** para adicionar uma nova configuração de HTTP ou selecione uma existente para editar:

The screenshot shows the Azure portal interface for managing an Application gateway named 'packt-appgateway'. The left sidebar has a 'Settings' section with 'HTTP settings' highlighted. The main content area is titled 'packt-appgateway | HTTP settings' and shows a table of existing HTTP settings. One row is visible with the following details:

Name	Port	Protocol	Cookie based affinity
HTTP	80	HTTP	Disabled

Figura 12.14: Localizar configurações de HTTP no painel Gateway de aplicativo

3. No novo painel, primeiro precisamos fornecer um nome (se você estiver editando uma configuração de HTTP existente, essa opção estará acinzentada). As próximas opções permitem desabilitar ou habilitar **Afinidade baseada em cookies** e **Descarga de conexão**. Além disso, selecionamos nosso **Protocolo**, **Porta** e o período de **Tempo limite da solicitação (segundos)**. As configurações opcionais permitem configurar **Usar investigação personalizada** e **Substituir com o novo nome do host**:

### Add HTTP setting

HTTP settings name  
HTTP

Backend protocol  
 HTTP  HTTPS

Backend port \*  
80

Additional settings

Cookie-based affinity ⓘ  
 Enable  Disable

Connection draining ⓘ  
 Enable  Disable

Request time-out (seconds) \* ⓘ  
20

Override backend path ⓘ

Host name  
By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name  
 Yes  No

Host name override  
 Pick host name from backend target  
 Override with specific domain name  
e.g. contoso.com

Use custom probe ⓘ  
 Yes  No

Figura 12.15: Definir configurações de HTTP

## Como funciona...

Como mencionado anteriormente, o objetivo principal das configurações de HTTP é garantir que as solicitações sejam direcionadas para o pool de back-end correto. No entanto, várias outras opções estão disponíveis. A afinidade baseada em cookies permite rotear solicitações da mesma fonte para o mesmo servidor de destino no pool de back-end. A descarga de conexão controlará o comportamento quando o servidor for removido do pool de back-end. Se estiver habilitado, o servidor ajudará a manter as solicitações em trânsito no mesmo servidor. As configurações de substituição nos permitem substituir o caminho da URL por um caminho diferente ou um domínio completamente novo, antes de encaminhar a solicitação para o pool de back-end.

## Configurar os ouvintes

**Os ouvintes** em um gateway de aplicativo escutam quaisquer solicitações de entrada. Depois que uma nova solicitação for detectada, ela será encaminhada para o pool de back-end com base nas regras e configurações que definimos. Nesta receita, adicionaremos um novo ouvinte ao nosso gateway de aplicativo.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para adicionar um ouvinte a um gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, localize o gateway de aplicativo criado anteriormente.
2. No novo painel **Gateway de aplicativo**, em **Configurações**, selecione **Ouvintes** e selecione **Adicionar ouvinte** para adicionar um novo ouvinte ou editar um existente:

Name	Protocol	Port	Associated rule
HTTP	HTTP	80	HTTP

Figura 12.16: Adicionar um novo ouvinte por meio do portal do Azure

3. No novo painel, precisamos fornecer um nome para o ouvinte (se você estiver editando um ouvinte existente, essa opção estará acinzentada), selecione a configuração de **IP do front-end** e forneça a **Porta** e o **Protocolo** que serão monitorados. Além disso, podemos configurar o **Tipo de ouvinte** e uma página de URL personalizada para erros:

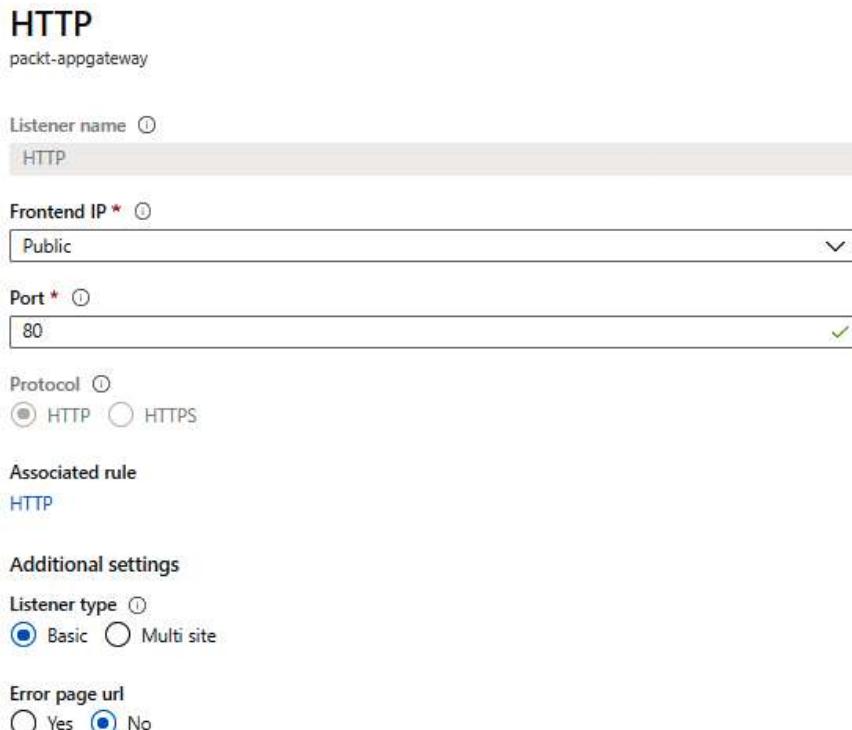


Figura 12.17: Configurar as configurações do ouvinte para o nosso gateway de aplicativo

## Como funciona...

Um ouvinte monitora novas solicitações que chegam ao gateway de aplicativo. Cada ouvinte monitora apenas um endereço IP de front-end e apenas uma porta. Se tivermos dois IPs de front-end (um público e outro privado) e tráfego chegando em vários protocolos e portas, devemos criar um ouvinte para cada endereço IP e cada porta à qual o tráfego pode estar chegando.

O tipo básico de ouvinte é usado quando o ouvinte escuta um único domínio; geralmente é usado quando hospedamos uma única aplicação por trás de um gateway de aplicativo. Um ouvinte de vários sites é usado quando temos mais de uma aplicação por trás do gateway de aplicativo e precisamos configurar o roteamento com base em um nome de host ou nome de domínio.

## Regras de configuração

As regras em gateways de aplicativo são usadas para determinar como o tráfego flui. Diferentes configurações determinam para onde uma solicitação específica é encaminhada e como isso é feito.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para adicionar uma regra ao gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, localize o gateway de aplicativo criado anteriormente.
2. No painel **Gateway de aplicativo**, em **Configurações**, selecione **Regras**.  
Adicione uma nova regra ou selecione uma existente para editar:

The screenshot shows the 'packt-appgateway' Application gateway configuration in the Azure portal. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnosis and solve problems, Configuration, Web application firewall, Backend pools, HTTP settings, Frontend IP configurations, Listeners, and Rules. The 'Rules' option is highlighted. The main pane displays the 'Request routing rule' section with a search bar and a table titled 'Search rules'. One rule is listed:

Name	Type	Listener
HTTP	Basic	HTTP

Figura 12.18: Adicionar uma regra de roteamento para nosso gateway de aplicativo

3. No novo painel, devemos fornecer um nome para a nova regra (se você estiver editando uma regra existente, essa opção estará acinzentada) e selecionar o **Ouvinte**, conforme mostrado na Figura 12.19:

The screenshot shows the 'HTTP' configuration interface. At the top, it says 'HTTP' and 'packt-appgateway'. Below that is a descriptive text: 'Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.' Underneath, there's a 'Rule name' field containing 'HTTP'. The 'Listener' tab is selected, indicated by a blue underline. Below it is a section for 'Backend targets'. A note states: 'A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.' A dropdown menu labeled 'Listener \*' shows 'HTTP'.

Figura 12.19: Configurar a regra de roteamento

4. Também precisamos configurar um destino de back-end, onde precisamos definir o **Tipo de destino** e selecionar opções para **Tipo de back-end** e **Configurações de HTTP**:

The screenshot shows the 'HTTP' configuration interface again. The 'Backend targets' tab is selected, indicated by a blue underline. Below it is a section for 'Target type'. It shows two options: 'Backend pool' (selected) and 'Redirection'. Under 'Backend target \*', there is a dropdown menu showing 'BackendPool'. Under 'HTTP settings \*', there is another dropdown menu showing 'HTTP'.

