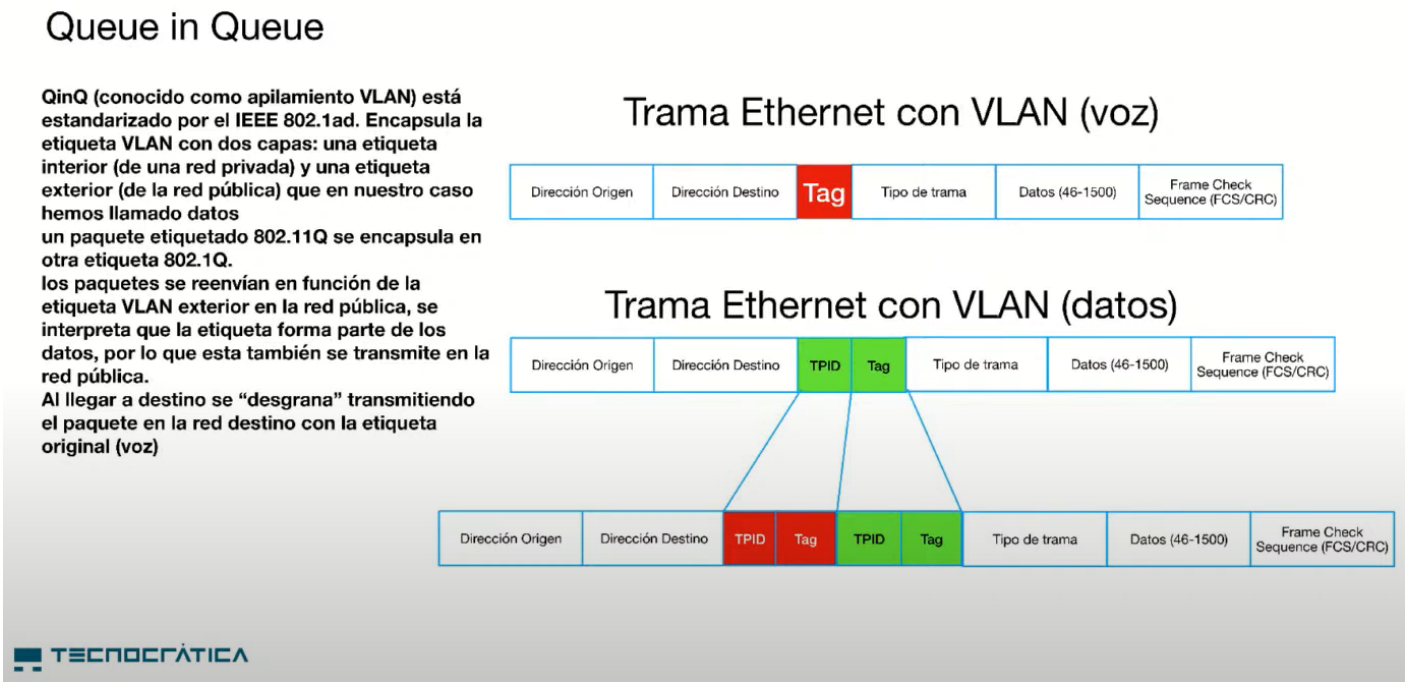
4.4.- SDN QinQ.

¿Qué es una VLAN Queue in Queue?



Eduardo Taboada (Tecnocratica.net)· *VLAN Queue in Queue* (Todos los derechos reservados)

> **La tunelización Q-in-Q en VLAN permiten crear una conexión Ethernet de capa 2 entre dos extremos y dentro del tunel podemos tener otras 4096 VLAN, es decir, lo que estamos haciendo es meter una VLAN dentro de otra VLAN.**

