



**SENAI**

A solid red vertical bar located to the left of the title.

# FIREWALL



# Introdução

**Firewall** é um **mecanismo de segurança** que controla o tráfego de pacotes em uma rede, permitindo ou negando essa troca de informações.

Existem vários tipos de firewall e várias camadas de aplicação e configuração de um firewall.

Aqui veremos o firewall presente nos sistemas operacionais (Windows e Linux)



# Introdução

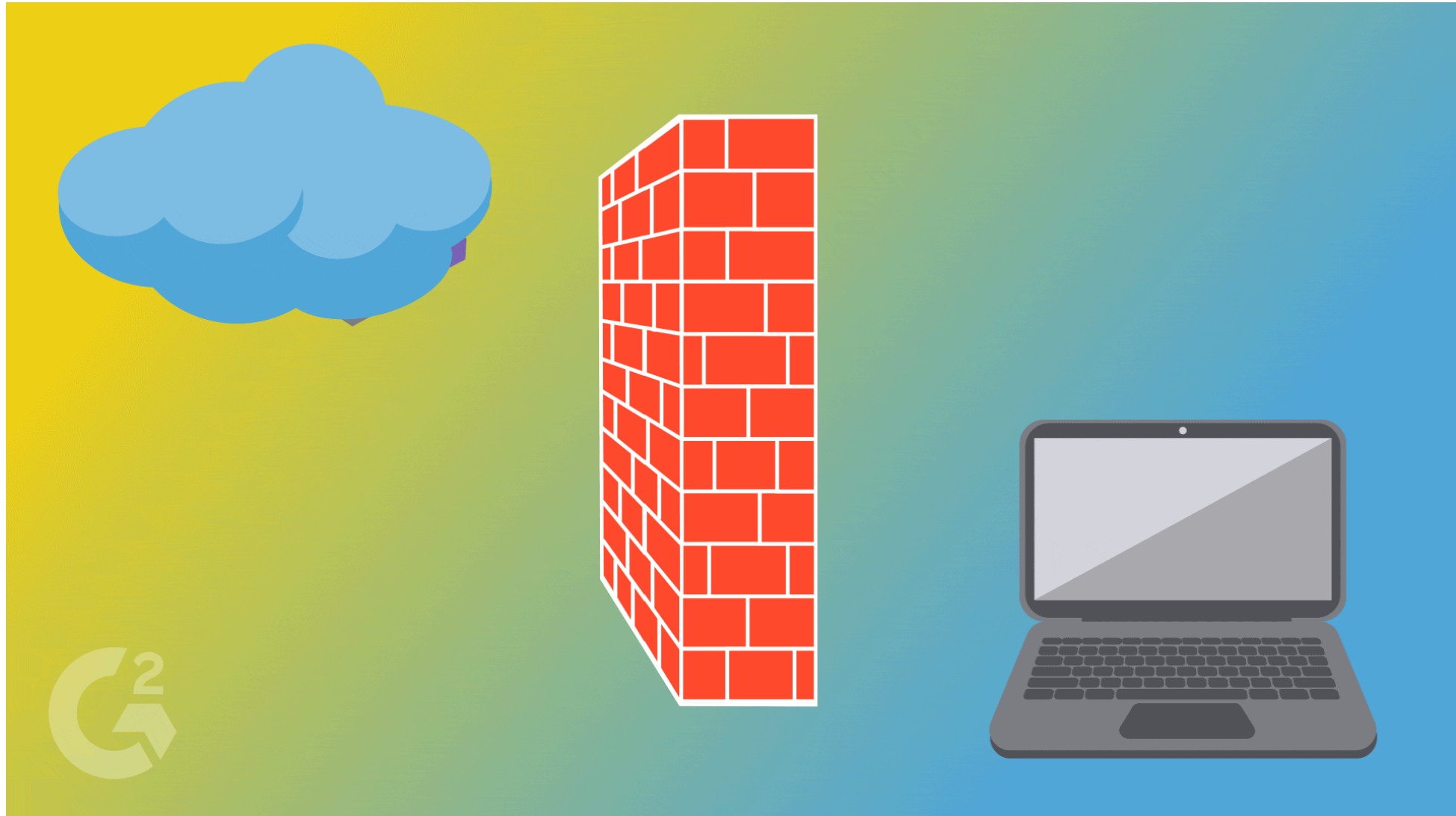
O **Firewall** presente no sistema operacional é um modelo básico que serve apenas para filtrar pacotes de rede.

Podemos configurar equipamentos na rede que podem ou não acessar uma pasta, um programa ou até uma porta.

As configurações que criamos no firewall são chamadas de regras de acesso.



