

06

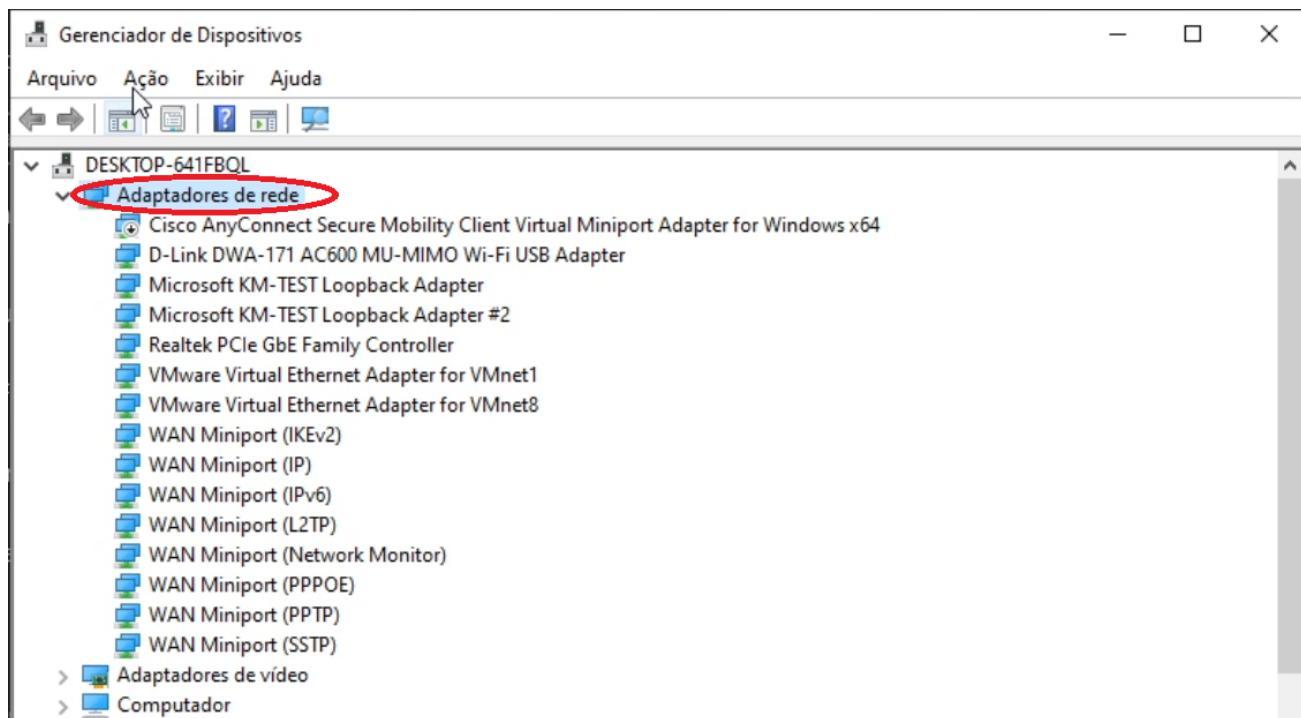
## Preparando o ambiente

Para acessar a interface gráfica dos firewalls **ASDM**, vamos precisar preparar nosso computador para se comunicar localmente com o GNS3.

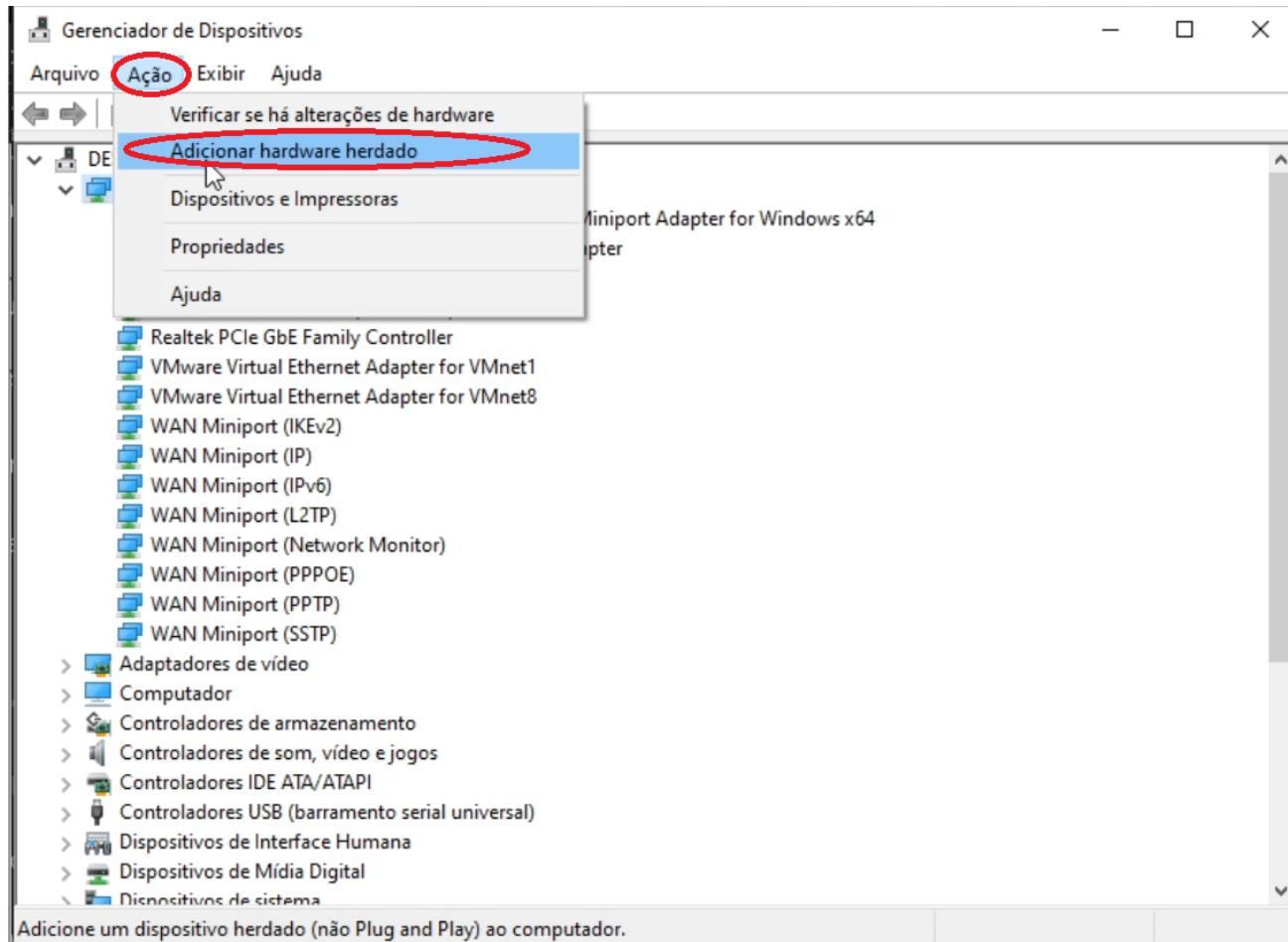
Essa comunicação será feita por meio de interfaces do tipo “loopback”.