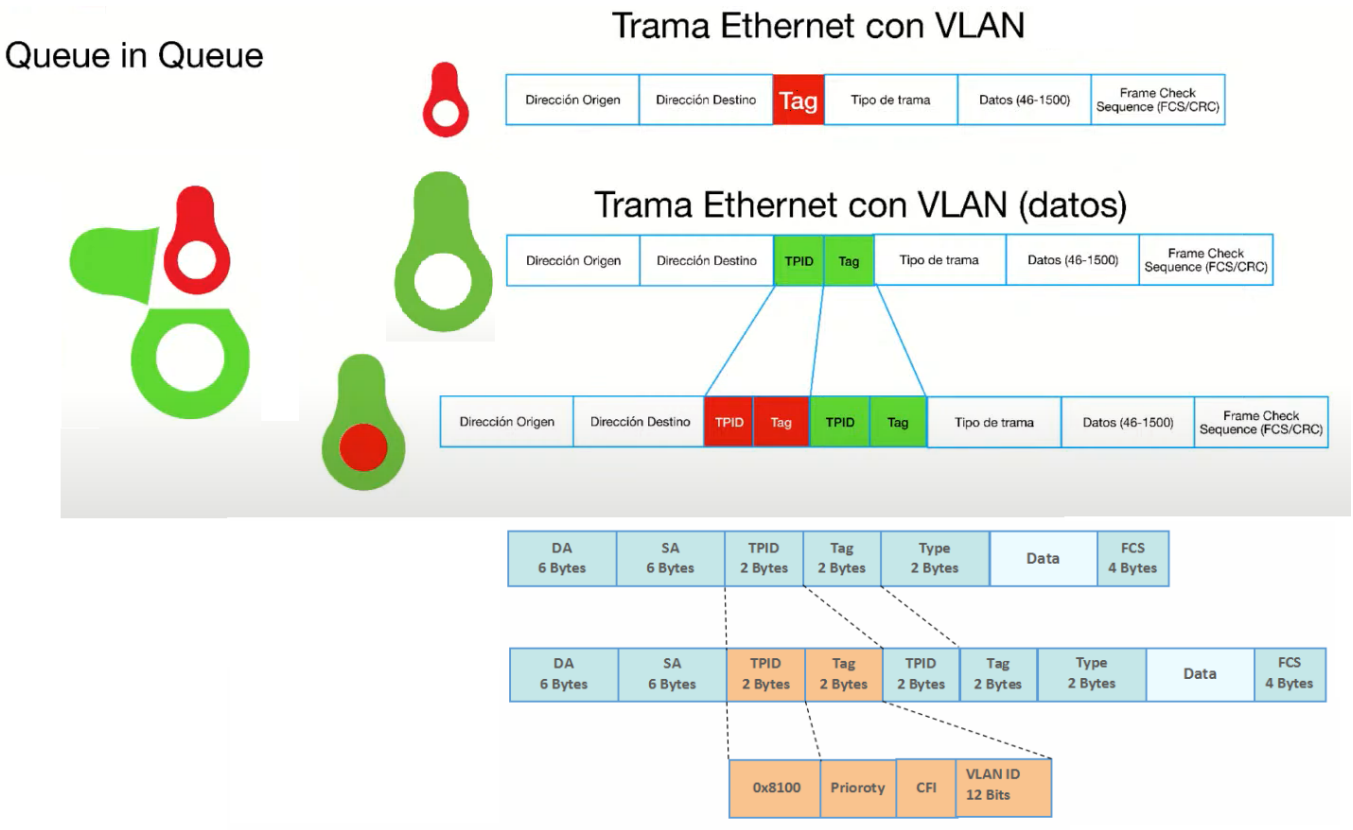


Imagen de elaboración propia· *Tunel QinQ de capa 2 y dentro una trama de VLAN de capa 2* (CC BY-NC-SA)

Q-in-Q está estandarizado por el IEEE 802.1ad. Encapsula la etiqueta VLAN con dos capas: una etiqueta interior (de una red privada) y una etiqueta exterior (de la red pública). El etiquetado VLAN tradicional que utiliza el IEEE 802.1Q es incapaz de identificar y aislar los datos de los usuarios en las tramas crecientes de Ethernet. La tecnología QinQ se utiliza para ampliar la cantidad VLANs hasta **4096×4096**, de este modo se podrán ahorrar ID de VLAN.

Los paquetes QinQ tienen un formato fijo. Normalmente, un paquete etiquetado 802.11Q se encapsula en otra etiqueta 802.1Q, de la que deriva el nombre «Q-in-Q». Durante la transmisión, los paquetes se reenvían en función de la etiqueta VLAN exterior en la red pública, se interpreta que la etiqueta forma parte de los datos, por lo que esta también se transmite en la red pública. Como contienen esta forma de doble etiqueta, los paquetes QinQ tienen 4 bytes más que los paquetes comunes con etiqueta VLAN 802.1Q.

Reduce la MTU en los vínculos de acceso en al menos 4 bytes para que las tramas no excedan la MTU del enlace de troncalización cuando se agreguen las etiquetas VLAN.

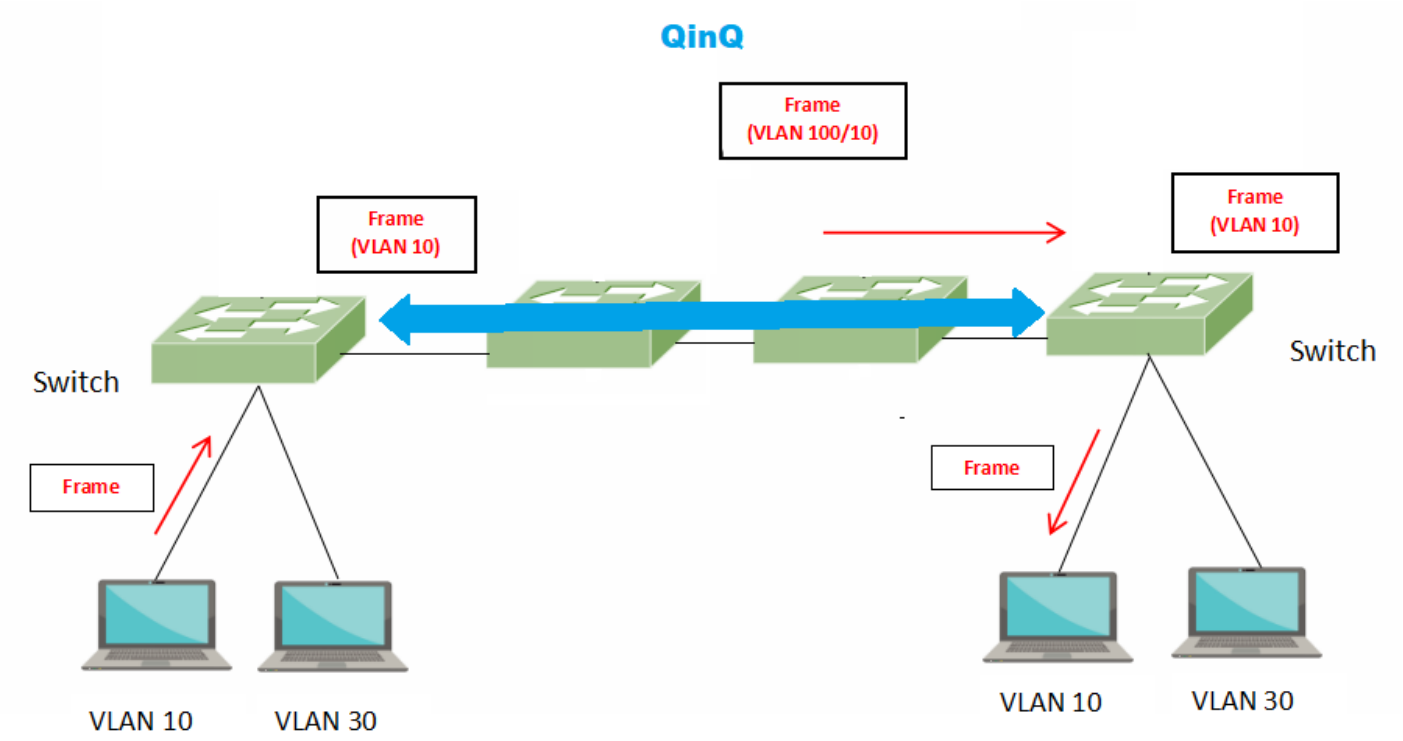


Imagen de elaboración propia· *Esquema de tunelización QinQ de VLAN* (CC BY-NC-SA)

Implementación de una Zona de SDN del tipo QinQ

Un caso de uso típico para esta configuración es un proveedor de hosting que proporciona una red aislada a los clientes para la comunicación de VM pero aísla las VM de otros clientes. Con QinQ cada cliente podría tener su propia VLAN (máximo de clientes 4096) pero para cada cliente se le podría proporcionar 4096 VLAN propias dentro de su tunel y aislar a su vez su tráfico de red.

