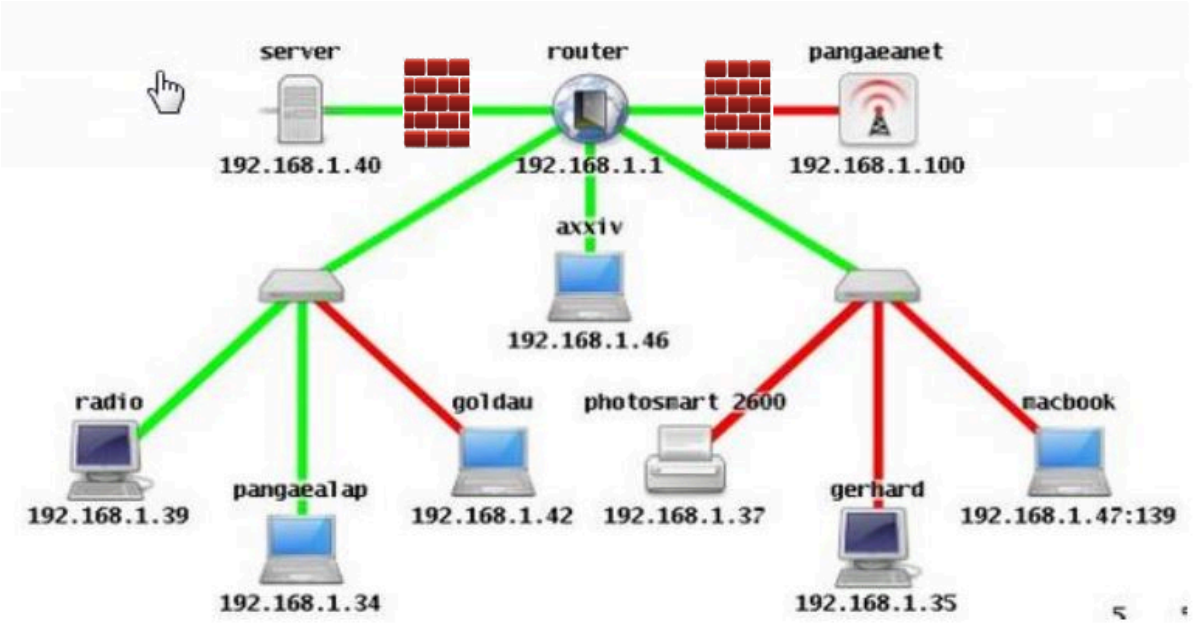
1-



Con los firewall ahi me parece que puedo controlar todo el trafico hacia el servidor y la antena. Puedo armar listas de Qos para que controlar las prioridades de trafico por ip

2.1-
access-list 100 permit ip host 10.20.20.50 host 10.10.10.51
access-list 100 permit ip host 10.20.20.50 host 10.10.10.50

2.2-

access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 101 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 102 permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 103 permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255

3-

1- Realizar un relevamiento
.Tenemos un Switch Principal
.Red de clientes remotos que pasan por un firewall.
.Red de impresoras.
.Servidor de aplicaciones.
.Servidor windows de Storage.
.Servidor windows business con un dispositivo de backup y un fax modem.
.Red de Pc de clientes con Scanner.
.Modem para una red de Wifi.

2- Determinar (improvisando) qué dispositivos se consideran proteger
La prioridad la tendrian los servidores, el dispositivo de backups
Tambien podria restringir los accesos de los clientes y la red de wifi e isp

3- Chequear si se encuentran bien posicionados dentro de la topología
Si, me parece que si.

4- Aplicar más medidas de seguridad si hicieran falta
Podria agregar listas acl para restringir los accesos de los clientes, tambien algun dispositivo de backup para el servidor de storage, si es que no comparten el que esta conectado al servidor de buisness, y el de aplicaciones supongo que necesitaria backups dependiendo del tipo de aplicaciones, si la informacion que tengan se guarda internamente o en una base externa.

5- ¿En caso de que se caiga la red, tengo alguna medida de backup?
Tengo backups conectado al servidor de business, no se si este resguardara la informacion solo de ese servidor o del resto tambien.