How to put security cameras on their own network (VLAN)

Cameras are small computers that rarely get patched. Putting them on their own network segment means a compromised camera cannot reach your office PCs, and a busy office cannot choke your video. Here is the practical way to do it.

Networking · Published 2026-10-25 · Online version: vuepointsecure.com/support/how-to-put-cameras-on-their-own-network-vlan

On a flat network, every camera can talk to every laptop, printer and server in the building, and the other way round. Segmenting cameras into their own network limits the damage if one is compromised, keeps video traffic away from office traffic, and makes firewall rules simple: cameras talk to the recorder, and almost nothing else.

Option 1: let the NVR do it

If your NVR has built-in PoE ports, cameras plugged into them are usually already on a separate internal network that the NVR manages. Only the NVR's LAN port connects to your main network. For small systems this is the simplest isolation available and needs no extra equipment. Some NVRs and many VMS servers also have two network ports, one for cameras and one for the office network, which achieves the same thing for larger systems.

Option 2: a camera VLAN

When cameras connect to separate PoE switches around the site, use a VLAN: a logically separate network running over the same switches and cables. You need **managed (or smart-managed) switches** and a **router or firewall that supports VLANs** and can route and filter between them.

Set up a camera VLAN

1. **Plan the numbers**
   Pick a VLAN ID (for example 30) and a subnet that does not overlap anything else (for example 192.168.30.0/24). Write down which switch ports go to cameras, which go to the recorder, and which are uplinks.

2. **Create the VLAN on the router or firewall**
   Add a VLAN interface with ID 30, give it an address in the new subnet (192.168.30.1), and enable a DHCP server on it, or plan static IPs for the cameras.

3. **Create the VLAN on each switch**
   Add VLAN 30. Set camera ports as **access/untagged** members of VLAN 30 (and set their port VLAN ID, often called PVID, to 30). Set uplinks between switches and to the router as **trunk/tagged** members carrying VLAN 30 and your main VLAN.

4. **Place the recorder**
   Simplest: put the NVR on the camera VLAN too and allow your office network to reach only the NVR. Alternatively, use an NVR or server with one port on each network.

5. **Write the firewall rules**
   See the rule table below. Default deny between VLANs, then allow only what is needed.

6 **Move cameras and test**

Move one camera first. Confirm it gets an address in the new subnet, records on the NVR, and has correct time. Then move the rest. Update any DHCP reservations and NVR channel settings to the new addresses.

From	To	Allow?	Why
Office / admin network	NVR (web and client ports)	Yes	Viewing and administration
Office / admin network	Individual cameras	Admins only, or no	Configure cameras through the NVR where possible
Camera VLAN	Office network	No	The main point of segmentation
Cameras	Internet	No, except time (NTP) if needed	Cameras rarely need the internet; firmware can be loaded manually
NVR	Internet	Only if you use the vendor's app or a monitoring service	P2P/cloud and monitoring connections are outbound from the NVR or edge device

A sensible starting rule set. Adjust to your system.

What usually breaks

Discovery tools (SADP, ConfigTool, Reolink Client LAN scan) and ONVIF discovery use broadcast or multicast, which does not cross VLANs. Run them from a machine on the camera VLAN, or add cameras to the NVR by IP. **Cloud apps** stop working if you block the NVR's internet access. **Time drift** appears if cameras cannot reach any NTP server; point them at the router or NVR.

Why this matters in practice

- **Containment.** Camera and DVR firmware has a long history of serious vulnerabilities. Segmentation means a compromised camera cannot be used to reach PCs or file servers.
- **Performance.** Dozens of video streams on the same segment as office traffic can congest older or unmanaged switches. A VLAN keeps the traffic separate.
- **Cleaner monitoring.** A monitoring service or edge device only needs access to the camera segment, not to the whole building network.

Frequently asked questions

Can I do this with unmanaged switches?

Not as a VLAN. You can still isolate cameras physically: a separate set of switches cabled only to the NVR's camera port or PoE ports, with no connection to the office network.

Will a VLAN stop me viewing cameras on my phone?

Not if the NVR keeps outbound internet access for the vendor's app. Cameras themselves can stay blocked from the internet.

Related guides

- How to secure a camera system — vuepointsecure.com/support/how-to-secure-a-camera-system-passwords-firmware-and-exposure
- PoE switch and cabling basics for IP cameras — vuepointsecure.com/support/poe-switch-and-cabling-basics-for-ip-cameras
- How to give a camera or NVR a static IP address — vuepointsecure.com/support/how-to-give-a-camera-or-nvr-a-static-ip-address
- All support articles — vuepointsecure.com/support

Need help with a site? Call (888) 203-2260 or visit vuepointsecure.com/contact. Menu names and defaults vary by model and firmware; check your device's documentation.