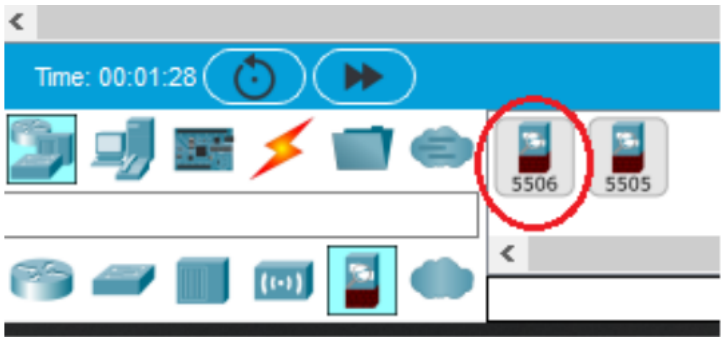
05

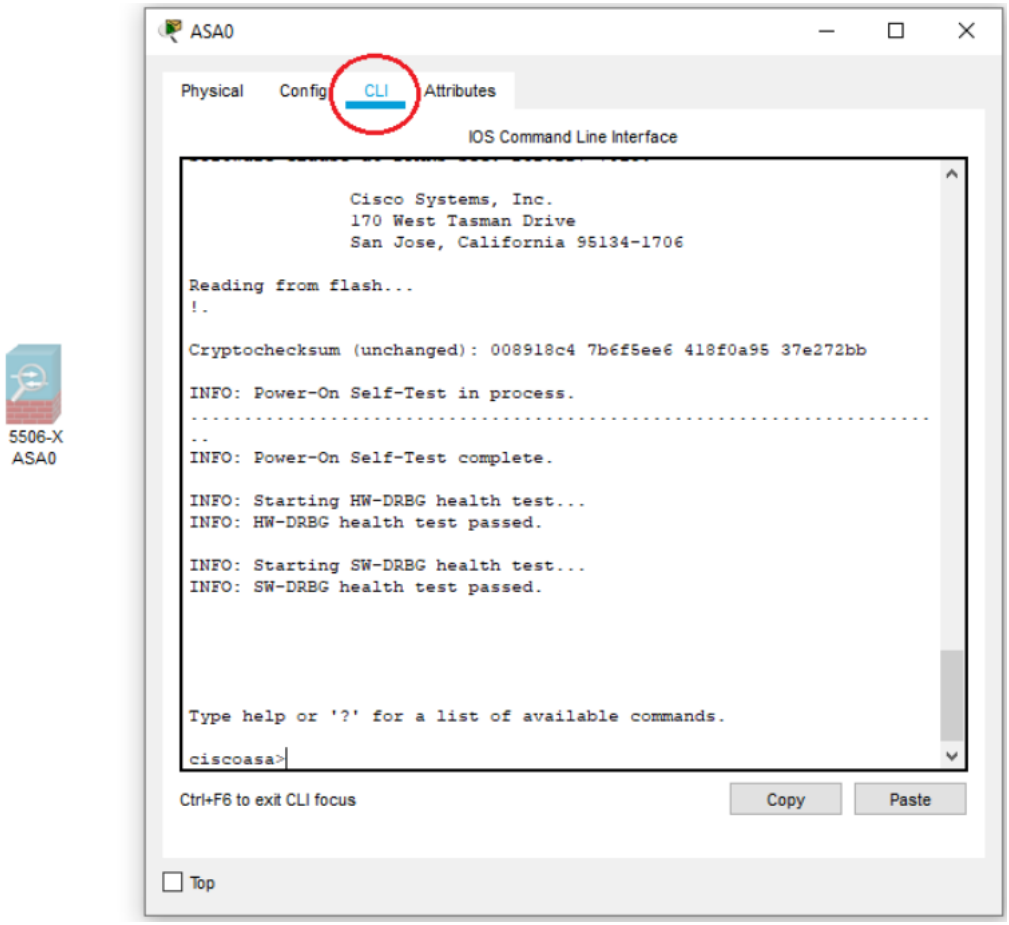
Mãos à obra: Configuração Inicial

Agora vamos realizar a configuração inicial do firewall e iniciar nossa topologia.

Iniciamos um projeto novo no Packet Tracer, selecionamos o equipamento Firewall do tipo 5506 e arrastamos para o espaço de trabalho.



Com o firewall adicionado na área de trabalho do Packet Tracer, basta clicar nele e então então na aba CLI para termos acesso à console de configuração do equipamento.



