01

Listas de acesso

Transcrição

Conseguimos implementar o nosso servidor interno, porém, ainda não conseguimos atender as requisições dos diretores. Eles pediram que somente os Gerentes de Finanças e Vendas tenham acesso à página de login do servidor.

A tarefa é configurar as listas de acesso no roteador, para garantir acesso somente aos gerentes de vendas e finanças.

Vamos clicar no roteador `1841 Router1` , e na aba `CLI` :

Na primeira etapa, criaremos a *lista de acessos* com o comando `ip access-list ?`

```
>enable
#configure terminal
#ip access-list ?
```

Podemos escolher entre a lista estendida ou a *standard*. A estendida nos permite realizar essa verificação tanto na origem como no destino. Já a *standard* só faz verificação na origem. Nós queremos permitir que o computador do gerente de finanças e do gerente de vendas, tenham acesso ao servidor `Server-PT Server0` .

Então, vamos realizar o filtro tanto na origem como no destino, por isso, usaremos a lista estendida:

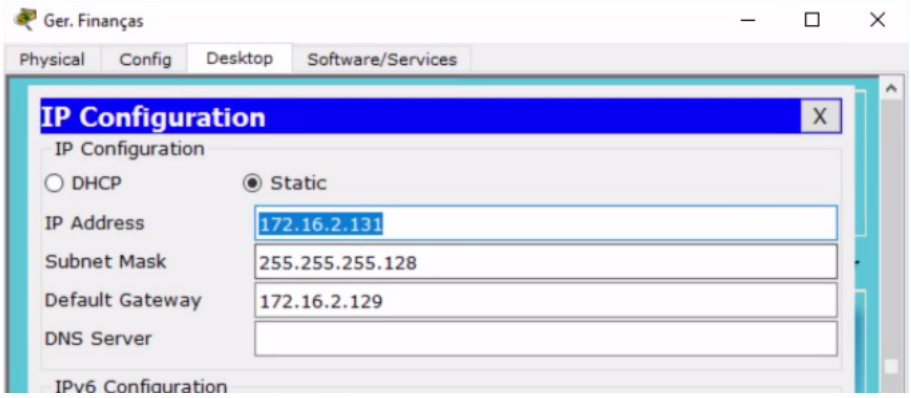
```
#ip access-list extended SERVIDOR-GERENTES
```

Criamos a nossa lista de acesso, e precisamos informar quais são as políticas de tráfego que serão analisadas pela lista de acesso. Por isso, vamos permitir o acesso dos computadores dos gerentes de vendas e de finanças.

Como vimos anteriormente, quem realiza o transporte da informação é o protocolo TCP, que depois dele, terá a transmissão do protocolo HTTP. No comando `#permit tcp` , não podemos nos esquecer de passar o endereço IP da nossa origem. No caso, inicializaremos primeiro com o computador do gerente de finanças.

O endereço IP que está relacionado a ele agora é o `172.16.2.131` . Entretanto, esse endereço está sendo fornecido de forma dinâmica. Quer dizer que, eventualmente, ele pode ser alterado.

Se colocarmos esse endereço dinâmico na lista de acesso, e esse valor for alterado, a nossa lista acaba não tendo mais utilidade... Para evitarmos esse problema, vamos alterar a forma de trabalhar com endereço IP no computador dos gerentes de finanças e de vendas. Usaremos esses endereços de forma estática, garantindo que esse endereço não seja alterado.



Agora sim podemos colocar o endereço no roteador:

```
#permit tcp 172.16.2.131
```

Adicionando o `?` no final do comando, aparece para nós um conceito novo a ser tratado: o **Source wildcard bits**!

