



Cristóbal Suárez Abad

2º ASIR

Seguridad y Alta Disponibilidad

Índice

.....	1
1. ¿Qué es OpenVPN Access Server? (La Puerta Blindada).....	2
2. ¿Qué es RADIUS?.....	2
3. ¿Qué aportan TRABAJANDO JUNTOS?	2
Actividad.....	4
Preparación del entorno	4
Fase 1: Configurar el Servidor RADIUS.....	7
Fase 2: Configurar la Pasarela OpenVPN.....	10
Fase 3: La Prueba Final y Evaluación	15

1. ¿Qué es OpenVPN Access Server? (La Puerta Blindada)

Es la **infraestructura de acceso**.

- **Función:** Es la puerta de entrada a nuestra red desde un acceso remoto. Se encarga de construir el túnel seguro desde lugar donde se encuentra el usuario hasta la red.
- **En modo "Solo":** Si solo usas OpenVPN AS, este tendrá un listado con los usuarios que pueden acceder.
 - *El problema:* Si tienes 5 entradas a tu red diferentes (VPN, Wi-Fi, Switch, Router), tienes que tener una copia de la lista de usuario en cada entrada. Si alguien deja de estar permitido o se agrega, tienes que manualmente cambiarlo en varios lugares

2. ¿Qué es RADIUS?

Es el **protocolo de "El que decide"**. RADIUS no es la base de datos en sí, es el **intermediario**.

- **Función:** Es un estándar que permite que diferentes entradas a la red (VPN, Wi-Fi, etc.) le pregunten a una central si alguien puede pasar.
- **Cómo funciona:** RADIUS tiene acceso a la "Base de Datos Maestra" (puede ser un fichero de texto, SQL, o Active Directory). Cuando alguien intenta entrar, RADIUS consulta esa base de datos y solo responde: **ACCESS-ACCEPT** (Déjale pasar) o **ACCESS-REJECT** (Largo de aquí).

3. ¿Qué aportan TRABAJANDO JUNTOS?

Cuando integras OpenVPN AS con RADIUS, consigues la arquitectura profesional con un único servidor de autenticación.

Aquí está el valor real de la unión:

A. Centralización (No te vuelvas loco)

- **Sin RADIUS:** Tienes que crear el usuario "Juan" en la VPN, "Juan" en el Wi-Fi y "Juan" en el servidor de correo. Si Juan cambia su contraseña, tiene que cambiarla en 3 sitios.
- **Con RADIUS:** Creas a "Juan" **una sola vez** en tu servidor central. OpenVPN (la pasarela) no sabe quién es Juan, simplemente le pasa las credenciales a RADIUS. Si RADIUS dice que son buenas, OpenVPN le deja pasar.
 - *Beneficio:* Gestión de usuarios en un solo punto.

B. Seguridad y Despido Rápido

- Si despides a un empleado o un alumno deja el centro, solo lo borras (o deshabilitas) en el servidor central (RADIUS/Base de datos).

- Automáticamente, **OpenVPN deja de permitirle el acceso** porque cuando pregunte a RADIUS, este le dirá "No".
- Si no tuvieras esto, tendrías que acordarte de entrar en la VPN y borrarlo manualmente.

C. Independencia (Escalabilidad)

- Hoy usas OpenVPN. Mañana compras un firewall Fortinet o pones Wi-Fi corporativo.
- Como ya tienes el servidor RADIUS montado, solo tienes que decirle al Wi-Fi: "Pregúntale a ese servidor RADIUS". No tienes que volver a crear los 500 usuarios en el nuevo aparato.

Actividad

Vamos a simular la integración usando **Docker Compose**. Levantaremos dos contenedores:

1. **freeradius**: Hará de Servidor de Autenticación.
2. **openvpn-as**: Hará de Pasarela VPN (usamos la versión Access Server porque trae interfaz web y facilita la integración en tiempo récord).

Aquí tienes la práctica lista para copiar y pegar ("Lab in a Box").

Preparación del entorno

Crea una carpeta llamada **practica-vpn-radius** y dentro creen un fichero llamado **docker-compose.yml**.

```
PS D:\> cd D:\2°_ASIR\Seguridad\'Tema 04'\Actividad 3 - OpenVPN Radius\practica-vpn-radius
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> dir

Directorio: D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius

Mode          LastWriteTime    Length Name
----          -----          ----  --
-a--  12/12/2025   11:45        1126 docker-compose.yml
```

1. El fichero `docker-compose.yml`

Este fichero define una red privada estática (para que sepamos las IPs de antemano) y los dos servidores.