A primeira coisa que fazer é na verdade *"desconfigurar"* o que já veio feito nele. Vamos limpar tudo o que o Packet Tracer deixa configurado e começar do zero mesmo a configuração do firewall. Entrando com os comandos abaixo, vamos apagar toda a configuração e então começar a preparar o nosso cenário.

```
ciscoasa>enable
Password:
```

```
ciscoasa#write erase
Erase configuration in flash memory? [confirm]
[OK]

ciscoasa#reload
Proceed with reload? [confirm]
```

Nesse ponto o firewall vai reiniciar e, quando ele perguntar se queremos utilizar a pré-configuração via prompts, podemos responder com não.

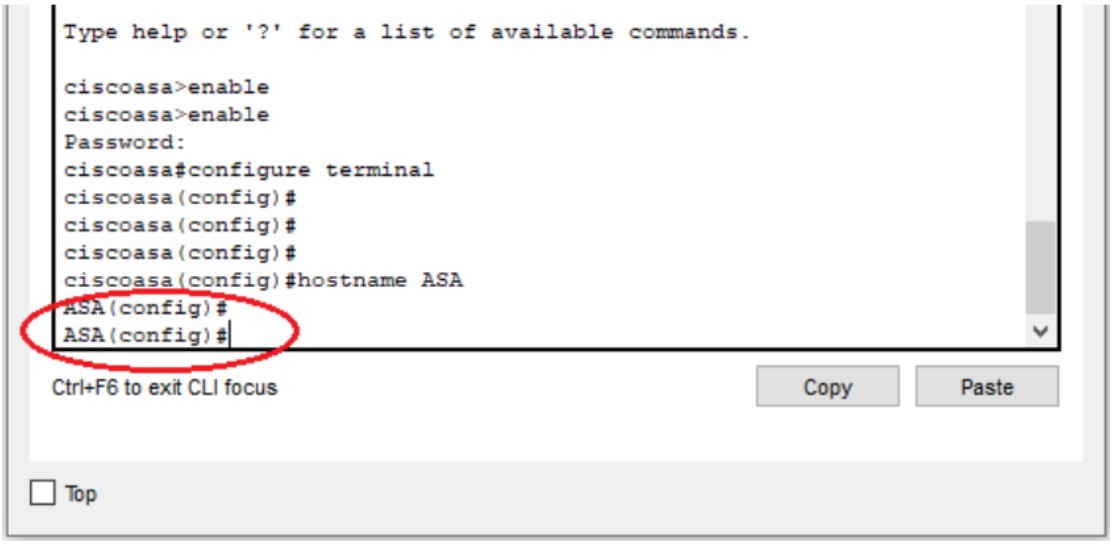
```
Pre-configure Firewall now through interactive prompts [yes]: no
```

Pronto, nesse ponto já temos um firewall novinho e sem nenhum resquício de configuração em sua memória.

O primeiro passo vai ser entrar no modo de configuração global (configure terminal) e configurar o hostname ASA:

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#hostname ASA
ASA(config)#
```

Dica: Podemos confirmar que a alteração foi realizada com sucesso pois o hostname já é modificado na hora:



Agora nosso objetivo é configurar o acesso remoto ao firewall. Para isso, vamos utilizar a interface **Management 1/1**.

O primeiro passo vai ser configurar a interface Management 1/1 com seu nome **(mgmt)**, ip address **(172.16.20.1)** máscara de sub-rede **(255.255.255.0)** e habilitá-la para tráfego (no shutdown).

```
ASA(config)#interface m1/1
ASA(config-if)#ip address 172.16.20.1 255.255.255.0
ASA(config-if)#nameif mgmt
INFO: Security level for "mgmt" set to 0 by default.
ASA(config-if)#no shutdown
```

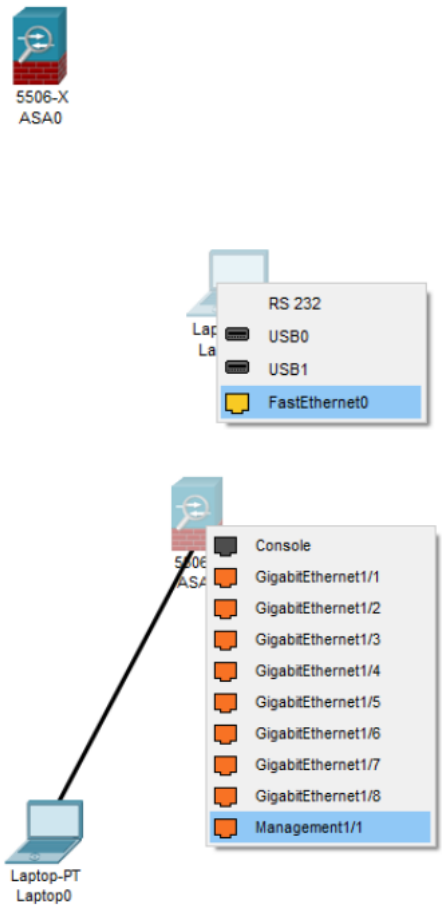
Agora que já temos uma interface habilitada e configurada, precisamos criar um usuário/senha e permitir que qualquer IP de origem na rede **172.16.20.x** acesse o firewall por meio da interface **mgmt** utilizando o protocolo **ssh**.

