SOPHOS
Cybersecurity evolved.

La cifratura ha reso il tuo attuale firewall obsoleto?

Cinque funzionalità essenziali di TLS Inspection da avere nel tuo prossimo firewall

Whitepaper Sophos. Giugno 2021

Cinque funzionalità essenziali di TLS Inspection da avere nel tuo prossimo firewall

Il rapido incremento del traffico di rete cifrato, unito all'incapacità della maggior parte dei firewall next-gen di ispezionare questo tipo di traffico, ha creato la tempesta di sicurezza perfetta, con conseguenze catastrofiche.

Oltre il 90% del traffico nella maggior parte delle reti è cifrato e normalmente attraversa il firewall medio senza essere soggetto ad alcun filtro. Questo non è dovuto a una decisione esplicita di non eseguirne l'ispezione, bensì al fatto che la maggior parte dei firewall non è in grado di farlo. Inoltre, anche quando il firewall è in grado di ispezionare il traffico cifrato, spesso la soluzione di ispezione TLS non è implementata in maniera adeguata e impedisce a molte pagine web di caricarsi correttamente. Il risultato è una pessima esperienza utente.

Non sorprende pertanto che tra gli hacker si stia diffondendo la tendenza a sfruttare questo enorme punto cieco nella sicurezza delle organizzazioni. I cybercriminali stanno cominciando ad approfittare di questa vulnerabilità per collocare minacce all'interno delle reti aziendali e garantirne la persistenza.

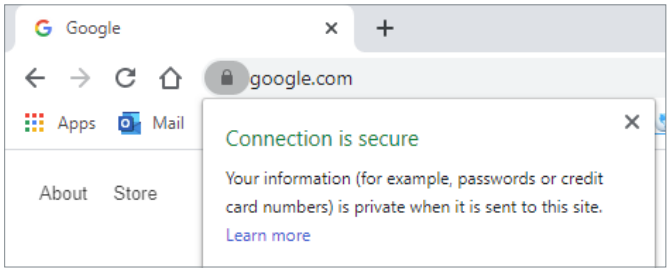
Leggete questo documento per scoprire come la cifratura ha reso obsoleta la maggior parte dei firewall next-gen, nonché quali sono le sfide derivanti dall'ispezione TLS e le funzionalità indispensabili per colmare questa lacuna di sicurezza. e

La cifratura tutela la privacy, ma non offre protezione

Spesso si tende a pensare che le connessioni internet cifrate siano "protette".

Transport Layer Security, o TLS, è lo standard di cifratura utilizzato attualmente su Internet. Spesso i termini SSL e TLS vengono adoperati in modo intercambiabile. In realtà, SSL è uno standard obsoleto che è stato surclassato da TLS. Tuttavia, il termine SSL rimane quello più comune. L'importante è sapere che molti dicono SSL ma intendono TLS.

TLS è progettato per garantire riservatezza e autenticità, cifrando le comunicazioni tra due parti e verificando l'identità del server in base al relativo certificato e alla rispettiva autorità di emissione.



Il simbolo del lucchetto nel browser indica che la connessione è cifrata per garantire la privacy.

Quello che la cifratura TLS NON offre è la protezione, o garanzia di protezione, dai contenuti della pagina web. Un sito che ospita payload di malware può avere una connessione perfettamente valida che è cifrata e "protetta".

Quando si sente dire che una connessione a un server web è protetta, significa semplicemente che è protetta dalle intercettazioni (sebbene a volte anche questo potrebbe non essere del tutto vero). Ed è per questo motivo che ispezionare il traffico cifrato è importantissimo.

L'ispezione TLS non è semplice

La principale sfida presentata dall'ispezione TLS è il fatto che TLS è un protocollo estremamente complesso. Prevede lo scambio di vari certificati e i pacchetti di cifratura da utilizzare devono essere negoziati per stabilire come cifrare la connessione. A complicare ulteriormente la questione, esistono diverse versioni di TLS e molte applicazioni e servizi web adottano approcci differenti.

Di conseguenza, è possibile riscontrare incompatibilità anche quando sono stati implementati standard rigorosi. Tutto questo implica sfide molto difficili da affrontare per qualsiasi soluzione che cerchi di inserirsi nell'intero processo, al fine di ispezionare e proteggere i contenuti trasferiti.

