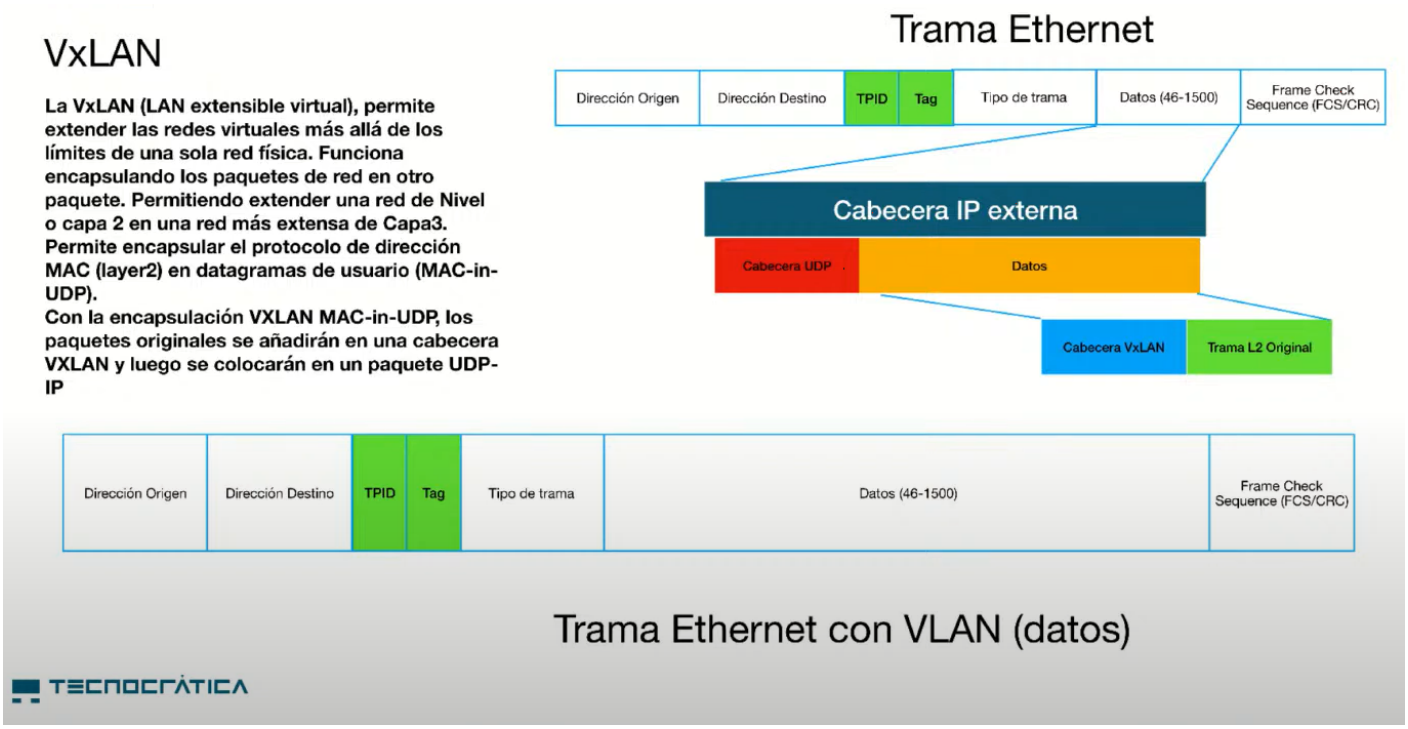
4.5.- SDN VxLAN.

¿Qué es una VxLAN?



Eduardo Taboada (Tecnocratica.net)· *VxLAN* (Todos los derechos reservados)

VxLAN (Red de área local virtual **extensible**) es una tecnología de superposición para la virtualización de redes, que establece un **túnel lógico en la red IP para extender la red de capa 2 sobre una red subyacente de capa 3 existente**. VXLAN utiliza el Punto de Túnel VXLAN (VTEP), que puede ser un host final o switches de red, o enrutadores, para encapsular y desencapsular el tráfico de capa 2.

VxLAN utiliza UDP (puerto por defecto 4789) de capa 4 por lo que no se preocupa de confiabilidad de la transmisión, por ello, puden perderse paquetes con tramas VLAN dentro de este, pero serán los extremos de la VxLAN quien deban de solicitar la retransmisión del tráfico perdido.

VxLAN se estandariza como un protocolo de encapsulación de superposición. Aumenta la escalabilidad hasta **16 millones redes lógicas** y permite la adyacencia de capa 2 a través de redes IP.

Licencia Creative Commons BY-NC-SA.

VxLAN es un protocolo de túnel IP estándar para ampliar las VLAN en una red. Conecta las VLAN de un extremo a otro de la red sin tunelización, es decir, los paquetes IP entre routers no van cifrados y por lo tanto, están expuesto a un sniffer de red. **VxLAN no debe ser utilizado en redes públicas.**

Para solucionar el problema de seguridad, Proxmox ha añadido la posibilidad de utilizar (que no viene por defecto) **VxLAN IPSEC Encryption, con un cifrado AES 256-sha1.** Para agregar cifrado IPSEC en una VxLAN, deberá reducir la MTU en 60 bytes adicionales para IPv4 u 80 bytes para IPv6 para manejar el cifrado. Entonces, con un MTU de 1500 reales predeterminados, debe usar un MTU de 1370 (1370+80(IPSEC)+50(VXLAN)==1500).

