appliedtechnicalservices.net · (541) 550-8299

INSIGHTS · WHITE PAPER · NETWORK SECURITY

Network Segmentation for Smart Homes and AV Systems

Why one flat network is a risk, what current guidance recommends, and how to segment without breaking AV and control.

By Russ Rowe · November 18, 2026 · 9 min read

Key takeaways

- The average connected home now has about 22 internet-connected devices and faces roughly 29 attack attempts per day. Streaming devices, smart TVs and IP cameras are the most targeted.[1]
- On a flat network, one compromised device can reach everything else. Segmentation contains the damage.
- The NSA's baseline for home networks is at least three separate segments: primary, guest and IoT.[2] AV and control systems benefit from going further.
- Segmentation must be designed around how AV actually works: multicast, device discovery and control traffic all need planned exceptions, or the system will break.
- Segmentation works best combined with secure remote access, no default passwords, current firmware and documentation.

Executive summary

Homes, yachts and businesses now run on networks crowded with connected devices: TVs, streaming players, cameras, thermostats, door stations, touch panels, control processors, conferencing systems and dozens more. Many of these devices are built to a price, rarely updated and impossible to inspect. Yet in most installations they share a single flat network with the computers, phones and storage that hold an owner's most sensitive information.

Network segmentation, dividing one network into separate zones with controlled communication between them, is one of the most effective protections available. U.S. government guidance from the NSA, CISA and the FBI all point in this direction. For AV and control systems, segmentation has a second benefit: when designed correctly, it also makes systems more reliable.

This paper explains the risk, summarizes current guidance, and lays out a practical segmentation model for residential, commercial and marine AV and control systems, including the design details that keep entertainment, conferencing and control working properly once the network is divided.

The problem: many devices, one network

The scale of the problem has grown quickly. A 2025 study by Bitdefender and NETGEAR, based on data from 6.1 million households, found the average connected home now contains about 22 IoT devices and faces nearly 29 attack attempts every day, up from about 10 per day in 2024.[1] Between January and October 2025 the researchers recorded 13.6 billion IoT attacks.[1]

The most targeted devices are exactly the ones AV integrators install. Streaming devices accounted for 25.9% of attacks, smart TVs for 21.3% and IP cameras for 8.6%.[1]

Some devices arrive compromised. In June 2025 the FBI warned that criminals were exploiting a botnet called BADBOX 2.0, made up of millions of infected devices including TV streaming boxes, digital projectors, digital picture frames and aftermarket vehicle infotainment systems.[3] Some were infected before purchase; others became infected after owners installed apps from unofficial marketplaces. Infected devices turn the owner's home connection into a proxy that criminals sell or use for other activity.[3]

On a flat network, any one of these devices can see and talk to everything else: the owner's laptop, the family's phones, the network storage, the camera recorder and the control processor. Attackers call this *lateral movement*, and it is what turns a cheap compromised gadget into a serious breach.

What network segmentation is

CISA describes segmentation as a physical or virtual architectural approach that divides a network into multiple segments, each acting as its own subnetwork, which limits access to devices, data and applications and restricts communications between networks.[4]

In practice, segmentation usually means:

- **VLANs** (virtual LANs) that separate traffic on the same switches and access points;
- **Separate wireless networks (SSIDs)** mapped to those VLANs;
- **Firewall rules** between segments that allow only the traffic each system genuinely needs.

The third point matters most. A VLAN alone separates traffic, but if the router simply passes everything between VLANs, little has been gained. The protection comes from rules that say, for example, "the guest network can reach the internet and nothing else" or "cameras can talk to the recorder but not to the family's computers."

