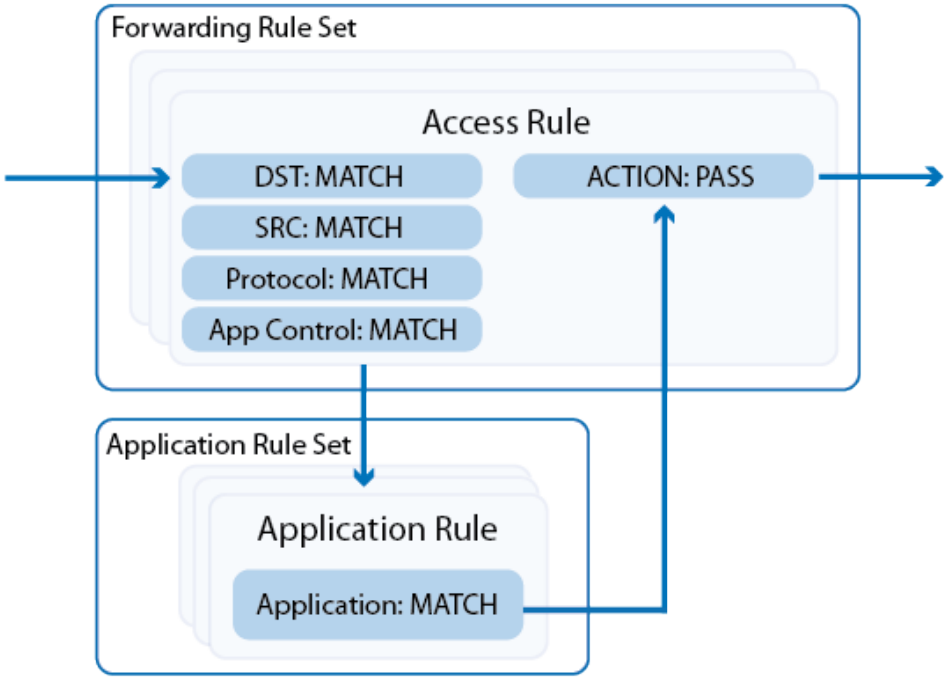
Forwarding Firewall

https://campus.barracuda.com/doc/72516439/

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

- **Firewall Policies**:
  - **Firewall Access Rule Set** – The access ruleset operates 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 ruleset 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 ruleset while next generation application-aware policies are applied in the dedicated application ruleset.



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 ruleset. 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.

Firewall Capabilities

Application Control (with or without SSL Interception), a tightly integrated Intrusion Prevention System (IPS), a URL Filter, File Content and User Agent filtering for content security, and Virus Scanning with ATP in the firewall all 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 the 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 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 firewall to be aware of which connection belongs to a specific user, use the Barracuda DC Agent or Barracuda TS Agent.
  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 a.m. to 9:00 a.m. An 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 preconfigured firewall objects or create custom objects to fit your needs. The main purpose of 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.

Advanced

You can also configure the following advanced firewall settings:

- **Interface Group** – When creating an access rule, you can assign interfaces that the source address is allowed to use. Arriving packets of traffic that match the rule are then processed to the specified network interfaces according to the interface group settings. For more information, see How to Create Interface Groups.
- **SYN Flood Protection** – SYN flood protection protects against a common kind of DoS attack. The firewall can eliminate SYN flooding attacks for inbound or outbound attacks. The firewall completes the handshake and only then performs a handshake with the actual target. This helps to protect the target from SYN flood attacks. Disabling SYN flood protection can cause an overhead in packet transmission, but can speed up interactive protocols like SSH. For optimal protection, SYN Flood Protection needs to know the maximum sessions and the maximum sessions per source IP address that can be opened before the firewall takes measures. In Always On mode, the firewall compares these two values against the current session values, blocks the source IP if one of the two limits is exceeded, and frees the allocated session resources. In Automatic mode, the firewall switches to a different TCP handshake mode to protect the network.

Figures