Application Control

https://campus.barracuda.com/doc/95258867/

HTTP/S traffic no longer consists of simple HTML websites. The Internet has become an important part of the modern world and provides a wide variety of different web-based applications. However, some of these applications are not business related and can have unwanted side effects, including:

- Opening backdoors into your network
- Distracting people from work
- Consuming business-critical bandwidth

Application Control provides the application ruleset that lets you expand the scope of the firewall engine to include application type as a matching criteria. The addition of application context to the traditional stateful packet inspection capabilities of the CloudGen Firewall gives you full, context-aware control, even for SSL-encrypted traffic. Application Control comes with a set of predefined application objects that contain detection patterns to give you control over the latest web applications, web services, and social media. To give you more granular control, it also detects embedded features (or sub-applications) within applications. For example, you can create policies that permit the general usage of social networks (such as Facebook or Twitter), but forbid embedded applications (such as chat, image uploading, or posting). Application Control is fully integrated into the firewall service. Application traffic can be dropped, throttled, prioritized, or just reported. Application Control for IPv6 is currently limited to application-detection only.

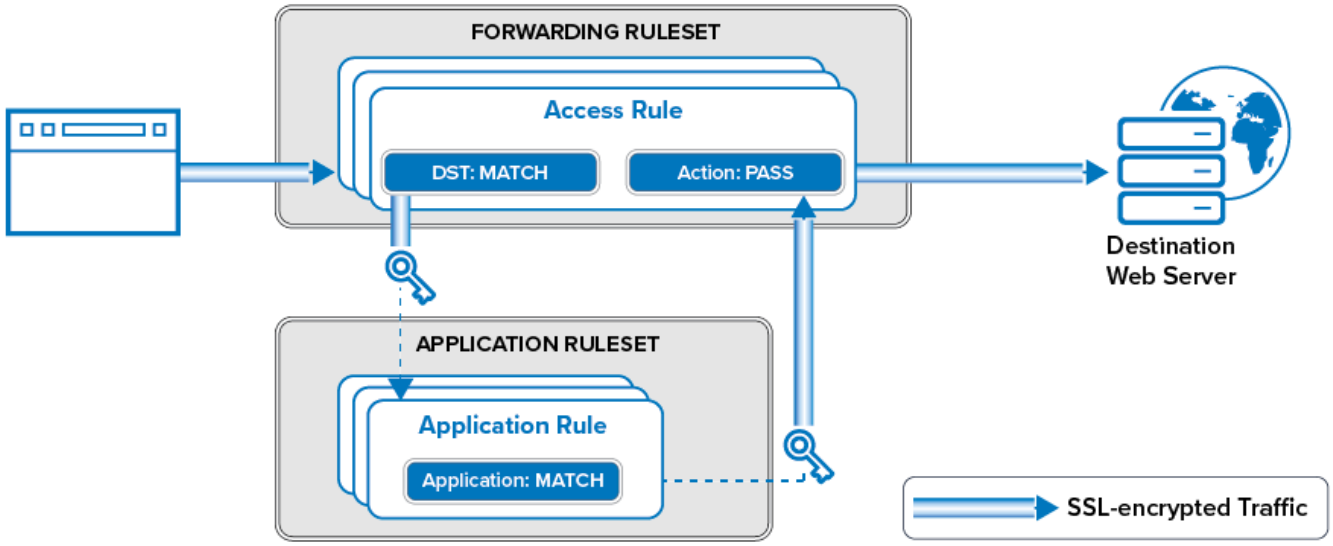
Modern browsers may use HTTP2, SPDY, or the QUIC protocol on UDP 443 instead of HTTP or HTTPS. Disable support for these protocols either directly in the browser, or block UDP 443 on the firewall. The browsers will then automatically fall back to HTTP or HTTPS.

The applications patterns and definitions are stored in the application pattern database. The database is continuously updated through your Energize Updates subscription. You can also add your own custom applications.

Application Ruleset and Application Control

Application Control uses a dedicated ruleset to detect and control application traffic. You can create application rules to drop, throttle, prioritize, or report detected applications and sub-applications. To detect the latest applications, traffic patterns are compared to predefined application objects containing detection patterns. You can also customize application definitions based on previously analyzed network traffic. To classify applications and threats, all application objects are categorized based on their properties, risk rating, bandwidth, and potential vulnerabilities. If Application Control and SSL Inspection is enabled in the Forwarding Firewall rule that handles the application traffic, the traffic is sent to the application ruleset and processed as follows:

1. SSL-encrypted 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.
4. SSL traffic is re-encrypted.
5. The traffic is forwarded to its destination.



For more information, see How to Enable Application Control.

Application Control Features

SSL Inspection

SSL Inspection decrypts both SSL and TLS connections so the firewall can allow Application Control features, such as Virus Scanning and ATP, to scan traffic that would otherwise not be visible to the firewall service. Using SSL Inspection allows the admin to enforce SSL/TLS security at the firewall by blocking outdated ciphers or refusing connections for connections attempting to use outdated SSL versions. For outbound SSL Inspection, the firewall can also handle SSL validation errors, depending on the SSL error policy assigned to the matching access rule of the SSL/TLS session.

Many applications transmit their data over connections encrypted with SSL or TLS. SSL Inspection intercepts and decrypts encrypted traffic to allow Application Control to 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, but the firewall does not differentiate between individual

features, such as Facebook chat or Facebook games.

For more information, see SSL Inspection in the Firewall.

URL Filtering

Websites accessed by the users are categorized based on the Barracuda Web Filter URL category database. Depending on the policy assigned to this URL category, the website can then be allowed, blocked, or allowed temporarily. You can create either an allow list (blocking everything except for selected sites) or a block list (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 domain of the website. It does not offer control over subdomains, or subdirectories of the website.

For more information, see URL Filtering in the Firewall.

Virus Scanning

Network traffic can be transparently scanned for malicious content while the traffic passes through the firewall. The Virus Scanner service includes two virus scanning engines: Avira and ClamAV. If a user downloads a file containing malware, the CloudGen 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 type of files to be scanned.

For more information, see Virus Scanning and ATP in the Firewall.

Advanced Threat Protection (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 Virus Scanning and ATP in the Firewall and Advanced Threat Protection (ATP).

File Content Scan

The Barracuda CloudGen Firewall can filter transmitted files depending on their file type, name, or MIME type. Network administrators can decide on a granular level what files are allowed to traverse the firewall.

For more information, see File Content Filtering in the Firewall.

User Agent Filtering

User Agent policies allow you to control access to a web-based resource based on the user agent string. The information contained in the user agent string allows you to create policies based on web browser / operating system combinations or to define generic patterns for more specific filters.

For more information, see User Agent Filtering in the Firewall.

Mail Security

Check the source IP address of incoming SMTP(S) connections against a DNSBL and modify the header and subject of the email if the sender is listed in the DNSBL.

For more information, see Mail Security in the Firewall.

SafeSearch

Enforce SafeSearch on Google, Bing, Yahoo, and YouTube.

For more information, see How to Enforce SafeSearch in the Firewall.

Google Accounts

Block all Google accounts (personal and G Suite) except for accounts in the allow-listed G Suite domains.

For more information, see How to Configure Google Accounts Filtering in the Firewall.

Application Control with HTTP Proxies

You can use Application Control in combination with HTTP(S) proxies. Depending on the configuration and type of proxy service, the detection of sub-applications may not be available.

For more information, see Using Application Control Features with HTTP(S) Proxies.

Figures

1. app_ctrl_overview.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.