



GETTING STARTED

A Guide to your MSP Environment Setup



This slide deck will provide you with set up links and instructions in alignment with those shared in the MSP onboarding webinar, to include:

Part 1

Set up instructions

Part 2

Use case specific guidance

Part 3

DNS circumvention prevention

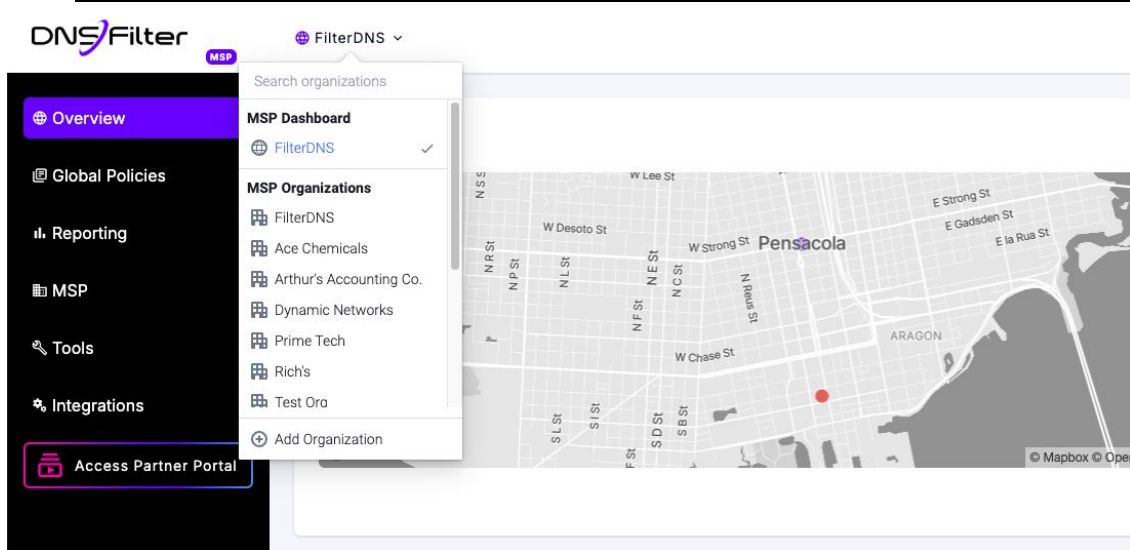
RESOURCE LINKS IN THIS DECK ARE [UNDERLINED](#)

NAVIGATING MULTI-TENANCY

Key benefits to multi-tenancy

- Separate client networks under a [singular dashboard](#)
- Assign [filtering Policies](#) and review reporting per client
- Easily toggle between client organizations to streamline management
- *Optional* Allow your clients [visibility into their own environments](#)

💡 **NEVER** add client users from the MSP Dashboard, this will give them privileges to your parent environment rather than their own client environment



GLOBAL POLICIES ALLOW YOUR TEAM TO

ESTABLISH GLOBAL AND
INDIVIDUAL BLOCK PAGES

MANAGE BROADSCALE FILTERING WITH
ASSIGNMENT ACROSS MULTIPLE CLIENTS

COORDINATE UNIVERSAL ALLOW
AND BLOCK LISTS FOR CONVENIENT
EXCLUSIONS



Simplest way to begin any new sub-org and then work through any one-offs

SETUP YOUR SITE

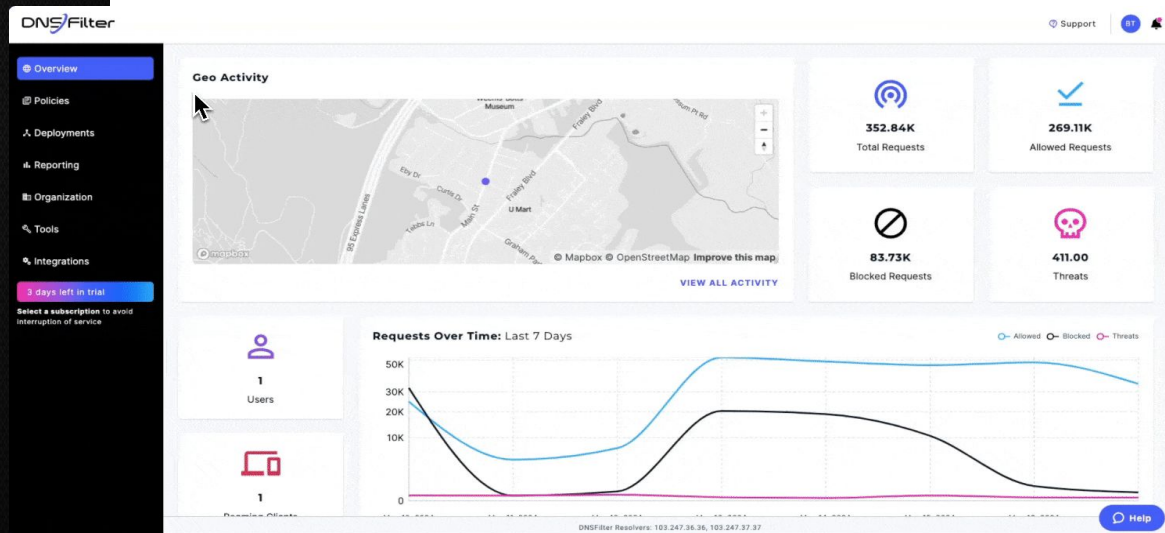
Different Network address abilities include:

