PRESENTADO POR ALFIO MUÑOZ

NUBE PRIVADA CON MIKROTIK CLOUD HOSTED ROUTER, VIRTUALIZACION, DISASTER RECOVERY Y TELEFONIA IP

Acerca de mi

Alfio Muñoz

- MikroTik Certified Consultant.
- Director de entrenamientos y capacitaciones de Issabel PBX.
- Consultor de infraestructura y telefonia para el Ministerio de Defensa RD.

Experiencia:

- 12 años de experiencia en Networking, routing y switching desde el 2007
- Implementacion de soluciones VoIP para empresas
- Virtualización de datacenters e infraestructura de servidores
- Capacitaciones de Voip, Virtualización, etc.
- Amante del software libre, pero no fanático.

AGENDA

- Que es un Cloud Hosted Router (CHR)
- Que es Proxmox
- Instalacion del CHR de Mikrotik
- Primeras configuraciones CHR
- Asignacion de Puentes virtuales Proxmox
- Creación de Nube privada
- Publicando servicios desde el CHR
- Creación de VPN L2TP IPSEC y BCP
- Plan de replicación de servidores de local a remoto por túnel VPN
- Telefonia IP mediante Tuneles BCP

CLOUD HOSTED ROUTER

- Cloud Hosted Router (CHR) es una version de RouterOS creada para ejecutarse como una maquina virtual. Soporta arquitectura x86 64-bit y puede ser utilizado por los principals hypervisores para virtualizacion como: VMWare, Hyper-V, VirtualBox, KVM y muchos mas. CHR Tiene todas las funcionalidades habilitadas por defecto pero viene con un modelo de licenciamiento diferente que las demas versions de RouterOS.

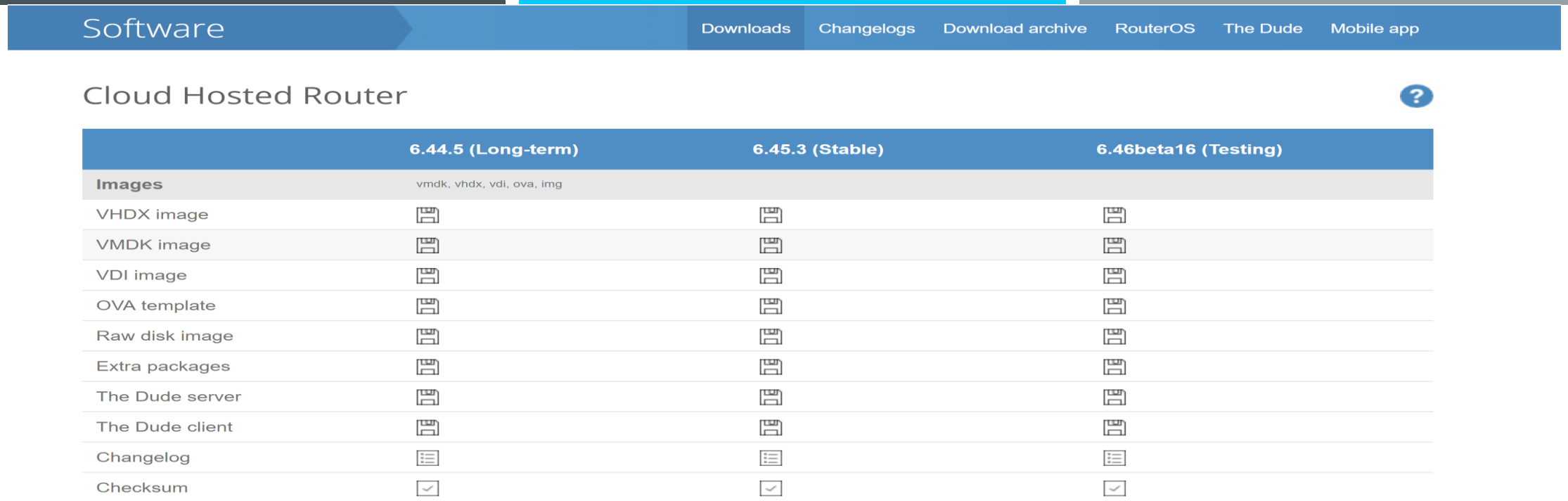
- Para mas detalles:

- https://wiki.mikrotik.com/wiki/Manual:CHR

PROXMOX

QUE ES PROXMOX

- Es un proyecto de código abierto, desarrollado y mantenido por Proxmox Server Solutions.
- Completa plataforma de virtualización basada en sistemas de código abierto que permite la virtualización tanto sobre LXC como KVM.
- Es una distribución bare-metal, basada en Debian con solo los servicios básicos para de esta forma obtener un mejor rendimiento.
- Permite la migración en vivo de maquinas virtuales, clustering de servidores, backups automáticos y conexión a un NAS/SAN con NFS, iSCSI, etc…



	6.44.5 (Long-term)	6.45.3 (Stable)	6.46beta16 (Testing)
Images	vmdk, vhdx, vdi, ova, img		
VHDX image			
VMDK image			
VDI image			
OVA template			
Raw disk image			
Extra packages			
The Dude server			
The Dude client			
Changelog			
Checksum			

DIFERENTES MANERAS DE INSTALAR EL CHR EN PROXMOX

DESCARGANDO LA IMAGEN DIRECTAMENTE DESDE EL SITIO WEB DE MIKROTIK

TIPOS DE INSTALACIONES

- Crear la VM y verificar bien el ID de esta, en nuestro caso de ejemplo 125, crear el disco en formato qcow2
- Subir o descargar el archivo .img al servidor proxmox
- Ubicar la carpeta donde se ha creado la VM
- Correr el siguiente commando en la misma carpeta que subimos la imagen del CHR : qemu-img convert -f raw -O qcow2 chr-6.44.5.img vm-125-disk-0.qcow2
- Luego ir a la carpeta que contiene el disco virtual de la VM que es /var/lib/vz/images/125 y reemplazarlo por la imagen ya convertida.
- Arrancamos nuestra VM y listo.

INSTALANDO DESDE UNA IMAGEN RAW

- https://www.youtube.com/watch?v=MeVfZvaGDAU&feature=youtu.be

INSTALANDO CON EL SCRIPT

- Notas a tener en cuenta:
- Crear el directorio /home/root/temp de forma manual con un mkdir /home/root/temp
- Colocarse en ese directorio y crear el archivo donde vamos a copiar el script dentro.
- Ejemplo: touch chrinstallscript.sh
- Darle permisos de ejecución: chmod 755 chrinstallscript.sh

INFORMACION DE LA WIKI

- https://wiki.mikrotik.com/wiki/Manual:CHR_ProxMox_installation

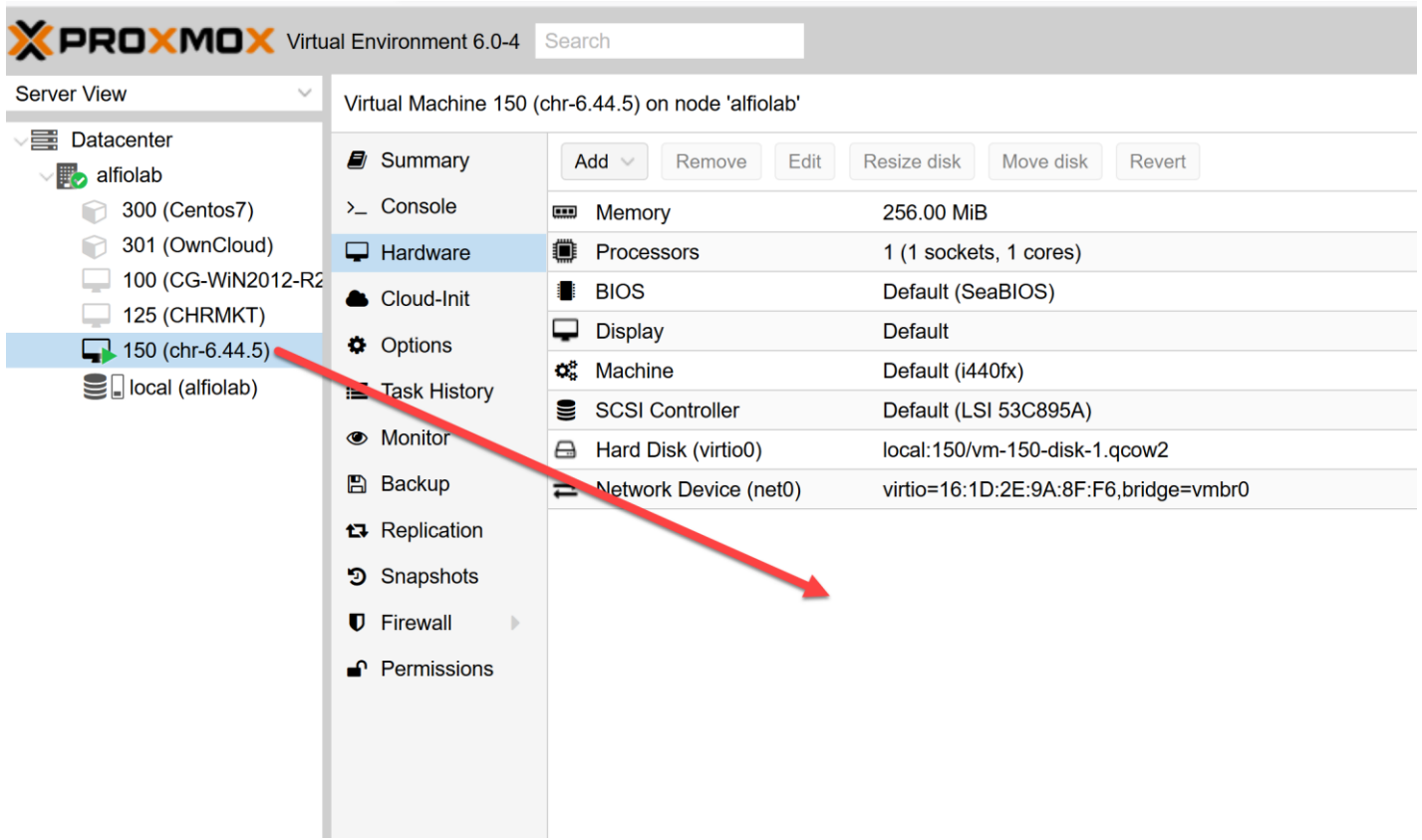
INSTALANDO CON EL SCRIPT

Modificamos la linea y le agregamos "/home" de otra forma no nos va a funcionar.

```
# Creating qcow2 image for CHR.
echo "-- Converting image to qcow2 format "
qemu-img convert \
    -f raw \
    -O qcow2 \
    /root/temp/chr-$version.img \
    /var/lib/vz/images/$vmID/vm-$vmID-disk-1.qcow2
# Creating VM
```

```
# Creating qcow2 image for CHR.
echo "-- Converting image to qcow2 format "
qemu-img convert \
    -f raw \
    -O qcow2 \
    /home/root/temp/chr-$version.img \
    /var/lib/vz/images/$vmID/vm-$vmID-disk-1.qcow2
# Creating VM
echo "-- Creating new CHR VM"
```

