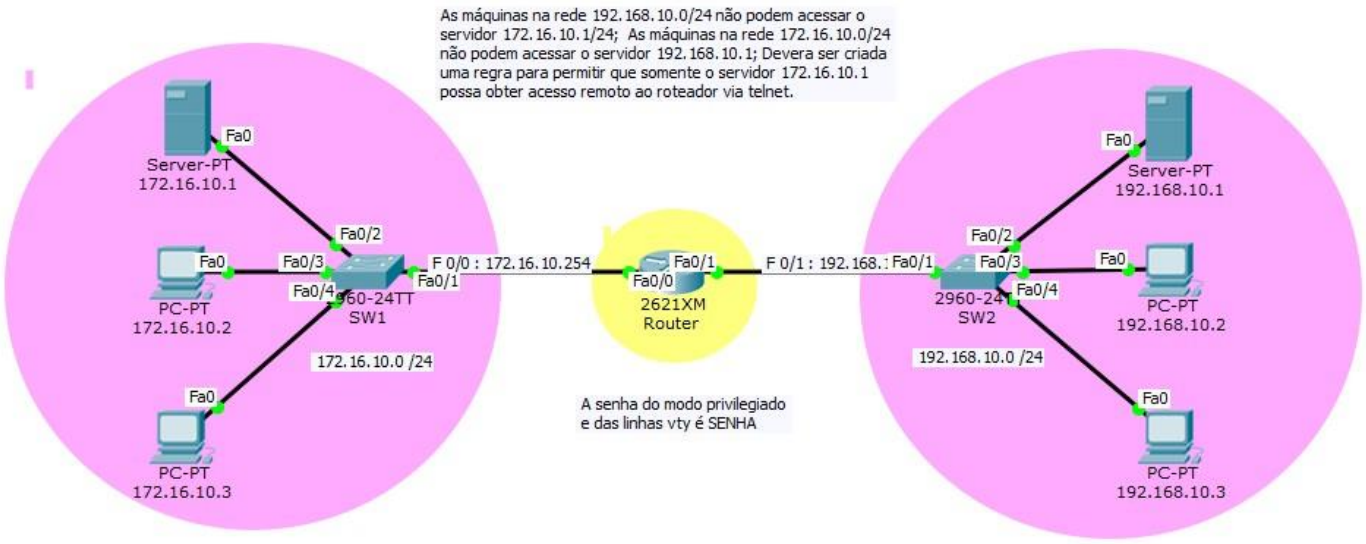

As máquinas na rede 192.168.10.0/24 não podem acessar o servidor 172.16.10.1/24; As máquinas na rede 172.16.10.0/24 não podem acessar o servidor 192.168.10.1; Devera ser criada uma regra para permitir que somente o servidor 172.16.10.1 possa obter acesso remoto ao roteador via telnet.

TRANSFORMANDO UM RETADOR EM UM FIREWALL - CRIANDO ACLs

---

permitindo acesso remoto ao roteador (telnet ou ssl)

line vty 0 15
password SENHA
login
enable secret SENHASECRETA

teste:
telnet <IP DO ROTEADOR>

---

obs: quando aplicamos regras ACL nas linhas vty estamos querendo controlar o acesso remoto.
quando aplicamos as regras ACL nas interfaces estamos querendo controlar o acesso às redes. Cada interface pode ter no máximo duas listas (IN e OUT)

REGRAS DO FIREWALL (ACL)

---

permitir apenas um ip para acesso remoto ao roteador

show access-lists

LISTA PADRÃO para liberação ou bloqueio de acesso remoto ao roteador "linha vty" (BASTA ESPECIFICAR A ORIGEM)
access-lista <1-99 (lista padrão)> <100-199 (lista estendida)>

access-list 10 remark "descrição da lista"

access-list 10 permit ?

access-list 10 permit <origem (que pode ser ANY, host =um IP especifico e uma rede inteira)>

access-list 10 permit 172.16.10.1 0.0.0.0 (wildcard permitindo somente esse IP)

Quando criamos uma regra, automaticamente todos os outros serão bloqueados por padrão e só o que permitimos será liberado.

PARA APLICAR A ACL NAS LINHAS VTY É NECESSÁRIO ENTRAR EM TODAS AS LINHAS E APLICAR A REGRA

line vty 0 15

access-class <numero da lista> <sentido>

access-class 10 in

OBS: ACCESS-CLASS É SO PARA ACESSO REMOTO ----------

CRIAR LISTA ESTENDIDA PARA AS INTERFACES

EXEMPLO: PROIBIR QUE NENHUMA MAQUINA DA REDE 192.168.10.0 ACESSE O HOST 172.16.10.1

access-list 100 deny ?

access-list 100 deny <protocolo> <origem wildcardmask> <destino wildcardmask>

access-list 100 deny IP 192.168.10.0 0.0.0.255 172.16.10.1 0.0.0.0

access-lista 100 permit IP any any (é necessário fazer isso, pois automaticamente um deny all é criada. a ORDEM TEM QUE SER ESSA, O DENY PRIMEIRO E O LIBERA ALL DEPOIS)

EXIT

INT F0/1

IP ACCESS-GROUP 100 IN

---

proibir acesso ao serviço web do 192.168.10.1 com origem na rede 172.16.10.0

IP ACCESS-LIST EXTENDED <NOME DA LISTA**>**

DENY TCP 172.16.10.0 0.0.0.255 192.168.10.1 0.0.0.0 eq <porta ou nome do serviço**>**

DENY TCP 172.16.10.0 0.0.0.255 192.168.10.1 0.0.0.0 eq 80 <ou> **www**

permit ip any any

exit

INT F0/0

IP ACCESS-GROUP <NOME DA LISTA**> IN**