L'importanza di TLS 1.3 e alcuni falsi miti da sfatare

La buona notizia è che il più recente standard TLS, ovvero TLS 1.3, include vari vantaggi rispetto ai suoi predecessori in termini di performance, privacy e risoluzione delle vulnerabilità.

L'adozione di TLS 1.3 sui server è ancora agli albori, ma attualmente tutti i principali browser supportano questo standard. Nonostante questo, poiché prevede un'implementazione molto complessa e un grande investimento di risorse in fase di ricerca e sviluppo, molti firewall con ispezione TLS attualmente disponibili sul mercato non offrono pieno supporto di TLS 1.3. Prevedono invece un downgrade forzato a TLS 1.2 e di conseguenza lasciano queste connessioni esposte ai tentativi di exploit e attacco, per via di vulnerabilità che sono invece state risolte nella versione più recente.

Proprio come avviene per molte nuove tecnologie, esistono vari falsi miti e fraintendimenti sull'ispezione di TLS 1.3. Alcuni sostengono persino che sia impossibile ispezionare il traffico TLS 1.3, ma non è assolutamente vero. Sebbene sia corretto dire che l'ispezione passiva di TLS (che veniva effettuata come extra) non è più possibile, questo traffico può essere ispezionato coinvolgendo un endpoint accessibile (ad es. uno appartenente alla rete aziendale).

Un'altra affermazione errata sostiene che il semplice atto di ispezionare flussi di traffico cifrato riduce il livello di protezione degli stessi. Questo è vero se si effettua il downgrade di una connessione TLS 1.3 a TLS 1.2, come fanno attualmente molte soluzioni di ispezione TLS. Le vulnerabilità presenti in TLS 1.2 possono favorire l'utilizzo di exploit da parte di un attacco Man-in-the-Middle (MITM) a scopo criminale. TLS 1.3 è stato progettato per risolvere queste vulnerabilità, per cui l'ispezione di questo traffico non introduce alcun rischio, se viene eseguita senza il downgrade.

Infine, alcuni sostengono che l'associazione del certificato rende l'ispezione TLS impossibile. Anche se questo è vero per alcune applicazioni con certificati hardcoded, la maggior parte delle applicazioni utilizza un approccio di associazione del certificato che rispetta il certificato della nuova firma e che è compatibile con le soluzioni di ispezione SSL.

L'importanza della convalida del certificato

La convalida del certificato è uno dei componenti essenziali di TLS, in quanto permette al client (o al dispositivo utilizzato per l'ispezione, ad es. il firewall) di verificare l'identità del server da cui proviene la comunicazione.

Tuttavia, per funzionare la convalida del certificato deve essere implementata correttamente, altrimenti i firewall e gli endpoint a cui sono connessi potrebbero essere indotti a ritenere di comunicare con un server diverso da quello effettivo, permettendo ai cybercriminali di infiltrarsi con un attacco MITM.

L'equilibrio perfetto tra performance, privacy e protezione

Oltre alle complessità tecniche dei flussi di traffico cifrati con TLS, occorre considerare e rispettare anche i limiti normativi e regolamentari applicabili. Inoltre, è possibile che buona parte del traffico cifrato con TLS sia generato da applicazioni aziendali attendibili e contenuti multimediali in streaming che potrebbero non richiedere ispezione.