```
ASA(config)#username admin password cisco
ASA(config)#ssh 172.16.20.0 255.255.255.0 mgmt
ASA(config)#aaa authentication ssh console LOCAL
```

Tudo pronto. Agora que o firewall está configurado para receber o acesso remoto, vamos testar agora e validar tudo o que fizemos:

Para o teste, vamos arrastar um Laptop para nossa topologia.

Por meio de uma conexão com cabo direto, vamos interligar a porta **FastEthernet0** do Laptop com a porta **Management 1/1** do firewall:

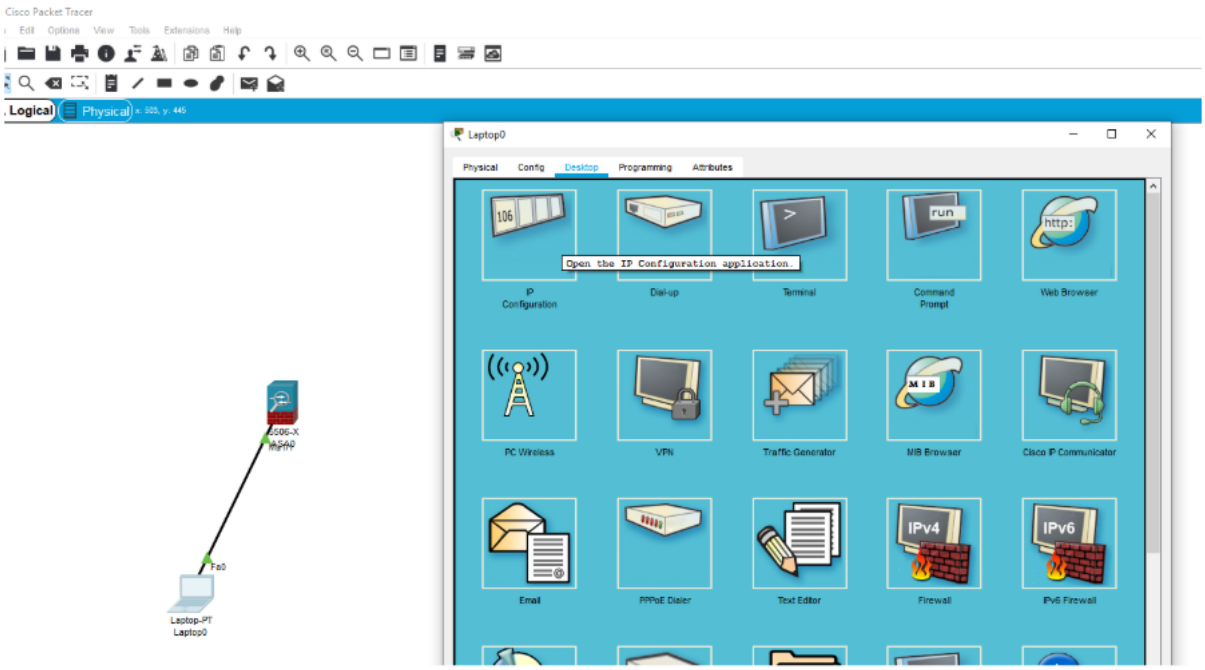


