

|  |
| --- |
| NXFiltering  Grootschalig DNS-filtering |
| **Opleiding: Cybersecurity**  **Academiejaar: 2024 - 2025**  **Thierry van Boxel, S160484**  Ernie de Magtige |

AP.BE

Inhoud

Inhoud

[NXFiltering 1](#_Toc197342580)

[Grootschalig DNS-filtering 1](#_Toc197342581)

[Inhoud 1](#_Toc197342582)

[Voorwoord 4](#_Toc197342583)

[1 Inleiding 5](#_Toc197342584)

[1.1 Belangrijke kenmerken van NXFilter zijn: 5](#_Toc197342585)

[1.2 Features van NXFilter 6](#_Toc197342586)

[2 Setup 7](#_Toc197342587)

[2.1 infrastructuur 7](#_Toc197342588)

[2.2 voorbereiding 7](#_Toc197342589)

[2.3 Vereisten (hardware en software) 7](#_Toc197342590)

[3 Configuratie en installatie 8](#_Toc197342591)

[3.1 Configuratie en static-ip 8](#_Toc197342592)

[3.1.1 Optioneel: 9](#_Toc197342593)

[3.2 Java installeren 9](#_Toc197342594)

[3.3 Nxfilter downloaden & installeren 9](#_Toc197342595)

[3.3.1 systeemconfiguratie 9](#_Toc197342596)

[3.3.2 logging 10](#_Toc197342597)

[3.3.3 Poort wijziging 10](#_Toc197342598)

[4 Firewall en router instellingen 11](#_Toc197342599)

[4.1 Firewall 11](#_Toc197342600)

[4.2 Router 11](#_Toc197342601)

[5 Webinterface en loggen 13](#_Toc197342602)

[5.1 webinterface bereiken en standaard instellingen. 13](#_Toc197342603)

[6 Configuratie via de webinterface 13](#_Toc197342604)

[6.1 Overzicht van het filter dashboard 14](#_Toc197342605)

[6.2 Basisinstellingen (config/system) 14](#_Toc197342606)

[6.2.1 Admin 14](#_Toc197342607)

[6.2.2 Gui acces control: 15](#_Toc197342608)

[6.2.3 Alert: 16](#_Toc197342609)

[6.3 DNS configuratie 18](#_Toc197342610)

[6.3.1 DNS > setup 18](#_Toc197342611)

[6.4 Gebruikers beheren 19](#_Toc197342612)

[6.4.1 Ip-gebaseerde gebruikers creëren 19](#_Toc197342613)

[6.4.2 Edit users 20](#_Toc197342614)

[6.4.3 Ip-address toekennen 20](#_Toc197342615)

[6.4.4 Member off 21](#_Toc197342616)

[6.5 Groepen beheren 21](#_Toc197342617)

[6.5.1 Groep aanmaken 22](#_Toc197342618)

[6.5.2 Groep editen 22](#_Toc197342619)

[6.5.3 Policy toewijzen 23](#_Toc197342620)

[7 Troubleshooting – Veelvoorkomende problemen oplossen 24](#_Toc197342621)

[7.1 “NXFilter lijkt niet te werken – DNS valt uit”: 24](#_Toc197342622)

[7.2 “Ik kan niet in de webinterface komen”: 24](#_Toc197342623)

[7.3 “Clients gebruiken NXFilter niet (filter gaat voorbij)”: 24](#_Toc197342624)

[7.4 “Sommige geblokkeerde sites laden toch door”: 25](#_Toc197342625)

[7.5 “NXFilter wordt heel traag of valt uit bij veel verkeer”: 26](#_Toc197342626)

[8 Testen en validatie 26](#_Toc197342627)

[8.1 Categorieblokkade testen: 26](#_Toc197342628)

[8.2 SafeSearch test: 27](#_Toc197342629)

[8.3 Schermtijd test: 27](#_Toc197342630)

[8.4 Whitelist/Blacklist test: 27](#_Toc197342631)

[8.5 Multi-user policy test: 28](#_Toc197342632)

[8.6 Externe filtering test: 28](#_Toc197342633)

[8.7 Performance test: 28](#_Toc197342634)

[9 Best practices en onderhoudstips 29](#_Toc197342635)

[1. Wachtwoordbeheer: 29](#_Toc197342636)

[2. Regelmatige updates: 29](#_Toc197342637)

[3. Categorie lijst onderhoud (Jahaslist): 29](#_Toc197342638)

[4. Back-ups van configuratie: 29](#_Toc197342639)

[5. Monitoring van logs: 30](#_Toc197342640)

[6. Monitoring & alerts: 30](#_Toc197342641)

[7. Performance & hardware onderhoud: 30](#_Toc197342642)

[8. Beveiliging van de Pi: 30](#_Toc197342643)

[9. Policy onderhoud: 30](#_Toc197342644)

[10. Gastnetwerk scheiding: 31](#_Toc197342645)

[11. Test na wijzigingen: 31](#_Toc197342646)

[Bronvermelding 32](#_Toc197342647)

Voorwoord

In een tijd waarin digitale dreigingen en cyberaanvallen steeds geavanceerder worden, is het beschermen van onze netwerken belangrijker dan ooit. Met de opkomst van nieuwe technologieën en een alsmaar groeiende afhankelijkheid van internet, is het essentieel om niet alleen bewust te zijn van de risico’s, maar ook te beschikken over de juiste tools om deze risico’s te minimaliseren.

Tijdens mijn studie in Systeem en netwerk-beheer heb ik gemerkt hoe cruciaal effectieve webfiltering is.

NXFilter biedt een krachtige en flexibele oplossing voor netwerkbeveiliging en helpt organisaties om een veilige digitale omgeving te creëren. Dit document is geschreven met als doel om zowel beginners als ervaren IT-professionals inzicht te geven in hoe NXFilter ingezet kan worden om netwerken te beschermen tegen ongewenste content en bedreigingen.

Naast technische uitleg zal ik ook praktische toepassingen en ervaringen delen, zodat het niet alleen een theoretisch document is, maar ook een waardevolle gids voor de praktijk. Cybersecurity gaat immers niet alleen over software en firewalls, maar ook over de mensen die ermee werken en de manier waarop we digitale veiligheid benaderen.

Ik hoop dat dit document bijdraagt aan een beter begrip van webfiltering en hoe NXFilter kan helpen om een veiliger netwerk te creëren zowel thuis als binnen een bedrijf.

Thierry van Boxel

# Inleiding

NxFilter is een krachtige DNS-filtersoftware die netwerk breed wordt ingezet om internetverkeer te monitoren en te beheren. Door te fungeren als een DNS-server met ingebouwde filtermogelijkheden, kan NxFilter DNS-verzoeken toestaan of blokkeren, wat zorgt voor efficiënte en snelle filtering zonder merkbare vertragingen.

## Belangrijke kenmerken van NXFilter zijn:

* **Websiteblokkering op basis van categorieën**: Dit stelt beheerders in staat om toegang tot ongewenste websites te beperken door domeinen te classificeren en te filteren op basis van hun inhoud.
* **Lokale caching DNS-server**: NXFilter slaat DNS-responses op, waardoor latentie wordt verminderd en de netwerkprestaties verbeteren.
* **Gebruikersauthenticatie**: Ondersteuning voor verschillende authenticatiemethoden, waaronder Active Directory-integratie en IP-gebaseerde authenticatie, maakt het mogelijk om gepersonaliseerde beleidsregels toe te passen en gedetailleerde rapportages per gebruiker te genereren.
* **Meerdere filterbeleidsregels**: Beheerders kunnen verschillende beleidsregels instellen op basis van gebruikers of groepen, inclusief opties zoals schermtijdbeheer en datalimieten om bandbreedte te besparen.
* **Veilige zoekfunctie afdwingen**: NXFilter kan veilige zoekinstellingen afdwingen voor zoekmachines zoals Google en Bing, wat bijdraagt aan een veiligere internetervaring.
* **Ondersteuning voor externe filtering**: Met tools zoals NXProxy en CXBlock kunnen beheerders internetactiviteit monitoren en filteren, zelfs wanneer gebruikers zich buiten het lokale netwerk bevinden.

Door deze functies biedt NxFilter een uitgebreide oplossing voor het beheren en beveiligen van netwerkverkeer binnen diverse omgevingen, van bedrijven tot onderwijsinstellingen.

## Features van NXFilter

NXFilter heeft een aantal belangrijke, maar zeker niet de enige funties.

Hier een aantal van de meest belangrijke:

* Blocking websites by categories
* Local caching DNS server to speed up your Internet connection
* User authentication in your network
* Multiple filtering policies according to user and group
* IP or IP range based user authentication
* Active Directory integration or single sign-on by Active Directory
* 802.1X Wi-Fi user authentication for mobile devices
* Active Directory integration over cloud
* Relaying server to identify users behind a router
* You can create user and group on NxFilter GUI
* Data cap for your users to save your bandwidth
* Screen time for your users
* Granular reporting with usernames
* Network level safe-search enforcing
* Remote filtering client
* Sub-admin accounts for limited admin roles
* Multi-tenancy cloud based filtering service
* Clustering for fail-safe and load balancing
* Dynamic website classification
* Custom categories for website classification
* Exporting traffic data using Syslog
* White label based commercial use
* Authoritative DNS server
* URL keyword filtering
* Filtering roaming iOS/Android devices by DNS over HTTPS

# Setup

## Infrastructuuroverzicht

NXFilter zal worden geïnstalleerd op een Raspberry Pi 5 binnen een thuisnetwerk en fungeren als centrale DNS-filter. Het idee is dat alle apparaten in het LAN hun DNS-verkeer naar de Raspberry Pi sturen, in plaats van direct naar een externe DNS. De Pi (met NXFilter software) beantwoordt die DNS-queries: als het verzoek naar een toegestane site gaat, geeft NXFilter het echte IP-adres terug (eventueel vanuit cache of via upstream DNS). Gaat het naar een geblokkeerde site, dan zal NXFilter zorgen dat de verbinding niet tot stand komt (door geen of een aangepast IP terug te geven) en dit loggen.

