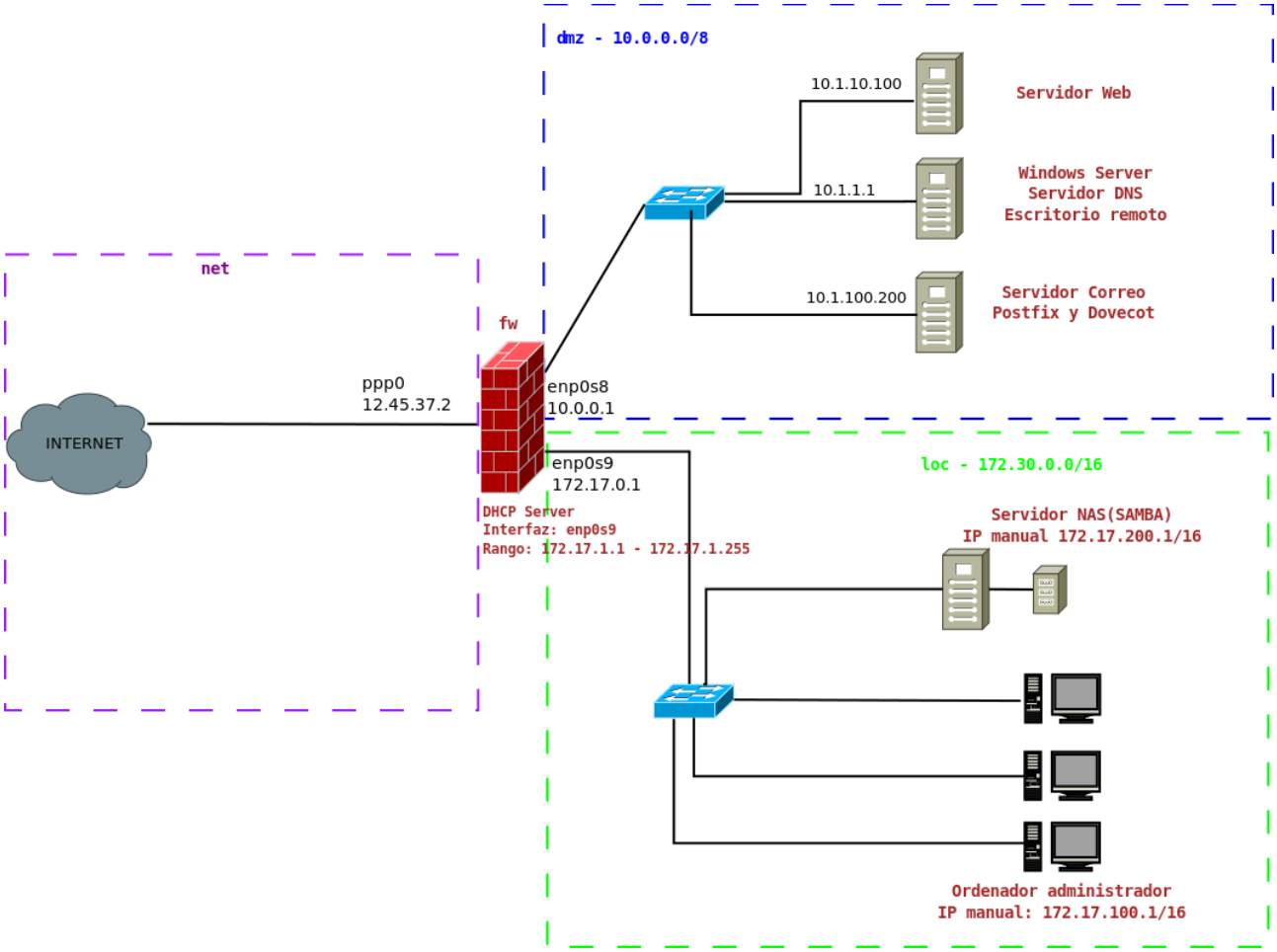
SGF. IES Haría
UT5. AER2TP1. Recuperación 2
Supuesto teórico práctico

Seguridad en redes locales

A partir del siguiente esquema de red de la empresa con dominio **cartrash.com**



Teniendo en cuenta que:

1) en el equipo firewall tiene instalado el sistema operativo Ubuntu Server y el software shorewall el contenido actual de los ficheros es el siguiente:

/etc/shorewall/zones

```
fw firewall
net ipv4
loc ipv4
dmz ipv4
```

/etc/shorewall/interfaces

```
net ppp0 detect tcpflags,routefilter,nosmurfs,logmartians,blacklist
loc enp0s9 detect dhcp,tcpflags,nosmurfs,blacklist
dmz enp0s8 detect tcpflags,nosmurfs,blacklist
```

/etc/shorewall/policy

```
loc net ACCEPT
net all DROP info
all all REJECT info
```

/etc/shorewall/masq

```
        ppp0 enp0s9
        ppp0 enp0s8
```

/etc/default/shorewall

```
        ...
        startup=1
        ...
```

/etc/shorewall/shorewall.conf

```
        ...
        IP_FORWARDING=Yes
        ...
```

2) Los dispositivos de red de todos los equipos de la empresa están correctamente configurados.

3) Cada uno de los servicios de los servidores de la zona dmz indicados en el esquema están iniciados y configurados de forma completa, incluyendo registros de DNS necesarios.