Para el primer nodo Proxmox, crea una zona QinQ llamada "Qinq100" con el servicio VLAN 100 (que será la VLAN que vean todos los switch):

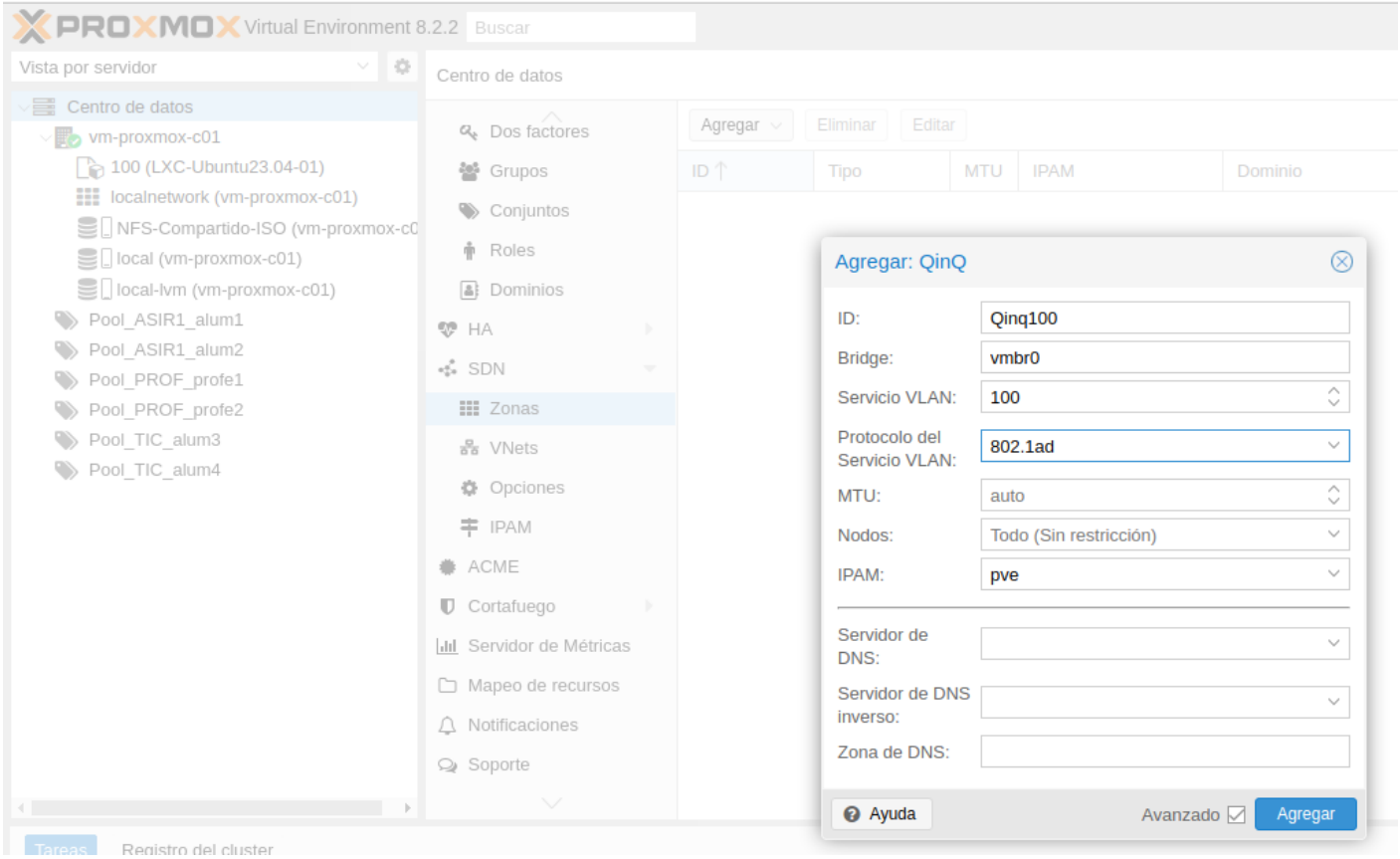


Imagen de elaboración propia· *Creación de la Zona SDN tipo QinQ* (CC BY-NC-SA)

Crea una VNet denominada "SQ10010" con VLAN-ID 10 en la zona "QinqZona100" creada anteriormente.

