ntopng: aggiunta di un nuovo check per notificare un numero anormale di host name contattati

Gaetano Barresi 579102 - Stefano Russo 544341 - A.A. 2020/2021

Introduzione

ntopng è un'applicazione web-based per il monitoraggio del traffico di rete. Oltre ad analizzare il traffico, collezionare e catalogare i flussi e molto altro, ha dei meccanismi per notificare le anomalie e i comportamenti sospetti del traffico analizzato. Questi meccanismi prendono il nome di alert e check.

Un alert viene creato da ntopng per flussi, host e altri elementi di rete e notifica la presenza di un possibile problema. Gli alert vengono creati all'interno dei check, frammenti di codice eseguiti periodicamente da ntopng per effettuare controlli su determinate condizioni, che se soddisfatte generano un alert.

Domain Names host check

ntopng è stato esteso con un nuovo check per il controllo del numero di host name diversi contattati da un host client. Ogni minuto il check effettua il controllo su un contatore e notifica l'eventuale superamento della soglia fissata, con valore di default uguale a 250. Il contatore verrà resettato alla fine di ogni controllo.

Dettagli sull'implementazione

È stato aggiunto un contatore di tipo HyperLogLog (HLL), una struttura dati probabilistica usata per stimare la cardinalità di un insieme, nella classe LocalHostStats con lo scopo di raccogliere i vari host name contattati. Al momento della creazione di un nuovo flusso, viene aggiunto un nuovo elemento nel contatore (operazione effettuata nella classe Flow). Successivamente, per implementare il controllo sul contatore sono stati creati i file relativi al check e all'alert, in aggiunta ad alcuni file lua necessari per la loro configurazione. La procedura completa per effettuare questi passaggi è spiegata nella documentazione ufficiale di ntopng.