03

Permitindo outros tráfegos

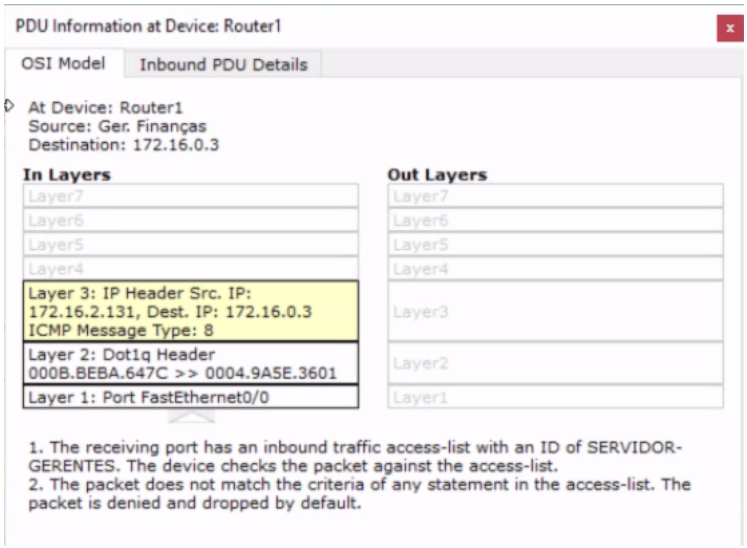
Transcrição

Nesta última etapa, fizemos que somente o servidor fosse acessado pelos gerentes de finanças e pelo gerente de vendas, entretanto a nossa comunicação entre os computadores que estão em VLANs diferentes, acabou sendo comprometida. Vamos entender o porquê.

No modo *Simulation*, realizaremos um **ping** no computador do gerente de finanças para o computador do funcionário de vendas:

```
>ping 172.16.0.3
```

O que chegou no roteador foi o pacote **ICMP**. Se clicarmos nesse protocolo, temos essa imagem:



Na entrada do roteador, temos a lista de acessos, mas essa lista comparou o tráfego com o protocolo ICMP com os dados inseridos. Sabemos que não temos nenhum tratamento para esse protocolo. Por isso, ele não conseguirá passar por não atinge nenhuma das restrições da lista.

Perceba que em nossa lista de acesso, estamos permitindo somente dois tipos de acesso que utilizam o protocolo TCP, cuja a origem está no gerente de vendas e no gerente de finanças para esse servidor. Mas, e todo o resto dos outros protocolos de comunicação? Da maneira como foi configurado, toda a comunicação está perdida!

Então temos que alterar a lista de acessos para permitir todos os outros protocolos de comunicação. O foco da nossa lista de acesso é só o servidor. O restante do tráfego que acontece na rede pode seguir normalmente. Então vamos **remover** a lista de acesso, e criaremos uma nova lista!

```
#configure terminal
#no ip access-list extended SERVIDOR-GERENTES
```

Usando essa linha de comando, conseguimos remover a lista de acessos que criamos. Criaremos uma nova lista de acessos com algumas informações adicionais.

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

Essa nova lista ainda deve manter a permissão do gerente de vendas e de finanças, para que eles acessem o servidor.

```
#permit tcp 172.16.2.131 0.0.0.0 172.16.3.2 0.0.0.0
#permit tcp 172.16.0.2 0.0.0.0 172.16.3.2 0.0.0.0
```

Depois disso, devemos permitir que os outros protocolos estejam habilitados. O comando `#permit` permite TUDO. Então, antes de permitir tudo, precisamos **negar** os outros computadores que estão lá no setor de finanças e do setor de vendas, para que eles não tenham acesso ao servidor.

Primeiro, vamos negar todos os outros computadores de finanças, cujo os endereços se iniciam com `172.16.2. .`

```
#deny tcp 172.16.2.128 0.0.0.255
```

E esses computadores serão negados para acessar o servidor `172.16.3.2` :

```
#deny tcp 172.16.2.128 0.0.0.255 172.16.3.2 0.0.0.0
```

Agora, negaremos os computadores do setor de vendas, seguindo a mesma linha de raciocínio:

```
#deny tcp 172.16.2.128 0.0.0.255 172.16.3.2 0.0.0.0
#deny tcp 172.16.0.128 0.0.0.255 172.16.3.2 0.0.0.0
```

Isto quer dizer que se não for nenhum desses endereços (`172.16.2.131` e `172.16.0.2`), o pacotinho será negado! Feito isso, vamos permitir que os outros protocolos de comunicação trabalhem normalmente:

```
#deny tcp 172.16.2.128 0.0.0.255 172.16.3.2 0.0.0.0
#deny tcp 172.16.0.128 0.0.0.255 172.16.3.2 0.0.0.0
#permit ip any any
```

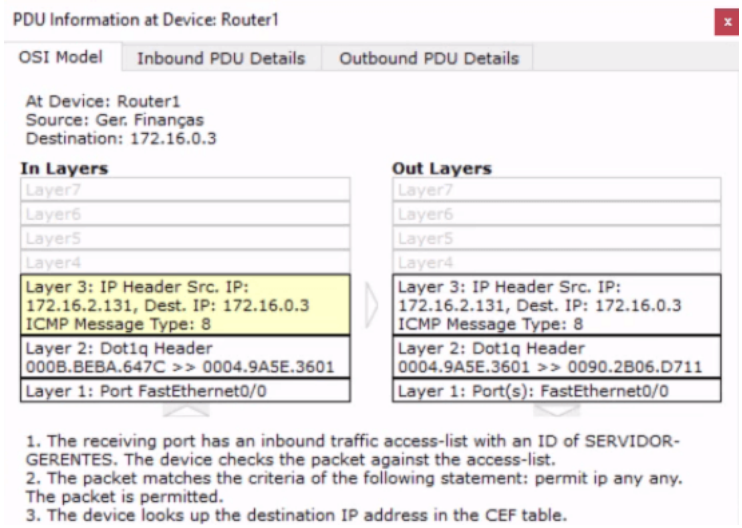
Com o `#permit ip any any` , estamos permitindo qualquer tráfego que não seja destinado ao servidor.

Veremos se o roteador permitirá a comunicação entre VLANs distintas, e permitir o protocolo ICMP de seguir adiante.

No modo *Simulation*, vamos "pingar" novamente o computador do gerente de finanças (VLAN 20), para os funcionários de vendas (VLAN 10):

```
>ping 172.16.0.3
```

Se clicarmos no pacotinho ICMP, teremos a seguinte imagem:



Analisando a imagem, vemos que há um critério que bate com o tráfego do pacote ICMP, que é o `permit ip any any`, pois esse pacote não está sendo destinado ao servidor. Uma vez que colocamos em nossa lista de acessos para ela permitir qualquer coisa, o pacote seguirá adiante.

No modo *Realtime*, conseguimos ver que a comunicação voltou a ser estabelecida!

Mas, será que somente os gerentes de finanças e vendas ainda conseguem acessar o servidor?

Depois de testarmos os quatro computadores da nossa rede, percebemos que somente os gerente de finanças e vendas tem acesso ao servidor!