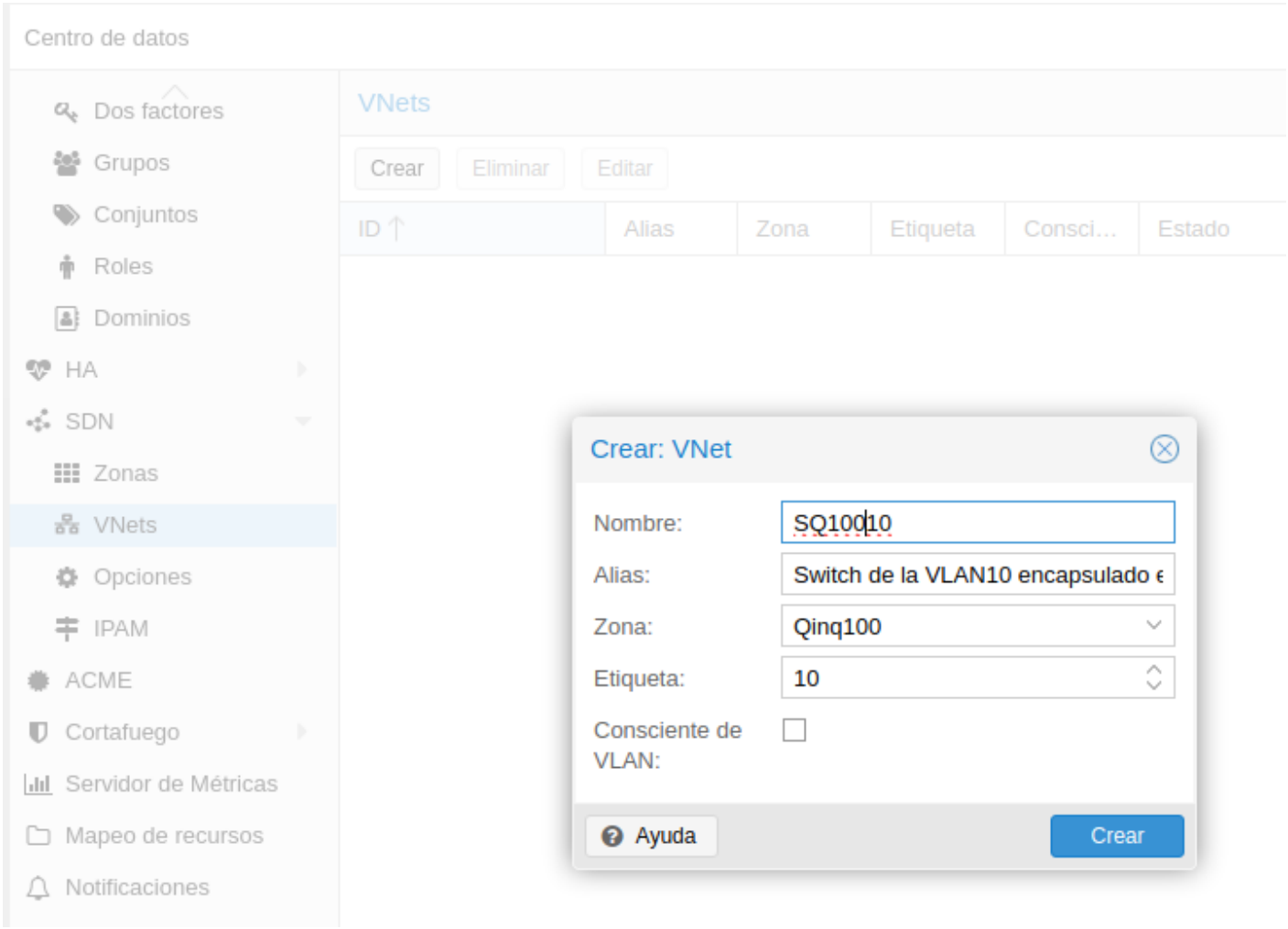


Imagen de elaboración propia· *Creación de la VNet SQ10010 con etiqueta VLAN 10 perteneciente a la Zona QinQ 100* (CC BY-NC-SA)

Crea una VNet denominada "SQ10030" con VLAN-ID 30 en la zona "QinqZona100" creada anteriormente.

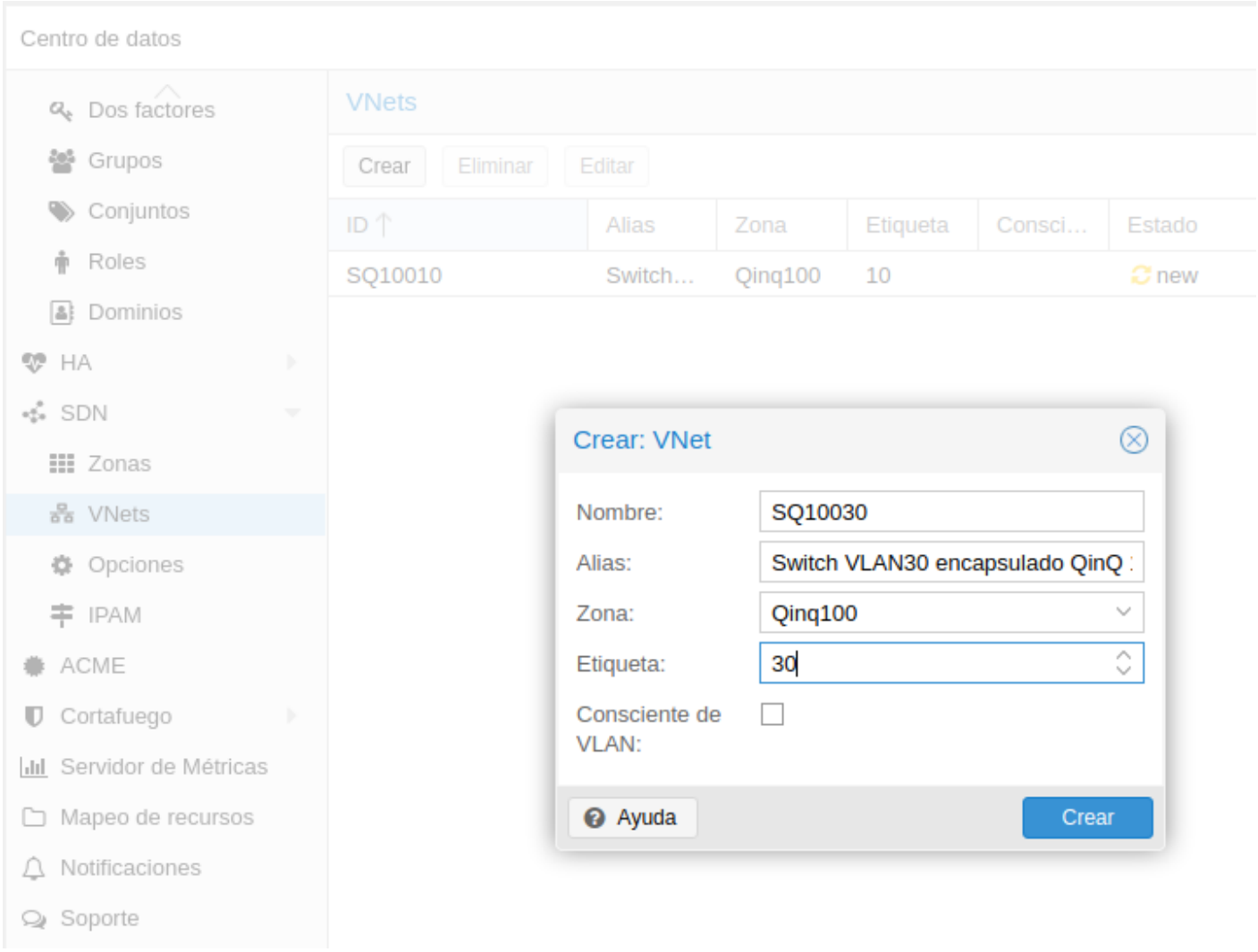


Imagen de elaboración propia· *Creación VNet SQ10030 con etiqueta VLAN 30 encapsulado en QinQ 100* (CC BY-NC-SA)

