



4.5.- SDN VxLAN.

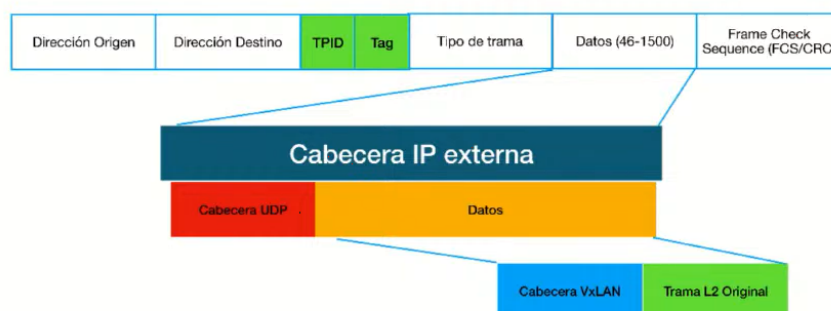
¿Qué es una VxLAN?

VxLAN

La VxLAN (LAN extensible virtual), permite extender las redes virtuales más allá de los límites de una sola red física. Funciona encapsulando los paquetes de red en otro paquete. Permite extender una red de Nivel o capa 2 en una red más extensa de Capa3. Permite encapsular el protocolo de dirección MAC (layer2) en datagramas de usuario (MAC-in-UDP).

Con la encapsulación VxLAN MAC-in-UDP, los paquetes originales se añadirán en una cabecera VxLAN y luego se colocarán en un paquete UDP-IP

Trama Ethernet



Trama Ethernet con VLAN (datos)



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, pueden 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.



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 ($1370 + 80(\text{IPSEC}) + 50(\text{VXLAN}) = 1500$).

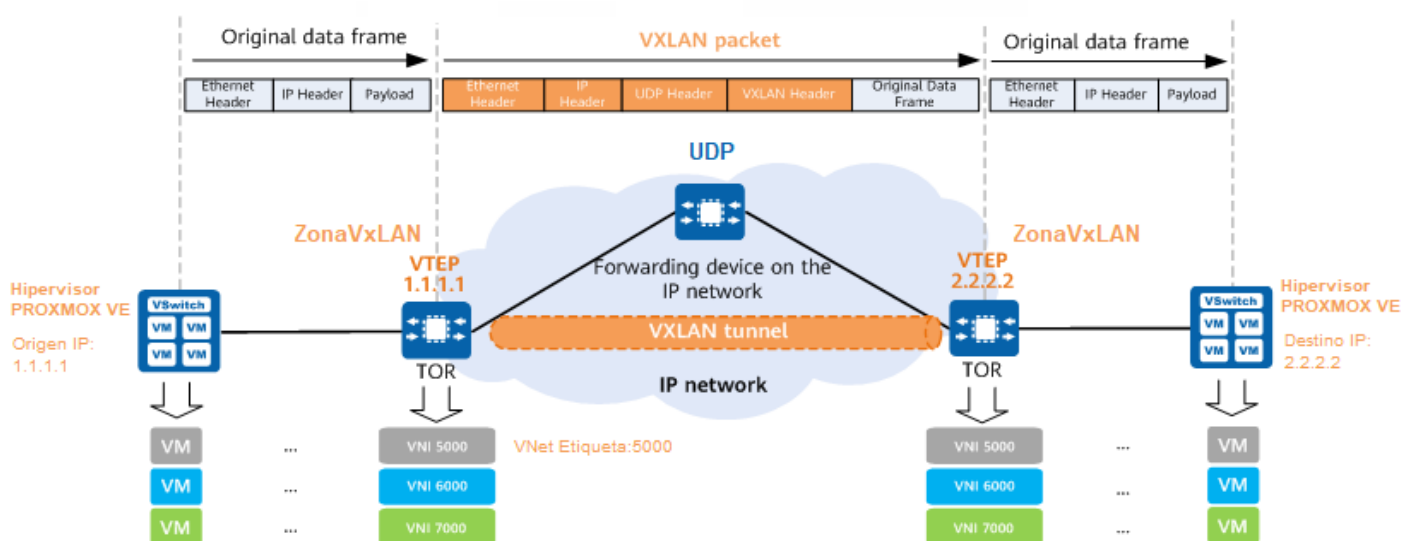


Imagen de elaboración propia: Esquema VxLAN en Proxmox VE 8.2 (CC BY-NC-SA)

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.