# Introdução

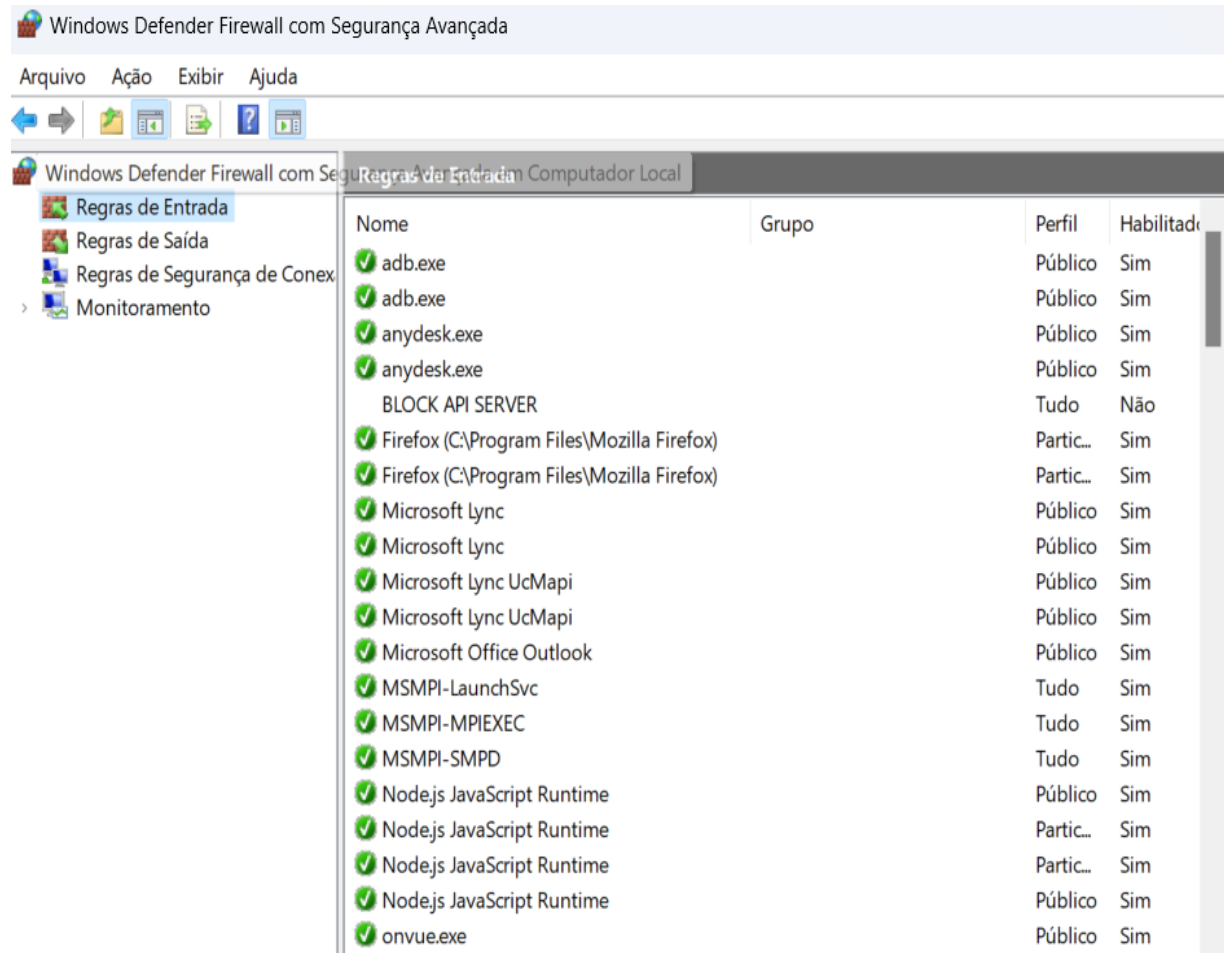




# Introdução



No Windows existem regras de entrada e saída já configuradas na instalação do sistema operacional.



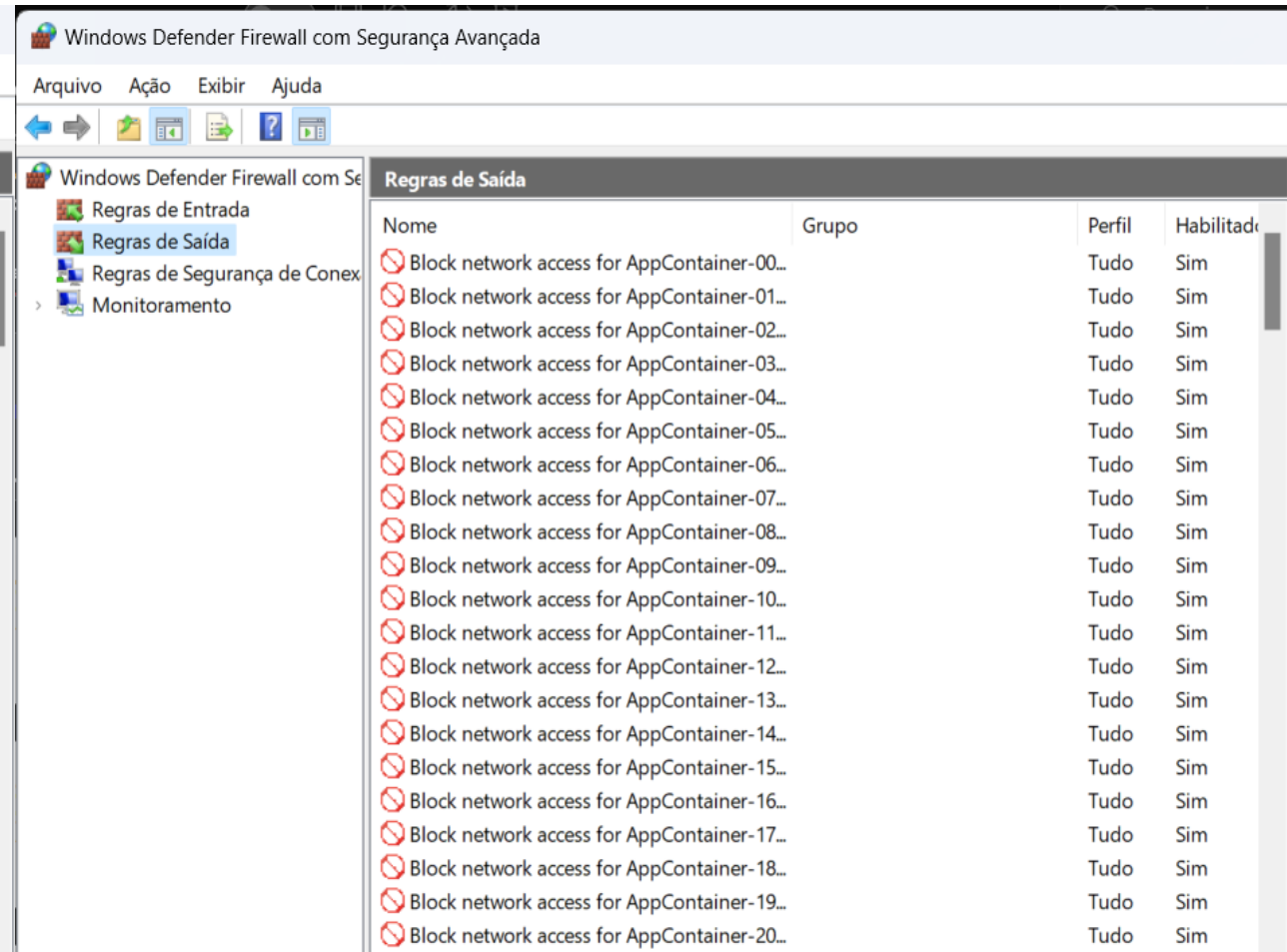
Windows Defender Firewall com Segurança Avançada