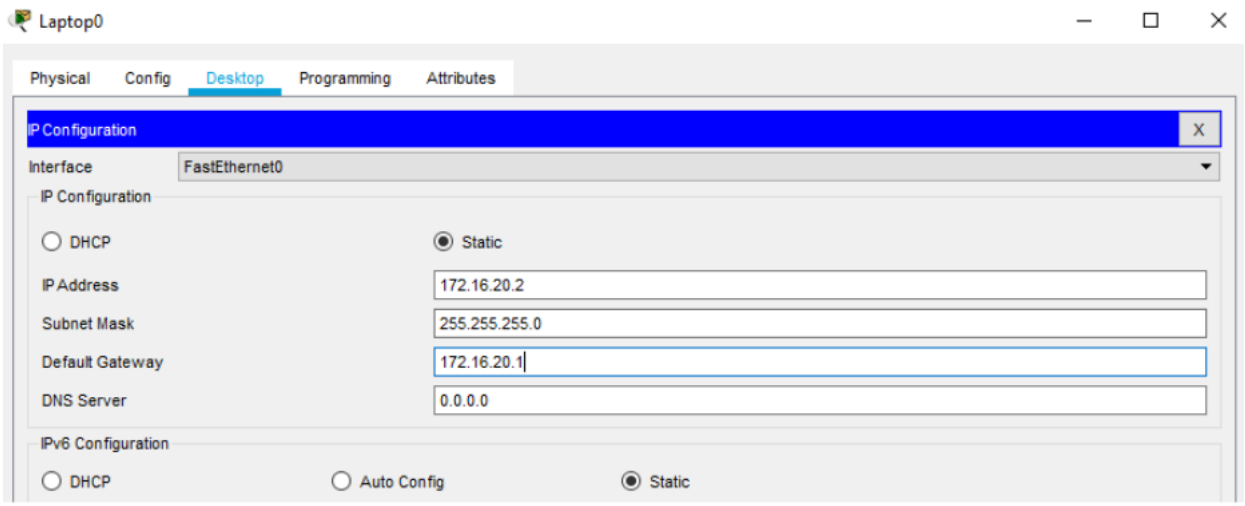
Agora vamos adicionar um IP no Laptop para que ele fique na mesma rede da interface que acabamos de configurar no firewall.

Clicar no Laptop, Desktop e então em IP Configuration e adicionar seu endereçamento IP:

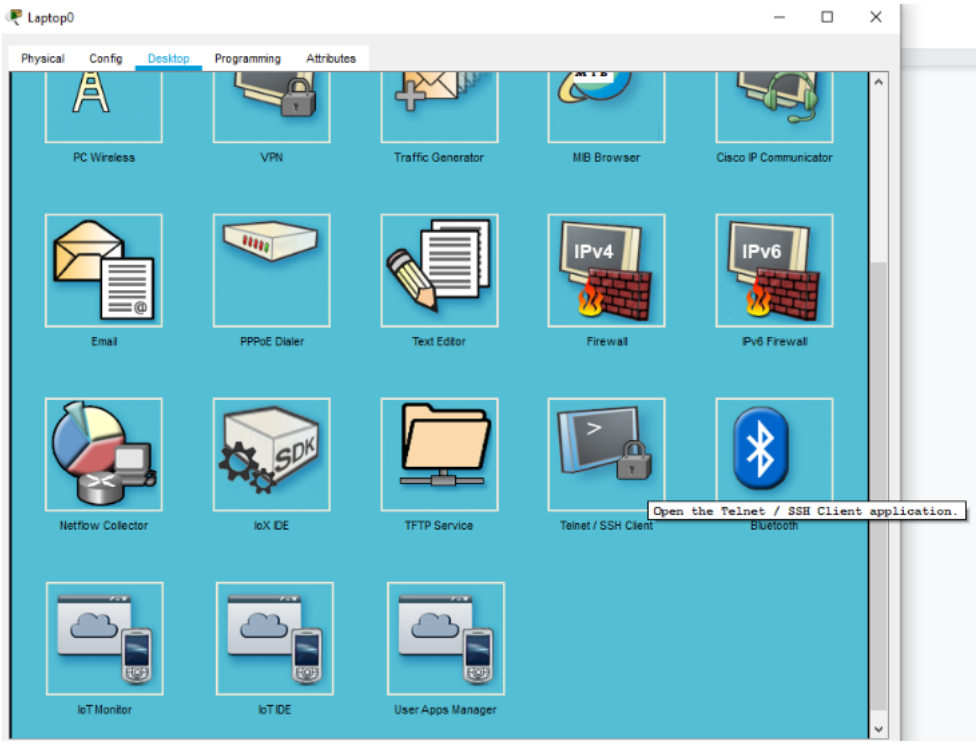
- **IP Address:** 172.16.20.2
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 172.16.20.1

Clicar no X para fechar a interface de configuração de IP.

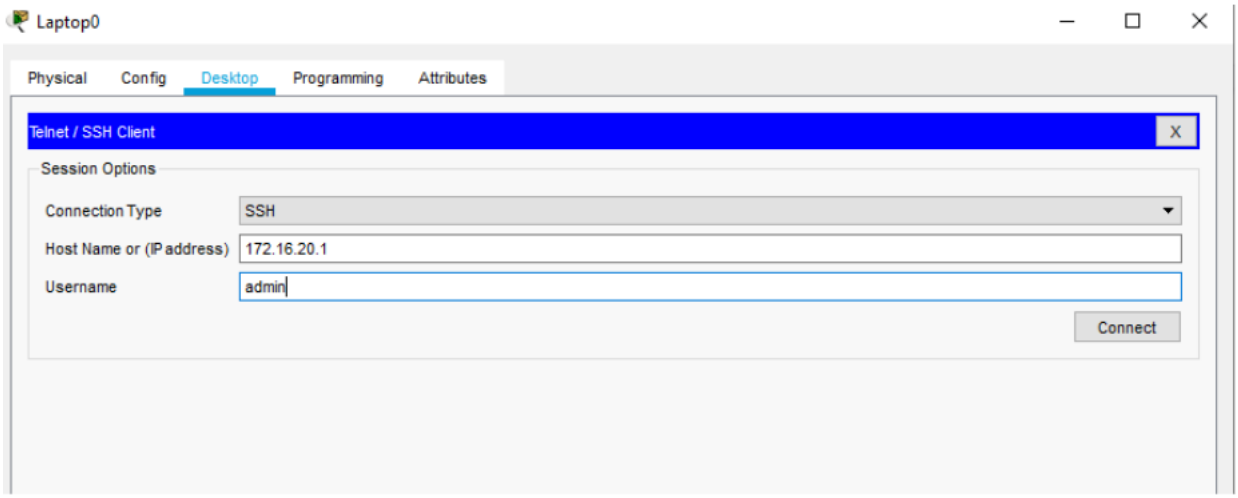