- https://www.youtube.com/watch?v=8i_vwywNMho&feature=youtu.be



NUESTRO CHR LISTO Y EJECUTANDOSE

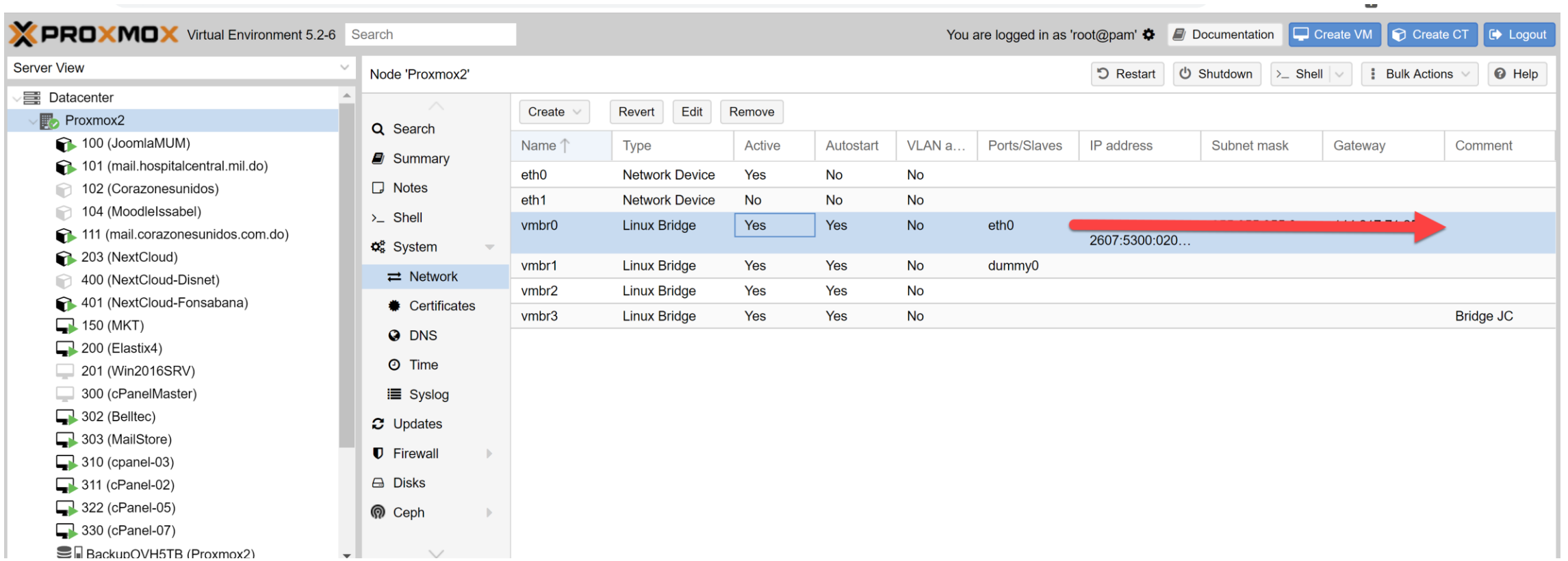
Escenario 1
Nube Privada

CREACION DE UN SEGMENTO PUENTE AISLADO EN PROXMOX PARA ASIGNARLO A NUESTRO CHR

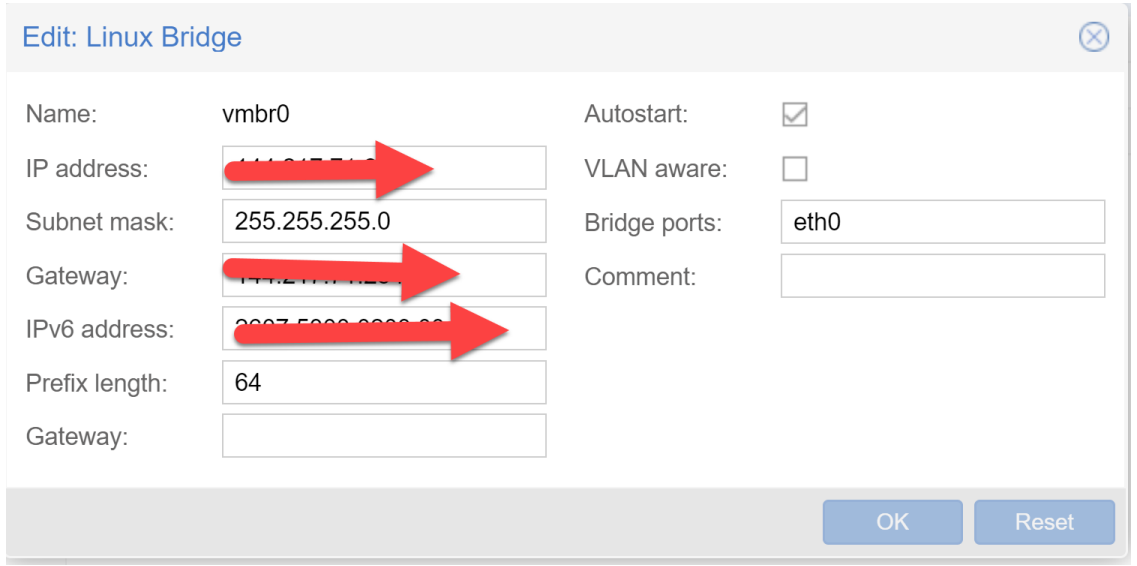
Como crear la nube privada y agregar una interfaz del CHR al segmento privado, de manera que solo se tenga acceso a dicho segmento mediante el CHR.

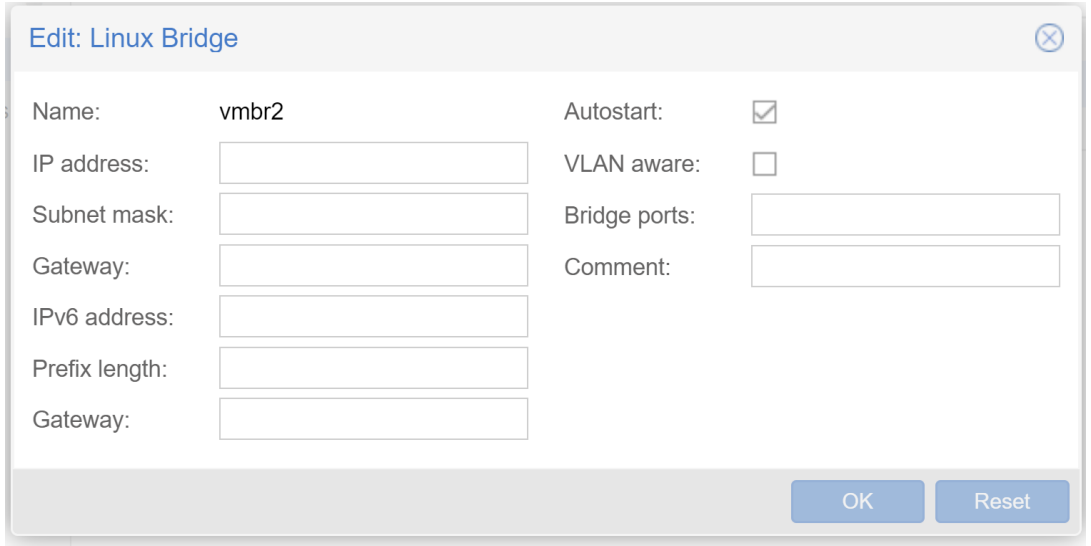
Podemos tener la opción de aislarnos totalmente de la red pública publicar servicios mediante nuestro nuestro CHR redireccionando puertos

BRIDGE EN PROXMOX CON UN PUERTO FISICO DE RED



PUENTES EN PROXMOX PARA EL CHR





ual Machine 150 (MKT) on node 'Proxmox2'

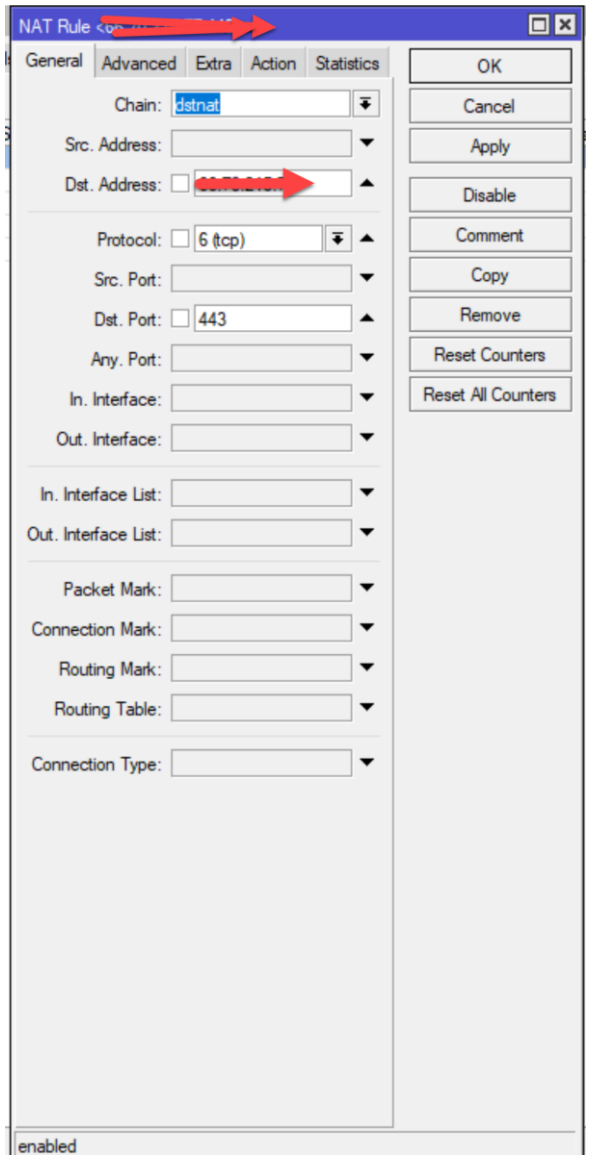
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions

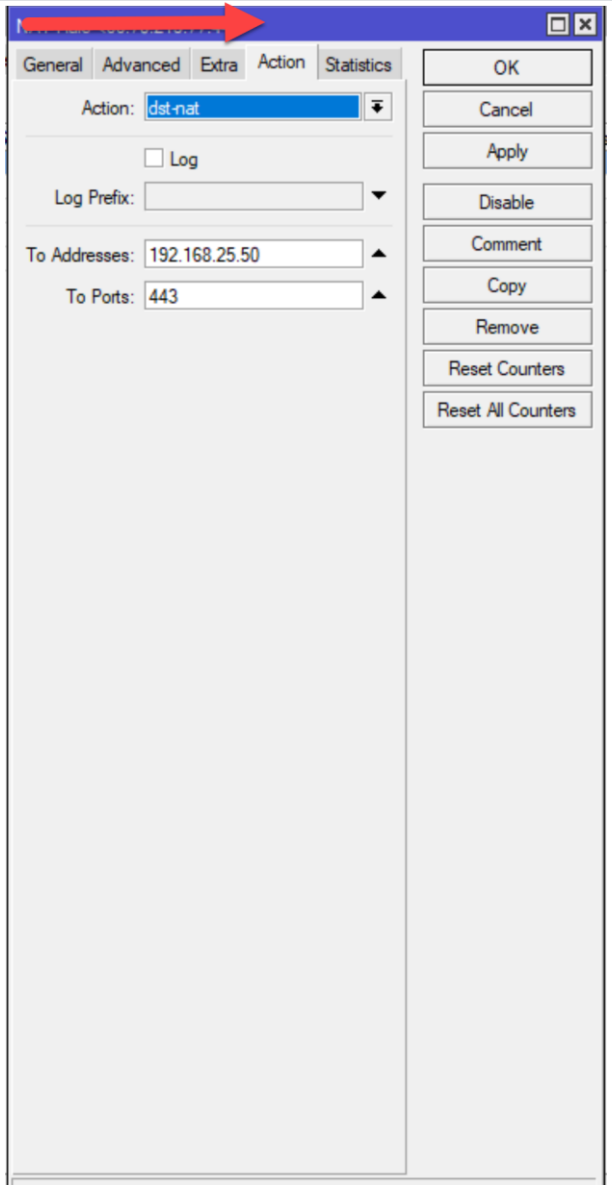
Add | Remove | Edit | Resize disk | Move disk | Revert