Arquivo Ação Exibir Ajuda

Windows Defender Firewall com Segurança Avançada - Computador Local

Regras de Entrada

Nome	Grupo	Perfil	Habilitado
adb.exe		Público	Sim
adb.exe		Público	Sim
anydesk.exe		Público	Sim
anydesk.exe		Público	Sim
BLOCK API SERVER		Tudo	Não
Firefox (C:\Program Files\Mozilla Firefox)		Partic...	Sim
Firefox (C:\Program Files\Mozilla Firefox)		Partic...	Sim
Microsoft Lync		Público	Sim
Microsoft Lync		Público	Sim
Microsoft Lync UcMapi		Público	Sim
Microsoft Lync UcMapi		Público	Sim
Microsoft Office Outlook		Público	Sim
MSMPI-LaunchSvc		Tudo	Sim
MSMPI-MPIEXEC		Tudo	Sim
MSMPI-SMPD		Tudo	Sim
Nodejs JavaScript Runtime		Público	Sim
Nodejs JavaScript Runtime		Partic...	Sim
Nodejs JavaScript Runtime		Partic...	Sim
Nodejs JavaScript Runtime		Público	Sim
onvue.exe		Público	Sim



Windows Defender Firewall com Segurança Avançada

Arquivo Ação Exibir Ajuda

Windows Defender Firewall com Segurança Avançada - Computador Local

Regras de Saída

Nome	Grupo	Perfil	Habilitado
Block network access for AppContainer-00...		Tudo	Sim
Block network access for AppContainer-01...		Tudo	Sim
Block network access for AppContainer-02...		Tudo	Sim
Block network access for AppContainer-03...		Tudo	Sim
Block network access for AppContainer-04...		Tudo	Sim
Block network access for AppContainer-05...		Tudo	Sim
Block network access for AppContainer-06...		Tudo	Sim
Block network access for AppContainer-07...		Tudo	Sim
Block network access for AppContainer-08...		Tudo	Sim
Block network access for AppContainer-09...		Tudo	Sim
Block network access for AppContainer-10...		Tudo	Sim
Block network access for AppContainer-11...		Tudo	Sim
Block network access for AppContainer-12...		Tudo	Sim
Block network access for AppContainer-13...		Tudo	Sim
Block network access for AppContainer-14...		Tudo	Sim
Block network access for AppContainer-15...		Tudo	Sim
Block network access for AppContainer-16...		Tudo	Sim
Block network access for AppContainer-17...		Tudo	Sim
Block network access for AppContainer-18...		Tudo	Sim
Block network access for AppContainer-19...		Tudo	Sim
Block network access for AppContainer-20...		Tudo	Sim

A solid red vertical bar is positioned to the left of the main title text.

# CRIANDO UMA REGRA (WINDOWS)



## Regras

Vez ou outra é necessário bloquear ou liberar alguma acesso via rede, seja para um aplicativo ou mesmo para que um serviço possa acessar nosso computador.

Iremos criar duas regras para entender a dinâmica do firewall, a primeira regra irá bloquear o acesso à internet.

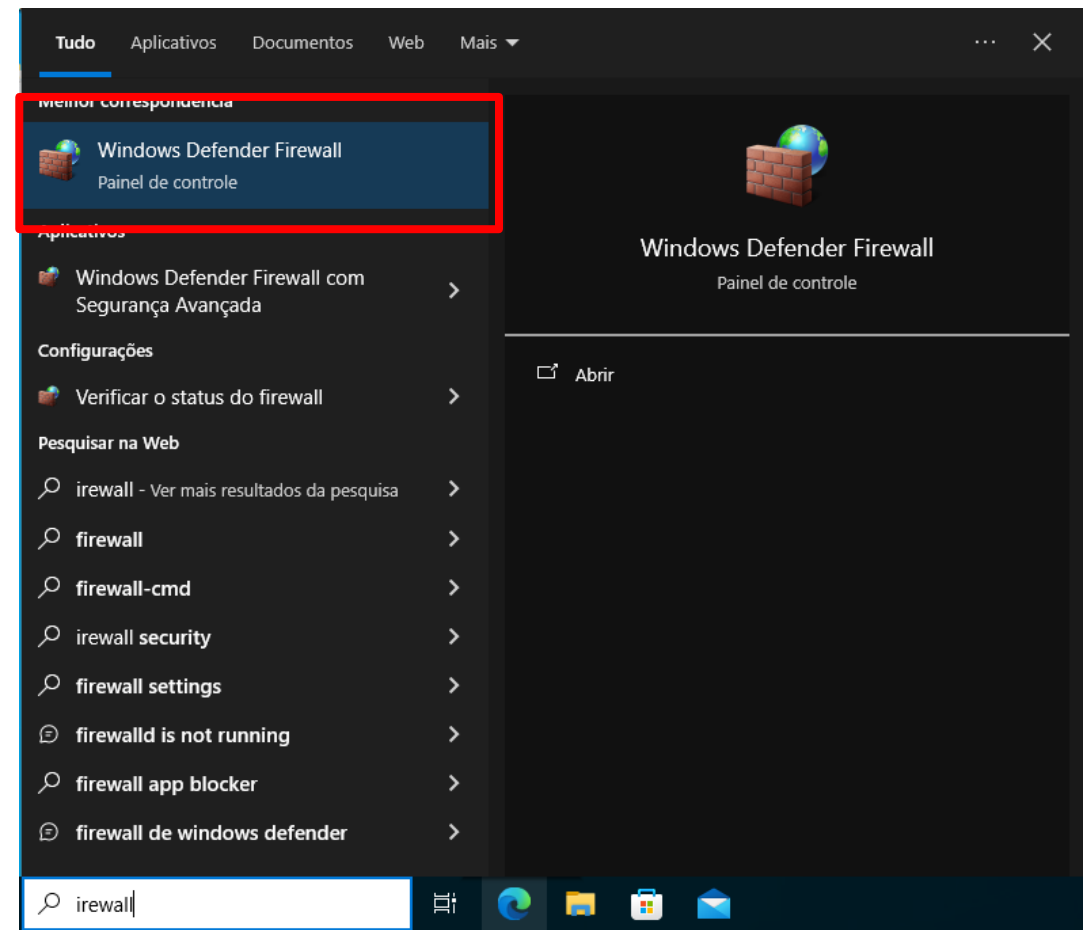
A segunda irá bloquear a comunicação ping ao nosso computador.





