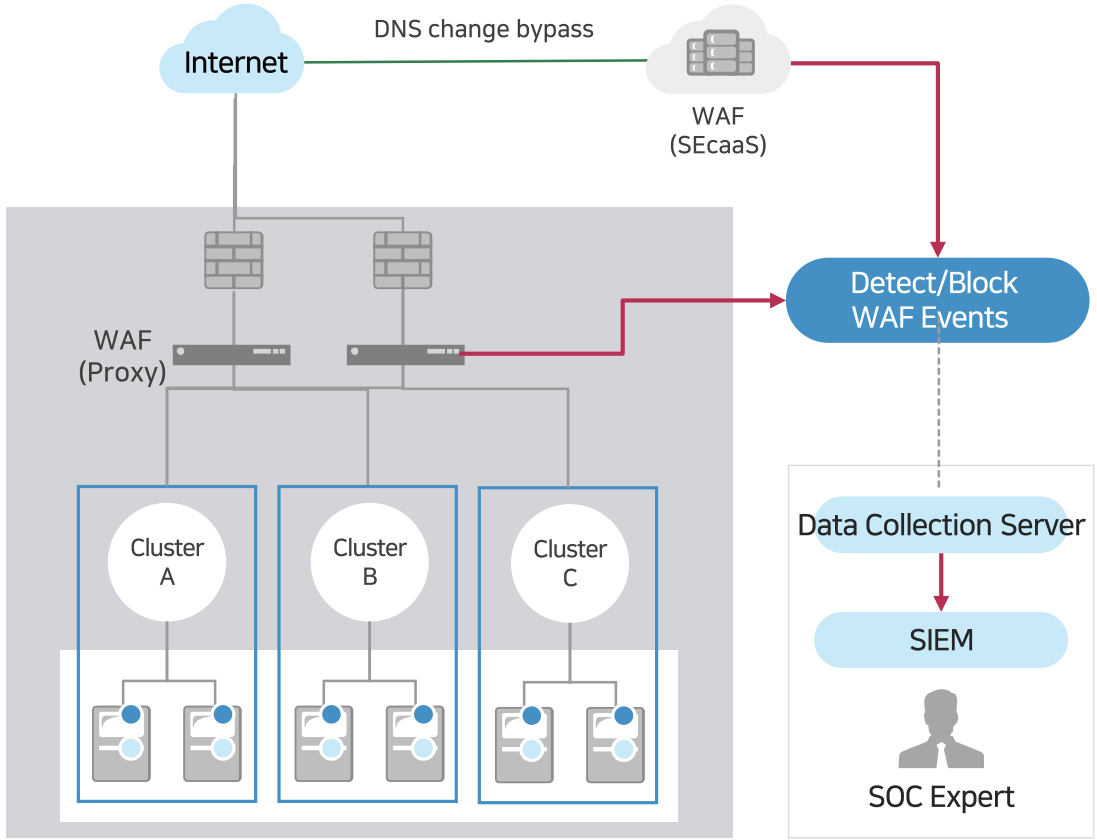
Security Service – Managed WAF Service

Identify, analyze, remediate, and prevent web attack attempts or web vulnerabilities with speed.

Managed WAF Service Structure



Log Collection & Event Detection/Alert System

Event Log Collection	• WAF(SEcaaS) events are transferred to data collection server from Scrubbing Center (detection logs) • WAF(Proxy) events are encrypted via Firewall VPN and sent to data collection server (detection logs)
Event Detection	• OWASP rule-based hacking attempt detection • Correlation analysis with IDS detection logs • The detected malicious events can be blocked/blacklisted upon discussion with customer

Alert/ Notification Criteria	Normal	Need Attention	Emergency
	• Suspicious activities • Email notification	• Failed web hacking attempts • SQL Injection, XSS, etc. • Detailed event analysis • Confirmation requests (email)	• Successful web hacking attempts • Detailed event analysis • Reporting (Phone/SMS/email)

Copyright © 2020 Samsung SDS Co., Ltd. All rights reserved.