Kona Site Defender

Innovare senza paura con una soluzione di sicurezza integrata e scalabile

Per avere successo nel mondo iperconnesso di oggi, le aziende devono essere in grado di innovare senza paura. Gli attacchi DDoS (Distributed Denial of Service), così come quelli alle applicazioni web e all'infrastruttura DNS, rappresentano alcune delle minacce più critiche per le aziende di oggi. Questi attacchi sono sempre più sfrontati e colpiscono le aziende di tutti i mercati verticali e i paesi del mondo, provocando downtime, aumentando i costi della larghezza di banda e determinando la perdita di informazioni riservate. Ma nonostante i rischi e le problematiche, consumatori e aziende si aspettano di poter vedere, sentire e fare sempre di più sul web. Per avere successo nel mondo iperconnesso di oggi, le aziende devono continuare a espandere le proprie offerte web senza sentirsi costantemente minacciate da potenziali intrusi. Devono essere in grado di innovare senza paura.

Caratteristiche

Sui server Akamai transita quotidianamente una quantità di traffico superiore ai 28 Tbps. Sulla rete Akamai gli attacchi dell'ordine delle decine, o addirittura migliaia, di Gbps vengono assorbiti senza grossi problemi.

Kona Site Defender protegge dagli attacchi DDoS, direct-to-origin e da quelli contro le applicazioni web, mentre la soluzione opzionale Akamai FastDNS consente di mitigare anche gli attacchi all'infrastruttura DNS. Kona Site Defender è implementato sulla Akamai Intelligent Platform™, costituita da oltre 170.000 server distribuiti in più di 1.300 reti e 100 paesi.

Mitigazione di attacchi DDoS Kona Site Defender, che sfrutta la Akamai Intelligent Platform, è progettato per contrastare gli attacchi DDoS assorbendo il traffico DDoS diretto al livello applicativo, dirottando tutto il traffico DDoS diretto al livello di rete, come i SYN flood o gli UDP flood, e autenticando il traffico valido alla periferia della rete.

Questa protezione integrata è "sempre attiva" e autorizza solo il traffico sulla porta 80 (HTTP) o 443 (HTTPS). Grazie al contenimento dei costi, è possibile evitare agli utenti un aumento delle spese per il servizio causato dal traffico degli attacchi DDoS. Inoltre, il caching flessibile massimizza l'offload dall'origine.

L'architettura distribuita in tutto il mondo e la scala elevatissima della Akamai Intelligent Platform garantiscono la disponibilità continua dei siti web dei clienti. Akamai gestisce in media 12 Tbps di traffico giornaliero, ma ha raggiunto anche picchi superiori ai 26 Tbps. Inoltre, le funzionalità di mitigazione sono implementate in modo nativo nel percorso, perciò la protezione viene applicata a poche reti di distanza dal punto della richiesta, e NON all'origine del cliente.

Protezione a livello di applicazioni Kona Site Defender incorpora un WAF (Web Application Firewall) dotato di funzioni complete, basato su una tecnologia proprietaria che fornisce ai clienti una protezione altamente scalabile dagli attacchi a livello di applicazione. Implementato inline sull'intera piattaforma Akamai distribuita in tutto il mondo, formata da decine di migliaia di server, Kona Site Defender è in grado di rilevare e dirottare le minacce nel traffico HTTP e HTTPS, generando avvisi o bloccando il traffico degli attacchi vicino alla fonte, prima che raggiunga l'origine del cliente. Il WAF (Web Application Firewall) incorpora le regole del Kona Rule Set per la protezione delle applicazioni.

Regole Kona

Kona Site Defender include una vasta serie di regole del firewall a livello di applicazione (che Akamai aggiorna regolarmente), predefinite e configurabili per diverse categorie di attacchi, quali: violazioni di protocollo, violazioni dei limiti di richieste, violazioni delle policy HTTP, robot nocivi, attacchi generici e CMDi (Command Injection), Trojan backdoor e perdita di contenuti in uscita. Insieme, tali regole prendono il nome di "Kona Rule Set".

