

# Web filtering

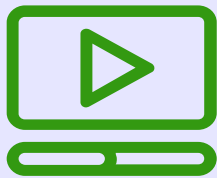
ISO 27002 Control 8.23

## Control

Access to external websites should be managed to reduce exposure to malicious content

## Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources



## Why is it important?

- It acts as a preventive measure against malicious content (e.g., viruses, phishing) which can compromise the organization's systems
- Ensures compliance with policy rules regarding appropriate use of online resources
- Web filtering effectiveness can depend on quality of threat intelligence

## What type of filtering ?

- URL blacklisting/whitelisting
- DNS-based filtering and blocking
- Category-based content filtering
- SSL/TLS traffic inspection
- Keyword and pattern matching
- IP reputation filtering
- Machine learning content classification



## Details are important

- Personnel should be advised not to overrule browser advisories that report an insecure website
- Filtering can use signatures, heuristics, or lists of acceptable/prohibited domains
- The rules should be kept up-to-date based on the threat landscape
- Training should cover the contact point for raising security concerns

## Link with other frameworks

- NIST 800-53 rev5 : AC-4, SC-7
- NIST CSF 2.0 : NA



Renaud Dardenne  
Asphalia Consulting