SWAP

CONFIGURACIÓN DE DMZ CON FIREWALL IPCOP

Juan Antonio Martín Quirós y Guillermo Muriel Sánchez lafuente

Introducción

A partir del cortafuegos IPCop y utilizando máquinas virtuales, simularemos una instalación con varias subredes. Tendremos que configurar una DMZ en la que se situaran los servidores, una subred en la que estarán las estaciones de trabajo y además dispondremos de otra subred para acceso wifi.
La red con las estaciones de trabajo debe quedar inaccesible desde cualquier otra red.
Dispondremos de los siguientes servidores: web, mysql, ftp

¿Qué es IPCOP?

IPCo es uno de los mejores cortafuegos basados en Linux, que nos permite gestionar el acceso a Internet, controlar de acceso a páginas mediante un filtrado URL, con lo que podemos evitar que nuestros usuarios ingresen a determinados sitios web (sexo, violencia, facebook, etc.)

Requiere un hardware dedicado, pero de muy bajos requerimientos (32 MB en RAM y un procesador 386 y unos 300MB en disco duro) cuenta con una interfase de usuario web lo que facilita mucho la administración del mismo.

Interfaces o zonas

IPCOP consta de 4 zonas que se describen a continuación:

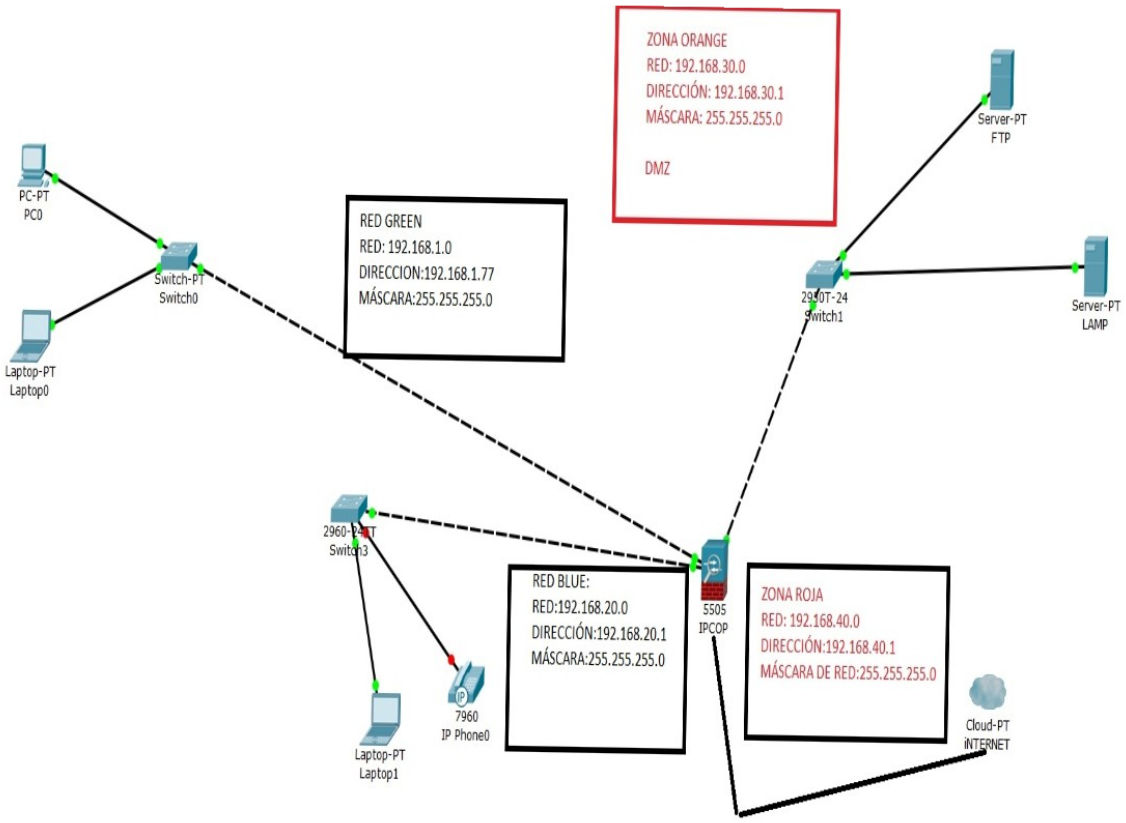
GREEN: Estos son los equipos que necesitan mayor proteccion. Los dispositivos que estén conectados a esta interfaz no tendrán acceso a las interfaces RED, BLUE o ORANGE, es decir no que podrán conectarse a Internet y tampoco podrán podrán conectarse a equipos que se encuentren en las otras interfaces,

