Monitorare la rete con Netflow

Autori: Nino Ciurleo, Alessandro Inzerilli, Simona Venuti

Abstract

Il monitoraggio della rete basato sul protocollo Netflow consente di superare alcuni limiti intrinseci dei sistemi tradizionali basati sul protocollo SNMP (MRTG, Cacti, Cricket, etc.). Questi ultimi infatti consentono di raccogliere statistiche esclusivamente sulla quantità di traffico che attraversa gli apparati di rete.

I sistemi che si servono del protocollo Netflow consentono invece di ottenere informazioni dettagliate sulla natura del traffico, quali i protocolli e le applicazioni utilizzate, la sorgente e la destinazione dei flussi di traffico.

L'analisi dei dati estratti dai flussi Netflow costituisce pertanto uno strumento importante al servizio degli amministratori di rete sia per tenere sotto controllo l'utilizzo delle risorse di rete che per individuare eventuali minacce dal punto di vista delle sicurezza informatica.

Nel corso del tutorial verrà spiegato come realizzare un sistema per l'esportazione, la collezione e l'analisi dei flussi Netflow, basato sulla suite software open source Nfsen/Ndump, scelta dal GARR per il monitoraggio della propria rete. Molto spazio verrà dedicato ad illustrare gli strumenti che la suite mette a disposizione e che consentono di estenderne le funzionalità, con particolare riferimento alla scrittura di plugin.

Sito di riferimento:
http://nfsen.sourceforge.net