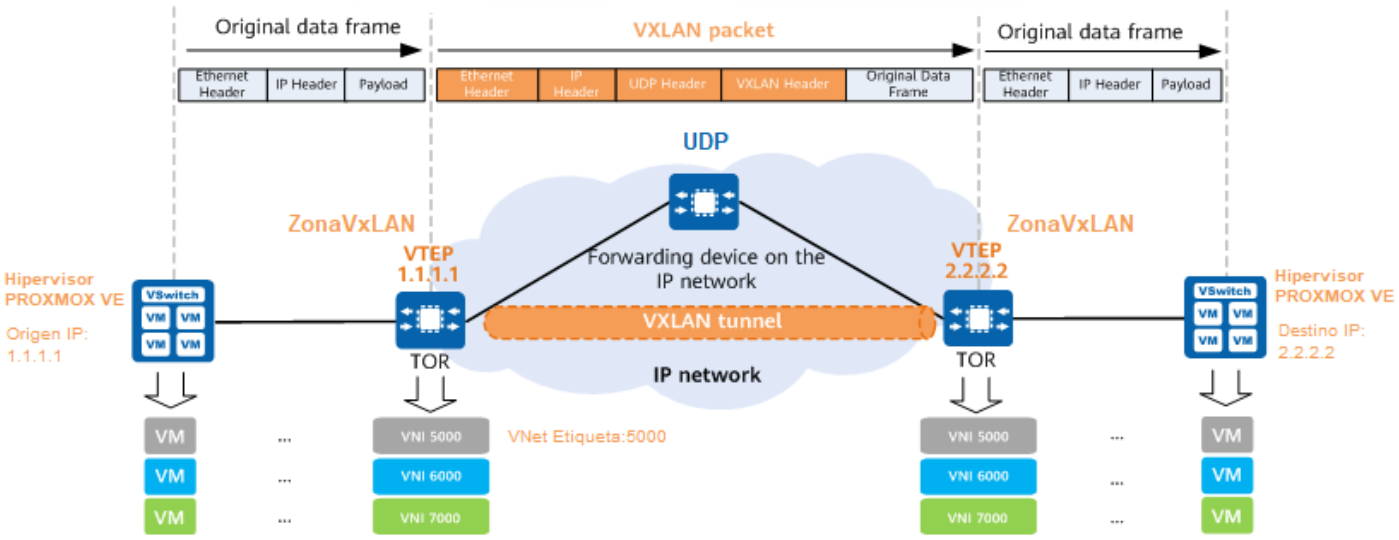


Imagen de elaboración propia· *Esquema VxLAN en Proxmox VE 8.2* (CC BY-NC-SA)

Implementar una Zona SDN del tipo VxLAN entre dos o más nodos Proxmox

Realizaremos una VxLAN entre dos nodos Proxmox, pero se pueden unir más, con las direcciones IP de nodo 192.168.30.221, 192.168.30.119.
Crearemos una zona VxLAN llamada ZonVxLAN, agregua todas las IP de los nodos a la lista de direcciones de pares. Utilizaremos una MTU predeterminada de 1450 en los contenedores o MV.

Licencia Creative Commons BY-NC-SA.

