PRODUCT BRIEF

DNS FILTER

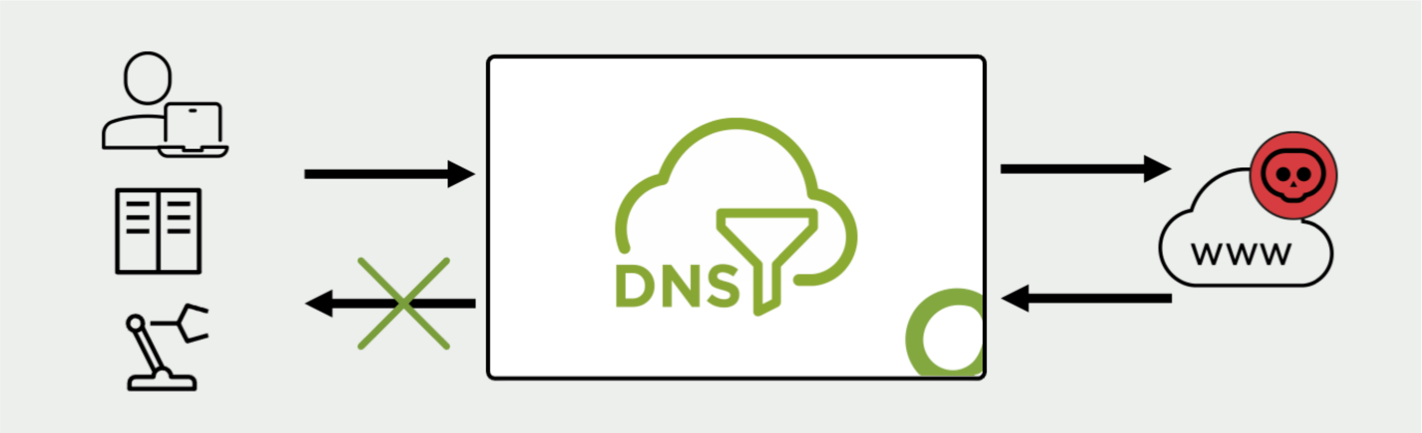
Control and protect web traffic of all your entities–guests, servers, machines and IoT

Why is a DNS Filter needed to complement Secure Web Gateways?

Every organization should have a global internet browsing security policy – not only to protect day-to-day operations but to defend the brand itself. Since Secure Web Gateways typically need to be explicitly configured on users' devices, it means users with unmanaged devices – as for example guests, servers, legacy machines and IoT – are neither protected from web threats nor forced to adhere the company web policy standards.

The DNS Filter ensures business-aligned and safe web browsing

The DNS Filter runs on the firewall and thus can apply URL filtering as well as threat protection on all web traffic that follows the default route. Enhanced functionality like malware protection, SSL scanning and authentication can be provided by the dedicated Secure Web Gateway module. However, it needs to be configured on users' devices and can't be enforced on unmanaged or legacy devices. With the Open Systems DNS Filter, business-aligned web access and protection of all users from malicious web content can be ensured.



The DNS Filter helps to enforce your policies and protects all entities from web threats

Why Open Systems DNS Filter?

WEB SECURITY FOR ALL USERS

We have a hybrid approach for web security: Secure Web Gateway for proxy-aware clients and DNS Filter for the rest.

With the DNS Filter, policy enforcement and threat protection for web traffic can be guaranteed for every user – including guests, legacy machines and IoT.

SEAMLESSLY INTEGRATED

Forget about the headaches of coordinating implementations of web policy exceptions or debugging latency due to proxy routing detours.

DNS Filter and Secure Web Gateway are seamlessly integrated into your SD-WAN and everything is handled by Open Systems.

EXPERT-LEVEL OPERATIONS

Enjoy the peace of mind that 24x7 monitoring, incident handling, and change management is being taken care of – provided by our expert-level engineers.

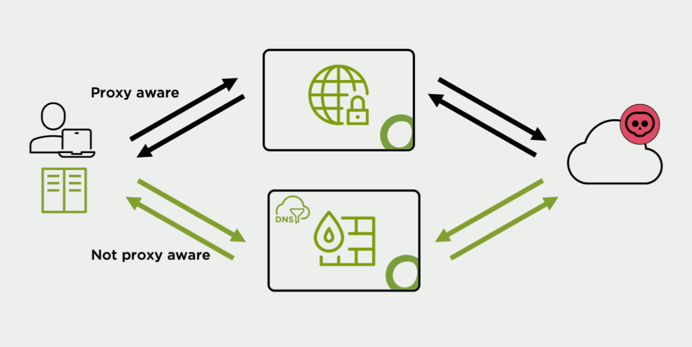
Central policy setup and control allows you to enforce consistent, global security policies and configuration.