Overzicht van NXFilter in een thuisnetwerk. De Raspberry Pi 5 draait NXFilter en is via de router verbonden met het internet. Alle clients (PC’s, telefoons, tablets) krijgen via DHCP de Pi als primaire DNS-server toegewezen. DNS-verkeer (blauwe pijlen) van de clients gaat naar NXFilter in plaats van naar een externe DNS-server. NXFilter filtert ongewenste domeinen en stuurt toegestane DNS-queries eventueel door naar upstream DNS-servers op het internet (bijv. die van de ISP, Cloudflare, Google). De beheerder kan via een aparte PC de NXFilter webinterface benaderen (groene pijlen) op poort 80/443 om instellingen te wijzigen en logs in te zien.

Zoals in het netwerkdiagram hierboven te zien is, verandert NXFilter de DNS-routing binnen je netwerk. De router blijft de gateway naar het internet voor al het verkeer, maar voor DNS-verzoeken fungeert de Raspberry Pi met NXFilter als tussenstation. Dit heeft als voordeel dat je één centrale plek hebt om internetgebruik te controleren en te filteren. Het verhoogt de netwerkveiligheid (blokkeren van malware/phishing) en kan helpen om afleiding of ongewenst gebruik te beperken zonder op elk apparaat apart software te hoeven installeren.

Afbeelding met tekst, schermopname, lijn, diagram

Door AI gegenereerde inhoud is mogelijk onjuist.

## voorbereiding

## NXFilter wordt ondersteund op meerdere besturingssystemen (Windows, Linux, macOS); in deze handleiding richten we ons op Linux (Ubuntu Server) op een Raspberry Pi 5. Voor we aan de installatie beginnen, zorg voor het volgende:

## Netwerkgegevens noteren: Bepaal welk statisch IP-adres de Raspberry Pi in het netwerk moet krijgen (bijvoorbeeld 192.168.1.10) en noteer het IP-adres van de router (gateway, bv. 192.168.1.1). Bedenk welke upstream DNS-servers de NXFilter moet gaan gebruiken – vaak gebruik je de DNS van je internetprovider of publieke servers zoals Cloudflare (1.1.1.1) en Google (8.8.8.8). Ook het lokale subnet (bijv. 255.255.255.0 of /24) is van belang bij configuratie.

## Toegang tot de Pi: Idealiter verbind je via een monitor en toetsenbord of via SSH om de Pi te configureren. Na het opzetten van het OS (Ubuntu) is het handig de laatste updates te installeren (sudo apt update && sudo apt upgrade -y).

## Download NXFilter software: Ga naar de officiële NXFilter-website en download de laatste versie (v4 of hoger) voor Linux. Je kunt dit direct op de Pi doen via wget of eerst op een PC en dan overzetten. Er is een DEB-installer beschikbaar en een ZIP-versie. In deze handleiding gebruiken we de Linux versie van NXFilter v4, die op Java (JRE) draait.

## Java Runtime: NXFilter vereist Java. Installeer een Java runtime (OpenJDK). Versie 11 of 17 van OpenJDK volstaat. Op Ubuntu kun je bijvoorbeeld sudo apt install openjdk-11-jre uitvoeren om Java te installeren.

## Zodra bovenstaande voorbereidende stappen zijn gedaan, kunnen we beginnen met de daadwerkelijke installatie en configuratie.

## Vereisten (hardware en software)

**Hardware:**

Een Raspberry Pi 5 (of vergelijkbaar model) met voeding en netwerkverbinding. Gebruik bij voorkeur een bekabelde Ethernet-verbinding voor stabiele DNS-respons. Een microSD-kaart (of eMMC/SSD als je Pi 5 dat heeft) met minimaal 8 GB opslag voor het besturingssysteem is nodig. Zorg ook voor eventuele koeling, aangezien de Pi 5 vrij krachtig is en 24/7 gebruik enige warmte kan genereren (zie ook sectie 10).

**Besturingssysteem:**

Ubuntu Server 22.04+ 64-bit voor Raspberry Pi (of Raspberry Pi OS Lite 64-bit) wordt aangeraden. Deze bieden de nodige stabiliteit en pakketbeheer. Tip: Geef de Pi een herkenbare hostname (bijvoorbeeld “nxfilter”) tijdens de OS setup, zodat je hem in het netwerk makkelijk herkent.

**Netwerk:**

Een thuisnetwerk met een router die DHCP-instellingen kan aanpassen. Toegang tot de routerinterface is nodig om DNS-instellingen via DHCP te wijzigen (tenzij je handmatig op elk apparaat de DNS instelt). Ook is het handig als de router statische DHCP leases kan instellen, zodat de Pi altijd hetzelfde IP krijgt (of configureer statisch IP op de Pi zelf – zie 3.1).

**NXFilter software:**

Download het NXFilter pakket (bijvoorbeeld nxfilter-4.x.x.zip of .deb). Controleer op de NXFilter-site of er specifieke instructies zijn voor jouw OS. Voor Raspberry Pi (ARM) is de ZIP-installatie vaak bruikbaar omdat de .deb mogelijk voor x86 is. We zullen de ZIP aanpak beschrijven (universeel voor Linux).

**Overige software:**

OpenJDK (Java) zoals genoemd. Daarnaast zijn tools als nslookup, dig en een text-editor (nano/vim) handig voor configuratie en troubleshooting.

# Configuratie en installatie

## Configuratie en static-ip

Omdat NXFilter als DNS-server fungeert, is het essentieel dat de Raspberry Pi beschikt over een statisch IP-adres. Dit garandeert dat netwerkapparaten consistent verbinding kunnen maken.

**Statisch IP instellen (via Netplan op Ubuntu):**

1. Bepaal het gewenste IP-adres voor je Raspberry Pi (bijvoorbeeld: 192.168.1.10) en noteer ook het IP-adres van je router (gateway) en je DNS-server(s) (meestal de router zelf of een externe DNS zoals Cloudflare).
2. Open het Netplan configuratiebestand (standaardpad):

* sudo nano /etc/netplan/50-cloud-init.yaml

1. Wijzig de configuratie naar bijvoorbeeld:

network:

version: 2

ethernets:

eth0:

dhcp4: no

addresses: [192.168.1.10/24]

gateway4: 192.168.1.1

nameservers:

addresses: [1.1.1.1, 1.0.0.1] # of je ISP/router DNS

In deze configuratie krijgt eth0 (ethernetpoort) het statische IP-adres 192.168.1.10. (pas dit aan naar het gewenste ip-address)

De router (gateway4) staat ingesteld op 192.168.1.1(wijzigen naar je eigen router ip-address), en Cloudflare DNS-servers (1.1.1.1 en 1.0.0.1) zijn ingesteld als upstream DNS.

* Sla het bestand op en voer netplan uit om de instellingen toe te passen:
  + sudo netplan apply
* Test of de Pi het gewenste IP heeft en of internet werkt met het ping commando:
  + ip addr show eth0
  + ping -c3 8.8.8.8

### Optioneel:

* Geef je Raspberry Pi een herkenbare hostnaam (bijvoorbeeld: nxfilter-pi) via:
  + /etc/hostname
  + /etc/hosts

Updaten van pakketten:

* sudo apt update && sudo apt upgrade -y

## Java installeren

NXFilter draait op Java. Daarom moet eerst een Java Runtime Environment worden geïnstalleerd.

**Installatie via apt:**

* + - sudo apt install openjdk-11-jre-headless

*(Je mag ook een nieuwere LTS-versie gebruiken, bijvoorbeeld OpenJDK 17.)* Verifieer de installatie met:

* + - java -version

Na succesvolle installatie zou dit een versie moeten tonen (bijv. OpenJDK 11.0.x).

## Nxfilter downloaden & installeren

Nu installeren we NXFilter zelf. De ontwikkelaars bieden een Debian-package (.deb) die we direct kunnen gebruiken:

1. **Download de NXFilter .deb:** Ga naar de officiële NXFilter downloadpagina of gebruik wget om het pakket op te halen. Voorbeeld (versienummer kan afwijken):
   * + wget <http://pub.nxfilter.org/nxfilter-4.7.1.7.deb>
     + sudo dpkg -i nxfilter-4.7.1.7.deb

Dit download en installeerd NXFilter versie 4.7.1.7. Controleer op de site of er een nieuwere versie is en pas het commando aan indien nodig. (De versie is afhankelijk van de hardware.)

### systeemconfiguratie

Eens nxfilter is geinstalleerd moeten we nog een aantal weizigingen toebrengen op het systeem.

Met volgende commando’s ga je nxfilter permanent activeren (na reboot van het systeem) en starten.

* + - sudo systemctl enable nxfilter
    - sudo systemctl start nxfilter

herstart het apparaat en gebruik volgend commando om te controleren of nxfilter actief is:

* + - systemctl starus nxfilter

### logging

Eens nxfilter gestart duurt het even voor je het via de Gui kan bereiken. Om het proces en activiteiten te bekijken kan je de loggin’s raadplegen door het volgende commando te gebruiken:

* + - tail -f /nxfilter/log/nxfilter.log

Als in de log word aangegeven dat de webservice luistert op poorten is de installatie gelukt.

### Poort wijziging

Nxfilter luistert naar standaard-poorten als 80,443 of 53. De webinterface is te bereiken op poort 80. Als we dit zouden laten staan zou het niet verandwoord zijn mits iedereen de standaard-poort kent. Dit kunnen we wijzigen door de poort in het cfs.properties aan te passen.

Eerst gaan we nxfilter stoppen:

* + - sudo systemctl stop nxfilter

Het installatiepad verschilt van systeem tot systeem, meestal staan ze op een van deze locaties:

* + - sudo nano /opt/nxfilter/conf/cfg.properties
    - sudo nano /usr/local/nxfilter/conf/cfg.properties
    - sudo nano /nxfilter/conf/cfg.properties # meest voorkomende

1

Afbeelding met tekst, schermopname, Lettertype, ontwerp

Door AI gegenereerde inhoud is mogelijk onjuist.in het bestand zoek je naar de regel:

* + - http\_port = 80
    - https\_port = 443

(**Listen\_ip** staat op 0.0.0.0 wat naar de ip van de pi leid)

Aan te raden is dat je dit wijzigt naar een Dynamische poort. (49152-65535)

Deze poorten dienen meer voor tijdelijke connecties, maar aangezien we later een verwijzing gaan doen kan dit perfect dienen en geeft het een extra beveiliging.

