perimeter 81

Protect Your Organization from the Internet with Web Filtering

Web Filter Rules

Control website access for members and groups with URL-based rules. Learn More

Search for a rule

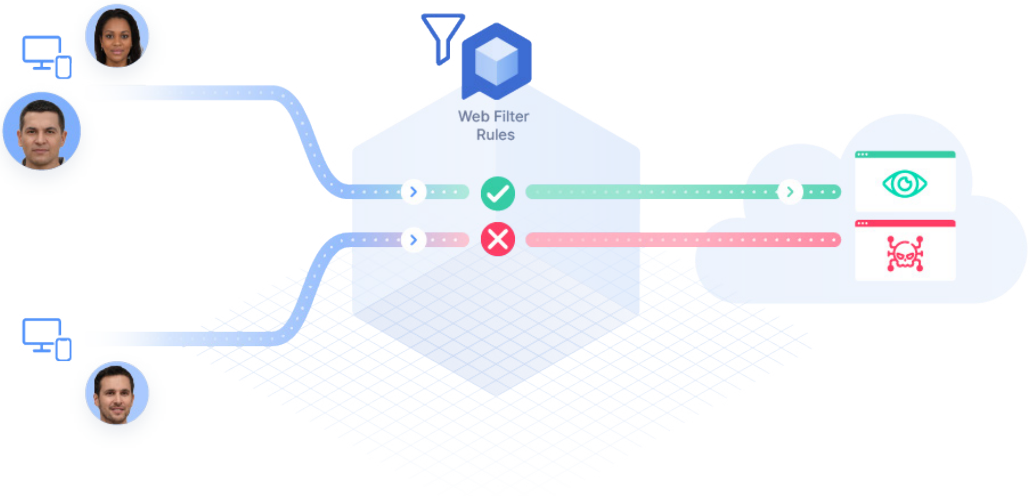
Total Rules: 4 | D

#	Name	Action	Source
1	Block malicious sites	Deny	Any
2	Block Facebook during working hours	Deny	Gr
3	Warn gaming site access	Warn	Any
4	Allow social media on weekends	Allow	Any

Control your web traffic

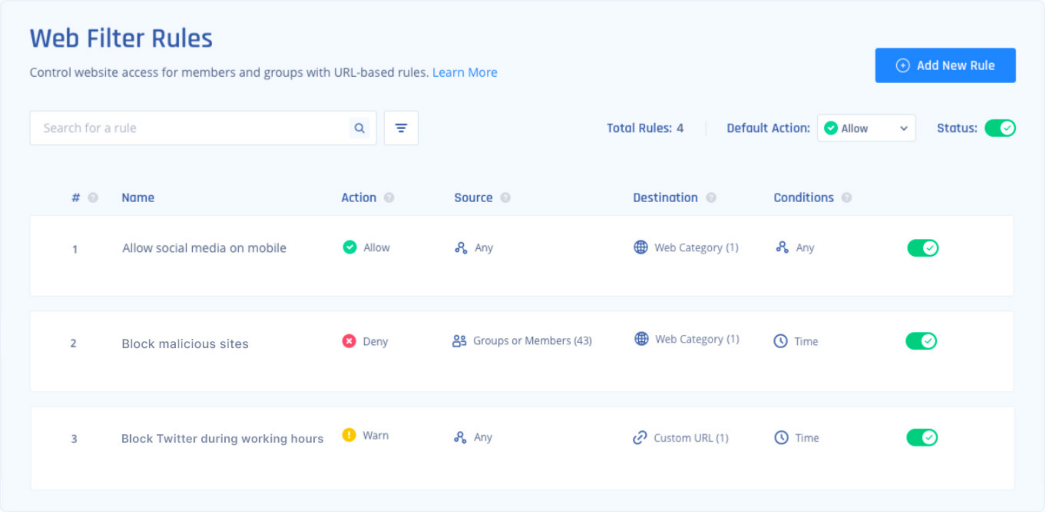
Not all websites can be trusted. Protecting your employees from potentially dangerous sites is the first line of defense for safer Internet browsing. With your users surfing hundreds (and sometimes thousands) of websites each day, securing them from potentially dangerous attacks is more important than ever for your organization's Internet safety.

