Best Practice - Web Filtering Features in the Firewall

https://campus.barracuda.com/doc/45024315/

The Barracuda NG Firewall now offers a lot of the functionality previously only seen in dedicated Web Filtering products. Use the features and instructions below to enforce your web access policies and protect your clients from malware and unwanted content.

URL Filter Policy and Match Objects

If you need to deny access to websites on the Internet based on the content category, use URL filter policy or match objects. You can also use a combination of application control and URL filter objects to improve the block rate when blocking an entire application category.

For more information, see How to Create an URL Filter Policy Object and How to Create an URL Filter Match Object.

Custom Block Pages / Response Messages

The Barracuda NG Firewall uses generic, unbranded block pages by default. You can change the HTML source of these pages to adjust the content and style to fit your needs. Each page has a predefined list of placeholder objects that are replaced on-the-fly by the Barracuda NG Firewall when the block page is delivered to the client. Custom block pages can be used for services using the Forwarding or Distributed Firewall services.

For more information, see How to Configure Custom Block Pages.

Safe Search

The users behind a Barracuda NG Firewall can be protected from undesired content in search results by enabling Safe Search for the access rule handling web traffic. No configuration is required on the clients. Safe Search is supported for Google, Bing, Yahoo, and YouTube search engines. Since most search engine providers default to HTTPS, using SSL Interception is highly recommended.

For more information, see How to Enforce Safe Search in the Firewall.

YouTube for Schools

The Barracuda NG Firewall can transparently add YouTube for Schools restrictions for all connections that the Barracuda NG Firewall forwards to YouTube without the need for any configuration on the clients. Since YouTube is only available via HTTPS, you must use this feature in combination with SSL Interception.

For more information, see How to Enforce YouTube for Schools in the Firewall.

Application Control 2.0

Application Control enables the Barracuda NG Firewall to detect and classify the traffic according to the application causing the traffic. Depending on the application, the Barracuda NG Firewall can also detect individual features or sub-applications, such as chat functions or picture uploads. Application rules define the policies that are applied to the detected applications and sub-applications. It is not only possible to block or deny an application, you can also reduce the bandwidth. Business- or latency-critical applications such as VOIP apps can also be prioritized.

Much of the application traffic is SSL-encrypted. SSL Interception allows the NG Firewall to decrypt this traffic and detect sub-applications that would otherwise go undetected. The main applications can be detected without SSL Inspection. For example the NG Firewall would detect that the HTTPS connection contains Facebook traffic, but would not be able to tell the difference between a Facebook image upload and Facebook chat.

For more information, see Application Control 2.0, How to Enable Application Control 2.0 and How to Create an Application Rule.

Application Based Provider Selection

A custom connection object containing the applications and the corresponding Internet connections allows the admin to decide which ISP to use based on the applications. For example, you may want to send business-critical traffic through an expensive, low-latency connection while undesired applications, such as music streaming or social media, is sent through a cheaper DSL line.

For more information, see Application Based Provider Selection.

Virus Scanning in the Firewall

The Barracuda NG Firewall scans incoming traffic for malware on a per-access rule basis when virus scanning in the firewall is enabled. If a user downloads a file containing malware, the Barracuda NG Firewall detects and discards the infected file and redirects the user to a customizable warning page. You can combine virus scanning with SSL Interception to also scan SSL-encrypted connections.

For more information, see How to Configure Virus Scanning in the Firewall.

ATD in the Firewall

Advanced Threat Detection offers protection against advanced malware, zero-day exploits, and targeted attacks that are not detected by the virus scanner or intrusion prevention system. ATD can be used for HTTP and HTTPS traffic in combination with the firewall service on a per-access rule basis.

For more information, see Advanced Threat Detection (ATD) and How to Configure ATD in the Firewall.