BLUE: Generalmente se la utiliza para redes inalámbricas aquí se conecta nuestro Access Point aunque también se puede conectar una red no inalámbrica, los dispositivos que estén en esta red no podrán iniciar conexiones con equipos en la red GREEN pero si con la red ORANGE.

ORANGE: Esta es la interface que se utilizará para montar una DMZ o zona desmilitarizada. Principalmente se utiliza para montar servidores web, de correo, de ftp, etc. que deban tener presencia en Internet; o sea que sean accesibles desde Internet, pero que en el caso que se produzca alguna intrusión a algún equipo de esta red, eso no comprometa la seguridad de nuestra red interna (GREEN). Los equipos que formen parte de la red ORANGE no podrán iniciar conexiones a ninguno de los dispositivos que se encuentren en las interfaces GREEN y BLUE. No es necesario activar esta interface en una instalación de IPCop si no utilizamos una DMZ.

RED: Por esta interfaz nos conectaremos a nuestro proveedor de Internet o al acceso a Internet que tengamos.

Diagrama de la red



Información detallada de la red.

Zona Green:

RED:192.168.10.0

MASCARA:255.255.255.0

PUERTA DE ENLACE:192.168.10.254

DNS :192.168.10.254, 8.8.8.8

DHCP:192.168.10.100-120

Zona Blue:

RED:192.168.20.0

MASCARA:255.255.255.0

PUERTA DE ENLACE:192.168.20.254

DNS :192.168.20.254, 8.8.8.8

DHCP:192.168.20.100-200

Zona Orange:

RED:192.168.30.0

MASCARA:255.255.255.0

PUERTA DE ENLACE:192.168.30.254

DNS :192.168.30.254, 8.8.8.8

DHCP:DESACTIVADO

SERVIDORES:WEB:192.168.30.203

FTP:192.168.30.201

MYSQL:192.168.30.202

Zona Red:

RED:192.168.1.0

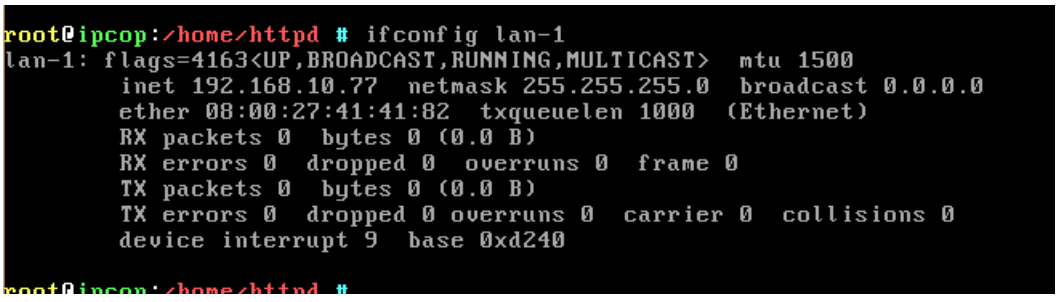
MASCARA:255.255.255.0

PUERTA DE ENLACE:192.168.1.254

DNS :192.168.1.254, 8.8.8.8

Configuración de red en IPCOP

RED GREEN



RED BLUE

```
root@ipcop:/home/httpd # ifconfig wlan-1
wlan-1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.10  netmask 255.255.255.0  broadcast 0.0.0.0
        ether 08:00:27:63:bf:4b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 11  base 0xd260

root@ipcop:/home/httpd # _
```

RED ORANGE

```
root@ipcop:/home/httpd # ifconfig dmz-1
dmz-1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.20  netmask 255.255.255.0  broadcast 0.0.0.0
        ether 08:00:27:46:dd:ee  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 11  base 0xd280

root@ipcop:/home/httpd # _
```