DISICO

Vlan + Nat en FreeBSD

Manual

Vlan + Nat en FreeBSD

Debido a la necesidad de segmentación de los distintos laboratorios se realiza esta por medio de Vlan en switch administrables 3com 4500, cada uno de estos realiza troncales que permiten dar conectividad a los equipos ubicados en los distintos laboratorios en este caso son 5, a continuación se describe la configuración realizada en un servidor con sistema operativo FreeBSD el cual entrega la conectividad hacia el exterior por medio de NAT.

Descripción

Para clarificar la configuración realizada se presenta el esquema implementado en la Figura 1, donde se aprecian los dispositivos y las redes que se requieren enrutar por medio de NAT hacia el exterior.

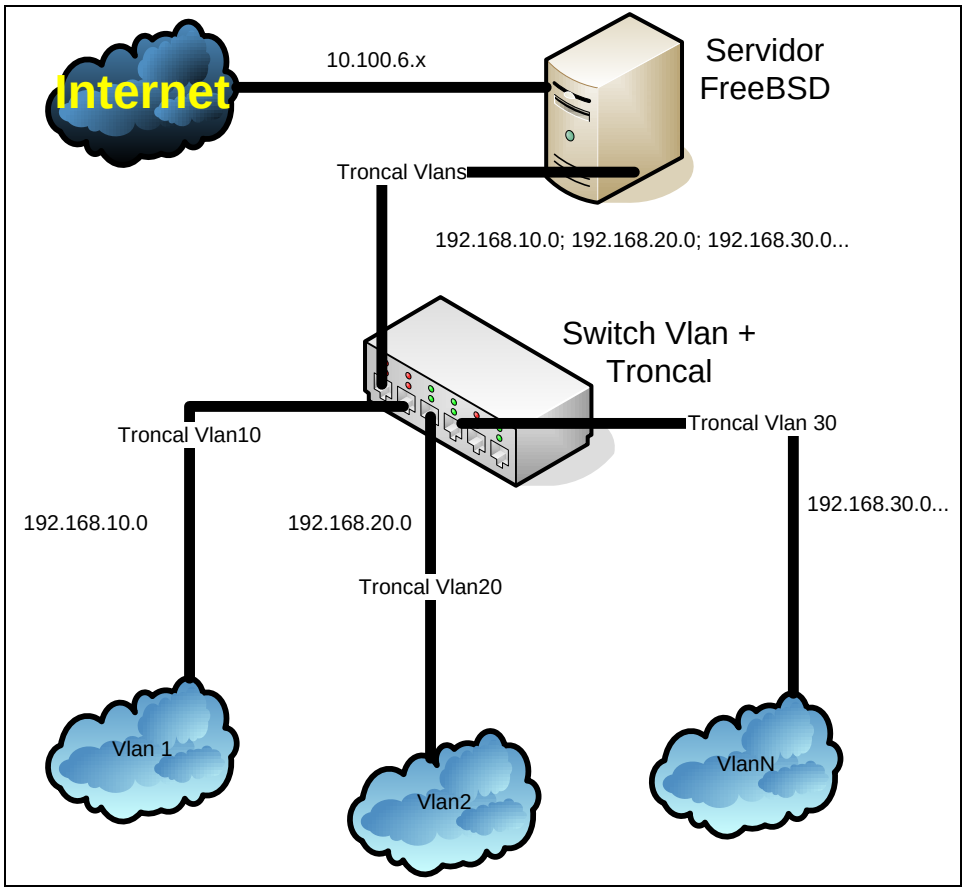

Figura 1

Como se aprecia en la figura 1 la navegabilidad de las distintas Vlans es realizada por medio de troncales configurados en el switch, para lograr realizar la conectividad de toda la red es utilizado un servidor que esta configurado con el sistema operativo FreeBSD en su versión 6.2, es este equipo el que permite reunir todas la vlan y realizar el nat entre la red publica y las distintas redes privadas, para realizar este proceso es necesario realizar una serie de configuraciones en el servidor.

Un punto importante es que posterior a la configuración es el servidor quien se convierte en la puerta de enlace de cada una de las redes privadas configuradas en las distintas Vlan.

