



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

# Web Filtering Best Practices

Most organizations have some level of web content filtering that restricts which types of websites guests and employees can access over corporate networks.

These systems are valuable in blocking harmful sites containing malware or illegal content, and often also block websites pertaining to adult content, violence, hate, weapons, gambling, proxy avoidance, and dating.

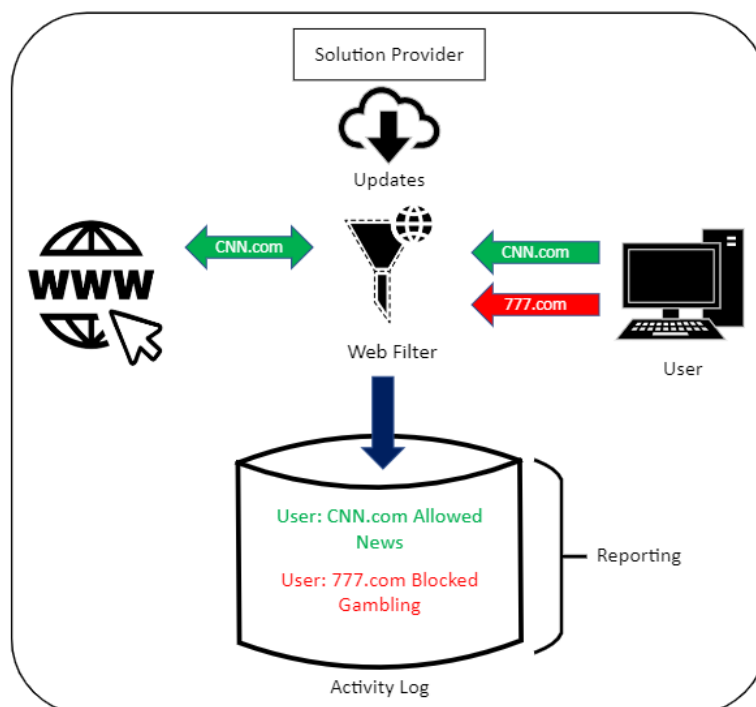
Websites are categorized, the organization decides which categories to block on their networks, and that's that.

But in the realms of digital forensics, insider threat detection, and employee productivity, web filtering solutions offer more than meets the eye.

## How does web filtering work?

We've broken it down step-by-step. Generally, the process is as follows:

1. Anytime a user accesses a website, the HTTP and HTTPS protocols that are involved get routed through the web filter for inspection by the system.
2. The system cross-references the website's category and its own settings about which website categories are blocked or permitted.
3. Websites are continually being added to this filter, too. The solution provider can update the reference table for all systems themselves, or the filter itself can check a provider's servers to determine the category of each site that's been visited.
4. Based on the system's settings, the user is allowed or blocked from visiting the website. No matter the verdict, the access attempt is recorded.



## Tips for picking the best solution

It's important to use a structured request for information process. That way, you'll be able to evenly appraise each solution you're considering. Document your needs, questions (and vendor responses), and align the vendor's responses and solution featured in a weighted average scorecard.

### Sample weights

- Approach – 10%
- Experience – 15%
- Functionality- 60%
- Innovation – 5%
- Cost – 10%

Check the latest Gartner Magic Quadrant reports too, and use them as a guideline to see how your prospective solution fares. While the Gartner reports offer good opinions and advice, they should really only represent a portion of your decision-making data.

### Other tips

- Your solution, ideally, should support both Active Directory integration and customized access from your business department.
- The web filter solution should “fail open,” meaning if the web filter shuts off, Internet traffic won't be cut off.
- All traffic transactions should be logged and retained. They should be kept for an appropriate period for forensics purposes, or should be shipped to a Security Information and Event Management (SEM) solution.
- Log data should be time stamped and contain a user ID, machine host ID, IP address, URL, category, and access determination (whether the website was accessed or blocked).
- The solution should provide a blocked message to the user that is branded, and includes a link for the user to directly contact your Information Technology or Information Security department and request access.
- The solution should support extracting logs for reporting purposes.
- The solution should also support traveling / remote users. That's usually done by using a PAC file that points HTTP and HTTPS traffic to a cloud proxy.