Agora só falta testar. Abrir mais uma vez o Laptop clicando nele e depois em Desktop e finalmente no aplicativo **Telnet / SSH** Client no Laptop.

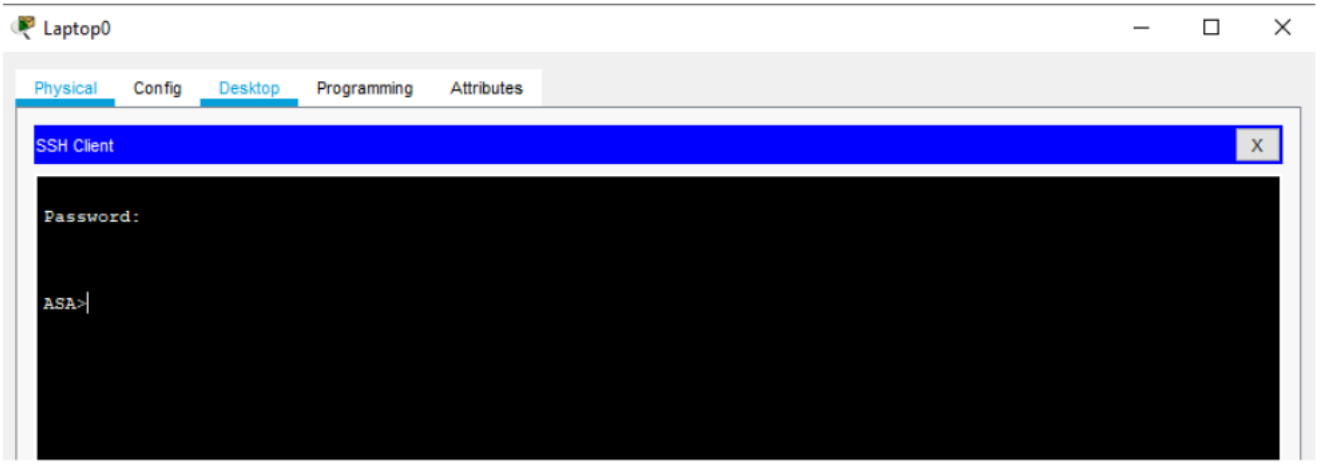


- **Connection Type:** SSH
- **Host Name or (IP address):** 172.16.20.1
- **Username:** admin



Se tudo funcionou, você verá a resposta do firewall solicitando a senha para o usuário **admin**. No nosso exemplo, configuramos a senha **cisco**.

Basta entrar com essa senha e pronto, temos acesso remoto ao firewall :)


Laptop0
Physical
Config
Desktop
Programming
Attributes
SSH Client
X
Password:
ASA>