How does the DNS Filter work?

Hybrid approach

For proxy-aware clients – as for example employees with managed devices, where an internet proxy can be configured – the Secure Web Gateway provides extensive functionality.

However, for non-proxy-aware clients like guests, legacy machines and servers or IoT – which are essentially users with unmanaged devices where nothing can be configured – the DNS Filter provides web security capabilities. The DNS Filter does URL filtering for web policy enforcement and includes web threat protection.



Hybrid approach with Secure Web Gateway and DNS Filter

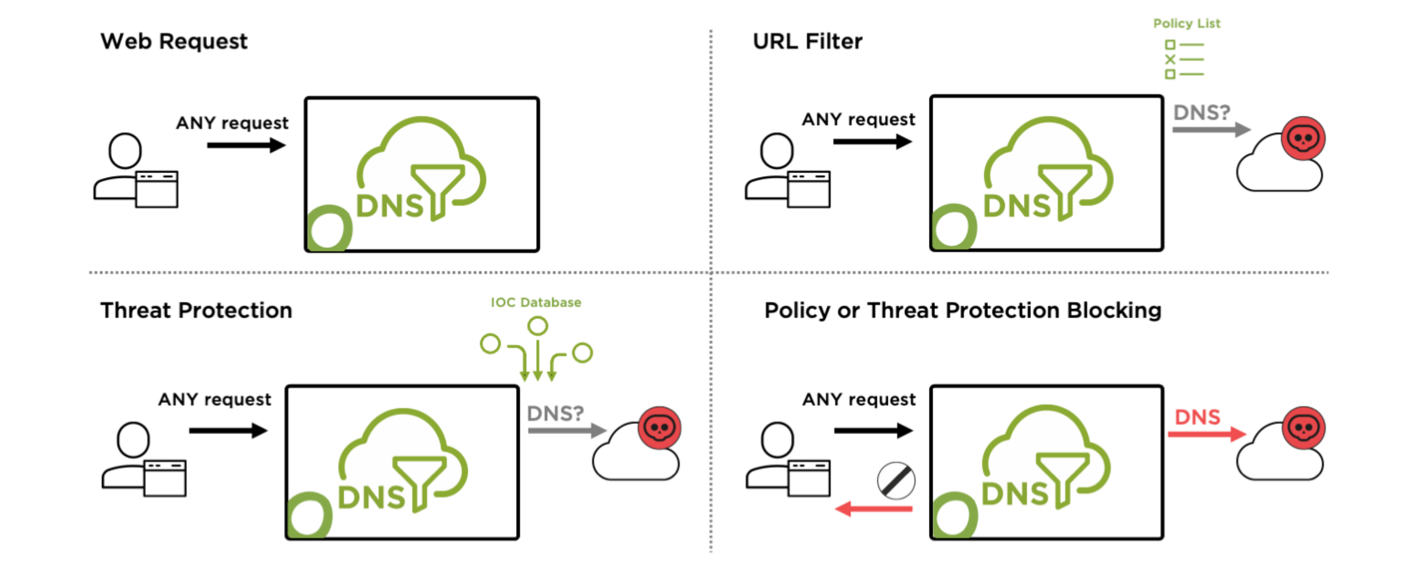
DNS Filter processing

1. If clients are **not proxy aware,** their **web requests** will simply follow the default route pointing to the edge device between the LAN and internet, which has a firewall and the DNS Filter running.

2. **URL filtering** enforces an organization's internet access policy and validates whether the requested domain name is part of the category of allowed web locations or not.

3. **Threat Protection checks** whether the requested DNS belongs to the IOC database, a smart repository that aggregates the different threat intelligence feeds that deliver known malicious URLs, domains, and IP addresses.

4. If a **request is blocked** by the DNS Filter due to security or business reasons, the client will get an error page displayed in the browser or the app in use.



Global overview and configuration

The Customer Portal provides an overview of all your users' web traffic no matter where they are located. In addition, drill-down options provide a high granularity level such as domains, countries, applications or endpoints.

Co-management

If desired, leverage the DNS Filter threat protection self-service features in the Customer Portal that allow you to apply changes yourself or make use of the API. Mission Control, our NOC, will of course still be there to support you in case of questions.

Open systems

Open Systems connects and protects users, apps, and data everywhere they reside with a comprehensive, unified easy-to-use technology platform combined with an excellent 24x7 Managed SASE service.

Discover more at open-systems.com |