Keyboard Layout	Default
Memory	1.00 GiB
Processors	4 (1 sockets, 4 cores)
Display	SPICE (qxl)
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (scsi0)	local:150/vm-150-disk-1.qcow2,size=32G
Network Device (net0)	virtio=02:00:00:e2:af:0b,bridge=vmbr0
Network Device (net1)	virtio=06:00:36:31:80:14,bridge=vmbr1
Network Device (net2)	virtio=12:86:C7:1F:21:37,bridge=vmbr3
Network Device (net3)	virtio=CA:2F:DA:6C:2F:A1,bridge=vmbr0
Network Device (net4)	virtio=AE:6D:E5:3D:42:7E,bridge=vmbr2

CADA TARJETA A UN PUENTE DISTINTO

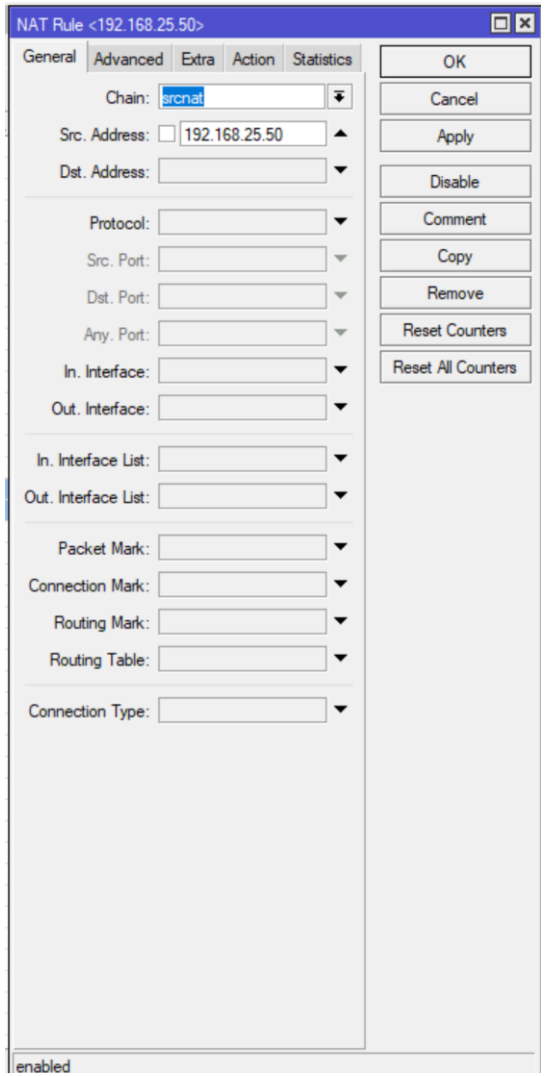
- El vmbr0 es el Puente que se comunica con el exterior y donde tendremos asignadas las IP públicas.
- Los otros puentes son segmentos aislados independientes en donde solo se pueden comunicar los equipos en el mismo Puente.
- En el CHR asignamos en cada interfaz de los otros puentes las IP privadas.
- En el CHR creo reglas para publicar Servicios que apunten a la red privada interna de un segmento o puente.
- Puedo crear tuneles VPN con BCP que se conecten directamente a cada segmento o Puente.

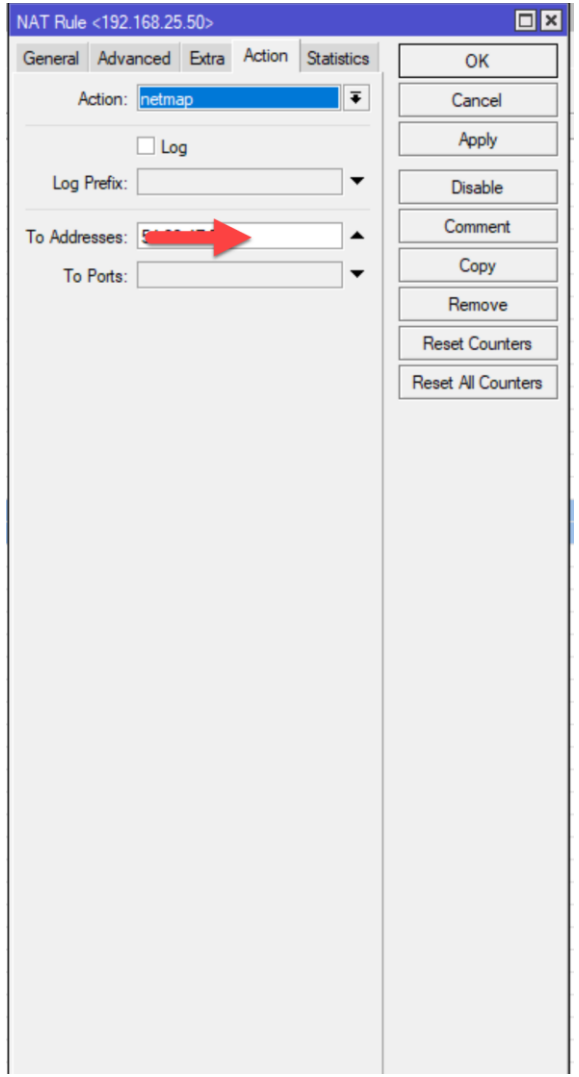


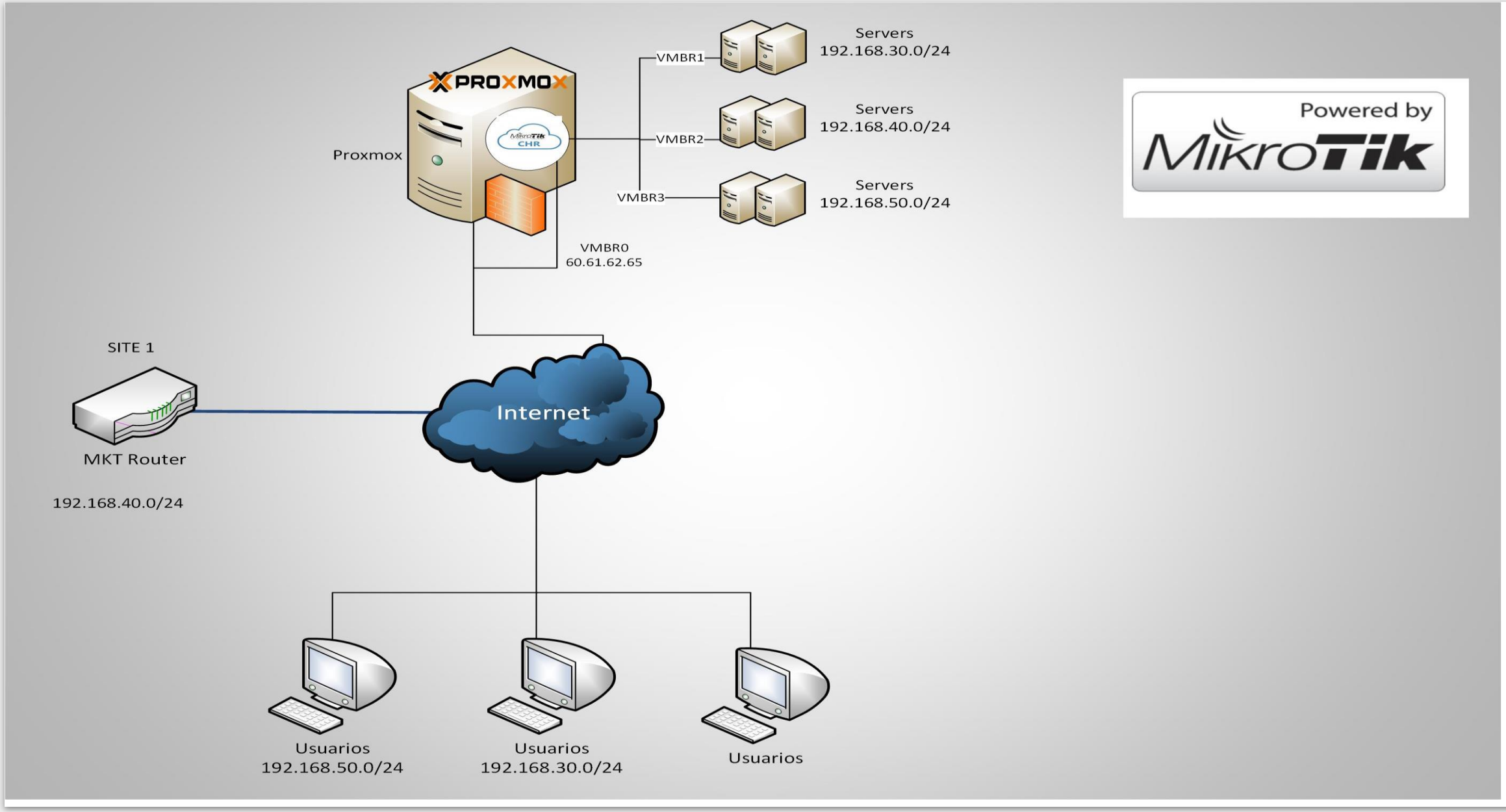


PUBLICANDO UN SERVICIO EN EL CHR

SALIDA UNO A UNO DE UN CLIENTE






Servers
192.168.30.0/24
VMBR1
Servers
192.168.40.0/24
VMBR2
Servers
192.168.50.0/24
VMBR3
Proxmox
VMBR0
60.61.62.65
Powered by
MikroTik
SITE 1
Internet
MKT Router
192.168.40.0/24
Usuarios
192.168.50.0/24
Usuarios
192.168.30.0/24
Usuarios

ESCENARIO 2: DISASTER RECOVERY Y FAILOVER 100% AUTOMATIZADO

- Mediante el túnel BCP conectamos tres centros de datos iguales donde tenemos Proxmox instalado

PPP + BCP

- Trataremos con:

- Layer 2 Tunneling Protocol (L2TP), el cual lo vamos a combinar con encriptacion IPSEC
- BCP es Bridge Control Protocol, el cual permite el envio de tramas Ethernet sobre PPP.
- Multilink Maximum Received Reconstructed Unit (MRRU)

MULTI-LINK PPP

- QUE ES MULTI-LINK PPP?

