See. Control. Secure.

Zero-Rated Apps Fraud Mitigation

Solution Use Case Overview

May 2025

Use-Case Overview: Zero-Rated Fraud Mitigation

The Use Case

Detection and prevention of fraud and abuse of zero-rated applications, free domains, and network protocols.

Value Proposition

Allot Smart Fraud Detection and Prevention solutions empower CSPs to prevent revenue leakage caused by fraud, employing zero-rated applications, free domains, and network protocols to bypass charging systems and avoid paying for data consumption.

Problem Statement

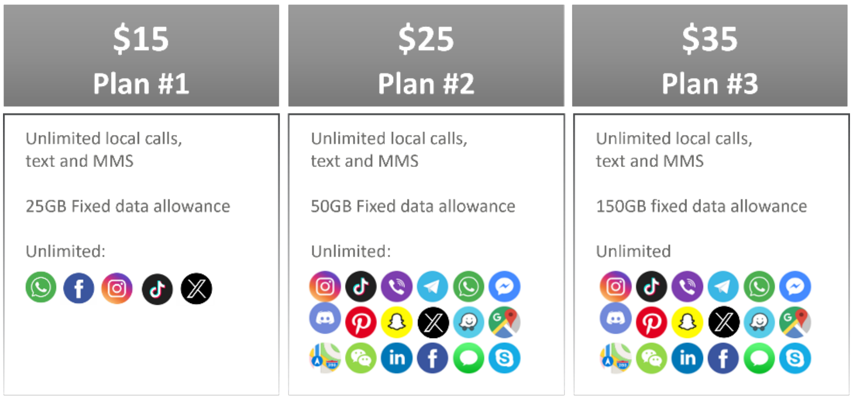
Operators worldwide are looking for ways to boost revenues with differentiated services to cope with the intensifying competition and price pressure. A widely employed offer includes special pricing for popular apps, such as social network applications like Facebook, WhatsApp, Instagram, etc. Another offering is free access to specific websites, including their operator portal, brand website, or business partners' websites, such as banks, entertainment websites, etc.

As those service plans gain traction, fraudulent users exploit the loopholes in the data charging systems, abusing zero-rating and avoiding payment for the corresponding data consumption.

Although only a small percentage of subscribers engage in data charge bypass fraud, it can account for significant network traffic and lead to substantial revenue loss over time.

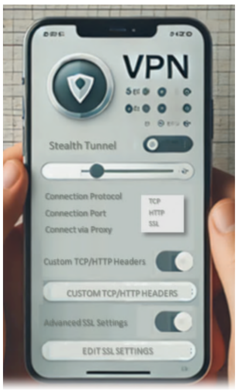
For instance, prepaid users may use their remaining credit while consuming more data than they have purchased, avoiding recharging their accounts. Similarly, postpaid users might subscribe to a lower-cost service plan and consume more data than their plan allows

For example, a customer with service plan #1 can pay $15 and consume more data than the 25GB allotment by masquerading the traffic as "WhatsApp zero-rated traffic."



$15 Plan #1	$25 Plan #2	$35 Plan #3
Unlimited local calls, text and MMS	Unlimited local calls, text and MMS	Unlimited local calls, text and MMS
25GB Fixed data allowance	50GB Fixed data allowance	150GB fixed data allowance
Unlimited:	Unlimited:	Unlimited

Figure 1 - Example of Tiered Service offering with Zero-rated apps



Fraud Technique: Zero Rating Abuse

Multiple fraud schemes are based on manipulations applied to the content delivery process to disguise the traffic as either special-rating application traffic or zero-rating domain traffic. VPNs and anonymizer apps can facilitate such fraud by leveraging capabilities like IP address spoofing and SNI field manipulation.

Figure 2 - Illustration of VPN application settings

For example, a fraudulent user might abuse a "Facebook zero-rating" service plan by utilizing a VPN that disguises the traffic and makes it look like Facebook traffic by modifying the SNI to "Facebook" while sending the traffic to the VPN server.

Another example is abusing free access to specific websites (URLs) by disguising fraudulent user traffic as zero-rated website traffic.

Similarly, fraudulent users may try to bypass charging by tunneling their traffic through zero-rated network protocols like DNS or ICMP. This fraud may be executed with DNS tunneling applications.

