INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Administração de Sistemas Proprietários
Aula 18: Introdução ao Windows Defender Firewall e Antivírus.

Olá, meu queridos!! Tudo bem??? Na aula de hoje iremos conhecer o Firewall e Antivírus do Windows. Vamos lá!!! Preparados???

Firewall

Um firewall é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Em outras palavras, realiza a filtragem de pacotes e funções. O tráfego pode ser bloqueado ou permitido com base nas características de cada pacote de rede, por exemplo, seu endereço IP de origem ou de destino, seus números de porta de origem ou de destino, o programa no dispositivo que recebe o pacote de entrada e assim por diante.

A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

Entretanto, no Windows, normalmente, quando você instala um programa que necessite aceitar o tráfego de rede de entrada não solicitado, o programa de instalação cria ou habilita as regras apropriadas no firewall para você. Por exemplo, quando você instala uma função de servidor, as regras de firewall adequadas são criadas e habilitadas automaticamente.

Inicialmente, iremos conhecer como ativar e desativar o Firewall. Na sequência iremos mostar como ativar uma determinada regra e criar novas regras.

Ativar/Desativar o Firewall

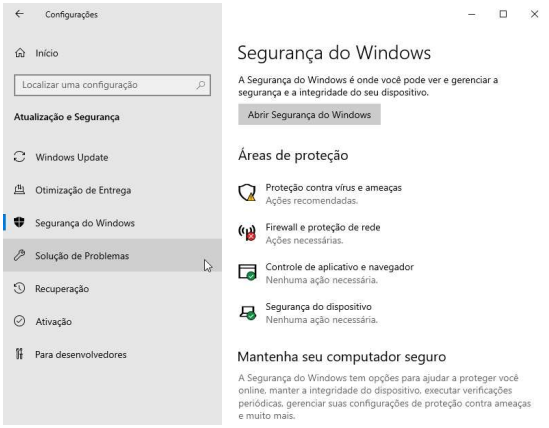
O Firewall do Windows está ativado por padrão. Isso permite todo o tráfego de saída e entrada seja submetido a regras específicas.

É importante ter o Windows Defender Firewall ativado, mesmo se você já tiver outro firewall ativado. Ele ajuda a proteger suas informações contra acesso não autorizado.

Para ativar o Windows Defender Firewall siga os passos:

1. Selecione o botão “Iniciar”.

2. Selecione “Configurações”, “Atualização e Segurança”, “Segurança do Windows” e “Firewall e Proteção de Rede”.



3. Selecione um perfil de rede.

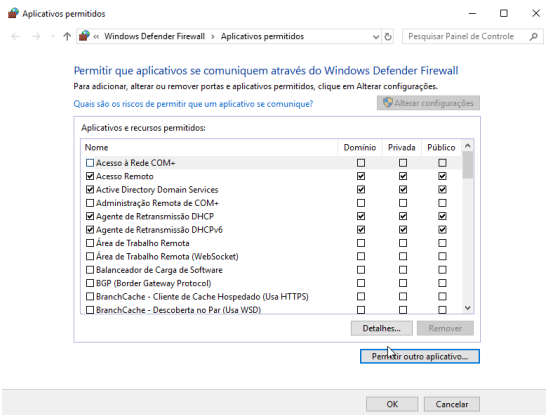
4. Em Windows Defender Firewall, alterne a configuração para Ativado.

Na figura acima podemos visualizar o status do firewall para os perfis de domínio, privado e público. Esses perfis são usados dependendo da sua conexão de rede. Por exemplo, se você ingressou em um domínio do Active Directory, as regras do domínio serão usadas, enquanto se você estiver conectado a uma rede sem fio pública, as configurações no perfil público serão usadas.

Permitir um Aplicativo

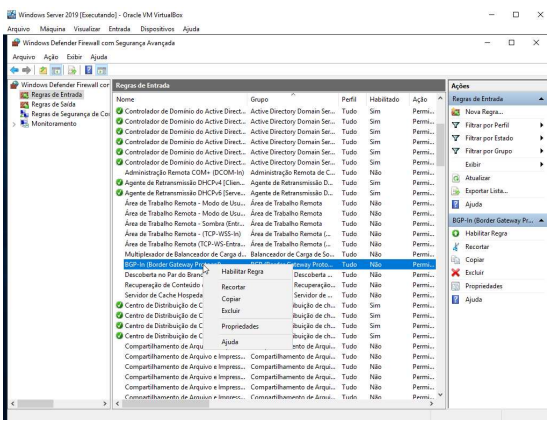
É possível dar permissão a um aplicativo pelo firewall através dos seguintes passos:

1. Selecione o botão “Iniciar”.
2. Selecione “Configurações”, “Atualização e Segurança”, “Segurança do Windows” e “Firewall”.
3. Selecione “Permitir um aplicativo pelo firewall”.
4. Selecione o aplicativo que você deseja usar com permissão do firewall.
5. Clique em “OK”.



