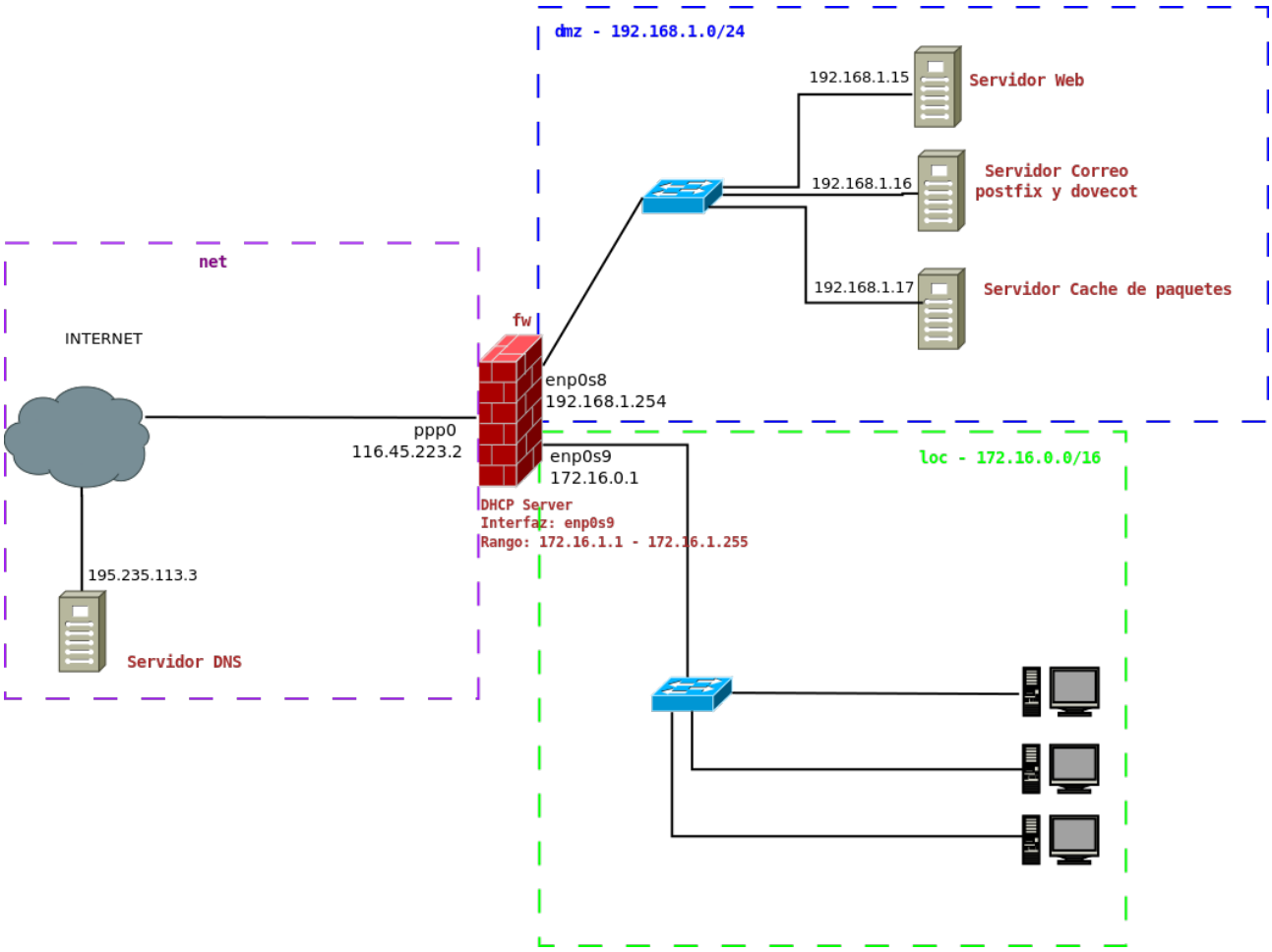
SGF. IES Haría
UT5. Supuesto teórico práctico

Supuesto teórico práctico

Seguridad en redes locales

A partir del siguiente esquema de red de la empresa con dominio **carrental.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 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
```

/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 `carental.com` hay creados registros A de DNS para los nombres `www.carental.com`, `mail.carental.com`, `server.carental.com` y `carental.com` todos ellos apuntando a la IP pública del firewall `116.45.223.2`.

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

Ejemplo resuelto:

Si tenemos en el equipo cortafuegos un servidor de DHCP instalado y configurado para servir configuraciones de red a los equipos conectados a la red 172.16.0.0/16. ¿Qué pasos tendríamos que dar para que funcione?

Editar en el equipo cortafuegos el fichero **/etc/shorewall/interfaces** y modificar la línea:

```
loc enp0s9 detect tcpflags,nosmurfs,blacklist
```

De forma que quede

```
loc enp0s9 detect dhcp,tcpflags,nosmurfs,blacklist
```

Reiniciar el cortafuegos ejecutando

```
sudo shorewall restart
```

En un equipo conectado a la zona **loc** tratar de obtener la configuración de la red por DHCP

```
sudo dhclient -r eth0
sudo dhclient -v eth0
```

El equipo debería obtener los parámetros de red de forma automática

1. Todos los equipos de la organización **sólo** puedan utilizar como servidor de DNS el que tiene dirección IP 195.235.113.3

2. Suponiendo que el servidor web tiene el servicio **ssh** a la escucha por el puerto **22**.

a) Pasos para poder acceder por ssh al servidor web desde cualquier equipo de red 172.16.0.0/16, excepto del que tiene la dirección IP 172.16.1.55

b) Acceder por ssh desde cualquier equipo conectado a Internet al servidor web

3. Uso del servidor de cache de paquetes, a la escucha por el puerto 3142, para instalar software desde cualquier equipo de la organización

4. Acceder a la web de la empresa desde cualquier equipo conectado a Internet y desde cualquier equipo de la red 172.16.0.0/16

5. Teniendo en cuenta que en el equipo servidor de correo **Postifx** ejecuta un servidor de **SMTP** a la escucha por el puerto **465** y **Dovecot** un servidor **IMAP** a la escucha por el puerto **993**. Y que, aparte de especificar los pasos necesarios en el cortafuegos, se han de indicar los las **direcciones** y **puertos** en el cliente de correo del equipo para el **correo entrante** y para el **correo saliente**.

a) Configurar en un equipo conectado a la red 172.16.0.0/16 una cuenta de correo del dominio **`carrental.com`**

b) Configurar en cualquier equipo conectado a Internet una cuenta de correo del dominio **`carrental.com`**

6. Si en el equipo cortafuegos está realizado la configuración inicial de squid como proxy de la red 172.16.0.0/16 a la escucha por el puerto 3128. Pasos para que funcione en modo transparente.

7. Poder hacer pruebas de conectividad (ejecutar ping) desde cualquier equipo de la red 172.16.0.0/16 a cualquier otro equipo de la empresa.