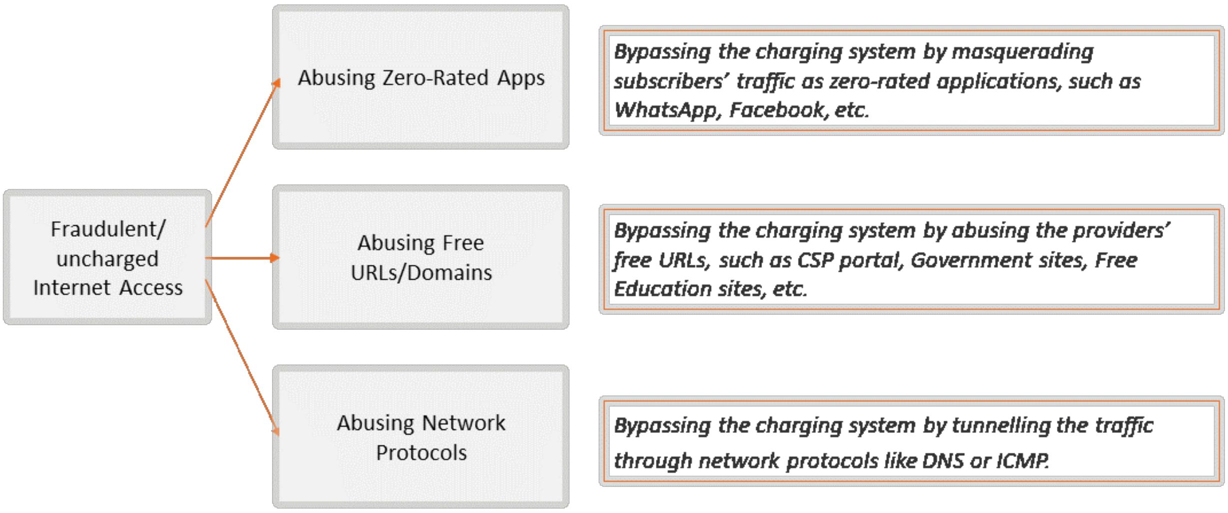

Fraudulent/ uncharged Internet Access
Abusing Zero-Rated Apps
Abusing Free URLs/Domains
Abusing Network Protocols
Bypassing the charging system by masquerading subscribers' traffic as zero-rated applications, such as WhatsApp, Facebook, etc.
Bypassing the charging system by abusing the providers' free URLs, such as CSP portal, Government sites, Free Education sites, etc.
Bypassing the charging system by tunnelling the traffic through network protocols like DNS or ICMP.

Figure 3 - Main charging fraud schemes

The VPN applications used for the above frauds are available on the App Store and the Google Play Store. Some of them are very powerful and simple to use. Information on executing the scam can be easily found on the Internet. CSPs need a solution to identify this fraudulent activity and stop revenue leakage.

Allot Smart Fraud Detection and Prevention Solution

The Allot SmartPCC solution enables the detection and prevention of frauds that intend to take advantage of zero-rating applications, free domain access, and network protocol access in several ways. Fraud prevention is based on granular application detection capabilities, policy enforcement, and advanced analytics capabilities.

The primary fraud detection and prevention mechanisms are summarized in the following figure:

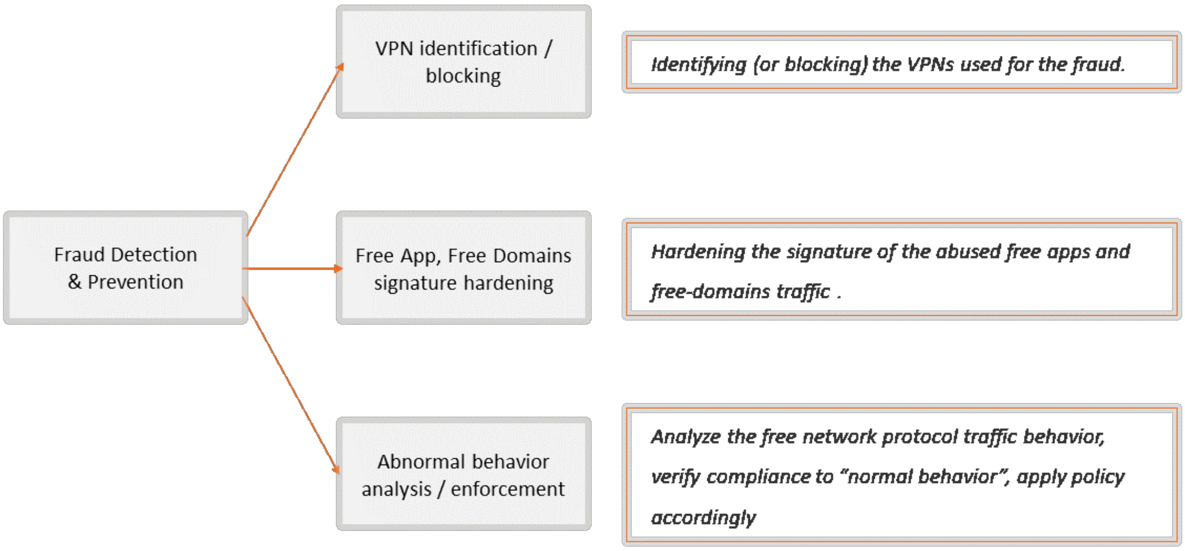

Fraud Detection & Prevention
VPN identification / blocking
Identifying (or blocking) the VPNs used for the fraud.
Free App, Free Domains signature hardening
Hardening the signature of the abused free apps and free-domains traffic .
Abnormal behavior analysis / enforcement
Analyze the free network protocol traffic behavior, verify compliance to "normal behavior", apply policy accordingly

Figure 4 - Primary fraud detection and prevention mechanisms

1. Allot's solution protects against the misuse of zero-rated applications, free websites/URLs, and free network protocols by comprehensive identification capabilities of VPN and anonymity applications used for this fraudulent purpose. Allot solution identifies many VPNs, which are commonly used for zero-rating abuse. When VPN is identified, the traffic is classified as VPN traffic and not as zero-rated application traffic, solving the revenue leakage.

   The VPN signatures are constantly updated to cope with rapid changes in VPN applications. There is an option to get a fast update for the signature protocol pack to ensure immediate updates in reaction to VPN changes.

2. Allot DNI (Deep Network Intelligence) offers an option for signature hardening for free applications and domains to prevent zero-rating misuse. It adds the server IP address and/or Autonomous System Number (ASN) criteria as a precondition for traffic classification as a zero-rated application or website traffic. It eliminates the potential manipulation executed by VPN/Anonymizer applications since it requires matching of both SNI and server IP address/ASN to classify traffic as zero-rated.

3. Allot facilitates comprehensive analytics reporting, which enhances fraud detection and prevention capabilities. Analysis of zero-rated application usage per subscriber can be utilized to provide alerts when the traffic of a specific zero-rated application exceeds a certain level beyond a reasonable volume.
   For example, to identify possible fraud based on network protocol abuse (e.g., DNS and DHCP) or zero-rated applications (e.g., WhatsApp), Allot offers detailed visibility into the traffic generated per subscriber, network protocol, and application.
   Network protocols consume a very small amount of data; thus, their abuse can be easily detected via consumption analysis. To prevent the abuse of network operation protocols, like DNS and ICMP, the bandwidth of those applications can be throttled, and they can be blocked when their consumption exceeds a certain level beyond a reasonable volume for such traffic.

   Similarly, Allot allows operators to track the data consumption of zero-rated applications or websites per user to identify extreme usage that may indicate fraud.