#### Welke poorten te gebruiken in jou netwerk

2

|  |  |  |
| --- | --- | --- |
| Soort | Gebruiksdoel | Bereik |
| Well-known-ports | http, https, dns, ssh, … | 0-1023 |
| Registerd ports | Rdp, mysql,alternatief http,… | 1024-49151 |
| Dynamic / private ports | Peer to peer verbindingen (p2p-applicaties) | 49152-65535 |

# Firewall en router instellingen

Standaard luistert NXFilter op poort **53/UDP** voor DNS-verkeer en poorten **80/TCP** en **443/TCP** voor de webinterface en gerelateerde diensten​.

## Firewall

Als je Raspberry Pi een firewall (zoals UFW) actief heeft, moeten we deze poorten openen:

* + - sudo ufw allow 53/udp
    - sudo ufw allow 80/tcp
    - sudo ufw allow 443/tcp

Dit zorgt ervoor dat DNS-verzoeken van clients de Pi bereiken en dat je via HTTP (poort 80) op de webinterface kunt. Poort 443 wordt gebruikt voor de NXFilter HTTPS-interface en voor veilige externe verbindingen (zoals NXProxy of DoH, later uitgelegd).

**Let op:** NXFilter kan niet starten als poort 53, 80 of 443 al door een andere service in gebruik is​.

Zorg dus dat er geen andere DNS-server of webserver op de Pi draait (bijvoorbeeld dnsmasq of Apache/Nginx op dezelfde poorten) of verander de poort ozals eerder beschreven.

## Router

Nu NXFilter draait, moeten we ervoor zorgen dat alle apparaten in je netwerk deze Pi gebruiken als DNS-server. De eenvoudigste manier is via je **routerinstellingen:**

* + - Log in op je router en zoek de DHCP-instellingen. Pas de **primaire DNS-server** aan naar het IP-adres van de Raspberry Pi (het statische IP dat je ingesteld hebt, bv. 192.168.1.10). Vaak kun je de secundaire DNS op een openbaar DNS (zoals 1.1.1.1 of 8.8.8.8) laten staan als fallback, maar het is beter om beide op NXFilter te zetten voor volledige filtering.
    - Sla de DHCP-instellingen op. Vanaf nu zullen clients die een nieuw IP via DHCP krijgen jouw NXFilter als DNS-server gebruiken. Je kunt bestaande clients dwingen te vernieuwen door hun netwerkverbinding even uit en aan te zetten.

Als alternatief kun je op individuele apparaten handmatig de DNS instellen naar NXFilter’s IP, maar via de router is centraal beheer eenvoudiger.

Zorg er ook zeker voor dat de pi een static-ip krijgt zodat er geen conflicten ontstaan.

**Voorkom omzeiling:**

In een gezin of kleine business wil je voorkomen dat gebruikers slim de filtering ontwijken door eigen DNS-servers te gebruiken. Een best practice is om op de router uitgaand DNS-verkeer naar andere servers te blokkeren of om te leiden. Concreet: stel een firewallregel in op de router die alle uitgaande DNS (poort 53) naar buiten blokkeert, behalve afkomstig van de NXFilter-server.

Zo **moeten** clients het interne filter gebruiken. Dit is optioneel maar verhoogt de effectiviteit.

# Webinterface en loggen

Met NXFilter draaiende en netwerkclients die ernaar wijzen, kun je de **webinterface** openen om verdere configuratie te doen.

## webinterface bereiken en standaard instellingen.

Open een webbrowser op een pc in hetzelfde netwerk en ga naar http://<IP-adres>/admin. NXFilter gebruikt standaard poort 80, maar in deze opstelling hebben we de poort gewijzigd naar een Dynamische poort. Om alsnog de web-interface te bereiken zet je achter een dubbel punt de ingestelde poort. Bv;

* + - http://192.168.1.10:56040/admin.

Afbeelding met tekst, schermopname, hemel, wolk

Door AI gegenereerde inhoud is mogelijk onjuist.Eens de interface geladen is kan je inloggen met de standaard admin-gebruikersnaam en wachtwoord:

3

* + - admin / admin

Na inloggen zie je het NXFilter dashboard (overzichtspagina). Belangrijk: Ga direct naar Config > Setup > Admin (of soortgelijke sectie) en wijzig het admin-wachtwoord naar iets sterks. Dit voorkomt dat onbevoegden je filter instellen.

# Configuratie via de webinterface

De NXFilter webinterface is het hart van de configuratie. Hier kun je instellingen aanpassen, gebruikers en policies aanmaken, logs bekijken, enz. We lopen de belangrijkste onderdelen langs: het **Dashboard**, het configuratiemenu (System/Config), **DNS-instellingen**, **Users/Gebruikersbeheer**, **Policies (Filterbeleid)**, **Categorieën & Whitelist**, logging/rapportage en geavanceerde opties om als laatste de testing en bugs te checken.

Afbeelding met tekst, schermopname, lijn, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.

4

## Overzicht van het filter dashboard

Na inloggen kom je op het **Dashboard**. Dit geeft in één oogomslag inzicht in de status van NXFilter en je netwerk:

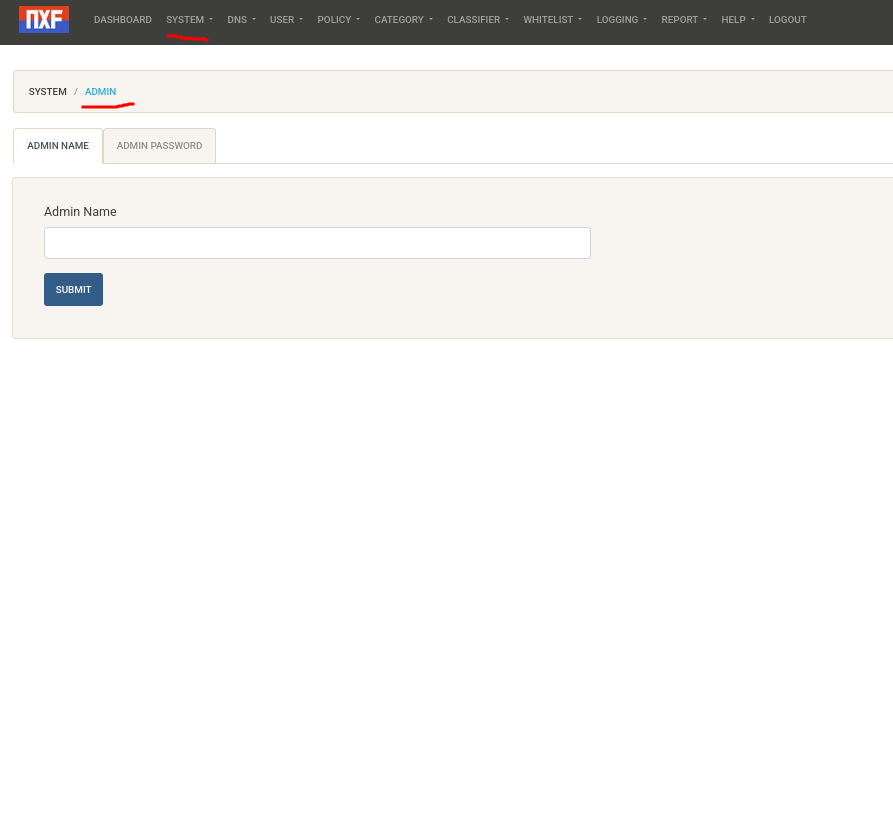
* Je ziet statistieken zoals het aantal DNS-verzoeken, hoeveel daarvan geblokkeerd zijn, en eventuele trends (grafieken over tijd). Zo kun je bijvoorbeeld zien op welke tijden veel verzoeken zijn en of er pieken in blokkades zijn.
* Statusinformatie: of de NXFilter-service actief is, hoeveel geheugen wordt gebruikt, enz.
* Overzicht van recente DNS-query’s en welke acties daarop zijn ondernomen (toegestaan of geblokkeerd). Zo kun je direct controleren of filtering werkt: als je bijvoorbeeld net een site probeerde te bezoeken die geblokkeerd is, zou je die hier moeten zien verschijnen als *blocked*.

## Basisinstellingen (config/system)

Alvorens we starten met de configuratie van **DNS, USERS,POLICy,...** gaan we eerst een paar basis-configuraties doen zoals;

### Admin

Username en wachtwoord wijzigen, zoals eerder al besproken. Verander ook de default username van de admin-user voor extra veiligheid.

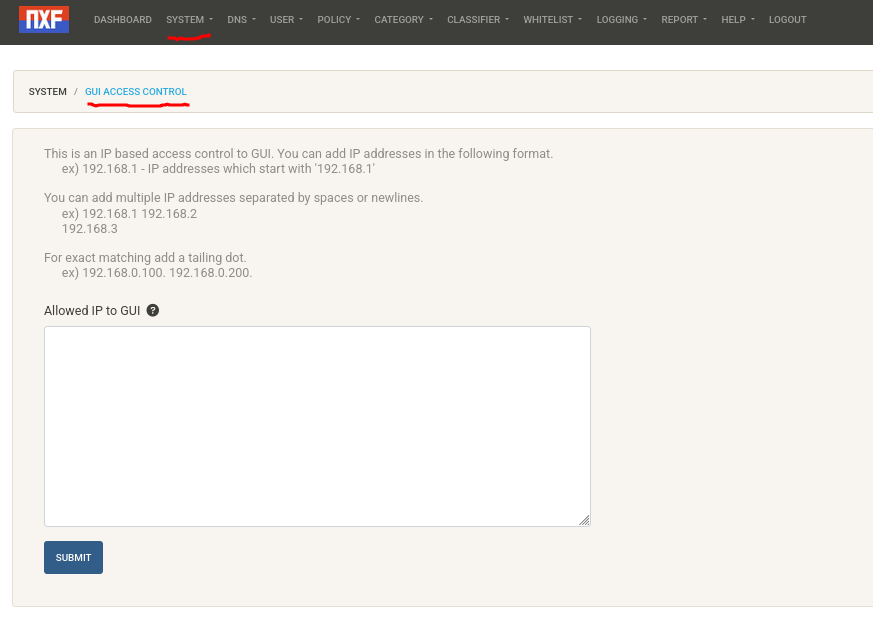


5

### Gui acces control:

Hier omschrijf je welke ip-adressen ‘wel’ toegang krijgen tot de nxfilter interface.

