SONICWALL™

BEST PRACTICES PER BLOCCARE LE MINACCE CRITTOGRAFATES

Come proteggere la rete dai criminali informatici che utilizzano SSL/TLS

Abstract

La crittografia SSL/TLS (Secure Sockets Layer/Transport Layer Security) o il traffico HTTPS sono ormai i metodi più utilizzati per proteggere i dati sensibili trasmessi attraverso Internet. Ma come fare per mantenere intatta l'integrità e la privacy delle comunicazioni SSL, garantendo al tempo stesso la sicurezza della rete e dei dati che vengono scambiati? Questo documento illustra alcune considerazioni e le pratiche migliori per proteggersi dalle minacce crittografate.

Introduzione

La soluzione consiste nel decrittografare il traffico criptato che entra in rete, per consentire al firewall di protezione della rete di analizzare il traffico e identificare le minacce nascoste. A questo scopo i firewall attuali applicano la tecnologia DPI-SSL, ovvero l'ispezione Deep Packet del protocollo Secure Socket Layer.

Tuttavia, anche i firewall che in teoria offrono l'ispezione e la decrittografia SSL potrebbero non disporre della potenza di elaborazione necessaria per gestire il livello di traffico SSL che passa attraverso una rete attuale. Per la valutazione di una soluzione DPI-SSL è consigliabile eseguire un test delle prove di concetto.

Le soluzioni migliori utilizzano un motore con tecnologia d'ispezione full-stack per analizzare il traffico SSL crittografato alla ricerca di minacce, trasmettendo poi il traffico a destinazione nel caso in cui non vengano rilevate minacce o vulnerabilità. È inoltre importante disporre di un processo di installazione semplice e sicuro per ridurre i tempi di configurazione e le complessità.

Considerazioni sull'implementazione

Per le implementazioni ad alta densità di traffico è necessario escludere le fonti attendibili per massimizzare le prestazioni

Con la giusta combinazione di firewall è possibile ripristinare le prestazioni d'ispezione SSL venute meno nei firewall esistenti o standalone e aumentare la velocità di analisi DPI-SSL fino a 80 Gbps.

della rete. Per applicare l'ispezione SSL a tipologie di traffico specifiche è opportuno creare una lista personalizzata di indirizzi e oggetti o gruppi di servizi o utenti.

È inoltre essenziale ispezionare tutto il traffico SSL, sia quello che proviene da dietro la LAN del firewall per accedere a contenuti sulla WAN che viceversa. Questo livello d'ispezione protegge tutti gli utenti della LAN da intrusioni pericolose, virus, Trojan e altri attacchi alla rete nascosti mediante la crittografia. Allo stesso tempo protegge anche tutti gli utenti della WAN, inclusi i client remoti, da attacchi crittografati nascosti.

Un'altra possibilità è la scelta di una soluzione di protezione hardware basata su firewall, scalabile e di costo contenuto, in grado di fornire l'analisi DPI-SSL sul lato server e client senza compromettere la sicurezza. In questo caso la risposta è un "firewall sandwich".

Un firewall sandwich è una configurazione basata su firewall di nuova generazione (NGFW) scalabile e dotata di analisi DPI-SSL del traffico in entrata e in uscita. Il firewall sandwich è altamente efficace perché è scalabile orizzontalmente in maniera lineare e utilizza un'architettura basata sulla rete che si affida a firewall di nuova generazione disposti su un solo livello, anziché su ulteriori appliance, per il filtraggio dei contenuti o la decrittografia SSL. Questo approccio permette di rafforzare la protezione senza influire sul throughput ed evita la scarsa scalabilità e i costi associati all'acquisto di un ulteriore prodotto di terze parti.

I firewall usati per questo approccio devono tuttavia essere progettati con processori multicore per poter garantire la scalabilità quando utilizzati in parallelo. Molti marchi di firewall di nuova generazione non consentono una scalabilità lineare, con un conseguente peggioramento delle prestazioni qualora uno dei componenti della configurazione dovesse raggiungere la capacità massima. Con la giusta combinazione di firewall è possibile ripristinare le prestazioni venute meno per analizzare il traffico SSL nei firewall esistenti o standalone e aumentare la velocità di analisi DPI-SSL fino a 80 Gbps.

Best practice di protezione

La buona notizia è che esistono diversi modi per beneficiare della sicurezza offerta dalla crittografia SSL/TLS senza il rischio di subire attacchi informatici:

1. Se negli ultimi tempi non avete svolto alcun controllo della sicurezza, effettuate un'analisi completa dei rischi per identificare i vostri rischi ed esigenze.
2. Eseguite l'upgrade a un firewall di nuova generazione ampliabile, con funzionalità d'ispezione IPS e SSL integrate e prestazioni scalabili per supportare la crescita futura.
3. Aggiornate le vostre policy di sicurezza per proteggervi da una gamma ancora più ampia di vettori di minacce e applicate diversi metodi di difesa per tutelarvi da attacchi sia HTTP che HTTPS.
4. Addestrate costantemente il vostro personale per renderlo consapevole dei pericoli relativi a social media, siti di social engineering, download sospetti, spam, phishing e altre truffe online.
5. Informate gli utenti di non accettare mai un certificato autofirmato non valido.
6. Assicuratevi che tutto il vostro software sia aggiornato. Questo vi aiuterà a proteggervi da vecchi exploit SSL che sono già stati neutralizzati.

Conclusioni

Esistono diversi modi efficaci per salvaguardare l'integrità e la privacy delle comunicazioni SSL, garantendo al contempo la sicurezza della rete e dei dati scambiati. Per maggiori informazioni su come SonicWall può aiutare la tua organizzazione a bloccare le minacce nascoste, visita la pagina www.sonicwall.com/solutions/security-solutions.

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla sicurezza della rete alla protezione degli accessi fino alla sicurezza dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti consentendo alle organizzazioni di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall permette ai suoi clienti di guardare al futuro con fiducia.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway,
Santa Clara, CA 95054

Consulta il nostro sito Web per informazioni sulle sedi regionali e internazionali.
www.sonicwall.com

SolutionBrief-BestPractices4StoppingThreats-EU-IMAG-22650