O primeiro passo é ir em **Iniciar, painel de controle** e localizar o **gerenciador de dispositivos**.

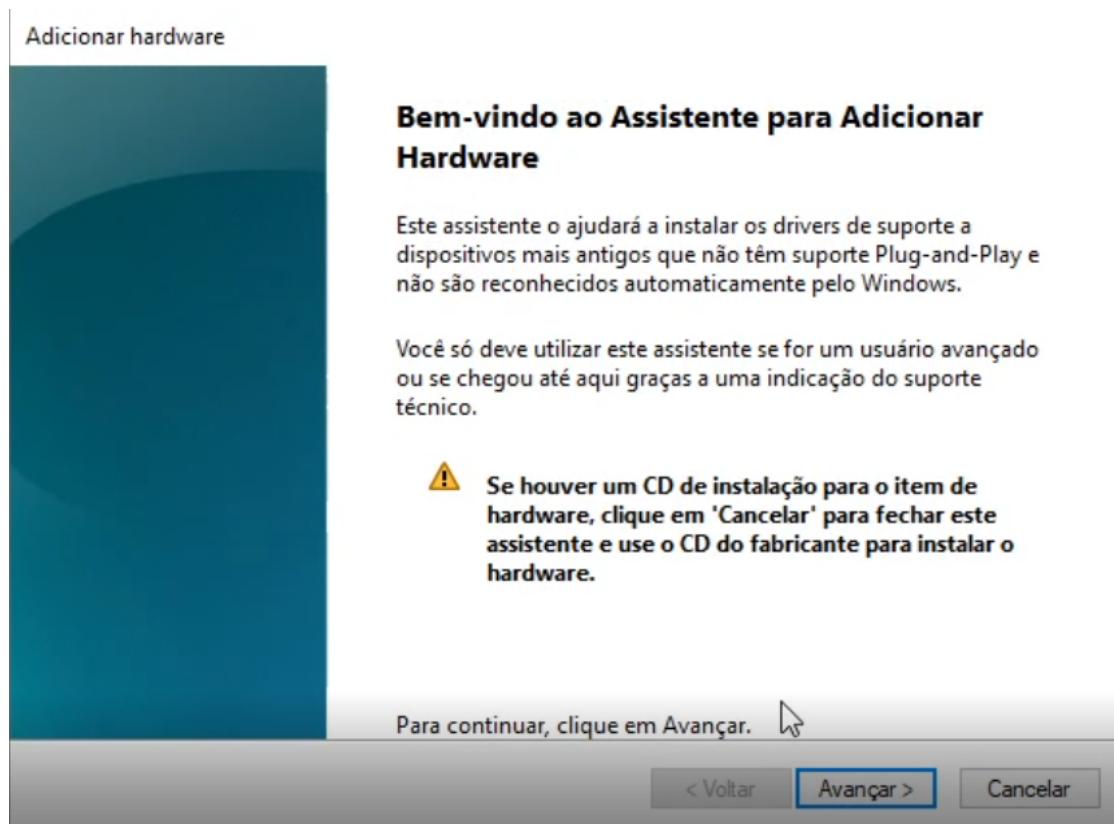
Com o gerenciador de dispositivos aberto, clicar em **adaptadores de rede**.



Em seguida, selecionar no menu a opção **Ação** e, depois, **Adicionar hardware herdado**.



Avançar:



Selecionar a opção **Instalar o hardware que eu selecionar manualmente em uma lista (avanhado)**.

**Adicionar hardware****Este assistente pode ajudá-lo a instalar outro hardware**

O assistente pode procurar outros itens de hardware e instalá-los automaticamente, ou, se você souber exatamente o modelo de hardware que deseja instalar, poderá selecioná-lo na lista.

O que você deseja que o assistente faça?

 Procurar e instalar automaticamente o hardware (recomendável) Instalar o hardware que eu selecionar manualmente em uma lista (avançado)

&lt; Voltar

Avançar &gt;

Cancelar

Selecionar **Adaptadores de rede** e, então, Avançar:

**Adicionar hardware****Na lista abaixo, selecione o tipo de hardware que você está instalando**

Se você não estiver vendo a categoria de hardware que deseja, clique em Mostrar Todos os Dispositivos.

Tipos comuns de hardware:

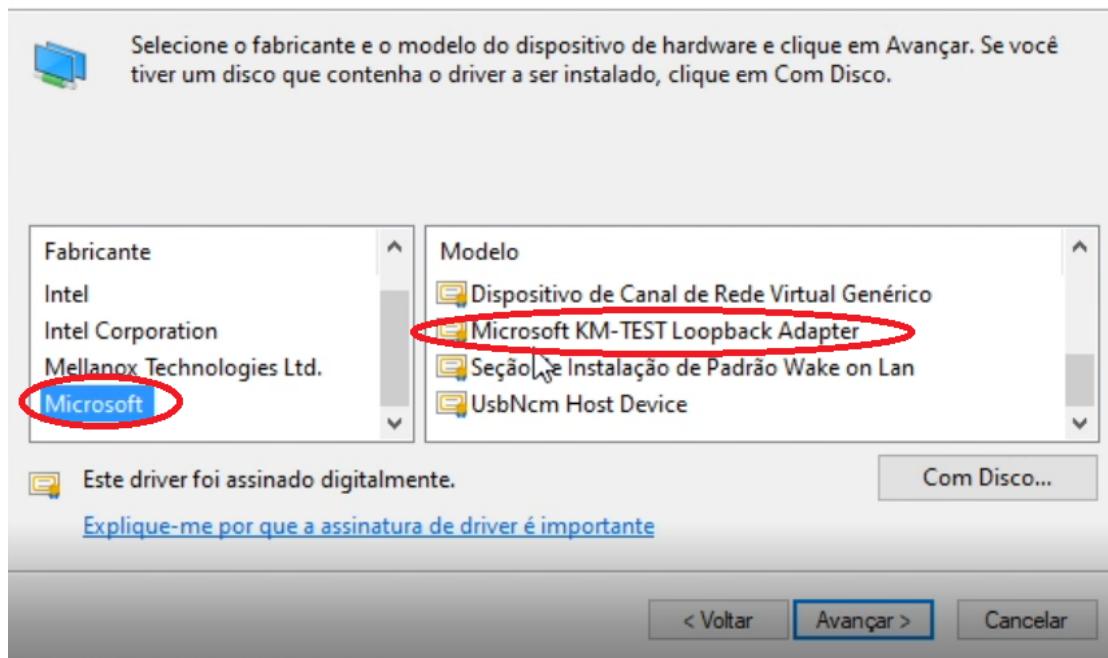
 Mostrar todos os dispositivos Adaptadores de host SD Adaptadores de rede Adaptadores de vídeo Adaptadores seriais para várias portas Bluetooth Devices Câmeras Cartões inteligentes Citrix USB Devices

&lt; Voltar

Avançar &gt;

