FlowIntegrator™

NetFlow LOGIC

Integrating Flow Technologies with Mainstream Event Management Systems

**Sasha Velednitsky**

svelednitsky@netflowlogic.com

**NetFlow Logic Corporation**

January 2012

Problem

- **Network infrastructure devices and devices connected to the network generate disparate types of information flows (syslog, SNMP, NetFlow, sFlow, etc.)**

- **Unless all sources of information are integrated, critical insights into network management or network security will be missed**

- **Unless security events are identified in real time, your enterprise is at risk**

- **Unless network problems are discovered in real time, your organization suffers**
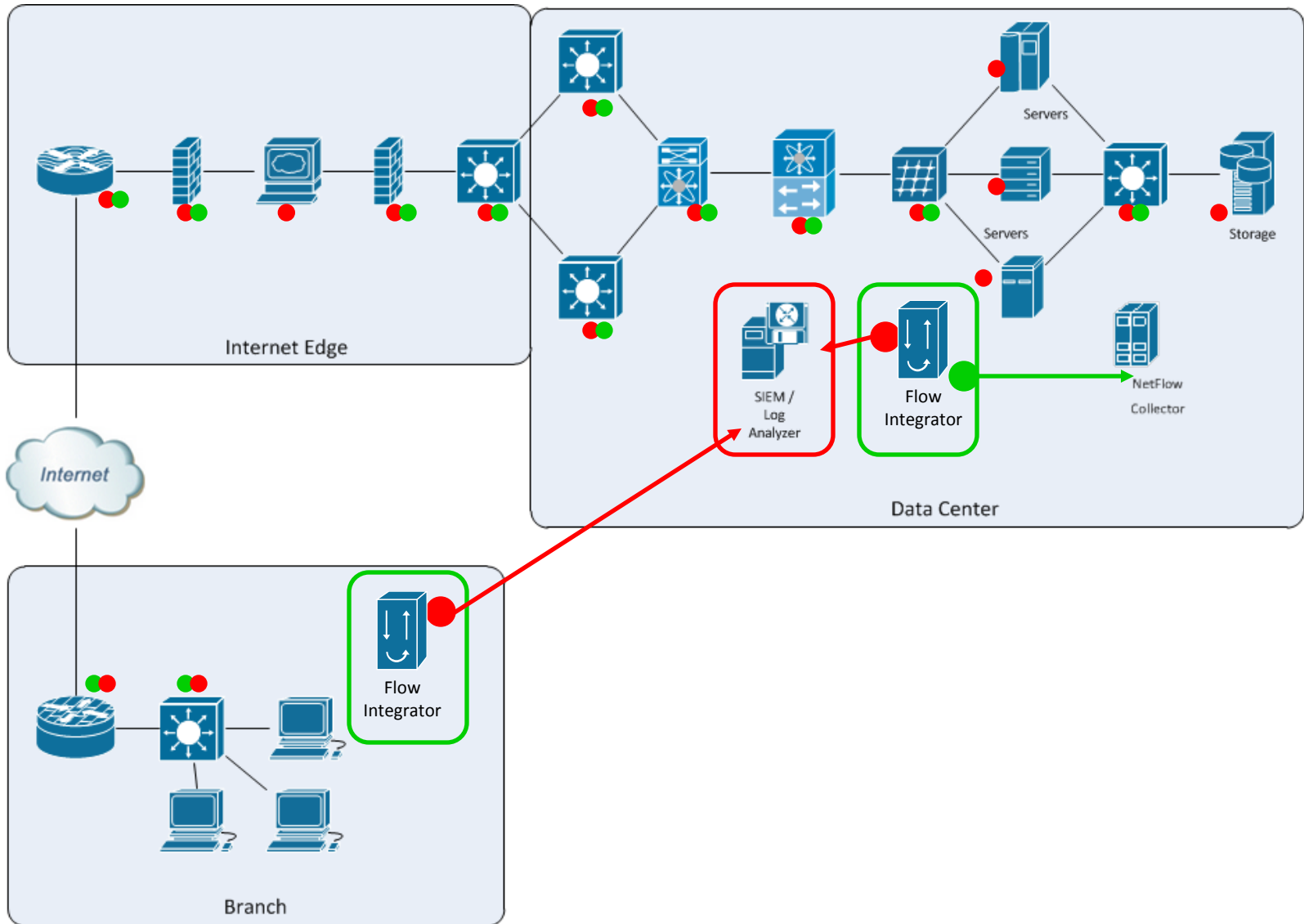
Collecting Syslogs
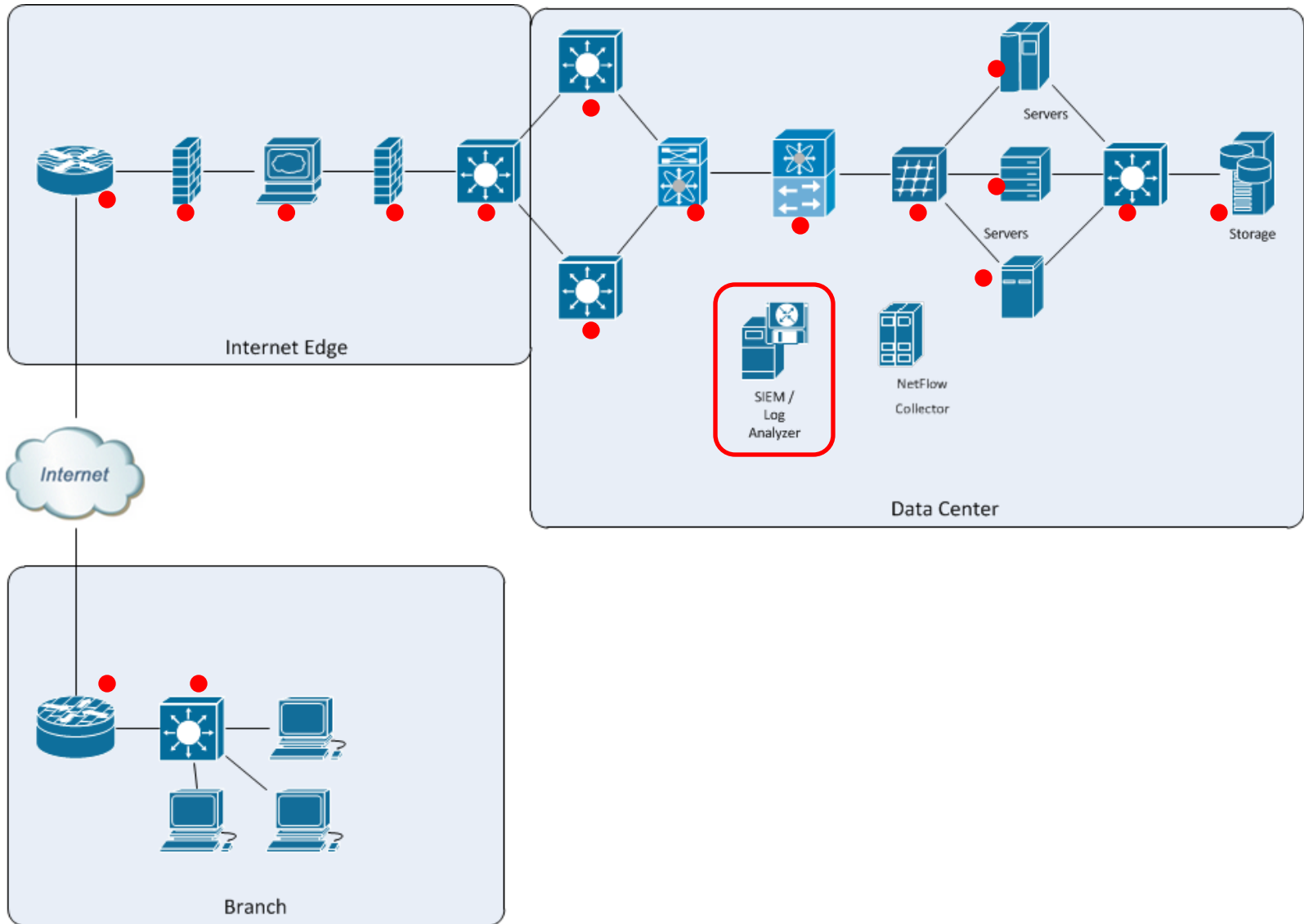
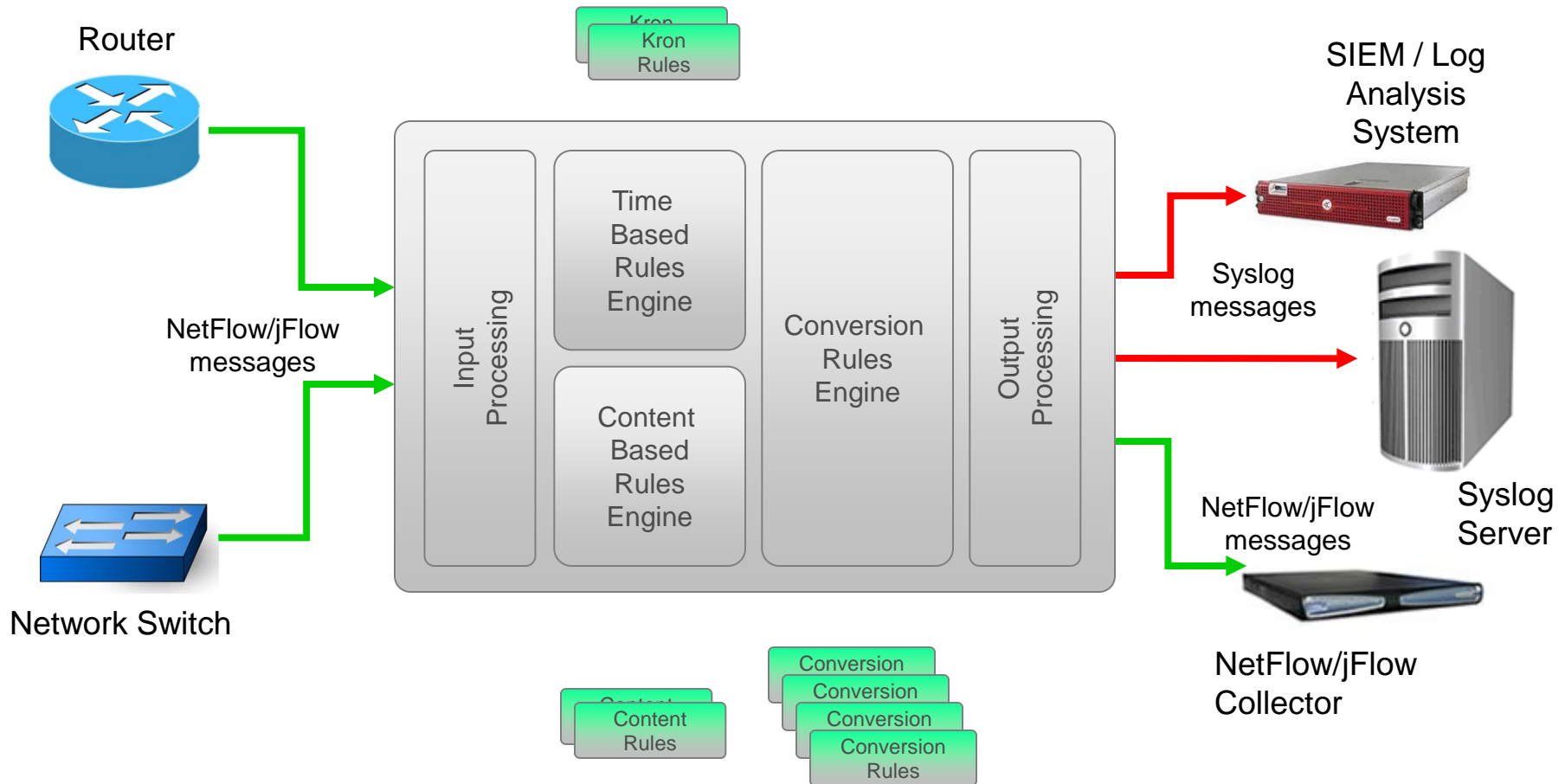# Collecting Flows
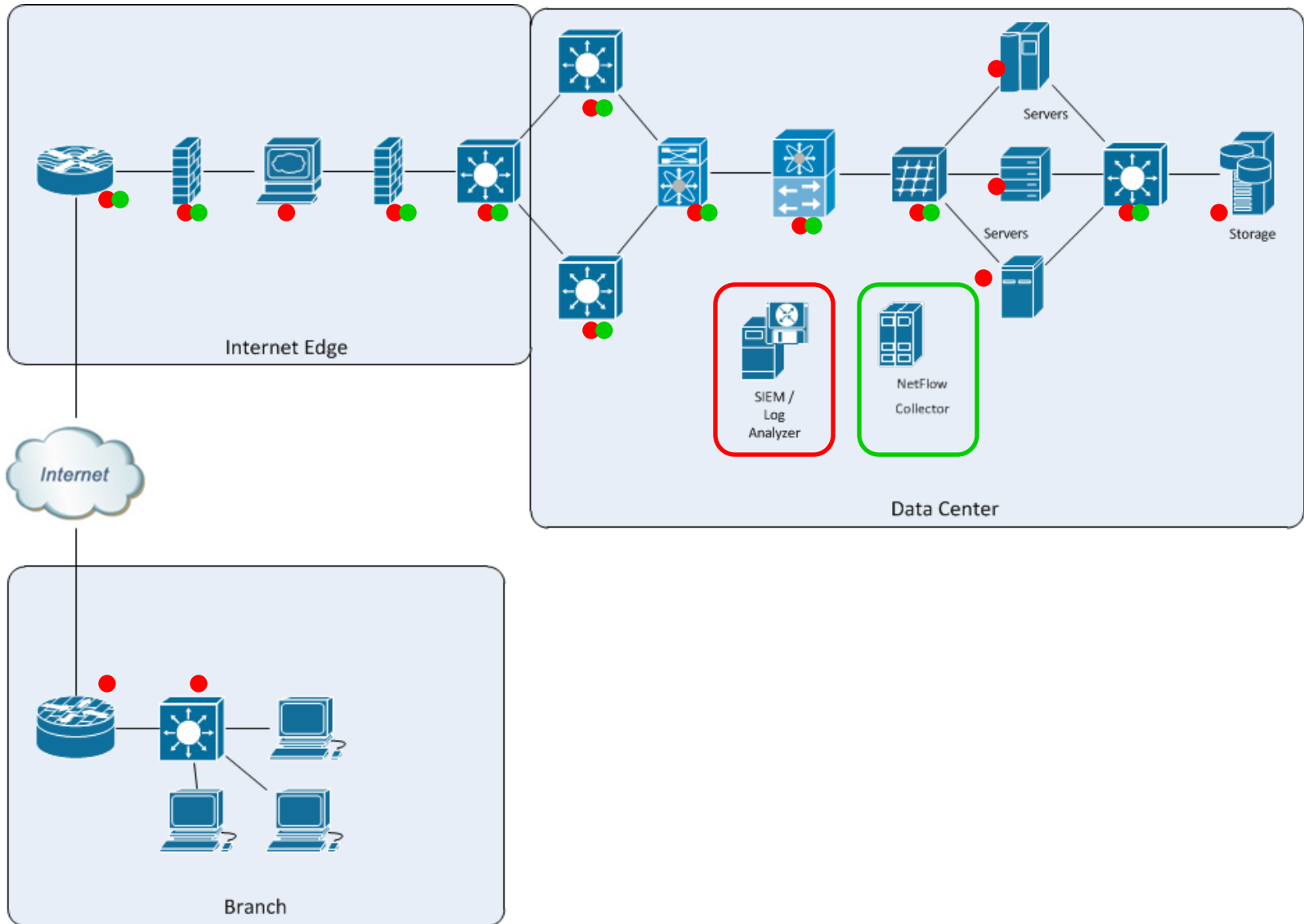
Putting It All Together!