6



### Alert:

Instellen van mailing event en melding op basis van categories, zodat je op de hoogte gehouden word van ongewone activiteiten:

1. **Mailing:**

7

(Configuratie is afhankelijk van welke mailserver je gebruikt maar de meest voorkomende SMTP-ports zijn 25,587 en 465)

Afbeelding met tekst, schermopname, software, Besturingssysteem

Door AI gegenereerde inhoud is mogelijk onjuist.

1. **Events:**

8

Afbeelding met tekst, software, Webpagina, Computerpictogram

Door AI gegenereerde inhoud is mogelijk onjuist.

1. **Categories:**

Hier geef je aan van welke categories je melding wil krijgen. Bv; als werknemers surfen naar ongepaste website’s wil je daar graag een melding van aankrijgen.

9

Afbeelding met tekst, schermopname, software, Computerpictogram

Door AI gegenereerde inhoud is mogelijk onjuist.

1. **Block Page:**

Je kunt de instellingen van de blokkeringspagina aanpassen. Standaard zal NXFilter bij het blokkeren van een HTTP-verzoek de gebruiker doorsturen naar een eigen pagina met melding dat toegang geweigerd is. Je kunt hier een eigen bericht of logo toevoegen indien gewenst.

Meer hierover in deze link: <https://tutorial.nxfilter.org/gui-config.php>

1. **Backup:**

Mogelijkheid om configuratie te back-uppen of te herstellen. Het is aan te raden na uitgebreide configuratie een backup te maken, voor het geval je Pi crasht of een update mislukt.

10

Afbeelding met tekst, schermopname

Door AI gegenereerde inhoud is mogelijk onjuist.

## DNS configuratie

Controleer hier of de **Upstream DNS servers** correct staan. Standaard kan NXFilter de DNS-verzoeken die niet geblokkeerd worden doorsturen naar bijvoorbeeld 8.8.8.8 (Google DNS) of je provider DNS. Je kunt tot 3 upstream servers invullen. Als je iets wilt wijzigen (bijv. Cloudflare DNS 1.1.1.1 gebruiken), pas dat hier aan. Je kunt ook caching-opties instellen.

11

Afbeelding met tekst, schermopname, software, nummer

Door AI gegenereerde inhoud is mogelijk onjuist.

### DNS > setup

Geef als eerste dns-upstream je router dns in of het ip-address van nxfilter.

De DNS-query timeout laat je beter op default staan. Voor de caching is het afhankelijk wat het doel is:

* 1. **Persistent caching:**

Hier word dns-cach permanent opgeslagen, zelfs bij het herstarten. Dit heeft als voordeel dat de performance beter sneller is en minder belasting is op upstream dns-server.

Nadeel is dat het veel geheugen inneemt en moet hier rekening gehouden worden bij het assembleren.

* 1. **Negative caching:**

Dit houd ook niet gevonden domainnamen bij wat voorkomt dat query’s niet worden herhaald. Het verhoogt de performantie door de mislukte domainverzoeken “tijdelijk” te onthouden.

Nadeel is dat de negatieve querys ook tijdelijk geheugen mee in beslag nemen bovenop de permanente caching.

* 1. **Minimal responses:**

Hier word enkel de belangrijke records bijgehouden wat voor minder netwerkverkeer zorgt en de prestatie verhoogd. Nuttig voor beperkte bandbreedte en privacy gerichte zaken.

Nadeel is dat verzoeken telkens opnieuw gedaan worden en niet in de cach worden opgeslagen.

## Gebruikers beheren

NXFilter biedt de mogelijkheid om **gebruikersaccounts** en **groepen** aan te maken zodat je per gebruiker of groep afwijkende filterregels kunt toepassen. In een thuisnetwerk kun je hiermee bijvoorbeeld elk gezinslid een eigen profiel geven, en in een bedrijfsomgeving kun je afdelingen of rollen onderscheiden.

Onder **User** (Gebruikersbeheer) kun je nieuwe gebruikers toevoegen. Je hebt verschillende manieren om gebruikers te identificeren:

### Ip-gebaseerde gebruikers creëren

IP-gebaseerde gebruikers: Je kunt een gebruiker aan een vast IP-adres of IP-bereik koppelen. Zo kun je bijvoorbeeld zeggen dat alle verzoeken van 192.168.1.50 “User Jan” zijn. Dit is handig in een thuisnetwerk waar apparaten vaak een vast (of reservatie) IP krijgen. NXFilter zal dan DNS-verzoeken van dat IP toeschrijven aan die gebruiker​.

Om te weten welke ip-address bij welk device hoort in een dhcp-setup kan je nmap gebruiken om de actieve apparaten, besturingssystemen,… te weten te komen.

Afbeelding met schermopname, tekst, software, Computerpictogram

Door AI gegenereerde inhoud is mogelijk onjuist.

12

### Edit users

Na het creëren van de gebruiker ga je naar user > user > edit en klik je bij de gewenste gebruiker op het edit icoontje aan de rechter zijde.

Hier kan je de credentials van de gebruiker beheren.

De work-time en free-time policy laten we voorlopig op default staan. (Dit wordt later nog besproken en kan later aangepast worden)

13

Afbeelding met tekst, schermopname, software, Besturingssysteem

Door AI gegenereerde inhoud is mogelijk onjuist.

### Ip-address toekennen

Bij de pagina user > user > add ip kan je de ip van de gebruiker/toestel meegeven.

Je kan ook een range aan ip’s meegeven maar als dit niet het geval is vul je enkel het start ip in.

Afbeelding met tekst, software, schermopname

Door AI gegenereerde inhoud is mogelijk onjuist.

14

### Member off

Hier kan je aangeven tot welke groep de gebruiker behoord. Dit is meer van toepassing in bedrijven of grote gezinnen. Je maakt groepen met de gewenste rechten en policy’s en voegt de gebruikers aan de gewenste groep/groepen.

Het aanmaken van groepen word later nog besproken maar voorlopig laten we het op de default staan. (allowed\_users)

Afbeelding met schermopname, tekst, software, Computerpictogram

Door AI gegenereerde inhoud is mogelijk onjuist.

15

## Groepen beheren

De **sectie “Groepen”** in de NxFilter-GUI (onder **User > Group**) stelt je in staat om gebruikers te groeperen en daar groepsbeleid op toe te passen. Concreet kun je:

1. **Groepen aanmaken** en beheren, inclusief een omschrijving en prioriteit (Policy Points).
2. **Groepsbeleid**:

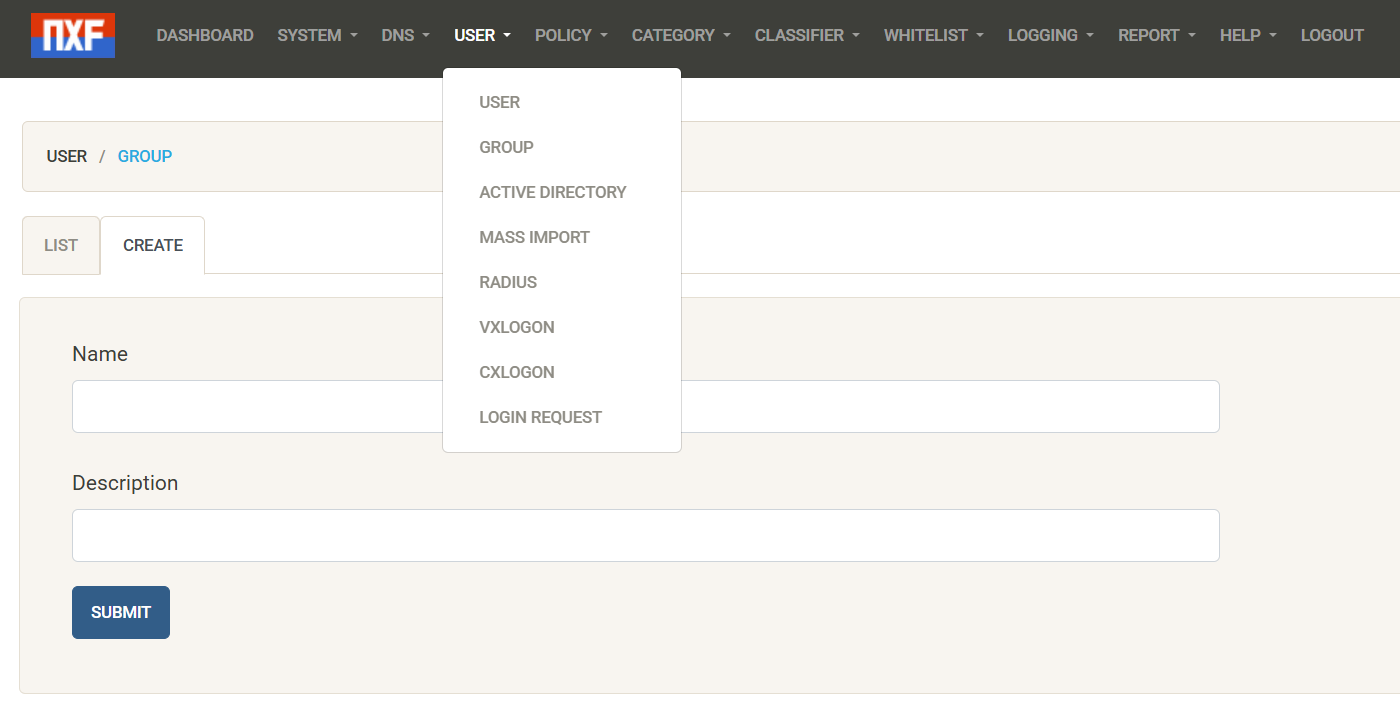
instellen: werk- en vrij-tijdbeleid (policies), schermtijd (“Screen Time”), datalimieten (“Data Cap”).