What current guidance says

NSA: segment the home network

The NSA's *Best Practices for Securing Your Home Network* recommends segmenting the network and states that, at a minimum, a wireless network should be split between primary Wi-Fi, guest Wi-Fi and an IoT network.[2] The same guidance recommends WPA3 or WPA2 encryption on wireless networks and limiting router administration to the internal network.[2]

CISA: limit lateral communication

CISA's guidance on securing network infrastructure recommends limiting unnecessary lateral communications and logically segregating networks so administrators can isolate critical devices onto their own segments.[5] In 2025, CISA went further and published microsegmentation guidance as part of its Zero Trust work, describing segmentation as foundational and applying it explicitly to IoT and operational technology environments.[6]

FBI: watch the devices you connect

In its BADBOX 2.0 warning, the FBI urged consumers to assess IoT devices on their networks for suspicious activity, avoid apps from unofficial marketplaces, and keep operating systems, software and firmware up to date.[3]

Crestron: isolate the control network

Manufacturers agree. Crestron's *IP Guidelines for the IT Professional* includes sections on isolating the network and on VLAN configuration for control systems.[7] Crestron has also noted that VLANs improve performance as well as security, because the control system is no longer competing with other network traffic.[8]

A practical segmentation model for AV and control

The NSA's three-network baseline is a good start for any home. Professionally integrated residences, yachts and commercial spaces benefit from separating further, because their devices have very different trust levels and traffic needs. The model below is a typical starting point; every project is adjusted to the owner's devices and how they live or work.

Segment	What lives there	Typical rule
Trusted	Owners' and staff's computers, phones, tablets, file storage	Can reach control interfaces and approved services; nothing on other segments can reach in unprompted
Control	Control processors, touch panels, keypads, lighting and shade gateways	Can reach the devices it controls; reachable only from trusted devices and approved apps
AV & media	Displays, AV receivers, streaming players, AV-over-IP encoders and decoders, audio DSPs	Internet access for updates and streaming; accepts commands from the control segment
Cameras & security	IP cameras, recorders, door stations, access control	Cameras talk to the recorder only; viewing through the recorder or a secure app
IoT	Smart appliances, voice assistants, thermostats, irrigation, pool and spa controllers	Internet access only; cannot initiate connections to other segments
Guest	Visitors, contractors, crew personal devices (on yachts)	Internet only, with client isolation so guests cannot see one another
Management	Switch, access point and firewall management interfaces	Reachable only by the integrator or IT administrator, never by users or guests

Smaller projects can combine segments. A modest home might merge AV and IoT, for example. The principle stays the same: devices that are hard to secure should not share a network with the information worth protecting.

Designing segmentation that doesn't break AV

Segmentation done carelessly is a common cause of "the system stopped working" calls. AV and control systems depend on traffic patterns that generic IT templates don't anticipate. Four areas need deliberate

design.

1. Control traffic between segments

A control processor must reach every device it controls: displays, receivers, matrix switchers, lighting, shades and thermostats. If those devices sit on other segments, the firewall needs specific rules allowing the control segment to reach them on the required ports, and ideally nothing more. Crestron and other manufacturers publish port lists for their equipment, which makes these rules precise rather than "allow all."[7]

2. Multicast and AV-over-IP

AV-over-IP video and networked audio (Dante, AES67, Q-SYS and others) often rely on multicast. Without proper switch configuration, multicast floods every port and can overwhelm a network. Switch manufacturers recommend placing these systems on a dedicated VLAN with IGMP snooping enabled, and applying QoS so time-sensitive audio and video are prioritized during congestion.[9] Segmentation and AV performance work together here: a dedicated AV VLAN is both more secure and more reliable.

3. Device discovery

Many consumer features, including screen mirroring, casting, wireless speakers and some apps, find devices using discovery protocols such as mDNS that normally stay within a single network. Once phones and displays are on different segments, these features can stop working unless the network is configured to relay discovery between specific segments. This should be planned and tested deliberately, not fixed later by opening everything up.

4. Wireless design

Each segment that needs wireless access gets its own network name mapped to its VLAN, with modern encryption (WPA3 where devices support it, WPA2 otherwise).[2] The fewer SSIDs the better for performance, so many devices that never move, such as displays, processors and recorders, should be wired whenever possible.

Remote access without open doors

Owners want to control their homes, yachts and rooms from anywhere, and integrators need to support systems remotely. The worst way to provide that is port forwarding: opening ports on the internet router directly to cameras, recorders or control processors. Those devices then face the internet's constant automated scanning.