← → ↻ No es seguro | https://192.168.30.221:8006/#v1:0:18:4::contentVztmpl::=consolejs:=sdnzone

PROXMOX Virtual Environment 8.2.2

Vista por servidor

Centro de datos

vm-proxmox-c01

1001 (LXC-Ubuntu23-SQ10010-01)

100 (LXC-Ubuntu23.04-01)

Qinq100 (vm-proxmox-c01)

Qinq200 (vm-proxmox-c01)

localnetwork (vm-proxmox-c01)

NFS-Compartido-ISO (vm-proxmox-c01)

local (vm-proxmox-c01)

local-lvm (vm-proxmox-c01)

Pool_ASIR1_alum1

Pool_ASIR1_alum2

Pool_PROF_profe1

Pool_PROF_profe2

Pool_TIC_alum3

Pool_TIC_alum4

Replicación

Permisos

Usuarios

Tokens de API

Dos factores

Grupos

Conjuntos

Roles

Dominios

HA

SDN

Zonas

VNets

Opciones

IPAM

ACME

ID ↑	Tipo	MTU	IPAM	Dominio
Qinq100	qinq		pve	
Qinq200	qinq		pve	
ZonVxLAN				

Editar: VXLAN

ID: ZonVxLAN

Lista de direcciones de pares: 192.168.30.221 192.168.30.119

MTU: auto

Nodos: Todo (Sin restricción)

IPAM: pve

Servidor de DNS:

Servidor de DNS inverso:

Zona de DNS:

☒ Avanzado

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:



Proxmox Virtual Environment 8.2.2

Vista por servidor

Centro de datos

- vm-proxmox-c01
 - 1001 (LXC-Ubuntu23-SQ10010-01)
 - 100 (LXC-Ubuntu23.04-01)
 - Qinq100 (vm-proxmox-c01)
 - Qinq200 (vm-proxmox-c01)
 - localnetwork (vm-proxmox-c01)
 - NFS-Compartido-ISO (vm-proxmox-c01)
 - local (vm-proxmox-c01)
 - local-lvm (vm-proxmox-c01)
 - Pool_ASIR1_alum1
 - Pool_ASIR1_alum2
 - Pool_PROF_profe1
 - Pool_PROF_profe2
 - Pool_TIC_alum3
 - Pool_TIC_alum4

Centro de datos

- Replicación
- Permisos
- Usuarios
- Tokens de API
- Dos factores
- Grupos
- Conjuntos
- Roles
- Dominios
- HA
- SDN
 - Zonas
 - VNets
- Opciones
- IPAM

VNets

ID	Alias	Zona	Etiqueta	Consci...	Estado
SQ10010	Switch...	Qinq100	10		
SQ10030	Switch...	Qinq100	30		
SQ20010		Qinq200	10		
SQ20030		Qinq200	30		

Crear: VNet

Nombre: SwVxLAN1

Alias: Swintch para la VxLAN entre proxm

Zona: ZonVxLAN

Etiqueta: 300

Consciente de VLAN: ☐

Ayuda Crear

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

https://192.168.30.119:8006/#v1:0:=lxc%2F4002:4:11:=sdnvn

Proxmox Virtual Environment 8.2.2

Contenedor 4002 (LXC-Ubuntu23.04-01)

Editar: Dispositivo de red (veth)

Nombre: eth0

Dirección MAC: BC:24:11:7F:9C:D3

Puente: SwVxLAN1

Etiqueta VLAN: Ninguna VLAN

Cortafuego: ☒

IPv4: ☒ Estático ☐ DHCP

IPv4/CIDR: 10.0.4.101/24

Puerta de enlace (IPv4):

