

NATIONAL MOBILE OPERATOR

SECURES MOBILE DATA TRAFFIC WITH CROSSBEAM

PROJECT GOALS:

Prepare for the continued mobile data traffic explosion - more users, more smartphones, more data traffic per user - with an incrementally scalable cost-effective solution

Secure the GSM interface to the Internet, and partner network and other internal interfaces (Gi, Gn, and Gp interfaces) with best-of-breed firewalls

Eliminate overbilling errors as a result of malicious exploits that were having a detrimental financial impact

Provide continuous availability to monitor and firewall traffic despite failures within the platform or across paired datacenters

BUSINESS CHALLENGE

Despite already significant market share in their national markets, each operator is seeking to grow their installed base. This growing number of users is also increasingly generating a soaring volume of mobile data traffic, propelling projections that smartphone sales will continue to double, and continue to outpace computer and notebook sales. The incremental revenue from data services is essential for growth, but necessitates expansion of the mobile network to accommodate these services and improve data speeds. Their desire to differentiate themselves with a superior network as users increasingly use smartphones to access social media sites has become increasingly difficult.



ABOUT THE COMPANY

This case study is a composite of many mobile operators, each operating a GSM network today, and each planning and starting implementation of a HSPA+ or LTE network.

Due to this exploding data traffic growth, they were looking for a highly scalable network security solution to support and protect the data traffic increasingly generated by their users. As part of updating and consolidating their security capabilities, they also wanted to avoid attacks that could target their billing systems or internal corporate network. One example is overbilling errors result after perpetrators maliciously make expensive calls in order to fatten the bank account of various intermediary sites. Often the calls happen in the background or at times when the user doesn't realize their phone is doing something. These exploits continue to evolve and now impact SMS and data traffic, such as sending messages to subscribe the victim to premium SMS numbers, and then deleting any incoming registration confirmations or fee consumption messages from the mobile operator, so users can only detect this scam by checking their bills, causing the operator considerable costs to remediate and credit customers.

CASE STUDY

Each operator was cautious to eliminate overbilling errors, but were cautious about adding complexity to their data centers. The objective became simplifying their network operations while improving security within their mobile network. These mobile operators wanted to monitor traffic for known malicious websites on both the Gi interface between the GSM network and the Internet, as well as the Gn interface within the core, and prevent infiltration of malicious traffic to mobile devices. They also wanted to protect its mobile network from partner's customers when they roam on their mobile network and traverse the Gp interface.

The backbone of these mobile operator's network is a series of datacenters or points of presence, each one covering a customer region. Due to the substantial growth they expect to experience, they initially investigated expanding the capacity of the firewalls on the Gi interface from 20 to 40 Gbps, but they also needed support for 10 million concurrent connections. Protection of the Gp perimeters was also important, as these firewalls had been logically turned off - permitting all traffic - generally because older products could not perform adequately. Due to the problems with overbilling attacks they also wanted a firewall to protect the Gn interface in the network core, meeting the same performance requirements as the Gi interface.

"We are anticipating a surge in demand for data services. To strengthen our leadership in the booming market we want to be ready for these soaring data volumes as well as secure the network from threats without needing to reduce security when traffic spikes. We need network security that is continuously available"

SOLUTION

They had a detailed profile of their network traffic on each interface, and had explicit performance expectations relative to throughput, connections per second, and policies they wanted enforced. Most important, they wanted the solution to scale up as their data traffic scaled. They chose Crossbeam X-Series Platform with Check Point firewalls after extensive performance and availability testing.

Each mobile operator typically tests out the Crossbeam X-series, and then implements up to three firewalls: Check Point Security Gateway with the High Concurrent Connections feature on the Gi interface, and Check Point Gx for Mobile Operators on the Gp and Gn interfaces. These 3 firewalled interfaces - Gi, Gp and Gn - were all installed in the same chassis initially and then typically add more X-series as needed. The Crossbeam approach proved to be very cost-effective and energy-efficient, without the need for clusters of appliances. Unlike competitive solutions, the Crossbeam solution afforded each mobile operator scaling beyond 40 Gbps per chassis.

Equally significant, the Crossbeam X-Series offers redundancy across the datacenters. Each datacenter has one SBHA (Single Box High Availability) chassis providing application processing across a series of modules within one modular chassis. They set up the datacenters to work in pairs, so that in the unlikely event that one datacenter fails, the mobile traffic is transferred to the alternate datacenter in the pair.

Key to implementation of the solution was willingness to demonstrate the scalability that they needed.

In the end, the results exceeded their expectations, including:

- A single consolidated platform - firewalling the Gi, Gp, and Gn interfaces with a single chassis per site
- Support for than 10 million concurrent connections
- 20-120 Gbps throughput, such as UDP 512 or other realistic traffic measurement. Scaling to meet traffic peaks confidently.
- Active-Active with Single Box High Availability
- Redundancy to 7 9's
- A solution that is far easier to manage than clusters of appliances
- Future scalability to meet performance needs, as well as implement additional applications such as an intrusion prevention solution

Crossbeam has enabled them to meet the needs of their mobile data users, and incrementally scale network security solution without needing to turn off security capabilities to meet performance needs as was previously necessary. With the ability to scale and support more users, more smartphones, more data traffic, and to protect against more attack vectors, Crossbeam has become essential for their network security.

ABOUT CROSSBEAM

We improve the sophisticated networks of enterprises, government agencies, and service providers by architecting platforms that are more adaptable, high-performing, reliable, and secure.