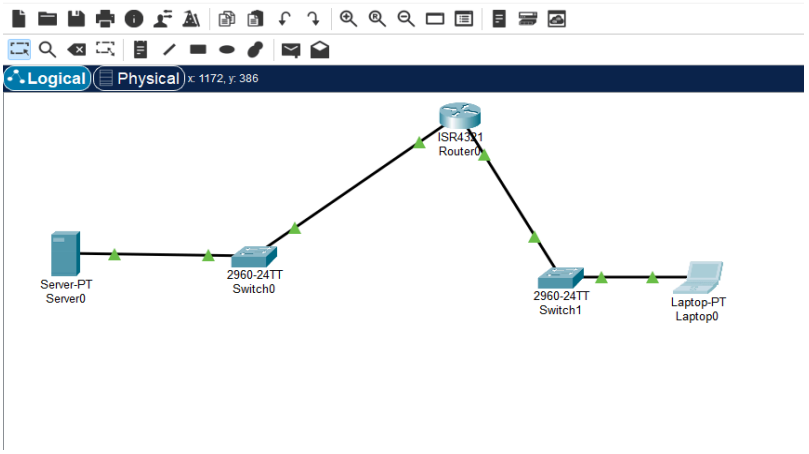
Examen Practico Modulo IV

Daniel Stix Soto

REGLA	IP ORIGEN	ORIGEN/ PROTOCOLO	IP DESTINO	DESTINO/ PROTOCOLO	ACCIÓN
1	10.10.20.10/ 24	ANY/TCP	10.10.10.1/24	80/TCP	ALLOW
2	10.10.20.10/ 24	ANY/TCP	10.10.10.1/24	433/TCP	ALLOW
3	10.10.20.10/ 24	ANY/TCP	10.10.10.1/24	25/TCP	ALLOW
4	10.10.20.10/ 24	ANY/TCP	10.10.10.1/24	ANY OTHER/TCP	DENY

Siguiendo con las especificaciones estipuladas, hemos creado esta tabla de reglas firewalls. Como podemos observar los 3 puertos que nos interesan de HTTP (80), HTTPS (433) y SMTP(25) utilizan el protocolo TCP. La regla n4 explícitamente bloquea todo el tráfico TCP del cliente al servidor hacia cualquier otro puerto, con lo cual no tendrá acceso a ningún otro servicio. Todo esto configurado mediante la interfaz gráfica de CLI en el router.



Estructura en Cisco

```
Press RETURN to get started!


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
```

Interfaces activadas