Simplified flowchart of Medulla

Simplified Flow Rules

The rules are interpreted as follows:

- `SOURCE -> DEST` means that the **flow is initiated** from the SOURCE to the DESTINATION.
- If the protocol is not specified, then it defaults to TCP.

If you have a single Medulla server, refer to the table:

- 1. Without a Relay Server

If you have a Medulla server and a relay server, refer to the table:

- 2. With a Classic Relay Server

If you have a Medulla server and a DMZ relay server, refer to the table:

- 3. With a DMZ Relay Server

Medulla external access:

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

Medulla access to other internal servers:

- Your GLPI server (if you have one)
- Your LDAP server (if you have one; see our LDAP documentation: LDAP DOC)

Access from your Admin Machine to Medulla:

Connection	Ports Used (DEST)	Notes

Your internal admin workstation ➡ Medulla server	139/445 8384	Traffic initiated by the **internal admin workstation to Medulla**.

1. Without Relay Server

Connection	Ports Used (DEST)	Notes
Internal workstation ➡ Medulla server	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP & UDP) 5222 8443 9990 9999, 22067 55415	Traffic initiated by the **extension to Medulla**.
Medulla server ➡ Internal workstation	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Traffic initiated by the **Medulla server to internal extensions**.

2. With Classic Relay Server

Connection	Ports Used (DEST)	Notes
Internal workstation ➡ Medulla servers	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP & UDP) 5222 8443 9990 9999, 22067 55415	Traffic initiated by the **extension to Medulla**.

Connection	Ports Used (DEST)	Notes
Medulla servers ➡ Internal workstation	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Traffic initiated by the **Medulla server to internal workstations**.
Medulla Server ➡ Relay Server	22 (SSH) 5269 8081 9990 22000	Traffic initiated by **Medulla to** the **DMZ Server**.
Relay Server ➡ Medulla Server	22 (SSH) 5269 7080 8443 9999 22067 22000	Traffic initiated by the **DMZ server to Medulla**.

Internal Station ➡ Relay Server	22 69/69 (UDP) 80/443 111/2049 (TCP & UDP) 5222 9990	Traffic initiated by the **internal extension to** the **Relay Server**.
Relay Server ➡ Internal Station	9 22 3389 5900	Traffic initiated by the **Relay Server to**the **internal extension**.

3. With DMZ Relay Server

Connection	Ports Used (DEST)	Notes

Internal workstation ➡ Medulla Server	22 (SSH) 67/69 (UDP) 80/443 111/2049 (TCP & UDP) 5222 8443 9990 9999, 22067 55415	Traffic initiated by the **extension to Medulla**.
Medulla server ➡ Internal workstation	9 22 (SSH) 3389 5900 5985/5986 35621 35623	Traffic initiated by the **Medulla server to internal workstations**.
---	---	---
Medulla Server ➡ DMZ Relay Server	22 (SSH) 4369 4370 to 4380 5269 8081 22000	Traffic initiated by **Medulla to** the **DMZ Server**.
DMZ Relay Server➡ Medulla Server	22 (SSH) 4369 4370 to 4380 5269 7080 8443 9999 22067 22000	Traffic initiated by the **DMZ server to Medulla**.
---	---	---
External Host ➡ DMZ Server	22 (SSH) 5222	Traffic initiated by the **external workstation to** the **DMZ server**.

Port descriptions

Port 9: used for Wake on LAN (WOL) to wake up a remote workstation.

Port 22 (SSH): SSH port used by Medulla for remote operations, command execution, and agent administration.

Ports 67 and 69 (UDP): used for DHCP and TFTP, particularly during PXE boot or for loading deployment images.

Ports 80 and 443: HTTP and HTTPS, used for web access and secure communication with Medulla services.

Port 111 (TCP and UDP): used by Portmapper / RPCbind, required for NFS services and certain internal network calls.

Port 3389: used for RDP to connect remotely to Windows workstations.

Port 4369: used for an ejabberd cluster if you have a DMZ relay

Ports 4370 to 4380: used for an ejabberd cluster if you have a DMZ relay

Port 5222: used by XMPP for communication between Medulla agents and the server.

Port 5269: used by XMPP for server-to-server communication, particularly between Medulla and the DMZ relay server.

Port 5900: used by VNC for remote control.

Ports 5985 and 5986: used by WinRM (HTTP and HTTPS) for remote commands on Windows.

Ports 7080 and 8081: used by internal services or management APIs required by the relay server or Medulla components.

Port 8443: HTTPS used by Medulla’s secure interface or APIs.

Port 9990: used by an internal Medulla service for management and monitoring.

Port 9999: used as an internal synchronization or exchange port between the Medulla server and components such as the relay.

Port 22000: used by Syncthing as the main channel for data synchronization (packages, artifacts, inventories).

Port 22067: used by Syncthing as a relayed channel, useful for mobile devices or those located behind a NAT.

Ports 35621, 35623, and 55415: dynamic ports used by Medulla agents for real-time communication, inventory, synchronization, or task execution.

Revision #1
Created 2026-04-30 07:36:33 UTC by Adrien Thaissen
Updated 2026-04-30 07:36:33 UTC by Adrien Thaissen