Application Control

https://campus.barracuda.com/doc/41103472/

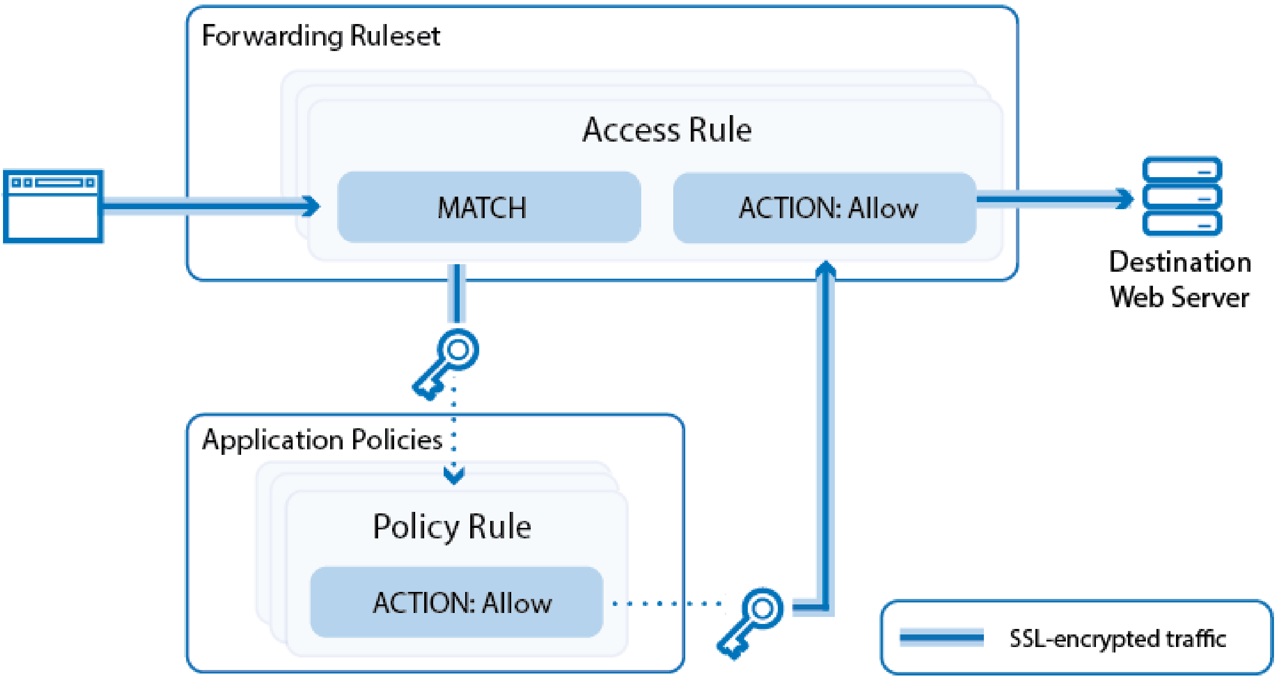
As a powerful next-generation firewall feature, Application Control allows the Barracuda NextGen Firewall X-Series to control application traffic, including sub-applications (e.g., chat function and picture uploading). It includes the following features:

- **Application Policy** – A list of policy rules to detect and control application traffic. You can create rules to drop or adjust the bandwidth of detected applications. Traffic patterns are compared to predefined application objects containing detection patterns to detect the latest applications. The application pattern database is updated with every NextGen Firewall X-Series firmware update. You can also customize application definitions based on previously analyzed network traffic. To classify applications and threats, all application objects are categorized based on risk, bandwidth, or vulnerabilities.
- **URL Filtering** – Based on the Barracuda Web Security Gateway URL category database. The URL Filter uses a large online database to filter according to the URL of the website. The websites are organized into URL categories based on the content of the website. You can use the URL Filter as a whitelist or blacklist. To use the URL Filter, you must have a Barracuda Web Security subscription.
- **SSL Inspection** – Most applications encrypt outgoing connections with SSL or TLS. SSL Inspection intercepts and decrypts encrypted traffic to let Application Control detect and handle embedded features or sub-applications of the main application. For example, you can create a policy that permits the general usage of Facebook, but forbids Facebook chat. If you choose not to enable SSL Inspection, the main applications can still be detected. For example, Facebook can still be detected without SSL Inspection, but you will not be able to determine if the Facebook chat or a Facebook app is being used.

Understanding Application Control

Because applications are either web-based or connect via SSL- or TLS-encrypted connections to servers in the Internet, they can be detected and then controlled as they pass the X-Series Firewall. If Application Control and SSL Inspection are enabled in the firewall rule that handles the application traffic, the traffic is evaluated by the application policies and processed as follows:

1. SSL traffic is decrypted.
2. Application policy rules are processed from top to bottom to determine if they match the traffic. If no rule matches, the default application policy is applied.
3. If a matching application rule is found, the detected application is handled according to the rule settings. The application can be reported, blocked, or restricted by time, bandwidth (QoS), user information, or content (e.g., MPEG).
4. If the traffic was decrypted, it is re-encrypted.
5. The traffic is sent back to the forwarding firewall, which forwards it to its destination.



In this Section:

Figures