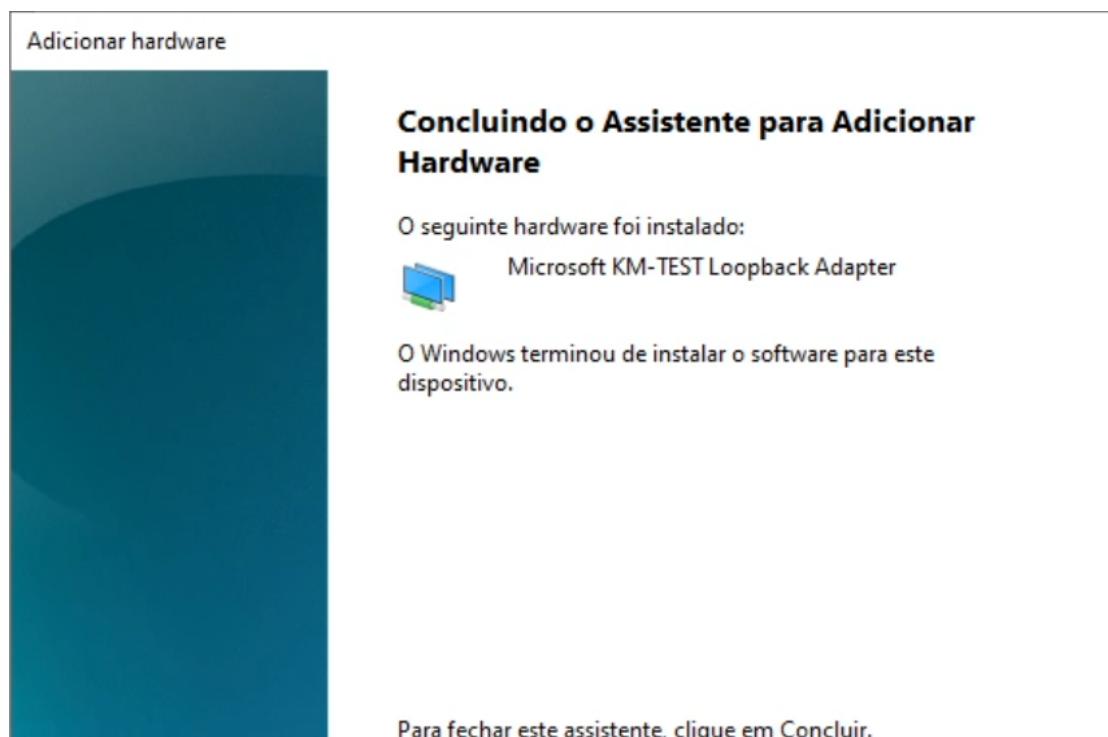
Cancelar

Em “Fabricante”, escolha **Microsoft**, e em “Modelo”, selecione **Microsoft KM-TEST Loopback Adapter**:

**Adicionar hardware****Selecione o driver de dispositivo que deseja instalar para este hardware.**

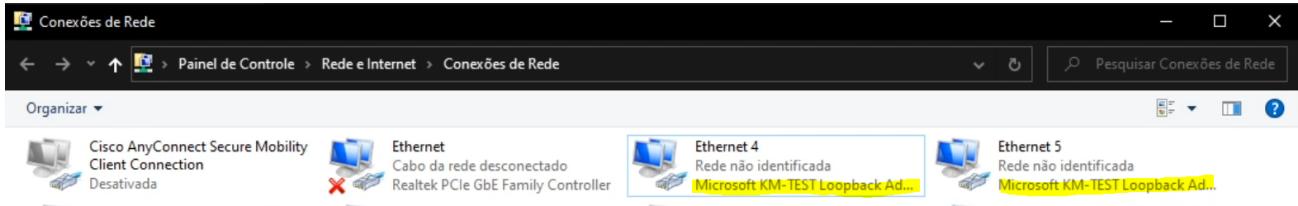
Dica: O nome ou modelo podem variar, mas o nome vai ser sempre algo parecido com “Loopback Adapter”.

Clique em avançar e, então, em Concluir:



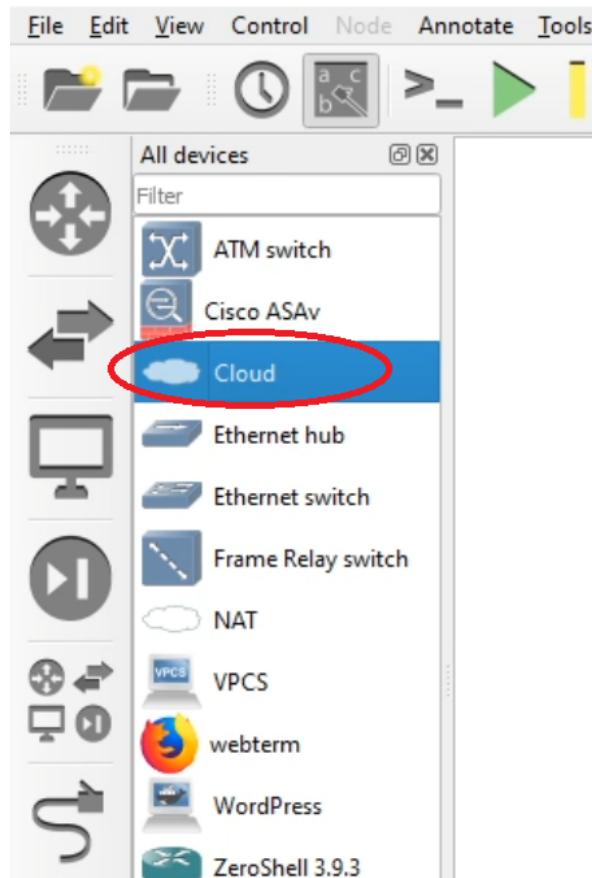
Repita os mesmos passos anteriores para adicionar outra interface do tipo “Loopback Adapter”.

Abra o menu iniciar e digite **conexões de rede**. Dessa forma, podemos ver o número das interfaces do tipo “Loopback” que foram adicionadas:

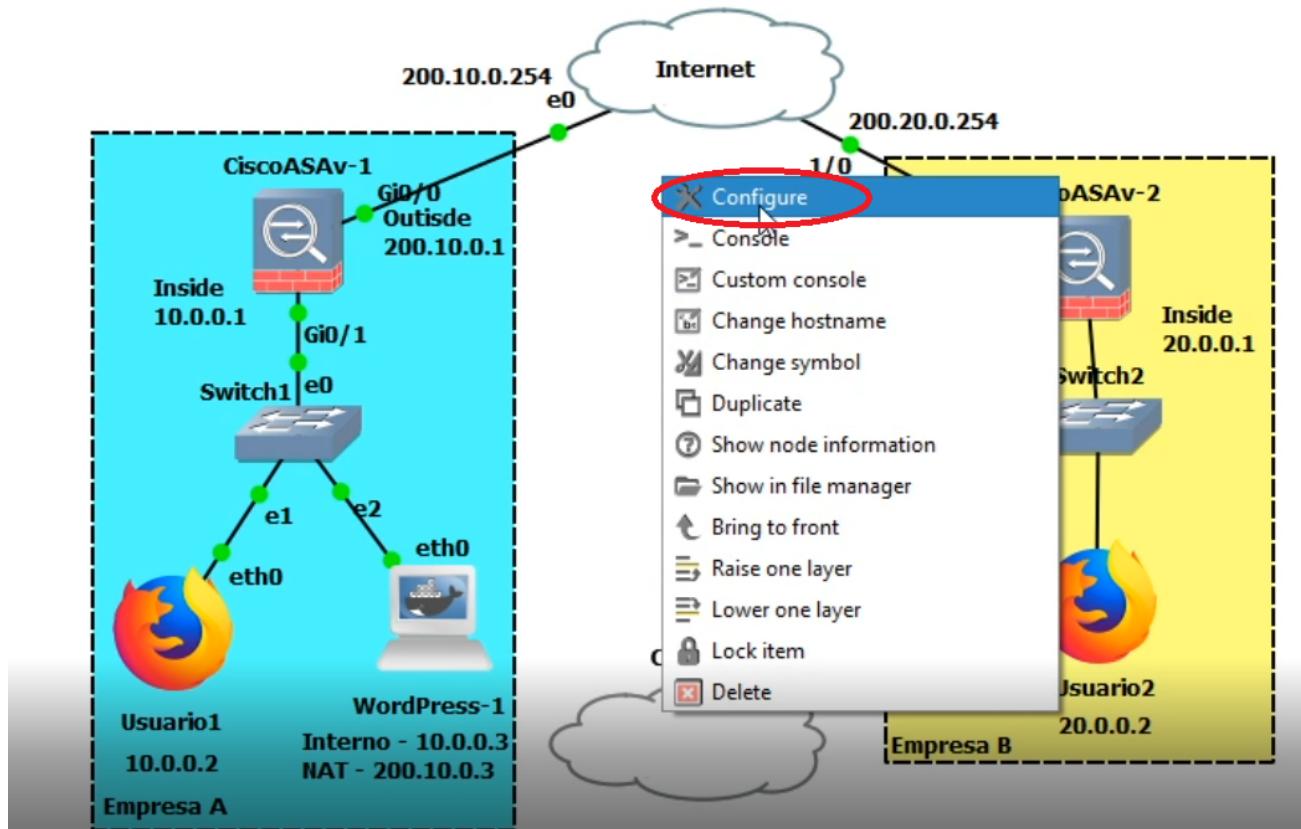


Com as interfaces adicionadas, vamos voltar ao GNS3.

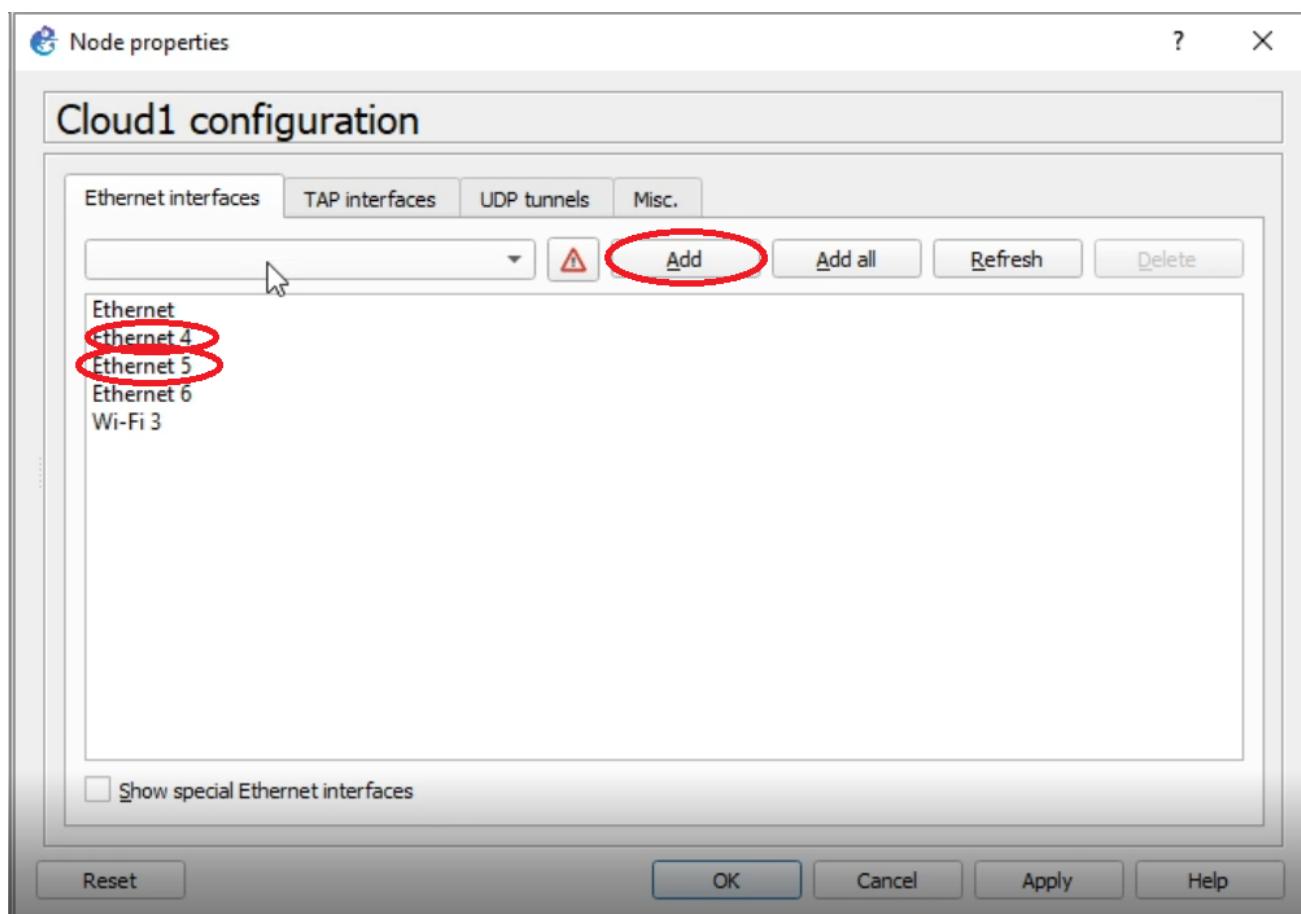
Adicione à topologia um elemento do tipo Cloud:



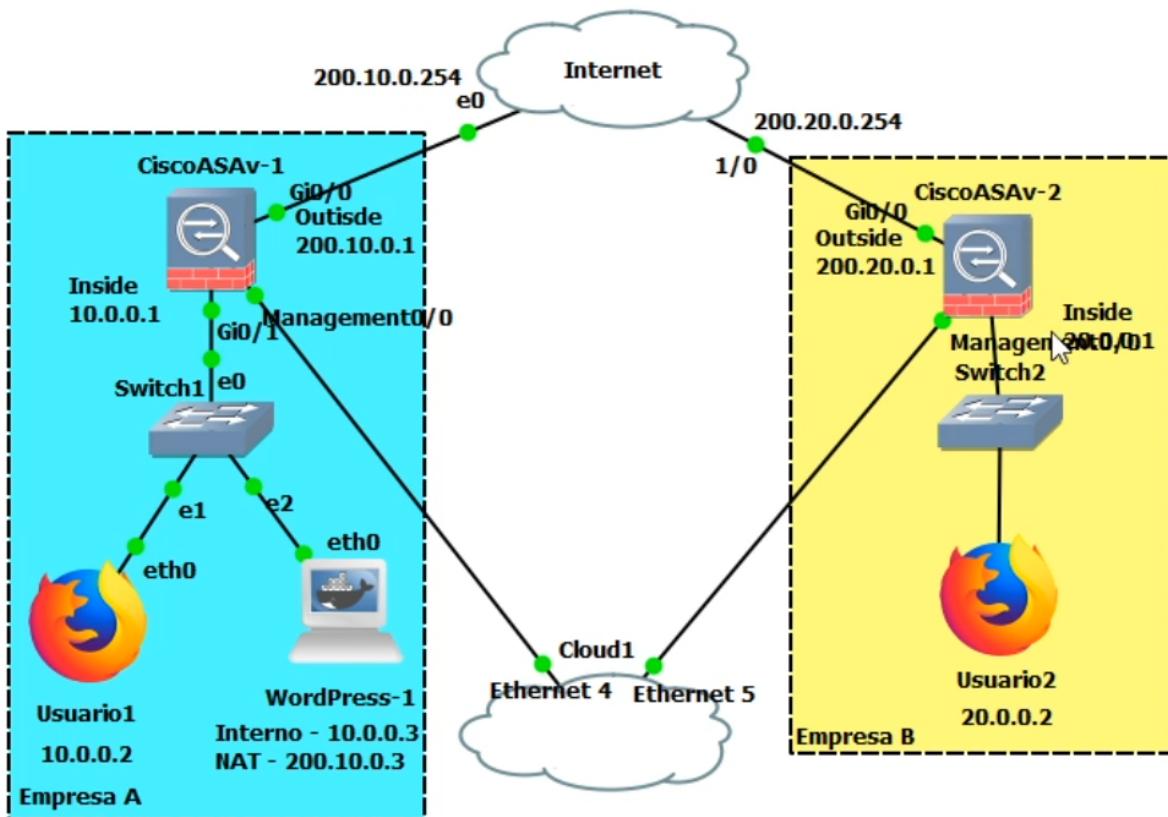
Clique com o botão da direita na nuvem e, em seguida, em “Configure”:



Confira se as duas interfaces Ethernet que acabamos de criar estão relacionadas na configuração. Se não estiverem, basta selecioná-las no menu lista e clicar em Add.



Faça a conexão da primeira “Loopback” (Ethernet 4) à “Management 0/0” do firewall da Empresa A e da segunda “Loopback” (Ethernet 5) à “Management 0/0” do firewall da Empresa B:



Configure no ASA da Empresa A os seguintes parâmetros: Interface M0/0 nameif: mgmt IP: 10.10.0.1 255.255.255.0 usuário: admin password: cisco Habilitar servidor http Permitir que qualquer endereço acesse o ASA via HTTP na interface mgmt

Vm QEMU (CiscoASA-1) - TightVNC Viewer

```

e
Type help or '?' for a list of available commands.
ASA01>
ASA01>
ASA01>
Warning: ASA-1 platform license state is Unlicensed.
Install ASA-1 platform license for full functionality.

ASA01>
ASA01> en
Password:
ASA01# conf t
ASA01(config)# inter
ASA01(config)# interface m0/0
ASA01(config-if)# nameif mgmt
ASA01(config-if)# ip add
ASA01(config-if)# ip address 10.10.0.1 255.255.255.0
ASA01(config-if)# exit
ASA01(config)# username admin password cisco privi
ASA01(config)# username admin password cisco privilege 15
ASA01(config)# http server ena
ASA01(config)# http server enable
ASA01(config)# http 0.0.0.0 0.0.0.0 mgmt
ASA01(config)# end
ASA01# 

```

```

ASA01# confi t
ASA01(config)# interface m0/0
ASA01(config-if)# nameif mgmt
ASA01(config-if)# ip address 10.10.0.1 255.255.255.0

```

```
ASA01(config-if)# exit
ASA01(config)# username admin password cisco privilege 15
ASA01(config)# http server enable
ASA01(config)# http 0.0.0.0 0.0.0.0 mgmt
ASA01(config)# end
ASA01# wr
```

Repeta o processo para o firewall da Empresa B, alterando o IP para 20.20.0.1.

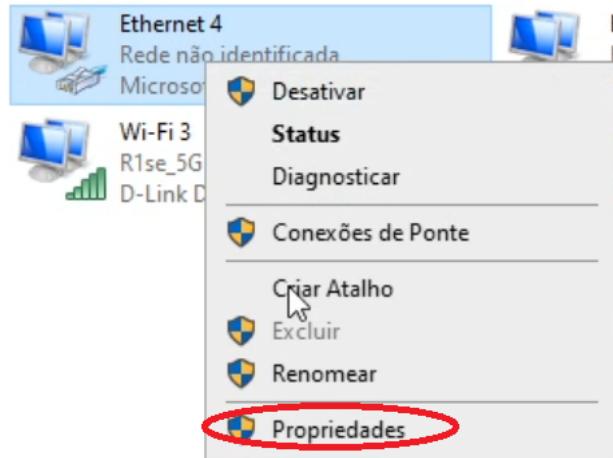
```
QEMU (CiscoASAv-2) - TightVNC Viewer
[Icons] [File] [Edit] [I] [||] [S] [Ctrl Alt] [Disk] [Search] [A] [Zoom]
ASA02(config-if)# nameif mgmt
ASA02(config-if)# ip add
ASA02(config-if)# ip address 20.20.0.1 255.255.255.25
Warning: ASA V platform license state is Unlicensed.
Install ASA V platform license for full functionality.
5.0
ASA02(config-if)# no shut
ASA02(config-if)# exit
ASA02(config)# username admin pas
ASA02(config)# username admin password cisco pri
ASA02(config)# username admin password cisco privilege 15
ASA02(config)# http server ena
ASA02(config)# http server enable
ASA02(config)# htt
ASA02(config)# http 0.0.0.0 0.0.0.0 mg
ASA02(config)# http 0.0.0.0 0.0.0.0 mgmt
ASA02(config)# end
ASA02# wr
Building configuration...
Cryptochecksum: 7bcd63c 113321e2 f78b9b73 f7bc0b99

7446 bytes copied in 0.310 secs
[OK]
ASA02# _
```