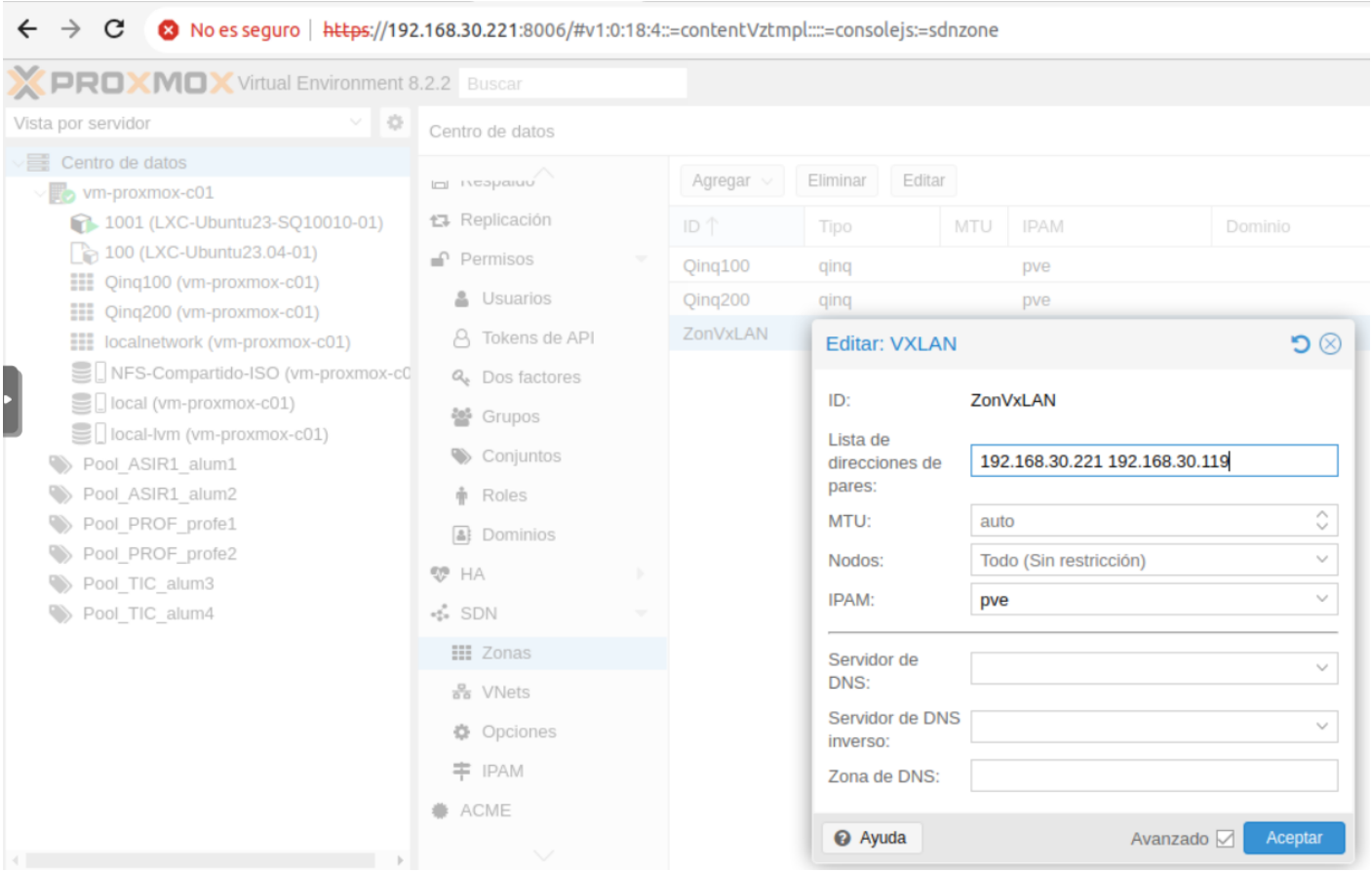


Imagen de elaboración propia· *Creación de la Zona SDN de tipo VxLAN entre dos nodos Proxmox* (CC BY-NC-SA)

Crea una VNet denominada "SwVxLAN1" utilizando la zona VXLAN "ZonVxLAN" creada anteriormente, con etiqueta 300:

Licencia Creative Commons BY-NC-SA.

