Protezione delle banda Internet con DefensePipe di Radware

DefensePipe è un servizio di scrubbing degli attacchi DDoS basato su cloud che impedisce la saturazione della banda Internet a causa di attacchi informatici. Si attiva solo quando l'attacco minaccia di saturare la banda Internet dell'azienda. Grazie alla sincronizzazione integrata tra data center, DefensePro e DefensePipe, la prevenzione nel cloud può iniziare immediatamente.

L'Attack Mitigation System (AMS) di Radware, composto da DefensePro e DefensePipe, offre alle aziende la soluzione più integrata e completa per contrastare le minacce alla sicurezza informatica di oggi.

L'AMS consente alle organizzazioni di contrastare gli attacchi informatici su tutti i fronti e assicurare una protezione end-to-end con un unico punto di contatto. Ciò risulta in un tempo più breve di attivazione della protezione e in una soluzione di sicurezza completa offerta da un unico fornitore.

Il 15% degli attacchi DDoS gestiti dall'Emergency Response Team (ERT) di Radware è relativo alla saturazione di banda Internet.

Panoramica della soluzione

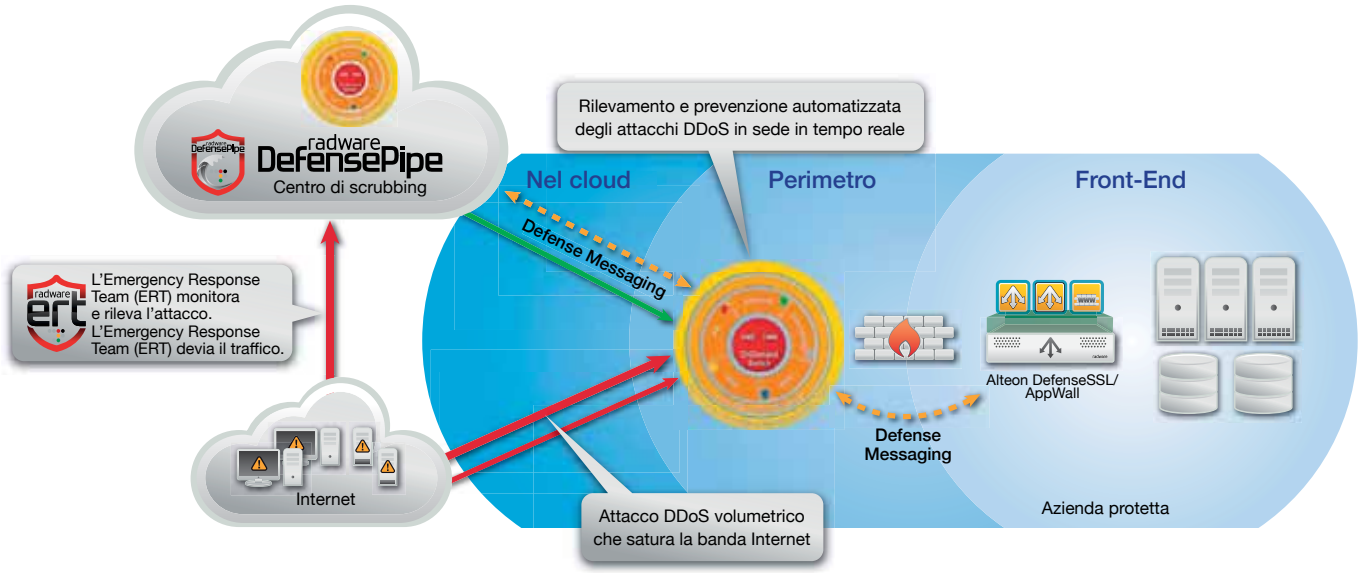
Un sistema di prevenzione degli attacchi informatici in sede offre l'approccio più efficace per contrastare le minacce informatiche attuali, compresi gli attacchi a livello di applicazione, gli attacchi invisibili low & slow, gli attacchi a livello di rete, nonché quelli basati su SSL. Tuttavia, una volta che gli attacchi si trasformano in un attacco flood volumetrico che minaccia di saturare la banda Internet dell'azienda, la prevenzione deve spostarsi al cloud. Secondo l'Emergency Response Team (ERT), solo il 15% degli attacchi DDoS è basato su attacchi volumetrici che bloccano realmente la banda Internet.