1. **Groepsspecifieke free-time:**

Definiëren, die wordt gecombineerd met de algemene free-time-instellingen onder **Policy > Free Time**.

1. **Leden toewijzen:**

Aan de groep, ofwel handmatig (via de GUI) of via import uit Active Directory.



16

### Groep aanmaken

De groep moet eerst aangemaakt worden voor we zaken kunnen specifiëren.

Dit kan je doen bij user > group > create zoals je kan zien i afbeelding 16.

Geef de groep een duidelijke naam. (Afdeling, gebied, kinderen,…)

Klik op ADD om te valideren.

### Groep editen

Bij het tab list kan je alle groepen terugvinden die gemaakt zijn. Standaard is er al een groep default maar wij gaan zelf groepen definiëren en gebruikers toevoegen aan de groepen met de juiste configuraties.

Ga naar user > group > list en klik op edit, je krijgt een nieuw tabblad te zien met

### Policy toewijzen

1. **Work-time Policy**:

Dit is enkel van toepassing in het bedrijfsleven zodat de werkgeven kan beheren tot welke resources de werktnemer toegang toe heeft.

Je kan dit in de privé ook gebruiken om aan te geven wat overdag toegelaten is gezien dat voor de privé gaan specificatie voorzien is.

1. **Free-time Policy**:

Hier kan je aangeven wat toegestaan is in de vrije tijd voor werknemers die een eigen apparaat word/werd toegewezen.

Voor de privé kan je dit toepassen om specificaties in te stellen in de avond/nacht.

1. **Screen Time** en **Data Cap**:

Optioneel, voor tijd- en datalimieten per groep.

1. **Group Specific Free Time**:

Stel hier extra vrije tijdstippen in.

1. **Priority (Policy Points)**:

Hoger getal heeft voorrang als een gebruiker in meerdere groepen zit.

# Externe filtering voor mobiele apparaten en thuiswerkers (NXProxy & DNS-over-HTTPS)

Het mooie van NXFilter is dat je het niet alleen binnen je LAN kunt gebruiken, maar ook roaming gebruikers kunt laten filteren. Denk aan kinderen met een smartphone buitenhuis, of werknemers die thuis of onderweg zijn op een laptop. NXFilter biedt twee hoofdopties om deze “externe” devices toch gebruik te laten maken van je DNS-filter:

1. **NXProxy:** een lichte client-applicatie die je installeert op Windows of Android, welke alle DNS-requests op dat apparaat versleuteld doorstuurt naar jouw NXFilter thuis.
2. **DNS over HTTPS (DoH):** je configureert het externe apparaat (of de browser daarop) om een DoH-endpoint te gebruiken dat door jouw NXFilter-server wordt aangeboden.

Beide methoden zorgen ervoor dat ook buiten het directe netwerk de DNS-aanvragen bij jouw NXFilter terechtkomen en gefilterd worden alsof ze lokaal zijn. We bespreken hieronder beide mogelijkheden.

## NXProxy – externe filteragent

NXProxy is een kleine client-applicatie van de makers van NXFilter. Je installeert deze op een externe pc of laptop die je wilt filtreren (er is een Windows-versie, en ook een variant voor Android). De NXProxy-app draait op de achtergrond, vangt DNS-verzoeken van het systeem op en stuurt ze versleuteld (over HTTPS) naar jouw NXFilter-server thuis. Het verkeer gaat dus over poort 443 in een HTTPS-tunnel, waardoor het lijkt op normaal webverkeer – handig, want dit werkt meestal overal zolang er internet is.

Om NXProxy te kunnen gebruiken moet je een paar stappen doorlopen:

1. **Poorten openen op de router:**

Zorg dat jouw thuisrouter inkomende verbindingen op poort **80/tcp** en **443/tcp** doorstuurt (port forward) naar de Raspberry Pi waarop NXFilter draait. NXProxy maakt namelijk via deze poorten verbinding. Poort 443 is essentieel (daar loopt de versleutelde DNS in ieder geval over); poort 80 is optioneel maar aanbevolen zodat ook de blockpagina’s en http-requests correct kunnen omgaan. Als je blockpagina’s extern niet nodig vindt, zou alleen 443 volstaan.

1. **DynDNS of vast IP:**

Omdat je thuis internet IP vaak dynamisch is, is het handig een **domeinnaam** te gebruiken die naar jouw huis verwijst. Bijvoorbeeld registreer een gratis DynDNS zoals *jouwnaam.dyndns.org*. Stel deze in op je router zodat hij bij IP-wijziging update. Dit domein gebruik je dan in NXProxy in plaats van een IP, wat robuuster is.

1. **NXProxy instellen:**

Download de NXProxy client van de NXFilter-website en installeer deze op de externe computer. Tijdens de installatie of eerste start zal hij vragen om een serveradres en een login-token. Vul hier je DynDNS of externe IP in (bijv. *mijnhuisfilter.dyndns.org*) en zorg dat de poort klopt (443). Het login-token haal je uit je NXFilter webinterface: onder *Policy > NxProxy* (of *User* settings) kun je per user een unieke code genereren. Je kunt bijvoorbeeld per kind/gebruiker een eigen NXFilter-account en token maken, zodat je in de logs kunt zien wie er via NXProxy binnenkomt. Voer dit token in op de NXProxy client.

1. **Verbinden en testen:**

Start NXProxy en kijk of hij verbinding maakt. In de NXFilter GUI kun je onder *Logging > Agent Signal* zien of NXProxy contact houdt. Als NXProxy actief is, zal de externe client zijn DNS nu via de tunnel sturen. Test door op die laptop een geblokkeerde site te bezoeken; als het goed is wordt deze geweigerd zoals thuis ook zou gebeuren. In de NXFilter logs zie je de verzoeken binnenkomen met de betreffende gebruikersnaam/token, zodat je weet van wie ze komen.

NXProxy heeft als voordeel dat de gebruiker er weinig van merkt: internet werkt normaal, de filtering gebeurt op de achtergrond. Zorg er uiteraard voor dat de thuis NXFilter altijd aan staat en dat je genoeg uploadbandbreedte hebt, anders hebben de roaming gebruikers geen DNS.

**Beveiliging:**

Omdat je nu je NXFilter openzet naar het internet, is het extra belangrijk om beveiligingsmaatregelen te nemen. Zet **altijd een sterk admin-wachtwoord**, en overweeg in de NXFilter config “Allowed IPs” voor de admin GUI te beperken tot bijvoorbeeld alleen jouw LAN en (eventueel) de IP-range van NXProxy (die kan variëren). Zo voorkom je dat onbekenden op de admin interface kunnen proberen in te loggen. NXProxy verkeer zelf is versleuteld en vereist het juiste token, dus dat is relatief veilig, maar houd de logs in de gaten voor ongeautoriseerde pogingen.

**Gebruik op Android:**

Er bestaat ook een NXProxy-versie voor Android, deze werkt iets anders (start een lokale VPN-service om DNS te onderscheppen, omdat Android apps niet direct DNS omleiden). Het principe blijft gelijk: het stuurt DNS naar je server. Voor iOS bestaat NXProxy niet; daarvoor zou je DoH (hierna) moeten gebruiken.

**Opmerking:**

Technisch gezien gebruikt NXProxy onder water *DNS over HTTPS* om met NXFilter te praten. Dit betekent dat als je NXProxy gebruikt, je op de client geen aparte DoH hoeft in te stellen – de NXProxy applicatie regelt alles. Het verkeer gaat via poort 443 en lijkt daarmee op gewoon HTTPS verkeer, wat het meestal ongehinderd door firewalls laat.

## DNS over HTTPS (DoH) voor roaming

Een alternatieve methode *zonder extra software* is om NXFilter zelf als een DNS-over-HTTPS server te gebruiken. Moderne apparaten en browsers ondersteunen aangepaste DoH-servers. Je kunt NXFilter zó configureren dat het op poort 443 HTTPS DNS-queries accepteert en verwerkt. Externe clients (browsers, telefoons) kun je dan instellen om die DoH-service te gebruiken voor DNS.

Stappen om DoH op NXFilter in te richten:

1. **Domeinnaam & certificaat:**

Net als bij NXProxy heb je een extern bereikbare domeinnaam nodig (bijv. dns.mijndomein.nl die naar je thuis-IP wijst). Daarnaast heb je een geldig SSL/TLS certificaat nodig voor dat domein, want browsers eisen een vertrouwd certificaat voor DoH. Dit kun je gratis regelen via Let’s Encrypt. Installeer het verkregen certificaat in NXFilter: dit doe je door de certificaatbestanden (.crt en .key) te plaatsen en in conf/cfg.properties naar te verwijzen, of via een NXFilter optie indien beschikbaar. (Raadpleeg de NXFilter documentatie *“How do I apply my own SSL certificate?”* voor details.)

1. **NXFilter DoH activeren:**

Controleer in de NXFilter configuratie of DoH functionaliteit ingeschakeld kan worden. Mogelijk is dit automatisch actief zodra je NXFilter met SSL op 443 draait. Zorg er in ieder geval voor dat poort 443 op de router doorgestuurd is naar NXFilter (dit hadden we bij NXProxy al gedaan).

1. **Login Token voor gebruikers:**

Net als bij NXProxy zal NXFilter voor DoH-clients gebruikers moeten herkennen aan de hand van een token. Ga in de NXFilter GUI naar een gebruiker en genereer een **Login Token** (of gebruik dezelfde als bij NXProxy user). Dit is een unieke code per gebruiker. Noteer deze code.