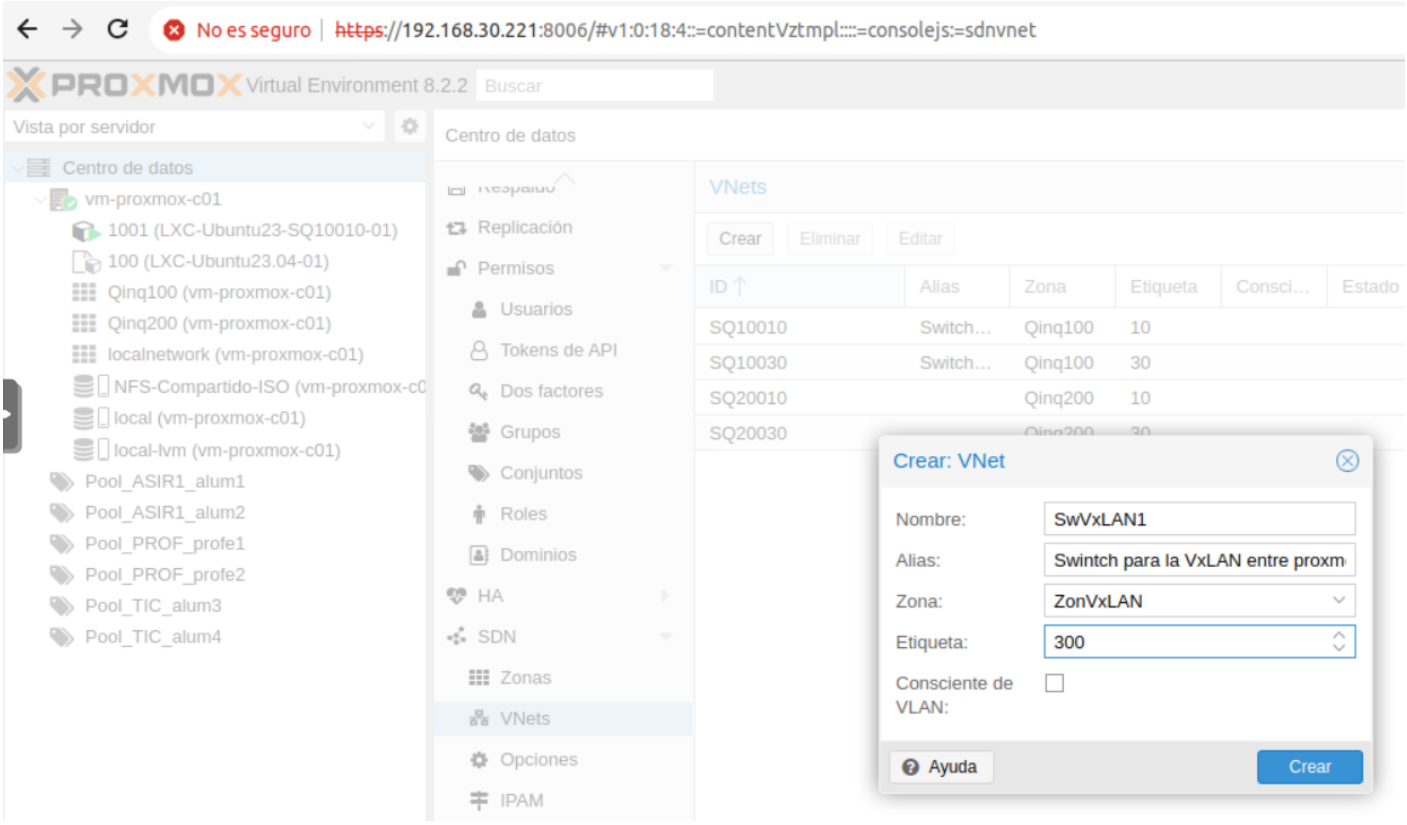


Imagen de elaboración propia· *Creación de VNet "SwVxLAN1"* (CC BY-NC-SA)

Aplica la configuración en la SDN para crear redes virtuales y crea un contenedor uniendo su interfaz de red al SwVxLAN1 con una MTU de 1450 y una IP estática 10.0.4.100/24

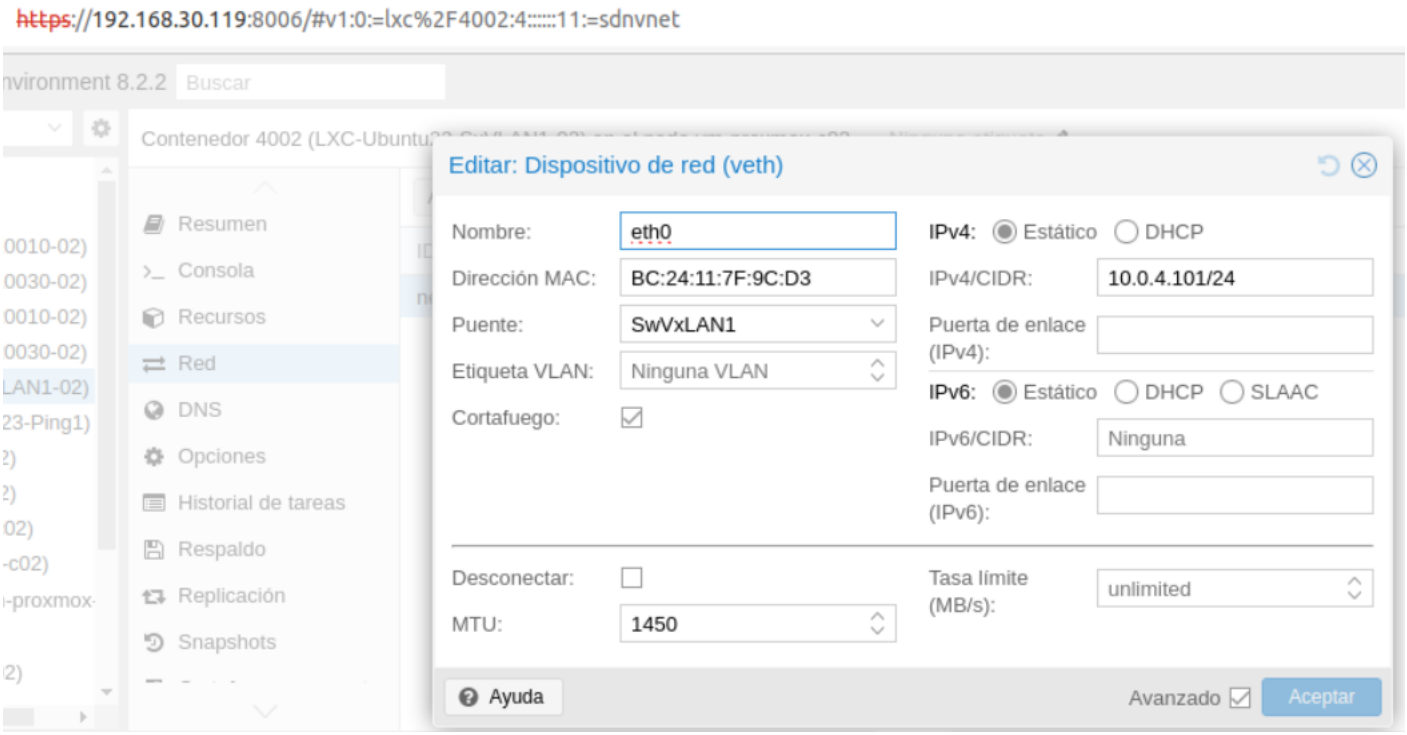


Imagen de elaboración propia· *Configuración de red de un contenedor en la VxLAN en el nodo c01 de Proxmox* (CC BY-NC-SA)

Licencia Creative Commons BY-NC-SA.