L'AMS di Radware offre protezione in sede con DefensePro e protezione basata su cloud con DefensePipe, condividendo informazioni essenziali su minacce e attacchi tramite un meccanismo di defense messaging. Durante un attacco che minaccia di saturare la banda Internet dell'azienda che subisce l'attacco, DefensePro in sede invia un allarme a DefensePipe informandolo dell'imminente raggiungimento della saturazione della banda Internet. Con questo allarme vengono comunicate numerose caratteristiche dell'attacco che consentono a DefensePipe di avviare la prevenzione nel cloud più rapidamente e in modo più accurato.

Una volta che la prevenzione è stata spostata nel cloud, tutto il traffico viene deviato al centro di scrubbing nel cloud, dove viene sottoposto a verifica prima di essere inviato nuovamente all'azienda.

Vantaggi

- Servizio basato su cloud che protegge le aziende dalla saturazione della banda Internet
- Completa le funzioni DefensePro in sede
- Attivato solo quando gli attacchi minacciano di saturare la banda Internet
- Centri di scrubbing multipli nel cloud forniscono copertura globale
- Singolo punto di contatto per risposte di emergenza
- Analisi successiva all'attacco, con report esaustivo

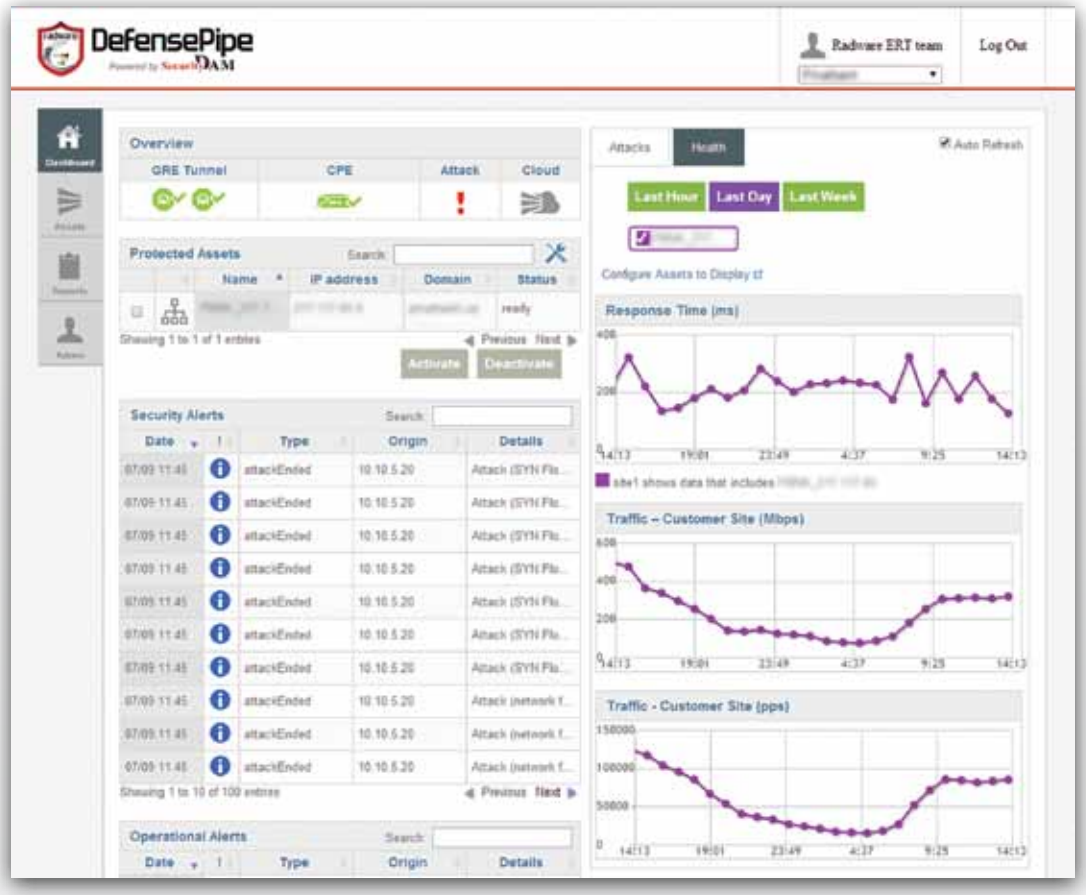


Servizio di prevenzione degli attacchi informatici: difesa di rete ibrida

Portale online di DefensePipe per i clienti

DefensePipe offre ai clienti completa visibilità a tutti i livelli DDoS grazie ad un centro di controllo intuitivo basato su Web che comprende:

- Monitoraggio in tempo reale (statistiche di traffico, informazioni sugli attacchi e allarmi per gli attacchi)
- Gestione del servizio cloud e delle apparecchiature in sede
- Attivazione/disattivazione della deviazione del traffico
- Raccolta di dati sugli attacchi da apparecchiature in sede e cloud
- Allarmi in tempo reale e funzioni complete di reporting



Dashboard del portale del servizio di prevenzione degli attacchi informatici

Vantaggi della soluzione AMS

L'Emergency Response Team (ERT) di Radware che fornisce servizi di sicurezza 24 ore su 24, 7 giorni alla settimana, ai clienti minacciati da attacchi di tipo DoS o da ripetuti attacchi malware, aiuta il cliente a contrastare gli attacchi durante l'intera campagna sia in sede che nel cloud.