1. **Client configuratie – Browser:**

In bijvoorbeeld Chrome of Edge ga je naar Instellingen > Privacy > Beveiliging > Beveiligde DNS. Kies “Aangepaste” provider en vul de URL in naar jouw DoH-service. Dit heeft meestal het formaat https://dns.mijndomein.nl/dns-query?token=<LoginToken>. Dus je domein gevolgd door dns-query pad en de token parameter. Bij Firefox vind je een soortgelijke optie onder Instellingen > Algemeen > Netwerkinstellingen > DNS over HTTPS (Custom). Vul daar je URL in. Vanaf dat moment zal die browser DNS over HTTPS sturen naar jouw NXFilter. Je kunt dit testen op Cloudflare’s testpagina (1.1.1.1/help) welke laat zien of DoH actief is, maar beter is gewoon een geblokkeerde site proberen om te zien of het filtert.

1. **Client configuratie – iOS/macOS:**

Apple biedt vanaf iOS 14 / macOS 11 een manier om op systeemniveau DoH in te stellen via een *configuration profile*. Gelukkig heeft NXFilter hiervoor iets handigs: ga in de NXFilter GUI naar *System > Mobile Config*. Je kunt daar een profiel (.mobileconfig) genereren voor een gebruiker en je domein. Stuur dat profiel naar de iPhone/Mac (bv. via mail of webdownload) en installeer het. Dit zal op het device een DNS-over-HTTPS server configureren (jouw NXFilter) als systeem-DNS. De telefoon gebruikt dan altijd jouw DNS (zolang er internet is).

1. **Client configuratie – Android:**

Android (vanaf 9) ondersteunt DNS over TLS op systeemniveau, maar DoH nog niet in de standaardinstellingen. DNS-over-TLS gebruikt poort 853 en is een optie, maar veel openbare wifi’s laten dat niet toe en het vereist ook certificaatwerk. Simpeler: gebruik een browser die DoH ondersteunt (bv. Firefox met jouw DoH server ingesteld, of Chrome als je via command line flags een custom provider toevoegt). Er bestaan ook apps die DoH kunnen forceren per verbinding. Totdat Android native DoH toevoegt, is NXProxy op Android eigenlijk makkelijker voor full-device filtering.

### Beheer en beveiliging bij DoH:

Net als bij NXProxy geldt dat je NXFilter nu open hebt staan op internet. Neem de eerdergenoemde beveiligingsmaatregelen in acht (sterke wachtwoorden, Allowed IPs beperken, admin interface eventueel op andere poort zetten of geheel dicht van buiten). NXFilter heeft de optie om bij DoH het verschil tussen gewone webinterface en DNS API te scheiden – een idee is om de admin GUI te verplaatsen naar bv. poort 8443 en 8080, en 443 uitsluitend te gebruiken voor DoH/NXProxy verkeer. Zo hoef je 80 niet eens open te zetten extern. Hoe dan ook, zorg dat alleen jij van buiten bij de admin kan als dat nodig is.

**Voordeel van DoH:** Het grote voordeel is dat je geen speciale software nodig hebt op de client (behalve eenmalig instellen). Het werkt ook voor apparaten waar je niets kunt installeren (bijv. een schoollaptop waarop je geen admin rechten hebt, maar waarop je wel een eigen Firefox kunt draaien voor internet met filter). Nadelen zijn de iets ingewikkelder setup (domein + certificaten) en het feit dat het per applicatie ingesteld moet worden (tenzij op iOS/macOS met profiel). NXProxy is daarentegen één install die heel het systeem pakt.

Veel gebruikers combineren deze methoden: bijvoorbeeld NXProxy voor Windows laptops en DoH-profielen voor iPhones. Het resultaat is in beide gevallen een consistent filter, ongeacht waar de gebruiker is – iets wat simpelere oplossingen als Pi-hole niet bieden (Pi-hole werkt immers normaal alleen binnen je LAAfbeelding met tekst, lijn, schermopname, diagram

Door AI gegenereerde inhoud is mogelijk onjuist.

Schematisch overzicht van externe filtering. Een remote laptop met NXProxy of een telefoon met DoH-client maakt via het internet verbinding met jouw thuisnetwerk. Inkomende HTTPS-verzoeken op je router op poort 443 worden doorgestuurd naar NXFilter op de Raspberry Pi 5 (blauwe pijlen). NXFilter verwerkt de DNS-vraag en gebruikt eventueel zelf ook upstream DNS-servers op internet (stippellijn) voor resolutie. Voor de externe client lijkt het alsof ze een gewone veilige DNS-server gebruiken, terwijl op de achtergrond jouw thuisfilter de toegestane en geblokkeerde domeinen bepaalt.

# Troubleshooting – Veelvoorkomende problemen oplossen

Zelfs na een goede installatie kun je tegen wat hobbels aanlopen. Hier behandelen we enkele veelvoorkomende problemen en hun oplossingen:

## “NXFilter lijkt niet te werken – DNS valt uit”:

Als geen enkele site meer laadt bij clients en je vermoedt dat NXFilter de oorzaak is, controleer eerst of de NXFilter service draait. Voer op de Pi sudo systemctl status nxfilter uit. Als de service gestopt is of errors geeft, bekijk de log (/opt/nxfilter/log/nxfilter.log). Een veelvoorkomend probleem is een *port collision* – bijvoorbeeld er draaide al een andere DNS-service (zoals systemd-resolved op Ubuntu) waardoor NXFilter niet kon binden op poort 53file-kjajipkw7dpfxkwqzjnsh4. De log zal iets aangeven als “Address already in use”. Los dit op door de andere service uit te schakelen (voor systemd-resolved: sudo systemctl disable --now systemd-resolved en verwijder eventueel symlink /etc/resolv.conf naar stub) en start NXFilter opnieuw. Bij webinterface poortconflict geldt hetzelfde principe (zie 3.3.3).

## “Ik kan niet in de webinterface komen”:

Je surft naar http://<pi-ip>/admin maar krijgt geen verbinding. Controleer eerst of NXFilter wel luistert op poort 80. Vanaf een andere machine kun je telnet <pi-ip> 80 proberen – als er geen connectie tot stand komt, blokkeert wellicht de firewall of NXFilter is niet goed gestart op de webserver.

Het zou er als volgt uit moeten zien:

Afbeelding met tekst, schermopname, Lettertype

Door AI gegenereerde inhoud is mogelijk onjuist.

Check UFW instellingen (zie 4.1) en NXFilter logs. Als poort 80 wel luistert maar de browser niets toont, kijk of je de juiste URL gebruikt: sommige NXFilter versies vereisen expliciet http://<ip>:80/admin.jsp.

Probeer dat indien /admin niets doet. Een andere mogelijkheid is dat je in NXFilter “Allowed IP” hebt aangepast en jouw PC daar nu buiten valt – in dat geval weigert NXFilter de GUI-verbinding. Oplossing: pas *Allowed IP* aan via de config file (cfg.properties) of vanaf een toegestane.

Afbeelding met tekst, schermopname, Lettertype, wit

Door AI gegenereerde inhoud is mogelijk onjuist.

## “Clients gebruiken NXFilter niet (filter gaat voorbij)”:

Je merkt dat sommige apparaten nog steeds naar geblokkeerde sites kunnen. Controleer op zo’n client welke DNS-server ze gebruiken. Voer nslookup example.com in de terminal uit (of gebruik ipconfig /all op Windows om DNS te zien). Als de server niet het Pi-IP is, dan gebruikt die client mogelijk nog oude DHCP info of heeft statisch een andere DNS ingesteld. Oplossing: laat het apparaat het IP lease vernieuwen (netwerkverbinding opnieuw opzetten of DHCP release/renew). Als een gebruiker stiekem een statische DNS had ingevoerd, zet dat terug op automatisch. Als laatste redmiddel kun je op de router een firewallregel instellen die alle DNS-verkeer van clients naar NXFilter dwingt (zoals besproken bij *Voorkomen van omzeiling*). Dit garandeert dat zelfs verkeerde DNS-instellingen uiteindelijk bij NXFilter uitkomen.

## “Sommige geblokkeerde sites laden toch door”:

Je hebt bijvoorbeeld categorie “Adult” geblokkeerd, maar een testwebsite in die categorie laadt nog. Mogelijke oorzaken en remedies:

* + *Caching:* Het domein kan nog in de DNS-cache van de client staan van vóórdat je het blokkeerde. Dan wordt geen nieuwe DNS-vraag gesteld en ziet de browser dus gewoon de site. Oplossing: leeg de DNS-cache op de client (op Windows ipconfig /flushdns, op macOS sudo killall -HUP mDNSResponder, of herstart de browser/computer)file-kjajipkw7dpfxkwqzjnsh4. Vraag daarna de site opnieuw op. NXFilter zelf cachet ook DNS-resultaten. Dus als je net een domein hebt geblokkeerd dat kort daarvoor nog toegestaan was, kan NXFilter zijn eerdere positieve antwoord nog even vasthouden. In de NXFilter GUI kun je onder *Config > DNS* op “Clear Cache” klikken om zijn cache te legen.

In cfg.properties kun je ook de TTL verkorten, maar meestal is dat niet nodig – wacht een minuut of twee en probeer opnieuw, dan zal NXFilter de nieuwe regel toepassen.

* + *DoH bypass:* Controleer of de browser soms DNS-over-HTTPS aan heeft staan richting een externe dienst (zie 6.2 hierboven). Als dat zo is, zal NXFilter überhaupt die verzoeken niet zien en dus niet blokkerenfile-kjajipkw7dpfxkwqzjnsh4. Dit herken je als geblokkeerde sites enkel in bepaalde browsers doorkomen. Oplossing: schakel Secure DNS uit in de browserinstellingen of configureer het naar je eigen NXFilter DoH. Eventueel kun je de bekende DoH-domeinen blokken via NXFilter zodat die optie niet werkt. Na aanpassing, test opnieuw of de site nu geblokkeerd wordt.
  + *NXFilter policy volgorde:* In complexere setups, check of het betreffende device wel onder de juiste policy valt. Misschien test je met een apparaat dat per ongeluk op de *Default* policy zit die weinig blokkeert. Log in de NXFilter GUI en kijk onder *User* of het IP/gebruikersaccount van de testclient de juiste policy heeft. Zo niet, pas aan en probeer opnieuw.