Challenges

- **Mid to high end routers may generate hundreds of thousands flow records per second**

  - Cisco ASR1000© series router Firewall and CGN features generate up to 400K NetFlow records per second

- **Too much data**

  - Flow data consumes terabytes of disk space

- **Flow data is transmitted in hard to decode binary format**

  - NetFlow v9/IPFIX protocol allows variable record structure

- **Difficult to process in real time**

  - Existing solutions require costly distributed infrastructure

FlowIntegrator Technology

- **Introduces a mechanism to intelligently process flows based on the content of records**

- **Permits configuring arbitrary filtering, aggregation, deduplication and obfuscation rules**

- **Time based rules allow for the reporting of flow aggregations and network events in real time with as little as 1 second resolution**

- **By converting flow information into the syslog format, seamlessly integrates flow data producers with all existing log collectors and SIEM systems**

- **Transparently fits into the existing flow data collection infrastructure**

- **Converts to syslog over 350K flow records per second on an 8 core Intel Xeon processor**

FlowIntegrator Ecosystem

Router

Kron
Kron
Rules

NetFlow/jFlow
messages

Network Switch

Input Processing

Time Based Rules Engine

Content Based Rules Engine

Conversion Rules Engine

Output Processing

SIEM / Log Analysis System

Syslog messages

Syslog Server

NetFlow/jFlow messages

NetFlow/jFlow Collector

Content
Content
Rules

Conversion
Conversion
Conversion
Conversion
Rules

Processing Rules

- **Rule-based technology able to process multiple flow formats such as NFv5, NFv9, jFlow, IPFIX, etc**

- **Rules are created via a GUI or SDK**

- **A rule may be applied to a specific record type or a subset of record types, or to all flow packets passing through FlowIntegrator**

- **Administrators may also specify one or more time-based ("kron") rules for reporting aggregated information**

- **Rules can be chained**
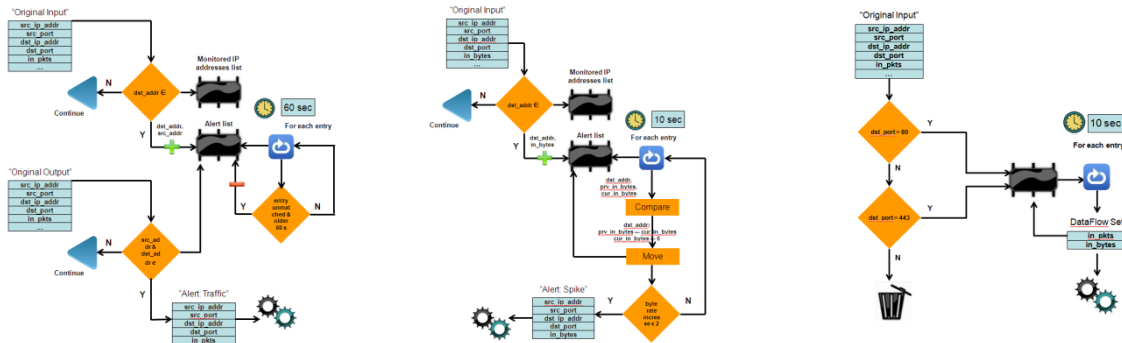
Conversion Rules

- **A conversion rule implements mapping of a flow record to one or more syslog messages or flow packets**

- **Flow protocol to syslog maps are created via the built-in GUI or SDK**

- **Default built-in conversion rule provides one-to-one mapping of data in a flow record to a syslog message**