- **Più ampia copertura di sicurezza:** AMS di Radware offre rilevamento e prevenzione degli attacchi informatici multi-vettore, gestendo attacchi a livello di rete, attacchi basati su server, propagazione malware e attività di intrusione. Grazie ad un meccanismo unico brevettato, la soluzione Radware è in grado di creare automaticamente in tempo reale una firma di identificazione dell'attacco che può essere usata per prevenire l'attacco laddove può essere contrastato più efficacemente. Ciò avviene tramite DefensePipe nel centro di scrubbing nel cloud o tramite DefensePro in sede.
- **Tempo di prevenzione minimo:** la funzione di protezione sempre attiva assicura che l'azienda sia protetta completamente in ogni momento e il tempo di attivazione della prevenzione degli attacchi è di pochi secondi. In caso un attacco richieda la deviazione del traffico al centro di scrubbing nel cloud, la protezione continua senza interruzioni o danni.
- **Singolo punto di contatto:** sia che l'attacco necessiti di essere prevenuto in sede o nel cloud, l'Emergency Response Team (ERT) di Radware contrasta l'attacco a fianco del cliente durante l'intera campagna di attacco. Ciò significa che i clienti non hanno bisogno di lavorare con più fornitori o servizi durante un attacco e non hanno bisogno di trasferire responsabilità da un fornitore all'altro, né di verificare che più fornitori siano sincronizzati tra di loro.
- **Il traffico viene deviato solo come ultima soluzione:** a differenza degli scrubber nel cloud e MSSP che deviano il completo traffico del cliente ai propri centri di scrubbing durante un attacco, AMS di Radware devia il traffico dell'attacco solo quando un attacco volumetrico minaccia di saturare la banda Internet. In tutti gli altri casi, il sistema di prevenzione degli attacchi informatici in sede contrasta l'attacco senza bisogno di deviare il traffico.
- **Sistema di reporting integrato:** offre informazioni sia in relazione alla prevenzione in sede che a quella nel cloud. Ciò consente al cliente di effettuare analisi più efficienti, comprendere meglio le minacce che sta affrontando e pianificare la sua strategia di prevenzione per minacce future.

Informazioni su Radware

Radware (NASDAQ: RDWR), è un'azienda leader a livello globale nella fornitura di soluzioni di application delivery e sicurezza delle applicazioni destinate ai data center in ambienti virtualizzati e in cloud. L'ampia offerta di premiate soluzioni Radware garantisce la resilienza completa delle applicazioni aziendali "Mission Critical", massima efficienza IT e totale agilità del business. Grazie alle soluzioni Radware, oltre 10.000 clienti di tutto il mondo, tra aziende e operatori TLC, riescono a reagire rapidamente alle sfide del mercato, mantenere la continuità operativa aziendale e ottenere la massima produttività, contenendo contemporaneamente i costi. Per ulteriori informazioni, visitare il sito www.radware.com.

Radware favorisce la partecipazione alla propria community e consiglia di seguire l'azienda su Facebook, Google+, LinkedIn, blog di Radware, SlideShare, Twitter, YouTube e sull'app Radware Connect per iPhone®.

Programma di assistenza

Radware offre supporto tecnico per tutti i suoi prodotti attraverso il Certainty Support Program. Ciascun livello del Certainty Support Program consiste di quattro elementi: assistenza telefonica, aggiornamenti software, manutenzione hardware e assistenza in sede. Radware dispone inoltre di personale tecnico dedicato in grado di assistere i propri clienti offrendo servizi professionali per l'implementazione di progetti avanzati.

Ulteriori informazioni

Per scoprire come le soluzioni integrate di application delivery e sicurezza delle applicazioni di Radware possano consentirvi di ottenere il massimo dalla vostra attività e dai vostri investimenti IT, inviate un'e-mail all'indirizzo info@radware.com oppure visitate il sito Web www.radware.com.