## “NXFilter wordt heel traag of valt uit bij veel verkeer”:

Voor thuisgebruik is een Raspberry Pi 5 ruim voldoende krachtig om DNS te handelen (honderden queries per seconde). Als je toch performance-issues ervaart (bijv. websites laden traag, video hapert vanwege DNS, of NXFilter service crasht regelmatig), kijk dan naar:

* + CPU/RAM gebruik op de Pi: htop of top draaien om te zien of NXFilter (java proces) 100% CPU pakt of out-of-memory gaat. Dit is onwaarschijnlijk tenzij er een bug of extreem veel verkeer is.
  + SD-kaart IO: intensief loggen kan de IO vertragen. Overweeg overstap naar SSD of minderen met loggen.
  + Versie problemen: Controleer of je de nieuwste NXFilter versie draait; misschien is er een bug gefixt in een update. Upgrade zonodig (maak wel backup van config).
  + In extreme gevallen met >100 gebruikers zou je aan NXFilter’s eigen clustering kunnen denken, maar dat gaat het thuisgebruik meestal te buiten.

Kortom, kijk eerst of het probleem in de DNS-configuratie zit (clients bereiken NXFilter niet of bypassen deze), of in NXFilter zelf (service gerelateerd). Door systematisch te testen en logs te raadplegen kun je 90% van de problemen oplossen. NXFilter is, eenmaal goed ingesteld, vrij onderhoudsarm. Maar mocht iets haperen, is de log je beste vriend om te zien *waarom* een site niet of wel doorgelaten wordt.

# Testen en validatie

Nadat je NXFilter hebt ingericht, is het verstandig om verschillende testscenario’s door te lopen om te valideren dat alle policies en instellingen werken zoals bedoeld. Enkele praktische tests:

## Categorieblokkade testen:

Kies een categorie die je geblokkeerd hebt (bijv. “Adult” of “Gokken”). Probeer een bekende site in die categorie te bezoeken (we noemen hier geen expliciete namen, maar bv. een populaire goksite). Je zou moeten zien dat de site niet laadt. Controleer in NXFilter’s *Logs* dat er een entry verschijnt die aangeeft dat het domein geblokkeerd is onder die categorie, voor de juiste gebruiker/policy. Test ook een site uit een categorie die **niet** geblokkeerd is om zeker te zijn dat normaal internetverkeer gewoon doorgelaten wordt.

Afbeelding met tekst, schermopname, Perceel, lijn

Door AI gegenereerde inhoud is mogelijk onjuist.

## SafeSearch test:

Zoals eerder beschreven, ga naar google.com of bing.com en kijk of SafeSearch aan staat (meestal staat er een indicator op de pagina als dit het geval is). Voer een aantal zoekopdrachten uit, zowel braaf als een paar woorden die expliciete content zouden kunnen opleveren. Ideaal gezien blijven schokkende resultaten uit. Op YouTube kun je kijken of Restricted Mode geforceerd is door naar beneden te scrollen. Als SafeSearch niet blijkt te werken, kijk na of je het in de juiste policy aangezet hebt en of de client onder die policy valt.

## Schermtijd test:

Als je de *Screen Time* functie gebruikt, kun je deze werking simuleren. Zet bijvoorbeeld tijdelijk de limiet erg laag (5 of 10 minuten) voor een bepaalde gebruiker en categorie (zeg YouTube onder “Streaming Media” categorie). Laat de gebruiker dan een YouTube-video kijken of voortdurend pagina’s laden in die categorie gedurende iets langer dan de ingestelde tijd. NXFilter zou na ~5 min moeten stoppen met het resolven van nieuwe DNS-requests voor die site(s) – de video stopt met nieuwe content laden of de pagina’s geven fouten. In de NXFilter log zul je bij verdere verzoeken iets van “Blocked (Screen Time)” zien. Zet daarna de limiet weer normaal. Dit bevestigt dat de schermtijd-functie werkt.

## Whitelist/Blacklist test:

Probeer de override-lijsten. Voeg een willekeurig domein toe aan de *Blacklist* (direct geblokkeerd), bijvoorbeeld example.com. Bezoek dat domein in de browser – het zou nu geblokkeerd moeten worden ongeacht categorie. Haal het weer van de blacklist af en zie dat de site weer toegankelijk is. Voor whitelist: blokkeer bijvoorbeeld tijdelijk de categorie “News”, voeg nu.nl toe aan de *Whitelist*, en bezoek nu.nl – die zou moeten laden terwijl andere nieuwssites (NOS bijvoorbeeld) geblokkeerd blijven. Zo check je dat de whitelist prioriteit heeft.

## Multi-user policy test:

Als je meerdere gebruikers of groepen hebt aangemaakt, test of ze de juiste policy krijgen. Bijvoorbeeld, stel op twee verschillende apparaten twee verschillende gebruikers in (of gebruik IP-based identificatie met twee verschillende IP’s). Geef de ene een strikte policy en de ander een mildere. Bezoek op beide apparaten eenzelfde site die voor de ene eigenlijk geblokkeerd moet zijn en voor de ander toegestaan. Check of dat in de praktijk ook gebeurt. Dit verifieert dat je gebruikersmapping en policyprioriteiten juist zijn ingesteld.

## Externe filtering test:

Indien je NXProxy of DoH hebt opgezet, test dat ook. Zet een laptop via een telefoon-hotspot online (dus buiten je LAN). Activeer NXProxy op die laptop of zorg dat de browser DoH naar jouw server gebruikt. Bezoek een site die je normaliter blokkeert. Als het goed is, wordt deze ook nu geblokkeerd. In de NXFilter logs zou je het verzoek moeten zien, meestal gelabeld met de betreffende externe gebruiker of token. Zo ben je zeker dat je filter ook extern functioneert.

## Performance test:

Dit is optioneel, maar je kunt eens meten of NXFilter de DNS-snelheid niet noemenswaardig negatief beïnvloedt. Gebruik bijvoorbeeld het programma dig om een reeks queries te doen en kijk naar de Query time. Of gebruik een DNS benchmark tool. Een Raspberry Pi 5 zou resultaten van <20ms moeten geven voor onbekende domains (inclusief upstream tijd), en slechts 1-2ms voor gecachte resultaten. Als je merkt dat DNS-query’s structureel lang duren (bijv. 300+ ms), onderzoek dan of je upstream DNS misschien traag is of er netwerkvertraging zit.

Voor elk testscenario is het aan te raden de resultaten in de gaten te houden via het NXFilter Dashboard of de Logging-pagina. Pas als alles naar verwachting werkt, kun je erop vertrouwen dat NXFilter op de achtergrond zijn werk goed blijft doen.

Mocht een test mislukken, gebruik dan de Troubleshooting tips uit hoofdstuk 8 om gericht te zoeken. Vaak zijn het kleine configuratie-dingetjes zoals een IP in de verkeerde group, of caching.

Tot slot, informeer – indien van toepassing – je gebruikers over het feit dat er een filter actief is. In een thuissituatie vertel je je kinderen bijvoorbeeld welke regels gelden (“na 22u werkt internet niet meer”, “porno en gokken hebben we geblokkeerd”). In een kantooromgeving kun je medewerkers laten weten dat bepaalde categorieën geblokkeerd zijn voor productiviteit of veiligheid, zodat men niet vergeefs blijft proberen of zich afvraagt waarom iets niet werkt. Open communicatie kan frustratie voorkomen en gebruikersalertheid verhogen.

# Best practices en onderhoudstips

Gefeliciteerd, je NXFilter omgeving draait! Om het in de toekomst soepel en veilig te laten blijven lopen, volgen hier nog enkele best practices en onderhoudstips.

## Wachtwoordbeheer:

Verander het default *admin/admin* wachtwoord meteen en hou het veilig. Gebruik een sterk wachtwoord en wijzig het periodiek. Deel het admin-wachtwoord alleen met vertrouwde personen die het beheer uitvoeren.

## Regelmatige updates:

Houd de NXFilter-software up-to-date. Check af en toe op de NXFilter website of het forum of er nieuwe releases of beveiligingsupdates zijn. Updaten gaat meestal door de nieuwe versie over de oude heen te installeren (configs blijven bewaard). Maak **vooraf een backup** van je configuratie (hele conf/ map en eventueel de db/ map met de H2 database) voordat je upgrade. Zo kun je altijd terug als er iets misgaat.

## Categorie lijst onderhoud (Jahaslist):

NXFilter gebruikt standaard de Jahaslist categoriedatabase. Voor thuisgebruik is dit gratis en wordt deze lijst periodiek automatisch bijgewerkt. Kijk in de GUI onder *Classifier > Jahaslist* of updates binnenkomen en hoeveel domeinen er gecategoriseerd zijn. Als de lijst veroudert (weinig entries, of last update is lang geleden), controleer je internettoegang van de Pi of licentie. Grote omgevingen vereisen een licentie voor Jahaslist, maar thuis normaal niet.

## Back-ups van configuratie:

Naast de interne backup-optie (waarmee je config kunt exporteren), is het slim zelf periodiek een backup te maken van de NXFilter-config. Kopieer de map /opt/nxfilter/conf en bewaar die ergens veilig. Noteer ook je licentie of Jahaslist key indien van toepassing. Zo kun je bij een crash of SD-kaart corruptie snel weer opzetten op een nieuwe kaart of Pi.

## Monitoring van logs:

Check regelmatig de NXFilter logs, met name op security-gericht verkeer. Als je ziet dat NXFilter frequent

## Monitoring & alerts:

Houd de logs en met name beveiligings-gerelateerde blokkades in de gaten. Als NXFilter frequent malware- of phishing-domeinen blokkeert, kan dat wijzen op een geïnfecteerd device in je netwerk dat naar die domeinen probeert te *phone-home*’en. Je moet dan actie ondernemen op dat apparaat (malwarescan, isoleren). In die zin kan NXFilter dienen als een soort IDS (Intrusion Detection System) door je attent te maken op verdachte DNS-activiteite】. NXFilter heeft ook een optie om alerts te configureren (bijv. een e-mail bij bepaalde blok-events); als je dit nuttig vindt, stel het dan in onder *Config > Alerts*.

