PRÁTICA LABORATORIAL 01

Objetivos:

- Criação de Access Control Lists em IOS CISCO

EXERCÍCIOS

Access Control List

A filtragem de pacotes e protocolos permite-nos controlar o tipo de acessos (internos e/ou externos) que circulam na rede Essa filtragem pode ser efetuada através de uma lista de controlo de acessos (ACL Access Control List) num router

As ACL's filtram conteúdos baseados em critérios. Os critérios diferem de acordo com o tipo de ACL. São lidas sequencialmente até encontrar uma linha que faça o match com o pacote IP em análise. Se o match não ocorrer, o pacote é descartado

Podem coexistir várias ACL's num dispositivo, sendo diferenciadas por um número identificador E por ser uma lista, podem existir várias linhas por ACL.

Uma ACL só é processada se aplicada a um interface

- Sentido inbound: a ACL é aplica da aos pacotes que entram no router por esse interface
- Sentido outbound: a ACL é aplicada aos pacotes que saem do router por esse interface

Não podem coexistir várias ACL's no mesmo sentido do mesmo interface, mas pode existir uma em cada sentido.

Como parâmetros de qualquer tipo de ACL temos:

- Permitir (permit) ou negar (deny) o pacote de acordocom os restantes parâmetros
- O endereço ou gama de endereços IP a analisar
- A definição de uma gama de endereços é efectuada com recurso a um par constituído por:
    - um endereço IP base
    - um wildcard

Há vários tipos de ACL's de acordo com o tipo de filtragem pretendida

Dois tipos muito utilizados são as ACL's standard e extended

Os primeiros filtram os pacotes de acordo com o endereço IP origem

Os segundos filtram os pacotes de acordo com vários critérios

- Protocolo (obrigatório)
- IP origem (obrigatório)

- IP destino (obrigatório)
- Serviço (opcional)

ACL standard

Possui um identificador (número) entre 1 e 99 há outros conjuntos de identificadores dependendo da versão do sistema operativo do dispositivo
Filtra com base no endereço IP de origem

Sintaxe

access-list identificador [permit/deny] endereço_ip wild-card [log]

A opção log envia uma mensagem para a consola sempre que houver um match (pode não estar disponível na versão do IOS)

ACL extended

Possui um identificador (número) de 100 a 199

Há outros conjuntos de identificadores dependendo da versão do sistema operativo do dispositivo
Filtra os pacotes baseadas no protocolo, endereço origem, no endereço destino e opcionalmente no serviço (porto)

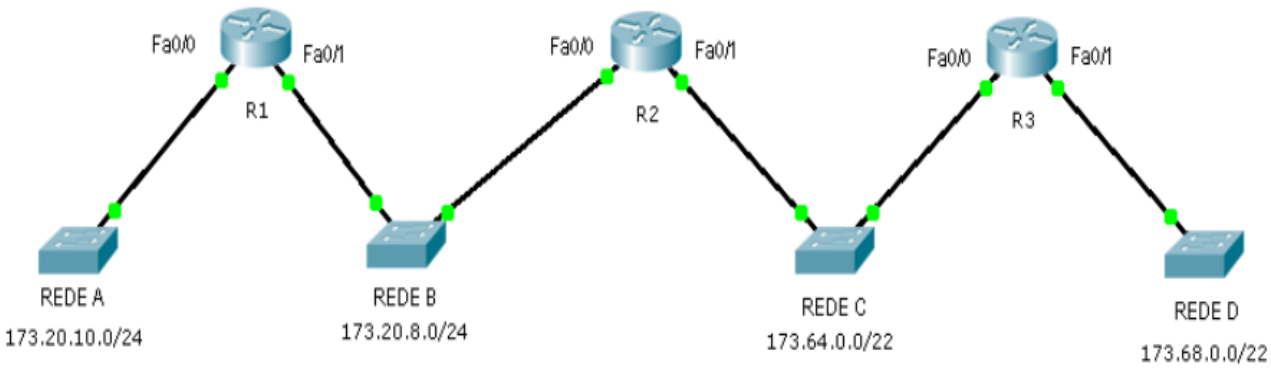
Sintaxe

access-list identificador [permit/deny] protocolo ip_origem wildcard_origem ip_destino wildcard_destino [comparação porto_destino | tipo | [established] [log]

Exemplo:

access-list 100 permit ip any 192.168.0.0 0.0.0.3

1. Quatro redes (A; B; C e D) estão interligadas por três “routers” (R1; R2 e R3) de acordo com o diagrama seguinte:



Escreva os comandos (CISCOIOS) a utilizar nos “routers” para implementaras seguintes regras de acesso:

- A rede A pode enviar para as redes C e D, mas não para a rede B;

- Da rede B, os nós 173.20.8.192 e 173.20.8.208 podem enviar para todas as outras redes, mas os restantes nós da rede B apenas podem enviar para a rede D;

- As redes C e D podem enviar para todas as redes.

Bom trabalho! ☺