

ESPACIALIZACION EN TELECOMUNICACIONES
FACULTAD DE ELECTRÓNICA Y ELECTRICA
UNIVERSIDAD INDUSTRIAL DE SANTANDER
EVALUACIÓN TALLER SOBRE IPTABLES

Por favor responder en el espacio correspondiente, de una forma clara y legible. Devolver este documento con los nombres de los integrantes del grupo y la solución a las preguntas, por correo electrónico a mi cuenta: hectorgil@intercable.net.co, antes del miércoles 16 de Marzo de 2005. Tener en cuenta la situación de la gráfica anexa y la siguiente situación:

El ISP les asigno la subred 200.21.238.34 / 28 . El dominio asignado para la empresa principal de Bucaramanga es : capacitacion.edu.co. El servidor DNS registrado en la universidad de los andes para atender ese dominio es fw.capitacion.edu.co, identificado con la IP : 200.21.238.34. Estos responderán a las direcciones públicas citadas en la parte inicial. Se implementará NAT en el firewall (con iptables) , tanto hacia fuera como para acceder los servicios prestados por algunos servidores.

El servidor web, tiene una dirección privada, pero desde internet se debe acceder con una dirección pública (200.21.238.35). El servidor de correo maneja entrega de correo encriptada y desde internet se debe acceder con una dirección pública (200.21.238.36).

Según estos requerimientos, se deben responder las preguntas que a continuación se presentan de forma clara y precisa con el o los comandos apropiados.

Si se recurre a reglas de IPTABLES, escribir la línea exacta para hacer :

- Como permitir que los equipos de la red principal y servidores pueden leer correo de sitios como hotmail, o intercable, o hacer telnet hacia equipos del exterior, pero desde clientes gráficos, como outlook o netscape identificándose con la IP publica del firewall

iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

- El servidor Web interno pueda atender las peticiones que se le hagan a la dirección pública designada para esto?

iptables -t nat -A PREROUTING -p tcp -d 200.21.238.35 --dport 80 -j DNAT --to 192.168.1.4:80

- El servidor de correo pueda atender las peticiones externas que se le hagan clientes gráficos de forma encriptada, a la dirección pública designada para esto?

iptables -t nat -A PREROUTING -p tcp -d 200.21.238.36 --dport 995 -j DNAT --to 192.168.1.3:995

- Permitir el ingreso de todo tipo de tráfico que provenga de la red interna por la tarjeta respectiva.

```
iptables -A INPUT -s 192.168.1.0/24 -i eth0 -j ACCEPT
```

- No deseo permitir que las personas naveguen sin utilizar el proxy. Se debe obligar a que todas las conexiones http pasen por el squid que esta instalado en el firewall

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

- Recibir peticiones externas dirigidas al servidor DNS que reside en el firewall

```
iptables -a input -s 0.0.0.0 -i eth1 -p tcp -dport 53 -j accept  
iptables -a input -s 0.0.0.0 -i eth1 -p udp -dport 53 -j accept
```