## Performance & hardware onderhoud:

Een Raspberry Pi 5 is krachtig genoeg voor thuisgebruik en kleine bedrijven. Let wel op de temperatuur en stabiliteit, vooral als de Pi in een kastje 24/7 aan staat. Gebruik een behuizing met voldoende ventilatie of een koellichaam/fan indien nodi】. NXFilter schrijft logs intensief weg; overweeg een hoogwaardige SD-kaart of beter nog een kleine SSD als opslag om de levensduur te verlengen. Het is ook raadzaam om periodiek een image-backup van de SD-kaart te maken (of de belangrijkste config- en logbestanden veilig te stellen), zodat je bij een crash snel een nieuwe kaart kunt inzette】.

## Beveiliging van de Pi:

Hoewel NXFilter zelf de DNS beveiligt, moet de onderliggende server (de Raspberry Pi) ook veilig blijven. Houd het OS up-to-date (sudo apt upgrade regelmatig uitvoeren). Schakel ongebruikte diensten uit. Beperk eventuele SSH-toegang tot alleen vertrouwde IP-adressen (bijv. via UFW firewallregels). Bedenk dat NXFilter poorten 53, 80, 443 gebruikt – draai geen andere services op deze poorten om conflicten te voorkome】. Mocht je de Pi voor meerdere doeleinden gebruiken, overweeg NXFilter op een aparte poort te zetten of, beter nog, dedicateer de Pi aan NXFilter zodat niets anders in de weg zit.

## Policy onderhoud:

Naarmate de tijd verstrijkt, herzie je de ingestelde policies. Kinderen worden ouder en misschien mag hun profiel wat meer toegang; of wellicht duiken nieuwe categorieën/websites op die je wilt blokkeren. NXFilter maakt het eenvoudig om aanpassingen te doen, maar doe dit bewust en communiceer waar nodig met de gebruikers. Het kan nuttig zijn om bij te houden welke extra domains je handmatig hebt ge-whitelist of -blacklist en waarom – zo onthoud je later waarom een bepaalde uitzondering ingesteld was.

## Gastnetwerk scheiding:

Als je NXFilter ook toepast op een gastnetwerk, zorg dan dat gasten geen toegang hebben tot de NXFilter beheerpagina. Gebruik bijvoorbeeld de *Allowed IPs* instelling om alleen het hoofdnetwerk toegang te geven tot de admin GUI, of houd het gasten-netwerk volledig gescheiden van het LAN waar NXFilter in zit. Je wilt niet dat een willekeurige gast probeert in te loggen of de filtering te omzeilen.

## Test na wijzigingen:

Voer na elke grote wijziging (bijvoorbeeld een NXFilter software-update, of het invoeren van nieuwe blokkades) weer even de belangrijkste tests uit (zie hoofdstuk 9) om te verifiëren dat alles nog functioneert. Zo ontdek je meteen als iets per ongeluk misgaat, in plaats van pas na klachten van gebruikers.

Met deze richtlijnen zorg je ervoor dat je NXFilter-installatie soepel blijft draaien en effectief blijft in het beschermen van je netwerk. Veel succes met het implementeren van DNS-filtering in jouw omgeving!

Nawoord

Het voltooien van dit NXFilter-project was zowel leerzaam als uitdagend. In dit nawoord wil ik kort reflecteren op het proces, mijn persoonlijke ervaringen en de conclusies die ik trek uit het project.

**Proces en leerervaring:**

Tijdens het opzetten en documenteren van NXFilter heb ik diepgaand inzicht gekregen in DNS-gebaseerde filtering. Ik begon met het besef hoe essentieel webfiltering is voor netwerkbeveiliging, en NXFilter bood mij een praktijkgerichte manier om dit toe te passen.

Stap voor stap heb ik geleerd een Linux-systeem (Raspberry Pi) te configureren, software te installeren, en policies vorm te geven die aan echte behoeften voldoen (zoals ouderlijk toezicht in een thuisnetwerk of beveiligingsfilters in een bedrijfsomgeving). Het schrijven van dit document dwong mij om elk aspect goed te doorgronden – van infrastructuurdesign tot troubleshootingscenario’s – zodat ik het duidelijk kon uitleggen. Hierdoor heb ik niet alleen technisch inzicht vergaard, maar ook geleerd om complexiteit te vertalen naar begrijpbare instructies en tips.

**Technische nauwkeurigheid en verbeteringen:**

Tijdens het herwerken van de originele tekst heb ik veel kleine verbeteringen kunnen doorvoeren: grammatica is aangescherpt, de structuur is logischer ingedeeld en waar nodig heb ik extra toelichting gegeven op technische stappen (zoals waarom je bepaalde poorten opent of hoe je certificaten installeert voor DoH). Ook heb ik gemerkt dat sommige Engelstalige termen het best onvertaald blijven of als begrip uitgelegd moeten worden (bijvoorbeeld Persistent Caching heb ik benoemd en toegelicht). Screenshots en diagrammen toevoegen vond ik belangrijk om de tekst te ondersteunen – een beeld zegt immers meer dan duizend woorden, vooral bij netwerkstructuren. De eenvoudige schema’s van de thuisnetwerkopstelling en externe filtering maken hopelijk in één oogopslag duidelijk hoe NXFilter in die context werkt.

**NXFilter in perspectief:**

NXFilter blijkt een zeer veelzijdig stuk software te zijn. In vergelijk tot populairdere tools zoals Pi-hole (bekend voor advertentiefiltering) heeft NXFilter een wat hogere instapdrempel, maar ook véél meer mogelijkheden op het gebied van gebruikersbeheer en beleidsregels. Dit project heeft me doen inzien dat voor omgevingen waar je onderscheid per gebruiker wilt maken, NXFilter eigenlijk onmisbaar is – iets dat Pi-hole niet kan zonder meer. Tegelijk vergt NXFilter actief beheer: je moet blijven opletten op updates, categorielijsten, en trends in het internetverkeer. Een DNS-filter is geen “set-and-forget” als je het optimaal wilt benutten.

Conclusies en persoonlijke reflectie: Ik sluit dit project af met de conclusie dat DNS-based filtering een effectieve en relatief efficiënte manier is om een extra laag beveiliging en controle aan een netwerk toe te voegen. NXFilter, specifiek, heeft zich bewezen als een betrouwbaar systeem tijdens mijn tests. Het is lichtgewicht genoeg om op een Raspberry Pi te draaien zonder noemenswaardige latency toe te voegen, en krachtig genoeg om zelfs in semi-professionele omgevingen in te zetten.

Persoonlijk heb ik door dit project mijn vaardigheden aangescherpt in systeembeheer (Linux en netwerken) en begrijp ik de samenhang tussen theorie en praktijk beter: het is één ding om te weten wat DNS-filtering doet, maar een ander om het werkelijk te implementeren en af te stemmen op gebruikersbehoeften. Ik heb ook geleerd hoe belangrijk documentatie is – zowel voor mezelf als naslagwerk, als voor anderen die dit wellicht volgen.

**Dankwoord:**

Ten slotte ben ik dankbaar voor de bronnen en community (NXFilter forums, tutorials, etc.) die hebben bijgedragen aan de kennis in dit document. De steun en informatie uit de community tonen aan dat open-source projecten als NXFilter leven door samenwerking en kennisdeling. Hopelijk draagt dit “magnum opus” op zijn beurt bij aan die kennisdeling, en helpt het anderen om NXFilter met vertrouwen te implementeren.

Conclusie: NXFilter is een robust en flexibel DNS-filter dat, mits goed geconfigureerd en onderhouden, zowel thuisnetwerken als professionele netwerken aanzienlijk veiliger en beheerbaarder kan maken. Dit project heeft laten zien hoe je stap voor stap zo’n systeem opzet en optimaliseert. Ik kijk met tevredenheid terug op wat er bereikt is en heb vertrouwen dat de opgedane kennis in de toekomst van pas zal komen bij nieuwe uitdagingen in cybersecurity en netwerkbeheer.

Bronvermelding

NXFiltering tutorial, <https://tutorial.nxfilter.org/a-before-installing.php?utm_source=chatgpt.com/>

Officiële guide website voor het voorafgaande installatieproces.

NXFiltering tutorial, <https://tutorial.nxfilter.org/>

Officiële guide website met de NXFiltering instructies.

Chatgpt, Opzet van DNS-Server op raspberrypi

Nxfilter installatie, <https://efcomputer.net.au/blog/3-steps-to-install-nxfilter-on-raspberry-pi/#:~:text=Step%201.%20Download%20the%20pre>

Stappen voor het installerenn van nxfilter op een raspberry pi 5.

Versie-beheer van nxfilter, <https://www.cvedetails.com/version-list/32403/155192/5/Nxfilter-Nxfilter.html?sha=db3d0984e7f5b893e5db920c6fd9e657922ce049&order=1&trc=260>

Dns en proxy en community input:

* + - <https://www.reddit.com/r/nxfilter/comments/x3w7v6/questions_about_nxfilter_and_nxproxy/#:~:text=Questions%20about%20NxFilter%20and%20NxProxy,ports%2080%20and%20443>
    - <https://www.reddit.com/r/nxfilter/comments/k8fhdq/active_safe_search/#:~:text=Active%20Safe%20Search%20%3A%20r%2Fnxfilter,propagate%20the%20same%20code>
    - <https://www.reddit.com/r/nxfilter/comments/x3w7v6/questions_about_nxfilter_and_nxproxy/#:~:text=The%20document%20states%20that%20NxProxy,ports%2080%20and%20443>

Authenticatie en doorvoer, <https://www.admin-magazine.com/Articles/DNS-filtering-with-authentication/(offset)/6#:~:text=The%20news%20gets%20better%3A%20Experience,Figure>

Youtube basic-tutorial nxfilter, <https://www.youtube.com/watch?v=l4mOFRQZoOU>