RFC 1990

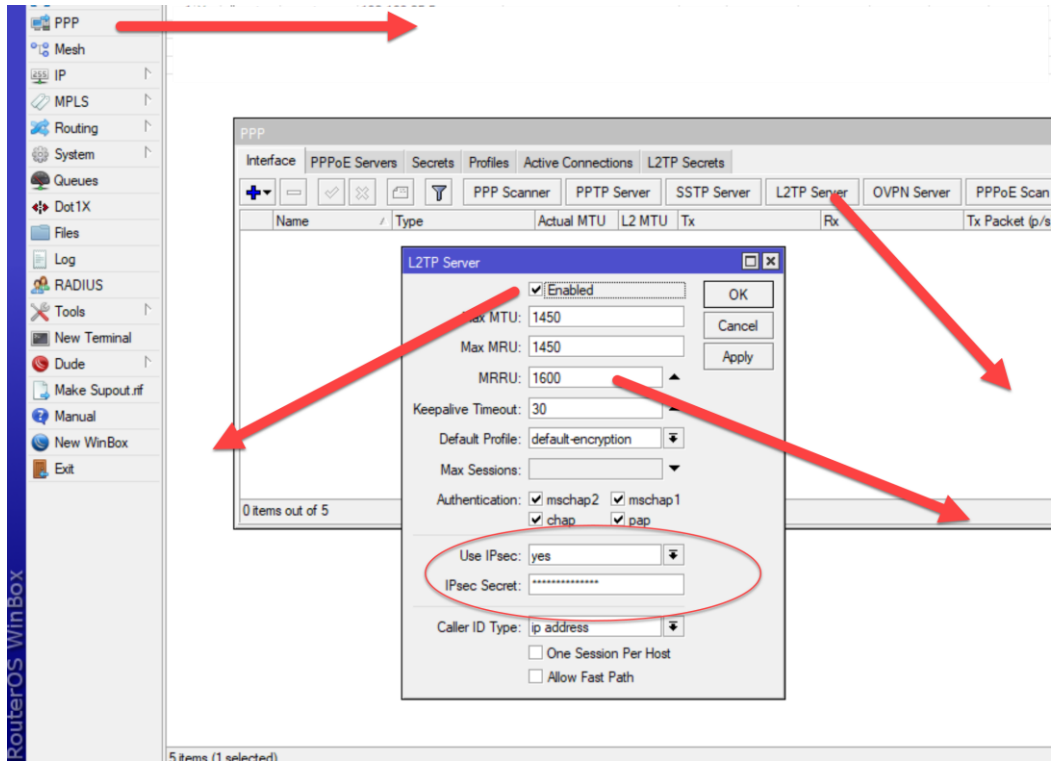
https://tools.ietf.org/html/rfc1990

Multi-Link Point to Point Protocol (MP, Multi-Link PPP, MultiPPP or MLPPP) es un metodo de dividir, recombinar and secuenciar datos a traves de multiples enlaces logicos de datos.

Fuente:
https://wiki.mikrotik.com/wiki/Manual:MLPPP_over_single_and_multiple_links

Para que una VPN capa 2 funcione las tramas ETHERNET tienen que viajar através del tunel VPN, pero generalmente el MTU de la VPN es mas pequeño que el tamaño de la trama ETHERNET. En ese orden para poder tener o manejar un MTU mayor debemos establecer multiples tuneles PPP y los combinamos todos juntos, esto se llama Multi-Link PPP

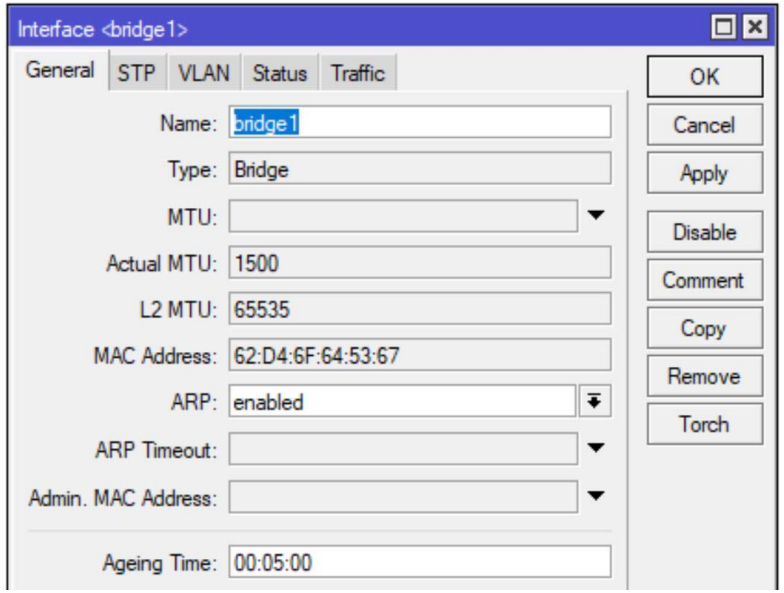
L2TP SERVER CON IPSEC

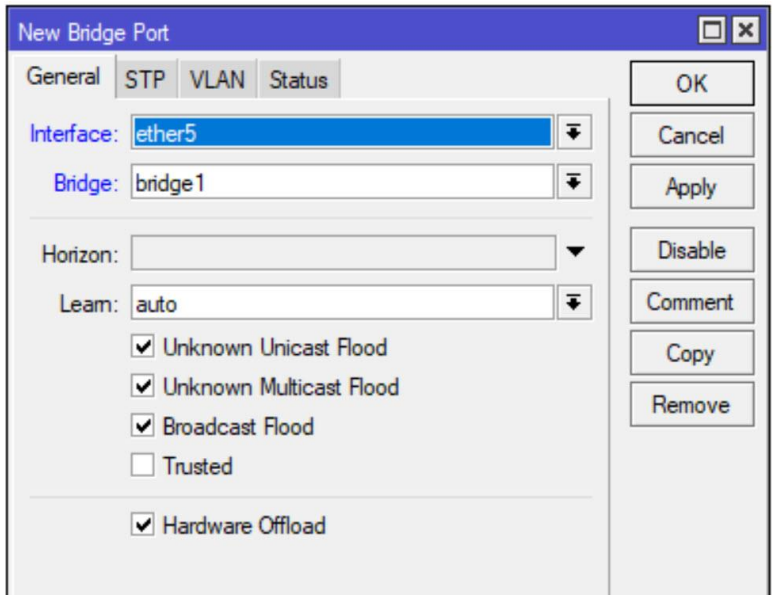


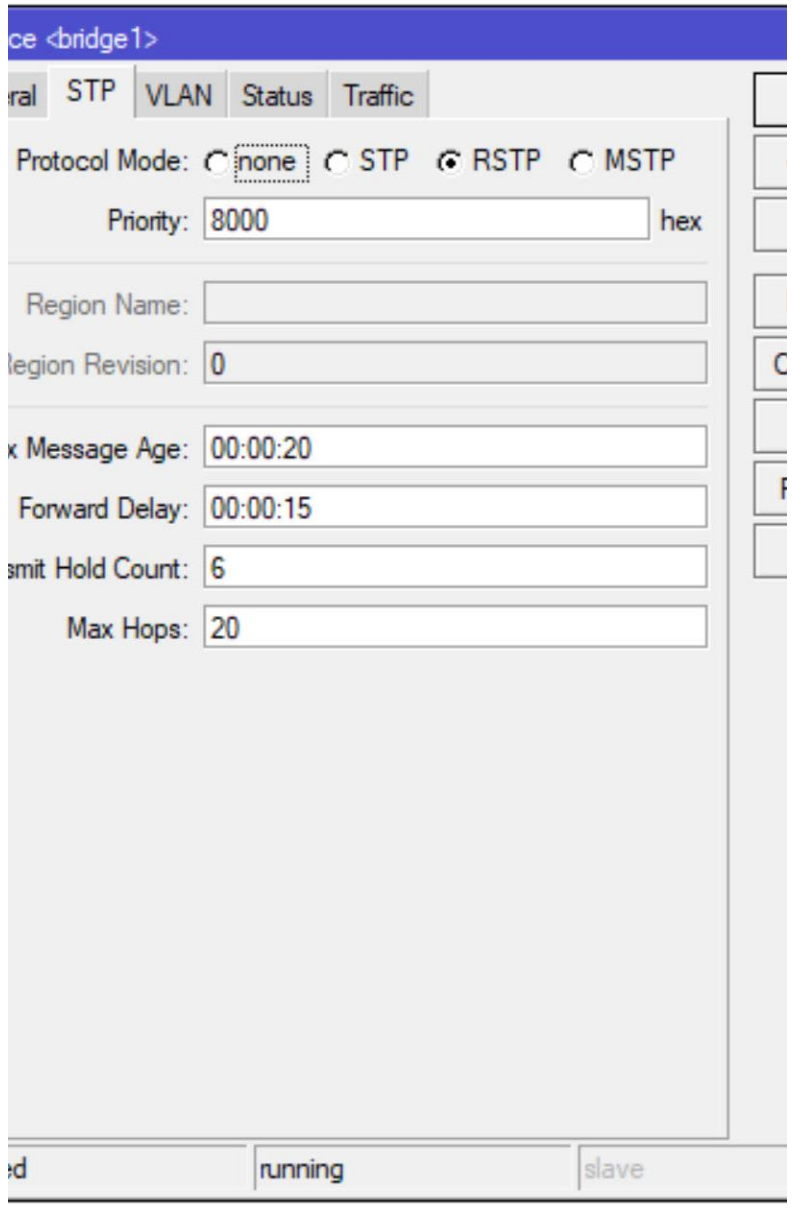
- En el servidor principal habilitamos el L2TP server con IPSEC Es muy importante cambiar el MRRU a 1600 por el tema del multilink anteriormente explicado.

EN EL SERVIDOR PRINCIPAL

- Creamos un Bridge y seleccionamos SRTP para el STP
- **Bridge** menu → **[+]**
- Luego agregamos el Puerto del CHR, aqui Podemos elegir un Puerto ethernet, en nuestro caso el eth5