YAML

```
version: "3"

services:
  # --- Servidor RADIUS ---
  freeradius:
    image: freeradius/freeradius-server:latest
    container_name: asir_radius
    restart: unless-stopped
    ports:
      - "1812:1812/udp" # Puerto de autenticación
      - "1813:1813/udp" # Puerto de accounting
    networks:
      vpn_net:
        ipv4_address: 10.5.0.5 # Le damos IP fija para no fallar en la config

  # --- Pasarela VPN (OpenVPN Access Server) ---
  openvpn-as:
    image: openvpn/openvpn-as:latest
    container_name: asir_pasarela
    cap_add:
      - NET_ADMIN # Necesario para crear interfaces de red VPN
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=Europe/Madrid
    ports:
      - "943:943" # Web Admin UI
      - "9443:9443" # Web Client UI (TCP)
      - "1194:1194/udp" # Tunel VPN (UDP)
    volumes:
      - ./config:/config
    restart: unless-stopped
    networks:
      vpn_net:
        ipv4_address: 10.5.0.6

# Definimos una red propia para controlar las IPs
networks:
  vpn_net:
    driver: bridge
    ipam:
```

config:

- subnet: 10.5.0.0/24

Una vez creado, ejecutado levantar los contenedores:

`docker-compose up -d`

```
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker-compose up -d
time="2025-12-12T11:47:14+01:00" level=warning msg="D:\\2º_ASIR\\Seguridad\\Tema 04\\Actividad 3 - OpenVPN Radius\\practica-vpn-radius\\docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 12/12
  ✓freeradius Pulled
    ✓7a7e7a8aa0e1 Pull complete          27.9s
    ✓a3be5d4ce401 Pull complete          10.0s
    ✓8843de228d96 Pull complete          9.9s
    ✓c6beeccf327f Pull complete          0.5s
    ✓83e5c90f3830 Pull complete          1.5s
  ✓openvpn-as Pulled
    ✓8f26b716f854 Pull complete          25.8s
    ✓20043066d3d5 Pull complete          23.0s
    ✓dfd24e1847b4 Pull complete          18.3s
    ✓c31637012b90 Pull complete          0.8s
    ✓ed91d5bfe53b Pull complete          0.8s
  ✓Network practica-vpn-radius_vpn_net Created          71.3s
  ✓Container asir_radius               Started          0.1s
  ✓Container asir_pasarela           Started          1.0s
  ✓Container asir_pasarela           Started          1.1s
```

<input type="checkbox"/>	<input checked="" type="checkbox"/>	● practica-vpn-radius	-	-	0.14%	399.34MB / 14.91	5.24%	77.8KB / 401MB	3.87KB / 410B	42, 6	45				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	● asir_pasarela	8e8d4921d73d	openvpn/oi	0.14%	356.9MB / 7.46Gi	4.68%	0B / 401MB	2KB / 284B	42	45				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	● asir_radius	7f0f9105086b	freeradius/	0%	42.44MB / 7.46Gi	0.56%	77.8KB / 4.1KB	1.87KB / 126B	6	45				

Fase 1: Configurar el Servidor RADIUS

Como estamos en Docker, usaremos `docker exec` para "entrar" en el servidor y configurarlo.

1. Entrar en el contenedor RADIUS:

Bash

```
docker exec -it asir_radius /bin/bash
```

```
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker exec -it asir_radius bash
root@7f0f9105086b:/# |
```

2. Autorizar a la Pasarela (Cliente): Tenemos que decirle a RADIUS que acepte peticiones desde la IP de OpenVPN (**10.5.0.6**). (*Dentro del contenedor, pegamos esto en la terminal*):

Bash

```
# Añadimos el cliente al final del fichero clients.conf
cat >> /etc/raddb/clients.conf <<EOF
```

```
client openvpn-pasarela {
    ipaddr = 10.5.0.6
    secret = secretoASIR
}
EOF
```

```
root@7f0f9105086b:/# cat >> /etc/raddb/clients.conf <<EOF

client openvpn-pasarela {
    ipaddr = 10.5.0.6
    secret = secretoASIR
}
EOF
```

