Atrium: Hotel Network & Firewall Requirements

One-page allowlist for the hotel's IT department: what the Atrium in-room TV system needs from the network, and what it does **not** need.

> **TL;DR** The TVs only need *outbound* HTTPS (TCP 443) to a short list of domains. No inbound ports, no port-forwarding, no static IPs, no VPN. Weather, flights, traffic and currency data are delivered by *our cloud platform*, so you do not open anything for those feeds.

1. Internet allowlist: outbound from the TV VLAN (TCP 443 unless noted)

Destination	Purpose	Required?
ota.mndev.co.za	Device management, OTA app updates, telemetry	**Always**
hoteltv.mndigitalservices.co.za	Config, content, guest screens, live commands (HTTPS + WebSocket)	**Always**
atrium.mndigitalservices.co.za	Reserved for the upcoming platform domain; allow now so the migration needs no firewall revisit	**Always**
dominate.musicnowsa.co.za	Background / ambient content (WebSocket)	**Always**
play.google.com, android.clients.google.com, *.googleapis.com, *.gstatic.com, dl.google.com, *.googleusercontent.com	Google Play + Google services (streaming apps install and auto-update from Play)	**Always**
Streaming service CDNs (per-service domains in **§1a** below)	The streaming apps fetch their own content directly (dominant bandwidth load)	**Always**
pics.avs.io	Airline logo images on the flight-board screen	**Optional: flight board feature only**
s3.eu-central-2.wasabisys.com	Training video media	**Optional: staff-profile training feature only**
*.teams.microsoft.com, *.office.com	Microsoft Teams meetings	**Optional: staff-profile Teams feature only**
tv.mndigitalservices.co.za	Samsung Hospitality panels: Atrium app install & updates (URL Launcher)	**Optional: Samsung panel deployments only**

Plus the basics every Android device needs: outbound **DNS (UDP/TCP 53)** and **NTP (UDP 123)**, usually already open.

> **All three Atrium domains are required** `ota.mndev.co.za`, `hoteltv.mndigitalservices.co.za` and `atrium.mndigitalservices.co.za` point at (or will point at) the same platform; the TV software uses more than one hostname internally, so allow all three.

> **TLS interception / SSL inspection** If the network inspects TLS, exempt the TV VLAN: certificate-pinned traffic (Google Play, streaming apps) will fail behind it.

1a. Streaming service domains (TCP 443)

Service	Domains
Netflix	*.netflix.com, *.nflxvideo.net, *.nflximg.net, *.nflxso.net, *.nflxext.com
YouTube	*.youtube.com, *.googlevideo.com, *.ytimg.com, *.ggpht.com (plus the Google domains above)
DStv Stream	*.dstv.com, *.connectedvideo.tv, *.multichoice.com
Disney+	*.disneyplus.com, *.disney-plus.net, *.dssott.com, *.bamgrid.com, *.disneystreaming.com

Service	Domains
Prime Video	*.primevideo.com, *.amazonvideo.com, *.aiv-cdn.net, *.media-amazon.com, *.amazon.com
Spotify	*.spotify.com, *.scdn.co, *.spotifycdn.com
Apple TV+	*.apple.com, *.itunes.apple.com, *.mzstatic.com, *.aaplimg.com
Crunchyroll	*.crunchyroll.com, *.crunchyrollsvc.com, *.vrv.co
Tidal	*.tidal.com, *.tidalhifi.com

Vendor domains: filter by hostname, not IP These are the streaming vendors' own domains and can change without notice. Most services front their media through shared CDNs (Akamai, CloudFront, Fastly) under the hostnames above, so *hostname/SNI filtering* is required, because IP-based rules will not hold. If a service misbehaves behind a strict allowlist, consult that vendor's current published list; only allow the services your hotel actually offers.

2. You do NOT need to open these

All guest-information data feeds (**weather, traffic / airport drive time, live flight arrivals & departures, and currency exchange rates**) are delivered by our cloud platform. The TVs never contact any third-party data provider directly, so no firewall rules are needed for these feeds.

