Chiarire l'impatto sulle prestazioni e le best practice per la decrittografia SSL/TLS su FTD

Sommario

Problema

Un utente sta pianificando di abilitare la decrittografia SSL/TLS su un dispositivo Firewall Threat Defense (FTD) e deve comprendere il potenziale impatto sulle prestazioni del dispositivo prima dell'implementazione. Le principali preoccupazioni includono:

- Impatto su throughput del firewall, latenza e prestazioni complessive di elaborazione del traffico.
- È previsto un aumento dell'utilizzo della CPU e della memoria dopo l'abilitazione della decrittografia.
- Linee guida per il dimensionamento e benchmark delle prestazioni per modelli FTD specifici.
- Limiti consigliati per le sessioni decrittografate simultanee.
- Procedure ottimali e prerequisiti per l'implementazione della produzione.

Ambiente

- Firepower 4115. Il problema potrebbe riguardare anche altre piattaforme hardware.
- FTD versione 7.4.2 (Build 172). Il problema può riguardare anche altre versioni software.
- Considerazioni sulla funzionalità di decrittografia SSL/TLS.
- Pianificazione dell'installazione dell'ambiente di produzione.

Risoluzione

La decrittografia SSL/TLS non aggiunge un sovraccarico di elaborazione a Firepower 4115, ma l'impatto effettivo dipende in larga misura dalla quantità di traffico decriptato e dal tipo di ispezione applicata dopo la decrittografia.

Analisi dell'impatto delle prestazioni

Gli impatti della decrittografia SSL/TLS includono:

- Throughput effettivo inferiore.
- Latenza più elevata.
- Aumento dell'utilizzo della CPU per snort/ispezione.
- Aumento di CPU e memoria che non può essere previsto con precisione come percentuale fissa senza un'analisi del profilo di traffico reale.

Benchmark delle prestazioni FPR 4115

Specifiche di benchmark Firepower 4115 pubblicate da Cisco:

- Velocità effettiva decrittografia hardware TLS: 6.5 Gbps.
- Throughput FW + AVC: 33 Gbps.
- Numero massimo di sessioni simultanee con AVC: 15 milioni.
- Numero massimo di nuove connessioni al secondo con AVC: 210 K.

Nota importante sul dimensionamento: Il benchmark per la decrittografia hardware TLS a 6,5 Gbps è basato su condizioni di test specifiche. La velocità di produzione può essere inferiore se si decrittografa una grande percentuale del traffico, si ispeziona il traffico decrittografato con policy di intrusione/file/malware o si elaborano molte sessioni TLS di breve durata.

Cisco non pubblica un numero separato di "sessioni decrittografate simultanee massime" per Firepower 4115 su FTD 7.4.2. In pratica, la capacità viene convalidata usando una combinazione di traffico, sessioni simultanee, velocità di connessione, suite di cifratura e caricamento della

policy di ispezione.

Approccio consigliato per l'installazione in produzione

Passaggio 1: Iniziare con un programma pilota limitato

- Inizialmente non abilitare le regole generali di "decrittografia totale".
- Iniziare con gli utenti, le subnet o le categorie di destinazione selezionate.
- Mantenere la gestione predefinita conservativa con Non decrittografare per il traffico che non richiede ispezione.

Passaggio 2: Escludere il traffico che in genere si interrompe con la decrittografia

- Siti bancari/finanziari.
- Portali medicali.
- Applicazioni protette da certificati.
- Alcune applicazioni SaaS (Software as a Service) e per la sicurezza degli endpoint/cloud.
- Applicazioni business-critical sensibili, se non testate esplicitamente.

Passaggio 3: Mantieni le regole SSL semplici e ordinate con attenzione

- Posizionare le esclusioni di Do Not Decrypt specifiche al di sopra delle regole di decrittografia più ampie.
- Evitare, se possibile, corrispondenze troppo estese o complesse.
- Non utilizzare la versione TLS o le condizioni della suite di cifratura per le regole Decrypt-Resign/Known-Key, in quanto i documenti Cisco possono causare comportamenti imprevedibili.

Passaggio 4: Convalida preparazione certificato

- Per Decrypt-Resign in uscita, il certificato CA di firma deve essere considerato attendibile dagli endpoint client.
- Per la decrittografia con chiave nota in ingresso, il firewall deve disporre del materiale del certificato del server o della chiave privata corretto.

Passaggio 5: Monitoraggio durante il rollout

- Monitoraggio dell'utilizzo complessivo della CPU e, ancora più importante, dell'utilizzo della CPU per l'esecuzione di operazioni di snort/ispezione.
- Rilevamento delle connessioni simultanee e delle nuove connessioni al secondo.
- Controllare lo stato del flusso SSL o gli errori di handshake negli eventi di connessione.
- Controllare gli indicatori di sovrascrittura TLS e gli errori specifici dell'applicazione.

Per ulteriori informazioni su come monitorare la CPU, controllare:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Pensa come un ingegnere TAC: Guida ai punti critici più comuni di Cisco Secure Firewall

Per tenere traccia delle connessioni e delle nuove connessioni al secondo, controllare:

- Registrazione delle procedure ottimali

Per tenere traccia degli errori di handshake o di stato del flusso SSL negli eventi di connessione, controllare gli indicatori di sovrascrittura TLS:

- Risoluzione dei problemi di sovrascrittura TLS/SSL

Passaggio 6: Eseguire il rollback o l'ambito ristretto se viene visualizzato:

- Saturazione continua della CPU.
- Aumento della latenza visibile all'utente.
- Errori di handshake TLS.
- Errore delle applicazioni aziendali dopo la decrittografia.

- Sovrabbonamento o errori SSL eccessivi.

Passaggio 7: Considerare l'impatto di TLS 1.3

L'adozione di TLS 1.3 può influire sulla visibilità e sul comportamento, in quanto alcune caratteristiche di handshake e ispezione differiscono da TLS 1.2.

Causa

La decrittografia SSL/TLS richiede ulteriori risorse di elaborazione per decrittografare, ispezionare e crittografare nuovamente i flussi di traffico. L'impatto sulle prestazioni varia in modo significativo in base ai modelli di traffico, ai criteri di ispezione applicati al traffico decrittografato e alla configurazione di distribuzione specifica. Senza una pianificazione adeguata e un'implementazione graduale, le organizzazioni possono sperimentare un peggioramento inatteso delle prestazioni negli ambienti di produzione.

Contenuto correlato

- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center - Regole di decrittografia
- Guida ai criteri di decrittografia del firewall sicuro Cisco
- Procedura consigliata per l'ordine delle regole dei criteri di decrittografia
- Semplificazione della decrittografia con Cisco Secure Firewall 7.7
- Procedure consigliate per le regole di decrittografia
- Scheda tecnica di Cisco Firepower serie 4100
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).