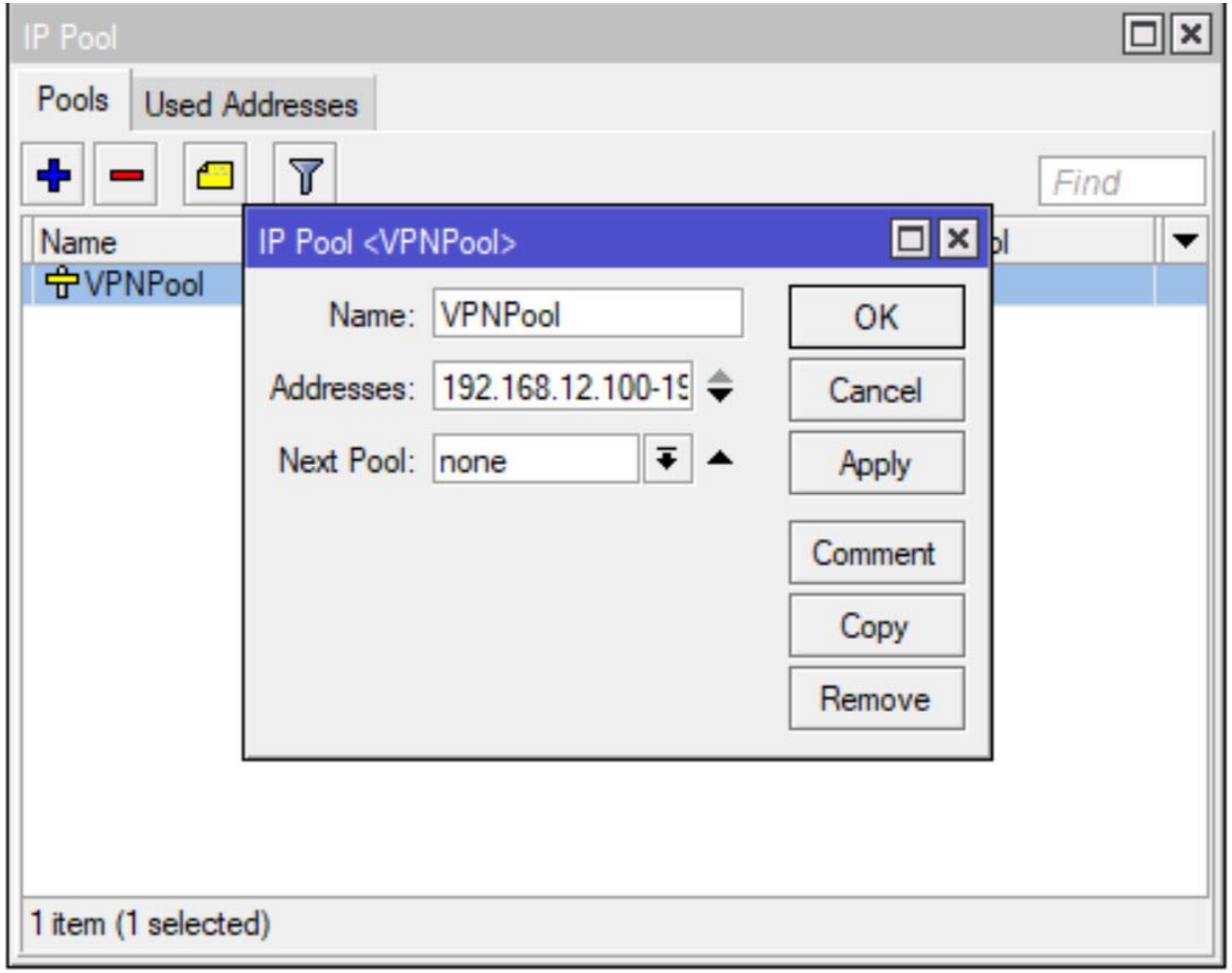






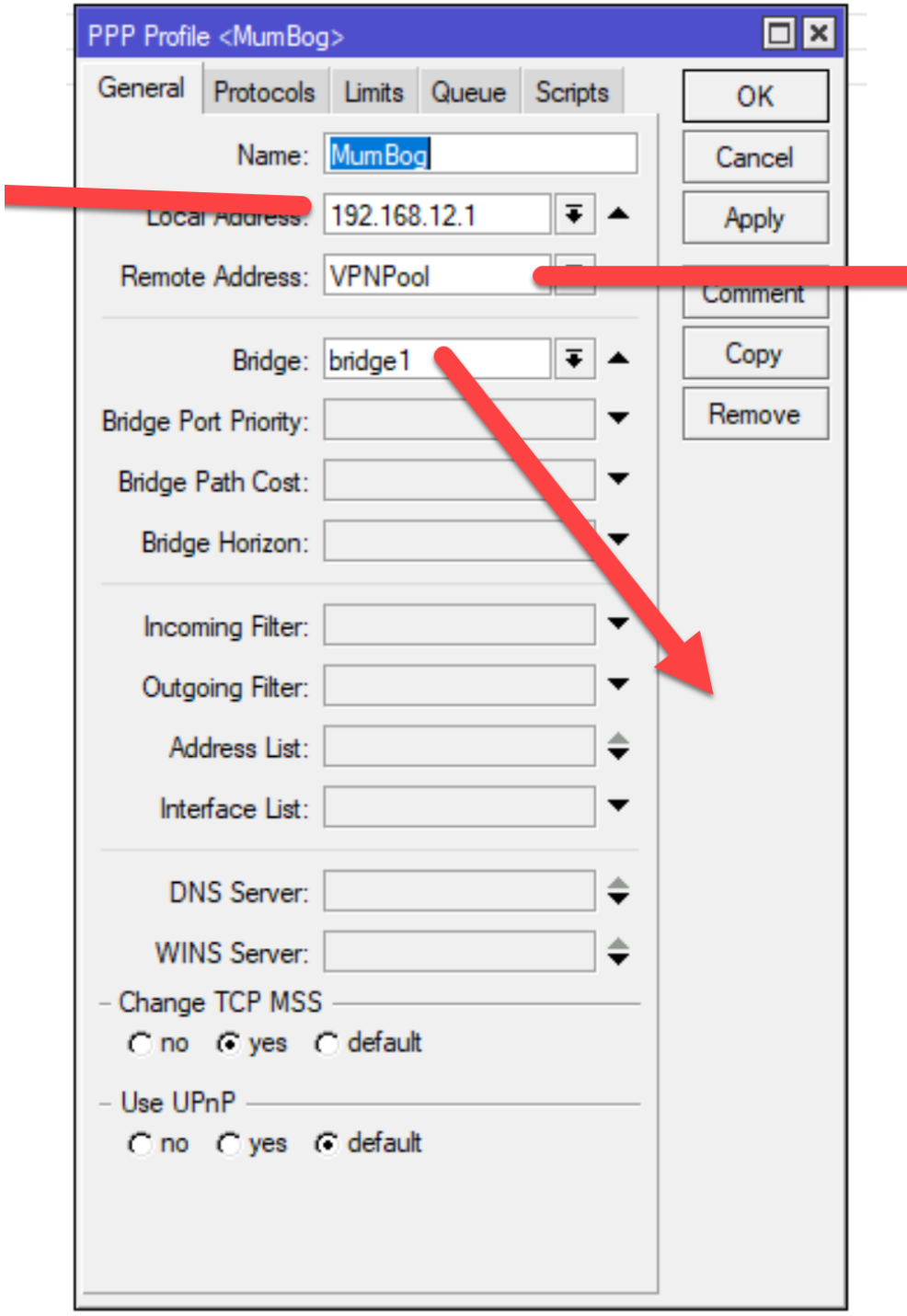
POOL PARA VPN

- Creamos un IP Pool para las VPN point-to-point IP:
- **IP** → **Pools** → **[+]**



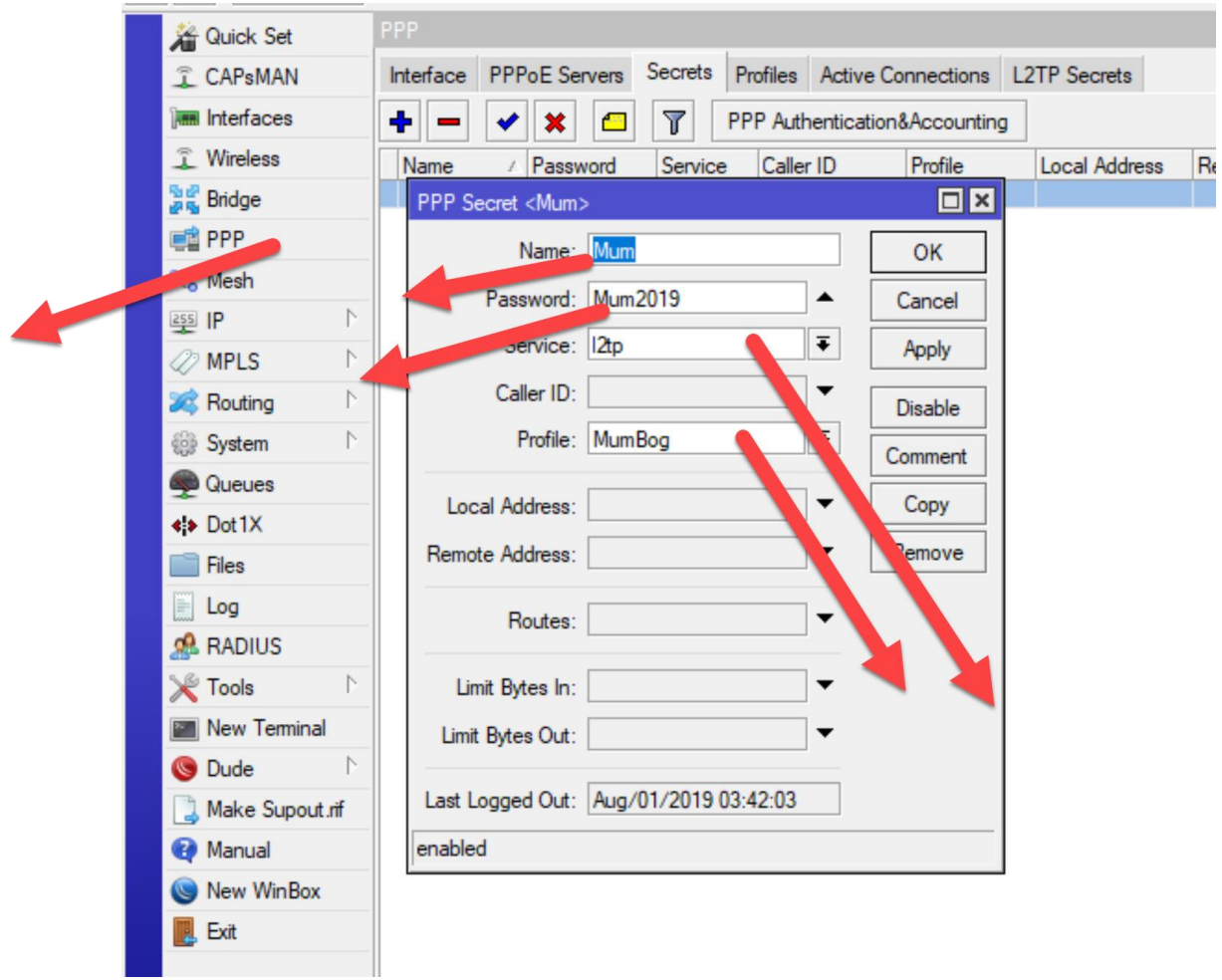
SERVIDOR PRINCIPAL

- Creamos un profile ppp y habilitamos el BCP cuando asignamos el bridge ya creado anteriormente al profile.