Usando o **Source wildcard bits**, conseguimos indicar para a lista de acesso qual a parte do endereço IP - que tem que ser exatamente igual ao digitado-, e qual parte não importa o valor. Temos que indicar por meio do Source wildcard bits, que a lista de acessos deve considerar como sendo origem, o primeiro intervalo do endereço IP `172`, o segundo intervalo sendo `16`, o terceiro intervalo sendo `2`, e o quarto intervalo não importa. Por isso, utilizaremos `255` para representar o intervalo que não importa, e `0` para os intervalos que importam, ou seja, eles devem ser exatamente iguais ao endereço IP.

```
#permit tcp 172.16.2.131 0.0.0.255
```

Então, quando temos uma rede de 100 computadores, por exemplo, não precisamos estar configurando em cada linha, o endereço IP exato de cada um desses computadores para que cada um tenha a permissão. Assim, dizendo que o endereço IP é global, e somente o último intervalo não importa, economizamos muito tempo, pois ele considera TODOS os endereços que começam com `172.16.2. .`

No entanto, no nosso caso, não queremos que todos tenham permissão. Queremos que esse endereço IP específico `172.16.2.131` tenha permissão de acessar o servidor. Para isso, em de colocar `0.0.0.255`, colocaremos `0.0.0.0`, assim a permissão só será concedida a esse endereço.

Agora, vamos indicar o endereço IP de **destino**, o endereço IP do servidor.

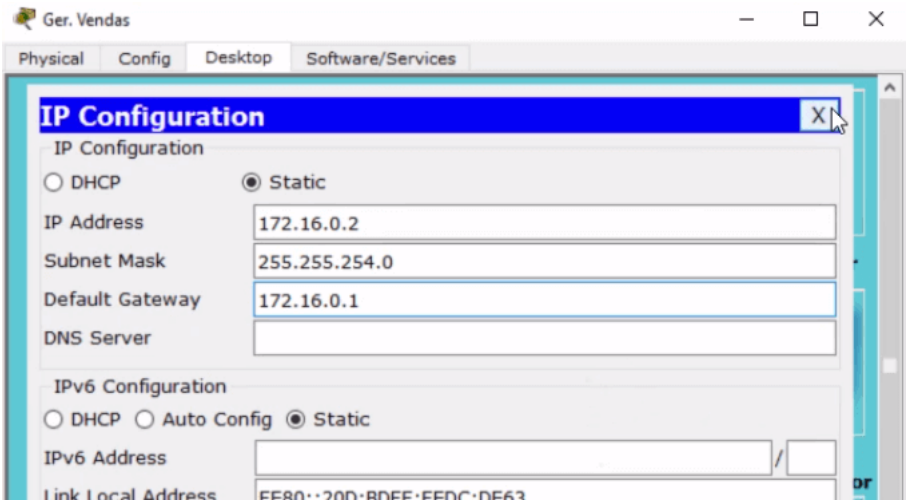
```
#permit tcp 172.16.2.131 0.0.0.0 172.16.3.2
```

Acrescentando um `?` no final do comando, especificaremos qual parte desse endereço IP de destino que tem que ser exatamente igual, e qual parte do endereço não importa. Queremos trabalhar exatamente o endereço `172.16.3.2` para esse servidor específico.

```
#permit tcp 172.16.2.131 0.0.0.0 172.16.3.2 0.0.0.0
```

Vamos fazer o mesmo processo para o computador do gerente de vendas.

Como podemos ver, o endereço IP do gerente de vendas também está dinâmico, e para evitar que eventualmente ser alocado algum endereço IP para esse computador, mudaremos a configuração para **static**, pois assim garantiremos que esse endereço IP desse computador não será alterado.



Realizaremos uma nova permissão para esse outro endereço IP:

```
#permit tcp 172.16.0.2 0.0.0.0 172.16.3.2 0.0.0.0
```

Criamos a nossa lista de acesso, e colocamos quais são os endereços que terão permissão de acessar o servidor.

Não podemos nos esquecer do seguinte. Os dois endereços " `172.16.2.131` " e " `172.16.0.2` ", estão configurados **estaticamente**. Será preciso informar ao **Pool DHCP** para que ele exclua esses dois endereços, para que ele não entregue esses mesmos endereços para outros clientes na mesma rede.

```
#exit
#ip dhcp excluded-address 172.16.2.131
#ip dhcp excluded-address 172.16.0.2
```

Desta forma, o Pool DHCP não vai considerar mais esses endereços na lista de endereços disponíveis. Vamos ver o resultado da configuração da lista de acessos.

O primeiro a ser testado é o gerente de finanças, e ele ainda possui acesso ao servidor. Entretanto, os funcionários de vendas ainda possuem acesso ao servidor! E por que eles continuam tendo acesso?