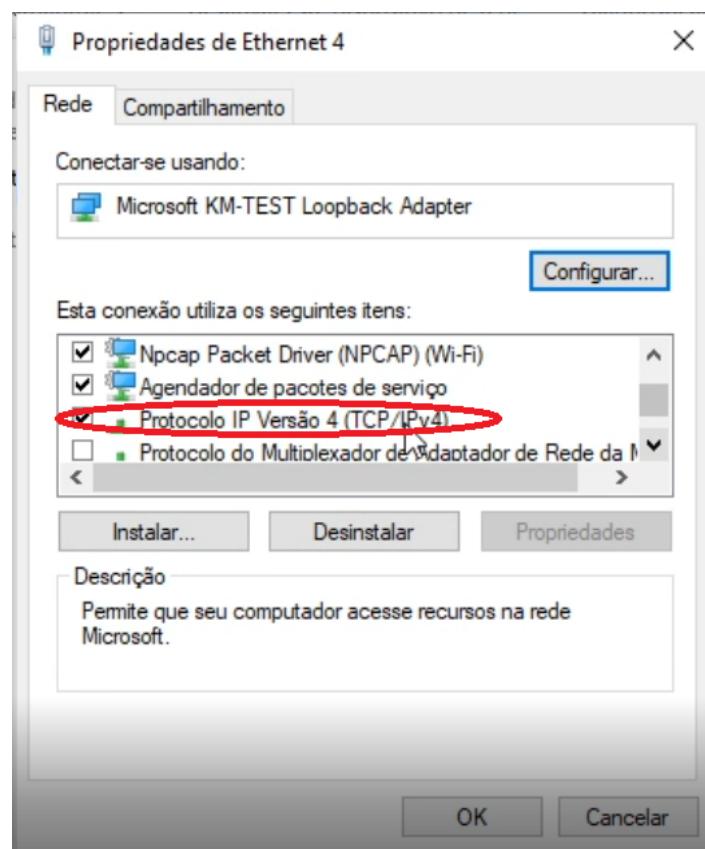
```
ASA02# config t
ASA02(config)# interface m0/0
ASA02(config-if)# nameif mgmt
ASA02(config-if)# ip address 20.20.0.1 255.255.255.0
ASA02(config-if)# exit
ASA02(config)# username admin password cisco privilege 15
ASA02(config)# http server enable
ASA02(config)# http 0.0.0.0 0.0.0.0 mgmt
ASA02(config)# end
ASA02# wr
```

Agora, vamos configurar o IP nas interfaces Loopback que adicionamos ao Windows.

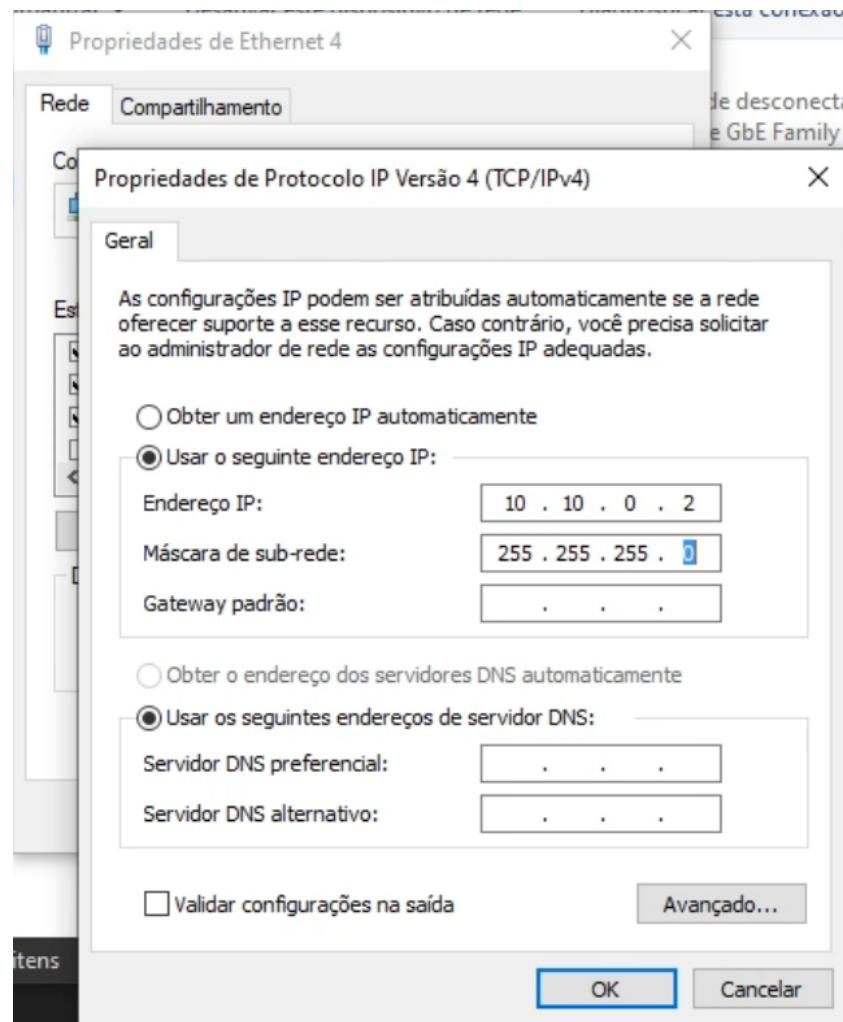
Para isso, volte em **Conexões de Rede**, clique com o botão da direita na primeira “Loopback” (Ethernet 4, em nosso exemplo) e, em seguida, clique em **Propriedades**:



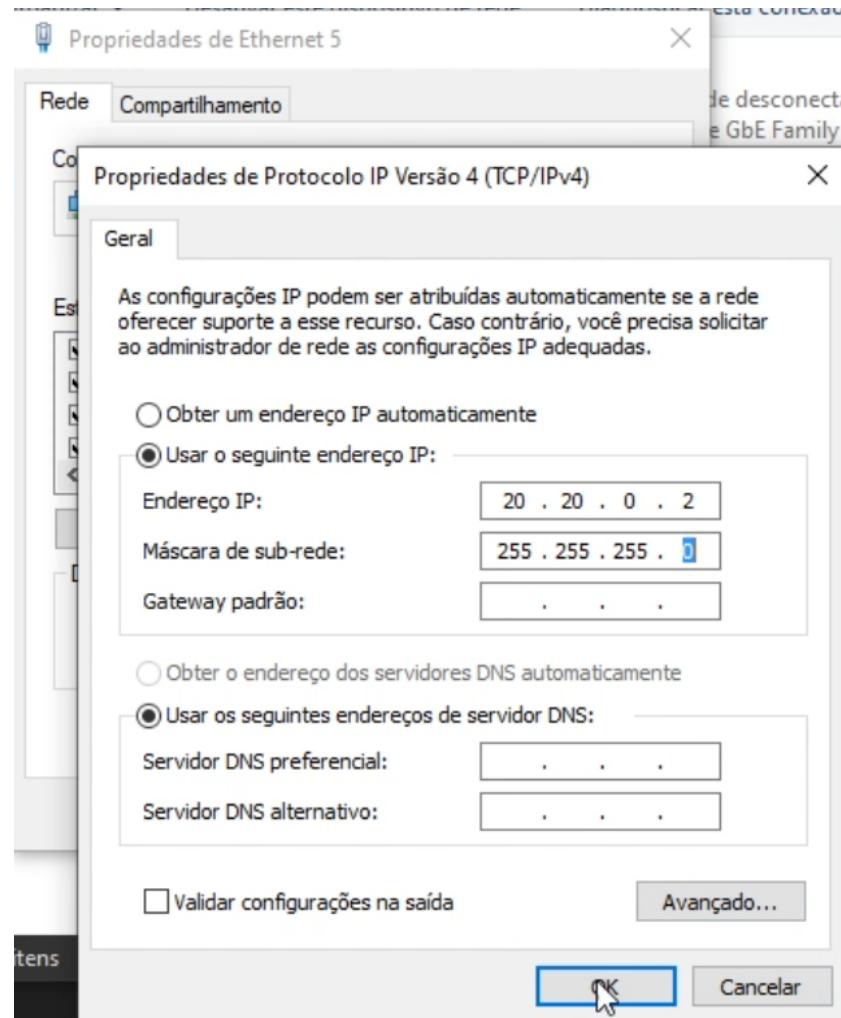
Dê um duplo clique em “Protocolo IP Versão 4”:



Preencha os Campos com Endereço IP: 10.10.0.2 e Máscara de sub-rede: 255.255.255.0.

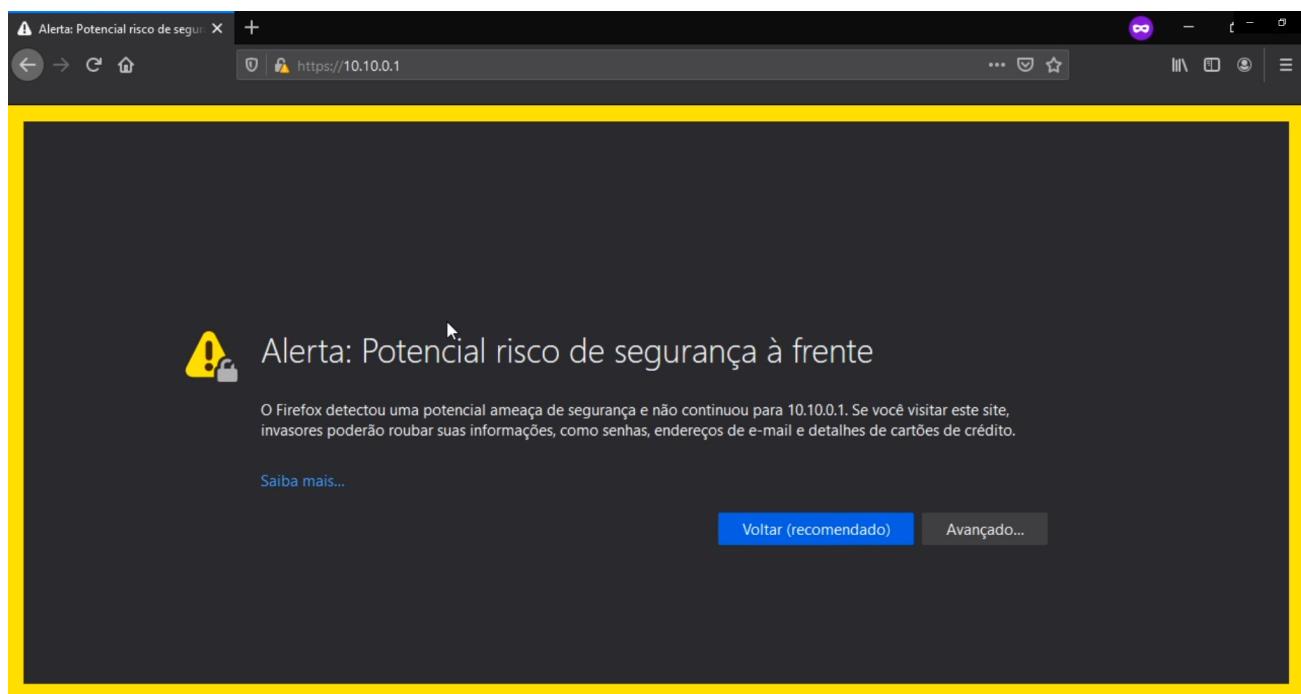


Repita os passos para a outra “Loopback” (Ethernet 5 em nosso exemplo), configurando o IP: **20.20.0.2** e Máscara de sub-rede: **255.255.255.0**.



Abra agora o navegador e digite o endereço <https://10.10.0.1>, que é o IP de gerência do firewall da Empresa A. Note o protocolo **HTTPS**.

Será apresentado o erro de certificado. Pista: clicar em “Avançado” e, então, “Aceitar o risco e continuar”.



A página do **Cisco ASDM** é então exibida. Vamos, em seguida, instalar a ferramenta ASDM, clicando no botão “Install ASDM Launcher”. Isso fará com que o instalador do ASDM seja copiado para sua máquina.



# Cisco ASDM 7.8(1)



Cisco ASDM 7.8(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

## Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

**Install ASDM Launcher**

## Run Cisco ASDM as a Java Web Start application

Java Web Start is required to run ASDM, but it is not installed on this computer.

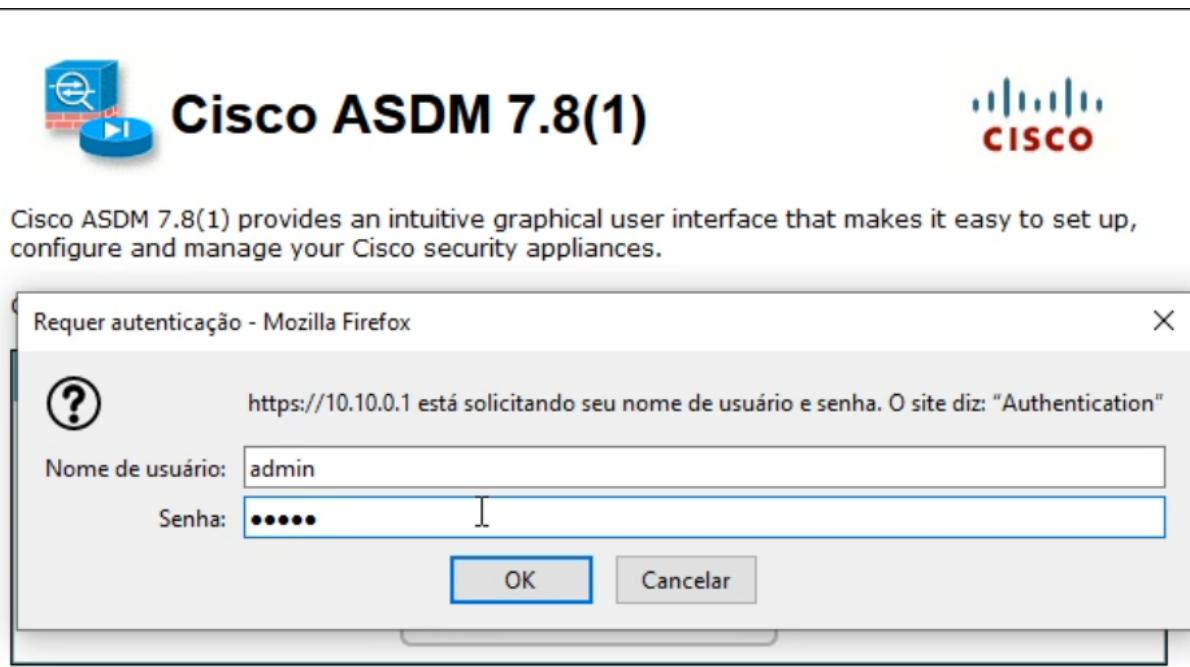
**Install Java Web Start**

Copyright © 2006-2017 Cisco Systems, Inc. All rights reserved.