4) Para el dominio `cartrash.com` hay creados registros A de DNS para los nombres `www.cartrash.com`, `servidor.cartrash.com` y `cartrash.com` todos ellos apuntando a la IP pública del firewall `12.45.37.2` y un registro `mail.cartrash.com` apuntando a `15.16.17.18`

Contesta a las siguientes cuestiones indicando para cada una de ellas:

- Los ficheros de configuración que hay que editar.
- El contenido de los mismos que se va a añadir/modificar
- Los comandos que habría que ejecutar.
- Las acciones a realizar para comprobar el funcionamiento indicando:
  - Equipo desde el que se haría la comprobación
  - Programa cliente a utilizar
  - Dirección introducida en el cliente
  - Comportamiento esperado

1. Poder hacer pruebas de conectividad (ejecutar ping) desde el equipo cortafuegos a cualquier otro equipo de la empresa.

```
PING(ACCEPT) fw dmz
PING(ACCEPT) fw loc
```

Comprobación:
Obtener respuesta al ejecutar desde el equipo cortafuegos

```
$ ping 10.1.1.1
$ ping 10.1.10.100
$ ping 172.17.200.1
```

2. Todos los equipos de la organización **sólo** puedan utilizar como servidor de DNS el que tiene dirección IP `10.1.1.1` y el servicio funcione correctamente (resuelva para las zonas de la red local

y para Internet)

```
DNS(ACCEPT) loc dmz:10.1.1.1
DNS(ACCEPT) fw dmz:10.1.1.1
DNS(ACCEPT) dmz:10.1.1.1 net
DNS(REJECT) loc net
```

Comprobación

Ejecutar desde cualquier equipo de la organización

```
$ dig @10.1.1.1 rediris.es +short ← obtener respuesta
$ dig @8.8.8.8 rediris.es +short ← No obtener respuesta
```

3. Acceso al servidor NAS utilizando el protocolo de compartición de archivos y carpetas SAMBA(SAMBA utiliza los puertos TCP 137, 138, 139 y 445) desde cualquier ordenador de la organización

```
ACCEPT fw loc:172.17.200.1 tcp 137
ACCEPT fw loc:172.17.200.1 tcp 138
ACCEPT fw loc:172.17.200.1 tcp 139
ACCEPT fw loc:172.17.200.1 tcp 445
ACCEPT dmz loc:172.17.200.1 tcp 137
ACCEPT dmz loc:172.17.200.1 tcp 138
ACCEPT dmz loc:172.17.200.1 tcp 139
ACCEPT dmz loc:172.17.200.1 tcp 445
```

4. Acceder a la web de la empresa

a) Desde cualquier equipo conectado a Internet

```
DNAT net dmz:10.1.10.100 tcp 80

Comprobación:
```

Desde equipo conectado a internet introducir la dirección `http://www.cartrash.com` y cargar la web de la empresa

b) Desde cualquier equipo de la red 172.17.0.0/16

```
HTTP(ACCEPT) loc dmz:10.1.10.100

Comprobación:
```

Desde equipo conectado a internet introducir la dirección `http://10.1.10.100` y cargar la web de la empresa

5. La empresa tiene configurado un servidor de correo (10.1.100.200) para el dominio **`cartrash.com`** Dicho servidor de correo ejecuta un servidor de **SMTP** a la escucha por el puerto

465 y un servidor **IMAP** a la escucha por el puerto **993**.

Indicar los **pasos necesarios en el cortafuegos** y las **direcciones** y **puertos** en el cliente de correo del equipo para el **correo saliente** y/o para el **correo entrante**.

a) Configurar en un equipo conectado a la red 172.17.0/16 una cuenta de correo del dominio **`cartrash.com`**

```
ACCEPT loc dmz:10.1.100.200 smtp 465
ACCEPT loc dmz:10.1.100.200 imap 993

IN: 10.1.100.200 993
OUT:  10.1.100.200 465
```

b) Configurar, en un equipo conectado a Internet externo a la empresa, un cliente de correo para poder envíar y recibir correo de la empresa

```
DNAT net dmz:10.1.100.200 tcp 465
DNAT net dmz:10.1.100.200 tcp 993

IN: mail.cartrash.com 993
OUT: mail.cartrash.com 465
```

6. Suponiendo que el servidor web (`10.1.10.100`) tiene habilitado el servicio de ssh **22**.

a) Pasos para poder acceder por **ssh** al servidor web sólo del equipo del administrador de la red (`172.17.100.1`)

```
SSH(ACCEPT) loc:172.17.100.1 dmz:10.1.10.100

Comprobación:

Ejecutar ssh 10.1.10.100 en equipo administrador de la red y conectar
Ejecutar ssh 10.1.10.100 en equipo cualquier otro equipo red loc y no conectar
```

b) Acceder por **ssh** al servidor web desde cualquier equipo conectado a Internet al servidor Windows poniendo como dirección **`servidor.cartrash.com:3344`**

```
DNAT net dmz:10.1.100.200:22 tcp 3344

Comprobación:

Ejecutar ssh servidor.cartrash.com:3344 en equipo de internet y conectar
```

7. Desde el equipo servidor Web pueda descargar el gestor de contenidos wordpress ejecutando **`wget http://download.wordpress.org/wordpress.tar.gz`**

```
ACCEPT dmz:10.1.10.100 net tcp http
```

Comprobación:

Ejecutar `wget http://download.wordpress.org/wordpress.tar.gz` en servidor web y descargar dicho archivo