DECRITTAZIONE E ISPEZIONE DEL TRAFFICO CRITTOGRAFATO

Protezione ad alte prestazioni contro l'uso maligno della crittografia

Secondo il Rapporto sulle minacce informatiche 2018 de SonicWall, il traffico crittografato rappresenta oggi quasi il 70% delle comunicazioni web complessive di un'organizzazione. Sebbene siano molti i vantaggi nel crittografare le sessioni Internet, come la protezione della privacy e l'integrità delle informazioni personali per lo scambio di dati, è possibile rilevare anche una tendenza meno positiva, in quanto gli autori di malware sfruttano queste capacità della crittografia per nascondere i loro attacchi agli occhi dei firewall. Gli aggressori possono non soltanto aggirare i firewall e sfruttare appieno i punti ciechi per introdurre direttamente il malware attraverso le porte aperte in qualsiasi rete, ma utilizzano anche il TLS/SSL per nascondere il traffico di comando e controllo al fine di manipolare sistemi compromessi praticamente da qualunque parte del mondo. Le aziende che non ispezionano il traffico crittografato perdono gran parte delle potenzialità dei loro sistemi firewall, non essendo in grado di vedere cosa contiene il traffico, individuare il download di malware, identificare i file dannosi o scoprire la trasmissione non autorizzata di informazioni privilegiate a sistemi esterni.

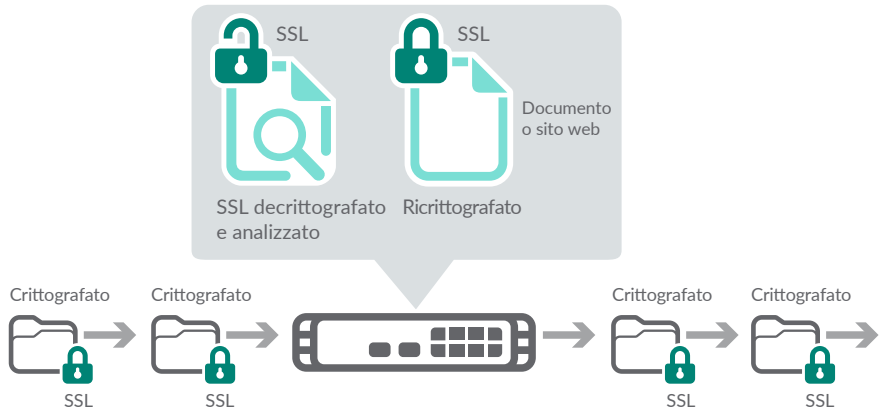
Le organizzazioni possono salvaguardare le loro reti da questi rischi per la sicurezza con SonicWall Deep Packet Inspection per TLS/SSL (DPI-SSL), un servizio add-on disponibile su tutti i firewall di nuova generazione SonicWall (NGFW, Next-Generation Firewall) e sulle appliance di sicurezza di rete Unified Threat Management (UTM). La DPI-SSL offre protezione avanzata da minacce crittografate utilizzando il motore brevettato di Reassembly-Free Deep Packet Inspection di SonicWall, si eseguire la scansione di un'ampia gamma di protocolli di crittografia, tra cui HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS e POPS, indipendentemente dalla porta che si sta utilizzando.

Il servizio permette di decodificare il traffico TLS/SSL, ispezionarlo alla ricerca di minacce e quindi ricodificarlo per mandarlo a destinazione se non vengono rilevate minacce o vulnerabilità. Si tratta di un servizio prezioso per garantire una sicurezza fondamentale, il controllo delle applicazioni e la prevenzione di perdite di dati.

Questo servizio offre sicurezza avanzata, controllo delle applicazioni e prevenzione di perdite di dati per analizzare il traffico HTTPS e altro traffico TLS/SSL crittografato.

Vantaggi:

- Maggiore visibilità sul traffico TLS/SSL crittografato
- Blocco dei download con malware nascosto
- Prevenzione di comunicazioni C&C ed esfiltrazioni di dati
- Personalizzazione delle liste di inclusione ed esclusione per conformità o requisiti legali



Requisiti di sistema

L'ispezione TLS/SSL è disponibile con i seguenti firewall SonicWall:
SOHO / SOHO W
TZ300 / TZ300 W / TZ300P
TZ400 / TZ400 W
TZ500 / TZ500 W
TZ600 / TZ600P
NS*a* 2650
NS*a* 3650
NS*a* 4650
NS*a* 5650
NS*a* 6650
NS*a* 9250
NS*a* 9450
NS*a* 9650
SuperMassive 9800
NS*sp* 12400
NS*sp* 12800
NS*v* 10
NS*v* 25
NS*v* 50
NS*v* 100
NS*v* 200
NS*v* 300
NS*v* 400
NS*v* 800
NS*v* 1600

Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

Caratteristiche

Prestazioni elevate e numerose connessioni – I firewall SonicWall di nuova generazione utilizzano un'architettura di processore avanzata e un numero molto elevato di connessioni per ottimizzare le prestazioni DPI-SSL e la protezione di tutti i dispositivi connessi.

