



Centros de Datos

P4 - Túneles cifrados con OpenVPN

David Ruano Ordás
Departamento de Informática

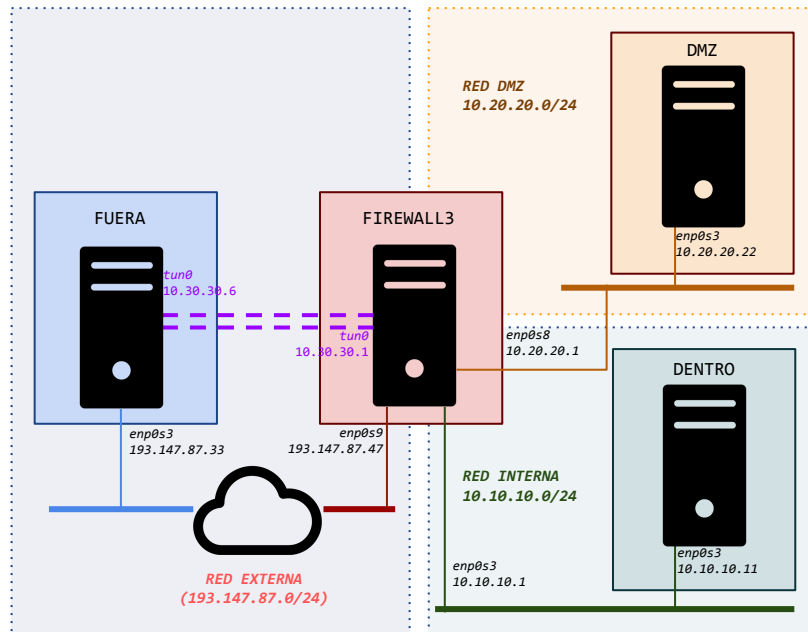
✉ drordas@uvigo.es

📍 Despacho 409

Contenidos

- Entorno de Trabajo
- OpenVPN
 - Pasos previos
 - Creación de un enlace VPN
 - Creación de la autoridad certificadora
 - Creación de certificados en servidor y cliente
 - Configuración y creación del enlace cifrado
 - Preparación del Shorewall
 - Crear una zona para el túnel OpenVPN en el shorewall
 - Dar de alta el túnel OpenVPN

Entorno de prácticas



DeMilitarized Zone

Subred que se utiliza para aislar servicios externos (servidores web, correo, DNS) de la red interna.

Red Interna

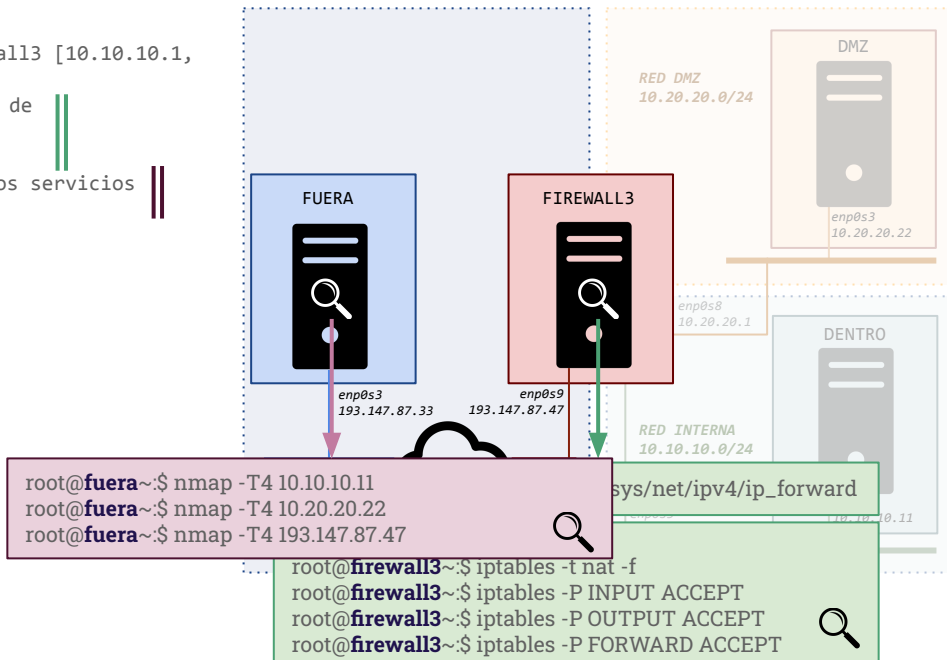
Subred que contiene los recursos y datos sensibles (como servidores, bases de datos, y equipos de los empleados) y está aislada del acceso directo desde Internet

OpenVPN



Uso de Enlaces Cifrados con OpenVPN

1. Pasos previos:
 - a. Establecer tráfico a través de la máquina firewall3 [10.10.10.1, 10.20.20.1, 193.147.87.47]
 - Establecer la configuración por defecto de NETFILTER/iptables (política ACCEPT)
 - Habilitar la redirección de tráfico.
 - b. Escaneo desde la máquina fuera para verificar los servicios accesibles inicialmente [Tarea 1]