Figura 12.20: Configurar um destino de back-end para nossa regra de roteamento

## Como funciona...

Usando regras, podemos unir algumas configurações criadas anteriormente. Definimos um ouvinte que especifica qual solicitação em qual endereço IP estamos esperando em qual porta. Em seguida, essas solicitações são encaminhadas para o pool de back-end. O encaminhamento é feito com base nas configurações de HTTP. Opcionalmente, também podemos adicionar redirecionamento às regras.

## Configurar investigações

As investigações no gateway de aplicativo são usadas para monitorar a integridade dos destinos de back-end. Cada ponto de extremidade é monitorado e, se um for descoberto como não íntegro, será temporariamente retirado de rotação e solicitações não serão encaminhadas. Depois que o status for alterado, ele será adicionado de volta. Isso impede que as solicitações sejam enviadas para pontos de extremidade não íntegros que não puderam atender a solicitação.

### Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para adicionar uma investigação ao nosso gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, localize o gateway de aplicativo criado anteriormente.
2. No painel **Gateway de aplicativo**, em **Configurações**, selecione **Investigações de integridade**. Selecione **Adicionar** para adicionar a nova investigação:

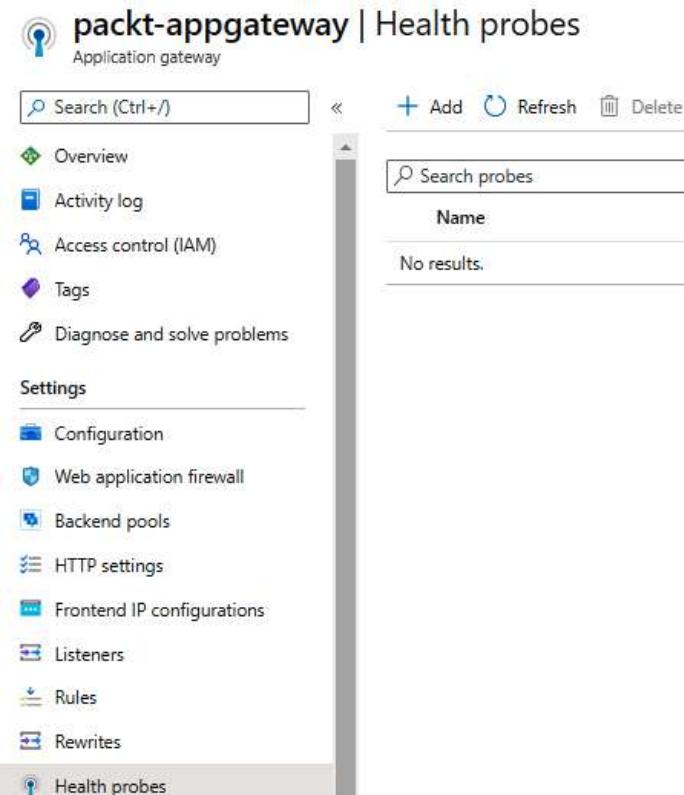


Figura 12.21: Adicionar uma nova investigação de integridade

3. No novo painel, devemos fornecer o **Nome** da investigação (essa opção estará acinzentada se uma investigação existente for editada), juntamente com o **Protocolo**, o **Host** e o **Caminho**. Também precisamos definir as configurações de **Intervalo**, **Tempo limite (segundos)** e **Limite não íntegro**: Também podemos optar por configurar **Usar condições de correspondência de investigação** e associar **Configurações de HTTP**:

**Add health probe**

packt-appgateway

Name *	probe1
Protocol *	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
Host *	toroman.cloud
Pick host name from backend HTTP settings	<input type="radio"/> Yes <input checked="" type="radio"/> No
Pick port from backend HTTP settings	<input checked="" type="radio"/> Yes <input type="radio"/> No
Path *	/video/*
Interval (seconds) *	30
Timeout (seconds) *	30
Unhealthy threshold *	3
Use probe matching conditions	<input type="radio"/> Yes <input checked="" type="radio"/> No
HTTP settings	0 selected

Figura 12.22: Configurar os detalhes da investigação de integridade

## Como funciona...

**Protocolo**, **Host** e **Caminho** definem qual investigação está sendo monitorada. **Intervalo** define a frequência com que as verificações são executadas. **Tempo limite** define quanto tempo deve passar antes que a verificação seja declarada como falha. Por fim, **Limite não íntegro** é usado para definir quantas verificações com falha devem ocorrer antes que o ponto de extremidade seja declarado como não disponível.

## Configurar um Firewall de Aplicativo Web (WAF)

O WAF é uma configuração adicional para o gateway de aplicativo. Ele é usado para aumentar a segurança de aplicações por trás do gateway de aplicativo e também fornece proteção centralizada.

## Preparação

Para habilitar um WAF, devemos definir o gateway de aplicativo para a camada de WAF. Para isso, devemos fazer o seguinte:

1. No painel **Gateway de aplicativo**, accese **Firewall de aplicativo Web**, em **Configurações**: Altere a seleção de **Camada de Padrão V2** para **WAF V2** e selecione **Salvar**:

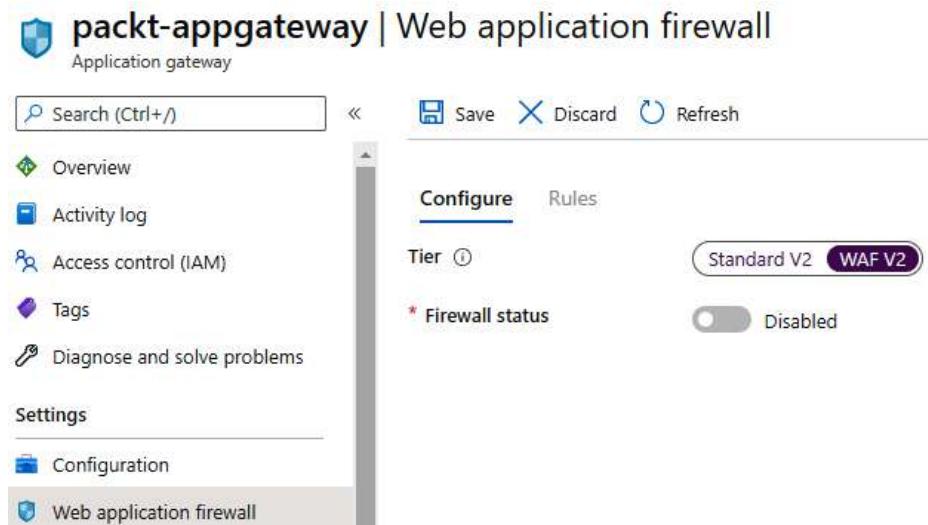


Figura 12.23: Habilitar o gateway de aplicativo para a camada de WAF V2

## Como fazer isso...

Depois que o gateway de aplicativo for definido como WAF, poderemos habilitar e definir as regras de firewall. Para isso, devemos fazer o seguinte:

1. No painel **Gateway de aplicativo**, acesse o **Firewall de aplicativo Web**, em **Configurações** e habilite **Status do firewall**. Depois de definir o **Status do firewall** como **Habilitado**, um novo conjunto de opções será exibido:

The screenshot shows the AWS Application Gateway configuration interface for the 'packt-appgateway' gateway. The left sidebar has a 'Web application firewall' section selected. The main area is titled 'Configure' and shows the following settings:

- Tier**: Standard V2 (selected)
- Firewall status**: Enabled
- Firewall mode**: Prevention
- Exclusions**: A note stating "packt-appgateway will evaluate everything in the request except for the items included in this list." followed by a table with three columns: Field, Operator, and Selector.
- Global parameters**:
  - Inspect request body: On
  - Max request body size (KB): [empty input field]
  - File upload limit (MB): [empty input field]

Figura 12.24: Habilitar um WAF para nosso gateway de aplicativo

2. Devemos selecionar um **Modo de firewall**, definir uma lista de exclusões e especificar os **Parâmetros globais** da seguinte maneira:

The screenshot shows the Azure Application Firewall configuration page. At the top, there's a section for 'Firewall status' with a switch set to 'Enabled'. Below it, 'Firewall mode' is set to 'Prevention'. A note says 'packt-appgateway will evaluate everything in the request except for the items included in this list.' Under 'Exclusions', there's a table with three columns: 'Field', 'Operator', and 'Selector'. The first row has 'Request header name' in 'Field', 'Equals' in 'Operator', and 'BearerToken' in 'Selector'. There are two empty rows below. Below this, under 'Global parameters', 'Inspect request body' is turned 'On'. It includes settings for 'Max request body size (KB)' (set to 8) and 'File upload limit (MB)' (set to 10), both with green checkmarks.

