

Home Network Security Assessment & Hardening

Router: TP-Link Archer AX55 Pro (v2.0)

Firmware: 1.0.5 Build 20240121 rel.56156(5553)

Network Type: Home Network

Assessment Type: Configuration Review & Security Hardening

Date: December 2025

1. Executive Summary

This report documents a security assessment and hardening review of a home network using a TP-Link Archer AX55 Pro router. The goal was to validate existing security controls, identify exposure risks, and ensure the network is configured according to modern home-network security best practices.

The assessment focused on wireless security, device visibility, management access, firmware status, network segmentation, and exposure discovery using passive and active techniques.

2. Environment Overview

- **Router Model:** TP-Link Archer AX55 Pro (v2.0)
- **Firmware Status:** Up to date
- **Wireless Security:** WPA3-Personal enabled
- **Network Segmentation:** Main, Guest, IoT networks
- **Total Connected Devices:** ~10
- **Assessment Tools:** Router UI, ARP table review, Nmap scan

Online Update

Update firmware for this router over the internet.

Firmware Version: 1.0.5 Build 20240121 rel.56156(5553)

Hardware Version:

CHECK FOR UPDATES

Firmware is up to date.

3. Connected Devices & Visibility

The router detected 10 active client devices. An ARP table review displayed 11 entries, which is expected behavior due to gateway presence and ARP caching.

This confirms accurate device visibility and no unexpected hosts at the router level.

The screenshot shows the TP-Link router's web interface. The top navigation bar includes the TP-Link logo, a search bar, TP-Link ID, and Log Out. The main menu has icons for Network Map, Internet, Wireless, HomeShield, and Advanced. The 'Clients' section is selected, showing a dropdown for 'All (10)' and a 'View Deny List' link. Below is a table of connected clients.

Device Info	Real-time Rate	Tx/Rx Rate(Mbps)	Duration	Speed Limit	Block
	↑ 0 Kb/s ↓ 0 Kb/s	 135 / 60	11 Days 15 h 16 min	---	

```
C:\Users\ >arp -a

Interface:
Internet Address      Physical Address      Type
dynamic
dynamic
dynamic
dynamic
static
static
static
static
static
static
static
static
```

4. Wireless Security Configuration

- WPA3-Personal was already enabled
- WPS was fully disabled to prevent brute-force enrollment attacks
- Strong wireless encryption in place with no downgrade mechanisms enabled

OFDMA/MU-MIMO:

Smart Connect: Enable [?](#)


Wireless Radio: Enable

[Share Network](#)

Network Name (SSID):

Hide SSID

Security:

WPS: 

5. Administrative & Management Security

- Router administrative interface protected with a unique password
- Remote management disabled
- HTTPS login enabled

These settings reduce the attack surface by preventing external management access and protecting administrative credentials during login.

Remote Management

Access and manage the router over the internet.

Note: Remote Management is not supported when you are connected to the internet only via IPv6. If you want to use Remote Management, please make sure you have set up an IPv4 connection first.

Remote Management: Enable

6. UPnP & Service Exposure

- UPnP enabled intentionally to support gaming devices (PS5 and PC)
- Risk acknowledged and documented
- No unnecessary port forwards observed

UPnP remains enabled only for functional requirements and is monitored as a known risk tradeoff.

UPnP

Enable UPnP (Universal Plug and Play) to allow devices on your local network to dynamically open ports for applications such as multiplayer gaming and real-time communications.

UPnP:

7. Firmware & DNS Configuration

- Firmware verified as current
- DNS resolution obtained dynamically from ISP
- No custom DNS filtering or third-party resolvers configured
- Baseline DNS state documented

Online Update

Update firmware for this router over the internet.

Firmware Version: 1.0.5 Build 20240121 rel.56156(5553)

Hardware Version:

CHECK FOR UPDATES

Firmware is up to date.

Internet

Set up an internet connection with the service information provided by your ISP (internet service provider).

Internet Connection Type:

Select this type if your ISP doesn't provide any information for internet connection.

MAC Clone

Set the MAC address of your router. Use the default address unless your ISP allows internet access from only a specific MAC address.

Router MAC Address:

8. Network Discovery & Exposure Testing

An Nmap scan identified **9 hosts**, aligning with known connected devices. No unexpected hosts or exposed services were discovered.

This confirms proper network segmentation and lack of unintended exposure.

```
nmap -sn 192.168.0.0/24
```

```
Nmap done: 256 IP addresses (9 hosts up) scanned in 7.46 seconds
```

9. Network Segmentation & Isolation

The network is segmented into:

- **Primary Network:** Trusted personal devices
- **Guest Network:** Isolated internet-only access
- **IoT Network:** Isolated from internal devices

This segmentation limits lateral movement and reduces impact from compromised or untrusted devices.

IoT Network

Create a dedicated wireless network to manage your IoT devices together, such as smart lights and cameras.

2.4GHz: Enable

[Share Network](#)

Guest Network

Enable the wireless bands you want your guests to use and complete the related information.

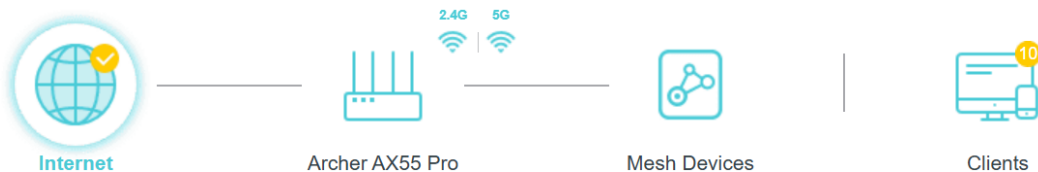
2.4GHz: Enable

[Share Network](#)

10. Final Validation

A final configuration review confirmed:

- No loss of connectivity
- No performance degradation
- Security controls remained active and functional



11. Summary & Portfolio Value

This project demonstrates:

- Practical network security assessment skills
- Safe configuration hardening without service disruption
- Risk-based decision making (UPnP tradeoff)
- Documentation suitable for client delivery

This assessment is representative of entry-to-mid level network security hardening engagements.