- [NAT IPs](#) (LAN subnet policy assignment)
- [Dynamic hostnames](#)
- IP subnets up to /24

DNSFilter does not serve requests to unknown IP addresses



A site must be added to recognize and respond to network queries



DEPLOYMENT OPTIONS

Select any individual or combination of the three options available

Network

Aggregate
Statistics

Roaming Client

Per Device and
Per User Statistics

Relay

Per IP
Statistics

💡 We recommend setting Site or Network level deployments
for every physical location that needs protection

DEPLOYMENT OPTIONS

Network Forwarding

PROTECTION GOALS

- Protection on your network
- No need for offsite protection
- Public or Guest Wi-Fi
 - E.g. hotels, airports, restaurants, schools, stores, and more
- [Simple deployment without extra software](#)
- Complete coverage of LAN devices

IMPLEMENTATION

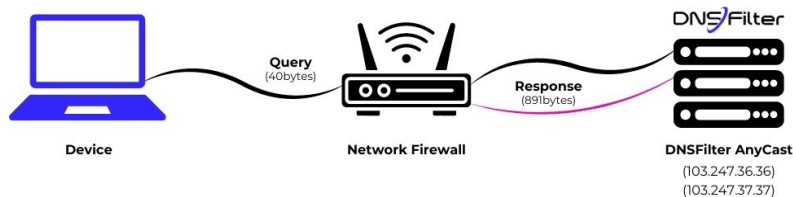
- Limited to 1 policy (up to 7 with NAT IPs)
- Reporting at the WAN level

DATA VISIBILITY

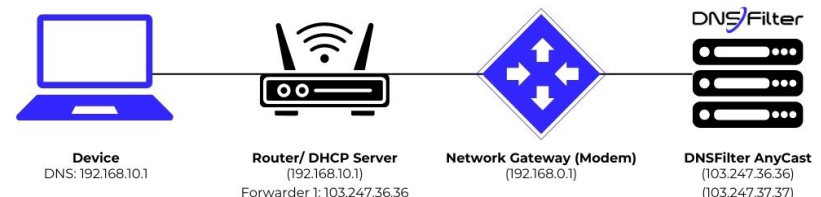
- Aggregate data with traffic visibility for the whole network

PREPARE YOUR ENVIRONMENT

- Check that your ISP is not [transparent proxying](#) DNS traffic or using [CGNAT](#)
- Confirm it is free of conflicting [software](#) or [hardware](#) settings:
 - Any existing firewall, VPN, and security app rules or settings are set to [allow traffic to the correct IPs](#)
 - End users cannot [circumvent the filtering policies](#)
- All of the necessary [IP address are accounted for](#) in the DNSFilter dashboard



OR



DEPLOYMENT OPTIONS

Relay



PROTECTION GOALS

- Apply filtering policies by IP or subnet on your network
- Desire for per-machine reporting and protection
 - When Roaming Client can't be installed

IMPLEMENTATION

- Requires machine, VM, or docket to run high availability
 - No user-level filtering or user-level reporting

DATA VISIBILITY

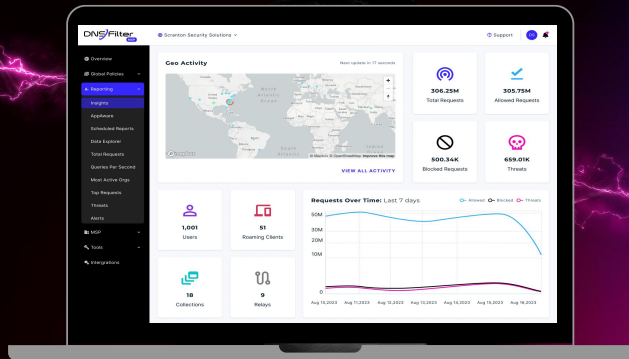
- Per machine or per IP statistics

PREPARE YOUR ENVIRONMENT

- DNS traffic isn't able to reach DNSFilter without issue:
 - [DNS response time is slow](#)
 - Dashboard Sites show [inactive or do not come online](#)
 - End users cannot [circumvent the filtering policies](#)
- [Relay](#) deployment isn't auto-updating as expected

