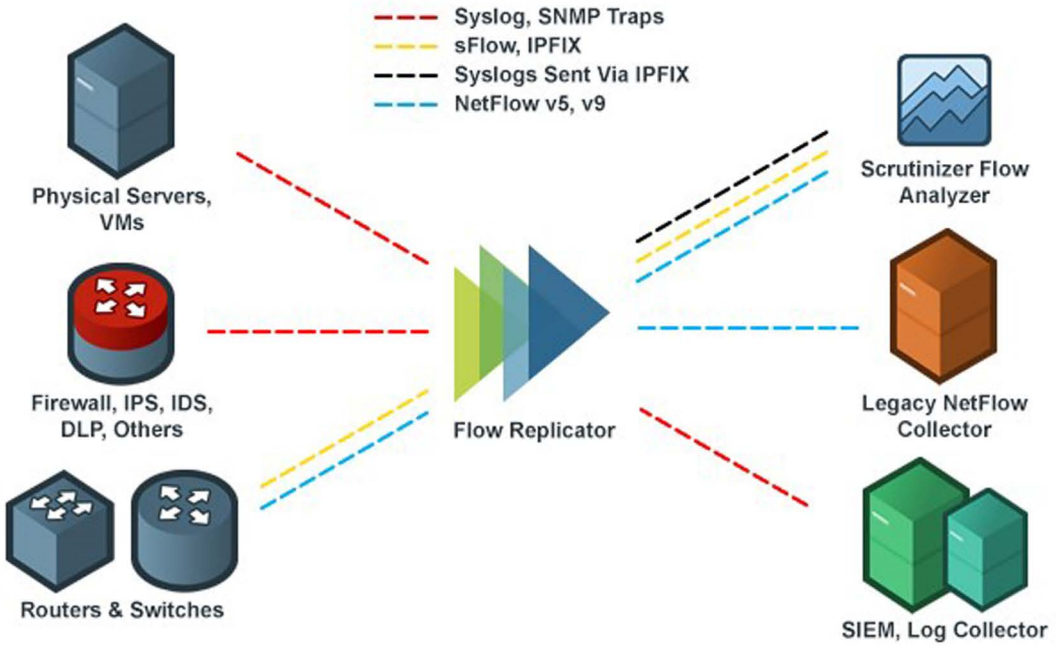
Scrutinizer Incident Response System: Replicator 3.1

Many routers, servers, and other systems can only send messages to a single log management system. The Flow Replicator™ allows a single stream of log and flow data to be transparently replicated to multiple destinations.

Flow Replicator™ Features include:

- Deterministic Packet Forwarding (DPS) feature detects when the destination hosts are offline and stops forwarding traffic
- Helps simplify network configurations by providing a single IP to which all routers and servers can send their log data
- Reduces the amount of traffic on the network and reduces the amount of load on routers and switches that are capable of exporting to more than 1 exporter. Reducing the export to a single destination allows the router, switch and server operating systems to recover hardware resources.
- Can provide redundancy by sending logs to multiple destinations simultaneously
- Ability to export replication statistics to an IPFIX enabled collector
- Interactive command line interface simplifies complex configurations
- High availability configurations (for Fault Tolerance)



Scrutinizer™
Incident Response System

Scrutinizer Incident Response System: Replicator 3.1

Syslog to IPFIX Gateway

The Replicator Appliance listens for syslogs, extracts the details and forwards them on inside IPFIX datagrams. Once Scrutinizer™ has the messages, reports can be run including details that stretch across the different devices exporting syslogs. Scrutinizer™ log analyzer can correlate the messages and trigger alarms for specified events which aids in security log analysis.

The Replicator allows companies who need to meet the needs of regulatory compliance to ensure a backup of all system messages and notifications should an audit become necessary. The Flow Replicator™ and Scrutinizer™ log reporting solution together provide:

- Detection of a wide range of network threats including APTs, employee misuse, DoS attacks, and C&C communications.
- Security Audit trails of all network traffic and behaviors, enabling rapid reaction to network incidents
- Detailed network utilization reports that provide insight into users, applications, and network misconfigurations

Scrutinizer™ is designed to peer deep into the network traffic enabling the administrator to easily see where threats are originating and how the communication fabric is being used. This capability aids in the reduction of the Mean Time to Know (MTTK) pertaining to a potential threat.

Scrutinizer™
Incident Response System