3. Inbound / remote access

None. All management (remote commands, screenshots, log capture, OTA updates) rides on connections the TV itself opens outbound to our servers. No inbound NAT rules, no exposed ports, no remote-desktop software.

4. LAN / VLAN requirements (only for the features you use)

Feature	Requirement
Guest casting (CastBridge appliance)	Runs through the on-site CastBridge appliance and needs **no router or firewall rules**. What matters instead is wireless controller behaviour: full detail in section 5.
IPTV / live TV from a local head-end	`udp://` / `rtp://` channels are multicast: enable **IGMP snooping** / **multicast** on the TV VLAN between the head-end and the TVs. Stays on the LAN; no internet rules.
Local APK mirror (optional, larger sites)	A LAN box that caches app downloads. TVs reach it over plain HTTP on the LAN and fall back to the cloud automatically if it's absent.
Provisioning (installation day only)	The installer's phone connects directly to each TV via **ADB, TCP 5555**, so the phone and the TVs must be on the same LAN segment **with client isolation off between them** (see the note below). The phone also needs outbound HTTPS (443) to hoteltv.mndigitalservices.co.za plus Google Play. Not needed after installation.

Installation day: the installer's phone must be able to reach every TV Guest Wi-Fi networks almost always have *client isolation* switched on (also called AP isolation, peer blocking or station isolation). It stops devices on the same network from talking to each other, so the TVs still reach the internet but the installer's phone cannot reach them, and the installation cannot start. **Do not install over guest Wi-Fi.** Either connect the installer's phone to a staff or back-office network that can reach the TVs, or switch client isolation off on the TVs' network until the installation is finished. After installation it can be switched back on: the TVs only need outbound internet access (if you use guest casting, see section 5 for what the CastBridge appliance needs).

5. Guest casting (CastBridge appliance)

Guest casting lets a guest cast YouTube and other Google Cast apps from their own phone to their room's TV. It runs through a small on-site appliance (CastBridge) with one network leg on the guest Wi-Fi and one on the TV network. **Guest phones never talk to TVs:** the phone talks only to the appliance, and the appliance talks to the TV on that guest's behalf. Casting therefore needs **no router rules, no VLAN changes and no firewall changes**. The checklist below is about wireless controller behaviour, not firewall openings.

From → To	Ports	Purpose
Guest phone → appliance (guest leg)	TCP 8443 · TCP 8008/8009 · dynamic high TCP · UDP 5353 both ways	Pairing page (8443), cast control relay (8008/8009), cast media (dynamic ports), mDNS discovery (5353)
Appliance (TV leg) → TVs	TCP 8008/8009 · dynamic high TCP · UDP 5353 unicast + multicast · TCP 5555 (ADB)	Cast delivery to the TV, mDNS discovery, and automated cast receiver repair (5555 stays open after installation day)
Appliance → internet	TCP 443 to ota.mndev.co.za only	Pairing token checks, status heartbeat, remote network diagnostics and software updates. **No inbound connections of any kind.**

Guest Wi-Fi checklist (controller settings, not firewall rules)

- **Client isolation / AP isolation / peer blocking:** must exempt the appliance's guest-leg IP (or MAC address). Guests never need to reach each other, only the appliance.
- **mDNS and multicast filtering:** UDP 5353 to and from 224.0.0.251 must pass between guest clients and the appliance, in both directions. Controller features named "multicast optimisation", "mDNS snooping", "mDNS gateway" or "broadcast filtering" commonly absorb this traffic; exempt the guest SSID or the appliance.
- **No web-only port policy for guests:** a cast session opens additional high TCP ports to the appliance after it starts. A policy limiting guests to ports 80/443 lets casting begin and then kills the video seconds later.

TV network checklist

- Multicast between the TVs and the appliance is preferred but **not required**: where APs or switches drop multicast between wireless and wired devices (common in hotels), the appliance automatically falls back to direct unicast mDNS queries (UDP 5353 to each TV).
- The appliance must reach the TVs on TCP 8008, 8009, dynamic high ports and TCP 5555 (ADB) within the TV segment.