DEPLOYMENT OPTIONS

Roaming Client



PROTECTION GOALS

- Protection on your network and when traveling or remote
- Easily set or change policies for large groups of computers
 - E.g. teachers/students, corporate departments, public/private computers
- Available on all platforms
 - [Windows](#), [Mac](#), [iOS](#), [Android](#), and [Chromebook](#)

IMPLEMENTATION

- Requires software installation and ongoing maintenance (either through manual or automatic updates)

DATA VISIBILITY

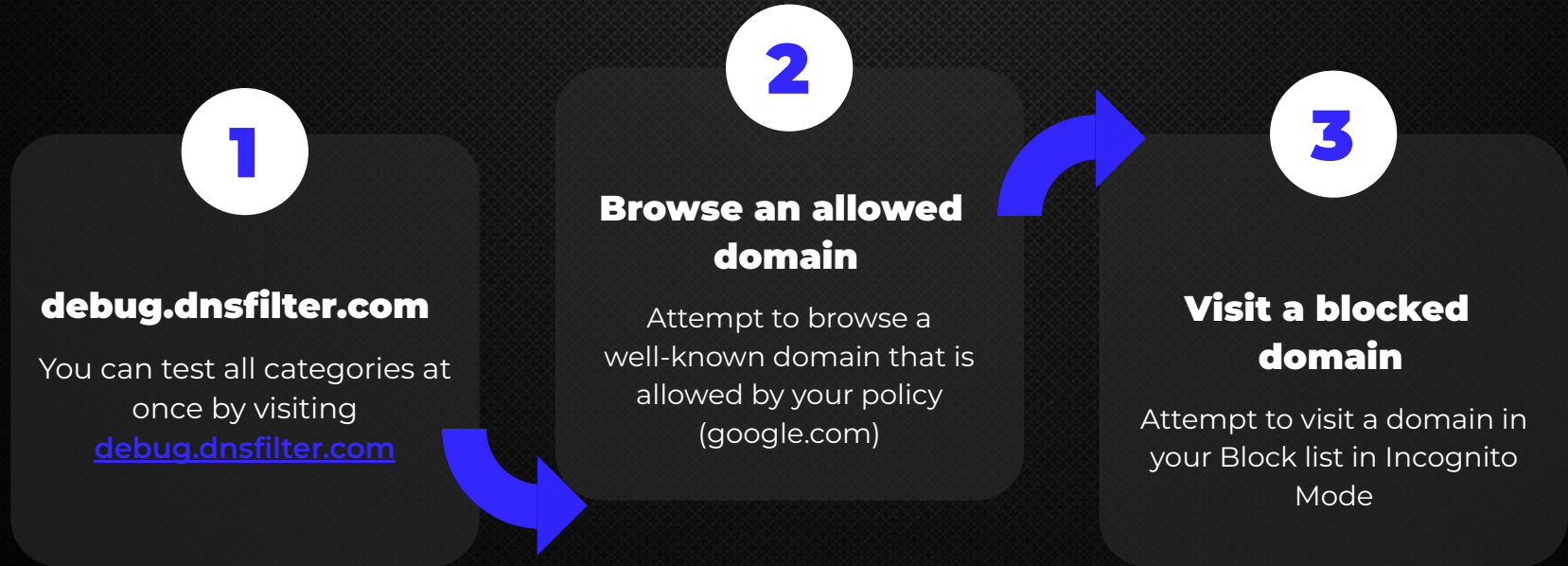
- Granular per device and per user reporting

PREPARE YOUR ENVIRONMENT

- [Losing Wi-Fi access](#) in public places like airports or hotels
- [VPNs](#) are set to allow DNS traffic to reach DNSFilter
- Roaming Client connectivity issues:
 - It cannot [bind to the correct port](#)
 - There's [limited internet connectivity](#) once installed and online
 - [macOS listener address and port](#) conflict

TESTING YOUR CONNECTION

Once you've configured your deployment, you can test your network connection by:



WHITELABELING DNSFILTER

Custom Domain Mapping

01

Utilize a CNAME to map a custom domain for a client-facing filtering dashboard.