IPv6: ☒ Estático ☐ DHCP ☐ SLAAC

IPv6/CIDR: Ninguna

Puerta de enlace (IPv6):

Desconectar: ☐

MTU: 1450

Tasa límite (MB/s): unlimited

Ayuda Avanzado ☒ Aceptar

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



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

← → ↻ No es seguro | <https://192.168.30.119:8006/#v1:0:18:4:::=-consolejs:53>

PROXMOX Virtual Environment 8.2.2

Vista por servidor ▾ ⚙

Centro de datos

- vm-proxmox-c02
 - 1021 (LXC-Ubuntu23-SQ10010-02)
 - 1022 (LXC-Ubuntu23-SQ10030-02)
 - 2021 (LXC-Ubuntu23-SQ20010-02)
 - 2022 (LXC-Ubuntu23-SQ20030-02)
 - 100 (Plantilla-LXC-Ubuntu23-Ping1)
 - QinQ100 (vm-proxmox-c02)
 - QinQ200 (vm-proxmox-c02)
 - ZonVxLAN (vm-proxmox-c02)
 - localnetwork (vm-proxmox-c02)
 - NFS-Compartido-ISO (vm-proxmox-c02)

Centro de datos

- Conjuntos
- Roles
- Dominios
- HA
- SDN**
- Zonas
- VNets
- Opciones

Estado

SDN	Nodo	Estado
localnetwork	vm-proxmox-c02	ok
QinQ100	vm-proxmox-c02	available
QinQ200	vm-proxmox-c02	available
ZonVxLAN	vm-proxmox-c02	available

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

<https://192.168.30.119:8006/#v1:0:=lxc%2F4002:4:::11:=sdnvnnet>

Virtual Environment 8.2.2

Contenedor 4002 (LXC-Ubuntu23-SQ10010-02)

- Resumen
- Consola
- Recursos
- Red**
- DNS
- Opciones
- Historial de tareas
- Respaldo
- Replicación
- Snapshots

Editar: Dispositivo de red (veth)

Nombre: IPv4: ☒ Estático ☐ DHCP

Dirección MAC: IPv4/CIDR:

Puente: Puerta de enlace (IPv4):

Etiqueta VLAN: IPv6: ☒ Estático ☐ DHCP ☐ SLAAC

Cortafuego: ☒ IPv6/CIDR:

Desconectar: ☐ Puerta de enlace (IPv6):

MTU: Tasa límite (MB/s):

☒ Avanzado

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:

The image shows two screenshots of the Proxmox Virtual Environment 8.2.2 console. The top screenshot shows the console for container 4001 (LXC-Ubuntu23-SwVxLAN1-01) on node vm-proxmox-c01. The console output shows a successful ping test to 10.0.4.101, with 4 packets transmitted and 4 received, 0% packet loss, and a time of 3005ms. The bottom screenshot shows the console for container 4002 (LXC-Ubuntu23-SxVLAN1-02) on node vm-proxmox-c02. The console output shows a successful ping test to 10.0.4.100, with 5 packets transmitted and 5 received, 0% packet loss, and a time of 4007ms.

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).



PROXMOX Virtual Environment 8.2.2

Vista por servidor

Centro de datos

- vm-proxmox-c01
 - 1001 (LXC-Ubuntu23-SQ10010-01)
 - 4001 (LXC-Ubuntu23-SwVxLAN1-01)**
 - 100 (LXC-Ubuntu23.04-01)
 - Qinq100 (vm-proxmox-c01)
 - Qinq200 (vm-proxmox-c01)
 - ZonVxLAN (vm-proxmox-c01)
 - localnetwork (vm-proxmox-c01)
 - NFS-Compartido-ISO (vm-proxmox-c01)
 - local (vm-proxmox-c01)
 - local-lvm (vm-proxmox-c01)
 - Pool_ASIR1_alum1
 - Pool_ASIR1_alum2
 - Pool_PROF_profe1
 - Pool_PROF_profe2
 - Pool_TIC_alum3
 - Pool_TIC_alum4

