allot
See. Control. Secure.

Success Story

Global CSP

Global CSP Grabs Mobile Data Market-Share with Zero-Rated Apps

About the Global CSP

This global communication service provider (Global CSP) operates mobile networks in numerous countries spanning multiple continents where mobile infrastructure often outpaces or eclipses fixed network infrastructure. To date, approximately 90% of their market comprises prepaid customers and 10% are postpaid.

Challenge

Prepaid users are price-sensitive consumers and often have a high churn rate. To combat this, the Global CSP innovated by introducing packages that bundled prepaid usage allowances with unlimited (i.e., zero-rated) use of popular social apps such as Facebook, WhatsApp, Line, and Twitter.

They were able to do this by using existing deployed Allot Service Gateways which monitor each free application and zero-rates its bandwidth consumption in real time so that it is not charged against the customer's prepaid data allowance. In fact, zero-rated apps can still be used, even when the data allowance is used up.

As the "Free Social" prepaid plans gained traction, the global CSP noticed discrepancies in actual usage vs billed usage reports. The findings indicated that some customers who had used up their prepaid data allowance were still accessing the Internet free of charge. In some countries, the discrepancy was more than 10% of usage volume, which translated to revenue loss of hundreds of thousands of dollars per month. The global CSP needed to find out why this was happening and stop the revenue leakage.

Vertical	Service Provider
Industry	Mobile
Region	LATAM
Solution	Policy Control & Charging

Challenge

- Differentiated prepaid services with per user visibility
- Revenue leakage caused by fraudulent use of zero-rated services
- Need for an engaging migration path to postpaid services

Solution

The operator deployed an Allot Service Gateway Tera at critical network junctures in each country to monitor and enforce charging policy per user and per application. By enhancing their ability to monitor traffic, the Global CSP could offer prepaid plans featuring zero-rated (or unlimited browsing) applications such as Facebook, which enabled them to capture more market share and convert more customers to similar postpaid service packages.

Benefits

- Preventing fraudulent zero-rated domain forging and captive portal domain forging
- Allowed the CSP to offer lucrative zero-rating inclusive packages which built customer loyalty
- Higher loyalty enabled conversion to postpaid plans at competitive price points

Solution

By utilizing Allot Smart Data Source to extract usage data in a focused investigation, they discovered why the redirect to captive portal wasn't working as expected. Some users were engaging in fraudulent practices that enabled them to bypass the data top-up and other terms of use.

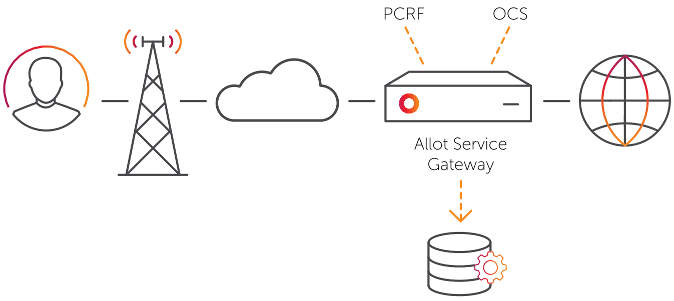
The first tactic is known as captive portal domain forging. When prepaid data allowance is used up, customers are redirected automatically to a captive portal where they can buy more data. Redirection to a captive portal requires permission for operational protocols such as DNS, ICMP, and DHCP as well as the portal itself to be accessed by the prepaid user. Customers were taking advantage of this permission policy in two ways: either to tunnel traffic through the permitted protocols, or to forge their domain to be the operator captive portal using an IP proxy so they could "fool" the system and bypass data charges.

> Allot's comprehensive Policy Control and Charging solutions enable new revenue streams from application-based services and prevents revenue leakage caused by fraudulent use of services. The result, a differentiated service that increases prepaid customer loyalty and ARPU"
>
> Director of Marketing,
> Global CSP LATAM

Allot's solution combats this activity in two ways:

- Captive portal function to validate redirected traffic and verify the destination IP
- Bandwidth limitation on DNS/ICMP/DHCP/Windows OCSP protocols to prevent the fraudulent tunneling.

The second tactic is known as zero-rated domain forging. Users of the operator's prepaid "Free Social" plans are redirected to a dedicated portal where they can access a limited set of Facebook features called "Free Basics." Some customers were using VPN anonymity tools to spoof the domain of the destination host in the HTTP header, making it look as if they were going to the Free Basics domain. Allot's Service Gateway can assign User Defined Signatures to validate the host and referrer in the HTTP header. Allot policy blocks VPN and anonymity applications being used for fraudulent purposes.



Central management and real-time charging are provided by Allot NetXplorer and Allot Subscriber Management Platform (SMP) respectively as the final elements of our comprehensive PCC solution for the operator.

Benefits

Allot's comprehensive policy control and charging solutions enable the global CSP to reap important business benefits every day as it:

- Differentiates prepaid services and revenue
  The global CSP's ability to offer zero-rating on one, few, or many applications, made its prepaid service more attractive than competing plans, increasing prepaid service uptake and loyalty.
- Stops revenue leakage
  The global CSP countries save hundreds of thousands of dollars per month in revenue leakage, which over time, could have increased to even greater losses with a significant impact on profitability.
- Fosters a prepaid-to-postpaid migration path
  Fast uptake of prepaid application-based services enabled the global CSP to advance its goal of growing the customer relationship and migrating prepaid users to postpaid plans that also offer zero-rate applications at competitive price points.

Resources

About Policy and Charging Rules Function

About Policy and Charging Enforcement Function

Learn more about
Allot's Solutions »

Aug 2019