Point your CNAME to cname.netalets.io in the DNS configuration for your domain.



Contact Email

03

Support requests submitted by your customers through the dashboard will be sent here.



05

Email Configuration

Set your preferred email address that clients will receive associated with their DNSFilter environment to [come directly from you](mailto:come_directly_from_you@netalets.io) or netalets.io.



Dashboard Name

02

The name associated with the Dashboard when accessed via the Custom Domain.

This is usually your company name.



Logo and Favicon

04

Replaces the DNSFilter logo in the Dashboard and the icon for bookmarking a page when accessed through the custom CNAME.



Site Creation Toggle

06

Enabling this allows the Admin to create Sites.

If disabled, only an MSP-level Admin can create Sites.



DNSFilter REPORTING

Effectively monitor and analyze your clients activity with ease



INSIGHTS

Full breakdown of traffic by domains, total blocked or allowed requests, as well as what domains were visited when and by who at a glance



QUERY LOG

Provides near real-time data of domains visited with visibility into time, device or user (if a Roaming Client is installed), associated categories, and more



SCHEDULED REPORTS

Automated reports delivered to your clients at a weekly, biweekly, or monthly cadence





INTEGRATIONS

Connect your existing tools and platforms to streamline workflows, enhance automation, and improve network security management



[API PROVISIONING](#)

Allows seamless automation of account setup, policy management, and user provisioning directly through your own systems



[REWST](#)

Enables seamless automation of threat response and policy management workflows for enhanced security efficiency.



[PROFESSIONAL SERVICES AUTOMATION](#)

Streamlines billing and account management by syncing customer usage and subscription data directly into your PSA tool



[SYNC TOOLS](#)

Automates user and group syncing from directory services, enabling seamless policy application and account management.

NAVIGATING PUBLIC WI-FI

PROTECT YOUR USERS AND YOUR ENVIRONMENT

BLOCKING ACCESS TO

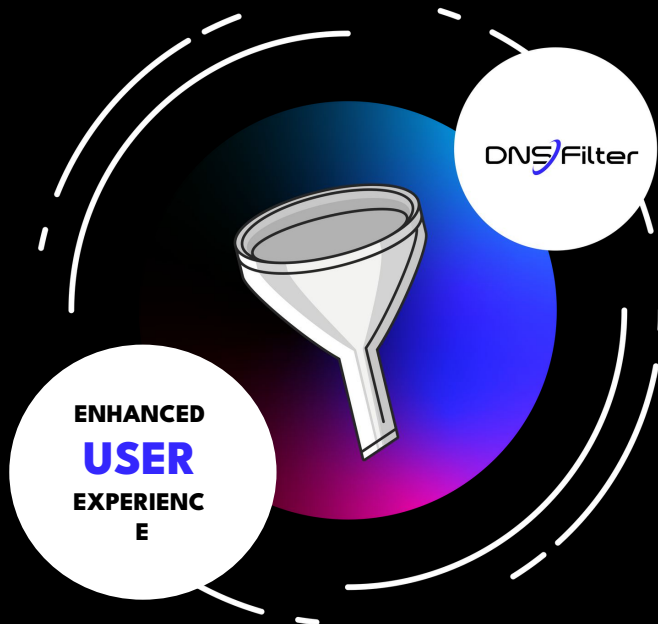
Safeguard users on public Wi-Fi from threats common to unsecured networks

PREVENTING ACCESS TO

Inappropriate or harmful content, important in family-friendly or business environments