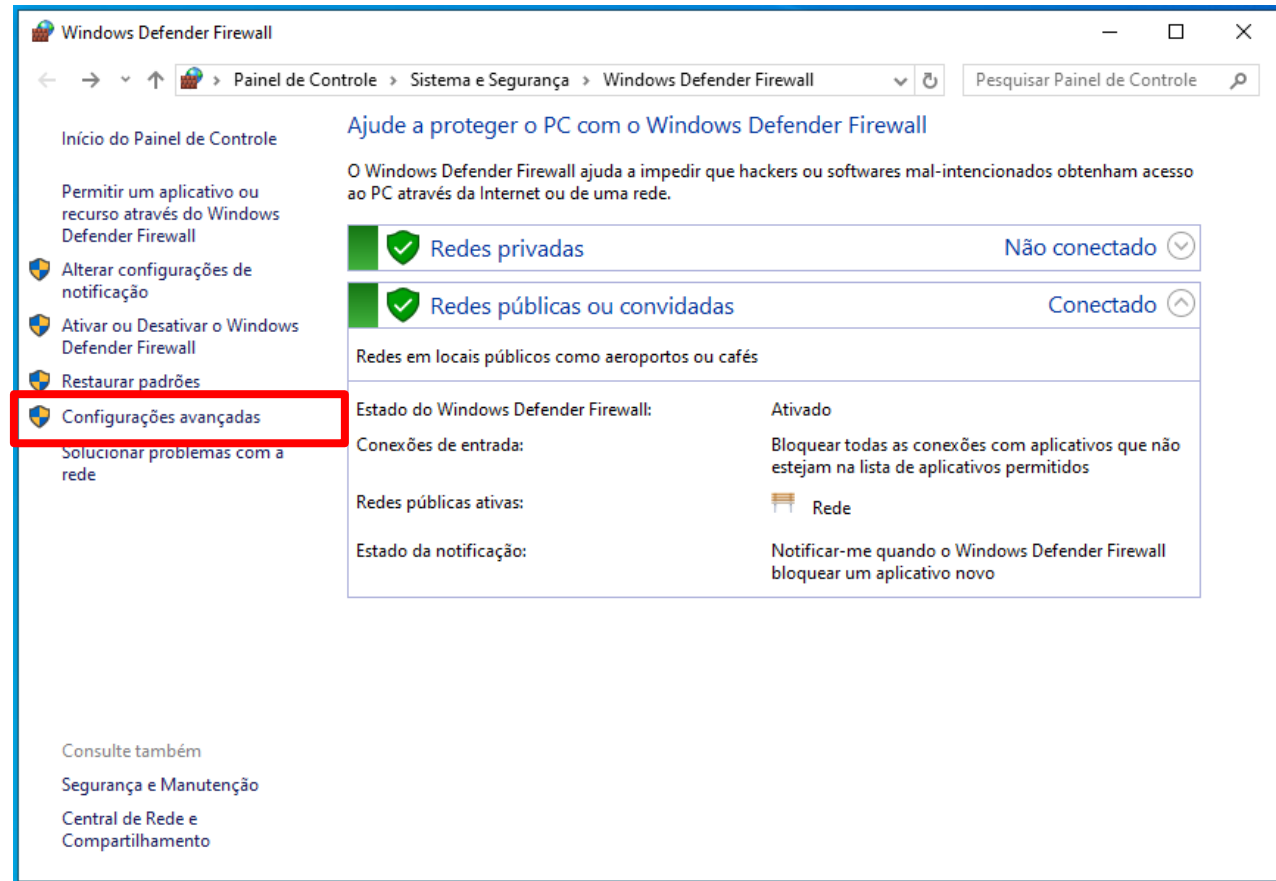
# Regras

Primeiro precisamos acessar o firewall do Windows, para digite firewall na barra de pesquisa e abra o seguinte aplicativo.