Configuración del Servidor

Una vez instalado y actualizado el sistema operativo FreeBSD en su versión 6.2 se debe realizar lo siguiente:

1. Modificar el Kernel

Para modificar el kernel es necesario primero copiar el código fuente que viene por defecto para esto se debe realizar lo siguiente

```
# cd /usr/src/sys/i386/conf/
# cp GENERIC MIKERNEL
```

Posterior a esto editamos MIKERNEL con el comando vi y agregamos las líneas como se describe a continuación

Editamos con:
```
# vi MIKERNEL
```

Y se agrega lo siguiente

```
options     BRIDGE                                  # linea alternativa
options     IPFIREWALL                              # Activa firewall ipfw
options     IPDIVERT                          #permite NAT con ipfw
options     IPFIREWALL_VERBOSE
options     IPFIREWALL_VERBOSE_LIMIT
options     IPFIREWALL_DEFAULT_TO_ACCEPT
options     DUMMYNET   #permite realizar adminstracion de ancho de banda
device      apic       # I/O APIC
device      miibus          #aunque es alternativo permite dar maor soporte a las
tarjetas de red
device      vlan            # permite generar soporte de Vlan con FreeBSD
```

Una vez ingresadas estas lineas sólo basta con guardar el archivo con los cambios esto depende del editos si se utilizó vi para esto se debe seguir la secuencia de

Esc :wq!

Con esto ya estamos listos para compilar el nuevo kernel, paras esto es necesario realizar los siguientes pasos:

```
# /usr/sbin/config MIKERNEL
# cd ../compile/MIKERNEL
# make depend
# make
# make install
```

Con esto ya se encuentra instalado el Nuevo Kernel del sistema operativo solo basta con reiniciar el servidor.

2. Crear las Vlan

Para crear las Vlan que sean necesarias los pasos a seguir son muy sencillos sólo basta con modificar el archivo rc.conf el cual se encuentra en /etc, para esto seguimos los siguientes pasos

```
# cd /etc
# vi rc.conf
```

Una vez abierto agregamos las siguientes lineas:

```
cloned_interfaces="vlan10 vlan20 vlan30"
ifconfig_vlan10="inet 192.168.10.1 netmask 255.255.255.0 vlan 10 vlandev em0"
ifconfig_vlan20="inet 192.168.20.1 netmask 255.255.255.0 vlan 20 vlandev em0"
ifconfig_vlan30="inet 192.168.30.1 netmask 255.255.255.0 vlan 30 vlandev em0"
ifconfig_em0="up"
```

Posteriormente solo vasta con reiniciar el servidor. Un punto importante es que la conectividad ocurre solo si la interfaz em0 se conecta a un troncal configurado del cual provengan las vlan, las que deben tener especificados los mismos números que se encuentran anterior a vlandev

3. Nat

Para esto utilizamos el demonio Natd que trabaja con la opcion IPDivert en conjunto con IPFIREWALL, ambos ya se encuentran instalados al realizar la recompilación del KERNEL.

```
firewall_enable="YES"
firewall_type="OPEN"
natd_enable="YES"
natd_interface="fxp0"
natd_flags="-f /etc/natd.conf"
```

Con estas líneas lo que estamos indicando es primero se habilita el demonio del ipfirewall, luego indicamos que su configuración es del tipo OPEN, posteriormente se inicia el demonio natd, y se indica que este esta en la interfase fxp0 siendo esta interfaz la interna o mejor dicho la privada, y se habilitan todas las configuraciones especiales en el archivo /etc/natd.conf.

Para dar mayores restricciones a la posibilidad de navegabilidad de la red privada a la red publica es necesario crear reglas de firewall, estas se realiza de la misma forma como ya se encuentran documentadas en otros tutoriales.

Por otro lado si es necesario realizar algún tipo de redireccionamiento ya sea de IP o de puerto, esto se debe ubicar en el archivo /etc/natd.conf donde se indica por medio de dos comandos redirect_addres en caso de reuquerir redireccionar la ip externa a una ip interna o redirect_port en caso de ser necesario redireccionar los distintos puertos en si la estructura del archivo es la siguiente

```
redirect_port tcp 192.168.20.5:80 80
redirect_port tcp 192.168.20.5:443 443
redirect_port tcp 192.168.20.5:25 25
redirect_port tcp 192.168.20.5:22 2222
```

En este caso de ejemplo lo que se encuentra en la red privada que es necesario redireccionar es un servidor de paginas web, entonces todas las solicitudes son realizadas a la ip “publica” y el natd se encarga de direccionar al equipo que se requiera en la red privada.

Ahora solo basta con reiniciar el computador y todo está listo. “Siendo que los troncales se encuentren bien configuraos en los distintos switchs”