Entre com a senha que acabamos de configurar:

Usuário: admin

Senha: Cisco



Cisco ASDM 7.8(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

**Requer autenticação - Mozilla Firefox**

https://10.10.0.1 está solicitando seu nome de usuário e senha. O site diz: "Authentication"

Nome de usuário: admin

Senha:  [REDACTED]

OK Cancelar

**Run Cisco ASDM as a Java Web Start application**

Java Web Start is required to run ASDM, but it is not installed on this computer.

Install Java Web Start

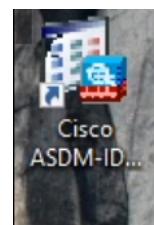
Copyright © 2006-2017 Cisco Systems, Inc. All rights reserved.

Execute o instalador:



Siga os passos para instalar o ASDM no computador.

Será adicionado ao seu “Desktop” o ícone do ASDM:



Basta clicar no ícone e, então, poderemos fornecer o IP da Interface Management dos firewalls e acessar sua console gráfica:



ASA01:

IP Management: **10.10.0.1**

Usuário: admin

Password: cisco

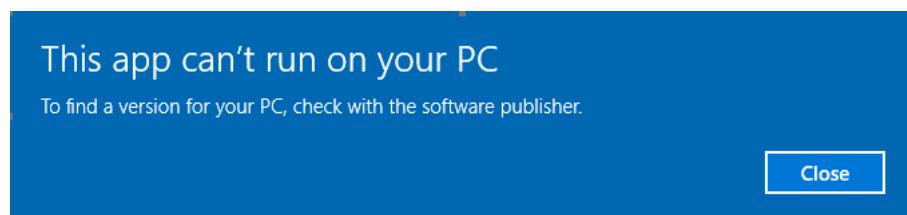
ASA02:

IP Management: **20.20.0.1**

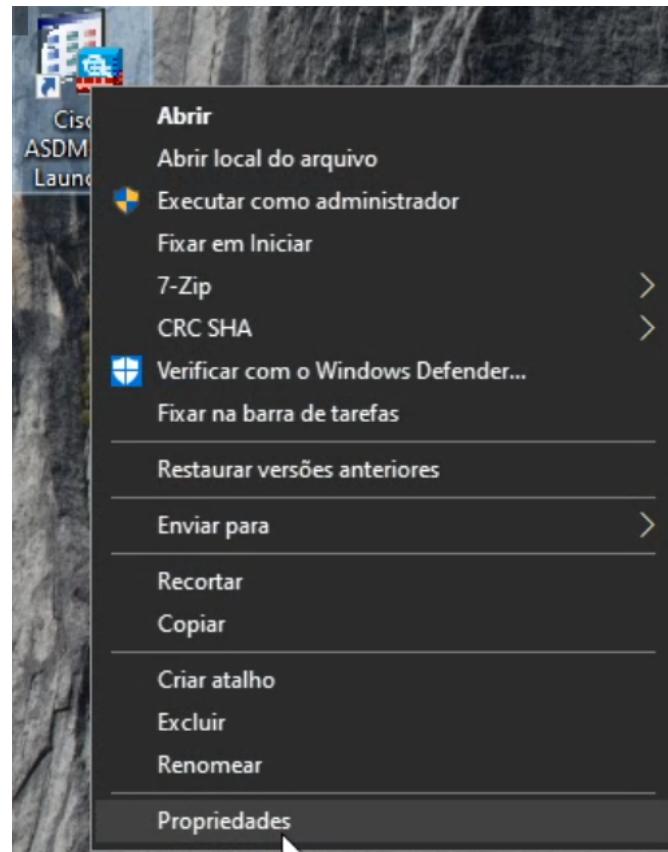
Usuário: admin

Password: cisco

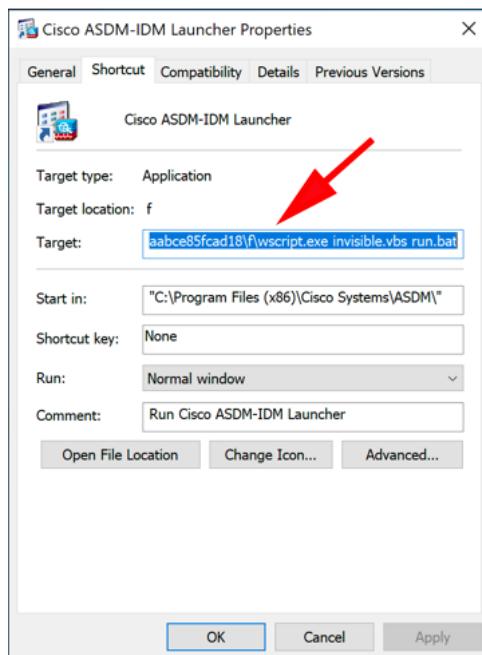
Dica: Se o ASDM não abrir, apresentando o erro “This app can't run on your PC”. Siga os passos abaixo para resolver:



Clique com o botão da direita no ícone do ASDM, e selecione Propriedades:

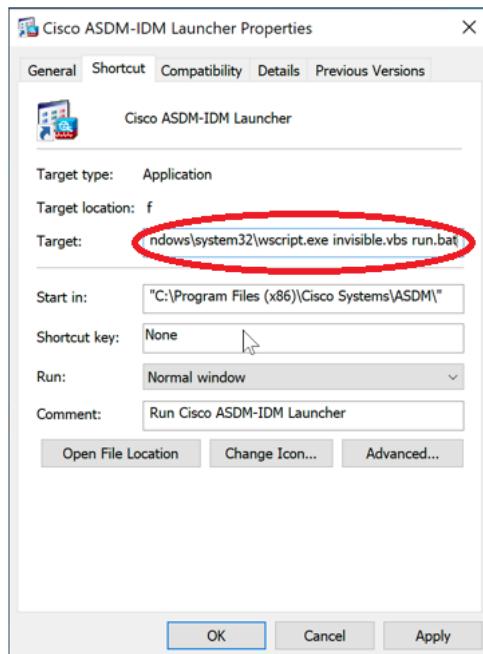


Em seguida, na aba Atalho, altere o “Destino (ou Target)” de:



Para:

C:\Windows\system32\wscript.exe invisible.vbs run.bat



Isso deve solucionar o problema.

Pronto. Basta acessar agora a console de gerenciamento gráfica!