Precisamos configurar essa lista de acessos para que ela esteja vinculada com as subinterfaces da VLAN 10 de vendas, e da VLAN 20 de finanças.

Na aba "CLI" de `Router1` , entraremos na subinterface do setor de vendas:

```
#interface fastEthernet 0/0.1
```

Para fazer essa associação da lista com essa interface, utilizaremos o comando `ip access-group` e também o nome da lista de acesso que queremos vincular com essa subinterface. Depois disso, diremos qual será o sentido que a análise deve ser feita. Utilizamos (**in**)quando o pacote estiver entrando no roteador por essa subinterface, ou (**out**) quando ele estiver saindo do roteador por essa subinterface.

Em nosso diagrama, o pacote TCP chegará no primeiro switch, depois ele vai para o switch principal, e daí ele vai entrar no roteador. Sabendo disso, podemos criar uma política de acesso para que o roteador verifique tudo o que estiver entrando nessa subinterface:

```
#ip access-group SERVIDOR-GERENTES in
```

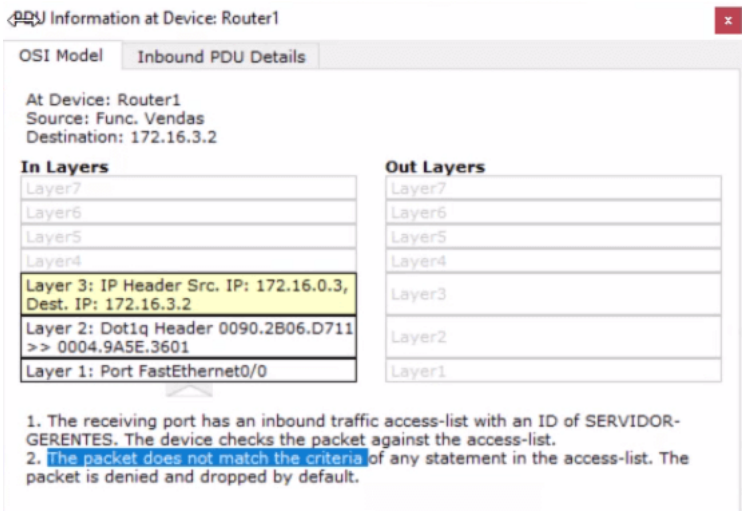
Será feita a mesma configuração para o setor de finanças na VLAN 20 através da subinterface 0/0.2.

```
#exit
#interface fastEthernet 0/0.2
#ip access-group SERVIDOR-GERENTES in
```

Vamos ver se agora temos sucesso em nossa análise com essa lista de acesso.

Depois que o pacotinho TCP saiu do computador do gerente de finanças e chegou até o roteador, passando pela lista de acessos configurada para a VLAN 20, e tendo permissão, o roteador vai mandar o pacotinho adiante para chegar até o servidor, e com isso, o gerente de finanças terá acesso ao servidor.

Vamos analisar o pacotinho TCP que saiu do computador dos funcionários de vendas.



A imagem acima nos diz que o pacote não bateu com nenhum critério existente na lista de acessos. Por isso, ele será *negado* e descartado. Isso quer dizer que os funcionários de vendas não conseguem mais acessar o servidor, e se fizermos o mesmo teste com os funcionários de finanças, veremos que eles também não terão mais acesso ao servidor.

Agora, precisamos testar se a comunicação feita antes não está quebrada. Vamos "pingar" o computador do gerente de finanças (VLAN 20), para os funcionários de vendas (VLAN 10).

Clicando no computador do gerente de finaças, em "Desktop > Command Prompt", colocaremos o comando:

```
>ping 172.16.0.3
```

Em seguida, recebemos a mensagem:

```
Pinging 172.16.0.3 with 32 bytes of data:
```

```
Reply from 172.16.2.129: Destination host unreachable.
Reply from 172.16.2.129: Destination host unreachable.
Reply from 172.16.2.129: Destination host unreachable.
Reply from 172.16.2.129: Destination host unreachable.

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Por que perdemos a comunicação entre os dispositivos que estão em uma VLAN diferente?