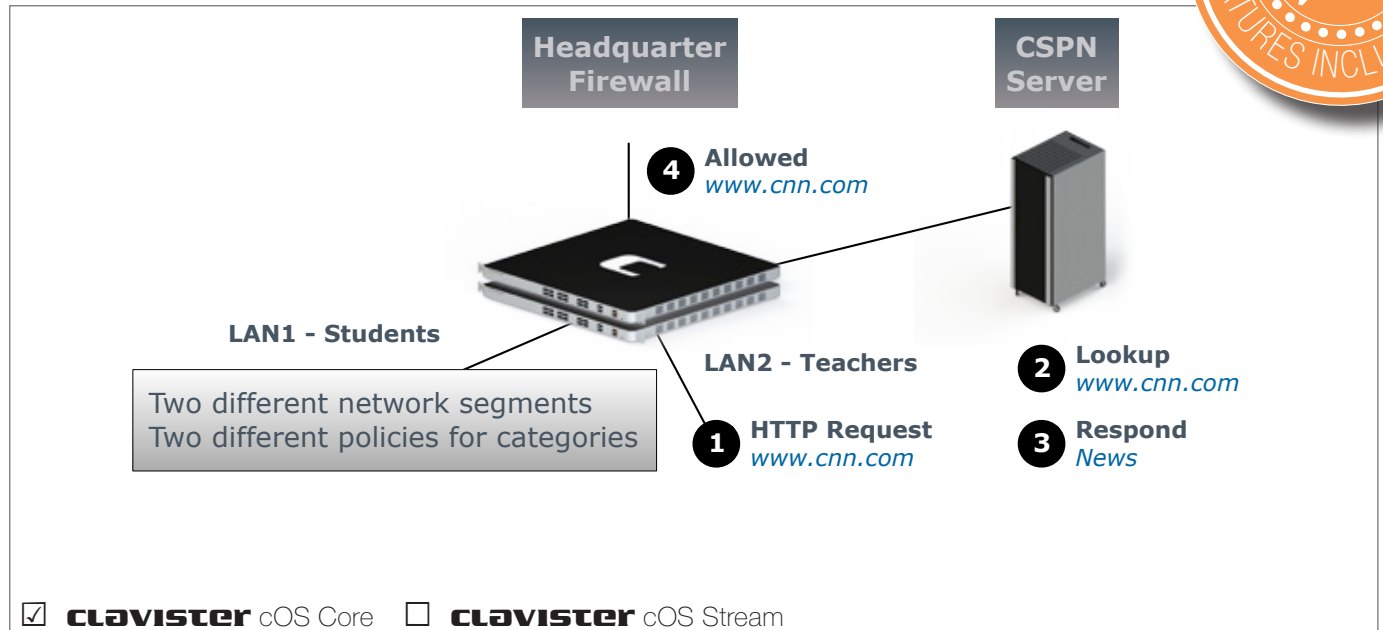




# Web Content Filtering Solution

Clavister cOS Core-based products can function as a Web content filtering solution that blocks specific URLs or URL-categories. Web pages are divided into one or several categories and maintained in an external database. For each Web request, the database is queried and filtered accordingly.



## Example

In this example, a school has configured two separate network segments on their headquarter firewall; LAN1 for students and LAN2 for teachers and staff. This enables them to separate access to certain Web categories, such as gambling, news or adult content.

This is especially important in an educational environment with a mix of students and teachers, but equally important in organizations who wish to limit the time staff spends on nonproductive activities.

1. A user, either a teacher or staff, wants to access *www.cnn.com* on LAN2

2. The headquarter firewall is configured for Web content filtering and performs a lookup on the requested URL through the nearest CSPN server
3. The content filter responds with content category News
4. Since this content category is allowed from LAN2 the requested URL is permitted and the user can access *www.cnn.com*
5. A student performing the same request on LAN1 would be disallowed.

**NOTE:** It is possible to configure content filtering to allow access but silently log the requests or allow users to override an access denial, and log the request.

## RESOURCES

For more information about **Web Content Filtering**, download the latest Clavister cOS Core Administration Guide from [www.clavister.com/my-clavister/downloads/clavister-cos-core](http://www.clavister.com/my-clavister/downloads/clavister-cos-core)

# CLAVISTER®

Clavister AB, Sjöгатan 6 J, SE-891 60 Örnsköldsvik, Sweden  
Phone: +46 (0)660 29 92 00 | [www.clavister.com](http://www.clavister.com)