CREAMOS EL PPP SECRET PARA LAS OFICINAS REMOTAS

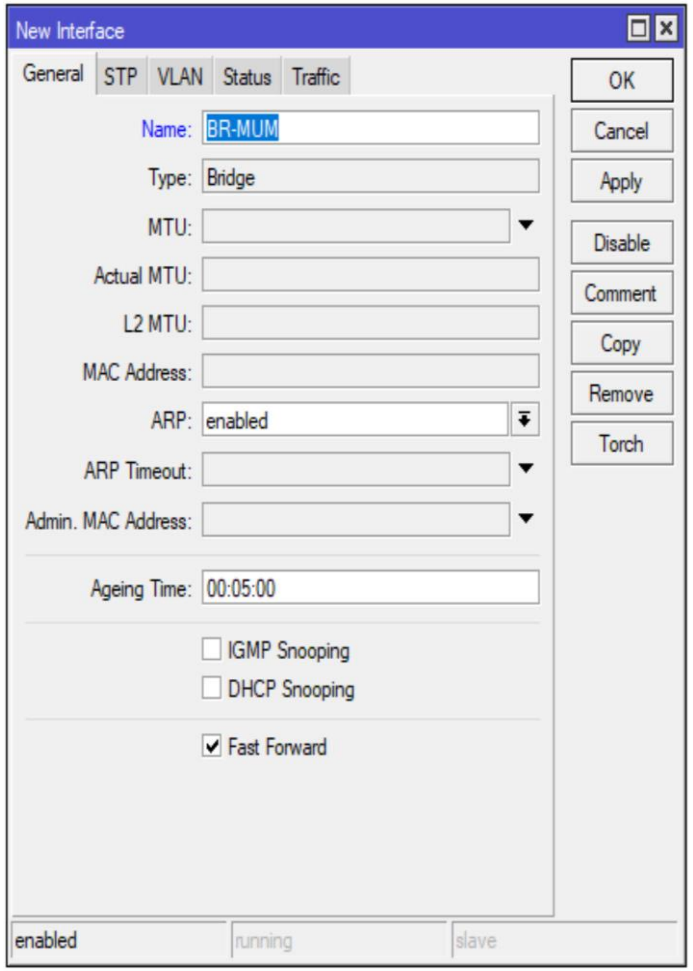
- Podemos si deseamos utilizar el mismo secret para todas las oficinas remotas

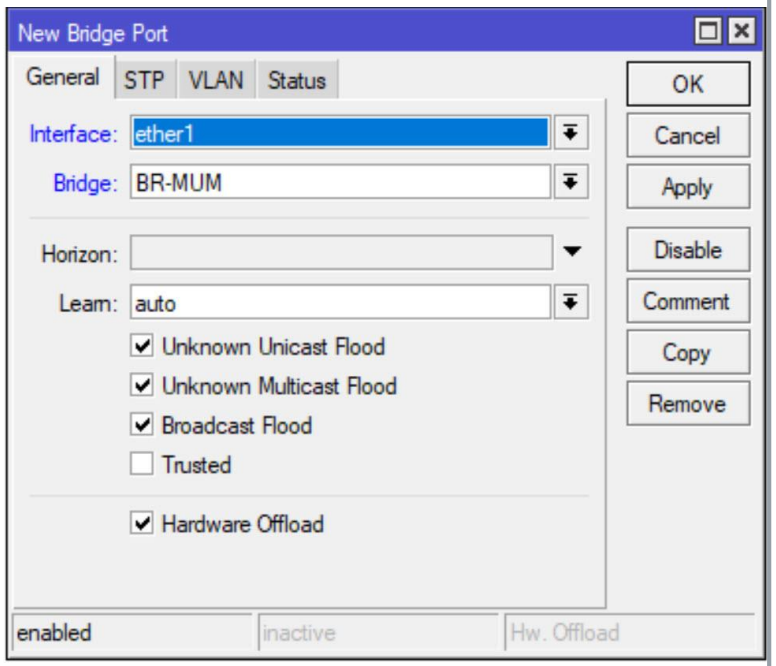


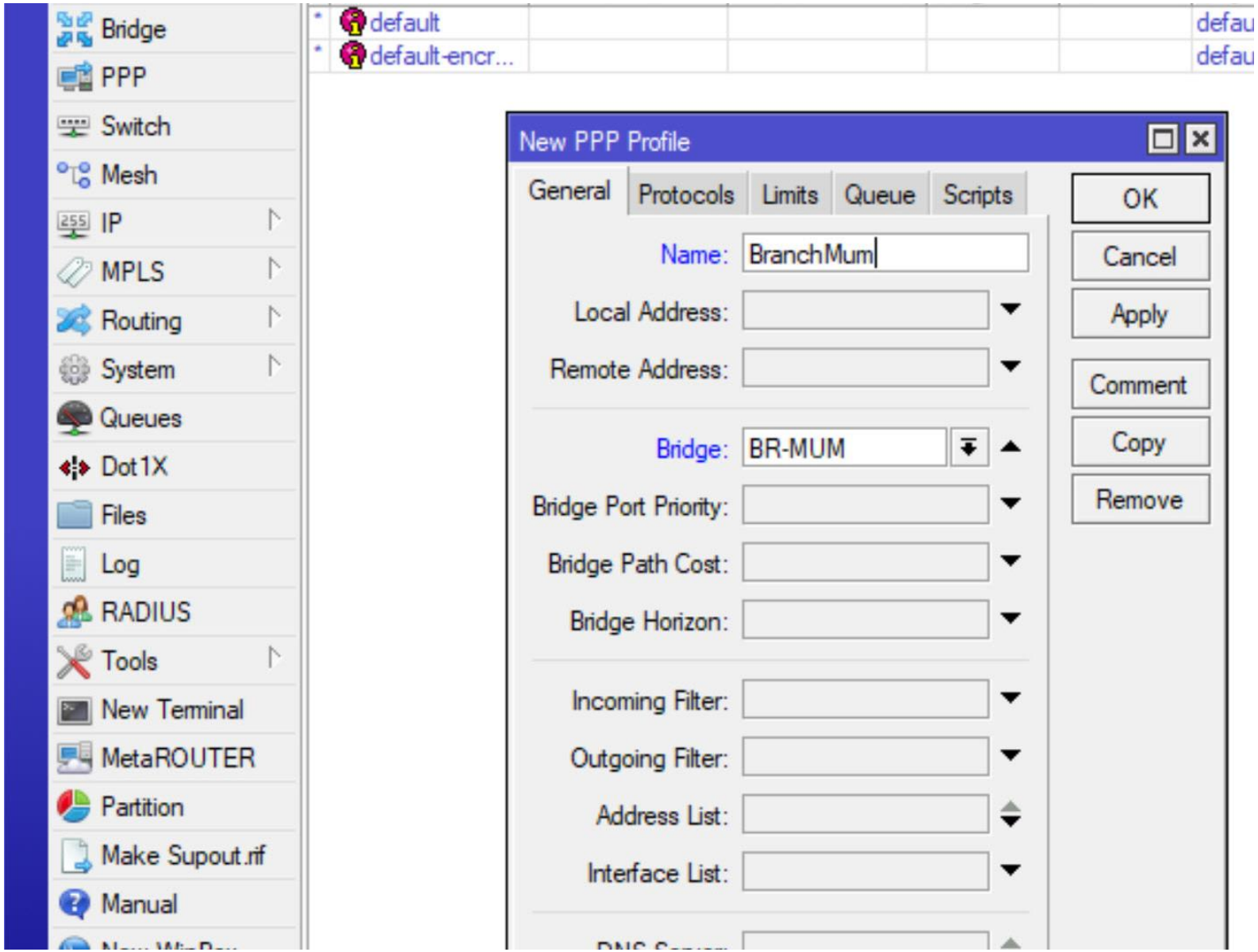
EN LAS OFICINAS REMOTAS AHORA

EN LAS OFICINAS REMOTAS

- Creamos el bridge “ BR-MUM” y asignamos el Puerto que será miembro de el.