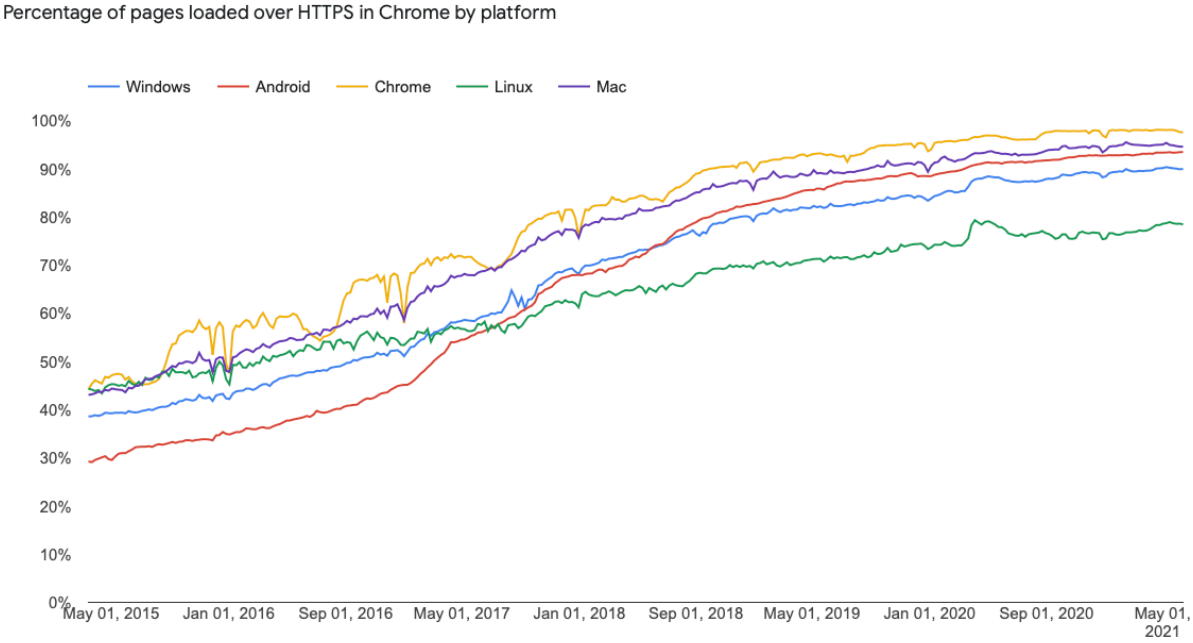
In pratica, non tutto il traffico cifrato può o deve essere gestito nello stesso modo. Si tratta di trovare il giusto equilibrio tra privacy, sicurezza, conformità e performance. Alcune giurisdizioni potrebbero imporre limiti specifici, mentre in altri luoghi spetta alle organizzazioni determinare tale equilibrio.

Purtroppo, i limiti delle soluzioni di ispezione TLS nella maggior parte dei firewall attualmente disponibili sul mercato costringono le organizzazioni ad adottare un approccio alquanto sbilanciato: sicurezza e conformità vengono spesso sacrificate per garantire livelli di performance e interoperabilità essenziali.

Il volume del traffico cifrato rasenta il 100%

La maggior parte delle connessioni Internet è completamente cifrata. Secondo il Rapporto sulla trasparenza di Google, più del 90% delle sessioni web su gran parte delle piattaforme è cifrato: un netto incremento rispetto al 60% di soli due anni fa.

Report sulla trasparenza di Google



Il volume del traffico cifrato ha subito un netto aumento negli ultimi due anni, con una tendenza che si avvicina al 100%.

La cifratura ha reso il tuo attuale firewall obsoleto?

A causa di questo enorme incremento del traffico cifrato, si è creato un enorme punto cieco nella sicurezza di gran parte delle organizzazioni. I firewall attuali non sono semplicemente in grado di ispezionare volumi così elevati di sessioni cifrate. Con la cifratura TLS, gran parte dei firewall è diventata a tutti gli effetti obsoleta, in quanto questi dispositivi non riescono più ad analizzare una fetta significativa del traffico di rete.

Il vero pericolo sono le minacce che si nascondono nel traffico cifrato

Con la crescita esponenziale della cifratura TLS negli ultimi anni, probabilmente non sorprende che gli hacker e i cybercriminali abbiano colto questa opportunità per infiltrare malware nelle reti e per garantirne la persistenza senza essere intercettati.