Comprobamos: `cat /etc/raddb/clients.conf`

```
client openvpn-pasarela {
    ipaddr = 10.5.0.6
    secret = secretoASIR
}
root@7f0f9105086b:/# cat /etc/raddb/clients.conf |
```

3. Crear un Usuario de prueba: Creamos el usuario `alumno` con contraseña `password`.

Bash

```
# Añadimos el usuario al fichero users  
cat >> /etc/raddb/users <<EOF
```

```
alumno Cleartext-Password := "password"  
EOF
```

```
root@7f0f9105086b:/# cat >> /etc/raddb/users <<EOF  
  
alumno Cleartext-Password := "password"  
EOF  
root@7f0f9105086b:/# |
```

Comprobamos: cat /etc/raddb/users

```
alumno Cleartext-Password := "password"  
root@7f0f9105086b:/# |
```

4. Recargar configuración y salir: Como FreeRADIUS corre como proceso principal, lo ideal es salir y reiniciar el contenedor desde fuera.

Bash

exit

docker restart asir_radius

```
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker restart asir_radius
asir_radius
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> |
```

5. Comprobación rápida: Podemos probar si RADIUS funciona desde nuestra propia máquina (si tenemos `radtest` instalado) o desde el mismo contenedor:

Bash

```
docker exec -it asir_radius radtest alumno password localhost 0 testing123
# Debe responder: Access-Accept
```

```
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker exec -it asir_radius radtest al
umno password localhost 0 testing123
Sent Access-Request Id 50 from 0.0.0.0:33205 to 127.0.0.1:1812 length 76
    User-Name = "alumno"
    User-Password = "password"
    NAS-IP-Address = 10.5.0.5
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "password"
Received Access-Accept Id 50 from 127.0.0.1:1812 to 127.0.0.1:33205 length 38
    Message-Authenticator = 0xeabb3622cefc51ac14dc0825a33f8844
PS D:\2º_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> |
```



Fase 2: Configurar la Pasarela OpenVPN

Ahora integramos la pasarela vía web.

1. Acceder a la administración:

- Abrir navegador: <https://localhost:943/admin> (Aceptar advertencia de certificado SSL).



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **localhost**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

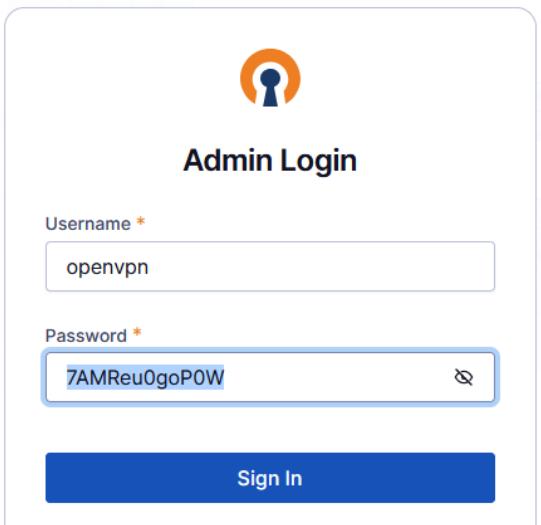
- **Usuario:** openvpn

Contraseña: Mirar los logs para ver la contraseña temporal que genera el contenedor la primera vez, buscar "Auto-generated pass".

Usamos: `docker logs asir_pasarela | find "Auto-generated pass"`

```
+ exec /usr/local/openvpn_as/scripts/openvpnas --nodaemon
Auto-generated pass = "7AMReu0goP0W". Setting in db...
Pass: 7AMReu0goP0W
```

Pass: **7AMReu0goP0W**



The image shows a login interface titled "Admin Login". At the top left is a blue keyhole icon. Below it, the title "Admin Login" is centered. The form consists of two input fields: "Username *" containing "openvpn" and "Password *" containing "7AMReu0goP0W". A blue "Sign In" button is at the bottom. The entire form is enclosed in a rounded rectangular border.

Admin Login

Username *

openvpn

Password *

7AMReu0goP0W

Sign In

2. Configurar RADIUS:

- Ir al menú **Authentication > RADIUS**.
- Click en "**Enable RADIUS Authentication**".

Authentication

General Settings Local LDAP **RADIUS** SAML

RADIUS Authentication

Enable RADIUS authentication

- **PAP/CHAP:** Dejar en PAP o Auto.