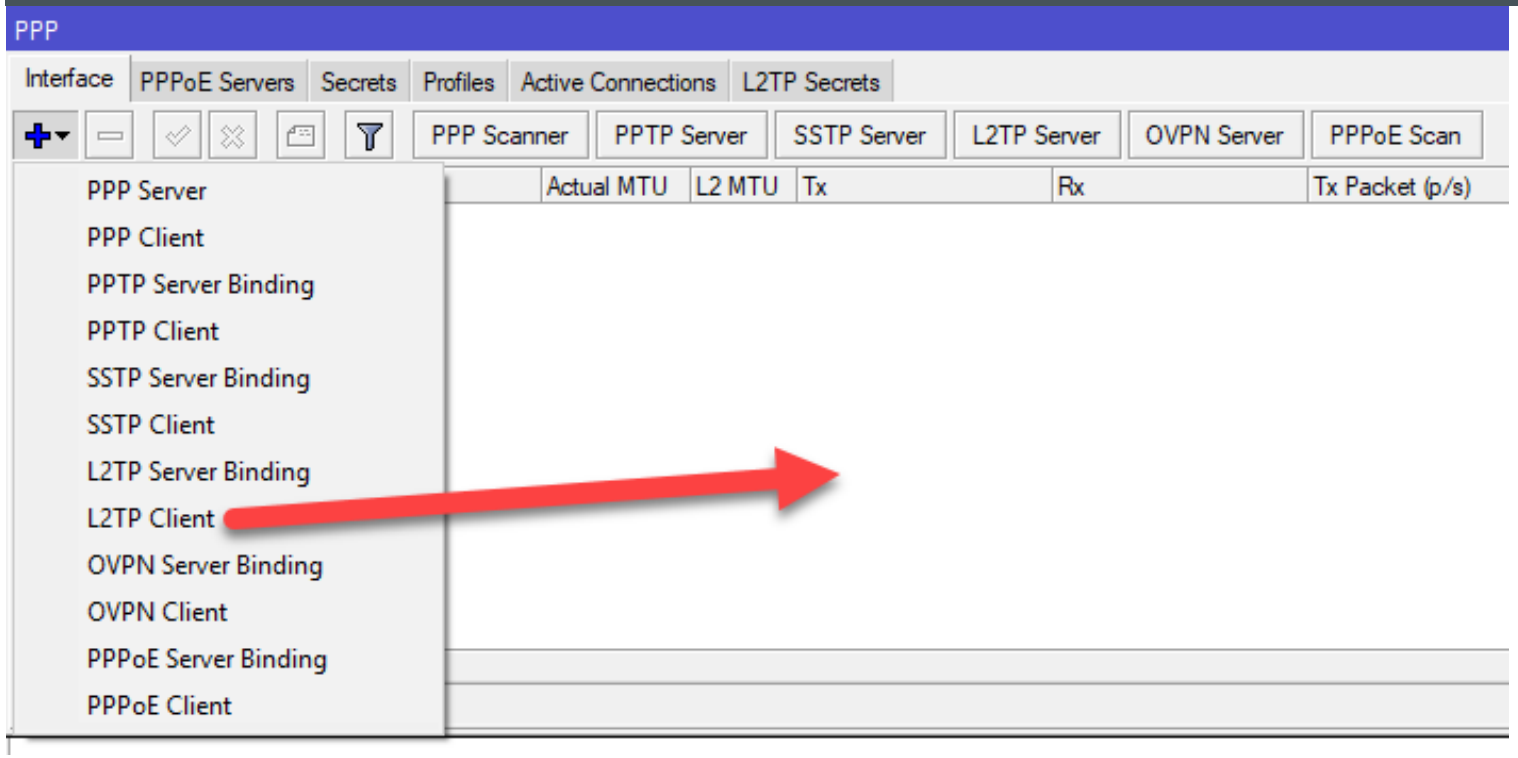






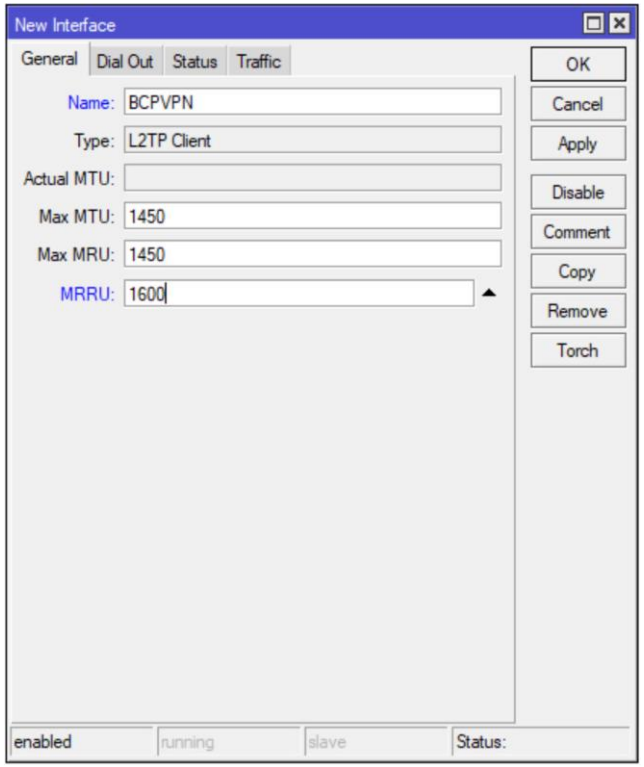
EN LAS OFICINAS REMOTAS

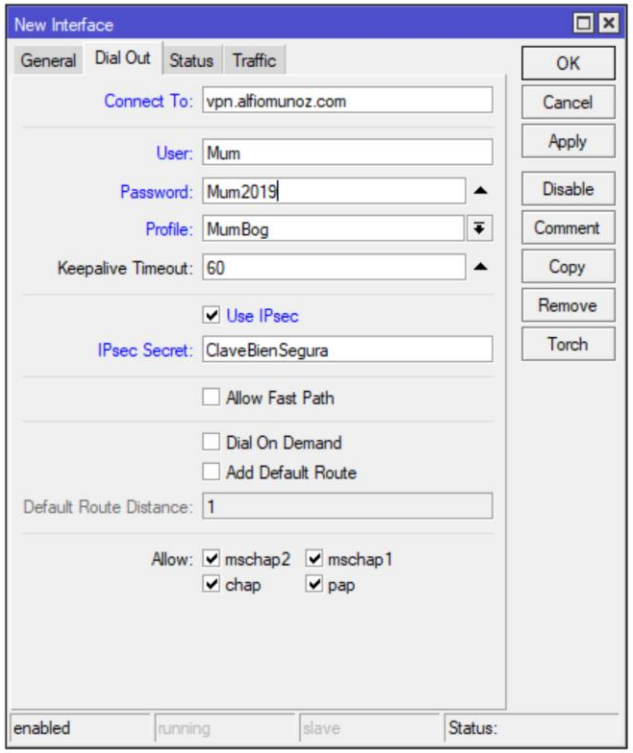
CREAMOS EL PROFILE PPP PARA CONEXION Y LE ASIGNAMOS TAMBIEN EL NUEVO BRIDGE CREADO.



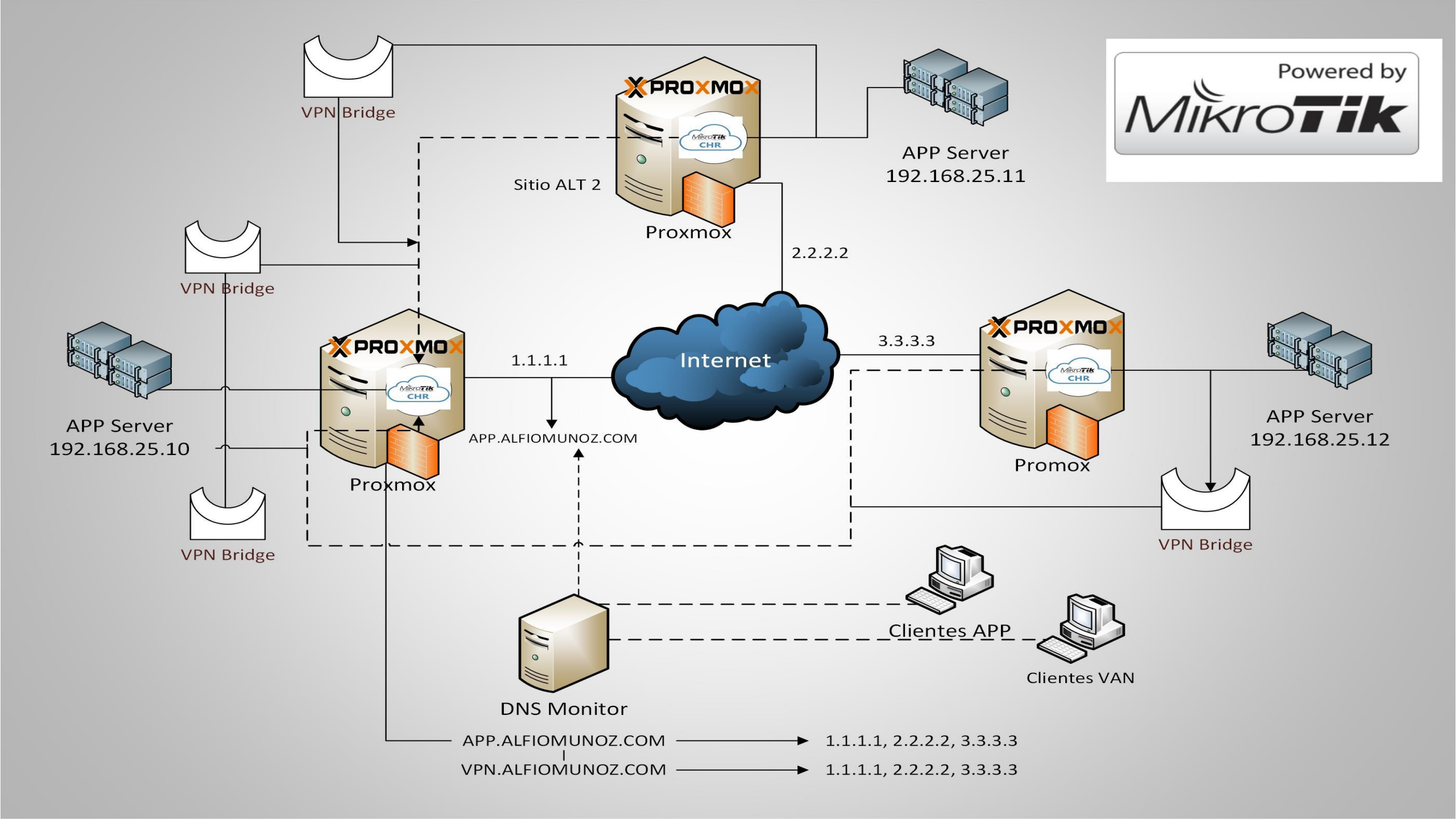
Creamos la interface cliente L2TP con Multi-Link PPP, para conectarnos a la oficina principal

EN LAS OFICINAS REMOTAS





EN LAS OFICINAS REMOTAS


VPN Bridge
PROXMOX
CHR
APP Server
192.168.25.11
Sitio ALT 2
Proxmox
2.2.2.2
VPN Bridge
APP Server
192.168.25.10
PROXMOX
CHR
1.1.1.1
Internet
3.3.3.3
PROXMOX
CHR
APP Server
192.168.25.12
APP.ALFIOMUNOZ.COM
Proxmox
Promox
VPN Bridge
VPN Bridge
Clientes APP
Clientes VAN
DNS Monitor
APP.ALFIOMUNOZ.COM
1.1.1.1, 2.2.2.2, 3.3.3.3
VPN.ALFIOMUNOZ.COM
1.1.1.1, 2.2.2.2, 3.3.3.3
Powered by
MikroTik

EXPLICACIÓN ESCENARIO FAILOVER AUTOMATICO

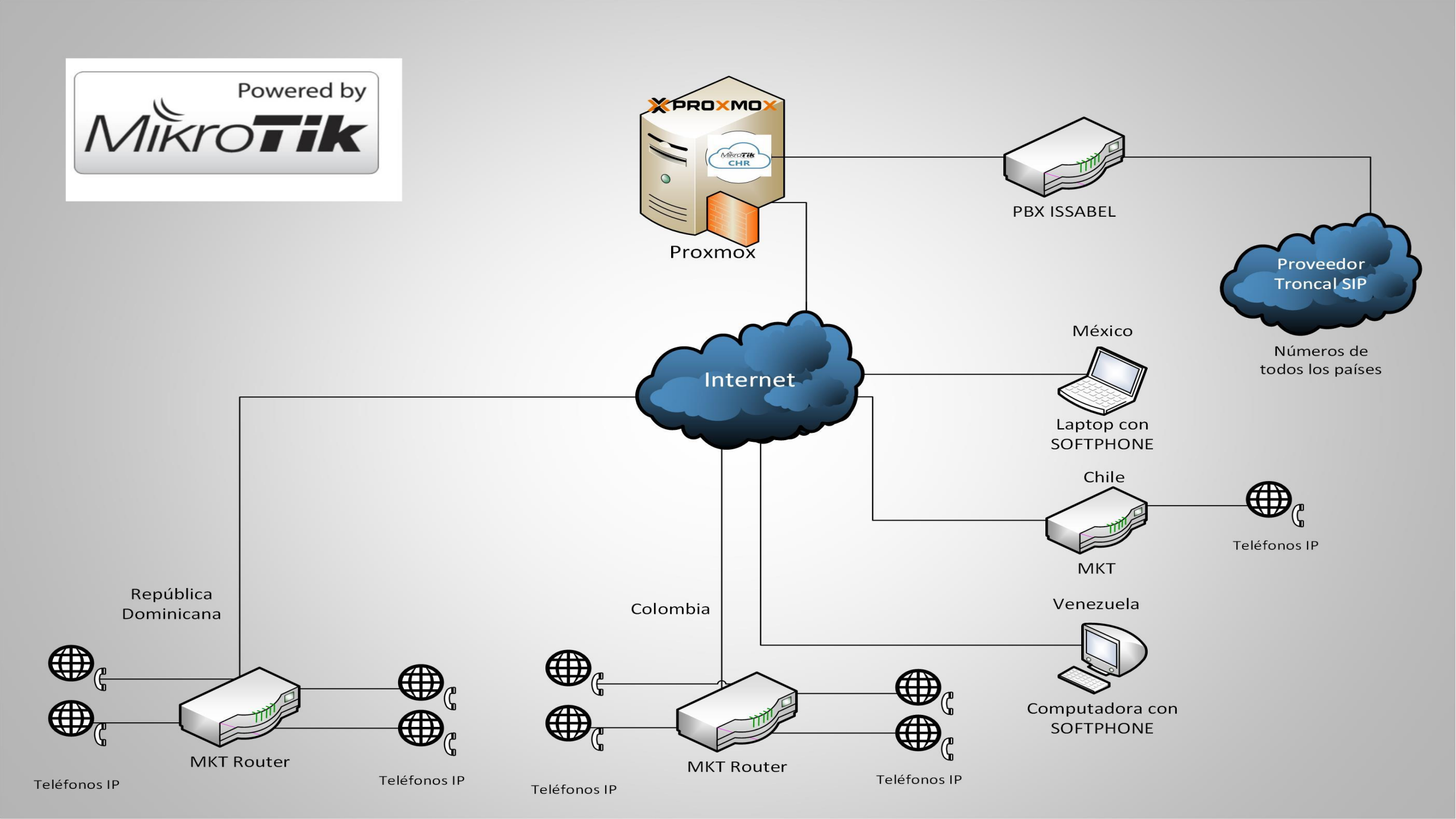
- Mediante el túnel BCP conectamos tres centros de datos iguales donde tenemos Proxmox instalado y hacemos lo siguiente:
- Tenemos una red exclusiva para servidores en el ambiente virtualizado, esa red la tenemos conectada a dos centros de datos alternos mediante los túneles con BCP, las máquinas virtuales replican entre ellas por medio de aplicaciones en tiempo real, es decir bases de datos, etc, entre cada uno de los puntos remotos, todo esto monitoreado por una aplicación de terceros en donde tenemos para cada una de los servidores un IP publico contratado y configurados en el CHR, adicional a esto les tenemos reglas de NAT, port Fowarding, etc para que sean accesibles desde el exterior.
- Site 1 : 1.1.1.1 -------→ 192.168.25.10
- Site 2 : 2.2.2.2 -------→ 192.168.25.11
- Site 3 : 3.3.3.3 -------→ 192.168.25.12
- La aplicación de terceros de monitoreo DNS permite monitorear hasta 4 IP diferentes en donde puede hacer los cambios de IP en caso de que nuestro IP primario sufra una caída. La aplicación automáticamente va a hacer el cambio al site 2 o al site 3 dependiendo las reglas que tengamos configuradas. Ahí entonces el CHR ya tiene el control de acceso de ese sitio y si tenemos VPNs y sitios remotos también van a subir y conectarse al centro alterno.
- Los sitios remotos y los usuarios VPN estarán conectados al servicio al igual que las aplicaciones antes mencionadas a un nombre de dominio, el cual como habíamos comentado estará asociado a varias IP, es decir todos apuntaran sus servicios a:
- vpn.alfiomunoz.com