Better approaches include:

- **VPN access** into a specific segment for administrators and integrators;
- **Manufacturer cloud services** designed for secure remote access, where they are well maintained;
- **Multi-factor authentication** on administrative and remote accounts wherever the platform supports it;

- **Administration limited to the internal network**, consistent with NSA guidance for routers.[2]

Beyond segmentation: the basics still matter

Segmentation contains problems; it doesn't prevent them on its own. A well-designed system also includes:

- **No default credentials.** Every device, from processors and cameras to switches and access points, gets a unique strong password, recorded securely.
- **Firmware management.** Updates applied on a schedule, and the FBI's advice to keep firmware current is followed.[3]
- **Careful device selection.** Off-brand streaming boxes and devices that require unofficial app stores are the kind of products the FBI flagged in its BADBOX 2.0 warning.[3]
- **Lifecycle planning.** Equipment replaced before manufacturers stop issuing security updates.
- **Documentation.** Network diagrams, VLAN and IP plans, firewall rules and credentials handed to the owner, so the system can be supported by anyone they choose.

A note on the U.S. Cyber Trust Mark

The FCC adopted a voluntary cybersecurity labeling program for consumer IoT devices, the U.S. Cyber Trust Mark, in March 2024.[10] The program was paused in June 2025 over concerns about its original lead administrator, and in April 2026 the FCC selected the ioXt Alliance as the new lead administrator.[11] On October 27, 2026, the FCC issued a public notice seeking comment on labeling and certification requirements.[12] Once labeled products reach stores, the mark will be a helpful signal when choosing devices. It won't replace good network design, since millions of unlabeled devices are already installed.

Recommendations

1. **Inventory every connected device.** You can't segment what you don't know is there.
2. **Separate guests and IoT at a minimum**, following the NSA's baseline of primary, guest and IoT networks.[2]
3. **Give control systems, AV and cameras their own segments** in professionally integrated homes, yachts and commercial spaces.
4. **Write firewall rules from what each system needs**, using manufacturer port lists, rather than allowing all traffic between segments.
5. **Design for AV traffic**: IGMP snooping and QoS for AV-over-IP, planned discovery relays, and wired connections for fixed equipment.[9]
6. **Eliminate port forwarding** in favor of VPNs or well-maintained secure cloud access, with multi-factor authentication.
7. **Change every default password and keep firmware current.**[3]

8. **Document everything** and give the owner a copy.

About Applied Technical Services

Applied Technical Services designs, engineers, programs and supports AV, control and network systems for residential, commercial, superyacht and private aviation clients. Founder Russ Rowe brings 30 years of AV/IT experience and has been a Crestron Certified Programmer since 2006, and the firm is a Crestron Services Provider. We design networks with segmentation and security built in from day one, and we help dealers and owners secure systems that are already installed.

Sources

1. Bitdefender & NETGEAR, *The 2025 IoT Security Landscape Report* (October 2025), with coverage via CE Pro, IT Brief and Insurance Business. cepro.com · itbrief.com.au · insurancebusinessmag.com
2. National Security Agency, *Best Practices for Securing Your Home Network*, Cybersecurity Information Sheet (February 2023). media.defense.gov
3. Federal Bureau of Investigation, Public Service Announcement I-060525-PSA on BADBOX 2.0 (June 5, 2025). ic3.gov
4. CISA, *Layering Network Security Through Segmentation* (infographic). cisa.gov
5. CISA, *Securing Network Infrastructure Devices*. cisa.gov
6. CISA, *Microsegmentation in Zero Trust, Part One* (2025). cisa.gov
7. Crestron, *IP Guidelines for the IT Professional*, Doc. 4579. docs.crestron.com
8. AV Network, "Networked AV: Security, Performance, or Both?" avnetwork.com
9. TP-Link Omada, *Suggested Configurations for AVoIP Protocols on Omada Switches* (Dante, AES67, Q-SYS). tp-link.com
10. Broadband Breakfast, "FCC Approves Cyber Trust Mark Program" (March 14, 2024). broadbandbreakfast.com
11. Broadband Breakfast, "FCC Seeking More Cyber Trust Mark Administrators" (January 2026) and "FCC Picks ioXt Alliance to Head Cyber Trust Mark Program" (April 13, 2026). broadbandbreakfast.com · broadbandbreakfast.com
12. Cooley, "FCC Advances US Cyber Trust Mark Program, Labeling and Certification Requirements" (November 10, 2026). cooley.com