Configurações Avançadas

Para visualizarmos as configurações avançadas podemos clicando no botão “Configurações Avançadas” na tela do Firewall do Windows. Também podemos executar “wf.msc” no PowerShell ou no Prompt de Comando para abrir diretamente a interface de segurança avançada.



Nesta janela, podemos ver uma visão geral dos perfis de domínio, privado e público, que, por padrão, devem estar todos habilitados, bloqueando parte do tráfego de entrada. Todas as saídas são permitidas por padrão.

No menu à esquerda, podemos selecionar regras de entrada ou saída. Podemos visualizar as regras que existem e que estão ativadas no momento.

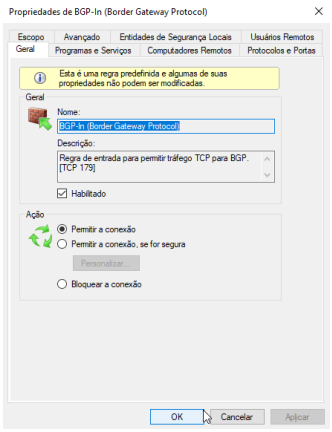
Ativando Regras

O Windows vem com várias regras de entrada e saída pré-definidas. Você poderá encontra-las selelcionando “Regras de Entrada” ou “Regras de Saída” na janela do Windows Defender Firewall com Segurança Avançada.

Para ativar uma determinada regra siga os passos:

1. Localize a regra que deseja ativar, selecione Regras de Entrada ou Regras de Saída e procure a regra desejada;
2. Clicando com o botão direito do mouse e selecione “Habilitar Regra”.

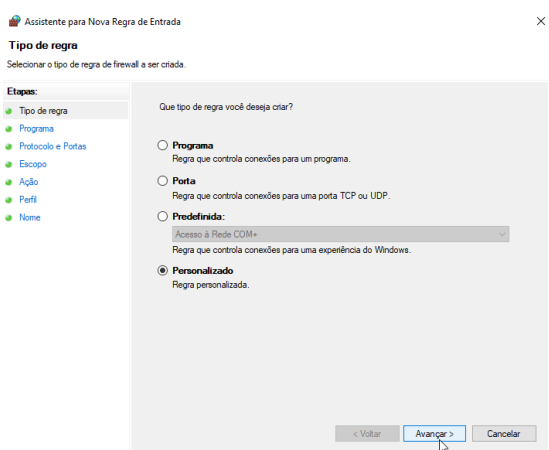
Podemos visualizar as propriedades da regra clicando com o botão direito do mouse e selecionando “Propriedades”. Isso permitirá que você veja o que a regra, está realmente fazendo, incluindo as portas que estão sendo permitidas pelo firewall para programas específicos.



Criando Regras

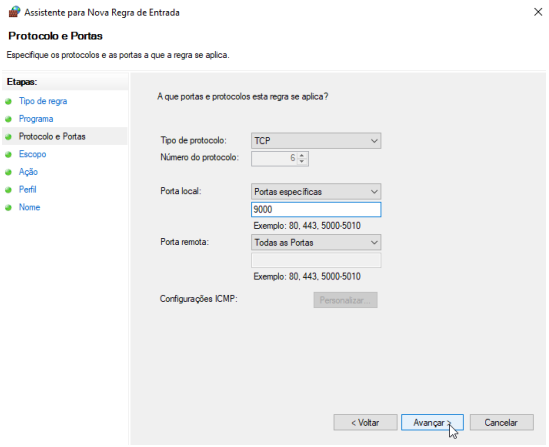
Caso você deseje uma regra que não é pré-definida pelo Windows, você poderá cria-la. Para criar uma nova regra, por exemplo, de entrada, faça:

1. Selecione “Regras de Entrada” no menu à esquerda e selecione “Nova Regra” no painel de ações à direita.
2. Isso abrirá o novo assistente de regra de entrada. A partir daqui, podemos selecionar se queremos criar uma regra para um programa específico, para uma porta específica ou com base em uma regra existente. Selecione “Personalizado”.

