# 30-09-2025 Building a Secure and Scalable Office Network: UniFi–Splunk Integration, Wi-Fi 6/6E Access Points, and Modern Endpoint Protection

## 1. How to Forward UDM-Pro / UniFi Logs to Splunk (Direct vs. Collector Setup)

Centralizing logs from your UniFi network devices into a SIEM (Security Information and Event Management) system like Splunk is a critical step for advanced monitoring, threat hunting, and troubleshooting.

#### Method 1: Direct Forwarding (The Simple Approach)

This method configures your UDM-Pro to send syslog data directly to your Splunk instance.

- **Concept:** `UDM-Pro ---> Splunk Server`
- **How to Implement:**
    1. **On the UDM-Pro / UniFi Network Controller:**
        - Navigate to **Settings > System > Advanced**.
        - Under the "Remote Logging" section, enable the **Syslog** option.
        - Enter the **IP address** of your Splunk server.
        - Enter the **port number** that Splunk will be listening on (the standard for syslog is UDP port 514).
        - Apply the changes. Your UDM-Pro will now start sending all of its system logs to that destination.
    2. **On the Splunk Server:**
        - Log in to Splunk and go to **Settings > Data Inputs**.
        - Create a new data input by clicking **UDP** or **TCP** (ensure this matches what UniFi supports, typically UDP).
        - Enter the same **port number** (514) you configured in UniFi.
        - Give it a name and follow the prompts to set the source type (e.g., `syslog`) and the index you want to store the data in.
        - Save the input. Splunk is now listening for the logs.
- **Pros:** Very easy and quick to set up.
- **Cons:** Less reliable, as UDP does not guarantee message delivery. There is no filtering, so all logs (including noise) are sent to Splunk, increasing indexing volume and cost. If the Splunk server is down, the logs are lost.

**Method 2: Using a Collector (The Robust & Scalable Approach)**

This method places a lightweight data collector between your UDM-Pro and Splunk. This is the best practice for production environments.

- **Concept:** `UDM-Pro ---> Syslog Collector (e.g., Splunk Universal Forwarder) ---> Splunk Server`
- **How to Implement:**
    1. **Set up the Collector:** On a small server (or virtual machine), install a **Splunk Universal Forwarder** or a standard syslog service like `syslog-ng`. Configure this service to listen for syslog data on UDP port 514. Then, configure it to reliably forward that data (using TCP) to your main Splunk indexing server on its management port (for Splunk Forwarders, this is typically 9997).
    2. **On the UDM-Pro / UniFi Network Controller:** Follow the same steps as the direct method, but for the IP address, enter the **IP of your collector server**, not your main Splunk server.
    3. **On the Splunk Server:** Configure Splunk to receive data from your Splunk Forwarder by going to **Settings > Forwarding and Receiving** and enabling the receiver port (e.g., 9997).
- **Pros: Highly reliable** (uses TCP and can buffer data if the connection drops). **Efficient** (can filter out unwanted logs at the collector level). **Scalable** (multiple devices can send logs to the collector, which manages the single connection to Splunk).
- **Cons:** Requires an additional component (the collector) to set up and manage.

## 2. How to Identify and Set Up TP-Link Archer AXE75 (Wi-Fi 6E) Router

- **Identification:** The Archer AXE75 is a high-performance **Wi-Fi 6E** router. Its key identifier is support for the **6 GHz band**, providing a new, uncongested wireless spectrum. Physically, it features multiple external antennas for wide coverage and a **2.5 Gbps WAN port**, designed for multi-gig internet plans.
- **Setup as an Access Point (AP) Mode):**
    1. **Initial Connection:** Before connecting it to your main network, plug the AXE75 into power and connect a computer directly to one of its LAN ports with an Ethernet cable.
    2. **Access the Web Interface:** Open a web browser and go to `http://tplinkwifi.net`. Log in or complete the initial setup wizard.
    3. **Change Operation Mode:** Navigate to the **Advanced** tab. In the left-hand menu, find **Operation Mode**.

4. **Select Access Point:** Choose the **Access Point** option and click **Save**. The router will reboot.
5. **Final Connection:** After it restarts, connect an Ethernet cable from a LAN port on your main UDM-Pro (or a connected switch) to the **2.5 Gbps WAN port** on the AXE75. It will now function as a powerful tri-band access point for your network.

## 3. How to Identify and Set Up Netgear Nighthawk AX1800 (Wi-Fi 6) Router

- **Identification:** The Nighthawk AX1800 (RAX20) is a capable **Wi-Fi 6** router. It is **dual-band**, meaning it operates on the 2.4 GHz and 5 GHz frequencies but lacks the 6 GHz band of Wi-Fi 6E. It features the characteristic angular "Nighthawk" design and supports speeds suitable for most home and small office environments.
- **Setup as an Access Point (AP Mode):**
    1. **Initial Connection:** Power on the router and connect a computer to one of its LAN ports.
    2. **Access the Web Interface:** Open a web browser and go to `http://www.routerlogin.net`. Log in with your admin credentials.
    3. **Change Operation Mode:** In the admin panel, navigate to **ADVANCED > Advanced Setup > Router / AP Mode**.
    4. **Select AP Mode:** Select the **AP Mode** checkbox and click **Apply**. The router will restart.
    5. **Final Connection:** Once rebooted, connect an Ethernet cable from your main UDM-Pro (or a switch) to the yellow **Internet (WAN) port** on the Nighthawk. It will now serve as a dual-band Wi-Fi 6 access point.

