

Adicionar Portas e Firewall

Quando realizado a instalação dos sistemas em um servidor, para que outras máquinas possam ter acesso aos módulos, é necessário fazer a liberação da porta 3050 (firebird) no firewall do Windows.

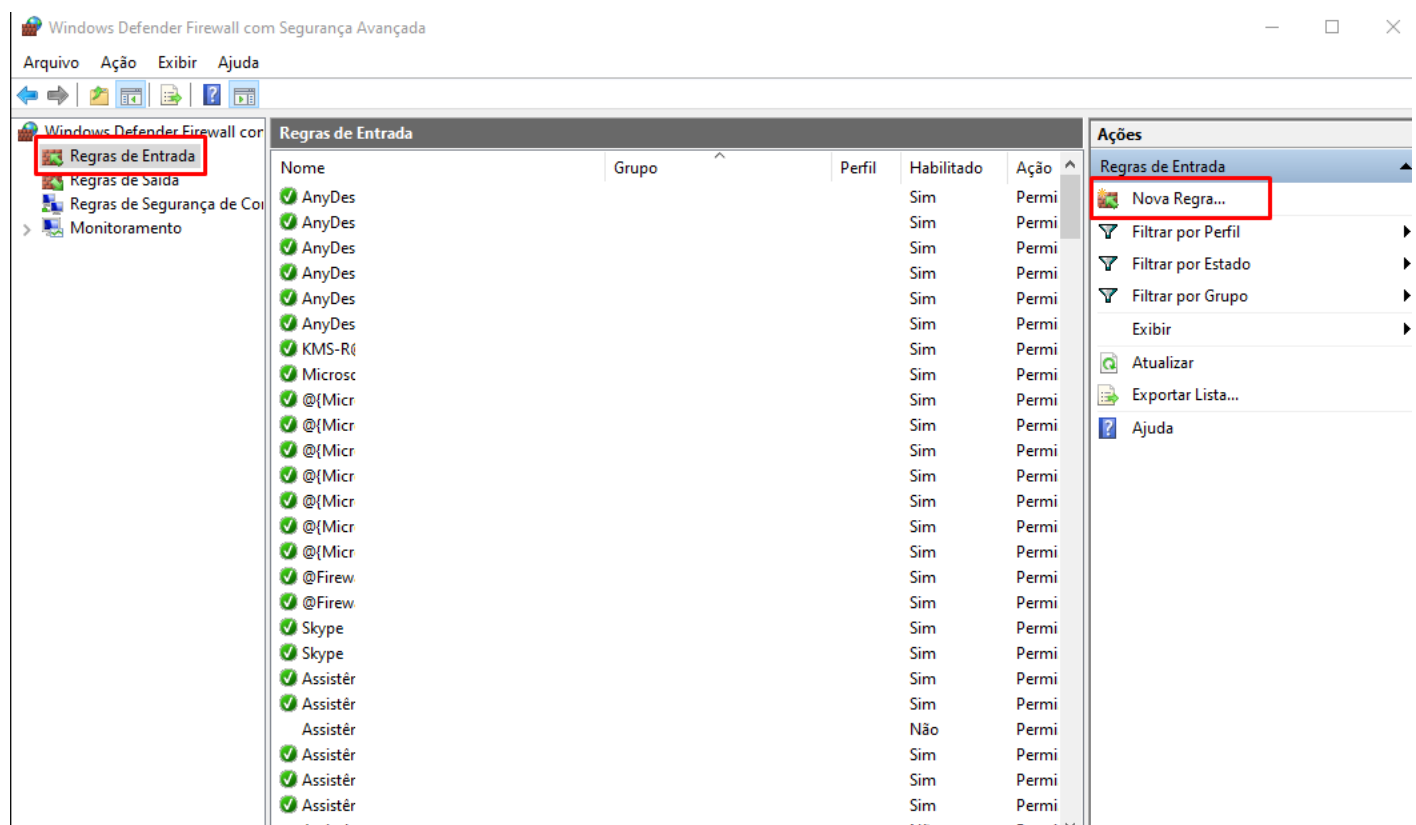
O Firewall é um aplicativo que verifica e filtra as informações que entram e saem de um computador e as permitem ou bloqueiam dependendo de como está configurado.

Ele é responsável por impedir que programas mal intencionados se conectem ao computador ou que envie informações indesejadas a internet ou outros computadores.

Observação: Nunca se deve desativar o firewall de um cliente e deixá-lo desativado, pois o computador fica vulnerável a ataques.

Para desbloquear a porta do Firebird no Firewall do Windows acesse: **Painel de Controle > Windows Defender Firewall > Configurações Avançadas:**

1) Selecione “Regras de Entrada” e “Nova Regra”:



2) Selecione a opção porta:

Tipo de regra

Selecionar o tipo de regra de firewall a ser criada.

Etapas:

- Tipo de regra
- Protocolo e Portas
- 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

3) Selecione a opção TCP e porta 3050:

Protocolo e Portas

Especifique os protocolos e as portas a que a regra se aplica.

Etapas:

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

Essa regra se aplica a TCP ou a UDP?

☒ TCP

☐ UDP

Essa regra se aplica a todas as portas locais ou a portas locais específicas?

☐ Todas as portas locais

☒ Portas locais específicas:

3050

Exemplo: 80, 443, 5000-5010

< Voltar

Avançar >

Cancelar

4) Selecione “Permitir a Conexão” e na tela Quando a regra de aplica, deixa as opções marcadas e avançar:

Ação

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

Etapas:

- Tipo de regra
- Protocolo e Portas
- 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

5) Defina a regra que será aplicada

Perfil

Especificar os perfis aos quais essa regra se aplica.

Etapas:

- Tipo de regra
- Protocolo e Portas
- 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

6) Nomeie a regra que você acabou de criar e clique em concluir:

Nome

Especificar o nome e a descrição desta regra.

Etapas:

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

Nome:

Firebird

Descrição (opcional):

Servidor Firebird dos Sistemas da Supersoft

< Voltar

Concluir

Cancelar

Revision #3

Created 5 August 2024 15:07:05 by ProjetosD

Updated 7 August 2024 20:34:16 by ProjetosD