Setting up a proxy server is a smart, centralized way to manage internet safety for a Small Office/Home Office (SOHO) network. Instead of configuring every single tablet, laptop, and phone individually, a proxy acts as a "gatekeeper" for all web traffic.

---

1. Choose Your Proxy Solution

For a SOHO environment, you generally have two paths:

- **Software-Based (Squid):** The industry standard. It's free, open-source, and highly customizable. It usually runs on a dedicated Linux machine or a Raspberry Pi.
- **Hardware/Plug-and-Play (pfSense/OPNsense):** These are firewall operating systems that include proxy capabilities (like Squid) built-in. This is often the most stable "set it and forget it" option for a home office.

---

2. Basic Network Architecture

To filter effectively, your proxy should sit between your local devices and the internet.

1. **Client Devices** (Kids' laptops, tablets) send a request to view a website.
2. **Proxy Server** receives the request and checks it against a "Blacklist."
3. **Filtering Engine** denies the request if it matches a forbidden category and serves a "Blocked" page instead.

---

3. Step-by-Step Configuration (Using Squid)

If you are using a Linux-based system (like Ubuntu), here is the high-level workflow to get filtering running:

A. Install Squid and SquidGuard

Squid handles the traffic, but **SquidGuard** is the plugin that specifically handles the URL filtering and blacklists.

Bash
```
sudo apt update
sudo apt install squid squidguard
```

B. Download a Blacklist

You don't want to manually type in every adult site on Earth. You need a pre-compiled list (often called a "Blacklist"). Popular sources include **Shallalist** or **UT1**.

- Download the archive.
- Extract it to `/var/lib/squidguard/db/`.

C. Configure SquidGuard Rules

You will edit the `squidGuard.conf` file to define what is blocked. It looks something like this:

Plaintext
```
dest adult {
   domainlist adult/domains
   urllist adult/urls
}

acl {
   default {
      pass !adult all
      redirect http://your-internal-site.com/blocked.html
   }
}
```

---

4. Enforcement: Transparent vs. Manual

This is where most people get stuck. How do you make sure the kids don't just bypass the proxy?

- **Manual Configuration:** You enter the proxy IP and port (usually 3128) into the Network Settings of every device. **Weakness:** A tech-savvy kid can just turn the setting off.
- **Transparent Proxy:** You configure your Router to force all traffic on Port 80 (HTTP) and 443 (HTTPS) through the proxy automatically.

- *Note:* Transparently filtering HTTPS (encrypted) traffic requires installing a **CA Certificate** on every device to allow the proxy to "peek" at the URL.

---

5. Alternative: The "Easy" Proxy (DNS Filtering)

If setting up a Linux server feels like overkill, you can use a **DNS Proxy** like **Cloudflare for Families** or **OpenDNS**.

1. Log into your Router settings.
2. Change the DNS Server IPs to:
    - **Cloudflare (Malware/Adult Block):** `1.1.1.3` and `1.0.0.3`
    - **OpenDNS FamilyShield:** `208.67.222.123` and `208.67.220.123`
3. **Result:** When a device tries to resolve "badsite.com," the DNS proxy simply refuses to give the IP address.

Final Pro-Tips

- **Whitelisting:** Always have a "Whitelist" for sites your kids actually need for school, just in case the filter is too aggressive.
- **Physical Security:** Ensure your router and proxy hardware are in a place where cables can't be swapped to bypass the filter.
- **The "Human" Element:** No filter is 100% perfect. These tools are best used alongside open conversations about internet safety.

This works well when creating this project on a old desktop PC or Raspberry Pi.