Packet Tracer – Configuração de ACLs IPv4 nomeadas padrão

Topologia

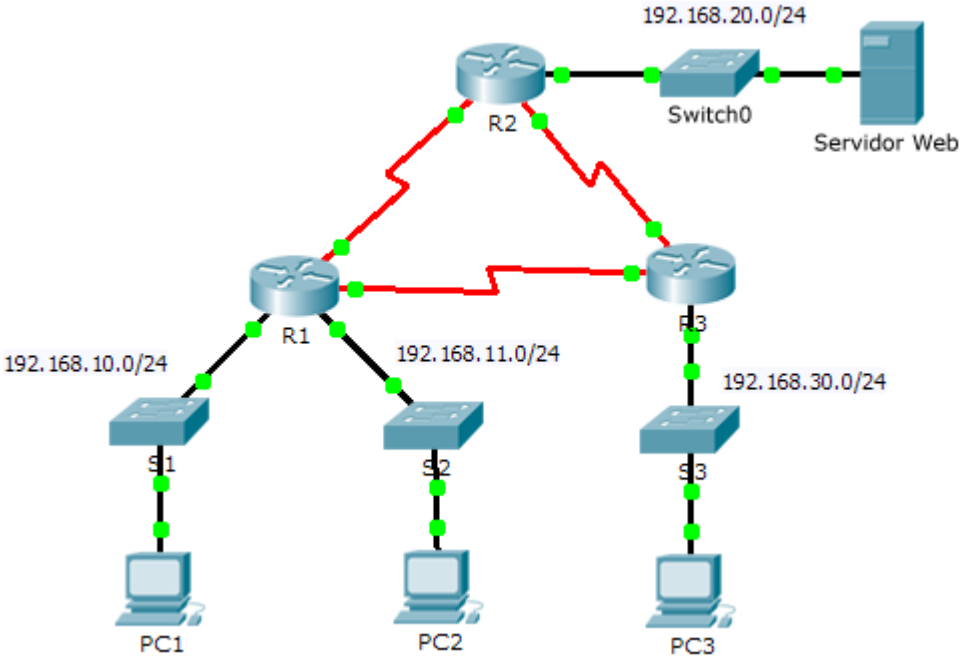

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway Padrão
R1	G0/0	192.168.10.1	255.255.255.0	N/D
	G0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
	S0/0/1	10.3.3.1	255.255.255.252	N/D
R2	G0/0	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
R3	G0/0	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	Placa de rede	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: Planejar uma implementação da ACL

Parte 2: Configurar, aplicar e verificar uma ACL padrão

Histórico/Cenário

As listas de controle de acesso padrão (ACLs) são os scripts da configuração do roteador que controlam se um roteador permite ou nega pacotes com base no endereço origem. Esta atividade se concentra em definir critérios de filtragem, configuração das ACLs padrão, aplicação de ACLs às interfaces do roteador e verificação e teste da implementação da ACL. Os roteadores já estão configurados, incluindo os endereços IP e o roteamento EIGRP (Enhanced Interior Gateway Routing Protocol).

Parte 1: Planejar uma implementação da ACL

Etapa 1: Investigue a configuração atual de rede.

Antes de aplicar qualquer ACL a uma rede, é importante confirmar se você tem conectividade completa. Verifique se a rede tem conectividade completa escolhendo um PC e fazendo ping em outros dispositivos na rede. Você deve poder acessar cada dispositivo com êxito.

Etapa 2: Avalie duas políticas de rede e implementações de ACL do plano.

a. As seguintes políticas de rede são implementadas executadas em **R2**:

- A rede 192.168.11.0/24 não pode acessar o **ServidorWeb** na rede 192.168.20.0/24.
- Todo o acesso restante é permitido.

Para restringir o acesso da rede 192.168.11.0/24 ao **ServidorWeb** em 192.168.20.254 sem interferir com outro tráfego, é necessário criar uma ACL em **R2**. A lista de acesso deve ser colocada na interface de saída para **ServidorWeb**. Uma segunda regra deve ser criada em **R2** para permitir qualquer outro tráfego.

b. As seguintes políticas de rede são implementadas em **R3**:

- A rede 192.168.10.0/24 não pode se comunicar com a rede 192.168.30.0/24.
- Todo o acesso restante é permitido.

Para restringir o acesso da rede 192.168.10.0/24 à rede 192.168.30/24 sem interferir com outro tráfego, será necessário criar uma lista de acesso em **R3**. A ACL deve ser colocada na interface de saída para **PC3**. Uma segunda regra deve ser criada em **R3** para permitir qualquer outro tráfego.

Parte 2: Configure, aplique, e verifique uma ACL padrão

Etapa 1: Configure e aplique uma ACL padrão numerada em R2.

a. Crie uma ACL usando o número 1 em **R2** com uma instrução que negará o acesso da rede 192.168.11.0/24 à rede 192.168.20.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. Por padrão, uma lista de acesso nega todo tráfego que não corresponder a uma regra. Para permitir todo tráfego restante, configure a seguinte instrução:

```
R2(config)# access-list 1 permit any
```

c. Para que a ACL realmente filtre o tráfego, ela deve ser aplicada em algumas operações do roteador. Aplicar a ACL colocando-a para o tráfego de saída na interface Gigabit Ethernet 0/0.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Etapa 2: Configure e aplique uma ACL padrão numerada em R3.

a. Crie uma ACL usando o número 1 em **R3** com uma instrução que negará o acesso da rede 192.168.30.0/24 da rede de **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. Por padrão, uma ACL nega todo tráfego que não corresponda a uma regra. Para permitir qualquer outro tráfego, crie uma segunda regra para a ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Aplicar a ACL colocando-a para o tráfego de saída na interface Gigabit Ethernet 0/0.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```


Etapa 3: Verifique a configuração e a funcionalidade da ACL.

a. Em **R2** e **R3**, insira o comando **show access-list** para verificar as configurações de ACL. Insira o comando **show run** ou **show ip interface gigabitethernet 0/0** para verificar as colocações de ACL.

b. Com as duas ACL estabelecidas, o tráfego de rede é restringido de acordo com as políticas detalhadas na parte 1. Use os seguintes testes para verificar as implementações da ACL:

- Um ping de 192.168.10.10 a 192.168.11.10 é confirmado.
- Um ping de 192.168.10.10 a 192.168.20.254 é confirmado.
- Um ping de 192.168.11.10 a 192.168.20.254 falha.
- Um ping de 192.168.10.10 a 192.168.30.10 falha.
- Um ping de 192.168.11.10 a 192.168.30.10 é confirmado.
- Um ping de 192.168.30.10 a 192.168.20.254 é confirmado.