Contenedor 4001 (LXC-Ubuntu23-SwVxLAN1-01) en el nodo vm-proxmox-c01 Ninguna etiqueta

Resumen

Consola

Recursos

Red

DNS

Opciones

Historial de tareas

Respaldo

Replicación

Snapshots

Cortafuegos

Permisos

ID	Nombre	Puente	Cortafu...	Etiquet...	Dirección MAC	Dirección IP
net0	eth0	SwVxL...	Sí		BC:24:11:05:...	10.0.4.100/24

Editar: Dispositivo de red (veth)

Nombre: IPv4: ☒ Estático ☐ DHCP

Dirección MAC: IPv4/CIDR:

Puente: Puerta de enlace (IPv4):

Etiqueta VLAN: IPv6: ☒ Estático ☐ DHCP ☐ SLAAC

Cortafuegos: ☒ IPv6/CIDR:

Desconectar: ☐ Puerta de enlace (IPv6):

MTU: Tasa límite (MB/s):

☒ Avanzado

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.

```
conn %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

conn 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
```

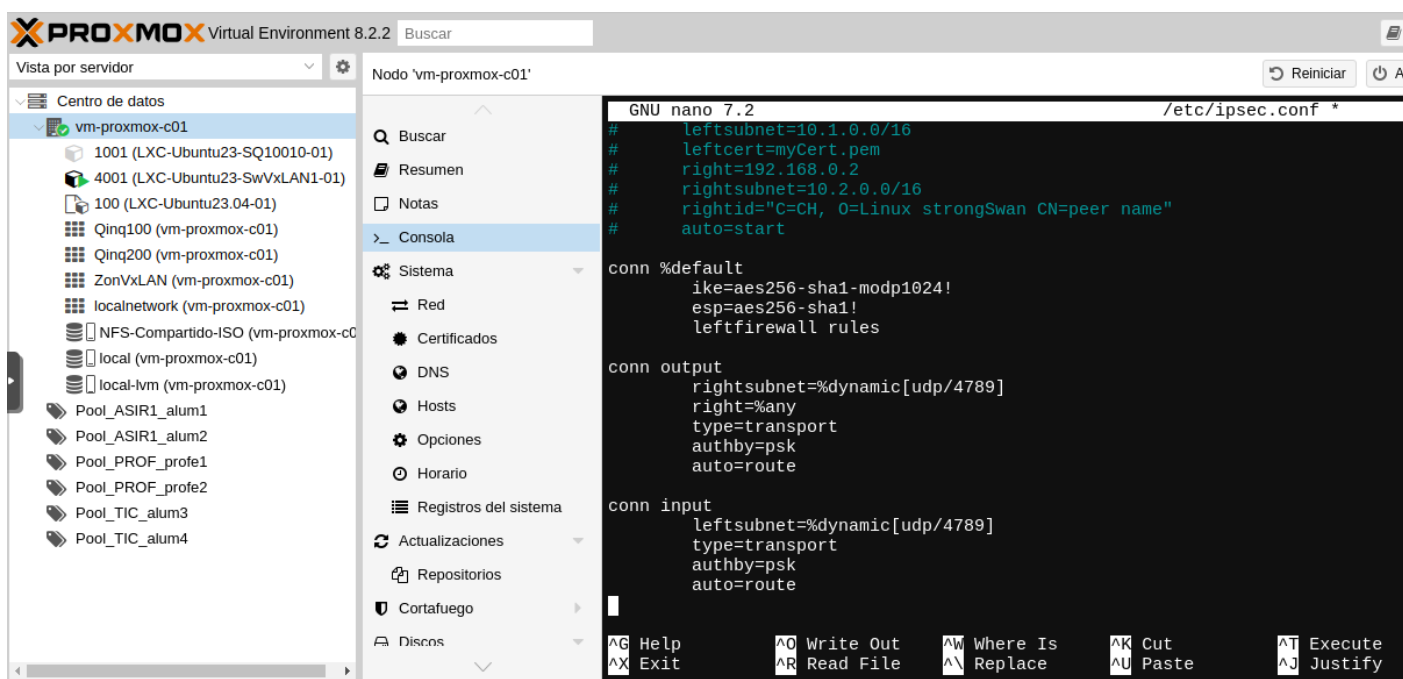


Imagen de elaboración propia: *Modificación del fichero /etc/ipsec.conf* ([CC BY-NC-SA](#))