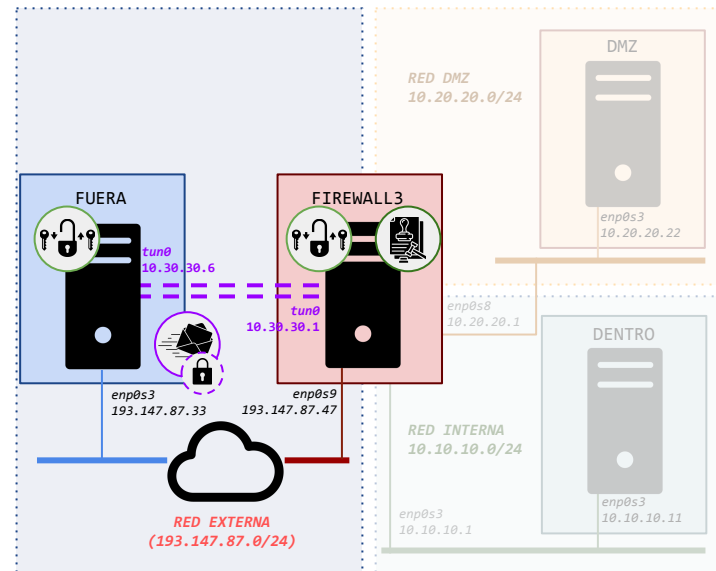
OpenVPN



Entregable: Uso de Enlaces Cifrados con OpenVPN

2. Creación de un enlace VPN

- a. Creación de la CA y de los certificados de servidor y cliente.
 - Crear la autoridad certificadora (CA) en el firewall
 - Crear el certificado del equipo "servidor" OpenVPN.
 - Crear el certificado del equipo "cliente" OpenVPN.
 - Crear los parámetros del algoritmo de intercambio de claves Diffie-Hellman necesarios para la negociación de claves secretas durante el establecimiento de la conexión TLS/SSL
- b. Configuración y creación del enlace OpenVPN.
 - Configuración del servidor: en la máquina firewall3, directorio /etc/openvpn/server.
 - Configuración de los clientes: en la máquina fuera (193.147.87.33), directorio /etc/openvpn/client
 - Crear el túnel OpenVPN
 - Comprobar el túnel creado [Tarea 2]



OpenVPN



Entregable: Uso de Enlaces Cifrados con OpenVPN

3. Integración del enlace OpenVPN con Shorewall:

a. Preparación de Shorewall

- Copiar los ficheros de configuración en /etc/shorewall
- Configurar las zonas
- Configurar los interfaces
- Definir el enmascaramiento (conversión dirección privada↔pública)
- Definir las políticas restrictivas (denegación de paquetes entre zonas)

b. Crear una nueva zona (road) para los clientes conectados con OpenVPN en el fichero /etc/shorewall/zones

c. Asociar el interfaz tun0 a la zona road en el fichero /etc/shorewall/interfaces

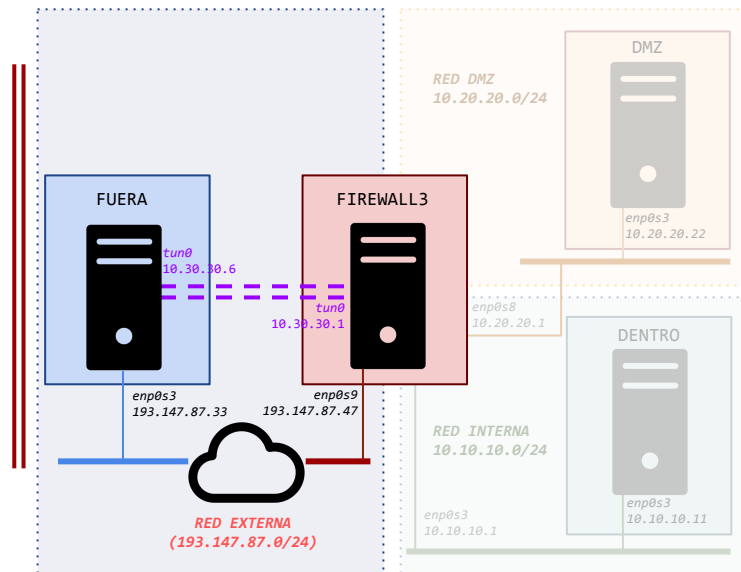
d. Definir las políticas y reglas que afectan a los clientes OpenVPN

e. Dar de alta el túnel OpenVPN /etc/shorewall/tunnels

f. Comprobar la configuración del firewall y el funcionamiento del túnel OpenVPN [Tarea 3]

4. Documentación a entregar:

- Detallar el escaneo de los servicios accesibles desde la máquina de fuera (Tarea 1)
- Detallar las comprobaciones realizadas en la Tarea 2
- Detallar las comprobaciones realizadas en la Tarea 3.





Centros de Datos

P4 - Túneles cifrados con OpenVPN

David Ruano Ordás
Departamento de Informática

✉ drordas@uvigo.es

📍 Despacho 409