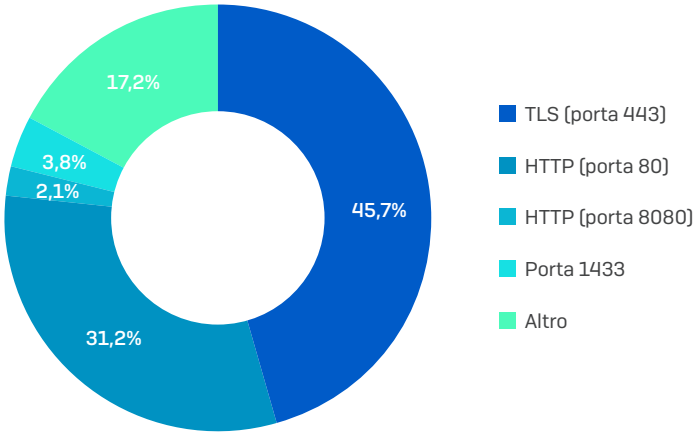
Durante gli ultimi 12 mesi abbiamo osservato in particolare un incremento nell'utilizzo di TLS per gli attacchi di ransomware, specialmente quelli con distribuzione manuale. Questo è in parte dovuto al fatto che gli hacker si servono di strumenti modulari che sfruttano la cifratura. Tuttavia, la maggior parte del traffico TLS dannoso proviene da malware realizzato per garantire l'accesso iniziale: loader, dropper e installer basati sui documenti, il cui compito è contattare pagine web sicure per recuperare i propri pacchetti di installazione.

Al momento quasi tutte le minacce sfruttano le connessioni cifrate per accedere alla rete.

Una volta infiltratasi nella rete, la minaccia sfrutterà tutti gli stratagemmi possibili per nascondere la sua presenza. L'utilizzo di TLS consente di eludere il rilevamento dei comandi inviati dai server di controllo al client. Allo stesso tempo, maschera le informazioni raccolte dalla rete e qualsiasi payload scaricato sull'host compromesso.

Di conseguenza, non sorprende che negli ultimi 12 mesi si sia osservato un netto incremento del malware che utilizza TLS per camuffare le proprie comunicazioni. Nel 2020 il 23% del malware che abbiamo rilevato utilizzava TLS per comunicare con un sistema remoto tramite Internet; oggi questa percentuale sfiora il 46%.

Comunicazioni del malware con i server di comando e controllo (C2), TLS vs altri, 1° trimestre del 2021

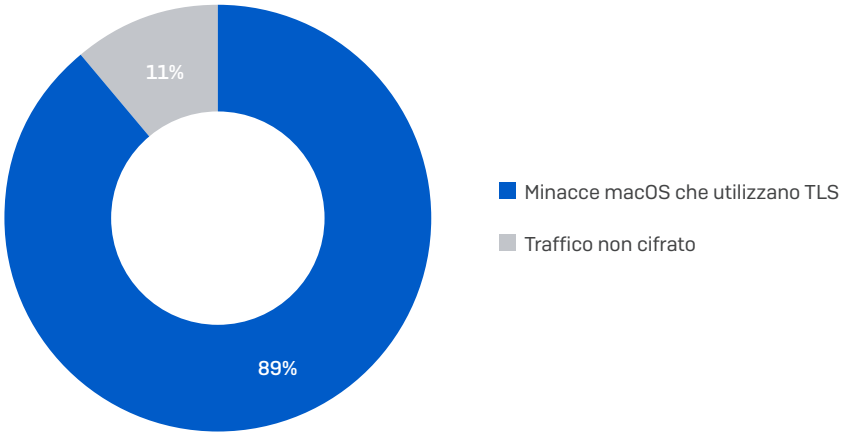


Analisi dettagliata delle comunicazioni in entrata del malware

È anche presente una frazione significativa di comunicazioni tramite TLS che adoperano una porta protocollo IP diversa dalla 443, come ad es. malware che utilizza un proxy Tor o SOCKS su un numero di porta non standard.

Gli hacker stanno cominciando anche a ospitare contenuti dannosi su servizi legittimi di condivisione come Discord, Github e Google Cloud, che impiegano la cifratura TLS per tutelare la privacy dei contenuti. Queste condizioni offrono al malware un ambiente di offuscamento perfetto, che consente alle minacce di infiltrarsi nella maggior parte delle reti senza essere rilevate.

Ma non sono solamente le minacce a sfruttare la cifratura per cercare di passare inosservate: anche applicazioni potenzialmente indesiderate come spyware, adware e barre degli strumenti nei browser, nonché client di condivisione dei file peer-to-peer e strumenti di elusione del proxy, utilizzano la cifratura per impedire di essere rilevate dal firewall. Lo dimostra il caso della piattaforma macOS, dove più dell'89% delle minacce macOS con comunicazioni verso centri di controllo C2 utilizza TLS per effettuare il call-home o recuperare altro codice dannoso.