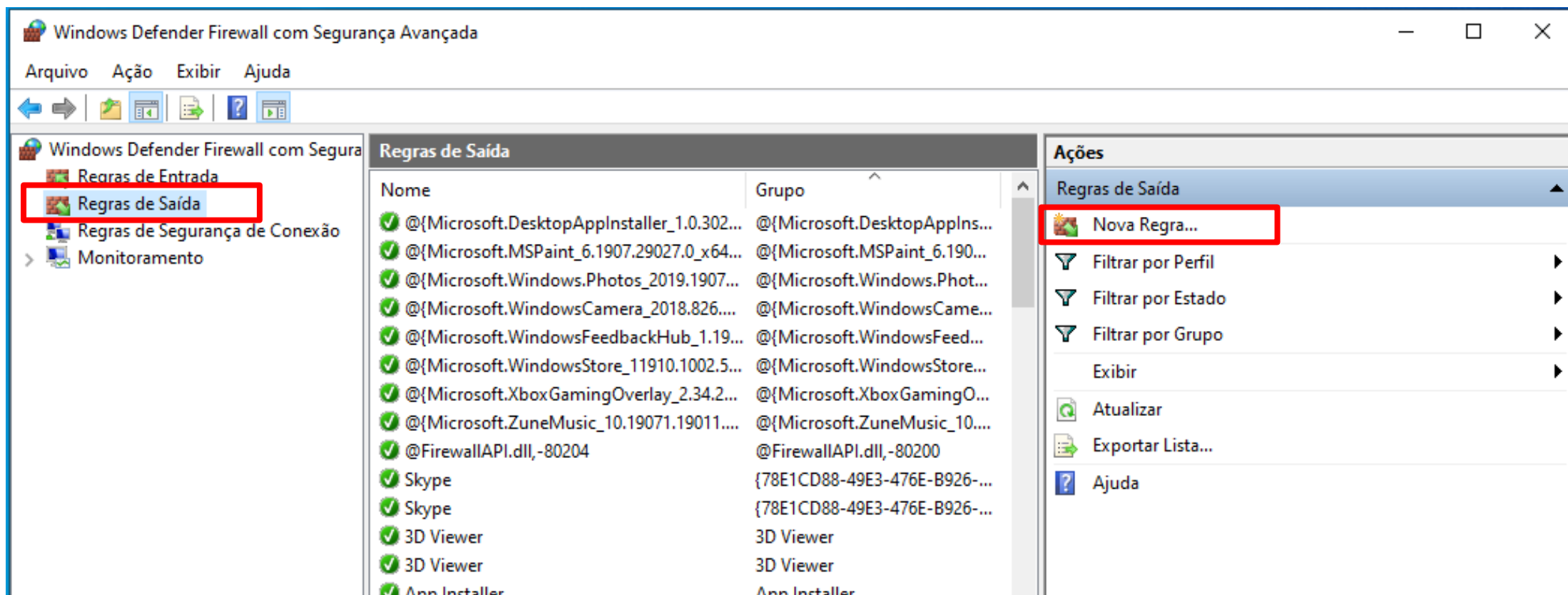
# Regras

Na janela aberta, clicamos na opção **Configurações avançadas**.



# Regras

Na janela das regras de firewall, vamos clicar em **Regras de Saída** no canto esquerdo depois em **Nova regra...** no canto direito.



# Regras

Na janela aberta, selecione a opção **Personalizado** depois **Avançar**

Assistente para Nova Regra de Saída

## Tipo de regra

Selecionar o tipo de regra de firewall a ser criada.

### Etapas:

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- Ação
- Perfil
- Nome

Que tipo de regra você deseja criar?

- ☐ **Programa**  
Regra que controla conexões para um programa.
- ☐ **Porta**  
Regra que controla conexões para uma porta TCP ou UDP.
- ☐ **Predefinida:**  
@FirewallAPI.dll,-80200  
Regra que controla conexões para uma experiência do Windows.

- ☒ **Personalizado**  
Regra personalizada.