TELEFONIA IP SIN PROBLEMAS

- Cluster de centrales, una local y otra en la nube.
- Protocolo SIP muy susceptible a problemas de NAT
- Con esta solucion de tunel L2TP/BCP se soluciona el problema del NAT.
- Pueden estar geograficamente separados y siempre se van a comunicar sin problemas.
- Las personas pudieran estar viajando con un mAP lite y ya con eso, su telefono IP o Softphone se registran sin problemas.
- Soluciona el problema de ataques y vulnerabilidades ya que la PBX no esta publicada al mundo exterior

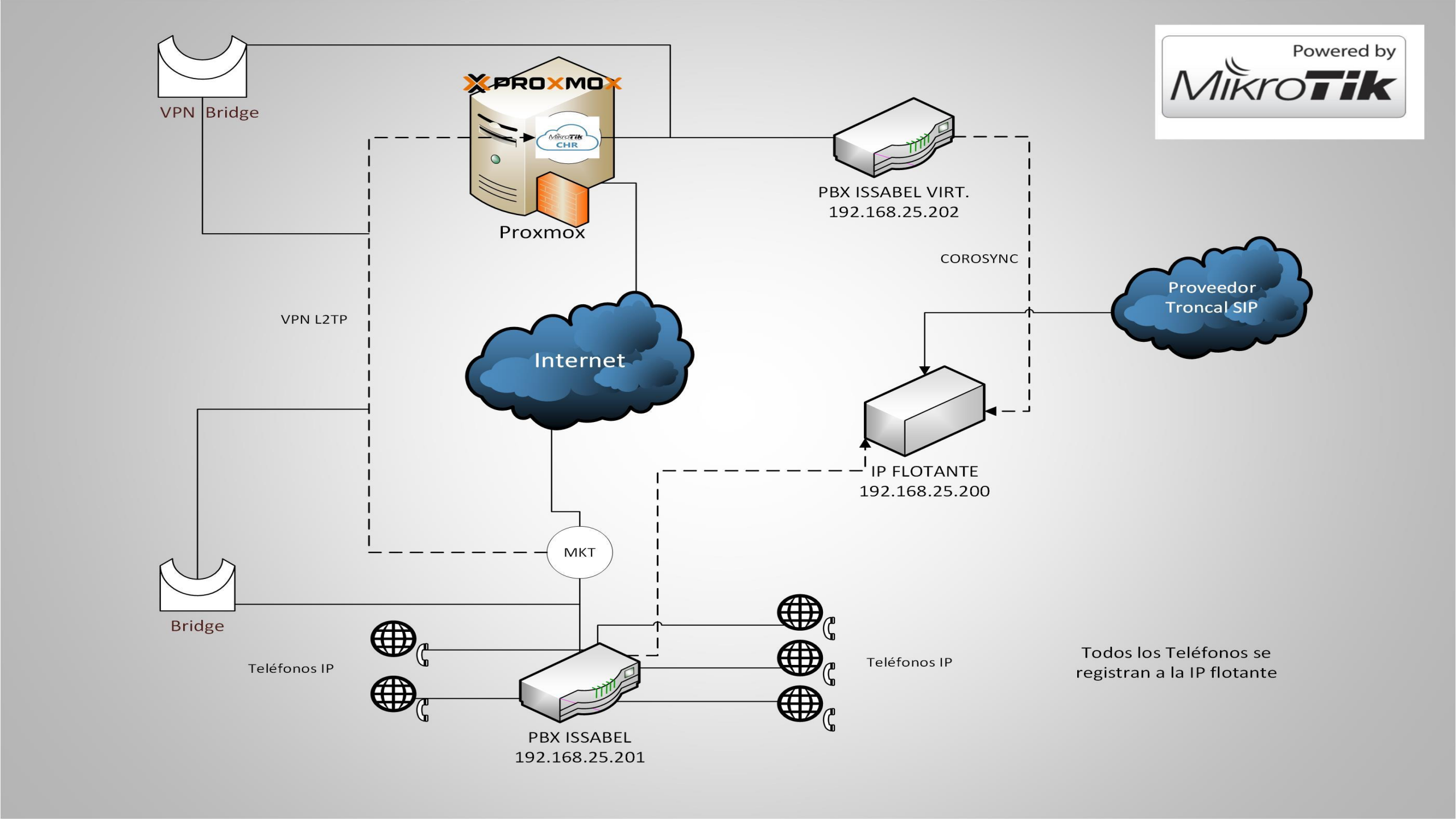
ESCENARIO I DE TELEFONIA IP

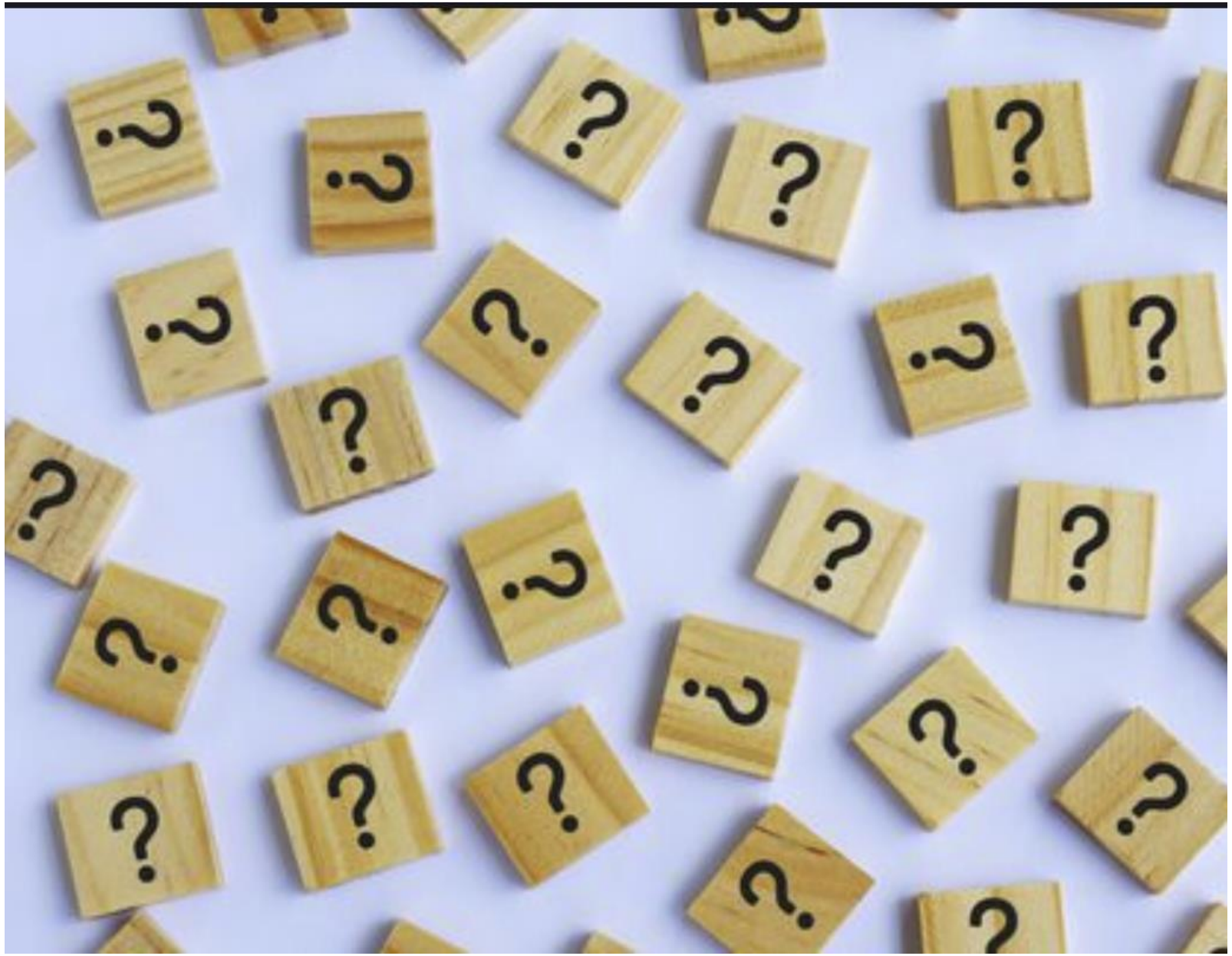
- La Central IP esta en la nube y todos los clientes se conectan remotos


Powered by MikroTik
PROXMOX
MikroTik CHR
Proxmox
PBX ISSABEL
Proveedor Troncal SIP
Números de todos los países
Internet
México
Laptop con SOFTPHONE
Chile
MKT
Teléfonos IP
Venezuela
Computadora con SOFTPHONE
República Dominicana
MKT Router
Teléfonos IP
Teléfonos IP
Colombia
MKT Router
Teléfonos IP
Teléfonos IP

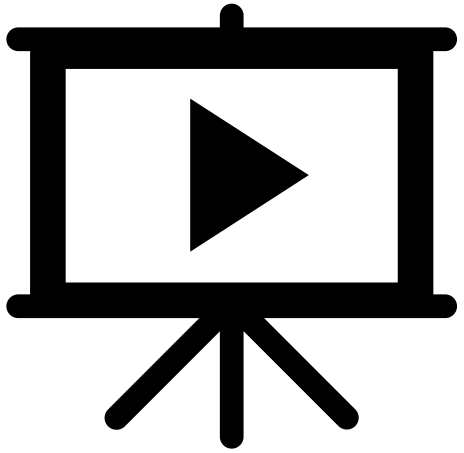
ESCENARIO 2 DE TELEFONIA IP

- Una empresa tiene su Central IP de forma Local y en la Nube tiene un respaldo en caso de desastres


Powered by MikroTik
VPN Bridge
PROXMOX
MikroTik CHR
Proxmox
PBX ISSABEL VIRT.
192.168.25.202
COROSYNC
Proveedor
Troncal SIP
VPN L2TP
Internet
IP FLOTANTE
192.168.25.200
MKT
Bridge
Teléfonos IP
Teléfonos IP
PBX ISSABEL
192.168.25.201
Todos los Teléfonos se
registran a la IP flotante



PREGUNTAS?



Gracias por su atención

Alfio Muñoz

alfiomunoz@gmail.com

alfio@issabel.com

Twitter. alfiomunoz

Facebook. Alfio Muñoz

Skype. alfiomunoz

https://t.me/IssabelPBXip