RADIUS authentication method

The connection to the RADIUS server is authenticated via one of these methods



PAP



CHAP

- **Hostname:** **10.5.0.5** (La IP fija que pusimos en el docker-compose).
- **Shared Secret:** **secretoASIR** (Lo que pusimos en clients.conf).

Fíjate que los puertos que se especifican sean los mismo que aparecen en el docker compose.

RADIUS server

Specify the RADIUS server connection details

Hostname or IP Address

10.5.0.5

Shared secret

••••••••••

Authentication port

1812

Accounting port

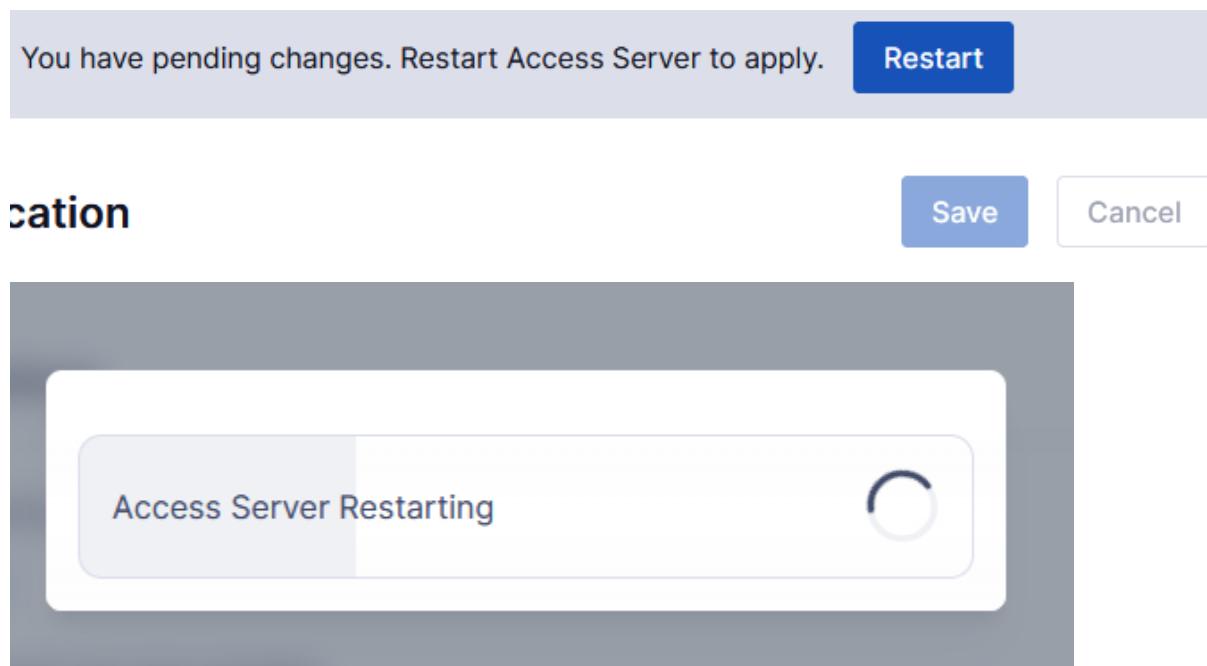
1813

Verify Message Authenticator attribute

?

+ Add another server

- Click en "**Save**" y luego arriba en "**Restart**".



3. Forzar RADIUS para todos

- Ve al menú **Authentication > General Settings**
- Busca la opción que dice **Default Authentication System** (Sistema de autenticación por defecto).
- Cámbialo de **Local** a **RADIUS**.

General Settings

Default authentication system

RADIUS

- Haz clic en **Save**
- Haz clic en **Restart** (el botón que aparece arriba).

You have pending changes. Restart Access Server to apply.

Save Cancel

Fase 3: La Prueba Final y Evaluación

Para evaluar que **realmente** hay integración, haremos la prueba de conexión y miraremos los logs.

1. Prueba de Usuario:

- Ir a <https://localhost:943> (Interfaz de usuario).
- Intentar entrar con Usuario: **alumno** / Contraseña: **password**.

- Si entra y muestra la pantalla de "Download Client", **Superado**.

Get connected

 Download OpenVPN Connect for Windows
 Include connection profile (User-locked)
[Download](#)

Already have your client installed? Download your profile below.

[Download Connection profile](#)

For other platforms