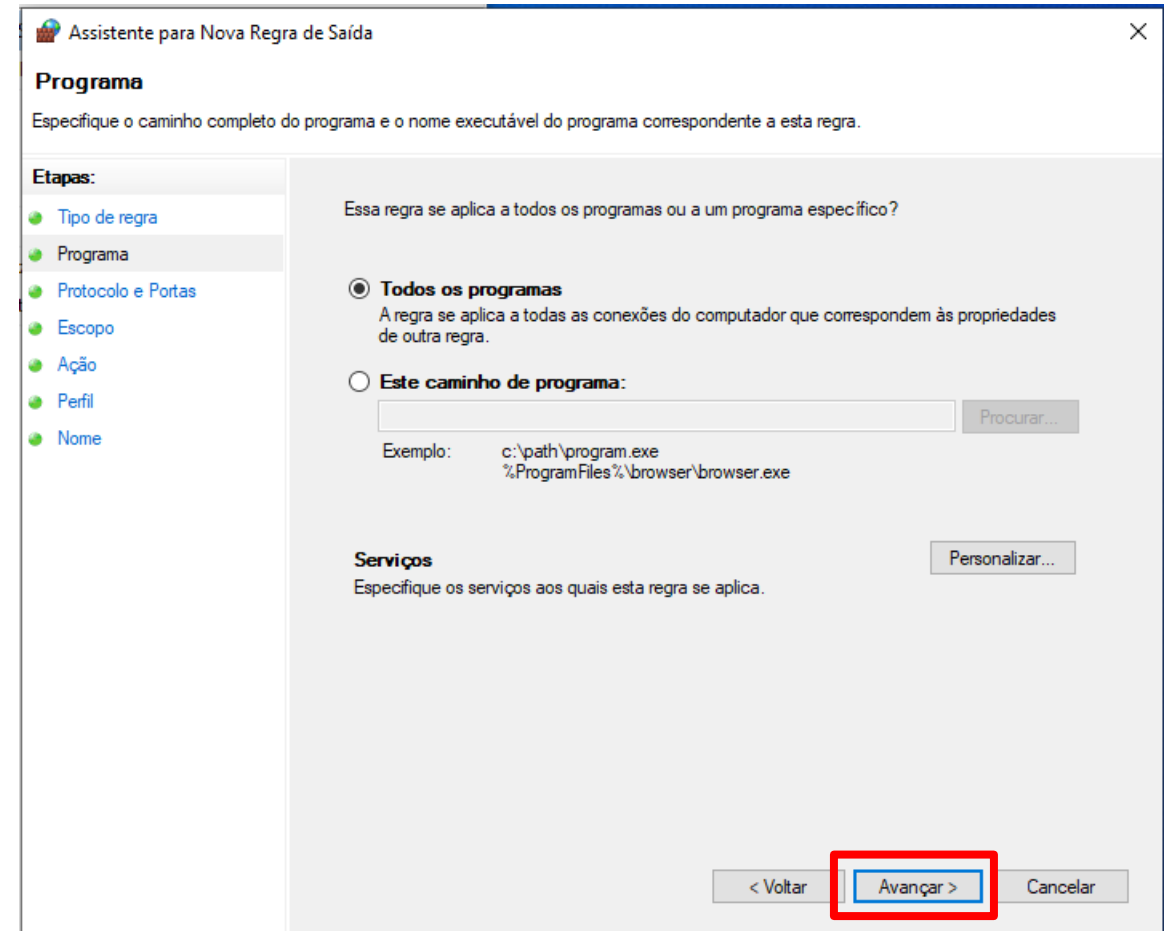
≤ Voltar

Avançar >

Cancelar

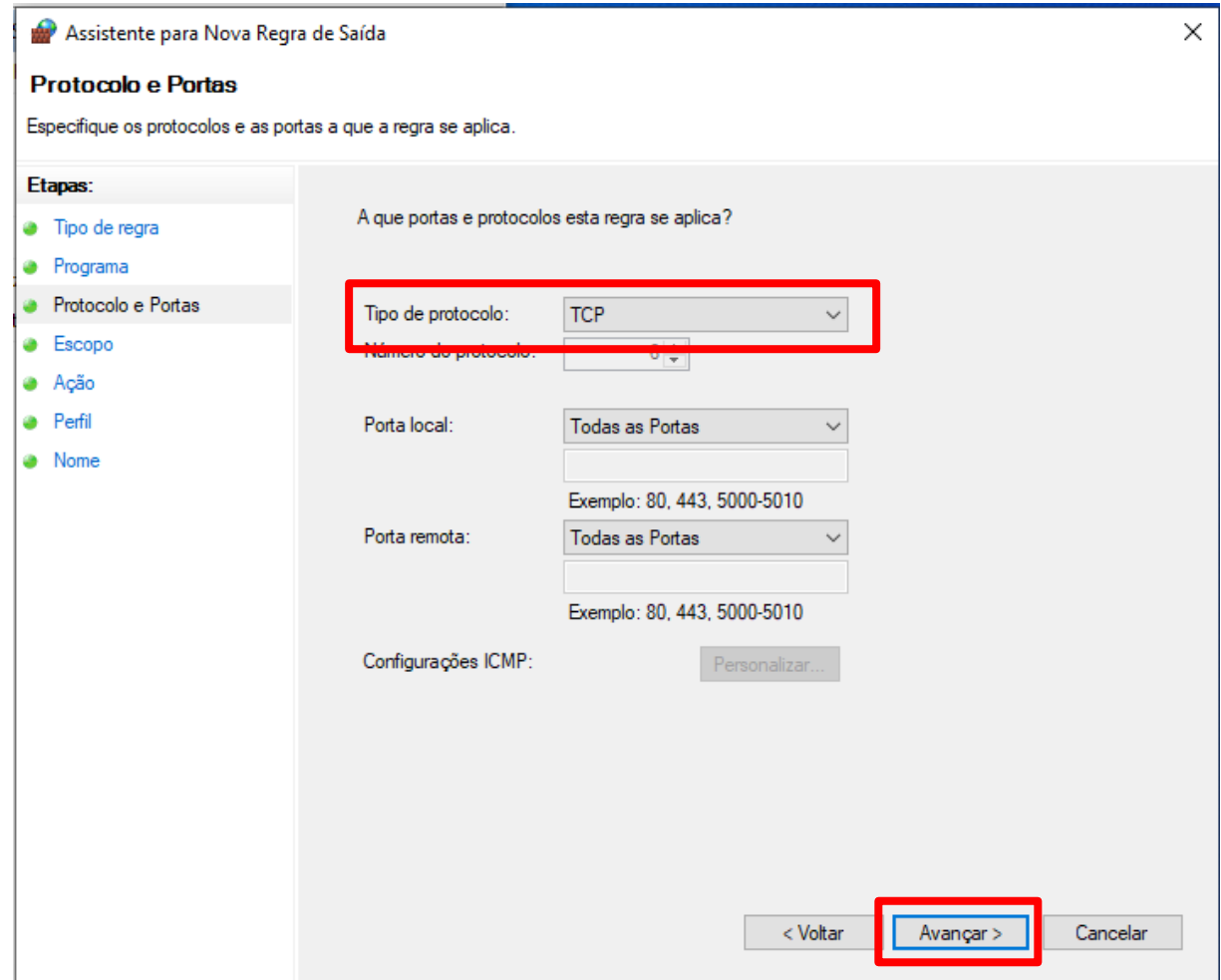
# Regras

Na próxima janela, temos a opção de bloquear a comunicação de um programa na rede, mas não vamos fazer isso, então só vamos clicar em Avançar



# Regras

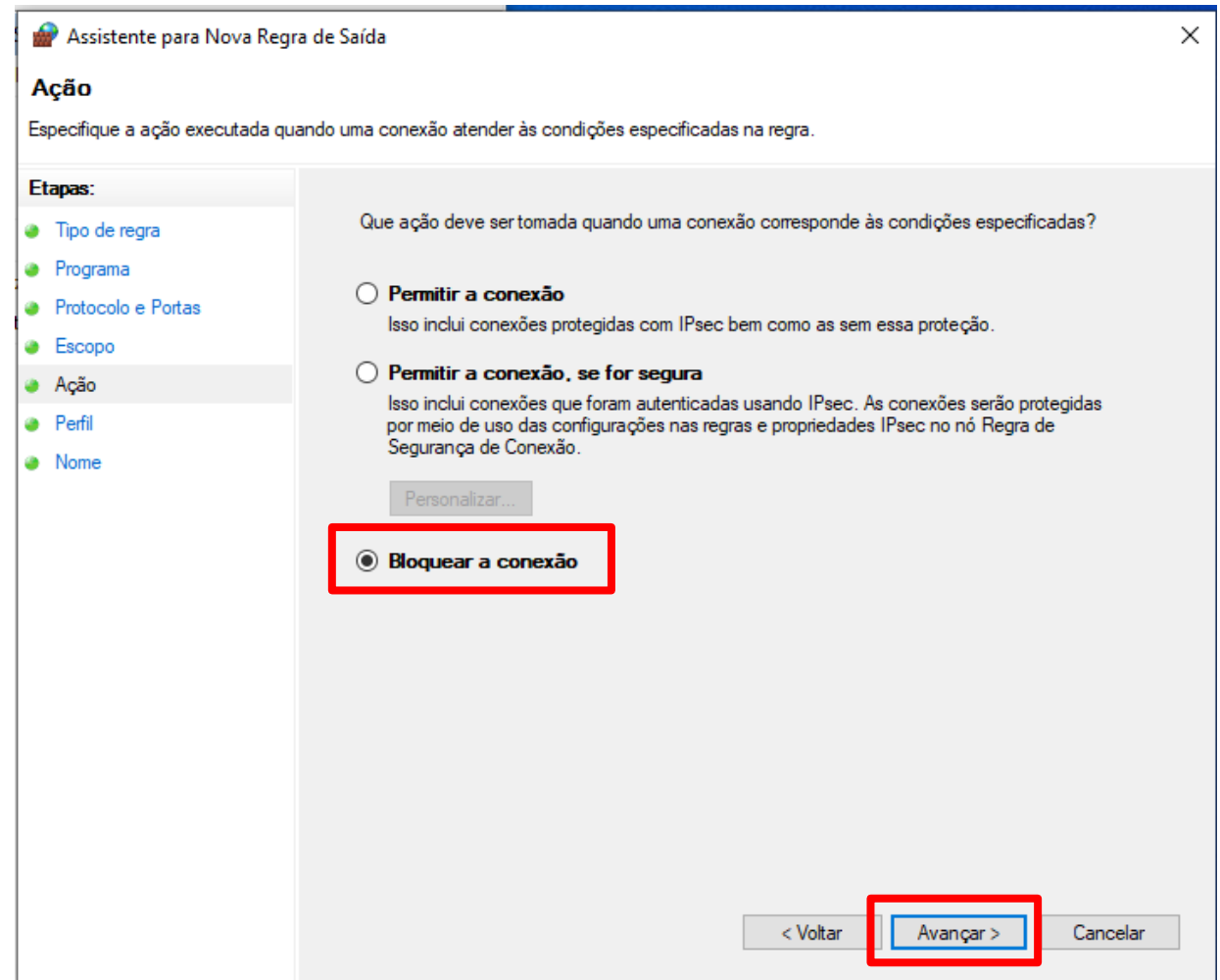
Na próxima janela **Protocolo e Portas**, vamos assinalar o **tipo de protocolo TCP** (um dos protocolos que faz comunicação com a internet)





