CICADA | RESOURCES

NETWORK | 60 MIN | WORKING KNOWLEDGE | UPDATED NOVEMBER 2026

Remote access without the front door open

Close exposed remote desktop, require MFA, and give people only the access they need.

The short version

- ✓ Never expose RDP directly to the internet.
- ✓ Use a VPN or zero-trust service with MFA.
- ✓ Restrict who can connect and from where.
- ✓ Turn off access that isn't being used.

Find what's exposed

Ask your IT provider for an inventory of anything reachable from the internet: remote desktop, VPN, web admin panels, file shares, cameras, printers. If you don't have a provider, use a reputable external scan service, with permission, or ask your ISP.

Look especially for RDP (port 3389), VNC, SSH and any login page that doesn't require MFA.

Replace direct exposure

- Turn off port forwarding for RDP and web admin panels.
- Use a VPN or zero-trust access product, with MFA and device checks.
- If you must use RDP, put it behind a gateway with MFA and restrict source addresses.

- Use the provider's own secure access rather than exposing a management console.
- Patch the remote-access software itself; it is a target.

Control who and when

Give access to named people, not a shared account. Review the list quarterly. Disable access for leavers and contractors the same day. Where possible, require re-approval for each session or limit hours.

> **CHECK THE LOGS**
>
> Look for repeated failed logins, logins from unexpected countries and sessions at odd hours. If nobody reviews the logs, the control is decorative.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] External exposure inventory completed
- [ ] RDP not reachable from the internet
- [ ] VPN / zero-trust access with MFA
- [ ] Access limited to named users
- [ ] Remote-access software patched
- [ ] Logs reviewed monthly

0 of 6 done