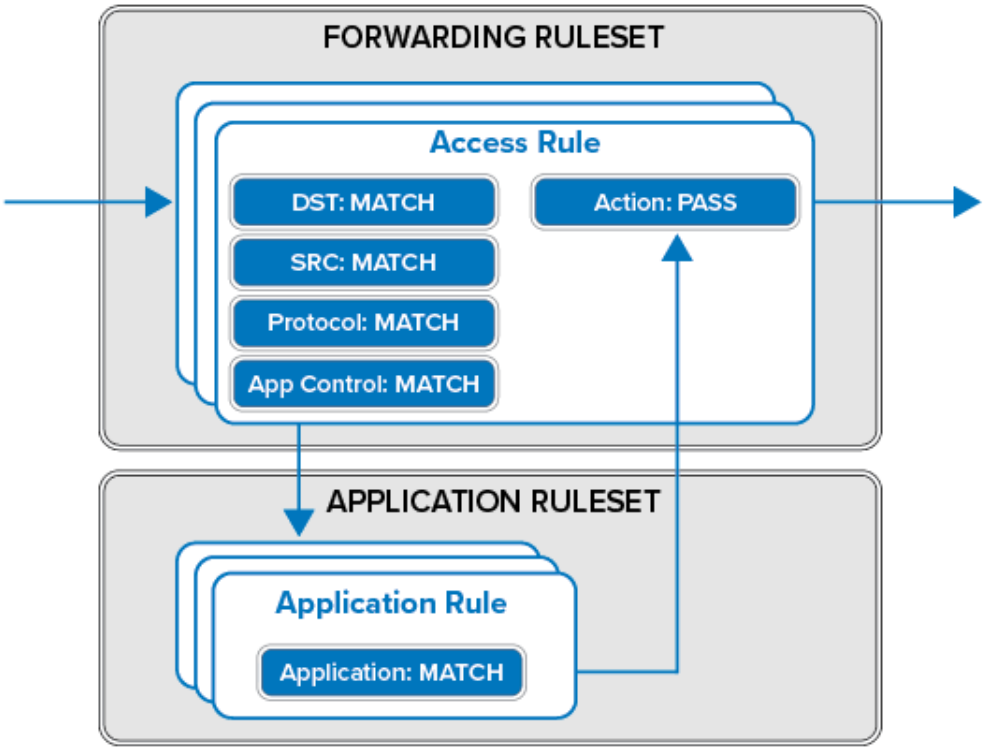
Forwarding Firewall

https://campus.barracuda.com/doc/96026187/

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

- **Firewall Policies**:
  - **Firewall Access Rule Set** – The access ruleset operate on the OSI network layers 3 and 4. The access ruleset contains a list of access rules to filter. 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.
  - **Application Rule Set** – The application ruleset operates on the OSI network layer 7. If Application Control is enabled in an access rule that is executed, the application rule set is evaluated. Application rules allow you to pass or block connections depending on the application type.
- **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.
- **Schedule (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 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 access rule is executed. If none of the rules match, the default BLOCKALL rule blocks the traffic.

For more information, see Access Rules.

Next Generation Firewall Capabilities

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

For more information, see Application Control.

Traffic Shaping (QoS)

You can adjust the QoS band of IPv4 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 access rule.
- Traffic shaping for application traffic can be configured in the application policy rules. For more information, see Application Control.

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 for both IPv4 and IPv6 traffic. 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 CloudGen Firewall. However, you can enable or disable IPS for each firewall rule.

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

Botnet and Spyware Protection

To protect your network against botnets and spyware, the CloudGen Firewall monitors what domains are accesses by the clients in the network. If malicious sites or domains are accessed, not only via HTTP or HTTPS but using any protocol, the client IP, the firewall redirects the traffic to a fake IP address and monitor access to that IP address to identify infected clients.

For more information, see Botnet and Spyware Protection in the Firewall.

Users/Time

For more granular control, you can configure access 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 CloudGen Firewall to be aware of which connection belongs to a specific user, use the Barracuda DC Agent, Barracuda TS Agent, or the Authentication Client.
  For more information, see User Objects.
- You can create access 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 access rule including this time object allows traffic only during the time span defined in the time object.
  For more information, see Schedule 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 CloudGen 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.

Policy Profiles

Policy profiles are centrally managed, (pre-)defined rules for handling network traffic and applications. The Barracuda CloudGen Firewall allows administrators to manage, create, and customize general policies that can then be applied to access rules on Control Center-managed or stand-alone firewall units. You can create SD-WAN policies and security policies to monitor local and forwarding traffic or to allow, block, or customize traffic for detected applications.

For more information, see Policy Profiles.

Figures

1. fwd_fw_rulesets.png

© 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.