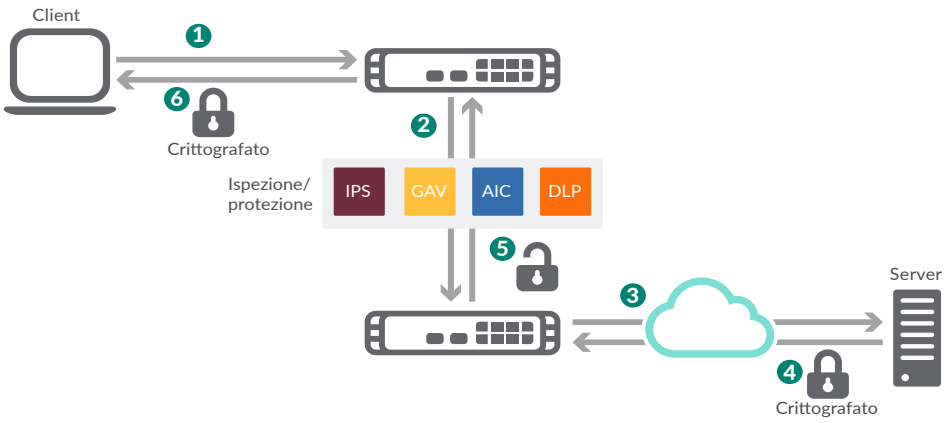
Sicurezza e semplicità di impostazione — Il servizio di decrittazione e ispezione DPI-SSL protegge gli utenti sulla rete con una configurazione e una complessità minime.

Elenco di inclusione/esclusione — Per implementazioni a traffico elevato gli amministratori possono escludere le fonti attendibili per massimizzare le prestazioni di rete. Inoltre, gli amministratori possono prendere di mira uno specifico tipo di traffico per l'ispezione TLS/SSL mediante la personalizzazione di un elenco che specifica indirizzo, servizio oppure oggetti o gruppi di utenti per conformità con i requisiti di privacy e/o di legge.

Modalità Client — Ispeziona il traffico TLS/SSL quando il client si trova nella LAN del firewall e accede a contenuti presenti nella WAN. Dopo che il dispositivo ha decifrato e ispezionato il traffico crittografato, provvede a riscrivere il certificato inviato dal server remoto e firma il nuovo certificato generato con il certificato specifico dell'utente. Come impostazione predefinita, è questa l'autorità di certificazione del dispositivo (CA), nonostante sia possibile selezionare un certificato diverso.

Modalità Server — Ispeziona il traffico TLS/SSL quando i client remoti si collegano via WAN per accedere a contenuti presenti nella LAN del firewall, permettendo all'amministratore di configurare associazioni tra un oggetto indirizzo e un certificato. Quando il dispositivo rileva connessioni TLS/SSL con l'oggetto dell'indirizzo, fornisce il certificato abbinato ed esegue la negoziazione TLS/SSL con il client che richiede la connessione. In questo scenario, il proprietario del firewall di nuova generazione SonicWall possiede i certificati e le chiavi private dei server dei contenuti di origine.

Supporto completo — Il supporto include la prevenzione delle intrusioni, la prevenzione del malware, il controllo delle applicazioni, il filtraggio di contenuti/URL e la prevenzione della comunicazione di comando e controllo del malware.



Ispezione TLS/SSL – Modalità Client

1. Il client avvia l'handshake TLS/SSL con il server
2. L'NGFW intercetta la richiesta e instaura la sessione utilizzando i propri certificati al posto del server
3. L'NGFW avvia l'handshake TLS/SSL con il server per conto del client utilizzando il certificato TLS/SSL definito dall'amministratore
4. Il server completa l'handshake e crea un tunnel sicuro fra se stesso e l'NGFW
5. L'NGFW ricodifica il traffico e lo invia al client
6. L'NGFW decodifica e ispeziona tutto il traffico proveniente dal client o diretto verso di esso alla ricerca di minacce e violazioni delle policy

Requisiti di sistema

L'ispezione TLS/SSL è disponibile con i seguenti firewall SonicWall di nuova generazione (NGFW):

FIREWALL	LICENZA ONE-TIME SENZA SCADENZA
SOHO / SOHO W	01-SSC-0723
TZ300 / TZ300 W	Inclusa nell'abbonamento Security Services
TZ400 / TZ400 W	Inclusa nell'abbonamento Security Services
TZ500 / TZ500 W	Inclusa nell'abbonamento Security Services
TZ600 / TZ600P	Inclusa nell'abbonamento Security Services
NSa 2650	Incluso nell'abbonamento Security Services
NSa 3650	Incluso nell'abbonamento Security Services
NSa 4650	Incluso nell'abbonamento Security Services
NSa 5650	Incluso nell'abbonamento Security Services
NSa 6650	Incluso nell'abbonamento Security Services
NSa 9250	Inclusa nell'abbonamento Security Services
NSa 9450	Inclusa nell'abbonamento Security Services
NSa 9650	Inclusa nell'abbonamento Security Services
SuperMassive 9800	Inclusa nell'abbonamento Security Services
NSsp 12400	Inclusa nell'abbonamento Security Services
NSsp 12800	Inclusa nell'abbonamento Security Services
NSv 10	Inclusa nell'abbonamento Security Services
NSv 25	Inclusa nell'abbonamento Security Services
NSv 50	Inclusa nell'abbonamento Security Services
NSv 100	Inclusa nell'abbonamento Security Services
NSv 200	Inclusa nell'abbonamento Security Services
NSv 300	Inclusa nell'abbonamento Security Services
NSv 400	Inclusa nell'abbonamento Security Services
NSv 800	Inclusa nell'abbonamento Security Services
NSv 1600	Inclusa nell'abbonamento Security Services

Informazioni su SonicWall

Da oltre 27 anni SonicWall combatte il crimine informatico proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

DataSheet-DecryptionAndInspection-US-VG-MKTG4095