Figura 12.25: Configurar o WAF

## Como funciona...

O recurso WAF ajuda a aumentar a segurança ao verificar todo o tráfego de entrada. Como isso pode desacelerar a performance, podemos excluir alguns itens que estão criando falsos positivos, principalmente quando se trata de itens de tamanho significativo. Os itens excluídos não serão inspecionados. Um WAF pode funcionar em dois modos: detecção e prevenção. A detecção só detectará se uma solicitação maliciosa for enviada, enquanto a prevenção impedirá essa solicitação.

## Personalizar regras de WAF

Um WAF vem com um conjunto predeterminado de regras. Essas regras são impostas para aumentar a segurança da aplicação e impedir solicitações maliciosas. Podemos alterar essas regras para resolver problemas ou requisitos específicos, conforme necessário.

## Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para alterar as regras de WAF, devemos fazer o seguinte:

1. Selecione **Firewall de aplicativo Web** em **Configurações** no painel **Gateway de aplicativo**.

2. Selecione **Regras** nas configurações de WAF. Selecione **Habilitada** em **Configuração de regra avançada**, conforme mostrado na Figura 12.26:

The screenshot shows the 'packt-appgateway | Web application firewall' interface. On the left, there's a sidebar with icons for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Configuration and Web application firewall), and Export template. The 'Web application firewall' option is currently selected. At the top, there's a search bar, save, discard, and refresh buttons. The main area has tabs for 'Configure' and 'Rules', with 'Rules' being the active tab. Below that, it says 'Rule set \* OWASP 3.0'. Under 'Advanced rule configuration', the status is shown as 'Enabled' (which is highlighted in purple) and 'Disabled'. A note says 'Advanced rule configuration (i)'.

Figura 12.26: Habilitar Configuração avançada de regras

3. As regras serão exibidas na forma de lista. Podemos selecionar ou desmarcar as caixas para habilitar ou desabilitar as regras:

The screenshot shows the same 'packt-appgateway | Web application firewall' interface as Figure 12.26, but now the 'Enabled' button in the 'Advanced rule configuration' section is highlighted in green, indicating it is selected. Below this, there's a 'Search rules' input field. The main area displays a table of rules with columns for 'Enabled' (checkboxes) and 'Name'. All 15 listed rules have their checkboxes checked, indicating they are all enabled. The rules listed are: General, REQUEST-911-METHOD-ENFORCEMENT, REQUEST-913-SCANNER-DETECTION, REQUEST-920-PROTOCOL-ENFORCEMENT, REQUEST-921-PROTOCOL-ATTACK, REQUEST-930-APPLICATION-ATTACK-LFI, REQUEST-931-APPLICATION-ATTACK-RFI, REQUEST-932-APPLICATION-ATTACK-RCE, REQUEST-933-APPLICATION-ATTACK-PHP, REQUEST-941-APPLICATION-ATTACK-XSS, REQUEST-942-APPLICATION-ATTACK-SQLI, and REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.

Enabled	Name
<input checked="" type="checkbox"/>	> General
<input checked="" type="checkbox"/>	> REQUEST-911-METHOD-ENFORCEMENT
<input checked="" type="checkbox"/>	> REQUEST-913-SCANNER-DETECTION
<input checked="" type="checkbox"/>	> REQUEST-920-PROTOCOL-ENFORCEMENT
<input checked="" type="checkbox"/>	> REQUEST-921-PROTOCOL-ATTACK
<input checked="" type="checkbox"/>	> REQUEST-930-APPLICATION-ATTACK-LFI
<input checked="" type="checkbox"/>	> REQUEST-931-APPLICATION-ATTACK-RFI
<input checked="" type="checkbox"/>	> REQUEST-932-APPLICATION-ATTACK-RCE
<input checked="" type="checkbox"/>	> REQUEST-933-APPLICATION-ATTACK-PHP
<input checked="" type="checkbox"/>	> REQUEST-941-APPLICATION-ATTACK-XSS
<input checked="" type="checkbox"/>	> REQUEST-942-APPLICATION-ATTACK-SQLI
<input checked="" type="checkbox"/>	> REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION

Figura 12.27: Personalizar regras de WAF no painel Gateway de aplicativo

## Como funciona...

Um WAF vem com todas as regras ativadas por padrão. Isso pode desacelerar a performance, para que possamos desabilitar algumas das regras, se necessário. Além disso, há três conjuntos de regras disponíveis: **OWASP 2.2.9**, **OWASP 3.0** e **OWASP 3.1**. O conjunto de regras padrão (e recomendado) é **OWASP 3.0**, mas podemos alternar entre conjuntos de regras, conforme necessário.

## Criar uma política de WAF

Uma política de WAF permite lidar com definições e configurações de WAF como um recurso separado. Ao fazer isso, podemos aplicar a mesma política a vários recursos, em vez de gateways de aplicativo individuais. Uma política de WAF pode ser associada ao Gateway de aplicativo, ao Front Door ou à CDN.

## Preparação

Antes de iniciar, abra o navegador e acesse o portal do Azure em <https://portal.azure.com>.

## Como fazer isso...

Para criar um novo gateway de aplicativo, devemos fazer o seguinte:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Firewall de Aplicativo Web** em **Rede** (ou pesquise **Firewall de Aplicativo Web** na barra de pesquisa).
2. No novo painel, devemos concluir a seção **Básico** primeiro. Precisamos definir para o que a política será usada (Gateway de aplicativo, Front Door ou CDN), configurar **Assinatura** e **Grupo de recursos** e preencher os campos **Nome de política** e **Local**. Além disso, podemos definir se a política será habilitada ou desabilitada após sua criação:

## Create a WAF policy

Basics Policy settings Managed rules Custom rules Association Tags Review + create

Malicious attacks such as SQL Injection, Cross Site Scripting (XSS), and other OWASP top 10 threats could cause service outage or data loss, and pose a big threat to web application owners. Web Application Firewall (WAF) protects your web applications from common web attacks, keeps your service available and helps you meet compliance requirements.

[Learn more about Web Application Firewall](#)

### Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Policy for *	<input type="text" value="Regional WAF (Application Gateway)"/>
Subscription *	<input type="text" value="Microsoft Azure Sponsorship"/>
Resource group *	<input type="text" value="packt-demo"/> <a href="#">Create new</a>

### Instance details

Policy name *	<input type="text" value="Policy01"/>
Location *	<input type="text" value="(Europe) West Europe"/>
Policy state	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figura 12.28: Criar uma nova política de WAF

3. Nas **Configurações de política**, podemos definir **Modo** como **Detecção** ou **Prevenção**, juntamente com **Exclusões** e **Parâmetros globais**:

### Create a WAF policy

A Web Application Firewall (WAF) policy allows you to control access to your web applications by a set of custom and managed rules. There are multiple settings that apply to all rules within the policy. [Learn more](#)

Mode  Prevention  Detection

**Exclusions**

Select specific parts of incoming requests to exclude. All other items in the request will be evaluated.

Match variable	Operator	Selector
Select what to exclude	Select an operator	Enter a selector

**Global parameters**

Inspect request body  On  Off

Max request body size (KB) \*

Max file upload size (MB)

Figura 12.29: Definir configurações de política para sua política de WAF

4. Em **Regras gerenciadas**, podemos selecionar um conjunto de regras (**OWASP 2.2.9**, **OWASP 3.0** ou **OWASP 3.1**) e desabilitar algumas regras, se necessário (não é recomendável desabilitar regras a menos que necessário):

A pre-configured rule set is enabled by default. This rule set protects your web application from common threats defined in the top ten OWASP categories. The default rule set is managed by the Azure WAF service. Rules are updated as needed for new attack signatures. [Learn more](#)

Managed rule set

Expand all  Enable  Disable

Name	Description	Status
> General		Enabled
> REQUEST-911-METHOD-ENFORCEMENT		Enabled
> REQUEST-913-SCANNER-DETECTION		Enabled
> REQUEST-920-PROTOCOL-ENFORCEMENT		Enabled
> REQUEST-921-PROTOCOL-ATTACK		Enabled
> REQUEST-930-APPLICATION-ATTACK-LFI		Enabled
> REQUEST-931-APPLICATION-ATTACK-RFI		Enabled
> REQUEST-932-APPLICATION-ATTACK-RCE		Enabled
> REQUEST-933-APPLICATION-ATTACK-PHP		Enabled
> REQUEST-941-APPLICATION-ATTACK-XSS		Enabled
> REQUEST-942-APPLICATION-ATTACK-SQL		Enabled
> REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION		Enabled

Figura 12.30: Definir regras para sua política de WAF

5. Em **Regras personalizadas**, podemos adicionar regras adicionais, se necessário. Selecione **Adicionar regra personalizada** para adicionar uma:

### Create a WAF policy

Basics Policy settings Managed rules **Custom rules** Association Tags Review + create

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

**+ Add custom rule**

Priority Name

Action

No custom rules to display.