Kona Rule Set protegge centinaia dei nostri clienti dalle minacce e dagli attacchi più recenti. Le regole vengono mantenute costantemente aggiornate dal team Akamai di ricerca sulle minacce e sono disponibili a tutti i clienti che utilizzano Kona Site Defender, per proteggerli da attacchi quali: Low Orbit Ion Cannon, High Orbit Ion Cannon, HULK, Dirt Jumper, Havij SQL Injection Tool, Netsparker, ApacheBench, Webhive e molti altri. Le regole Kona includono:

- assegnazione di punteggi alle anomalie, in cui ogni regola contribuisce al calcolo del punteggio complessivo del rischio, su cui sono basate le decisioni relative ad avvisi e negazioni dell'accesso.
- Attivazione dell'ispezione dell'intestazione delle richieste/risposte HTTP e del corpo delle richieste/risposte HTTP POST tramite una serie di regole REGEX a cascata, con lo scopo di proteggere da attacchi quali SQL Injection e XSS (Cross-Site Scripting).

VANTAGGI PER IL BUSINESS

- **Riduce il rischio** di downtime, defacing e furto di dati.
- **Protegge la redditività**, la fedeltà dei clienti e il valore del marchio.
- **Mantiene le prestazioni** durante gli attacchi.
- **Riduce i costi** associati alla gestione di picchi di traffico generati dagli attacchi.
- **Riduce il CAPEX** dell'hardware e del software di sicurezza.

VANTAGGI TECNICI E OPERATIVI

- **Semplifica l'integrazione** con l'infrastruttura IT esistente.
- **Ottimizza il tempo di attività e la disponibilità** durante gli attacchi DDoS.
- **Difende** l'infrastruttura delle applicazioni Web.
- **Protegge** dagli attacchi direct-to-origin
- **Aumenta la disponibilità** dell'infrastruttura DNS.
- **Scala on demand.**
- **Consente di accedere** alla massima competenza in materia di protezione delle applicazioni.

Kona Site Defender

- Una vasta gamma di funzionalità che semplifica l'aggiornamento delle regole:
  - » Un aggiornamento guidato che permette ai clienti attuali di aggiornare le policy WAF (Web Application Firewall) all'ultima versione delle regole Kona.
  - » Una modalità di valutazione che permette ai clienti di mantenere regole e protezioni legacy e al tempo stesso di definire nuove regole KRS.
- Una funzione di gestione della versione delle regole, che permette ai clienti di adottare regole nuove o modificate a una frequenza in linea con i propri processi di controllo delle modifiche.

I **controlli a livello di rete** permettono alle aziende di applicare whitelist e blacklist di indirizzi IP definite dal cliente. Entro pochi minuti, gli aggiornamenti delle liste vengono propagati in tutta la rete globale Akamai, garantendo una risposta rapida agli attacchi. Le altre caratteristiche includono la possibilità di limitare le richieste provenienti da indirizzi IP specifici, per proteggere l'origine del cliente dagli attacchi a livello di applicazione e implementare il blocco geografico. Sono supportate fino a 10.000 voci CIDR, inclusi elenchi denominati quali i nodi di uscita TOR. Le whitelist e le blacklist possono essere inoltre caricate tramite le API di blocco IP.

I **controlli dei tassi** forniscono una protezione dagli attacchi DDoS a livello di applicazione, monitorando e controllando la frequenza delle richieste indirizzate ai server Akamai e all'origine del cliente. Kona Site Defender è in grado di rispondere in pochi secondi ai picchi di richieste.

Con **Site Shield**, Kona Site Defender offre la possibilità di nascondere l'origine del cliente dalla rete Internet pubblica. Le mappe Site Shield possono essere configurate da Professional Services o dai clienti, da Luna e tramite le API. Site Shield è progettato per integrare l'infrastruttura esistente e prevenire gli attacchi direct-to-origin.

La funzione di **monitoraggio della sicurezza** di Kona Site Defender offre agli esperti di protezione una visibilità in tempo reale sugli eventi di sicurezza, oltre alla possibilità di esaminare a fondo gli avvisi di attacco per recuperare informazioni dettagliate sugli autori e gli obiettivi degli attacchi, sulle funzionalità di difesa che hanno attivato la dichiarazione di attacco e sugli elementi della richiesta che hanno attivato le difese del sito. Il monitoraggio della sicurezza include la possibilità di visualizzare i dettagli delle intestazioni di richieste e risposte per perfezionare le regole e indagare sugli attacchi.