La maggior parte delle organizzazioni ha le mani legate

Come abbiamo osservato, l'ispezione TLS è complessa e richiede molte risorse; inoltre, visto che più del 90% del traffico di rete è cifrato, sono pochi i firewall in grado di ispezionarlo.

Il problema è che nella maggior parte dei casi i firewall attualmente disponibili non hanno adeguate funzionalità di ispezione TLS. Non sono in grado di stabilire in maniera intelligente gli elementi da ispezionare e quelli da non esaminare; in più, non hanno la capacità di decifrare l'elevato volume di traffico rappresentato da tutti gli elementi da analizzare. Come se non bastasse, i loro motori di elaborazione e ispezione approfondita dei pacchetti (Deep Packet Inspection, DPI) non sono progettati per gestire l'ispezione TLS con efficienza. Inoltre, sono caratterizzati da un'implementazione scadente del processo di ispezione, che non supporta gli standard più recenti e che pertanto porta al downgrade della sicurezza; tutto questo a sua volta espone le organizzazioni a maggiori vulnerabilità e contribuisce a creare condizioni pessime per gli utenti.

Il rapido incremento del traffico di rete cifrato, unito all'incapacità della maggior parte dei firewall next-gen di ispezionare questo tipo di traffico, ha dato origine a una tempesta perfetta nella protezione della rete.

Cinque Caratteristiche Indispensabili Per Il Tuo Nuovo Firewall

Per minimizzare il rischio costituito dal traffico di rete cifrato, verificate che il vostro prossimo firewall includa queste cinque funzionalità essenziali per l'ispezione TLS:

1. Un motore di streaming all'avanguardia con alti livelli di performance per l'ispezione, in grado di supportare gli standard più recenti (come appunto TLS 1.3), compatibile con tutte le porte e tutti i protocolli, in modo da identificare il traffico rischioso e le minacce.
2. Un elenco preimpostato e intelligente di esclusioni che vengono aggiornate in maniera dinamica per evitare problemi di accesso a Internet per siti e servizi che non supportano o non richiedono la decifratura.
3. Massima visibilità direttamente dalla dashboard sui flussi di traffico cifrato e sui potenziali problemi derivati da siti e servizi non compatibili, per poter aggiungere eccezioni sul momento, prima che si creino problemi gravi.
4. Un sistema efficace di convalida dei certificati, in grado di gestire i certificati non validi, autofirmati, revocati o non attendibili, per evitare potenziali attacchi di tipo Man-in-the-Middle (MITM).
5. Strumenti per le policy che consentano di gestire la privacy degli utenti, la sicurezza dell'organizzazione e la performance della rete, al fine di raggiungere il giusto equilibrio in base alle vostre esigenze.

Sophos Firewall: progettato per l'attuale traffico Internet cifrato

La nuovissima architettura Xstream di Sophos Firewall e le nuove appliance XGS rappresentano la migliore soluzione di ispezione TLS disponibile in un firewall: la loro interazione permette di eliminare il punto cieco dell'ispezione TLS, senza alcun impatto sulla performance. Offrono:

- Performance elevatissima: un motore di streaming leggero con alta capacità di connessione e un nuovo design
- Livelli di visibilità insuperabili e disponibili direttamente dalla dashboard sui flussi di traffico cifrato e su eventuali errori, con l'opzione di aggiungere esclusioni con soli due clic
- Massima sicurezza: supporto di TLS 1.3 e di tutti i più recenti pacchetti di cifratura, con efficaci opzioni di convalida dei certificati
- Ispezione di tutto il traffico, essendo non dipendente da applicazione e porta
- Un elenco esteso e integrato di esclusioni per una performance ottimale e un'ottima esperienza utente, grazie all'ampia interoperabilità che consente di evitare problemi di Internet
- Potenti strumenti per le policy, che offrono un equilibrio perfetto tra performance, privacy e protezione

Per saperne di più, leggete il Briefing della soluzione XG Firewall oppure avviate una demo on-line immediata alla pagina www.sophos.it/firewall.

Effettuate subito una prova gratuita

Per una prova on-line gratuita di Sophos Firewall, visitate: sophos.it/demo

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

21-06-17 IT (DD)

SOPHOS