Figura 12.31: Adicionar uma regra personalizada à nossa política de WAF

6. Isso abrirá um novo painel que permitirá definir uma regra personalizada. Precisamos preencher o campo **Nome de regra personalizado** e definir **Prioridade** como **1**. Em **Condições**, estamos criando um tipo de correspondência e variáveis que precisam ser combinadas para acionar a regra. Por fim, definimos uma resposta (permissão, negação ou log):

### Add custom rule

X

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. [Learn more about custom rules](#)

Custom rule name \*

Rule1

Priority \*

1

#### Conditions

If

Match type

IP address

Match variable

RemoteAddr

Operation

Does contain

Does not contain

IP address or range

195.222.45.5

IPv4 or IPv6 address or ranges

**+ Add new condition**

Then

Deny traffic

Figura 12.32: Definir condições para sua regra personalizada

7. Depois que a regra personalizada for criada, ela será exibida na lista e podemos seguir para a seção **Associação**:

### Create a WAF policy

Basics Policy settings Managed rules **Custom rules** Association Tags Review + create

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more ↗](#)

**+ Add custom rule**

Priority	Name	Action
1	Rule1	Block

Figura 12.33: Lista mostrando a nova regra personalizada

8. Na seção **Associação**, estamos criando uma associação com o serviço ao qual queremos aplicar a política. Essa seção dependerá do tipo de serviço selecionado anteriormente (no nosso caso, o gateway de aplicativo). Selecione **Associar um gateway de aplicativo**:

### Create a WAF policy

Basics Policy settings Managed rules **Association** Tags Review + create

#### Associated application gateways

Associate this WAF policy with a specific application gateway. This will remove and replace any existing WAF policy associations with the selected application gateway. A WAF policy can be associated with multiple application gateways. [Learn more ↗](#)

**+ Associate an application gateway**

Search resources:

Application Gateways

Add a resource to get started

#### Associated HTTP listeners

Associate this WAF policy with a specific listener for a particular application gateway. A WAF policy can be associated with multiple listeners and application gateways. [Learn more ↗](#)

**+ Associate listeners**  Remove associated listeners  Collapse all

Application Gateways

Listeners

No results

Figura 12.34: Criar uma associação com o nosso gateway de aplicativo

9. No novo painel, selecione **Gateway de aplicativo** no menu suspenso. Observe que somente o **WAF V2 SKU** é compatível:

### Associate an application gate...

×

Application Gateway (WAF v2 SKU) \*

packt-appgateway

▼

Apply the Web Application Firewall policy configuration even if it is different from the current configuration

Figura 12.35: Escolher seu gateway de aplicativo no menu suspenso

10. Depois que o **Gateway de aplicativo** for selecionado, precisamos associar ouvintes. Selecione **Associar ouvinte** em **Associar ouvintes HTTP**. No novo painel, no menu suspenso, selecione o ouvinte que deseja usar:



Figura 12.36: Selecionar o ouvinte no menu suspenso

11. Depois que o ouvinte estiver associado, poderemos começar a criar nossa política de WAF:

#### Create a WAF policy

Figura 12.37: Configuração final da nossa nova política de WAF

### Como funciona...

Nossa política de WAF contém todas as definições e configurações necessárias para o nosso WAF e pode ser associada ao Gateway de aplicativo, ao Front Door ou à CDN. Ela pode ser associada a vários recursos, mas somente um tipo de cada vez. O **Modo** determinará qual tipo de medida será tomada quando um problema for detectado. **Prevenção** bloqueará solicitações suspeitas e **Detectação** criará somente a entrada de log.



# 13

## Azure Front Door e CDN do Azure

Vários serviços de rede no Microsoft Azure são dedicados à entrega de aplicações. O **Azure Front Door** e a **CDN do Azure** são serviços que nos permitem criar aplicações para entrega global e aproveitar a rede global de datacenters do Azure. Aproveitando esse recurso, podemos fornecer a mesma experiência aos nossos usuários, independentemente de sua localização física.

Abordaremos as seguintes receitas neste capítulo:

- Criar uma instância do Azure Front Door
- Criar um perfil da CDN do Azure

### Requisitos técnicos

Para este capítulo, é necessário o seguinte:

- Uma assinatura do Azure

## Criar uma instância do Azure Front Door

O Azure Front Door é usado para o roteamento global do tráfego da Web para aplicações distribuídas em diferentes regiões do Azure. Com o Azure Front Door, podemos definir, gerenciar e monitorar o roteamento do nosso tráfego da Web e habilitar o failover global rápido. Ele permite a entrega de nossas aplicações com a melhor performance e alta disponibilidade. O Azure Front Door é um balanceador de carga L7, semelhante ao Gateway de Aplicativo. No entanto, há uma diferença em termos de distribuição global. Em termos de distribuição global, ele é semelhante a outro serviço, o Gerenciador de Tráfego. Basicamente, o Azure Front Door combina os melhores recursos do Gateway de Aplicativo e do Gerenciador de Tráfego: a segurança do Gateway de Aplicativo e a capacidade de distribuição do Gerenciador de Tráfego.

### Preparação

O Azure Front Door exige serviços que serão adicionados ao pool de back-end. Você pode usar um script na seção **Preparação** da receita **Adicionar um ponto de extremidade**, no Capítulo 11, **Gerenciador de Tráfego**.

Depois disso, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar uma nova instância do Azure Front Door, siga estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **Front Door** em **Rede** (ou pesquise **Front Door** na barra de pesquisa).
2. No novo painel, temos várias seções para abordar. Em **Básico**, precisamos fornecer detalhes para **Assinatura** e **Grupo de recursos**. O **local do grupo de recursos** é selecionado e acinzentado automaticamente:

## Create a Front Door

Basics Configuration Tags Review + create

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(s) load balancer. It provides built-in DDoS protection and application layer security and caching. Front Door enables you to build applications that maximize and automate high-availability and performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more about Front Door](#)

### PROJECT DETAILS

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Microsoft Azure Sponsorship"/>
Resource group *	<input type="text" value="Packt-Networking-Portal"/> <a href="#">Create new</a>
Resource group location	<input type="text" value="West Europe"/>

Figura 13.1: Fornecer detalhes de Assinatura e Grupo de recursos

3. Na seção **Configuração**, precisamos fornecer detalhes para **Front-ends/ domínios, Pools de back-end e Regras de roteamento**. Clique na caixa **Front-ends/domínios** para iniciar o painel de configuração:

**Create a Front Door**

Basics Configuration Tags Review + create

Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. [Learn more](#)

The screenshot shows the 'Create a Front Door' configuration page. At the top, there are tabs for 'Basics', 'Configuration' (which is selected), 'Tags', and 'Review + create'. Below the tabs, there is a brief description of the configuration process: 'Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool.' A link to 'Learn more' is provided. The main area contains three tabs: 'Frontends/domains', 'Backend pools', and 'Routing rules'. The 'Frontends/domains' tab is active, showing a message: '\* Step 1 Get started by adding a frontend host.' There is a plus sign icon to add a new frontend host.

