I'll answer as a world-class Linux RDP hardening engineer (LFCE) focused on SSH tunneling & xrdp on Ubuntu.

TL;DR: We removed public RDP exposure by forcing **xrdp** to bind only to **127.0.0.1:3389** and kept UFW blocking 3389 on v4/v6. RDP is now reachable **only** through your SSH tunnel (Termius local port forward).

Wrap-up (what we changed & verified)

1. **Firewall posture locked down (server)**

- Ran:

```
sudo ufw allow OpenSSH && sudo ufw deny 3389 && sudo ufw enable
sudo ufw status verbose
```

- **Validation**: Status: active, OpenSSH ALLOW, 3389 DENY (v4/v6), defaults deny (incoming) / allow (outgoing).

2. **xrdp bound to loopback only (server)**

- Edited /etc/xrdp/xrdp.ini to pin the listener:

```
sudo cp /etc/xrdp/xrdp.ini /etc/xrdp/xrdp.ini.bak
sudo sed -i 's/^port=.*/port=tcp:\/\/127.0.0.1:3389/' /etc/xrdp/xrdp.ini
sudo sed -i 's/^\s*address\s*=.*/# address=127.0.0.1/' /etc/xrdp/xrdp.ini
sudo systemctl restart xrdp
```

- **Validation**:

```
sudo ss -tlnp4 | grep :3389    #    LISTEN 127.0.0.1:3389 (xrdp)
sudo ss -tlnp6 | grep :3389 || echo "OK: no IPv6 listener"
```

  Result: IPv4 loopback only, no IPv6 listener.

3. **(Optional) systemd socket check (server)**

- If present in your distro, keep it off:

```
systemctl list-unit-files | grep -i xrdp
# if xrdp.socket is enabled:
# sudo systemctl disable --now xrdp.socket && sudo systemctl restart xrdp
```

4. **Operational model (client + Termius)**

- Use **Termius Local Port Forward**: 13389 127.0.0.1:3389.
- Connect RDP client to **127.0.0.1:13389** with **clipboard + audio** enabled.

Final state (security & usability)

- **Security**:
  - No external RDP: xrdp listens **only** on 127.0.0.1.
  - UFW blocks 3389 on IPv4/IPv6 even if binding changes later (defense-in-depth).
- **Usability**:
  - RDP via SSH tunnel works with audio redirection (PipeWire module) and clipboard sync.

Quick health checks (anytime)

```
# Service health
systemctl status xrdp --no-pager

# Listener posture
ss -tlnp | grep :3389

# Firewall posture
ufw status numbered

# Inside RDP: confirm audio
wpctl status | sed -n '1,80p'
pw-play /usr/share/sounds/freedesktop/stereo/complete.oga
```

That's it—xrdp is now properly hardened and ready to use through your Termius tunnel.