- If your traffic is stored in a cloud-based solution, solution resides somewhere that meets your data security requirements. Some providers distribute operations globally for resiliency, data transport latency reduction or cost.
- Support should be available 24/7/365 and have a documented escalation process to level 2 or level 3 support in a reasonable time frame.
- The solution should compliment your company's disaster recovery architecture, so that filtering remains effective even if your primary datacenter or Internet connectivity goes offline.
- As with any technology selection, try to avoid providers who have just merged with other providers, or have been acquired by another vendor. This avoids support issues and unexpected changes to the solution you bought.
- Determine whether support will be from the solution provider directly, or a third-party channel.
- Build contacts and relationships with people working for the vendor who can influence speedy support resolutions, should normal support channels fail to meet your expectations. There may be a time when you will need to ask a VP of support for help.
- Ensure the solution's terms and conditions or master agreement meets your contractual needs.
- Many privacy policies are now only available online and will change at any time without warning. In your terms, try to lock in static privacy policies as of a certain date and provide yourself an early out of the contract, should the vendor make material changes that jeopardize data security.

## Best practices for configuration

- Integrate filter access with your Active Directory, and create object groups to apply access to.
- Create access groups based on need:
  - For productivity reasons, some departments will need social media access, but others do not.
  - The fraud team may need full access (including adult categories) for card charge disputes.
  - Information Security may need access to hacker-adjacent websites, or other security related categories.
  - Information Technology may need access to application downloads, or technical blog sites for support issues.
- Create a whitelist for each access group you create, so that override access is restricted to only those users who need it.

## Web filtering solution caveats

- Sites are sometimes miscategorized, which leads to users not being able to access relevant website for work. In these cases, user access records will also incorrectly report access attempts to blocked content.
- Not all sites can be reviewed by the solution provider, and in these cases the sites are categorized as “unclassified.” If unclassified sites are blocked (the safest approach, by the way), then new, small, and local business websites may be blocked.
- A whitelist to allow access to otherwise blocked websites can be maintained, but do consider that this can add to administrative overhead.
- Forensics and Human Resource reporting needs an educated eye on your web traffic and what it represents, so that users are not incorrectly shown to be conducting intentional abuse.
- Ads need to be blocked when possible. Bad actors and cyber criminals frequently hijack web ads to distribute malware, and some ad providers have low standards and will lease ad space to anyone.
- In general, ads are a category that should just be blocked. Bad actors frequently hijack advertisement feeds to purvey malware. Some advertisement providers will lease to anyone as well. Do keep in mind, however, that many credible websites rely on credible advertising, and won't let you load their webpages unless you also load their advertisements.

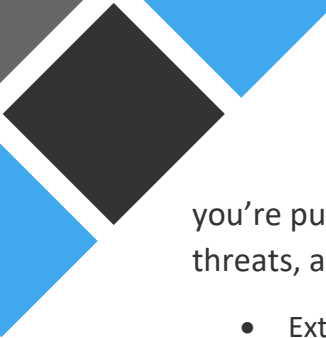
## Best practices for reporting

Web filter activity can be reviewed for forensics purposes to discover what users and what computers have been accessing what websites. When you're trying to discover where malware originated from, or trying to see how someone's browser redirected to an unseen web address, web filter forensics are particularly useful.

Through these forensics, your IT team may detect computers systematically trying to reach malware command and control sites.

Information Security may detect computers systematically attempting to reach malware command and control sites. Web filter records can also be used to discover violations relating to your corporate computer use policy.

We advise you run monthly reporting for your HR department. While it may seem over-diligent, it's important to identify and intervene in abuse as soon as possible. Otherwise,



you're putting your organization at risk for reputation loss, illegal activity, internal threats, and productivity loss.

- Extract the prior period's (month or quarter) activity, and sort out your blocked categories.
- List blocked activity by category, and adjust your findings to grant 5 attempts to filter out harmless accidental blocks. Focus on repetitive attempts only. A few blocked attempts around Christmas to hit up the outdoorsman apparel shop BassPro.com (it falls under the weapons category) is vastly different than a user trying to access every single gun and ammo website.
- Sort all user access by count and by user, and run the data through a statistics model to derive standard deviation. Report on the users in the top deviations to determine users who accessed the Internet far more than the rest; this may indicate lost productivity. Remember to review what they accessed, and determine if the sites align to their job function.
- Reviews and reporting should be conducted by senior Information Security management. Reports should include all users, and should be conducted on a schedule for reliability. These reports could be called on as evidence in wrongful employee termination lawsuits.
- Reports that identify outlier user counts, and instances of abuse, can be used as key performance indicators. Specifically, they can be used as guidance for the company's acceptable computer use policy and its training effectiveness.

## Wrapping up



A lot of organizations approach web filtering as a “setting and forgetting” situation. But unless your filter is wide open, there's a lot more to web filtering than meets the eye.

Deer Brook's team has extensive experience working with web content filters. If you need an extra hand, we can manage your web filters for you, and provide effective and concise reporting for your HR department, as well as forensic reporting when needed.

deer-brook.com



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