# Regras

Avance até a janela **Ação**, nela selecione a opção **Bloquear a conexão** depois **Avançar**.



The screenshot shows the 'Assistente para Nova Regra de Saída' window. The 'Ação' step is selected in the 'Etapas' list on the left. The main area asks 'Que ação deve ser tomada quando uma conexão corresponde às condições especificadas?'. There are three radio button options: 'Permitir a conexão', 'Permitir a conexão, se for segura', and 'Bloquear a conexão'. The 'Bloquear a conexão' option is selected and highlighted with a red rectangle. Below the options is a 'Personalizar...' button. At the bottom right, there are three buttons: '< Voltar', 'Avançar >', and 'Cancelar'. The 'Avançar >' button is highlighted with a red rectangle.

Assistente para Nova Regra de Saída

**Ação**

Especifique a ação executada quando uma conexão atender às condições especificadas na regra.

**Etapas:**

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- **Ação**
- Perfil
- Nome

Que ação deve ser tomada quando uma conexão corresponde às condições especificadas?

☐ **Permitir a conexão**  
Isso inclui conexões protegidas com IPsec bem como as sem essa proteção.

☐ **Permitir a conexão, se for segura**  
Isso inclui conexões que foram autenticadas usando IPsec. As conexões serão protegidas por meio de uso das configurações nas regras e propriedades IPsec no nó Regra de Segurança de Conexão.

Personalizar...

☒ **Bloquear a conexão**

< Voltar Avançar > Cancelar

# Regras



Avance até a janela **Perfil**, deixe todas as opções selecionadas e clique **Avançar**.

Assistente para Nova Regra de Saída

**Perfil**

Especificar os perfis aos quais essa regra se aplica.

**Etapas:**

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- Ação
- Perfil**
- Nome

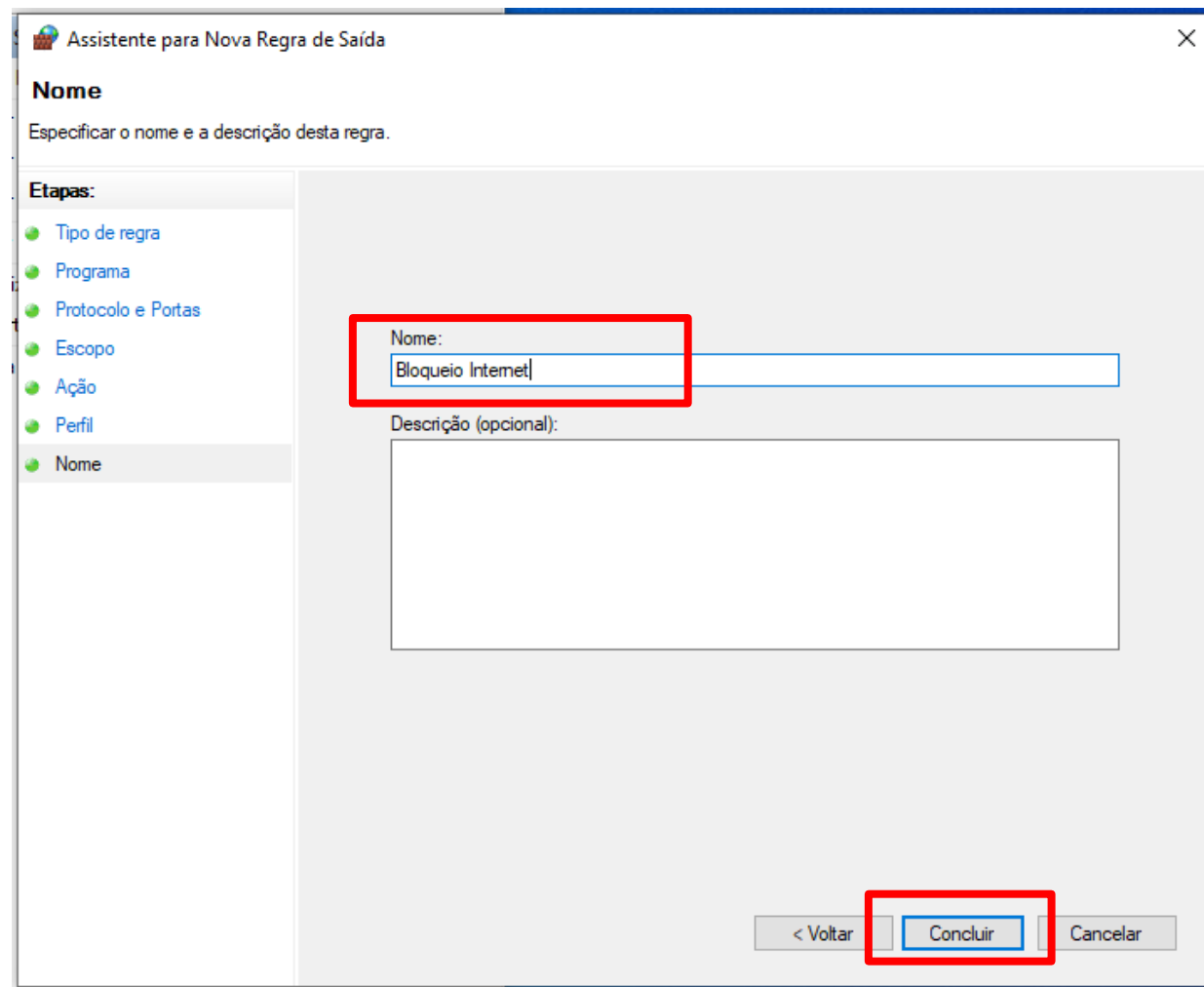
Quando esta regra se aplica?

