



Laboratorio 02: "Seguridad y VPN"

1 Objetivos

- Aplicar reglas de filtrado en un firewall GNU/Linux.
- Implementación de un acceso remoto mediante VPN.

2 Preparación previa

2.1 Configuración de red en GNU/Linux

Se deben conocer los siguientes puntos:

- Uso de comando ifconfig y route para configuración red IPv4.
- Uso de iptables para realizar NAT y PAT.

2.2 Configuración OpenVPN

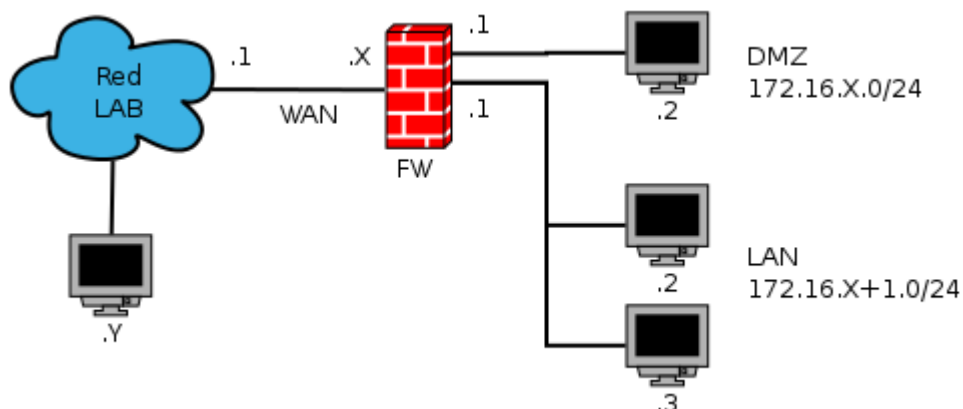
Se deben investigar los siguientes puntos:

- Comándo openssl para crear certificados digitales para OpenVPN.
- Revisar opciones del archivo de configuración en anexo 6.1

2.3 Revisión actividades de laboratorio

Estudiar el punto 4 y como se implementan en GNU/Linux.

3 Topología





4 Actividades en el laboratorio

4.1 Configuración reglas de filtrado – utilizando iptables

- LAN → WAN
 - Puertos TCP 53, 80 y 443.
 - Puerto UDP 53.
- DMZ → WAN
 - Puertos TCP 53 y 80.
 - Puerto UDP 53.
- LAN → DMZ
 - Puerto TCP 80 de máquina .2
 - PC .2 puerto TCP 22 de máquina .2
- DMZ → LAN
 - Nada (excepto lo de la nota).
- WAN → LAN
 - Nada (excepto lo de la nota).
- WAN → DMZ
 - Puerto TCP: 80 máquina .2
- INPUT
 - PC .2 puerto TCP 22.

Nota: se debe definir política por defecto como DROP, se debe permitir ping y todas las conexiones ya establecidas en cualquier dirección (nuevas se rechazan por defecto).

4.2 Configuración VPN Roadwarrior – utilizando openvpn

- Instalación de openvpn en el firewall y configuración roadwarrior (ver anexo 6.1).
- Crear certificados digitales para clientes (con uno basta).
- Instalación de cliente openvpn en máquina laboratorio (.Y).



5 Informe laboratorio

Se deberá entregar un informe (escrito a mano en hoja cuadernillo cuadrado) al finalizar el laboratorio con los pasos realizados para cumplir las actividades (punto 4).

6 Anexos

6.1 Ejemplo configuración servidor openvpn para roadwarrior

```
port 1194
proto udp
dev tun1
persist-tun
keepalive 10 60
user nobody
group nogroup
persist-key
status /var/log/openvpn-roadwarrior-status.log
log /var/log/openvpn-roadwarrior.log
verb 5
ca /etc/openvpn/cert/cacert.pem
cert /etc/openvpn/cert/roadwarrior.crt
key /etc/openvpn/cert/roadwarrior.key
dh /etc/openvpn/cert/dh1024.pem
# red para los clientes
server 172.16.255.0 255.255.255.0
# rutas que se entregaran a los clientes
push "route 172.16.0.0 255.255.255.0" # LAN
push "route 172.16.1.0 255.255.255.0" # DMZ
push "route 172.16.255.0 255.255.255.0" # Clientes
```