Ahora, haremos lo mismos pasos en el nodo c02 de Proxmox:



Imagen de elaboración propia· *Creación de Zona SDN del tipo VxLAN en el nodo c02 de Proxmox* (CC BY-NC-SA)

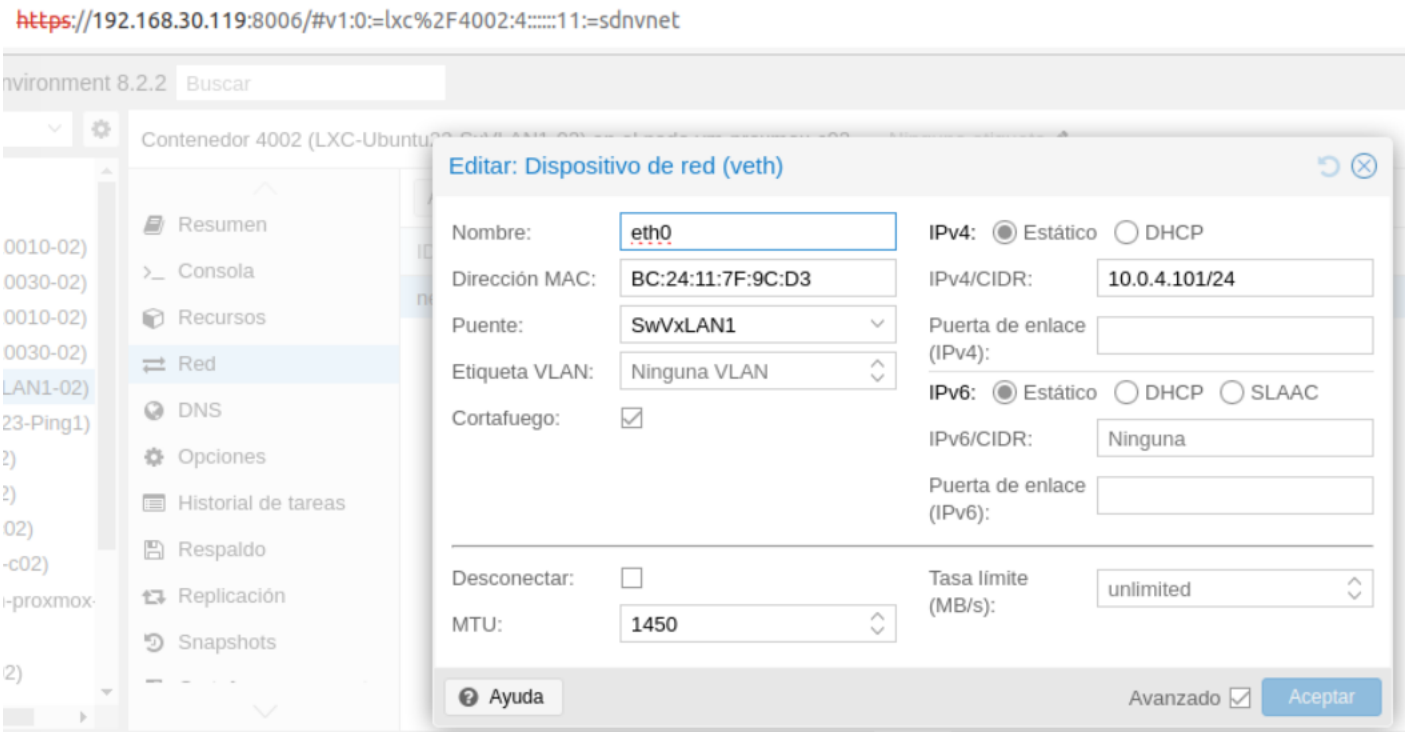


Imagen de elaboración propia· *Configuración de red del CT 4002 en el nodo c02 de Proxmox* (CC BY-NC-SA)

Comprobaremos la interconexión entre contenedores de la VxLAN:

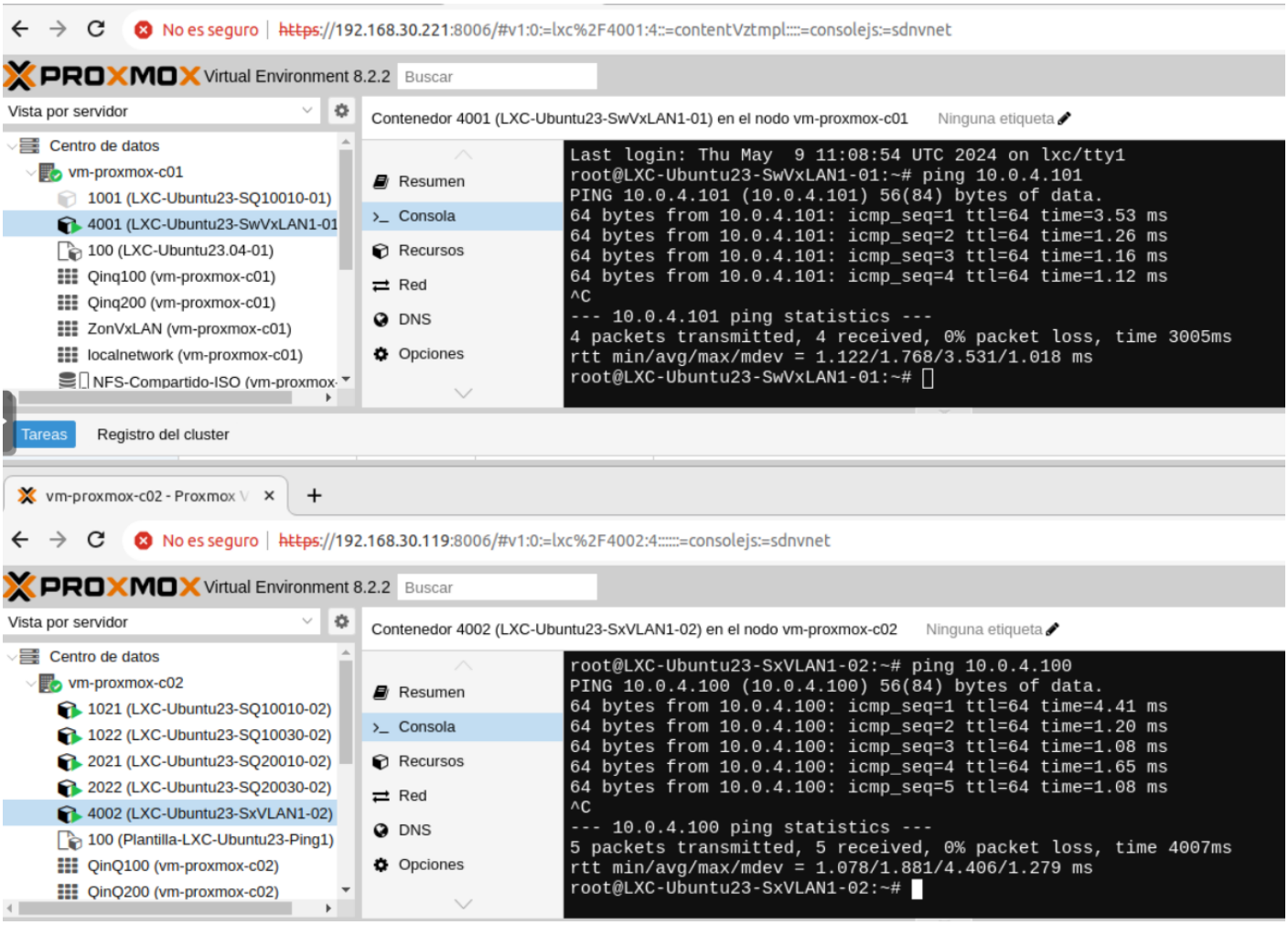


Imagen de elaboración propia· *Ping entre CT4001 y CT4002 que se encuentran en dos nodos Proxmox distintos* (CC BY-NC-SA)

Ahora solo nos quedaría cifrar el tunel. Proxmox ha añadido la posibilidad de utilizar (que no viene por defecto) VxLAN IPSEC Encryption, con un cifrado AES 256-sha1. Para agregar cifrado IPSEC en una VxLAN, deberá reducir la MTU en 60 bytes adicionales para IPv4 u 80 bytes para IPv6 para manejar el cifrado. Entonces, con un MTU de 1500 reales predeterminados, debe usar un MTU de 1370 (1370+80(IPSEC)+50(VXLAN)==1500).

Licencia Creative Commons BY-NC-SA.