In this example the resulting syslog message contains a standard header (blue), sourceIP:sourcePort , destIP:destPort, and the number of packets exchanged in this flow (prefixed with "P")
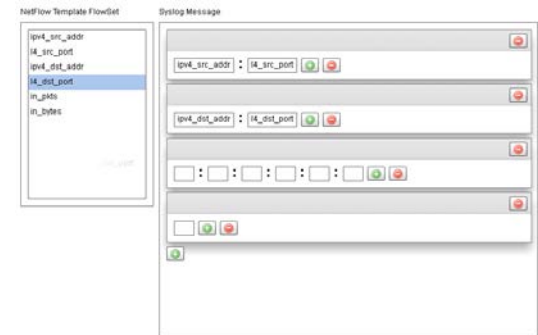
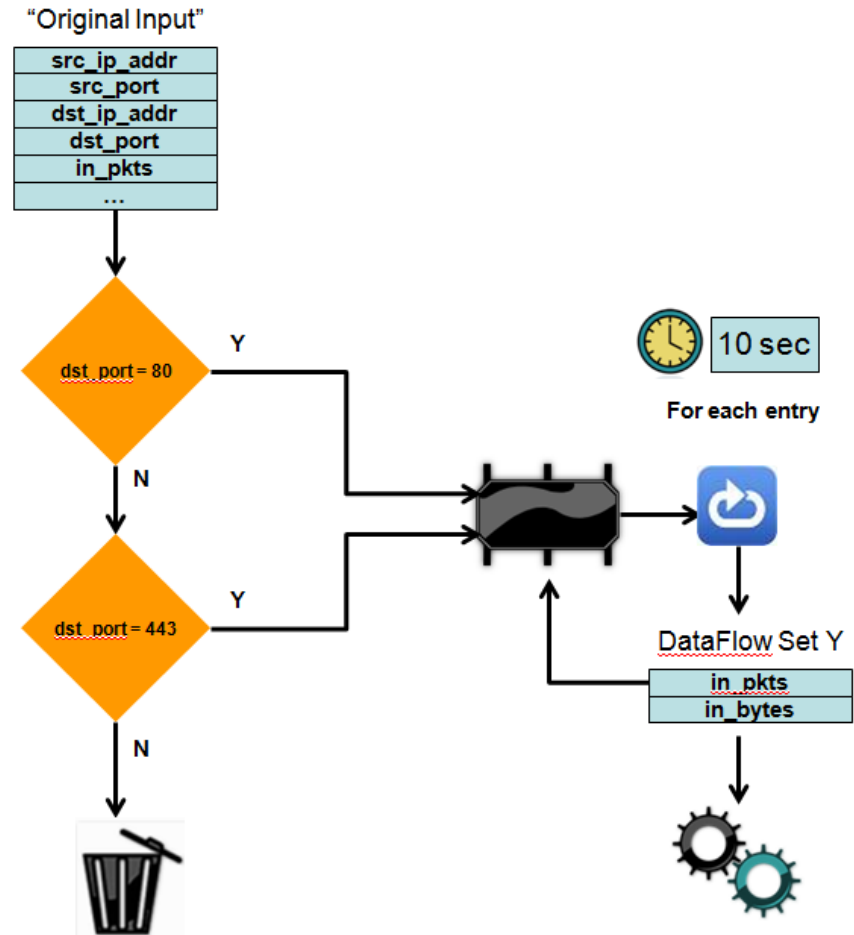**Feb 26 18:23:47 10.10.0.2 0:0:2:2 10.10.1.14:28382 10.10.2.7:389 P:876**

Example Rule: Aggregation

Objective:

Report current traffic load by application by router. In this simplified example we show a rule that reports incoming traffic to all web servers

FlowIntegrator Solution:

Sum up the number of bytes and packets of the observed web traffic, and report accumulated volume every 10 seconds

"Original Input"

| src_ip_addr |
| src_port |
| dst_ip_addr |
| dst_port |
| in_pkts |
| ... |

dst_port = 80 → Y

dst_port = 80 → N

dst_port = 443 → Y

dst_port = 443 → N

10 sec — For each entry

DataFlow Set Y

| in_pkts |
| in_bytes |

**Feb 26 18:23:47 10.10.0.2 0:0:2:2 Server=10.10.1.14 Packets=976 Bytes=999423**

Example Rule: Detecting Unusual Traffic

Objective:

Detect an infected host on internal network. In this example the rule identifies an "off-limits" device on the internal network which responds to an outside peer

FlowIntegrator Solution:

Examine NFv9 "Original Input" and "Original Output" records and send a syslog message when one of the monitored internal devices attempts an egress communication in response to an ingress communication
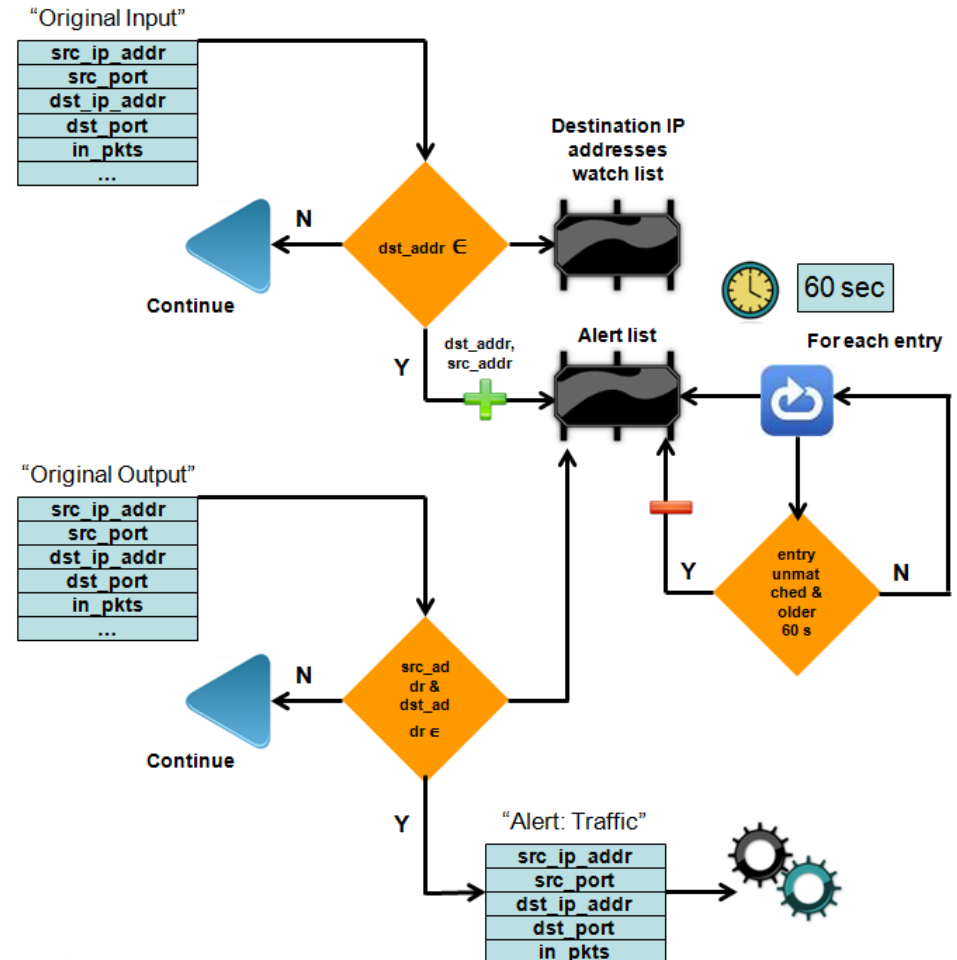

Feb 26 18:23:47 10.10.0.2 0:0:2:2 Ext=77.10.1.14:22213 Int=10.10.1.21: 8080 Alert=Traffic Pkts=425

Features and Benefits

- **FlowIntegrator is a NetFlow/IPFIX Mediator providing real time integration of network metadata into existing SIEM systems, syslog analyzers, flow data collectors, and network management systems**

