

Visibilità per traffico SSL

Problema

Al giorno d'oggi più del 90% del traffico Web su Internet è crittografato. Di fatto, la notizia che Google non indicizzerà i siti Web non crittografati è stato il fattore decisivo che ha provocato l'abbandono del protocollo HHTP a favore di HTTPS: Senza dubbio, questo comporta il fatto che le imprese perdono la possibilità di avere la visibilità del traffico necessaria sul posto di lavoro e questo rende impossibile individuare le minacce su Internet. D'altra parte, chi fa attacchi consapevoli di fatto utilizza già vettori di attacco con crittografia SSL per la maggior parte degli attacchi noti, Command&Control, Criptolockers, ecc.

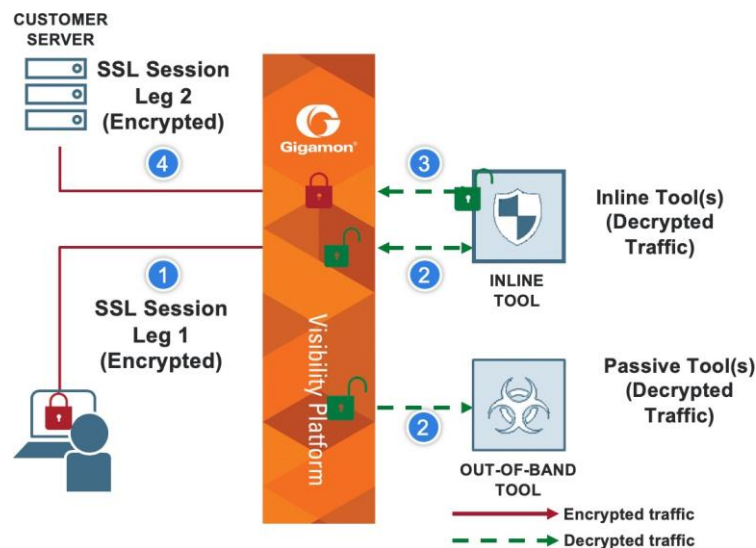
Soluzione

Grazie alla soluzione di de-crittografia unificata di Gigamon è possibile conservare la visibilità del traffico in uscita tramite internet anche quando è crittografato tramite l'uso di tecniche MitM (Man-in-the-Middle).

Gigamon offre la possibilità di decriptare SSL una sola volta, per consentire che tutte le soluzioni di sicurezza possano vedere il traffico in chiaro e una volta messo in sicurezza tale traffico possa essere nuovamente crittografato fino alla destinazione finale. Le caratteristiche di tale soluzione comprendono:

- ✓ Soluzione unificata per strumenti online e offline.
- ✓ Selezione della versione di SSL da TLS1.0 a TLS1.3.
- ✓ Supporto RSA, DHE, PFS, ECC
- ✓ Protocolli di revoca: CRL e/o OCSP
- ✓ Rilevazione di traffico non bilanciato.
- ✓ Uso di due certificati, uno noto e uno non valido, per poter replicare lo stato del certificato remoto.

Schema



SSL in linea
OOB-SSL
Flow Mapping
Load Balancing

[LINK](#)