

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to segment smart TVs and cameras on a separate VLAN

<https://cyberguardlab.com/blog/smart-tv-camera-vlan-segment>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



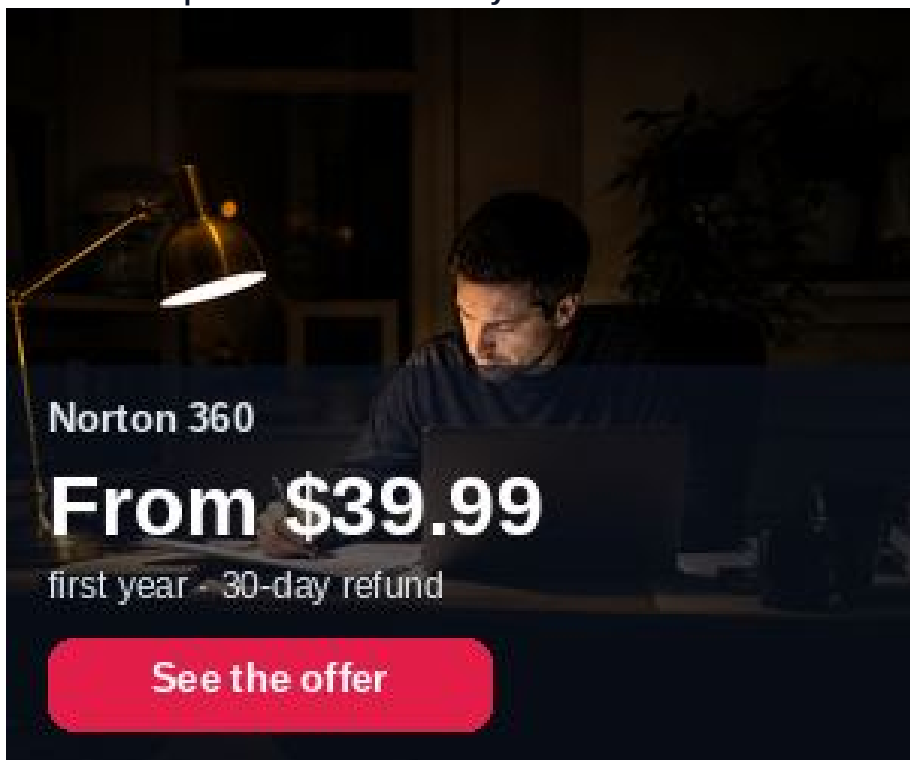
Put smart TVs and cameras on a separate VLAN or isolated IoT/guest SSID so a compromised gadget cannot freely scan laptops and NAS on your main LAN. You need a router or firewall that supports VLANs/guest isolation (or a mesh vendor's "IoT network" feature). This how-to is LAN segmentation-not Android Private DNS, not WPA3 alone, and not ISP phishing.

1. What you need

- * Router/firewall/AP firmware with VLAN, "guest network," or "IoT network" controls (prosumer and many mesh systems).
- * Ability to set a second SSID or wired VLAN membership for TVs/cameras.
- * Optional: firewall rules blocking IoT -> LAN while allowing IoT -> internet (and limited LAN -> IoT if you use a viewing app). Exact menus differ by vendor-use the vendor manual for click-by-click paths; the pattern below is portable.

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

[See the offer](#)

[See the Norton first-year offer](#)

Offer page: <https://cyberguardlab.com/norton>

Convenience casting is why many homes skip isolation. If a cheap camera is wormed, flat LANs hand attackers a path to file shares-segment first, then open only the ports you prove you need.

2. VLAN vs Private DNS vs WPA3

Control | Primary job | Not a substitute for

IoT VLAN / guest SSID | Isolate device groups on LAN | DNS-over-TLS on phones

Private DNS | Encrypt DNS on one Android device | Stopping camera?laptop LAN worms

WPA3 | Strong Wi-Fi handshake | Separating trusted vs untrusted devices once joined

3. Steps: segment TVs and cameras

- * Update the router/AP firmware from the official vendor source.
- * Create a new IoT / Guest network or VLAN ID (example pattern: VLAN 20 named `iot`).
- * Assign a dedicated SSID (e.g., `Home-IoT`) to that VLAN; use strong WPA2/WPA3 settings appropriate for those clients.
- * Enable client/AP isolation on that SSID if you do not need camera-to-camera chatter.
- * Firewall defaults to prefer: IoT may reach the internet; IoT may not initiate connections to your main LAN; your phone on main LAN may reach cameras only on required ports if the app needs it-or use the vendor cloud (understand the privacy tradeoff).
- * Move smart TVs and cameras onto `Home-IoT` (forget the old SSID on each device).
- * Keep PCs, phones, and NAS on the main LAN/SSID.
- * Test: phone on main LAN still streams the camera app if that is required; a TV on IoT should not see your NAS shares.
- * Document the VLAN ID and SSID in your household notes.
- * Recheck IoT update support so segmented devices still get patches.

4. If your ISP gateway cannot VLAN

- * Add your own router behind the ISP modem in true router mode (avoid double-NAT surprises-follow vendor guidance).
- * Or use the gateway's Guest Wi-Fi as a lighter isolation layer when full VLANs are unavailable.
- * Still change router admin credentials and keep endpoints patched with Norton or Bitdefender (TotalAV, McAfee, Avast on-site).

FAQ

Will casting from phone to TV break?

Sometimes. You may need mDNS/reflection rules or keep the phone on a network that can reach the TV. Prefer vendor-documented cast ports over "allow all."

Is guest Wi-Fi good enough?

Guest isolation is a practical middle ground when VLANs are unavailable. True VLANs give cleaner wired + wireless policy.

Does this stop ISP bill phishing?

No. Phishing is an account problem-see the ISP phishing guide.

Do cameras still need passwords?

Yes. Segmentation limits blast radius; unique camera passwords and updates remain mandatory.

If you still want a paid suite

Avoiding how to segment smart TVs and cameras on a separate VLAN does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * CISA: Secure your home network
- * FTC: Internet of Things security basics
- * CISA: Internet of Things security tips
- * Example vendor VLAN help (TP-Link Omada concept docs)

Also read

- * How to turn on Private DNS on Android
- * How to check if an IoT device still gets security updates
- * How to set up a guest Wi-Fi network at home
- * How to turn on WPA3 or the strongest Wi-Fi encryption you have
- * How to change your router admin password safely