Application Control 2.0

https://campus.barracuda.com/doc/41115749/

With Application Control 2.0, you can control application traffic, including sub-applications (e.g., chat function and picture uploading). It includes the following features:

- **Application Rule Set** – Dedicated rule set to detect and control application traffic. You can create rules to drop, throttle, prioritize, or report 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 Barracuda NG Firewall 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 Filter URL category database.
- **SSL Interception** – Most applications encrypt outgoing connections with SSL or TLS. SSL Inspection intercepts and decrypts encrypted traffic to let Application Control 2.0 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 Facebook chat or a Facebook app is being used.
- **AV Scanning** – If AV scanning is activated in a forwarding firewall rule, all matching traffic is scanned for malicious content. You can use Avira and/or clamav scanners.
- **ATD** – If ATD is enabled in an access rule, all matching traffic is scanned for malicious content by the virus scanner and if no virus is found and the file matches the ATD policy, the file is uploaded to the Barracuda Content Security Cloud for scanning.

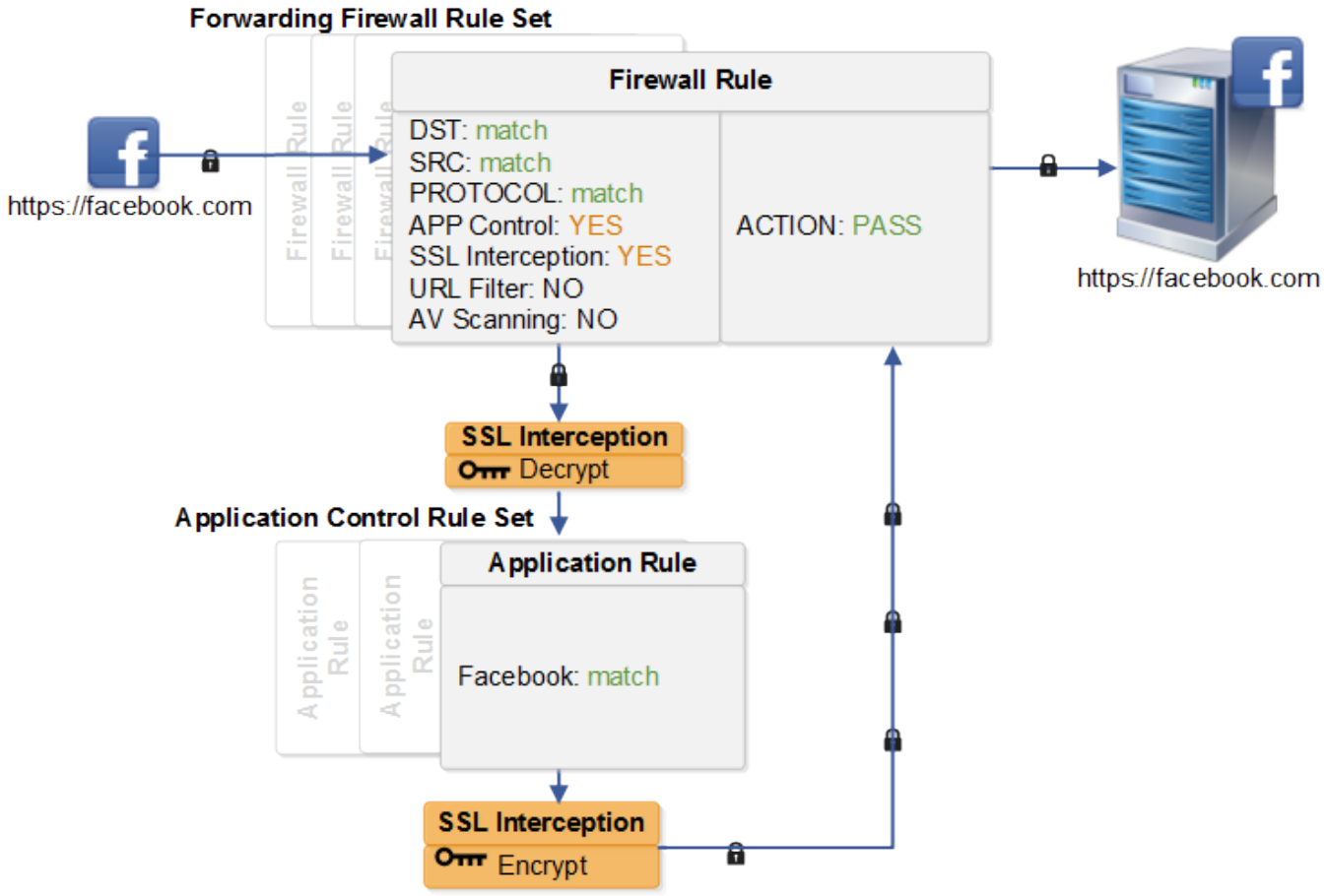
You can use Application Control 2.0 in combination with HTTP(S) proxies. However, the detection of sub-applications might not be available depending on the configuration and type of proxy service. For more information, see Using Application Control 2.0 with HTTP(S) Proxies.

In this article:

Understanding Application Control 2.0

Because applications either are 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 Barracuda NG Firewall. If Application Control 2.0 and SSL Interception is enabled in the forwarding firewall rule that handles the application traffic, then the traffic is sent to the application rule set and processed as follows:

1. SSL traffic is decrypted.
2. Application 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, or it can be 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.



Using Application Control 2.0

Figures

© Barracuda Networks Inc., 2019 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.