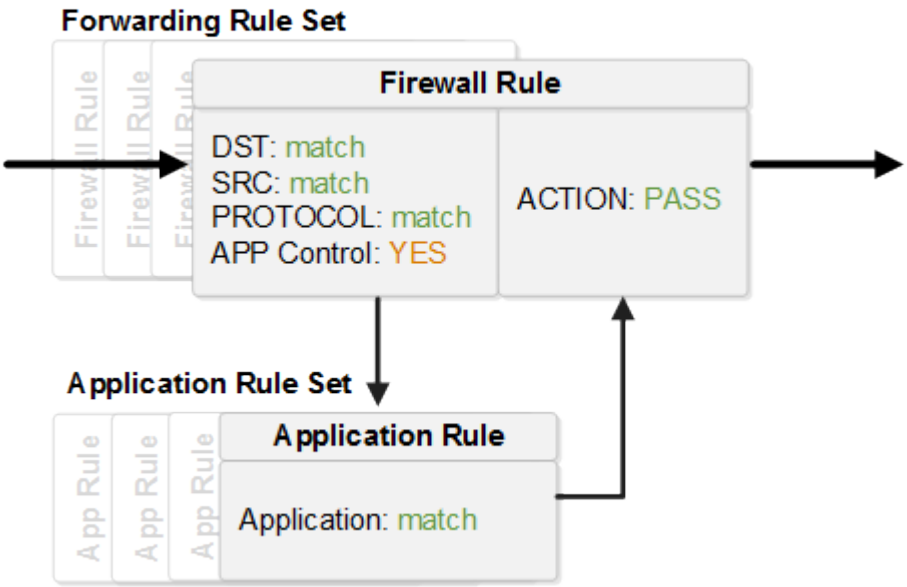
Forwarding Firewall

https://campus.barracuda.com/doc/41115830/

The forwarding firewall service provides a policy framework to direct and manage traffic passing through the Barracuda NG Firewall:

- **Firewall Policies**:
  - **Firewall Access Rule Set** – The firewall rule set contains a list of access rules. Incoming traffic is compared against the matching criteria set within each access rule. When a match is found, the action set in the access rule is executed. You can enable advanced features (Application Control, QoS, IPS) on a per-rule basis.
  - **Application Rule Set** – If application control is enabled in an access rule that is executed, the application rule set is called. Applications and (if applicable) URL categories are detected and compared to the list of application rules. Upon a match, the application traffic is either passed or blocked depending on the action set in the application rule.
- **IPS Policies** – Detect and block network attacks, by comparing incoming traffic with predefined, constantly updated patterns.
- **Traffic Shaping (QoS) Policies** – Shape traffic to improve use of the available bandwidth, by prioritizing connections that are important for your business.
- **User Policies** – Allow or block access to network resources based on user information.
- **Time Policies** – Allow or block access to network resources based on time or date.

Traditional packet forwarding capabilities are handled by the access rule set while next generation application-aware policies are applied in the dedicated application rule set.



Access Rules

The basic job of the firewall is to manage traffic between various trusted and untrusted network segments. Incoming network traffic is compared to the first firewall access rule in the rule set. If the traffic does not match the criteria set in the rule, the next rule is evaluated, continuing from top to bottom until a matching rule is found. The first matching firewall rule is executed. If none of the rules match, the default BLOCKALL rule blocks the traffic.

For more information, see Firewall Access Rules.

Next Generation Firewall Capabilities

Application Control 2.0 (with or without SSL Interception), a tightly integrated Intrusion Prevention System (IPS), URL filtering for content security, and Virus Scanning in the firewall offer granular control over your network traffic.

- **Application Detection** – For each firewall rule, you can enable Application Control. Application Control detects applications and subapplications. Detected application traffic can then be manipulated by the application rule set. By using custom application-based link selection connection objects, you can route traffic based on application type.
  For more information, see Application Control 2.0
- **SSL Interception** – Most application traffic is SSL encrypted. SSL Interception transparently decrypts the SSL connections and re-encrypts the connection before it is forwarded it to its destination. SSL Interception enables Application Control to better 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 block inappropriate web-based content from your network, use the Barracuda Webfilter to filter a large number of websites based on categories. With the URL filter, you can create either a whitelist (blocking everything except for selected sites) or a blacklist (blocking known unwanted content). If a site is not in the URL database, you can define a custom URL policy for it. 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 URL Filter.
- **Virus Scanning** – To protect against malware and viruses, enable antivirus (AV) scanning in the firewall. If a user downloads a file containing malware, the Barracuda NG Firewall detects and discards the infected file and then redirects the user to a warning page. You can use the Avira and/or the ClamAV antivirus engines and specify the MIME types of all files that are to be scanned.
  For more information, see How to Configure Virus Scanning in the Firewall.
- **ATP** – Barracuda 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).

Traffic Shaping (QoS)

You can adjust the QoS band traffic to prioritize business-critical traffic over less important traffic:

- Traffic shaping protects the available overall bandwidth of a connection. Network traffic is classified and throttled or prioritized within each firewall rule.
- Traffic shaping for application traffic can be configured in the application policy rules. For more information, see Application Control 2.0.

For more information, see Traffic Shaping.

Intrusion Prevention System (IPS)

The tightly integrated Intrusion Prevention System (IPS) monitors the network for malicious activities and blocks detected network attacks. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signature database for known attack patterns. IPS must be globally enabled on a Barracuda NG Firewall. However, you can enable or disable IPS for each firewall rule.

For more information, see Intrusion Prevention System (IPS).

Users/Time

For more granular control, you can configure firewall rules that are only applied to specific users or during specific times.

- Users can be used as a criteria for a rule. To enable the Barracuda NG Firewall to be aware of which connection belongs to a specific user, use the Barracuda DC Agent, Barracuda TS Agent, or the The Barracuda NG Firewall Authentication Client.
  For more information, see User Objects.
- You can create firewall rules that are only active for specific times or dates. For example, you can create a time object that only includes Mondays and the hours of 8:00 am to 9:00 am. A firewall rule including this time object allows traffic only during the time span defined in the time object.
  For more information, see Time Objects.

Firewall Objects

Use firewall objects to reference specific networks, services, time and dates, user groups, or connections when creating firewall rules. You can use firewall objects that are preconfigured on the Barracuda NG Firewall or create custom objects to fit your needs. The main purpose for firewall objects is to simplify the creation and maintenance of firewall rules. Firewall objects are re-usable, which means that you can use one firewall object in as many rules as required. Each firewall object has a unique name that is more easily referenced than an IP address or a network range.

For more information, see Firewall Objects.

Layer 7 Application Control (Legacy)

> Barracuda Networks recommends using Application Control 2.0.

Layer 7 Application Control is a legacy feature using Deep Packet Inspection (DPI) and behavioral traffic analysis to detect and classify network traffic based on Layer 7 applications and protocols.

For more information, see Layer 7 Application Control.

Figures

1. FW_Rulesets.png