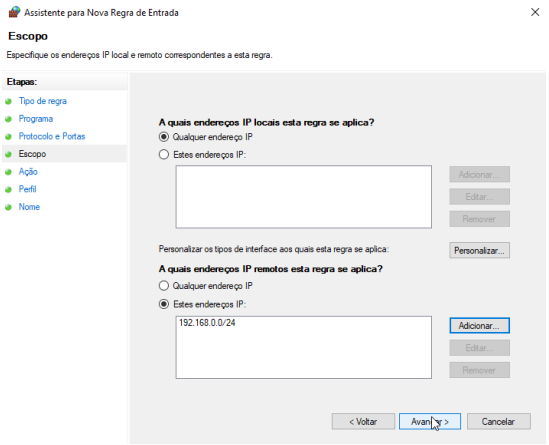


3. Na próxima tela, podemos selecionar se a regra será para todos os programas ou para um programa específico. Selecione “Todos os programas”.

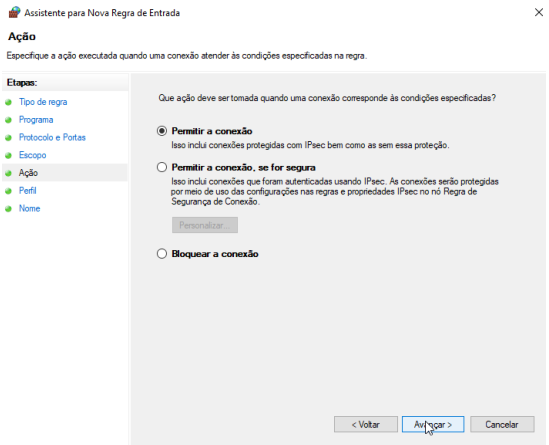
4. Em seguida, podemos selecionar a porta e o protocolo aos quais a regra deve ser aplicada. Por exemplo, iremos especificar que a porta TCP local 9000 deve ser permitida através do firewall.



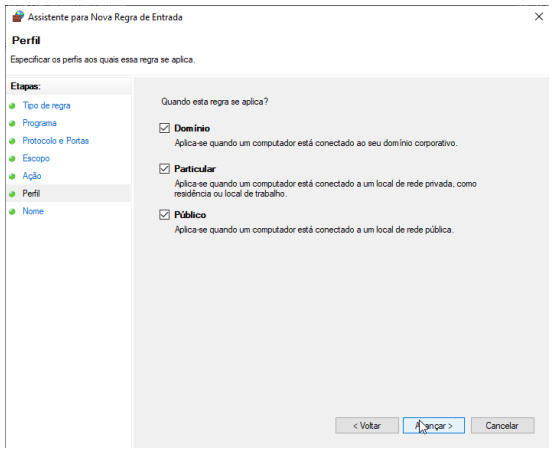
5. Agora podemos selecionar um endereço IP ou um intervalo de endereços que irão entrar na nova regra do firewall. Nesse caso, estou permitindo que o intervalo de endereços remotos 192.168.0.0/24 entre através do firewall, portanto, somente esse intervalo de IP poderá se conectar ao servidor na porta TCP 9000.



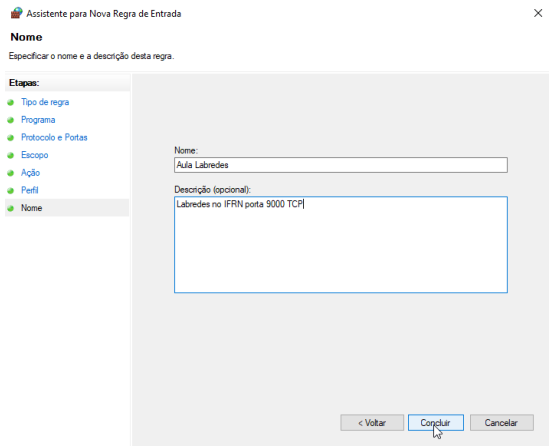
6. Na sequência, iremos especificar se queremos permitir ou negar a regra que estamos criando. No exemplo, iremos “Permitir a conexão”. Clique em “Avançar”.