Figura 13.2: Selecionar a opção de configuração Front-ends/domínios

4. No novo painel, devemos fornecer um nome de host e selecionar se queremos habilitar a **AFINIDADE DE SESSÃO** e o **FIREWALL DE APPLICATIVO WEB**:

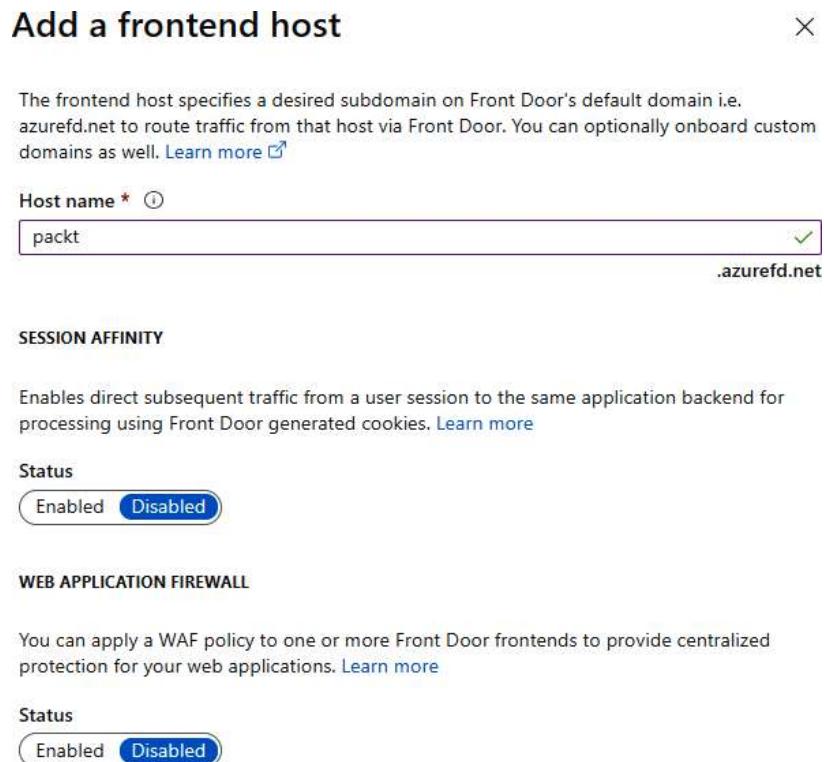


Figura 13.3: Habilitar AFINIDADE DE SESSÃO e FIREWALL DE APPLICATIVO WEB

5. Depois que o front-end for criado, voltaremos à seção **Configuração**. Selecione **Pools de back-end** para iniciar o próximo painel de configuração:

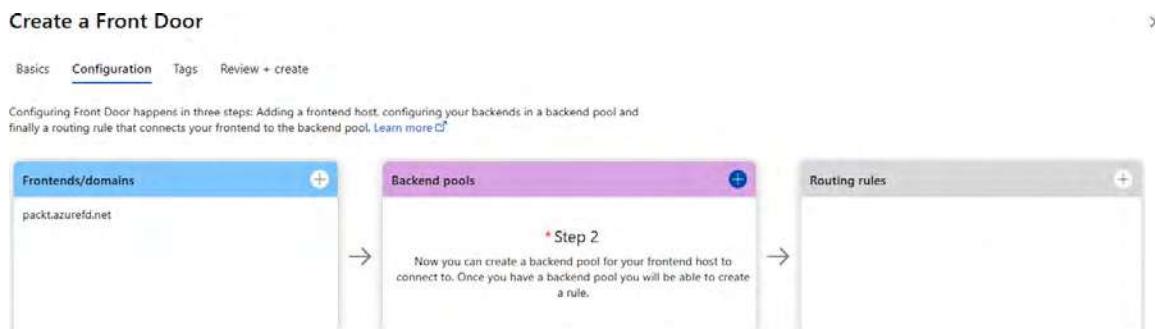


Figura 13.4: Selecionar a opção de configuração Pools de back-end

6. Precisamos fornecer um nome para nosso pool de back-end e adicionar serviços a ele. Para adicionar um back-end, selecione a opção **Adicionar um back-end**:

**Add a backend pool**

A backend pool is a set of equivalent backends to which Front Door load balances your client requests. [Learn more](#)

**Name \***  
backend

**BACKENDS**

Backend host name	Status	Priority	Weight
Add a backend to get started			

+ [Add a backend](#)

Figura 13.5: Adicionar um pool de back-end

7. Para adicionar um back-end, devemos selecionar o **Tipo de host de back-end** e a **Assinatura** primeiro. Com base em nossa seleção, poderemos escolher serviços (de um tipo selecionado na assinatura selecionada) em nome do **Host de back-end**. Também precisamos fornecer detalhes para **Cabeçalho do host de back-end**, portas (HTTP e HTTPS), **Prioridade** e **Peso**. Por fim, precisamos selecionar a opção **Habilitado** para **Status**:

**Add a backend**

← Go back to backend pool

Backends are your application servers where Front Door will route your client requests to. You can assign weights to your backends to define proportion of traffic to be sent and set priority for the backends to define active/stand-by kind of architectures. [Learn more](#)

**Backend host type \***  
App service

**Subscription \***  
Microsoft Azure Sponsorship

**Backend host name \* ⓘ**  
packt-demo-webapp-01.azurewebsites.net

**Backend host header ⓘ**  
packt-demo-webapp-01.azurewebsites.net

**HTTP port \* ⓘ**  
80

**HTTPS port \* ⓘ**  
443

**Priority \* ⓘ**  
1

**Weight \* ⓘ**  
50

**Status**  
Disabled **Enabled**

Figura 13.6: Detalhes do pool de back-end

8. Repita esse processo para adicionar pelo menos outro ponto de extremidade ao pool de back-end:

## Add a backend

[← Go back to backend pool](#)

Backends are your application servers where Front Door will route your client requests to. You can assign weights to your backends to define proportion of traffic to be sent and set priority for the backends to define active/stand-by kind of architectures. [Learn more ↗](#)

**Backend host type \***

App service

**Subscription \***

Microsoft Azure Sponsorship

**Backend host name \* ⓘ**

packt-demo-webapp-02.azurewebsites.net

**Backend host header ⓘ**

packt-demo-webapp-02.azurewebsites.net

**HTTP port \* ⓘ**

80

**HTTPS port \* ⓘ**

443

**Priority \* ⓘ**

1

**Weight \* ⓘ**

50

**Status**

Disabled Enabled

The screenshot shows the 'Add a backend' configuration page. It includes fields for host type (App service), subscription (Microsoft Azure Sponsorship), host name (packt-demo-webapp-02.azurewebsites.net), host header (packt-demo-webapp-02.azurewebsites.net), port numbers (HTTP: 80, HTTPS: 443), priority (1), weight (50), and status (Enabled). Each field has a green checkmark indicating it is valid.

Figura 13.7: Adicionar outro ponto de extremidade ao pool de back-end

9. Depois de adicionar pontos de extremidade suficientes ao pool de back-end, podemos prosseguir com a configuração:

The screenshot shows the 'Add a backend pool' configuration page. At the top, it says 'Add a backend pool' and has a close button 'X'. Below that, a descriptive text states: 'A backend pool is a set of equivalent backends to which Front Door load balances your client requests.' with a 'Learn more' link. The main section is titled 'Name \*' with a field containing 'backend' and a green checkmark icon. Under 'BACKENDS', there is a table with two rows:

Backend host name	Status	Priority	Weight
packt-demo-webapp-01.azurewebsites.net	<input checked="" type="checkbox"/> Enabled	1	50
packt-demo-webapp-02.azurewebsites.net	<input checked="" type="checkbox"/> Enabled	1	50

At the bottom left, there is a '+ Add a backend' button.

Figura 13.8: Configurar o pool de back-end

10. As investigações de integridade exigem informações para **Caminho** (use / para a opção padrão ou adicione o seu próprio), **Protocolo** (HTTP ou HTTPS), **Método de investigação** (HEAD ou GET) e **Intervalo** em segundos (a frequência com que a investigação verificará a integridade do back-end):

The screenshot shows the 'Configure health probes' configuration page. It starts with a heading 'HEALTH PROBES' and a note: 'Front Door sends periodic HTTP/HTTPS probe requests to each of your configured backends to determine the proximity and health of each backend to load balance your end user requests.' with a 'Learn more' link. Below this, there are several configuration fields:

- Status:** A radio button group where 'Enabled' is selected.
- Path \***: A text input field containing '/'.
- Protocol**: A radio button group where 'HTTPS' is selected.
- Probe method**: A dropdown menu showing 'HEAD'.
- Interval (seconds) \***: A text input field containing '30'.

Figura 13.9: Configurar investigações de integridade para verificar a integridade do back-end

11. Na seção **BALANCEAMENTO DE CARGA**, devemos fornecer informações para **Tamanho da amostra, Amostras bem-sucedidas necessárias e Sensibilidade da latência:**

#### LOAD BALANCING

Configure the load balancing settings to define what sample set we need to use to call the backend as healthy or unhealthy. The latency sensitivity with value zero (0) means always send it to the fastest available backend, else Front Door will round robin traffic between the fastest and the next fastest backends within the configured latency sensitivity. [Learn more ↗](#)

**Sample size \*** ⓘ

4

**Successful samples required \*** ⓘ

2

**Latency sensitivity (in milliseconds) \*** ⓘ

0

Figura 13.10: O painel **BALANCEAMENTO DE CARGA**

12. Depois de adicionar todas as informações necessárias, podemos criar um pool de back-end. Isso nos levará de volta à seção **Configuração** novamente. Selecione **Regras de roteamento** para iniciar o painel **Regras de roteamento**:

Create a Front Door

Basics Configuration Tags Review + create

Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. [Learn more ↗](#)

**Frontends/domains**

packt.azurefd.net

**Backend pools**

backend

**Routing rules**

\* Step 3  
You can now add a rule to connect your frontend host to backend pool(s).

