Subject: Request for Assistance: Investigating SameSite Attribute for F5 BIG-IP Persistence Cookie

Dear Load Balancer Team,

Hope you're doing well.

We are currently investigating an issue with our vendor-created hybrid mobile application (specifically the Android version) which is experiencing HTTP 401 Unauthorized errors. The application uses a bank-authored webcomponent that communicates with our bank's middleware (SSP), and session affinity for these interactions is managed by an F5 BIG-IP load balancer using a persistence cookie.

Observations & Context:

During our investigation, we've observed that the F5 BIG-IP persistence cookie doesn't appear to have an explicit SameSite attribute set. We'd like to explore if this might be a contributing factor to the issues we're seeing on Android.

Our understanding is that on our Android hybrid app (especially for versions targeting Android 12/API 31+), the Android WebView defaults to treating cookies without a SameSite attribute as SameSite=Lax.1 Since the Cordova application often loads content from a file:/// or custom scheme origin, requests from the webcomponent to the bank's SSP are considered cross-site. If the F5 persistence cookie is indeed treated as SameSite=Lax in this context, it might not be sent with these cross-site API requests, which could potentially lead to broken session affinity and the HTTP 401 errors.

Additionally, we are looking ahead to potential future impacts on our iOS application. There are indications that upcoming changes in iOS 18 may lead WKWebView to also default to SameSite=Lax for cookies lacking an explicit attribute.3 Addressing this proactively would be beneficial.

Request for Your Expertise & Assistance:

To help rule out a potential cause and to ensure robust future compatibility, we would greatly appreciate it if you could check the current configuration of the F5 BIG-IP persistence cookie.

If it's found that the SameSite attribute is not explicitly set, we would like to request your assistance in configuring it to include SameSite=None and Secure. We understand this is often implemented via an iRule.5

Setting SameSite=None would allow the cookie to be sent in the necessary cross-site context from our mobile applications, and the Secure attribute is mandatory for SameSite=None, ensuring the cookie is only transmitted over HTTPS.7

We believe that ensuring the SameSite attribute is explicitly set could be a key step in resolving the current Android issue and in preemptively addressing potential future changes in iOS.

Please let us know if this is something your team can investigate and if you require any further information from our side. We are, of course, available to discuss this in more detail at your convenience.

Thank you for your time and assistance.

Best regards,