- ☒ **Domínio**  
Aplica-se quando um computador está conectado ao seu domínio corporativo.
- ☒ **Particular**  
Aplica-se quando um computador está conectado a um local de rede privada, como residência ou local de trabalho.
- ☒ **Público**  
Aplica-se quando um computador está conectado a um local de rede pública.

< Voltar Avançar > Cancelar

# Regras

Por fim dê um nome para a regra e clique em **Concluir**.



Assistente para Nova Regra de Saída

**Nome**

Especificar o nome e a descrição desta regra.

**Etapas:**

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- Ação
- Perfil
- Nome**

Nome:

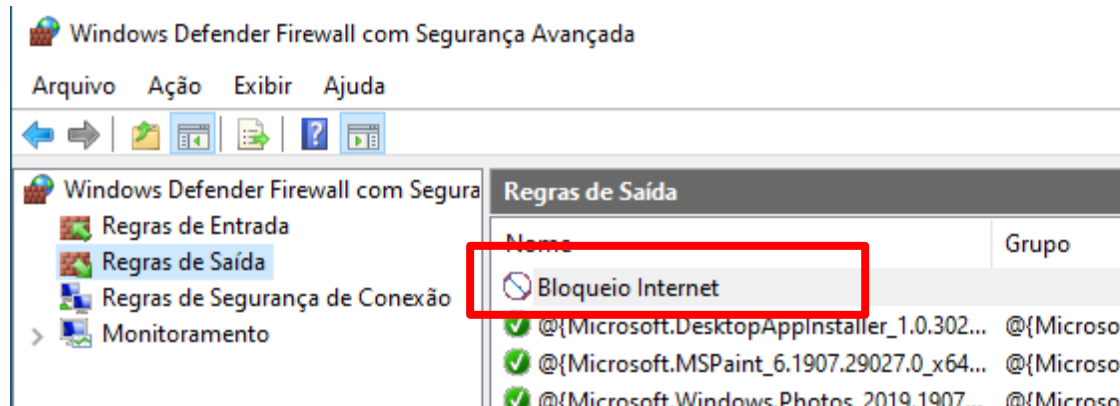
Bloqueio Internet

Descrição (opcional):

< Voltar Concluir Cancelar

# Regras

Regra criada, agora se tentarmos abrir alguma página web, seremos bloqueados pelo firewall.



## Hum... O acesso à Internet está bloqueado

Firewall ou software antivírus podem ter bloqueado a conexão.

### Tente:

- Verificando a conexão
- [Verificação de configurações de firewall e antivírus](#)
- [Executar o Diagnóstico de Rede do Windows](#)

ERR\_NETWORK\_ACCESS\_DENIED

▼ Detalhes



A solid red vertical bar located to the left of the main title text.

# CRIANDO UMA REGRA (LINUX)



## Regras

Por ser um sistema operacional de código aberto, existem vários programas para configurar um firewall no Linux.

O mais comum é o **UFW**, que normalmente já vem instalado nas distribuições.

Caso seja necessário instalar no Ubuntu basta digitar o comando:

```
sudo apt install ufw
```





## Regras



Para configurarmos uma regra de firewall no Linux, vamos usar a linha de comandos.

Antes de mais nada, vamos confirmar que o UFW está habilitado, para isso digite o comando

**sudo ufw enable**

A terminal window with a dark background. The title bar shows "renato@ubuntu: ~" and standard window controls. The terminal text is as follows:

```
renato@ubuntu:~$ sudo ufw enable
[sudo] password for renato:
Firewall is active and enabled on system startup
renato@ubuntu:~$
```

# Regras



Para bloquear a saída de pacotes é necessário digitar o comando abaixo

A terminal window with a dark background. The title bar shows "renato@ubuntu: ~". The prompt is "renato@ubuntu:~\$". The command entered is "sudo ufw default deny outgoing".

```
renato@ubuntu:~$ sudo ufw default deny outgoing
```

Após isso não deve ser mais possível acessar a internet

Hmm. We're having trouble finding that site.

We can't connect to the server at [www.google.com](http://www.google.com).

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

## Regras



Para desbloquear a saída de pacotes é necessário digitar o comando abaixo

A terminal window with a dark background. The title bar at the top reads "renato@ubuntu: ~". On the left is a window control icon (a square with a plus sign). On the right are icons for search (magnifying glass), menu (three horizontal lines), and window management (minus, maximize, and close buttons). The terminal text shows the prompt "renato@ubuntu:~\$" followed by the command "sudo ufw default allow outgoing" in a light green monospace font.

```
renato@ubuntu:~$ sudo ufw default allow outgoing
```

Após isso a navegação deve voltar a funcionar



## Regras

Para bloquear a comunicação de uma porta é usado o comando **ufw deny 8080/tcp**

Para liberar a comunicação de uma porta é usado o comando **ufw allow 8080/tcp**

Para bloquear a comunicação de um programa é usado o comando **ufw deny OpenSSH**

Para liberar a comunicação de um programa é usado o comando **ufw allow OpenSSH**



# Regras

Para exibir as regras criadas **ufw status**

```

renato@ubuntu: ~$ sudo ufw status
Status: active

To Action From
--
80 DENY Anywhere
8080/tcp ALLOW Anywhere
22/tcp ALLOW Anywhere
3000/tcp DENY Anywhere
OpenSSH DENY Anywhere
80 (v6) DENY Anywhere (v6)
8080/tcp (v6) ALLOW Anywhere (v6)
22/tcp (v6) ALLOW Anywhere (v6)
3000/tcp (v6) DENY Anywhere (v6)
OpenSSH (v6) DENY Anywhere (v6)

```

# | Dúvidas