Figura 13.11: Selecionar a opção de configuração **Regras de roteamento**

13. No painel **Adicionar uma regra**, devemos fornecer detalhes para **Nome** (para nossa regra), **Protocolo aceito** (**HTTP, HTTPS ou ambos**), **Front-ends/ domínios** (escolha a opção selecionada anteriormente) e **PADRÕES A SEREM CORRESPONDIDOS** (os padrões de caminho de URL que a rota aceitará):

## Add a rule

A routing rule maps your frontend host and a matching URL path pattern to a specific backend pool. [Learn more](#)

**Name \***  
rule1

**Accepted protocol** ⓘ  
HTTP and HTTPS

**Frontends/domains**  
packt.azurefd.net

**PATTERNS TO MATCH**

Set this to all the URL path patterns that this route will accept. For example, you can set this to /users/\* to accept all requests on the URL www.contoso.com/users/\*. [Learn more](#)

/\* /path

Figura 13.12: Adicionar detalhes de regras de roteamento

14. Em **DETALHES DA ROTA**, precisamos fornecer detalhes para **Tipo de rota**, **Pool de back-end** e **Protocolo de encaminhamento**. Opcionalmente, podemos escolher se queremos habilitar as opções **Regraváculo de URL** e **Cache**:

**ROUTE DETAILS**

Once a route for a Front Door is matched, the Rules Engine configuration associated with this routing rule is executed, followed by general route configuration defined below. [Learn more](#)

**Route type** ⓘ  
 Forward  Redirect

**Backend pool \***  
backend

**Forwarding protocol** ⓘ  
 HTTPS only  HTTP only  Match request

**URL rewrite** ⓘ  
 Enabled  Disabled

**Caching** ⓘ  
 Enabled  Disabled

Figura 13.13: O painel DETALHES DA ROTA

15. Depois que a regra de roteamento for criada, teremos todos os componentes necessários e poderemos prosseguir com a criação da instância do Azure Front Door navegando até a guia **Revisar + Criar**:

### Create a Front Door

x

Basics Configuration Tags Review + create

Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. [Learn more](#)



Figura 13.14: Todos os componentes são configurados

## Como funciona...

Todas as solicitações de aplicações estão chegando ao front-end. Com base nas regras que criamos, as solicitações são encaminhadas para pontos de extremidade no back-end. As regras de平衡amento de carga garantirão que as solicitações serão enviadas para o back-end mais rápido disponível.

A amostra de taxa bem-sucedida garante que os pontos de extremidade no back-end estejam disponíveis e determina quantas amostras são enviadas por vez. **Amostras bem-sucedidas necessárias** definem quantas solicitações precisam ser bem-sucedidas para que um ponto de extremidade seja considerado íntegro. **Sensibilidade de latência** define a tolerância entre o ponto de extremidade com a menor latência e o restante dos pontos de extremidade. Por exemplo, digamos que a configuração de **Sensibilidade de latência** seja 30 ms, enquanto a latência do ponto de extremidade A é 15 ms, a do ponto de extremidade B é 30 ms, e a do ponto de extremidade C é 90 ms. Os pontos de extremidade A e B serão colocados no pool mais rápido, pois a diferença de latência é menor do que o limite de sensibilidade, e o ponto de extremidade C está fora, pois está acima do limite.

Regras de roteamento definem como o tráfego é tratado e se o tráfego específico precisa ser redirecionado ou encaminhado. Se **Regravamento de URL** estiver habilitada, poderemos criar uma URL que será encaminhada para um back-end. Se o cache estiver habilitado, o Azure Front Door armazenará conteúdo estático em cache para entrega mais rápida.

### Observação

Muitos termos e opções são os mesmos que para o Gateway de Aplicativo, e não vamos explicá-los novamente. Além disso, o **Firewall de Aplicativo Web (WAF)** é uma opção que pode ser habilitada no Azure Front Door para melhor segurança. Para obter mais informações sobre o WAF, consulte as receitas relacionadas no *Capítulo 12, Gateway de Aplicativo do Azure e WAF do Azure*.

O Azure Front Door também inclui várias opções e regras configuráveis que podem ajudar suas aplicações Web a oferecer um serviço centrado no cliente e na marca. Aqui estão alguns recursos mais importantes relacionados ao Azure Front Door:

- **Saiba mais sobre domínios personalizados:** <https://docs.microsoft.com/azure/frontdoor/front-door-custom-domain>
- **Saiba mais sobre domínios curinga:** <https://docs.microsoft.com/azure/frontdoor/front-door-wildcard-domain>
- **Saiba mais sobre o mecanismo de regras :** <https://docs.microsoft.com/azure/frontdoor/front-door-rules-engine>
- **Saiba mais sobre as condições de correspondência do mecanismo de regras :** <https://docs.microsoft.com/azure/frontdoor/front-door-rules-engine-match-conditions>
- **Saiba mais sobre as ações do mecanismo de regras :** <https://docs.microsoft.com/azure/frontdoor/front-door-rules-engine-actions>

Depois de criar a instância do Azure Front Door, vamos avançar para a próxima receita e aprender a criar um perfil da CDN do Azure.

## Criar um perfil da CDN do Azure

A **Rede de Distribuição de Conteúdo do Azure (CDN do Azure)** é uma rede distribuída que permite a entrega mais rápida do conteúdo da Web aos usuários finais. A CDN do Azure armazena conteúdo em cache em servidores de borda em vários locais (regiões do Azure). Esse conteúdo está disponível para os usuários finais mais rapidamente, com latência de rede mínima.

### Preparação

Antes de iniciar, abra seu navegador e acesse o portal do Azure em <https://portal.azure.com>.

### Como fazer isso...

Para criar um novo perfil da CDN do Azure, siga estas etapas:

1. No portal do Azure, selecione **Criar um recurso** e escolha **CDN** em **Rede** (ou pesquise **CDN** na barra de pesquisa).
2. No novo painel, devemos fornecer informações para os campos **Nome**, **Assinatura**, **Grupo de recursos** e **Nível de preços**. Se decidirmos fornecer um ponto de extremidade da CDN neste momento, precisaremos fornecer detalhes para **Nome do ponto de extremidade da CDN**, **Tipo de origem** e **Nome do host de origem**. **Nome do host de origem** estará disponível na lista suspensa, com base na opção de **Tipo de origem** selecionada:

## CDN profile

Name \*

Subscription \*

Resource group \*

[Create new](#)

Resource group location ⓘ

Pricing tier ([View full pricing details](#)) \*

Create a new CDN endpoint now

CDN endpoint name \*

Origin type \*

Origin hostname \* ⓘ

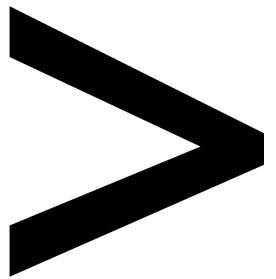
Figura 13.15: Adicionar detalhes do perfil da CDN do Azure

3. Agora, podemos criar um perfil da CDN do Azure. Após a implantação, a CDN do Azure começa a armazenar o conteúdo da origem e podemos começar a usá-lo imediatamente.

### Como funciona...

A CDN do Azure armazena o conteúdo da nossa aplicação em servidores de borda. Como esses servidores de borda são distribuídos entre regiões do Azure, temos cópias de conteúdo em praticamente todas as regiões do mundo. O conteúdo é entregue aos usuários finais pelo local mais próximo, que fornece latência de rede mínima. Vamos supor que uma aplicação seja hospedada na Europa Ocidental e um usuário esteja localizado na parte ocidental dos EUA. Nesse caso, o conteúdo não será entregue pelo local original, mas do local mais próximo do usuário, nessa instância, Oeste dos EUA. Dessa forma, podemos garantir que cada usuário tenha a melhor experiência e entrega onde quer que esteja.





