UNIVERSIDAD ICESI	**Administración de plataformas y seguridad** **2do Parcial**

En una ciudad no muy lejana, se decidió implementar un sistema de transporte masivo llamado SUYO (Sistema Único Y Ordenado de buses), el cual necesita tener una infraestructura de red inalámbrica y se encuentra implementada en toda la ciudad de "ilac ed ogaitnas". Actualmente el sistema cuenta con 5 buses, cada uno con una dirección IP y están matriculados en un servicio de DNS en la zona suyo.com. y su correspondiente reversa.

Después de dos meses de ajustes y pruebas desde el primer parcial, la red de suyo.com quedó con un esquema de red como el de la Figura 1.

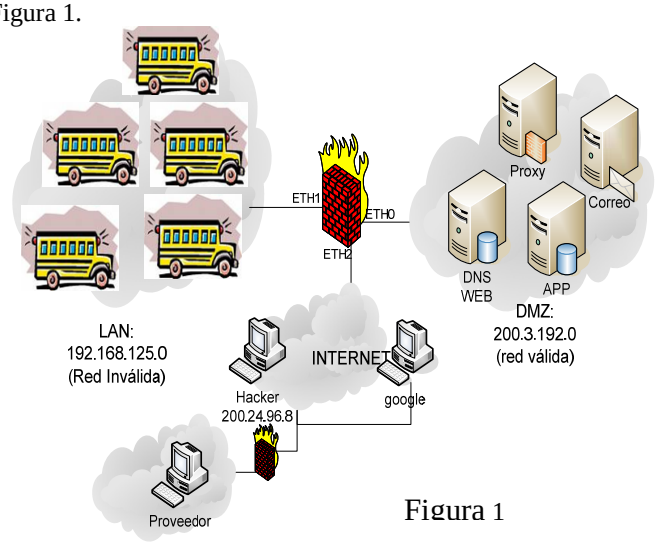

Figura 1

Equipo	SO	MAC	Dirección IP	Servicios	Puerto
Bus01	Fedora	AAFE	192.168.125.11	MSG FTP	TCP/778 TCP 20,21
Bus02	Fedora	A1DE	192.168.125.12	MSG FTP	TCP/778 TCP 20,21
Bus03	Fedora	ABDE	192.168.125.13	MSG FTP	TCP/778 TCP 20,21
Bus04	Fedora	A1FE	192.168.125.14	MSG FTP	TCP/778 TCP 20,21
Bus05	Fedora	A1D3	192.168.125.15	MSG FTP	TCP/778 TCP 20,21
DNS/WEB	Linux	54DA	200.3.192.53	BIND APACHE SSH	UDP/53 TCP 81 TCP/22000
APP	W2K3	45DC	200.3.192.80	IIS TERMINAL	TCP/80 TCP/3805
PROXY	Linux	12AC	200.3.192.21	SSH	TCP22000
CORREO	Solaris	3CE4	200.3.192.25	POSTFIX POP3s	TCP/25 TCP/995
Firewall	Linux	A1E3 A1E4 A1E5	ETH0/200.3.192.55 ETH1/192.168.125.55 ETH2/200.3.193.55	SSH	TCP/22000

El servicio de proxy es prestado a través de un túnel SSH, así que los buses que deseen navegar deben crear este túnel y navegar a través del equipo proxy (usted no es el responsable por la configuración de los clientes)
Los buses cuentan con un moderno sistema de publicidad, el cual le permite a grandes vendedores publicar avisos cuando pasan por sus establecimientos, para esto se debe cceder al bus a través del servicio MSG con la peculiaridad que el puerto fuente **no** es >1024 sino el mismo puerto del servicio, para publicar el servicio en Internet la empresa suyo.com ha adquirido un rango de direcciones válidas: 200.3.193.56:200.3.193.60

PROXY

1. **(Vale 1.2)** Basado en la práctica de túneles SSH y la figura 1, muestre como es la conexión hacia cualquier servicio WEB desde un bus a través del proxy, Las direcciones las puede especificar como: MAC_BUS, IP_PROXY, IP_FW_VAL, PUERTO_WEB. Tenga en cuenta que usted debe especificar el sentido de la conexión, Por ejemplo: Bus → FW

Bus → FW						
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD
MacFuente	MacDestino	IPFuente	IPdestino	Transporte	PF	PD

2. **(Vale 0.8)** ¿Qué significa que un firewall tenga como “default disposition REJECT”?, incluyendo la acción de REJECT (rechazar)

FIREWALL/NAT:

3. **(Vale 3.0)** Basado en la figura 1 y la tabla adjunta, usted debe configurar las siguientes reglas de firewall/NAT, en formato de iptables, con el **default disposition DROP:**

a. **(Vale 0.2)** El servicio DNS debe ser visto desde Internet y desde la red de buses.

b. **(Vale 0.25)**El servicio Web y el servicio de correo (SMTP) deben poderse visualizar desde todas las redes.

c. **(Vale 0.2)**La consulta de correo (POP3s) debe ser permitido exclusivamente desde los buses.

d. **(Vale 0.4)**Todos los equipos de la red pueden navegar hacia Internet, a través del proxy, por medio de los nombres. *Los puertos permitidos para navegar son: 80,8180 y 8080 del protocolo TCP*.

e. **(Vale 0.35)**El bus01 es el único que tiene autorización para navegar directamente a través de todos los puertos 80,443 y todos los puertos >1024

f. **(Vale 0.2)**El Firewall debe tener acceso al puerto 9090 hacia todos los equipos en Internet.

g. **(Vale 0.2)**EL servidor APP debe comunicarse con los buses a través del servicio MSG, para administrar los mensajes de publicidad

h. **(Vale 0.3)**El servicio de CORREO debe tener acceso al DNS y poder enviar y recibir correos hacia y desde Internet.

i. **(Vale 0.35)**El servicio MSG de los buses debe ser accedido desde Internet.

j. **(Vale 0.2)**Sólo el equipo APP debe poder realizar la gestión del Firewall por medio de ssh.

k. **(Vale 0.35)**Se ha detectado que desde el equipo hacker están tratando de vulnerar el sistema de mensajería, por esto usted debe prohibir cualquier conexión desde ese equipo hasta los **buses** las conexiones puerto TCP/445 hacia todas las redes de suyo.com

P	Predecesora	Cadena	Dir IP Fuente	Dir IP Destino	Protocolo	Puerto Fuente	Puerto Destino	IE	IS	Acción	Opcional

Código_____ Nombre:_____ Fecha:_____