Il servizio di aggiornamento delle regole di **Kona Site Defender** fornisce revisioni periodiche programmate delle configurazioni di Kona Site Defender e WAF (Web Application Firewall), create dal team Professional Services di Akamai, che includono l'analisi dei falsi positivi dei log del monitor di sicurezza, oltre a consigli su Kona Site Defender e sulla regolazione e l'ottimizzazione della configurazione di origine.

Il componente di protezione rapida del DNS (sistema dei nomi di dominio), FastDNS, fornisce una soluzione solida, affidabile e scalabile, progettata per garantire che gli utenti finali raggiungano direttamente i siti web desiderati. La soluzione FastDNS di Akamai sfrutta i server dei nomi attendibili secondari della Akamai Intelligent Platform, distribuita in tutto il mondo. Non richiede alcuna modifica ai processi di amministrazione DNS attuali e fornisce una risoluzione DNS incredibilmente solida, affidabile, scalabile e sicura.

Il modulo opzionale **Client Reputation** completa Kona Site Defender con un livello di protezione aggiuntivo e consente di ottenere informazioni sugli autori degli attacchi. Client Reputation fornisce tale protezione concentrandosi sulla fonte della minaccia, ovvero sui client web, anziché sui vettori di attacco. Akamai esamina miliardi di indirizzi IP ogni trimestre e Client Reputation applica avanzati algoritmi ai dati raccolti dai client web per identificare gli autori degli attacchi. Ai client web nocivi viene assegnato un punteggio basato sulla probabilità di coinvolgimento in tre diversi tipi di comportamenti dannosi, ovvero scansione dei siti web, attacchi web generici e attacchi DoS.

L'ecosistema Akamai

Akamai rende Internet veloce, affidabile e sicura. Le nostre soluzioni complete sono basate sulla piattaforma Akamai Intelligent Platform, distribuita su scala globale, vengono gestite tramite il portale unificato e personalizzabile Luna Control Center, che garantisce visibilità e controllo, e sono supportate dagli esperti del team Professional Services, che aiutano i clienti a essere subito operativi, proponendo loro soluzioni sempre nuove, in linea con l'evoluzione delle strategie aziendali.

TIM è la principale azienda italiana di telecomunicazioni. Tramite la sua rete, offre in Italia ed in molti paesi del mondo servizi di telefonia fissa e mobile, connessioni ad alta velocità in fibra ottica, ed una offerta completa di entertainment, dalla TV alla musica in streaming, al gaming. Opera in Italia ed in Brasile dove è uno dei principali operatori, con il marchio Tim. L'offerta specifica per la clientela Business è denominata TIM Impresa Semplice. A partire dal 13 gennaio 2016 la società ha adottato il marchio unificato TIM, per una nuova identità che rappresenta i valori e le caratteristiche di un'azienda proiettata verso il futuro. Per saperne di più visitate i siti www.tim.it e www.telecomitalia.com.

Akamai FASTER FORWARD

Leader mondiale nel settore dei servizi CDN (rete per la distribuzione dei contenuti), Akamai si impegna per offrire ai propri clienti una rete Internet più veloce, affidabile e sicura. Le soluzioni avanzate di web performance, mobile performance, cloud security e media delivery dell'azienda stanno rivoluzionando il modo in cui le imprese ottimizzano le esperienze di consumatori, imprese e intrattenimento per qualsiasi dispositivo, ovunque nel mondo. Per scoprire come le nostre soluzioni e il nostro team stanno aiutando le aziende a espandere il proprio business, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter.

La sede principale di Akamai si trova a Cambridge (Massachusetts), negli Stati Uniti, ma la società è presente in tutto il mondo con ben 40 uffici. I nostri servizi e la rinomata assistenza clienti consentono alle aziende di offrire ai propri clienti un'esperienza di navigazione su Internet senza precedenti su scala globale. Indirizzi, numeri di telefono e informazioni di contatto per tutte le località sono elencati sul sito web www.akamai.com/locations.