- **Enables network administrators to:**

  - detect important network events in real time

  - identify applications for network management and security purposes

  - monitor and troubleshoot their networks for packet loss and jitter

  - filter and aggregate network metadata information

  - enable assured delivery of network metadata information to log collectors

- **Eliminates storage and sifting through terabytes of flow data**

FlowIntegrator – Performance

Throughput, rec/sec, '000
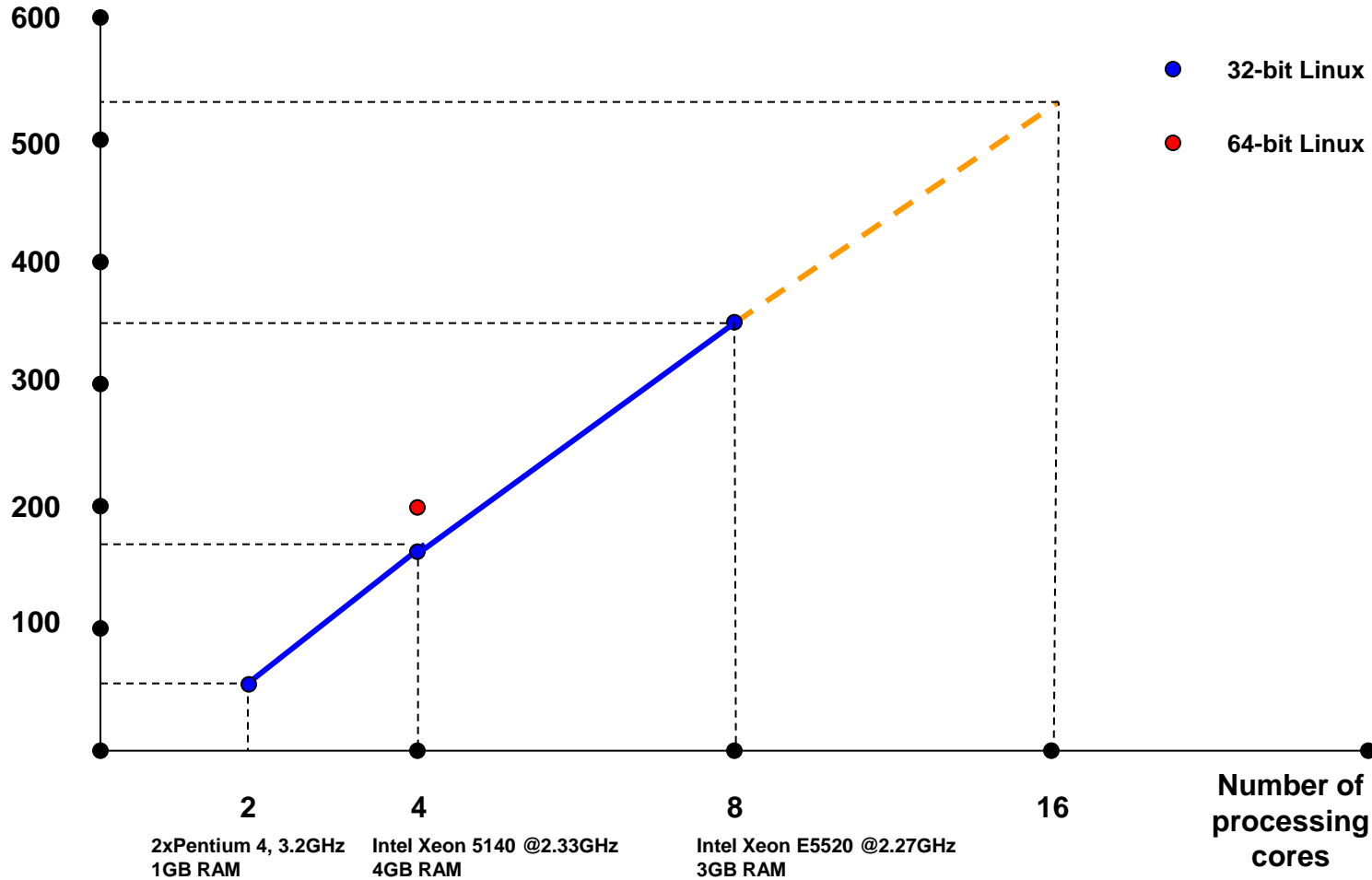
Thank You for Your Time

Contact information:

- **Company: NetFlow Logic Corporation**

- **www.netflowlogic.com**

- **Email: info@netflowlogic.com**