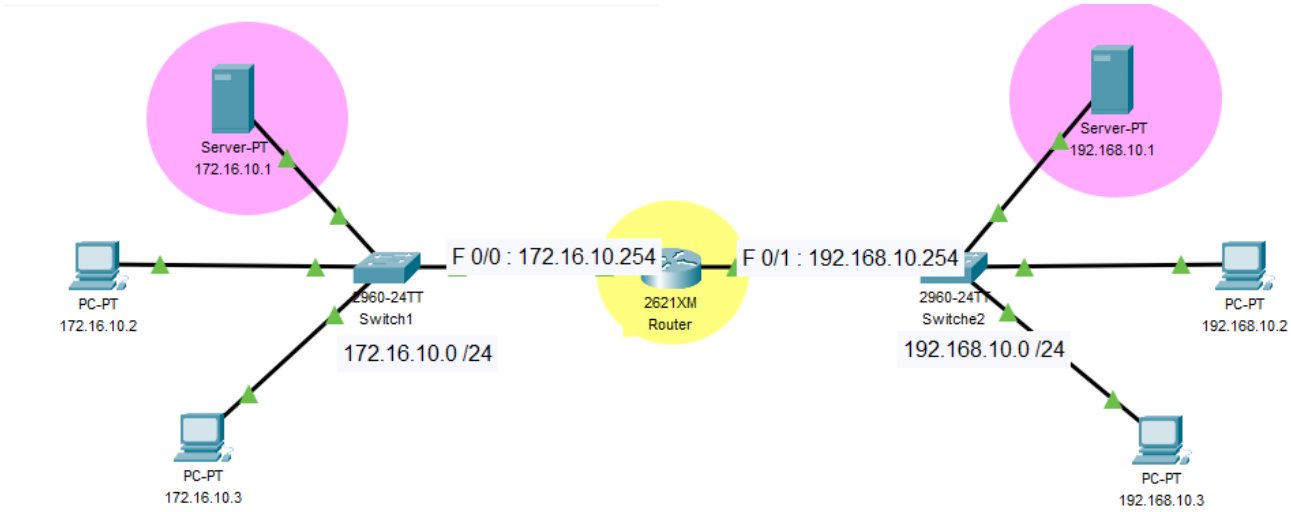
FUNDAÇÃO EDSON QUEIROZ
UNIVERSIDADE DE FORTALEZA
ENSINANDO E APRENDENDO

ACL

Disciplina: Redes Convergentes
Prof: Wellington Alves de Brito
Aluno: Luan M. D. Lima
Matrícula: 1710532
Curso: Engenharia da Computação
Introdução

Introdução

Usando o programa de simulação Packet Tracer deve-se a topologia de rede mostrada abaixo realizar a configuração da rede de forma que as máquinas na rede 192.168.10.0/24 não podem acessar o servidor 172.16.10.1/24 e as máquinas na rede 172.16.10.0/24 não podem acessar o servidor 192.168.10.1; Portanto, deve-se ser criada uma regra para permitir que somente o servidor 172.16.10.1 possa obter acesso remoto ao roteador via telnet.



ACL

Os ACLs Cisco são caracterizados por declarações de permissão/negação única ou múltipla. O objetivo é filtrar pacotes de entrada ou saída em uma interface de rede selecionada. Existem uma variedade de tipos de ACL que são implantados com base nos requisitos. Apenas dois ACLs são permitidos em uma interface Cisco por protocolo. Isso incluiria, por exemplo, uma única ACL ip aplicada de entrada e uma única ACL IP aplicada de saída.
Existem algumas práticas recomendadas ao criar e aplicar listas de controle de acesso (ACL). O administrador de rede deve aplicar uma ACL padrão mais próxima do destino. A instrução ACL padrão é composta por um endereço IP de origem e máscara curinga. Há um número ou nome comum que atribui várias declarações à mesma ACL. ACLs padrão são um tipo mais antigo e muito geral. Como resultado, eles podem filtrar inadvertidamente o tráfego incorretamente. A aplicação da ACL padrão perto do destino é recomendada para evitar possíveis *over-filtering*. A ACL estendida deve ser aplicada mais próxima da fonte. ACLs estendidos são granulares (específicos) e fornecem mais opções de filtragem. Eles incluem endereço de origem, endereço de destino, protocolos e números de porta. A aplicação de ACLs estendidos mais próximos da fonte impede que o tráfego que deve ser filtrado entrelhá-lo. Isso conserva a largura de banda e o processamento adicional necessários em cada roteador de origem para pontos finais de destino.

Conclusão

Aplicanto as técnicas citadas acima o objetivo da prática foi cumprido, objetibo este, de limitar o acesso aos servidores e ao roteador utilizando ACL, através do comando PING e utilização do navegador web emulado nos End Devices pôde-se atestar o mesmo.

Na próxima página seguem respectivamente as respostas do roteador aos diversos comandos SHOW, comandos estes que mostram respectivamente as portas do roteador, as ACLs criadas definindo quais redes tem acesso permitido ou restrito aos servidores e por fim as relações entre as portas do roteador e ACLs criadas.

show run

```
interface FastEthernet0/0
 ip address 172.16.10.254 255.255.255.0
 ip access-group 110 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.254 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
!
ip classless
!
ip flow-export version 9
!
!
access-list 10 permit host 172.16.10.1
access-list 100 deny ip 192.168.10.0 0.0.0.255 host 172.16.10.1
access-list 100 permit ip any any
access-list 110 deny ip 172.16.10.0 0.0.0.255 host 192.168.10.1
access-list 110 permit ip any any
!
```

show ip access-list

```
Router#show ip access-list
Standard IP access list 10
    10 permit host 172.16.10.1
Extended IP access list 100
    10 deny ip 192.168.10.0 0.0.0.255 host 172.16.10.1
    20 permit ip any any
Extended IP access list 110
    10 deny ip 172.16.10.0 0.0.0.255 host 192.168.10.1
    20 permit ip any any
```

show ip interface f 0/0

```
Router#show ip interface f 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 172.16.10.254/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 110
```

show ip interface f 0/1

```
Router#show ip interface f 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.10.254/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 100
```