Web Filtering, a key component of your Secure Web Gateway (SWG), makes this defense possible by controlling which URLs employees can access. Web Filtering protects your employees from potential threats, reduces malware infections, blocks distracting websites and increases workspace productivity.



How it works

By creating rules that limit access to web categories or specific URLs, you can gain total control over your employees' web traffic, whether or not they are logged on to the company network at the time. Web Filter rules also allow you to monitor your users' web activity with up-to-date, easily filterable reports.



Web Filter Rules

Control website access for members and groups with URL-based rules. Learn More

Total Rules: 4 | Default Action: Allow | Status: ✓

#	Name	Action	Source	Destination	Conditions	
1	Allow social media on mobile	✓ Allow	Any	Web Category (1)	Any	✓
2	Block malicious sites	✕ Deny	Groups or Members (43)	Web Category (1)	Time	✓
3	Block Twitter during working hours	! Warn	Any	Custom URL (1)	Time	✓

Customize Web Filter rules for different groups, web categories and conditions

Benefits and Features

- Filter out malicious sites and protect your employees and network from web-based threats
- Increase productivity by decreasing distractions from unwanted websites
- Prevent shadow IT and ensure that employees are only using authorized sites and web applications for business functions
- Track web activity and increase compliance with web auditing requirements
- Define bypass rules as necessary to comply with user privacy regulations and prevent issues with commonly used web applications

Easy to implement, easy to manage

Setting up Web Filter rules is quick and easy, and the impact is essential for network safety. With flexible rules, you can allow access, block the user from visiting the site, or give the user a warning which they can bypass to open the web page. All warned and blocked attempts are logged for auditing and security purposes.

Perimeter 81's user-centric granular control extends to your Web Filter rules. Website access rules can be customized for different individuals or groups of users and according to time of access. For example, social media sites can be blocked during work hours for all employees except for the members of the digital marketing department.

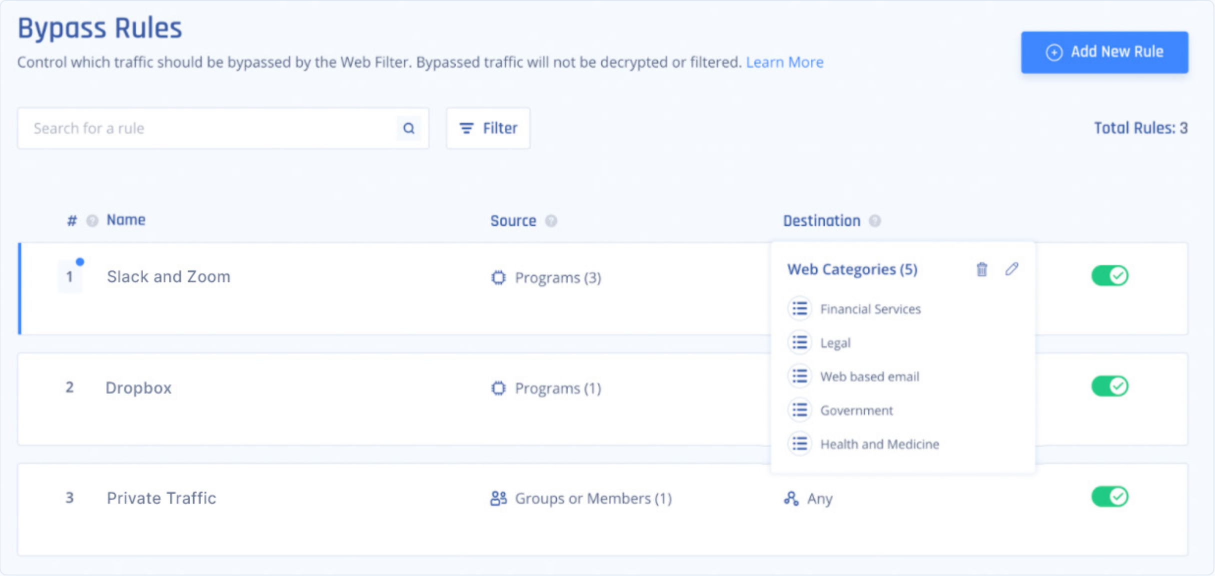
Control access to one site or hundreds

Whether it's to increase workspace productivity or to block dangerous sites, Web Filtering is simple and totally customizable. You can manage access to a single URL or to entire categories of sites, such as malware, gaming, and social media. These categories are dynamically updated daily as new sites appear.

