Diagrama de flujo simplificado de Medulla

Reglas de flujo simplificadas

Las reglas se interpretan de la siguiente manera:

- `FUENTE -> DESTINO` significa que el **flujo se inicia** desde la FUENTE hacia el DESTINO.
- Si no se especifica el protocolo, se utiliza TCP por defecto.

Si dispone de un único servidor Medulla, tenga en cuenta la tabla:

- 1. Sin servidor de retransmisión

Si dispone de un servidor Medulla y un servidor de retransmisión, tenga en cuenta la tabla:

- 2. Con servidor de retransmisión clásico

Si dispone de un servidor Medulla y un servidor de retransmisión DMZ, tenga en cuenta la tabla:

- 3. Con servidor de retransmisión DMZ

Acceso de Medulla al exterior:

- updates.siveo.net:443
- download.windowsupdate.com:80

Acceso de Medulla a otros servidores internos:

- Su servidor GLPI (si dispone de uno)
- Su servidor LDAP (si dispone de uno, consulte nuestra documentación sobre LDAP: LDAP DOC)

Acceso desde su máquina de administración a Medulla:

Conexión	Puertos utilizados (DEST)	Observaciones
Tu equipo de administración interno ➡ Servidor Medulla	139/445 8384	Tráfico iniciado por el **puesto de administrador interno hacia Medulla**.

1. Sin servidor de retransmisión

Conexión	Puertos utilizados (DEST)	Observaciones
Puesto interno ➡ Servidor Medulla	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP y UDP) 5222 8443 9990 9999, 22067 55415	Tráfico iniciado desde la **extensión interna hacia Medulla**.
Servidor Medulla ➡ Extensión interna	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Tráfico iniciado por el **servidor Medulla hacia los puestos internos**.

2. Con servidor de retransmisión clásico

Conexión	Puertos utilizados (DEST)	Observaciones

Terminal interno ➡ Servidores Medulla	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP y UDP) 5222 8443 9990 9999, 22067 55415	Tráfico iniciado desde el **extensión interna hacia Medulla**.
Servidores Medulla ➡ Terminal interno	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Tráfico iniciado por el **servidor Medulla hacia los puestos internos**.
---	---	---
Servidor Medulla ➡ Servidor de retransmisión	22 (SSH) 5269 8081 9990 22000	Tráfico iniciado por **Medulla hacia** el **servidor DMZ**.
Servidor de retransmisión ➡ Servidor Medulla	22 (SSH) 5269 7080 8443 9999 22067 22000	Tráfico iniciado por el **servidor DMZ hacia Medulla**.

Terminal interno ➡ Servidor de retransmisión	22 69/69 (UDP) 80/443 111/2049 (TCP y UDP) 5222 9990	Tráfico iniciado por el **teléfono interno hacia** el **servidor de retransmisión**.
Servidor de retransmisión ➡ Extensión interna	9 22 3389 5900	Tráfico iniciado por el **servidor de retransmisiónhacia**la **extensión interna**.

3. Con servidor de retransmisión DMZ

Conexión	Puertos utilizados (DEST)	Observaciones
Terminal interno ➡ Servidor Medulla	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP y UDP) 5222 8443 9990 9999, 22067 55415	Tráfico iniciado desde la **extensión interna hacia Medulla**.
Servidor Medulla ➡ Extensión interna	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Tráfico iniciado por el **servidor Medulla hacia los puestos internos**.
---	---	---
Servidor Medulla ➡ Servidor de retransmisión DMZ	22 (SSH) 4369 4370 a 4380 5269 8081 22000	Tráfico iniciado por **Medulla hacia** el **servidor DMZ**.
Servidor de retransmisión DMZ➡ Servidor Medulla	22 (SSH) 4369 4370 a 4380 5269 7080 8443 9999 22067 22000	Tráfico iniciado por el **servidor DMZ hacia Medulla**.
---	---	---
Terminal externo ➡ Servidor DMZ	22 (SSH) 5222	Tráfico iniciado por el **puesto externo hacia** el **servidor DMZ**.

Descripción de los puertos

Puerto 9: utilizado para Wake on LAN (WOL) con el fin de activar un puesto de forma remota.

Puerto 22 (SSH): puerto SSH utilizado por Medulla para operaciones remotas, ejecución de comandos y administración de agentes.

Puertos 67 y 69 (UDP): utilizados para DHCP y TFTP, especialmente durante el arranque PXE o para la carga de imágenes de implementación.

Puertos 80 y 443: HTTP y HTTPS, utilizados para el acceso web y las comunicaciones seguras con los servicios de Medulla.

Puerto 111 (TCP y UDP): utilizado por Portmapper / RPCbind, necesario para los servicios NFS y algunas llamadas de red internas.

Puerto 3389: utilizado para RDP con el fin de conectarse de forma remota a equipos Windows.

Puerto 4369: utilizado para un clúster ejabberd si dispone de un relé DMZ

Puertos 4370 a 4380: utilizados para un clúster ejabberd si dispone de un relé DMZ

Puerto 5222: utilizado por XMPP para la comunicación entre los agentes Medulla y el servidor.

Puerto 5269: utilizado por XMPP para la comunicación de servidor a servidor, en particular entre Medulla y el servidor de retransmisión en la DMZ.

Puerto 5900: utilizado por VNC para el control remoto.

Puertos 5985 y 5986: utilizados por WinRM (HTTP y HTTPS) para comandos remotos en Windows.

Puertos 7080 y 8081: utilizados por servicios internos o API de gestión necesarios para el servidor de retransmisión o los componentes de Medulla.

Puerto 8443: HTTPS utilizado por la interfaz o las API seguras de Medulla.

Puerto 9990: utilizado por un servicio interno de Medulla para la gestión y la supervisión.

Puerto 9999: utilizado como puerto interno de sincronización o intercambio entre el servidor Medulla y componentes como el relé.

Puerto 22000: utilizado por Syncthing como canal principal para la sincronización de datos (paquetes, artefactos, inventarios).

Puerto 22067: utilizado por Syncthing como canal de retransmisión, útil para equipos móviles o situados detrás de un NAT.

Puertos 35621, 35623 y 55415: puertos dinámicos utilizados por los agentes de Medulla para la comunicación en tiempo real, el inventario, la sincronización o la ejecución de tareas.

Revision #1
Created 2026-04-30 07:39:08 UTC by Adrien Thaissen
Updated 2026-04-30 07:39:08 UTC by Adrien Thaissen