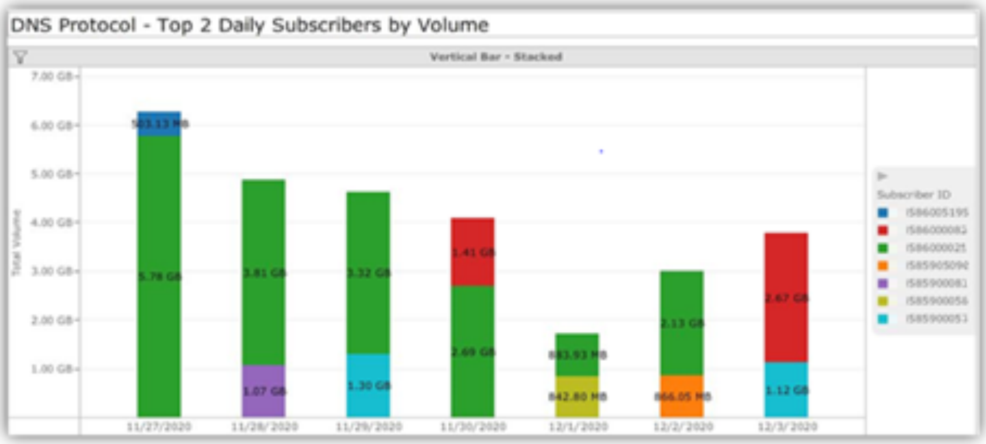


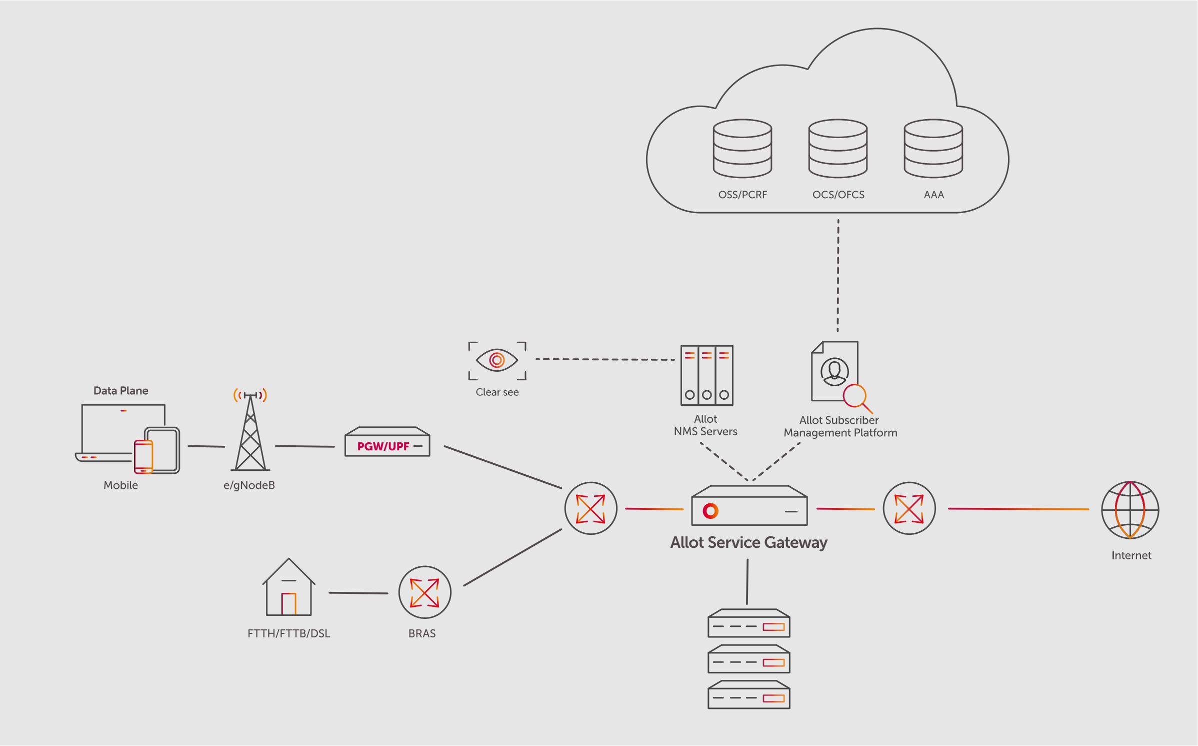
Figure 5 - Network Analytics of Top DNS protocol consumers by volume

Benefits

- Identify fraudulent activity
- Assure revenue per actual usage
- Prevent/block revenue leakage
- Close loopholes in charging differentiated services

Implementation

The solution integrates seamlessly with existing network infrastructure, offering a flexible and scalable approach to traffic management and QoE enhancement without significant upfront investment.



About Us

Allot stands at the forefront of network management innovation, empowering communications service providers (CSPs) with cutting-edge, cost-effective solutions. Our SmartTraffic QoE Management solution exemplifies our unwavering commitment to excellence and customer satisfaction in telecommunications. But we're not just about solving today's challenges; we're future-focused, ensuring our partners stay ahead in a dynamic digital world. Join us in redefining connectivity, where every solution is designed with your success in mind.

Learn more about us at **ALLOT CORPORATE**.