# índice

## Sobre

Todas as principais palavras-chave usadas neste livro são capturadas em ordem alfabética nesta seção. Cada uma é acompanhada pelo número da página onde aparece.

## A

acesso: 19, 24, 39, 49, 55-56, 123-124, 136, 143, 145, 163, 166, 170, 173, 190 conta: 115-116, 217 ação: 36, 38, 48, 104, 241 endereço: 1, 3-4, 6-14, 16, 19-20, 24, 26-27, 45, 49, 51-66, 68-69, 71, 74, 76, 78, 80-81, 90-91, 94, 100-103, 105, 109-112, 118-121, 128, 134, 145, 148-151, 154, 156-157, 160-161, 166, 172, 176, 178-180, 187-190, 192-193, 199, 209-211, 214, 227, 229, 234 afinidade: 219, 224-226, 246 aliases: 90 alocação: 68, 192-193 análise: 116 anycast: 83 dispositivo: 100-103, 120, 163, 166 atribuir: 20, 40, 42, 44, 55-57 associar: 33, 40-44, 46-48, 56, 69, 93-95, 121, 165, 182, 231, 240-241 auditar: 114, 116 automatizar: 6, 34, 54, 79 autônomo: 78, 154

## B

back-end: 12, 44, 171, 175-176, 178, 180-184, 186-188, 190, 192-193, 196-197, 201, 203, 207, 210, 212, 214-216, 218-219, 221-224, 226, 229-230, 244-249, 251, 253 balanceador: 37, 170-173, 175-182, 184-191, 195, 201, 209-212, 221, 244 bastion: 5, 145-151

## C

cache: 254 sem classe: 6 cliente: 91, 136, 156-157, 188 fechado: 54 nuvens: 123 comando: 6-7, 11-12, 34, 39, 44, 54, 76, 112-114 condições: 231, 239, 253 configuração: 114 configurar: 20, 39, 47, 73-74, 93, 112, 121, 128, 130, 133, 152, 154, 163, 180, 201, 203-204, 208-209, 218, 225, 227, 231, 236 conexão: 19, 53, 61, 74-78, 81, 102, 123-128, 130, 133, 136-143, 145-146, 150-153, 156, 158-160, 162-166, 170, 219, 224-226

console: 6, 34, 39, 44, 54, 76, 79, 112-113 controle: 31-32, 45-46, 48, 108, 110, 140, 143, 152, 158, 173, 193, 211, 226 controlado: 124, 145 no cliente: 253

## D

banco de dados: 124 datacenter: 2, 6, 18-19, 23 dedicado: 23, 148, 193, 243 definido: 3, 7, 10-11, 13-14, 20, 24, 27, 33, 88, 91, 96, 100, 102, 116, 121, 158, 184, 197, 201, 221, 226 delegação: 8, 148 delegar: 93, 98, 103-105, 207 entrega: 243, 253-255 negado: 37, 42, 44, 143 implantado: 2, 6-7, 33-34, 71, 150 desanexar: 26, 29 detectar: 184, 186, 234 detecção: 234, 238, 241 dispositivo: 78, 124, 128-130, 160-163 diagnóstico: 107, 114-116 direcionar: 188, 197 direcionado: 91, 184, 196-197, 224, 226 desabilitar: 20, 58, 93, 123, 160, 207-208, 219, 225, 235-236, 238 desabilitar: 190, 208 dissociar: 96, 99 distribuir: 175, 195, 197, 201, 203

baseado em dns: 195  
-dnsname: 131  
domínio: 83-85, 88, 91,  
121, 196, 226-227  
domínios: 83, 86,  
245, 250, 253  
download: 128-130,  
136, 162  
descarga: 219, 224-226  
menu suspenso: 18,  
56, 88, 110, 134, 140,  
240-241, 254  
descartado: 193  
dinâmica: 27, 54, 58-61,  
65-66, 79, 172, 176

## E

econômico: 139  
editor: 135  
efeito: 113, 122, 201  
elementos: 26  
codificado: 132  
criptografado: 128, 139  
ponto de extremidade:  
54-55, 146, 166-170,  
173, 175, 184, 186, 195,  
197-201, 203-207,  
210, 230-231, 244,  
248, 252, 254  
aplicar: 110  
impostas: 234  
entradas: 196  
erros: 217, 227  
exceção: 27, 114  
excluir: 16, 190, 234  
expandir: 212  
esperar: 229  
explícito: 175, 190  
exportar: 131-133  
exposto: 123, 166  
extensão: 45, 107  
externo: 195, 199, 201

## F

fator: 42, 65  
falha: 231  
failover: 202, 210, 244  
filtragem: 45, 121-122  
firewall: 5, 70-71, 74, 76,  
80-81, 107-108, 110-114,  
116, 118-122, 166, 212,  
231-234, 236, 246, 253  
firmware: 129  
cinco tuplas: 188  
flutuante: 187  
forçado: 107, 110, 116, 120  
forçar: 148  
formato: 6, 8, 12, 100,  
121, 132, 201  
encaminhar: 188, 201,  
226, 229, 251  
front door: 253  
front-end: 5, 12, 49,  
172, 175-176, 178,  
180, 184, 186-190,  
192-193, 197, 201, 208,  
210-212, 214, 217, 227  
front-ends: 214,  
216, 245, 250  
funções: 130

## G

gateway: 10-11, 73-81,  
92-93, 100, 102-103,  
117, 120, 125-128,  
133-134, 136, 138-139,  
143, 148, 154-155, 157,  
160, 211-214, 220-224,  
226-228, 230-236,  
240-241, 244, 253

gateways: 73, 125-126,  
136, 139, 143, 151,  
221, 224, 228, 236  
gerar: 116, 130  
geração: 77  
geográfico: 197, 205  
global: 234, 238, 243-244  
grupos: 25, 31, 45-47,  
54, 107, 120-121  
gwipconfig: 79

## H

cabeçalho: 201, 247  
cabeçalhos: 201  
integridade: 171, 175,  
184-188, 190, 201,  
210, 230-231, 249  
hospedado: 84-85, 91, 255  
nomes de host: 211-212  
híbrido: 19, 114,  
123-124, 156

## I

implícito: 187, 190  
entrada: 19, 35, 37,  
39-40, 48-49, 54,  
108, 175 188-190  
entrada: 31, 48, 107,  
186-187, 197, 201,  
211, 221, 226, 234  
Incompleto: 224  
individual: 26, 121,  
170, 201, 236  
em trânsito: 226  
inicial: 6, 13, 61  
iniciar: 162  
inspecionado: 120, 234  
inspeção: 116  
instalar: 6

instância: 18-19, 108, 110, 112, 121, 146-147, 149-150, 190, 192-193, 213, 243-244, 252-253, 255  
integrar: 87, 170  
interface: 17, 25-29, 31-32, 42-44, 55, 57, 61, 63, 65, 67, 151, 178  
interno: 123, 175-179, 181, 184, 186-188  
internet: 2, 24, 37, 39-40, 51, 100-102, 117-118, 120, 166, 178, 180, 190  
intervalo: 185-186, 231, 249  
problemas: 59, 70, 105, 184, 234

## K

-keylength: 130-131  
-keyspec: 130-131  
-keyusage: 131

## L

rótulos: 165  
latência: 197, 204, 250, 252, 254-255  
limitado: 193, 195, 207, 209-210, 213  
limites: 178  
ouvinte: 217, 226-227, 229, 241  
local: 7, 36, 38, 53, 74, 76, 111-114, 127, 133, 138, 152, 166, 195, 197-198, 204-205, 236, 243-244, 255  
-location: 6-7, 34, 40, 54, 76, 79, 111, 114, 198  
bloqueado: 127, 138

## M

máquina: 17-18, 31, 52, 146, 150-151, 171, 176, 189, 215, 222  
malicioso: 234  
gerenciado: 110, 238  
gerenciamento: 11, 22, 120-121, 123-124, 136, 145, 150-151  
gerenciador: 91, 140, 195-198, 200-210, 244  
obrigatório: 20, 216  
mapeamento: 186-190, 211  
mestre: 1, 32, 52, 74, 108, 124, 176, 196  
máximo: 116, 192, 209, 221  
métodos: 197, 201  
intermediária: 178  
migrar: 56  
migrado: 55  
mínimo: 254  
falta: 79, 100, 216  
modificar: 80  
modificação: 73, 80-81  
momentos: 28-29, 33  
monitorar: 110, 152, 184, 186, 188, 210, 230, 244  
monitorado: 217, 227, 230-231  
monitores: 227  
vários: 11-12, 26, 28, 44, 52, 67, 69, 73, 80, 88, 91, 99, 105, 121, 143, 152-153, 175, 197, 201-203, 205, 209, 211-212, 221, 223, 227, 236, 241, 254  
multissite: 227  
várias camadas: 178

