

Security

DDoS Protection



Detect and Block Large-Scale Network Traffic Attacks

DDoS Protection service detects and blocks DDoS (Distributed Denial of Service) attacks, which cause service failure by creating a high volume traffic. Protect Samsung Cloud Platform's internal servers by detecting and blocking external traffic attacks through a 24/7 automated detection system. In the event of a DDoS attack, the availability of web services is ensured by minimizing the traffic load of servers in the Samsung Cloud Platform through the means of blocking attack traffic.



Prompt Detection

In case of large inbound traffic, real-time detection of DDoS attacks is provided. Continuous updates on DDoS defense mechanisms allow staying on top of the latest attack tactics.



Effective Blocking

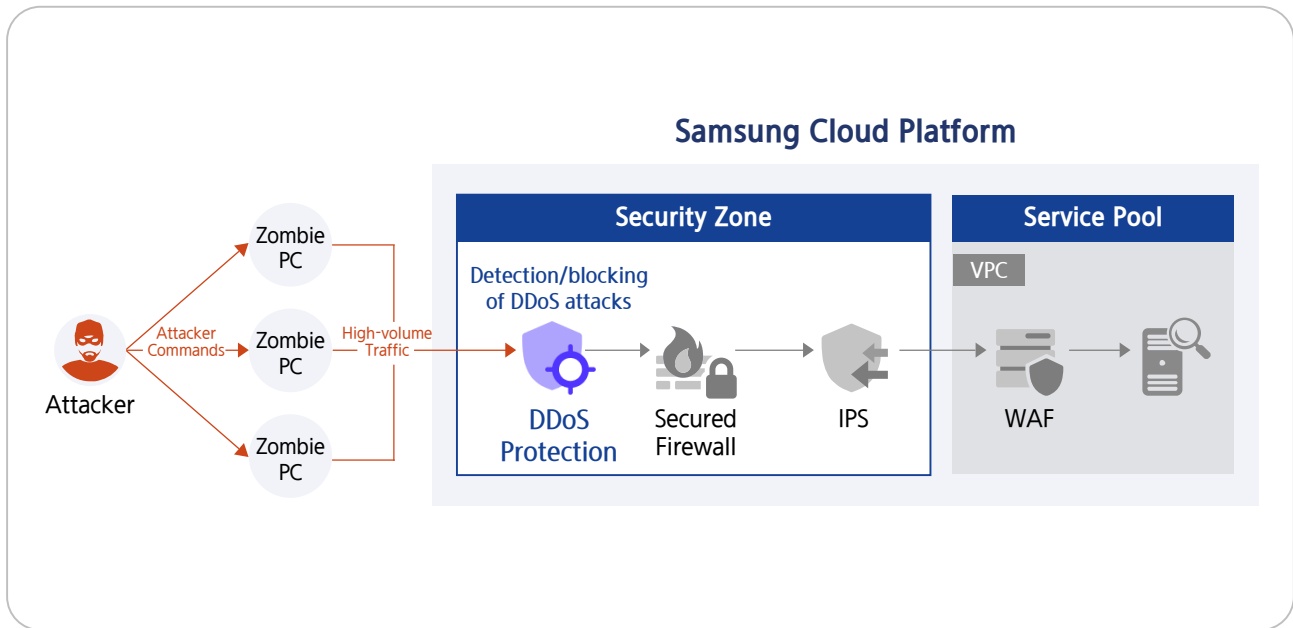
Real-time DDoS attack detection and attack traffic blocking can ensure service availability and allow legitimate users to access the website.



Reliable Web Service Operations

Based on experience operating large-scale networks, DDoS Protection provide defense systems optimized for the latest types of DDoS attacks.

Service Architecture



Key Features

- **Automatic DDoS attack detection**
 - Detect abnormal heavy traffic to identify DDoS attacks
- **Blocks L3 and L4 attacks**
 - Detects and blocks various DDoS attacks at the L3 or L4 layer using a learning-based approach

SAMSUNG SDS

 www.samsungsds.com / cloud.samsungsds.com
 contact.sds@samsung.com / scp_sales@samsung.com
 youtube.com/samsungsds