The pairing page is plain HTTP on port 8443, by design A closed hotel network cannot carry a publicly trusted TLS certificate, and a self-signed one shows every guest a browser security warning. The page carries only a signed, single-use pairing token, no personal data, and the traffic never leaves the hotel LAN.

What casting does NOT need No port forwarding, no static routes, no mDNS gateway on the router (the appliance performs per-guest, per-room discovery itself). The recommended hardening stays in place: one rule, *deny guest VLAN → TV VLAN*, because the appliance does not use that path. The appliance also reports **live network diagnostics** to our management portal, so if casting misbehaves we can tell your team exactly which of the paths above is blocked, with evidence, without needing access to your network.

6. Sizing: how much bandwidth do the TVs actually need?

Streaming is the only load that matters (idle TV traffic is a heartbeat every ~2 minutes; app updates can come from a LAN mirror). Netflix's commercial spec of **4 Mbps is per active stream, not per room**. It assumes every room streams simultaneously, which never happens. What actually matters:

- **Occupancy**: only occupied rooms stream.
- **Concurrency**: at prime time (19:00 to 22:00) typically **40 to 50% of occupied rooms** are streaming; the rest of the day is far lower.
- **Per-stream rate**: Atrium TVs are 1080p panels, so streams settle at **3 to 5 Mbps** (no 4K pulls). Plan on 4 Mbps.

Formula peak Mbps ≈ rooms × occupancy × 50% × 4 Mbps, roughly *2 Mbps per occupied room*.

Worked example, 100 rooms at 60% occupancy (60 occupied):

Scenario	Calculation → bandwidth
Theoretical worst case	all 60 occupied rooms streaming at 4 Mbps → **240 Mbps**
Realistic prime-time peak	50% of occupied (30 streams) × 4 Mbps → **~120 Mbps**
Typical evening	~30% of occupied (18 streams) × 3.5 Mbps → **~65 Mbps**
Provisioning target (TV side)	prime-time peak + 30% headroom → **~155 Mbps**

Recommendation: add **~30% headroom** to the prime-time peak, then add the hotel's own budget for guest Wi-Fi and operations on top. The line should cover that total. For a 100-room property that means **200 Mbps** for the TV side at ~60% occupancy (~155 Mbps target) and **300 Mbps** for full-occupancy cover (~260 Mbps target). **100 Mbps** is a workable floor at ~60% occupancy with a per-TV QoS cap (~5 Mbps per room on the TV VLAN): adaptive bitrate then steps every stream down gracefully in a freak all-rooms moment instead of anyone buffering. Guest **personal devices** (phones/laptops on guest Wi-Fi) are usually a larger load than the TVs. The portal's bandwidth calculator takes the hotel's Wi-Fi figure and sizes the whole line.

Appendix A: Free-to-air channel pack (only if used)

Optional Applies only to hotels using Atrium's built-in free-to-air channel pack instead of (or alongside) their own head-end. These channels are public internet HLS streams played directly by the TVs, so a strict allowlist must include their CDNs. They are third-party hosts and can change; hotels with their own head-end can ignore this section.

Purpose	Destinations (TCP 443)
SABC channels	*.cdn.mangomolo.com
Other SA channels	cdn.freevisiontv.co.za, cdnstack.internetmultimediaonline.org, streamdot.broadpeak.io, livestream2.bokradio.co.za
International news	static.france24.com, dwamdstream102.akamaized.net, live-hls-web-aje-fa.thehlive.com, live-gbnews.simplestreamcdn.com, bloomberg.com, 247wlive.foxweather.com
Other international	*.cloudfront.net, nmx1ota.akamaized.net, *.mediapackage.us-east-1.amazonaws.com, world.lls.pbs.org, livestream.pbskids.org, fast-channels.sinclairstoryline.com, rpn.bozztv.com, bozztv.com
Channel logos	i.imgur.com, admango.cdn.mangomolo.com

Last updated 2026-10-06 · Atrium Connected Room Platform, MN Digital Services.
Questions? Email support@mnsa.co.za or ask your Atrium installer.