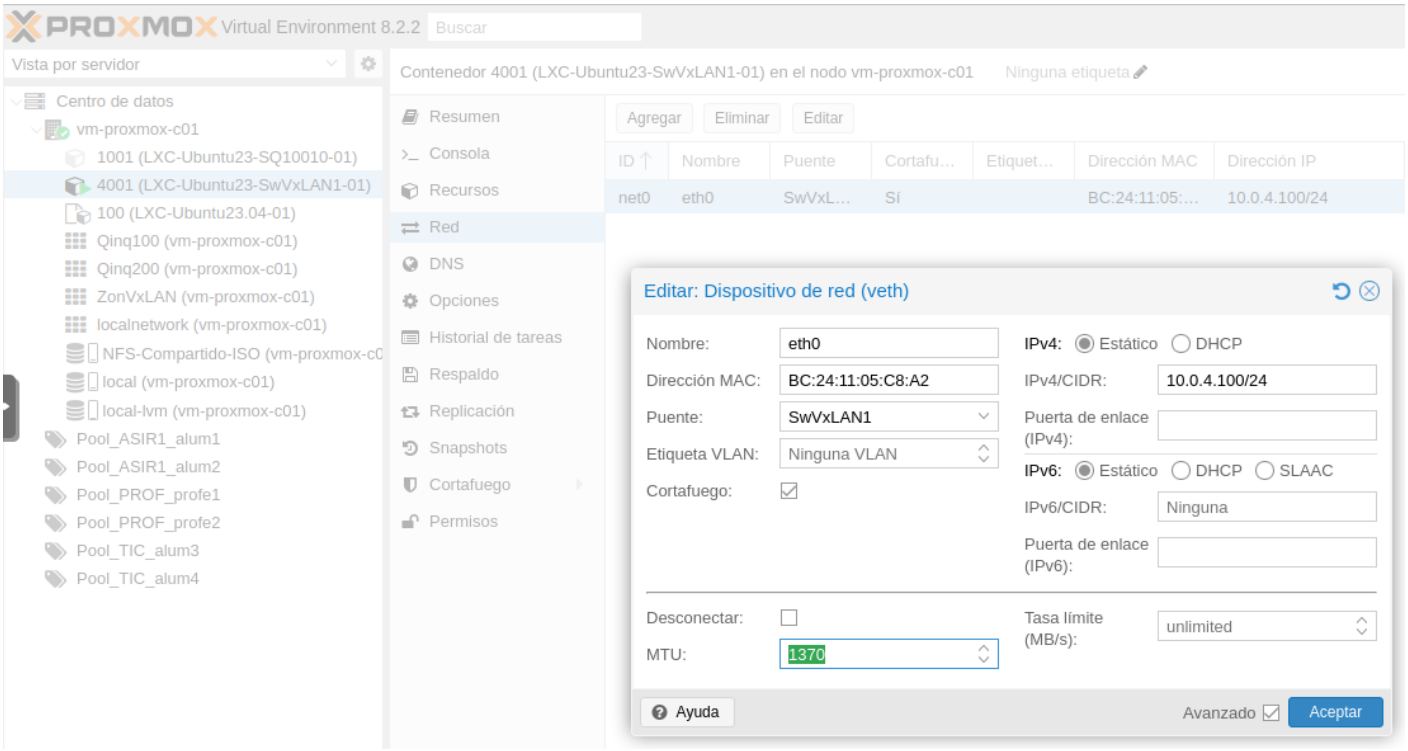


Imagen de elaboración propia· *Cambio el MTU a 1370 en cada contenedor o MV pertenecientes a la VxLAN* (CC BY-NC-SA)

En primer lugar debemos instalar el paquete "strongswan" en los nodos Proxmox de los extremos de los pares de la VxLAN:

```
apt install strongswan
```

Debemos modificar el fichero de configuración **/etc/ipsec.conf**. Cifraremos el tráfico UDP por el puerto 4789 que es el utilizado por VxLAN.

```
conf %default
    ike=aes256-sha1-modp1024!  # the fastest, but reasonably secure cipher on modern HW
    esp=aes256-sha1!
    leftfirewall=yes        # this is necessary when using Proxmox VE firewall rules

conf output
    rightsubnet=%dynamic[udp/4789]
    right=%any
    type=transport
```

```
    authby=psk
    auto=route

conn input
    leftsubnet=%dynamic[udp/4789]
    type=transport
    authby=psk
    auto=route
```

