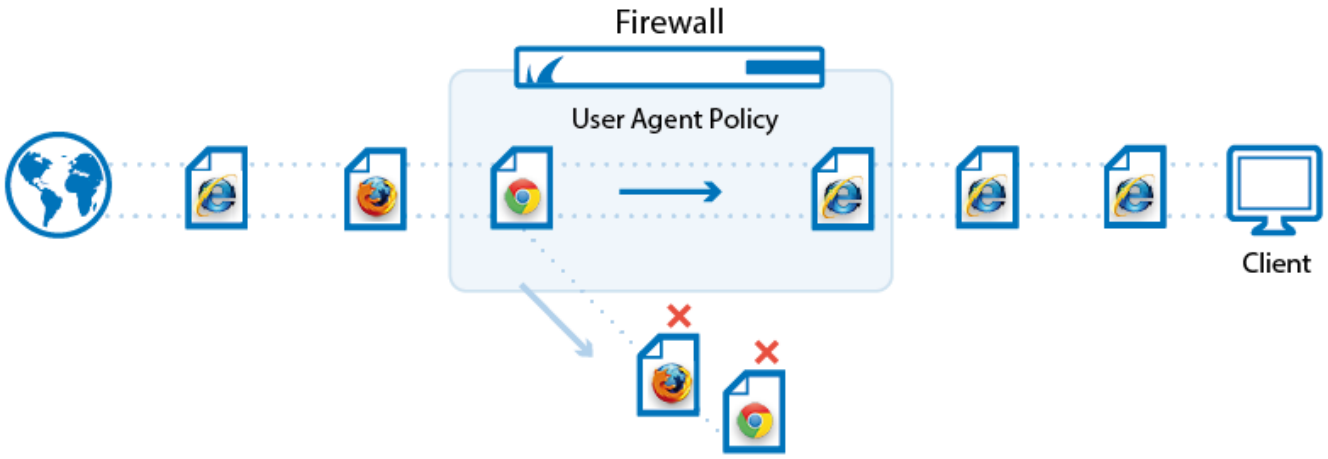
User Agent Filtering in the Firewall

https://campus.barracuda.com/doc/73719229/

User Agent policies allow you to control access to a web-based resource based on the user agent string. The information contained in the user agent string allows you to create policies based on web browser / operating system combinations or to define generic patterns for more specific filters. This feature also allows you to block website crawlers. Keep in mind that the user agent strings can be overridden on the client. Definitions for new user agents are updated regularly via Energize Updates.



User Agent Policy Objects

User Agent policies contain a list of browser type / operating systems combinations. You can also enter up to five custom user agent patterns to match specific parts of the user agent string, such as the browser version.

For more information, see How to Create User Agent Policies.

User Agent Filtering in the Firewall

To use User Agent policies, you must create an access rule matching your HTTP and HTTPS traffic and enable Application Control and, optionally, SSL Inspection. The User Agent policy object is then added to the matching application rule.

For more information, see How to Configure User Agent Filtering in the Firewall.

Figures

1. user_agent_policy.png