Crea una zona QinQ llamada "Qinq200" con el servicio VLAN 200 (que será para otro cliente):

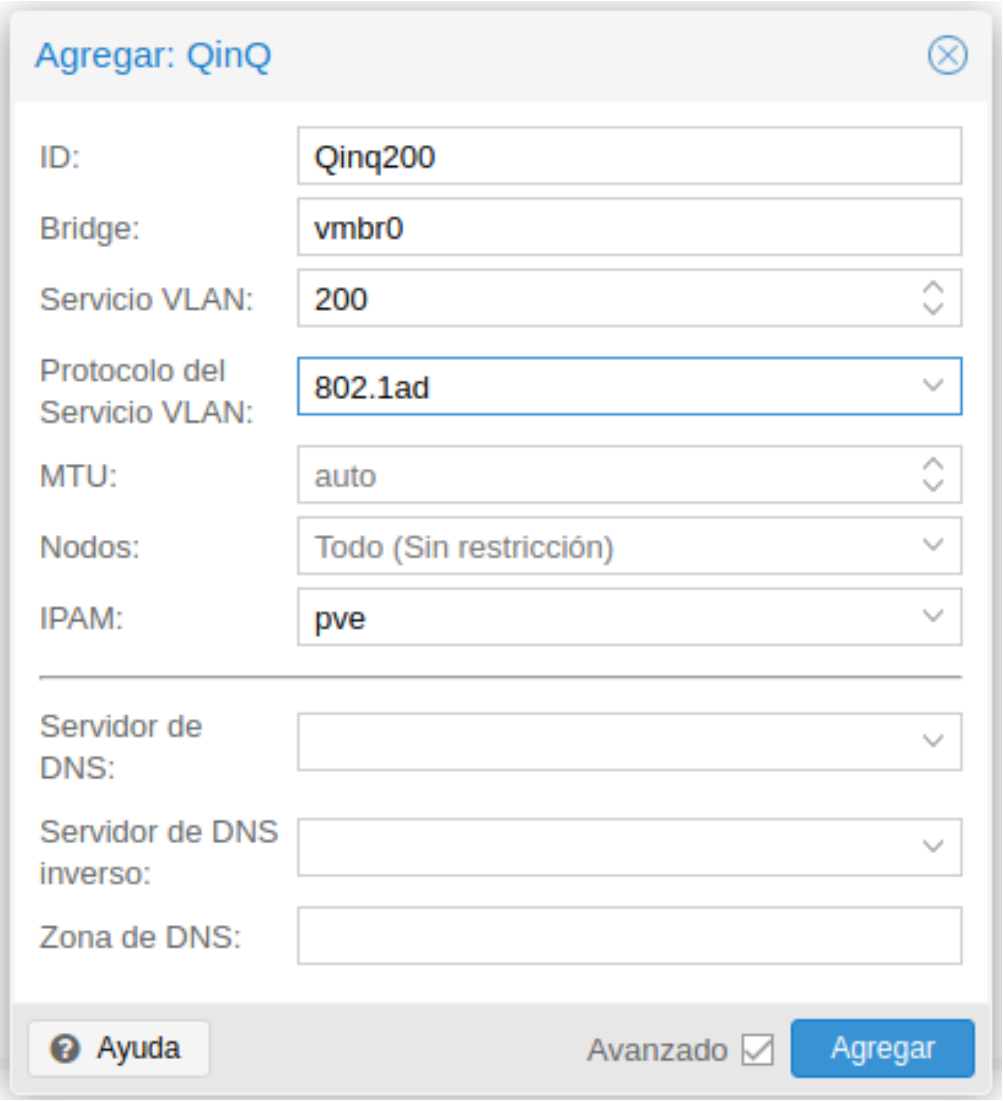


Imagen de elaboración propia· *Creación de otra Zona QinQ para comprobar el aislamiento del tráfico Ethernet* (CC BY-NC-SA)

Crea una VNet denominada "SQ20010" con VLAN-ID 10 en la zona "Qinq200" creada anteriormente.

Crea una VNet denominada "SQ20030" con VLAN-ID 30 en la zona "Qinq200" creada anteriormente.

Aplica la configuración en SDN y repetir en mismo proceso en el nodo 2 de Proxmox.

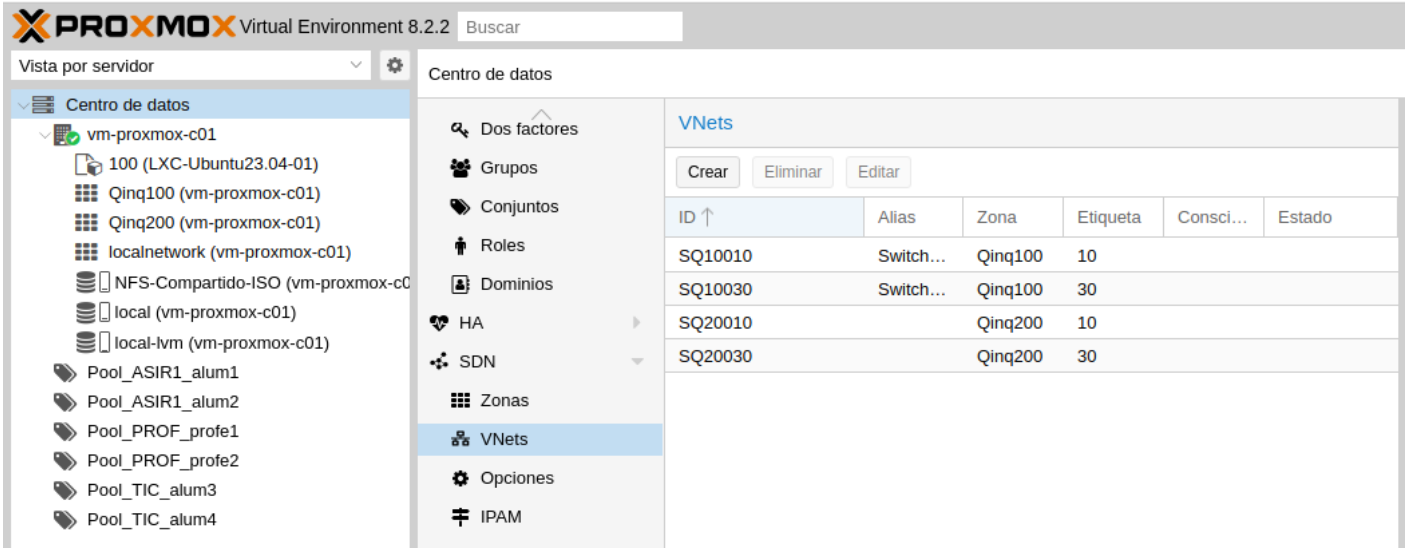


Imagen de elaboración propia· *Aplicar cambios en la SDN para crear toda la configuración de red* (CC BY-NC-SA)

