Firewall

https://campus.barracuda.com/doc/8650771/

The basic job of the Barracuda NextGen Firewall X-Series is to manage traffic between various trusted and untrusted network segments. Incoming network traffic is compared to the first firewall access rule in the ruleset. If it doesn't match the next rule is evaluated, continuing from top to bottom until a matching rule has been found.

Criteria for matching access rules are:

- Source IP address or network
- Destination IP address or network
- Service (protocol, port/range)
- Application
- Users
- Time
- Interface

The first matching access rule is executed. If none of the rules match the default Block-all rule will block the traffic.

Next Generation Firewall capabilities

Application Control (with or without SSL Inspection), a tightly integrated Intrusion Prevention System (IPS) and URL filtering for content security offer granular control over your network traffic.

- **Application Control** – Application Control enables you to manage traffic caused by applications on your network. Knowing which applications use the most traffic lets you create rules to optimize bandwidth for business critical applications while limiting unwanted application traffic.
- **SSL Inspection** – Most of the application traffic is SSL encrypted. SSL Inspection transparently decrypts the SSL connections and after passing through Application Control reencrypts the connection and forwards it to its destination. SSL Inspection enables Application Control to detect sub-applications making it possible to block single features such as Facebook games, while still allowing access to the rest of the site.
- **URL Filter** – If you want to keep out inappropriate web based content from your network, the Barracuda Web Security Gateway enables you to filter a large number of websites based on categories. The URL filter can be used to create a whitelist (blocking everything except for selected sites) or a blacklist (blocking known unwanted content). If the site is not in the URL database you can define a custom URL policy. The URL Filter can only filter based on the URL of the website. It does not offer the more granular control over sub-applications that Application Control does. For more information, see Application Control.

- **Virus Protection** – HTTP(S), FTP and SMTP(S) traffic can be transparently scanned for malicious content while the traffic passes through the firewall. For more information, see Virus Protection in the Firewall.
- **Advanced Threat Protection (ATP)** – Advanced Threat Protection secures your network against zero day exploits and other malware not recognized by the IPS or virus scanner. You can choose between two policies, which either scan the files after the user has downloaded them and, if perceived to be a threat, quarantine the user, or scan the file first and then let the user download the file after it is known to be safe. For more information, see Advanced Threat Protection (ATP/ATD).
- **Mail Security** – Check the source IP address of incoming SMTP(S) connections against a DNSBL and modify the header and subject of the e-mail if the sender is listed in the DNSBL. For more information, see Mail Security in the Firewall.,
- **Intrusion Prevention System (IPS)** – The tightly integrated Intrusion Prevention System will monitor the network for malicious activities and block detected network attacks. For more information, see Intrusion Prevention System or IPS.

To create, edit, or change the order of access rules, go to the **FIREWALL > Firewall Rules** page. For more about matching criteria and possible access rule actions, see Firewall Rules. If you are new to the Barracuda NextGen Firewall X-Series, see Pre-Installed Access Rulesto review the rules that are already set up in the appliance. You can use these preinstalled rules as a starting point for your own rules.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.