BLOCKING MALICIOUS SITES

Helps protect users' privacy and secure their data on public Wi-Fi networks



DEPLOYMENT IS EASY

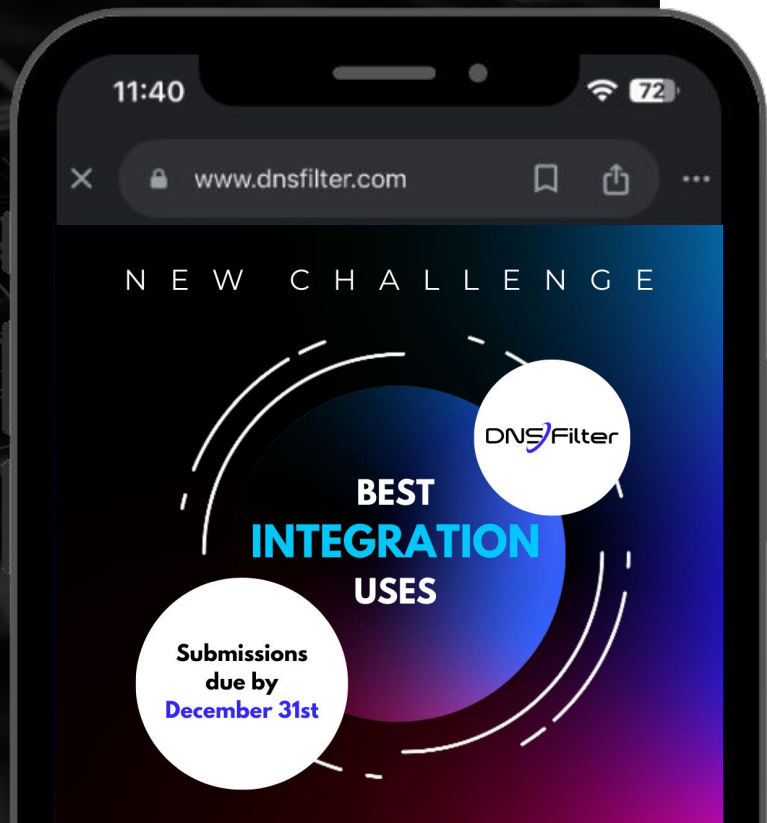
Begin protecting your environment with Network Forwarding. This provides a blanket policy that covers all devices on your network.

CONFIGURE YOUR NETWORK

Depending on the size of your business, you'll likely configure your network traffic to point toward DNSFilter from the DHCP Server, though small businesses may find it easier to configure from a router.

QUESTIONS?

If you have questions later, you can always reach out to us in the [Community](#)!



partners.dnsfilter.com

Partner Program Certification

[Direct download link](#)

New Customer Roadmap Checklist

community.dnsfilter.com

Join our Community!

help.dnsfilter.com

DNSFilter Knowledge Base



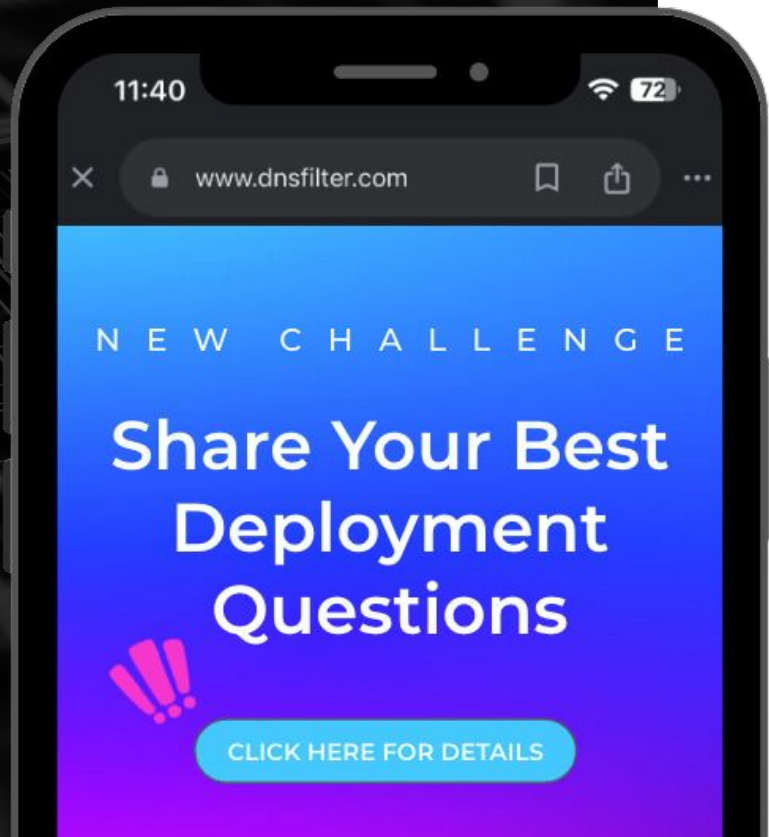
Loving DNSFilter? [Leave us a review!](#)



Loving DNSFilter? [Leave us a review!](#)

QUESTIONS?

If you have questions later, you can always reach out to us in the [Community!](#)



help.dnsfilter.com

DNSFilter Knowledge Base

[Direct download link](#)

New Customer Roadmap Checklist

[Understanding DNS Insights](#)

Reporting Dashboard Guide

Review the guides below

Migrating to DNSFilter

- [Cisco Umbrella](#)
- [OpenDNS](#)
- [Cloudflare](#)
- [ZScaler](#)
- [Webroot](#)