## 4. Comparison: TP-Link AXE75 vs. Netgear AX1800

| Feature | TP-Link Archer AXE75 | Netgear Nighthawk AX1800 (RAX20) | Key Consideration |
|---|---|---|---|
| **Wi-Fi Standard** | **Wi-Fi 6E** | Wi-Fi 6 | The AXE75 is more future-proof with access to the new 6 GHz band. |
| **Wireless** | **Tri-Band** (2.4 GHz, 5 GHz, 6 GHz) | Dual-Band (2.4 GHz, 5 GHz) | The 6 GHz band on the AXE75 offers a dedicated, high-speed, |

| | | | |
|---|---|---|---|
| **Bands** | | | low-interference lane for compatible devices. |
| **WAN Port Speed** | **2.5 Gbps** | 1 Gbps | The AXE75 can support internet speeds greater than 1 Gbps. |
| **Performance** | Higher overall throughput (AXE5400) | Standard throughput (AX1800) | The AXE75 is built for higher device density and more demanding tasks. |
| **Ideal Use Case** | A high-performance access point for a dense office environment with cutting-edge devices. | A solid, budget-friendly access point for standard Wi-Fi 6 coverage. | Choose the AXE75 for performance-critical areas and the AX1800 for general coverage. |

## 5. Use One Main Router; Others are Wi-Fi Access Points

This is the foundational principle for a stable and scalable network. When you have multiple devices capable of routing, only one should be in charge. Your UDM-Pro is your **router, firewall, and DHCP server**—it manages your entire network, assigns IP addresses, and controls traffic to and from the internet. If you plug in another router in its default mode, it will also try to assign IP addresses, creating a "Double NAT" situation and IP conflicts. This isolates devices on different sub-networks, preventing them from communicating. By switching all other routers to **AP Mode**, you turn off their routing functions. They become simple devices that convert the wired network signal from the UDM-Pro into a wireless one, acting as powerful extensions of your single, unified network.

## 6. A Fast Internal Network is Crucial for Local Office Tasks

It's vital to differentiate between your **internet (WAN) speed** and your **internal (LAN) speed**. Your 300 Mbps internet plan dictates how fast you can download from or upload to the web. Your internal LAN speed, determined by your switches and access points, dictates how fast devices *inside your office* can talk to each other. With Gigabit switches (1,000 Mbps) and Wi-Fi 6 access points, your internal network is over three times faster than your internet connection. This high-speed LAN is critical for office productivity tasks such as:

- Transferring large design files between computers.
- Backing up workstations to a central Network Attached Storage (NAS) device.
- Streaming high-resolution video from a local media server.

## 7. Protect Your Network Perimeter and Each Individual Computer

A complete security strategy requires a layered defense.

- **Perimeter Security (The Castle Wall):** This is the role of your UDM-Pro. Its firewall inspects all traffic entering and leaving your network, blocking known threats and unauthorized access attempts from the internet. It protects your entire network as a whole.
- **Endpoint Security (The Guard on Every Door):** This is the software you install on every individual device (laptops, servers). Threats can bypass the perimeter through phishing emails, malicious USB drives, or employee error. Endpoint security software acts as the last line of defense, monitoring the device itself for suspicious behavior and stopping attacks like ransomware before they can execute. You need both to be secure.

## 8. Use Modern AI Security to Block New, Unknown Threats

Traditional antivirus software worked by matching files against a list of known virus "signatures." This is ineffective against modern attacks because hackers create thousands of new threats every day ("zero-day attacks") that have no signature. **Modern Endpoint Protection Platforms (EPP/EDR)** use Artificial Intelligence and behavioral analysis. Instead of looking for a known bad file, they watch for suspicious *behavior*. For example, they can recognize the *actions* of a ransomware attack (e.g., a Word document suddenly trying to rapidly encrypt thousands of files) and terminate the process instantly, even if it's a brand-new, never-before-seen strain.

## 9. Affordable, Enterprise-Grade Security Exists for Small Businesses

For years, the most advanced security tools (like EDR and proactive threat hunting) were complex and expensive, accessible only to large corporations. The shift to cloud computing and subscription models has changed this. Companies like Microsoft have packaged these powerful tools into affordable, easy-to-manage solutions. **Microsoft Defender for Business**, included in the **Microsoft 365 Business Premium** subscription, provides a complete, enterprise-grade endpoint security platform that is managed from a simple cloud dashboard. This gives small businesses access to the same level of protection as large enterprises without the high cost or complexity.