## N

nativo: 173  
navegar: 252  
animado: 199, 201  
rede: 1-8, 10-14, 16-18, 20-21, 24-29, 31-34, 37, 41-44, 51, 54-55, 57, 61, 63, 65, 67, 71, 73-81, 83, 86-88, 91-96, 100, 102-103, 107-108, 110, 112, 114, 118, 120, 122-128, 130, 133-134, 136, 138-140, 143, 145-152, 163-166, 170-173, 176, 178-179, 182, 188-190, 197, 204, 213, 243, 254-255  
redes: 1-2, 17-20, 22, 25-29, 33, 45-46, 53, 70, 74, 77, 83-84, 86, 92, 107, 110, 114, 116, 120, 149, 152-153, 170-171, 176, 178, 196, 213, 236, 243-244, 254

## O

sob demanda: 136  
openvpn: 134  
operação: 211  
operações: 80, 124, 223  
otimizar: 212  
otimizado: 211, 221  
origem: 204-205, 254-255  
saída: 35, 37-39, 107-108, 110, 172, 175, 187, 190-193  
saída: 31  
saída: 7  
fora: 14, 102, 123  
sobrepor: 8, 11-12, 16, 134

substituir: 219, 224-226  
visão geral: 89, 128, 208

## P

parâmetros: 6-7, 11, 33, 39, 45, 48, 53-54, 74, 76, 111, 234, 238  
aprovação: 24  
senha: 19, 151  
padrões: 250  
emparelhamento:  
  124, 139-140,  
  142-143, 151-152  
permissão: 136  
físico: 23, 243  
política: 116, 162,  
  212, 236-241  
possível: 123  
powershell: 1, 6-7, 11-12,  
  32-34, 39-40, 44,  
  52, 54, 73-76, 79-80,  
  107-108, 111-113,  
  123-124, 130, 198  
predefinido: 129, 134  
prefixo: 12, 52, 70-71,  
  76, 100-103, 118, 148  
premium: 20  
pré-compartilhado: 162  
prioridade: 36-39, 42, 44,  
  48, 112-113, 195, 197,  
  203-204, 239, 247  
privado: 2, 11, 24, 26,  
  51-52, 61-69, 71, 73,  
  83, 85-88, 132, 139,  
  143, 145-146, 154,  
  160, 166-173, 176, 178,  
  180, 201, 214, 227  
investigações: 171,  
  175, 184-185, 212,  
  219, 230, 249  
processo: 18, 24, 26-29,

  34, 54, 79, 116, 136, 180,  
  200, 210, 221, 248  
processar: 223  
perfil: 195-198, 201-202,  
  204-205, 207-208,  
  243, 253-255  
projeto: 213  
protocolo: 36, 38, 48,  
  74, 78, 93, 123, 127,  
  160, 162, 184-189,  
  192, 211, 217, 219, 225,  
  227, 231, 249-251  
-protocol: 39-40, 112-113  
protocolos: 187, 202,  
  211-212, 221, 227  
provedor: 161  
proximidade: 23  
público: 4, 19-20, 24, 26,  
  51-63, 65, 67, 69-71,  
  74, 76, 78, 80-81,  
  86, 101, 110-112, 120,  
  123, 128, 135, 145,  
  149-151, 171, 175-176,  
  178-181, 184, 186, 188,  
  190-191, 197, 199, 201,  
  209-210, 214, 227

## Q

qualificado: 84, 121, 196  
consultas: 83

## R

intervalos: 48, 121  
reinicializado: 59  
registro: 59, 83-85, 87-92  
redirecionar: 217, 224  
redundante: 54  
regiões: 195, 197-198, 201,  
  209, 244, 254-255  
registrado: 84, 88  
remoto: 123, 143

repositório: 129  
solicitações: 175, 178, 180,  
  184, 188, 201, 210-212,  
  221, 224, 226-227,  
  229-230, 234, 241, 252

redirecionar: 100

resolução: 83,  
  87-88, 91, 170

recurso: 2, 6-7, 11, 18,  
  26-27, 33-34, 40, 45,  
  48, 51-62, 70, 74, 76-77,  
  84, 86, 88, 92-93, 110,  
  116-117, 120-121, 127,  
  138, 140, 149, 152, 154,  
  160, 165-166, 169-170,  
  172, 176, 178-179, 196,  
  199, 209-210, 212-213,  
  223, 236, 244-245, 254

resposta: 184, 239

restrito: 136, 173

retenção: 115-116

regravação: 251, 253

baseado em função: 173

rotação: 230

-route: 114

routebased: 79

rotas: 91, 93, 100, 102,  
  104-105, 112, 116-117,  
  120, 122, 165

roteamento: 6, 69,  
  78, 83, 92, 165-166,  
  175, 196-197, 201,  
  203-205, 212, 216-218,  
  220-221, 223, 227-229,  
  244-245, 250-253

## S

amostra: 129, 250, 252

escalar: 175, 203

schildcert: 131

-scope: 6

script: 7, 12, 34, 39-40, 54, 79-80, 130, 198, 244  
seguro: 2, 4, 123-124, 128, 130, 136, 139, 145-146, 150, 166, 170  
segurança: 5, 8, 20, 25-27, 31-33, 35, 37-38, 45-49, 54, 107, 123, 127, 146, 148, 173, 178, 231, 234, 244, 253  
seletor: 162  
servidor: 18, 23, 36, 83, 121-122, 136, 166, 171, 184, 186, 190, 211, 226  
servidores: 23, 26, 61, 83-84, 156-157, 169, 180, 190, 211, 223, 254-255  
compartilhado: 127, 138  
assinatura: 130-131  
-signer: 131  
origem: 36, 38, 45, 48, 172, 188, 190, 226  
srootcert: 130-131  
autônomo: 52, 87  
padrão: 20, 54, 70, 78, 111, 170-171, 173, 176, 178-179, 190, 232  
iniciar: 64  
estática: 27, 54, 56, 58-60, 62, 111, 165-166, 172, 176, 253  
status: 130, 139, 142, 230, 233, 247  
armazenamento: 20, 115-116, 217  
sub-domínio: 89, 91  
sub-domínios: 84, 88  
-subject: 130-131

sub-rede: 1, 3-8, 10-12, 14-16, 20-21, 26-27, 31-33, 40-42, 44-45, 48-49, 62, 64, 76-77, 79-80, 83, 92-100, 102, 108-112, 116, 118-121, 128, 147-149, 151, 170, 172, 176, 178-179, 197, 213  
-subnetid: 79  
sub-redes: 1, 3, 5, 8, 11-12, 14, 16, 31, 40, 42, 49, 80-81, 91-97, 99-100, 108, 118, 121, 147, 176  
compatível: 128-129, 201, 240  
suspeito: 241  
interruptor: 236  
sistema: 6, 78, 83, 114, 154

**T**

tabelas: 85, 91-92, 98, 105, 113-114, 165  
destino: 169, 171, 178, 180, 189, 199, 210, 215, 218, 222-223, 226, 229  
limite: 185-186, 231, 252  
tempo limite: 53, 187, 189, 192, 231  
tolerância: 252  
tráfego: 31-32, 35-39, 42, 44-46, 48-49, 54, 73, 85, 91-92, 100-103, 107-108, 110, 112-114, 116, 120, 123, 139-140, 143, 148, 162, 166, 175, 178, 180, 184, 186-188, 190, 195-198, 200-212, 221, 223-224, 227-228, 234, 244, 253

túnel: 107, 110, 116, 120  
duas tuplas: 188

## U

cancelar atribuição: 57  
atribuição cancelada: 56-58  
desmarcar: 235  
indefinido: 14  
não detectado: 184  
não íntegro: 185-186, 230-231  
tempo de atividade: 78  
nome de usuário: 19, 151

## V

validar: 177, 180  
valores: 3, 54, 68, 88, 100, 109-110, 138  
variáveis: 239  
fornecedor: 128-129, 160  
verificar: 136, 209  
versão: 53-54, 70, 129, 185, 187, 189  
exibir: 11, 16-17, 25-26, 55, 61  
visibilidade: 77, 120-121  
vnetname: 111  
-vpnctype: 79

## W

webappname: 198  
peso: 203, 247  
permitir: 112  
curinga: 253  
janelas: 18, 124