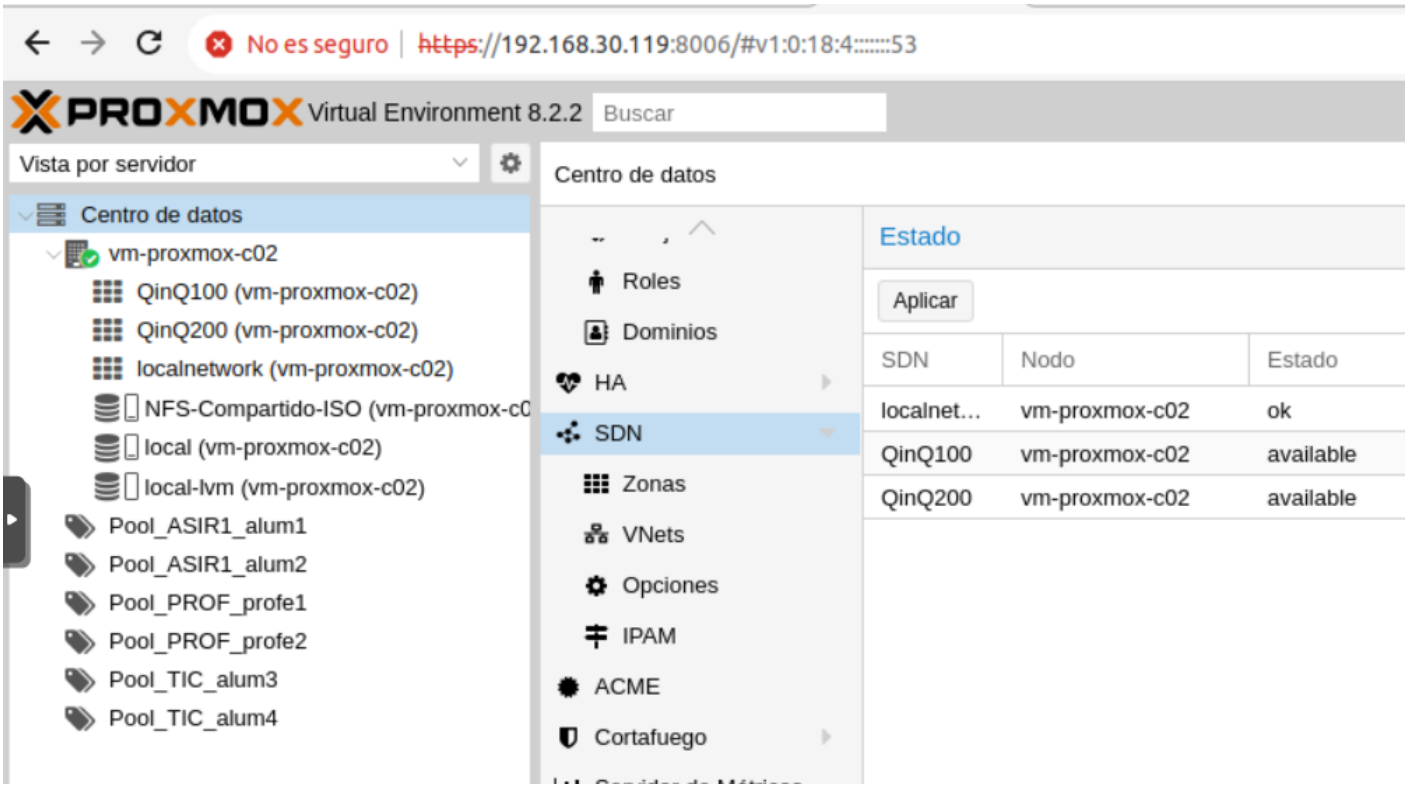


Imagen de elaboración propia· *Creación de las dos QinQ en el nodo 2 de Proxmox al igual que hemos hecho en el nodo 1* (CC BY-NC-SA)

Crea 4 contenedores en el nodo 1 de Proxmox, asignándoles IP según la siguiente tabla:

CLIENTE CPD	ID CONTENEDOR	IP CONTENEDOR	Zona QinQ	VNet VLAN
1	1001	10.0.1.110/16	QinqZona100	SQ100-10
	1002	10.0.1.130/16		SQ100-30
2	2001	10.0.1.210/16	QinqZona200	SQ200-10
	2002	10.0.1.230/16		SQ200-30

Ahora, crea 4 contenedores en el nodo 2 de Proxmox, asignándoles IP según la siguiente tabla:

CLIENTE CPD	ID CONTENEDOR	IP CONTENEDOR	Zona QinQ	VNet VLAN
1	1021	10.0.2.110/16	QinqZona100	SQ100-10
	1022	10.0.2.130/16		SQ100-30
2	2021	10.0.2.210/16	QinqZona200	SQ200-10
	2022	10.0.2.230/16		SQ200-30

De tal manera que el CT1001 solo puede hacer ping al CT1021 y viceversa, y no podrá hacer ping al resto de contenedores porque se encuentra el tráfico de tramas Ethernet aislado por su QinQ:

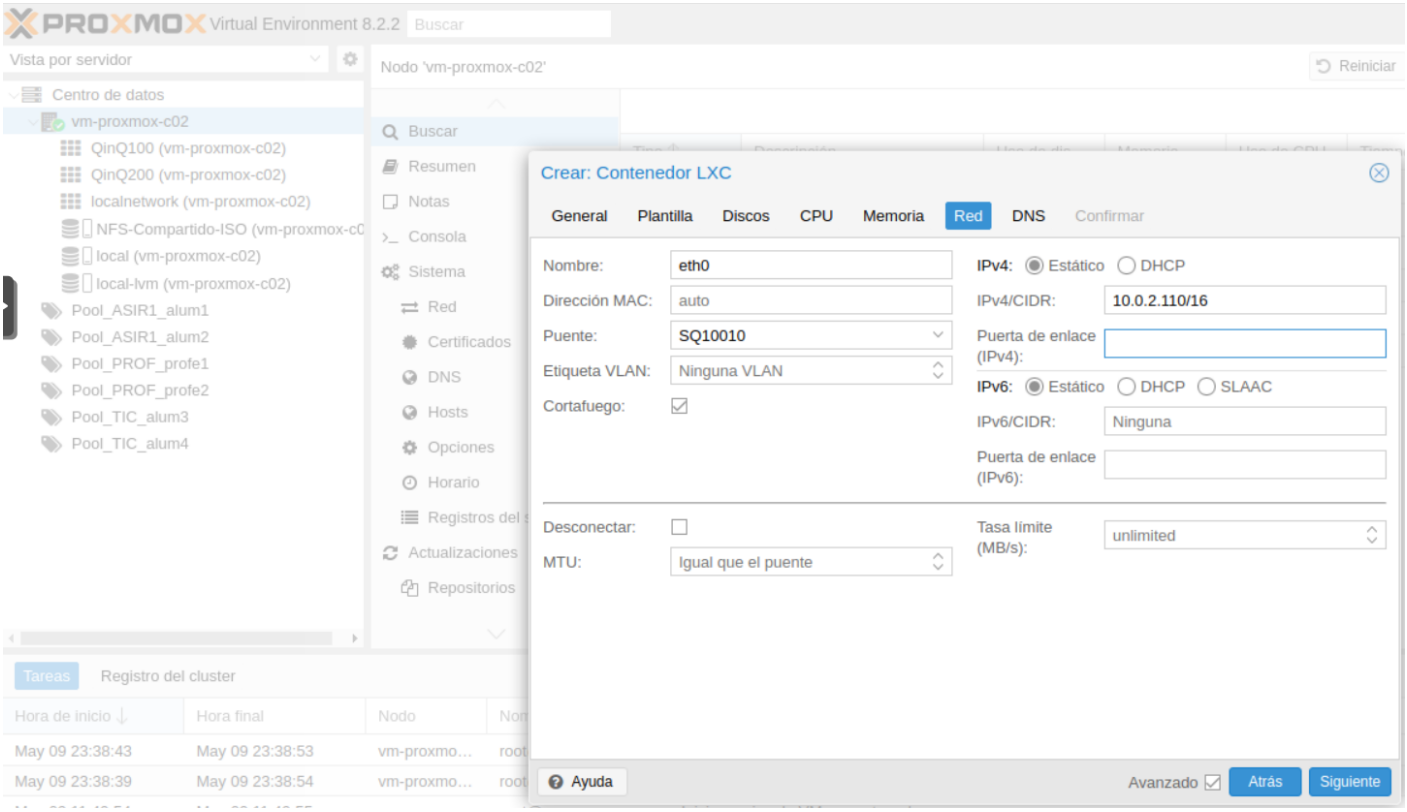


Imagen de elaboración propia· *Creación del contenedor 1021* (CC BY-NC-SA)

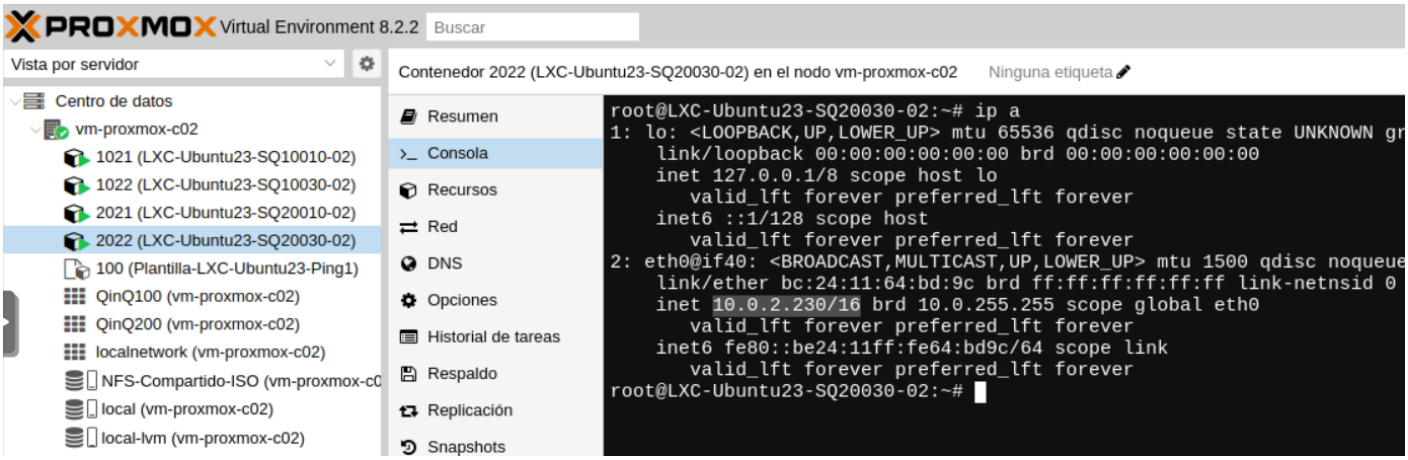


Imagen de elaboración propia· *Configuración de red del contenedor 2022* (CC BY-NC-SA)

