MEA
Middle East Airlines - Air Liban

Customer

Middle East Airlines, Lebanon

Requirements

- Rapid, real-time protection from DDoS attacks
- Clean traffic re-routing through secure GRE tunnel
- Active filtration system to block malicious bots and scripts
- Central policy management to set clear boundaries for traffic

Solution

BlockDOS Web Application Firewall and secure GRE tunnel protects entire infrastructure of MEA from malicious threats online and makes sure compliance goals are met.

Bottom Line

- MEA infrastructure is now completely secure against DDoS attacks.
- The application layer attacks are countered through Web Application Firewall (WAF).
- Through clean pipe network implemented via GRE, only clean traffic enters the network.

Overview

Middle East Airlines – Air Liban S.A.L., more commonly known as MEA, is the national flag-carrier airline of Lebanon, with its head office in Beirut, near Beirut Rafic Hariri International Airport. It operates scheduled international flights to Asia, Europe, the Middle East and Africa from its base at Rafic Hariri International Airport.

The Business & Technical Challenge

As the national airline of Lebanon, Middle East Airlines processes countless tickets online every second. In order to support its multitude of operations, the airline had deployed a secure IT network consisting of several backup servers, load balancers and dynamic firewalls (both software & hardware). Running this network on US Internet Networking and later ServerBeach, everything was going perfect until the website came under an array of massive DDoS attacks. These attacks were geographically distributed and consisted of several botnets hitting their network with series of Syn flood and Application Layer7 attacks.

As a result of the attacks, the e-ticketing system went offline causing disruptions and delays to passengers all across Lebanon and internationally. The backup servers kept bringing the service up momentarily thanks to IP failover mechanism instilled in the proprietary infrastructure MEA had laid however the continuous DDoS attacks made sure the service was continuously disrupted. The scale of DDoS attack was so large and the volume of traffic was so massive that the security system was overloaded. This caused great panic and the management had a decision to make regarding permanent resolution. They needed to find a protection service that could give them complete protection against Layer7 attacks, preventing which is really not a strong suite of majority of DDoS protection providers in the market.

The Solution

After much deliberation due to sensitivity of the situation, MEA contacted BlockDOS primarily due to our solid market reputation in providing total protection against complex Distributed Denial of Service (DDoS) attacks. BlockDOS's security infrastructure is based on highly protected redundant network environment carefully structured to maximize system uptime. Our rapid protection leverages Border Gateway Protocol (BGP) routing to shield critical network infrastructure from similar large-scale protocol-based DDoS attacks executed directly or through DNS/MX attacks. The solution secures all core services from DDoS attacks including direct-to-IP attacks.

As soon as BlockDOS protection took over MEA's core infrastructure, all the traffic was re-routed from MEA's ISP to highly sophisticated secure network of BlockDOS. Within minutes, all incoming traffic towards IP ranges of MEA was moving towards BlockDOS for thorough inspection and rapid filtering. Once the legitimate traffic was filtered out, it was passed through a secure GRE tunnel towards MEA web services.

Moreover, MEA opted for complete Cloud Security which is offered through our Web Application Firewall (WAF). All the traffic passing through WAF is closely monitored and only clean traffic is allowed to access the network infrastructure by following a set of custom rulesets which define which traffic is to be allowed access to the web services. This cuts malicious traffic, bots and application layer attacks thereby patching up vulnerabilities against common web exploits and ensuring a far greater uptime than ever before.

“We hope and look forward to move ahead with greater strength and capability to safeguard our clients from malicious DDoS attacks and other security threats,” said A. J Rana, General Manager of BlockDOS in a press release. In addition to this, Mohammad El-Hout, Chairman & Director General Middle East Airlines stated: “When the Board of Directors took office in early 1998, it set for itself goals that can be summed up as building an airline that would be a source of pride for passengers, for the Lebanese, and for MEA employees. After 15 years, we were able to achieve these goals by implementing a restructuring plan, reviewing the network, and increasing the level of service.”

Results and Benefits

BlockDOS is now an integral part of MEA's security infrastructure. By using BlockDOS's secure network infrastructure, MEA received the following benefits:

- Automatic protection from diverse threats, with strong default rule sets and extensive customization providing Layer 7 protection that is fully integrated with DDoS mitigation
- Lightning-fast 0.3 ms processing times with instant global updates
- Cost-effectively fulfill PCI compliance by utilizing BlockDOS's WAF
- Prevention from SQL injection, comment spam, Cross-site scripting (XSS), Distributed denial of service (DDoS) attacks and Application-specific attacks.
- Lightning fast performance through geographically distributed network endpoints

BlockDOS's highly skilled technical engineers are available 24x7x365 to make sure clients are served round-the-clock.