ONE PAGER

DNS vs URL Filtering

What's the Difference and Why it Matters.

Cyberattacks often begin with a single click. That's why content filtering is more critical than ever in today's digital landscape. But not all filtering technologies are the same and understanding the difference between DNS and URL filtering can help your organization build a smarter, layered security strategy for web access.

What is DNS Filtering?

DNS filtering works at the Domain Name System (DNS) level. This is the same system that translates a website (like linkedin.com) into the IP address your device uses to connect. When DNS filtering is enabled, requests for malicious, risky, or non-compliant domains are blocked before a full connection is established.

Benefits of DNS Filtering:

- **Fast and lightweight** – stops threats before a page even loads
- **Great for remote/hybrid work** – protection travels with users
- **Broad protection** – blocks entire domains known for hosting malware, phishing, or botnets.

Example:
If a user clicks a phishing link to malicious-phish.com, DNS filtering stops it from resolving so no connection or download is made (and no risk).

What is URL Filtering?

URL filtering goes deeper. It analyzes the full web address (URL), including the specific page, folder, or file path, after DNS resolution.

This allows organizations to enforce more granular web access policies and send the entire URL for more in-depth evaluation. Benefits of URL Filtering:

- **Granular control** – Send specific pages for further risk-based evaluation (e.g., example.com/sports/basketball)
- **Advanced Threat Protection** – Stops users from accessing compromised subpages or dangerous downloads on otherwise "safe" domains

Example:
A site like example.com may be generally safe, but example.com/freeware.exe could contain malware. URL filtering catches this.

sonicwall.com

SONICWALL®

DNS vs. URL Filtering: Key Differences

Feature	Dns Filtering	URL Filtering
Layer	Network (DNS)	Application (HTTP/S)
Granularity	Domain-wide	Path-specific (URLs, subpages, files)
Speed	Fast, blocks early	Slightly slower, more detailed
Use Cases	Stop known threats early	Enforce deeper inspection
Best For	Lightweight, broad protection	Granular content filtering and policy enforcement

Why You Need Both

DNS filtering is your first line of defense by keeping users from even reaching known bad destinations. URL filtering is your second layer which analyzes deeper content on the fly to catch what DNS filtering didn't.

Together they give you:

- Comprehensive threat coverage to prevent data loss and breaches
- Flexible policy-based controls based on user groups
- A layered security approach that secures web access wherever your users are

CSE Makes Both Simple

SonicWall's Cloud Secure Edge (CSE) delivers both DNS and Risk-Based URL filtering as part of its SWG capabilities to ensure that your users can safely access the internet wherever and whenever. It's cloud-delivered and built for today's hybrid workforces so that growing organizations and MSPs can proactively stop threats and enable disruption-free access to both internal resources, cloud applications, and the internet.

Learn more by getting a personalized demo or reaching out to our team today.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.