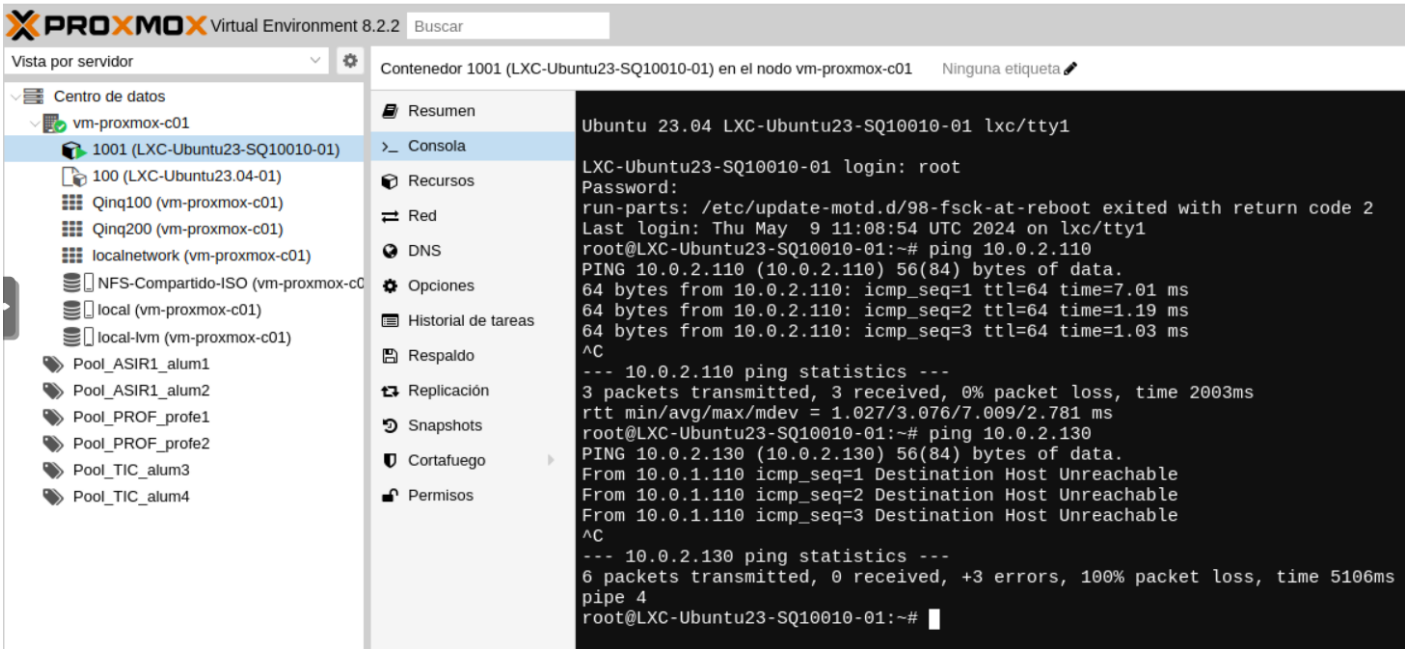


Imagen de elaboración propia· *Ping desde el CT 1010 del nodo 1 al CT 2010 del nodo 2 y rechazados todos los demás* (CC BY-NC-SA)

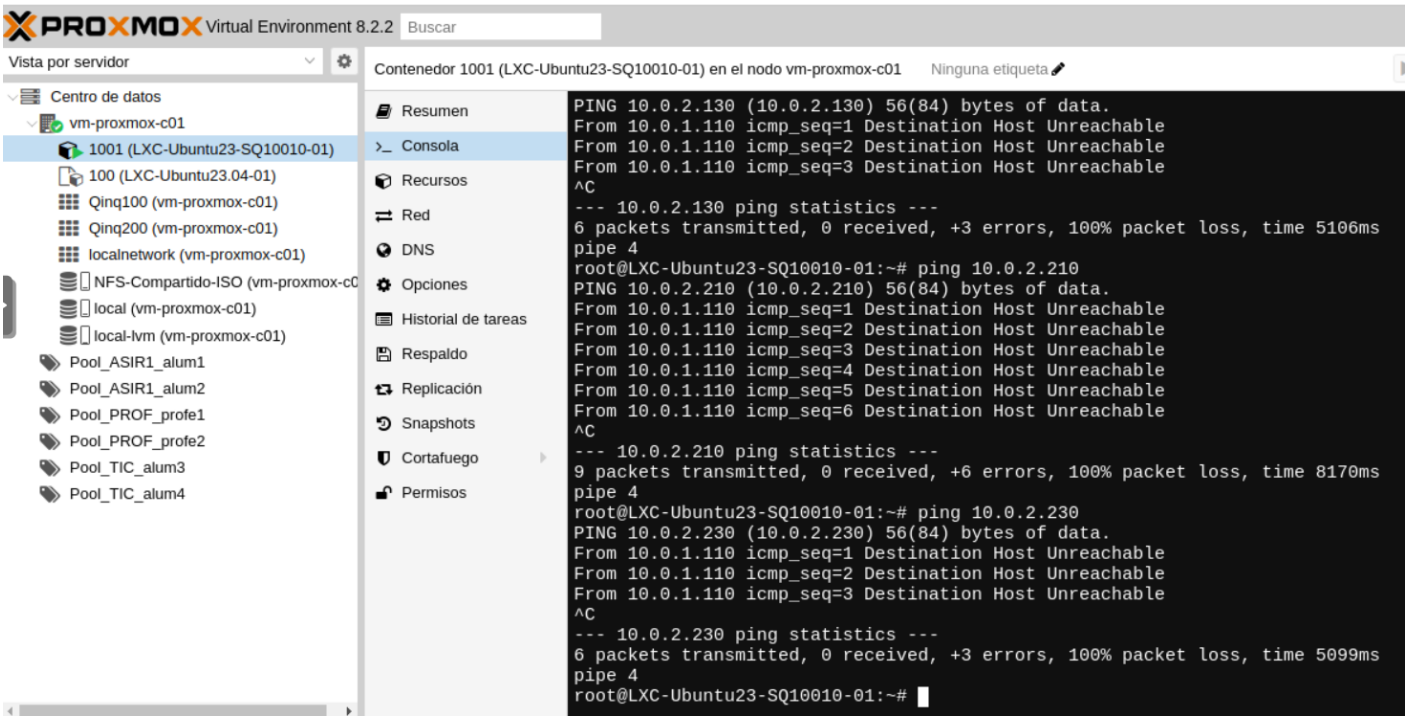


Imagen de elaboración propia· *Rechazados todos los ping al resto de CT tal y cómo se esperaba* (CC BY-NC-SA)

Revisión #1
Creado 11 mayo 2024 20:09:23 por Daniel Cano Verdú
Actualizado 12 mayo 2024 16:53:02 por Daniel Cano Verdú