Understanding Data Access

https://campus.barracuda.com/doc/79466797/

When you enable Barracuda Active DDoS Prevention, you route your application traffic through Barracuda. This article explains the access Barracuda has to your application data and the measures Barracuda takes to ensure your data remains confidential.

For more information on traffic flow with Active DDoS Prevention, see Understanding Service Architecture with Barracuda Active DDoS Prevention.

HTTP and HTTPS Services

When you set up a service using the unencrypted HTTP protocol, your application's traffic is sent – unencrypted – over the public Internet. Anyone with access to that traffic can see everything, including passwords or personally identifiable information. You can use the Instant SSL feature on your Web Application Firewall to quickly encrypt traffic.

> Never use unencrypted HTTP for services that send or receive any personally identifiable or confidential information.

Normal Operation

Although all your application traffic is routed through Barracuda so Barracuda can perform DDoS mitigation, during normal operation, Barracuda does not decrypt your application traffic, and does not have access to any of the potentially confidential information your application transmits or receives to or from your users. The encrypted channel is established directly between your users and your Web Application Firewall.

When Under Attack

When Barracuda detects a DDoS attack, it automatically deploys mitigations to ensure your application is not affected. For more information, refer to Understanding Operating Modes.

For some attacks, Barracuda will intercept requests to your application in the Barracuda Cloud Scrubbing Center and respond to the client with a *challenge*. This helps Barracuda differentiate

between attackers and legitimate users of your application. Attackers will be blocked and legitimate clients will be allowed to access your application.

When intercepting a request, Barracuda will decrypt the request from your user, meaning Barracuda will have access to any data sent by the user with that request. Barracuda only decrypts the request to challenge the client to determine if it is a legitimate user. After the client is determined to be a legitimate user, that data is immediately discarded and no more requests from that user are decrypted. The decrypted data is not logged or stored.

As stated above, only the first request from a client is ever intercepted. Confidential or personally identifiable information (PII) is not likely to be contained in this request, because users will typically first load a login page or other form before submitting data. Even if confidential information is included in the request, it is immediately discarded by Barracuda and is not logged.

Barracuda will never decrypt responses from your application to your users and will never see any potentially confidential data you send to your users.