

Practica No 10  
Planeación y Gestión de Redes  
Universidad Icesi  
Firewall iptables

PROCEDIMIENTO

1. Inicie la maquina Servidor de la empresa
  2. Realice una conexión con la aplicación putty al servidor
  3. Inicie un archivo por medio del siguiente comando
    - a. vi iptables.sh
  4. Cree las siguientes las primeras reglas que son las reglas por defecto

```
#!/bin/bash
iptables -F FORWARD
iptables -P FORWARD DROP
iptables -F INPUT
iptables -P INPUT DROP
iptables -F OUTPUT
iptables -P OUTPUT DROP
```
  5. cambie los permisos del archivo para que pueda ser ejecutable por el usuarios
    - a. chmod 700 iptables.sh
  6. Revise la lista de la reglas actuales cual es su condición?
  7. Ejecute el script creado en los puntos anteriores que comando utiliza para ejecutarlo?
- 
8. Que paso cuando ejecuto el nuevo script?
  9. Revise la condicion de la lista de las reglas vigentes desde la consola del virtual PC.
  10. Hay algún cambio en las reglas listadas anteriormente y que significa ?
- 
- 
11. Ahora cambie de nuevo la política a aceptación por defecto

```
#!/bin/bash
iptables -F FORWARD
iptables -P FORWARD ACCEPT
iptables -F INPUT
iptables -P INPUT ACCEPT
iptables -F OUTPUT
iptables -P OUTPUT ACCEPT
```
  12. Reconecta la aplicación putty
  13. Garantice la conectividad de administración por medio de la siguiente comandos
  14. Agregue al iptables.sh las siguientes líneas

```
#!/bin/bash
iptables -F FORWARD
iptables -P FORWARD DROP
iptables -F INPUT
iptables -P INPUT DROP
iptables -F OUTPUT
iptables -P OUTPUT DROP
iptables -A INPUT -m tcp -p tcp -s <IP_windows> --dport 22 -d
<IP_Empresa> -j ACCEPT
```

```
iptables -A OUTPUT -m tcp -p tcp -s <IP_Empresa> --sport 22 -d  
<IP_Windows> -j ACCEPT
```

15. En este caso que paso con la conectividad de la aplicación putty

---

---

16. verifique de nuevo el listado de reglas vigentes que observa ahora

---

---

17. Por que en las dos ultimas reglas la posición de los IP de las maquinas han cambiado?

---

---

18. Agregue las siguientes lineas al ip

```
iptables -A INPUT -m tcp -p tcp -j LOG  
iptables -A OUTPUT -m tcp -p tcp -j LOG
```

19. vuelva ejecutar el script iptables.sh

20. Compruebe el estado actual de la reglas, nota algún cambio?

---

---

21. Compruebe que esta funcionando el servicio de http

22. Realice una nueva conexión con el Putty y ejecute el siguiente comando

```
tail -f /var/log/messages
```

23. Intente conectar el navegador al servidor de practica

24. Que indica el mensaje que aparece en la nueva Terminal de la aplicación Putty

---

---

25. Que habilitan las dos líneas agregadas al final ?

---

---

26. Habilite las reglas para el acceso al web para toda la subred 192.168.0.0, agregue las líneas al final del archivo

27. Verifique las reglas actuales nota algún cambio con los servicios que el sistema reconoce?

---

---

28. Porque se necesita siempre un conjunto de 2 reglas para especificar un trafico?

---

---

29. En la maquina de Windows ejecute el siguiente comando

- a. Inicio → Ejecutar → cmd
- b. Ping -t <IP\_Empresa>

30. Que pasa con este comando y porque?

---

---

---

31. Agregue las siguientes líneas al script

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT  
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

32. Revise la lista actual de las reglas que pasa si en la reglas no se especifica dirección de origen y de destino?

---

---

---

33. Ejecute el siguiente comando en el fedora de la empresa

a. ping 192.168.130.1

34. Que pasa con este comando y que reglas se deben incluir para que el ping funcione?

---

---

---

35. Una vez complementado este script el cual acepta los servicios específicamente permitidos y niega el resto, cada cuanto piensa usted que se debe ejecutar este comando?

---

---

---

36. Cual de las dos políticas de reglas piensa que en la mejor y mas aplicable para un servidor que da servicio a usuario reales?

---

---

---

---