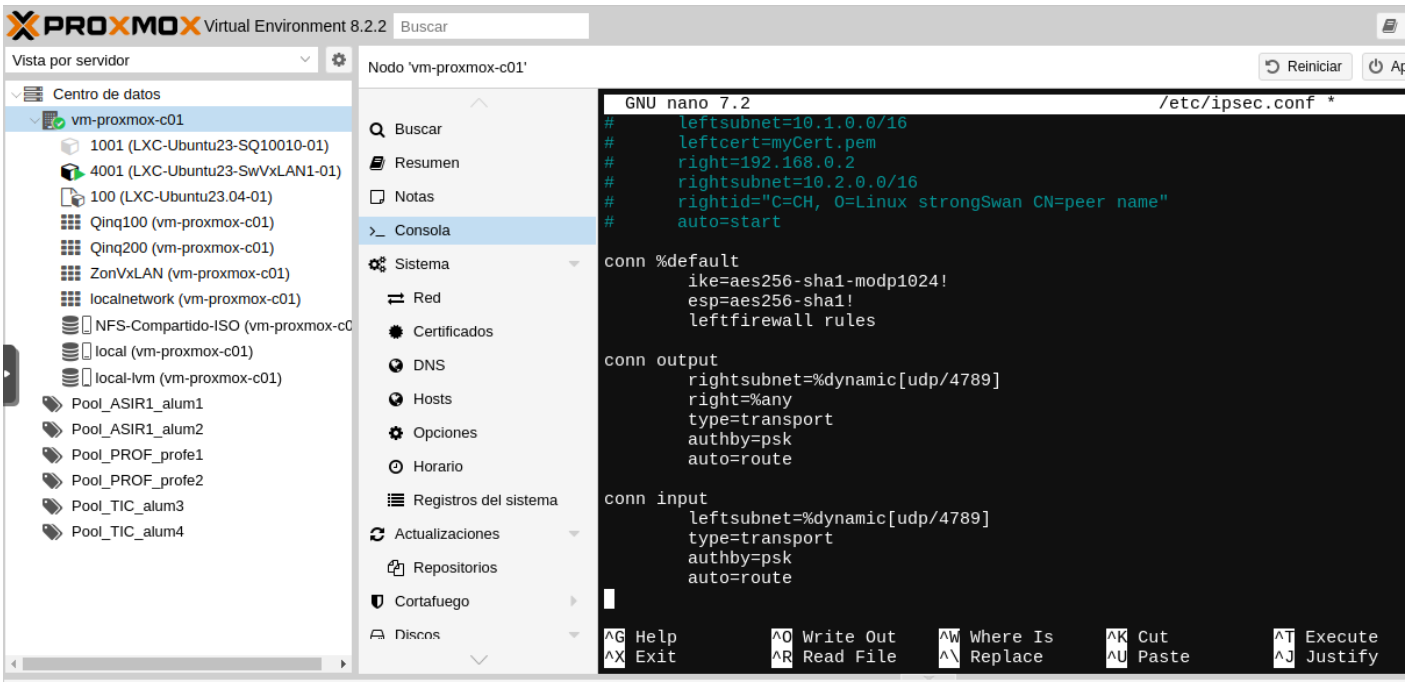


Imagen de elaboración propia· *Modificación del fichero /etc/ipsec.conf* (CC BY-NC-SA)

Tenemos que generar una clave pre-compartida, para poder comenzar la negociación de seguridad en el tunel:

```
openssl rand -base64 128
```

y añadimos la clave al fichero /etc/ipsec.secrets

: PSK <generatedbase64key>

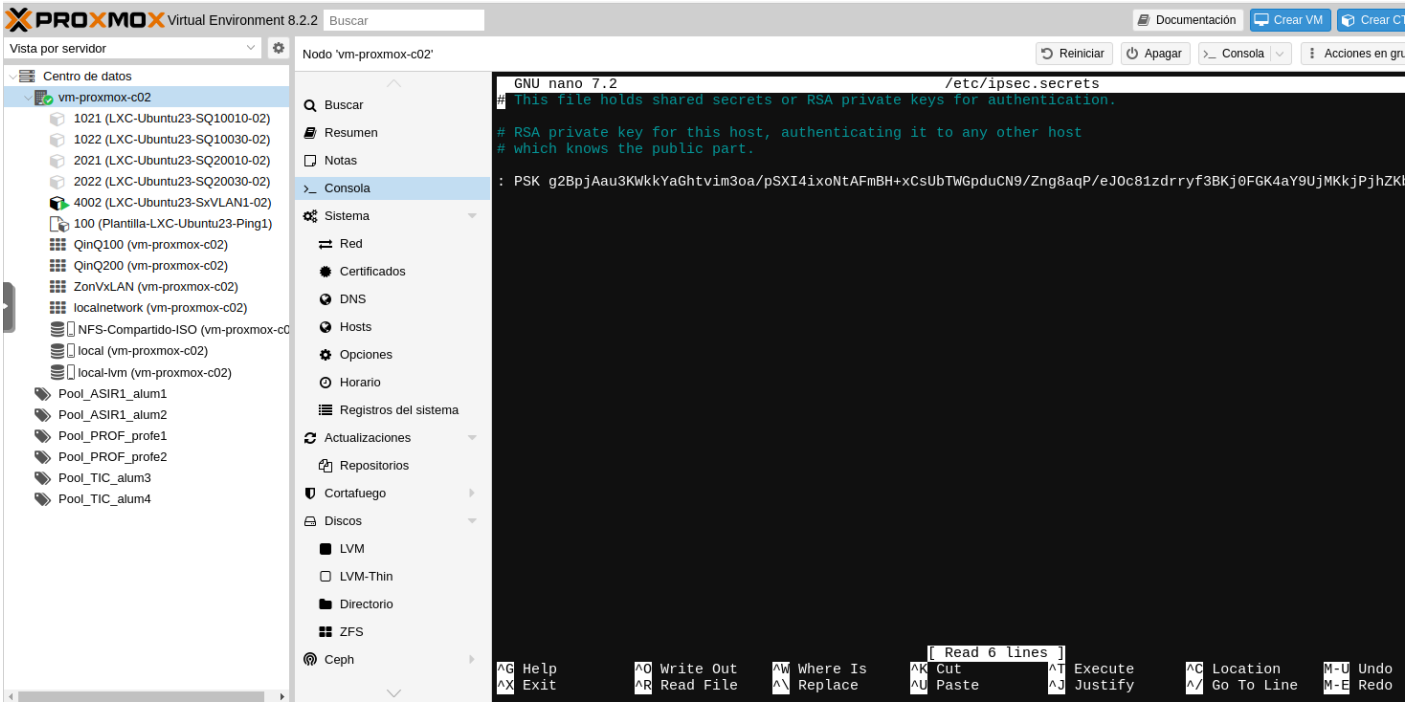


Imagen de elaboración propia· *Modificación del fichero /etc/ipsec.secrets* (CC BY-NC-SA)

Copia los dos ficheros en todos los nodo de Proxmox que formen parte de la VxLAN.

Revisión #1
Creado 11 mayo 2024 20:24:34 por Daniel Cano Verdú
Actualizado 12 mayo 2024 16:53:02 por Daniel Cano Verdú

Licencia Creative Commons BY-NC-SA.