Taming Big Flow Data

Intelligent Approach to Integrating Flow data with Mainstream Event Management Systems

Igor Balabine, CTO
Sasha Velednitsky, Co-Founder

NetFlow Logic

www.netflowlogic.com

© Copyright 2011-2012 NetFlow Logic Corporation
Modern network devices can create 400K flows / sec. (1.6TB/day of NetFlow data from a single device)

NetFlow collectors are incapable of processing that much data at reasonable cost

This problem requires a drastically new approach

NetFlow collectors / analyzers often are isolated from other log management
● Consolidated flow information is sent to SIEM in syslog format
● SIEM may request to provide detailed NetFlow data in $\Delta t$ around interesting events
- Traffic Summary
- The number of network policy violations, such as ACL, exceeds a certain threshold
- A host on internal network generates unusual traffic volume
- A host on internal network generates unusual number of connections
- Events based on host reputation
- And so on… just add rules to NetFlow Integrator
- Event: configuration change
- Was the user who made the change associated with the network flow of the source IP address assigned to that user?
- Request is sent to NetFlow Integrator: provide network traffic detailed for $\Delta t$ around the event
- If the user who made the change was not associated with the network traffic – we discovered an imposter!
Example: NFI-Storage + Splunk

- Splunk App for Enterprise Security detects security event and requests the underlying flow information through NetFlow Integrator Proxy.
- NetFlow Integrator retrieves flow records for $\Delta t$ around the event and sends them in syslog format via Splunk Technology Add-on.