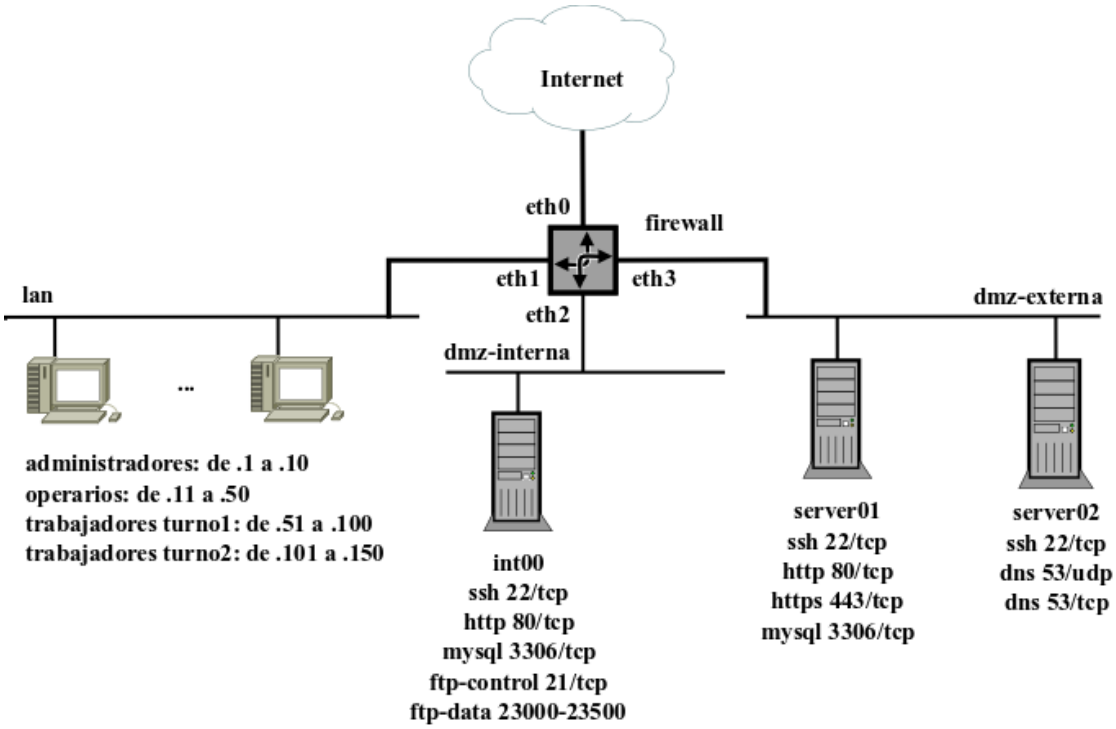
	fw	Operario	server01	int00
IPs Principal	eth0 – 198.51.100.254 /24 eth1 - 192.168.205.254 /24 eth2 - 10.255.255.254 /24 eth3 - 172.27.0.254 /24	192.168.205.11/24	172.27.0.10/24	10.255.255.10 /24
Pasarela	198.51.100.1	192.168.205.254	172.27.0.254	10.255.255.254
Acceso por ssh	sad / magasix	sad / magasix	root / magasix	
DNS	8.8.8.8 y 8.8.4.4			

En base a la infraestructura de la figura:



NETFILTER

Configura el equipo firewall para satisfacer los siguientes requisitos de filtrado:

Consideraciones Generales:

a) Reglas persistentes.
b) Registros con NFLOG.
c) Se trabaja siempre con estados.
d) Las comunicaciones dentro de la organización se harán sin ningún tipo de NAT.
e) Los servicios indicados en la figura corren en los puertos especificados y no se pueden cambiar.
f) Los servicios *públicos* deben ser accesibles por los puertos estándar.
g) El firewall no permitirá ningún otro tipo de tráfico a mayores del indicado (ni equipos ni protocolos). El descarte es no informado y se registra con el prefijo "*TUNOMBRE: CleanUp*".

Firewall:

a) Se permite el tráfico de loopback.

b) Administración por ssh del firewall desde los equipos administradores y desde la IP 198.51.100.1 situada en Internet.
   - Se usará una **cadena de usuario** para controlar este tipo de tráfico.
   - Los intentos de acceso desde equipos no autorizados deben registrarse y rechazarse con descarte silencioso. Para ayudar en la interpretación de los logs se registrará con un prefijo "*TUNOMBRE: ssh fw*"

c) Se permiten resoluciones DNS contra 8.8.8.8 y 8.8.4.4

d) Se permite el acceso a los repositorios oficiales de Ubuntu.

e) No Logging Rule para tráfico 'ruidoso' (broadcast y multicast) de la red lan entrante que se eliminará silenciosamente y sin registarlo. Multicast: 224.0.0.0/4

LAN:

a) El tráfico web se controla con una cadena de usuario:
   - Se permite a los administradores, operarios y trabajadores turno1 visitar páginas web http/https
   - Se permite a los trabajadores turno2 visitar páginas web http/https de lunes a viernes de 07:00 a 17:00 horas.
   - Los intentos de acceso no autorizados deben registrarse y rechazarse con descarte informado de tipo *icmp-admin-prohibited*. Para ayudar en la interpretación de los logs se registrará con un prefijo "*TUNOMBRE: lan web*"

b) Se permite a los administradores, operarios, trabajadores turno1 y 2 hacer resoluciones DNS contra 8.8.8.8 y 8.8.4.4.

DMZ Interna:

a) **int00:**
   - se permite a los equipos de la LAN de la figura acceder al servidor web y a los puertos ftp-control y ftp-data.
   - Se permite a los administradores y operarios accceder al servidor MySQL.

DMZ Externa:

a) **server01:**
   - Se permite el acceso desde cualquier lugar a los servicios http y https.
   - Se permite el acceso por ssh desde los equipos administradores y la IP 198.51.100.1 situada en Internet.

DMZ Interna y Externa:

a) **Sneaky:** todo tráfico no autorizado iniciado desde las DMZs deberá registrarse con prefijo "*TUNOMBRE: Sneaky*" y descartarse silenciosamente.

Documentos a entregar:

a) Fichero de reglas.

b) Desde el equipo anfitrión de los contenedores documenta las siguientes comprobaciones (comandos y salidas):
   - Accedes por ssh al firewall.
   - Accedes por ssh a server01 a través de la Ip pública del firewall.
   - Ejecutas: `curl http://198.51.100.254`