Flexible Web Filtering with Bypass Rules

Worried about privacy concerns? Bypass rules allow you to select programs or sites that will bypass SSL inspection while allowing this traffic to remain encrypted and override the filtering rules you've enforced. You can also select programs which may need to bypass Web Filter rules in order to function correctly, such as Zoom or Slack.

Depending on your employee privacy policies, you can also enable certain web categories or IP addresses to bypass the filtering rules, such as Financial Services or Government sites. Your employees can rest assured knowing that they have total privacy on those sites.



Bypass Rules

Control which traffic should be bypassed by the Web Filter. Bypassed traffic will not be decrypted or filtered. Learn More

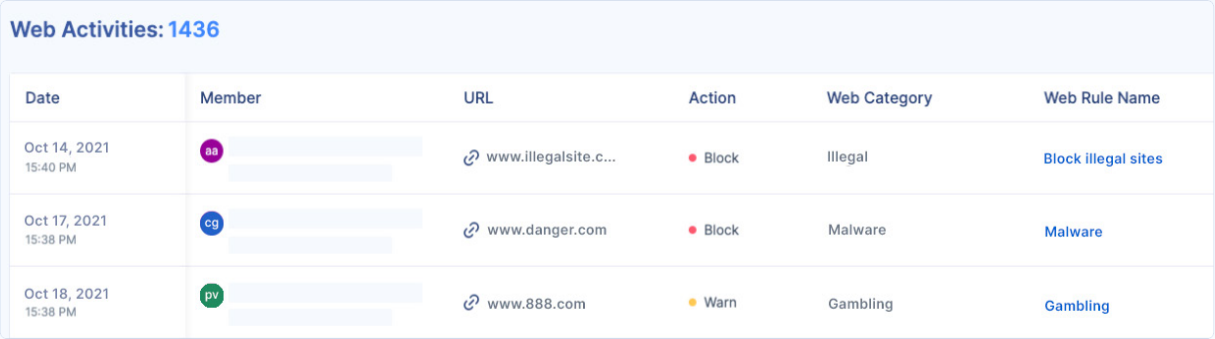
Total Rules: 3

#	Name	Source	Destination	
1	Slack and Zoom	Programs (3)	Web Categories (5) Financial Services Legal Web based email Government Health and Medicine	✓
2	Dropbox	Programs (1)		✓
3	Private Traffic	Groups or Members (1)	Any	✓

Define bypass rules to comply with web application needs and company privacy policies

See it all with Web Activity Monitoring

A secure network requires clear visibility into your users' web activity. Easily view which users tried to access blocked or warned sites and filter reports to drill down to specific employees, sites, or web categories. For auditing purposes, this data can be easily exported and further analyzed as a CSV file.



Web Activities: 1436

Date	Member	URL	Action	Web Category	Web Rule Name
Oct 14, 2021 15:40 PM	aa	www.illegalsite.c...	● Block	Illegal	Block illegal sites
Oct 17, 2021 15:38 PM	cg	www.danger.com	● Block	Malware	Malware
Oct 18, 2021 15:38 PM	pv	www.888.com	● Warn	Gambling	Gambling

See who was blocked and warned from websites across the Internet perimeter 81

Don’t take the risk

It’s no surprise that more and more organizations rely on SWG for safer Internet browsing. Filtering out malicious and potentially dangerous sites goes a long way to securing your organization. With so many daily threats on the web, it’s important to keep company users safe and protected. Allow members to enjoy Internet access without putting your organization’s cybersecurity at risk with trusted Web Filtering.

Contact Us

Perimeter Ltd.

www.perimeter81.com

1-929-575-9307

Request a Demo

Follow Us