Policy Management and Filtering Features

How can I block all subdomains of a specific domain?

To block all subdomains of a certain domain, you should add the specific record to your **Denylist**. You must add the domain without the leading WWW to ensure the block is effective. For instance, if your goal is to block subdomains of the https://www.google.com domain, you would simply enter google.com into the Denylist.

What is NAT DNS, and is it included in my plan?

Network Address Translation over DNS (NAT DNS) is a specialized feature used for identifying and filtering traffic in specific network environments. However, this feature is not included in all service tiers; it is **not available for the Safe Home and Basic plans**.

How can I create a custom schedule for blocking content?

SafeDNS provides a Schedule feature that offers more granular control than standard filtering systems. While many systems utilize simple schedules that completely block internet access during set times, the SafeDNS system allows for **content filtering schedules**. This allows administrators to adjust what types of content are blocked at different times of the day without cutting off internet access entirely.

How do I configure the block page that users see when a website is filtered?

The **block page** is the landing page displayed to a user whenever they attempt to access a website that is restricted by your active filtering rules. The documentation includes a dedicated Block Page Setup guide to assist administrators in configuring this interface.

How can I use the same list of domains across multiple policies?

To avoid manually entering the same information multiple times, you can use the Allow/Denylists and Named Lists feature. This feature is specifically designed for situations where you need to **apply the same list of domains to different policies** across your network, streamlining the management of multiple user groups or filtering levels.

How can I prevent users from bypassing web filtering?

To maintain the integrity of your network policies, SafeDNS offers several Web Filtering Bypass Prevention recommendations. A primary recommendation is to **block the "Proxies & Anonymizers" category**, which prevents users from accessing external services designed to circumvent DNS-based filters.

Additionally, administrators should **block specific browser settings or "flags"** in Google Chrome and Mozilla Firefox that enable DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) directly within the browser. Because these browser-level settings can sometimes bypass system-wide DNS configurations, disabling them is a critical step in ensuring all traffic remains filtered.

Revision #2
Created 25 January 2026 19:16:50 by Val Redman
Updated 25 January 2026 19:20:13 by Val Redman