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>
```

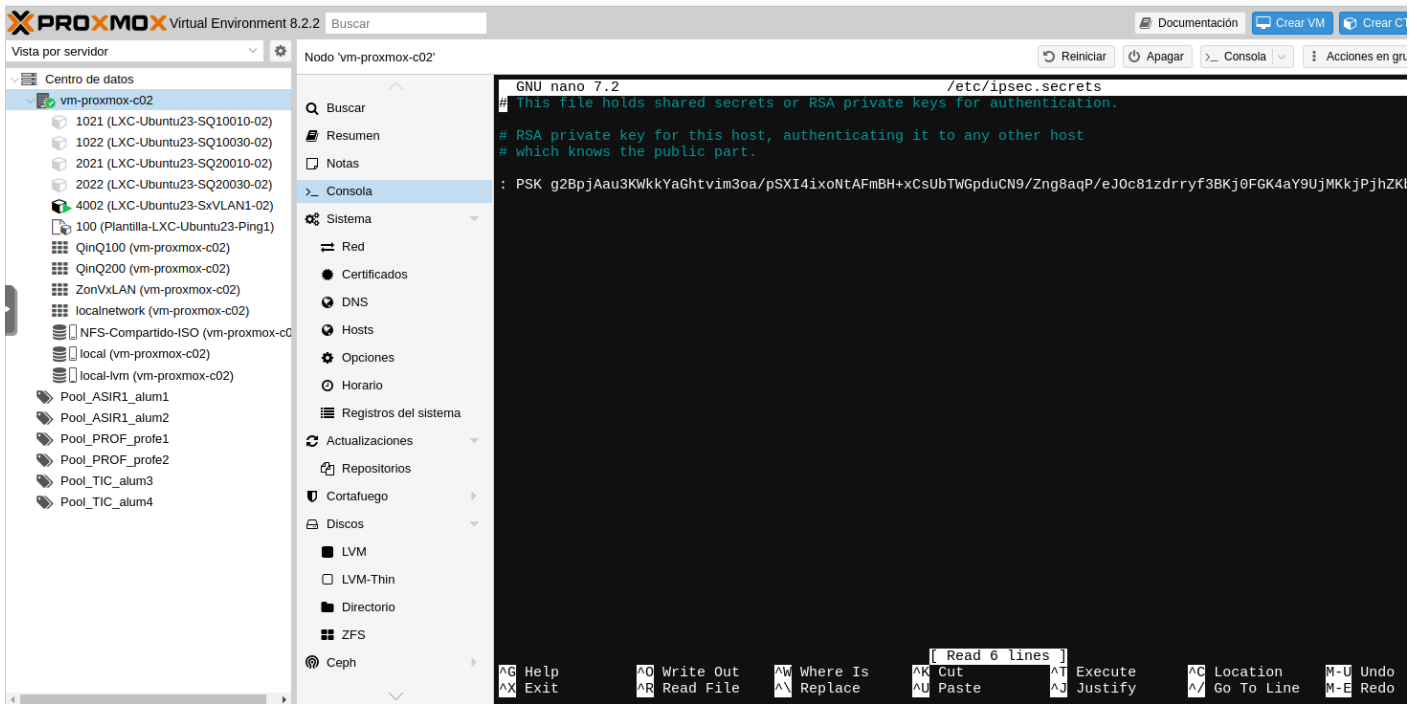



Imagen de elaboración propia: *Modificación del fichero /etc/ipsec.secrets* ([CC BY-NC-SA](#))

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