7. Podemos selecionar a quais perfis de firewall nossa nova regra será aplicada. Por padrão, todos os perfis são selecionados, no entanto, você pode alterar isso de acordo com seus requisitos. Pode deixar todos os perfis e clicar em “Avançar”.



8. Finalmente, devemos especificar um nome e uma descrição para identificar a nossa regra. Depois, clique em “Concluir”.



Nossa regra está criada, habilitada e funcionando.

Atividade

Iremos testar configurações no Firewall do Windows para permitir conexões TCP em determinada porta (85). Para isso, será utilizado um script em PowerShell, que simula um serviço de rede escutando em uma porta específica.

01. Crie um script em PowerShell capaz de abrir uma porta TCP específica (porta 8080) e permanecer aguardando conexões de clientes da rede. O script deverá exibir uma mensagem sempre que uma conexão for estabelecida, informando o endereço IP do cliente que realizou a conexão.

```
$port = 85
$listener = [System.Net.Sockets.TcpListener]
 new($port)

$listener.Start()
Write-Host "Escutando na porta $port..."

$client = $listener.AcceptTcpClient()

# Obtém informações do cliente
$endpoint = $client.Client.RemoteEndPoint
$ipCliente = $endpoint.Address
Write-Host "Cliente conectado! com
 IP $ipCliente"

$client.Close()
```

02. Execute o script para testar a conectividade a partir de outro computador da rede local, utilizando ferramentas como o comando Test-NetConnection. Nesse primeiro momento, nenhuma regra de liberação deverá ser criada no Firewall do Windows, permitindo observar o comportamento padrão do sistema diante de conexões de entrada.

```
PS C:\Users\ifrn> Test-NetConnection 192.168.0.1 -Port 85
AVISO: TCP connect to (192.168.0.1 : 85) failed


ComputerName            : 192.168.0.1
RemoteAddress           : 192.168.0.1
RemotePort              : 85
InterfaceAlias          : Ethernet
SourceAddress           : 192.168.0.2
PingSucceeded           : True
PingReplyDetails (RTT) : 2 ms
TcpTestSucceeded        : False
```

03. Em seguida, configure o Firewall do Windows, criando uma regra de entrada que permita conexões TCP na porta utilizada pelo script. Com a nova regra ativa, os testes de conexão deverão ser realizados novamente, observando-se as diferenças de comportamento em relação ao cenário anterior.

```
PS C:\Users\ifrn> Test-NetConnection 192.168.0.1 -Port 85


ComputerName     : 192.168.0.1
RemoteAddress    : 192.168.0.1
RemotePort       : 85
InterfaceAlias   : Ethernet
SourceAddress    : 192.168.0.2
TcpTestSucceeded : True
```

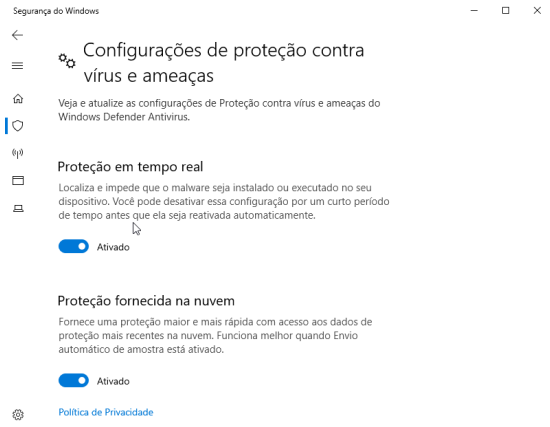
Windows Defender Antivírus

O Windows Defender Antivírus é uma proteção contra malware. Por padrão, ele está instalado e funciona no Windows Server 2022. Ele deve ser atualizado regularmente para conhecer novas definições antimalware por meio de Windows Update.

A Proteção contra vírus e ameaças na Segurança do Windows ajuda a verificar se há ameaças em seu dispositivo. Você também pode executar diferentes tipos de verificação, ver os resultados das verificações de vírus e ameaças anteriores e obter a proteção mais recente oferecida pelo Windows Defender Antivírus.

Para ativar o Windows Defender Antivírus siga os passos:

1. Selecione o botão “Iniciar”.
2. Selecione “Configurações”, “Atualização e Segurança”, “Segurança do Windows”, “Proteção contra vírus e ameaças” e “Gerenciar Configurações”.
3. Em “Proteção em tempo real”, alterne a configuração para “Ativado”.



Se deseja parar a execução da proteção em tempo real por um tempo? Você pode usar a configuração Proteção em tempo real para desativá-la temporariamente. No entanto, a proteção em tempo real será ativada automaticamente após um período para continuar protegendo o dispositivo. Enquanto a proteção em tempo real estiver desativada, os arquivos que você abrir ou baixar não serão verificados em busca de ameaças.

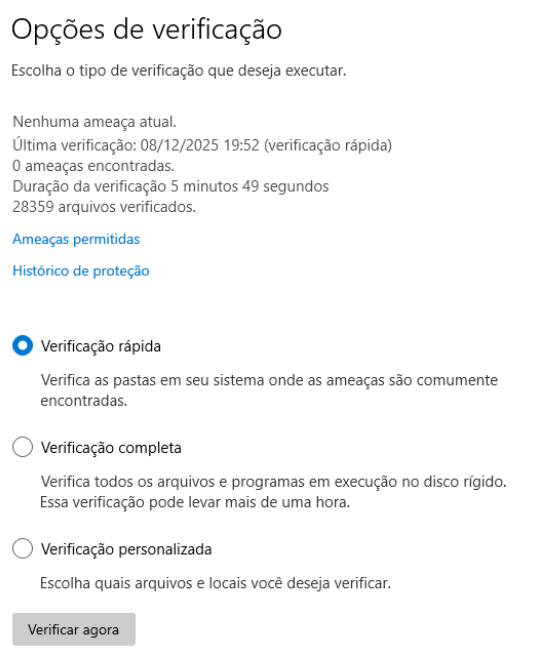
Na parte “Obter acesso à proteção entregue na nuvem” fornece ao seu dispositivo acesso às definições de ameaças mais recentes e à detecção de comportamento suspeito na nuvem. Deixe ele ativada.

Verificar Ameaças

A verificação rápida na proteção contra vírus e ameaça é usada para verificar imediatamente seu dispositivo em busca de qualquer ameaça recente. Essa opção será útil quando você não quiser gastar tempo executando uma verificação completa em todos os arquivos e pastas. Caso precise executar um dos outros tipos de verificações, você receberá uma notificação quando a verificação estiver concluída.

1. Selecione o botão “Iniciar”, “Configurações”, “Atualização e Segurança”, “Segurança do Windows”, “Proteção contra vírus e ameaças” e “Opções de Verificação”.

2. Selecione, “Verificação Rápida” para analisar as pastas onde as ameaças são normalmente localizadas, em “Verficação Completa” para verificar todos os arquivos e programas e em “Verficação Personalizada” para escolher os arquivos.



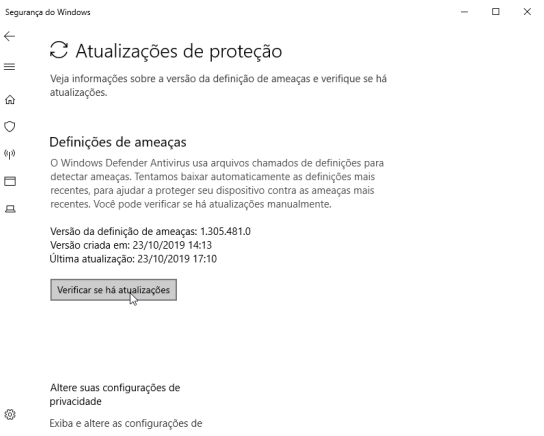
3. Depois de selecionar o toipo, clique em “Verificar agora”.

Atualizar a Proteção

Você poderá examinar a versão de atualização de segurança e baixe as atualizações mais recentes no aplicativo segurança do Windows. Para isso:

1. Selecione o botão “Iniciar”, “Configurações”, “Atualização e Segurança”, “Segurança do Windows”, “Proteção contra vírus e ameaças” e “Verificar se há atualizações”.

2. Na tela que irá surgir, clique em “Verificar se há atualizações”. A versão instalada atualmente é exibida juntamente com algumas informações sobre quando ela foi baixada.



Atividade

1. Verifique se o Firewall está ativado, caso contrário ative para todos os perfis de rede.

2. Verfique se o aplicativo da Área de Trabalho Remota está habilitada no firewall, caso negativo, habilite-a;

3. Crie as seguintes regras no Firewall que bloquei o acesso a Internet.

4. Verifique se o Windows Defender Antivírus está instalado e em operação. Caso negativo, instale e deixe rodando.

5. Faça a atualização de proteção do antivírus

6. Faça uma verificação de ameaças.