BROCADE AND IBM
REAL-TIME NETWORK SECURITY
INTELLIGENCE GATHERING
AND ANALYSIS SOLUTION

HIGHLIGHTS
• Seamless integration between Brocade® MLXe® Series telemetry-enabled devices and IBM® InfoSphere™ Streams real-time intelligence-gathering analytics platform allows you to non-disruptively extract and analyze massive data flows from production networks in real time.
• Sophisticated algorithms from IBM for processing enormous volumes of raw structured and unstructured data enables delivering intelligence-related alerts in milliseconds.
• The streaming analytics paradigm applies analysis and modeling to data in motion, significantly reducing the time to produce actionable data.
• An open-ended platform allows you to aggregate and correlate data from a wide variety of sources and deliver results to your choice of mediation devices.

REAL-TIME ANALYTICS

Real-Time Analytics on Massive Data Flows with IBM InfoSphere and Brocade MLXe Telemetry Devices

OVERVIEW
Today, IP networks must carry enormous levels of traffic that behave unpredictably, so it is becoming increasingly important to have a sophisticated level of visibility within the network. Network telemetry is used by organizations to monitor their networks for packet inspection and analysis, security intrusion and attack detection, intelligence-gathering, application performance management, and a wide range of other applications. If an organization is not able to monitor its network effectively it may miss out on valuable security information needed to protect vital assets from internal and external threats.

SOLUTION
The Brocade MLXe is a high-performance network telemetry-enabled device that can non-disruptively and transparently tap into a production network with no loss of performance. The Brocade MLXe is able to replicate the ingress data to any number of egress ports by applying filtering rules while operating at full line rate. A sophisticated interface between IBM InfoSphere Streams to the Brocade MLXe allows the filtering rules to be dynamically modified in real time based on the analytics being performed. The Brocade MLXe can automatically load balance traffic at a per-flow level towards a cluster of IBM InfoSphere Streams servers. With industry-leading port densities, this provides a scalable, advanced, and carrier-class solution that focuses on the need for high-end, demanding customer environments where low-latency, throughput, flexibility, and performance are of paramount importance.

IBM InfoSphere Streams is a powerful analytics engine that can collect and analyze data in real-time from the Brocade MLXe, as well as other static and dynamic data sources, including databases, files, the Web, sensor networks, and social media. Sophisticated, powerful, and breakthrough pattern recognition and anomaly detection algorithms allow users to respond to events in real-time and in changing environments. IBM InfoSphere Streams can adapt to rapidly varying data forms and data types and can process massive volumes of data at rates far superior to traditional data processing solutions.

IBM InfoSphere Streams shifts away from the traditional computing paradigm in which queries are run against relatively static sources of data. Instead, it uses a stream computing framework in which results are continuously updated in real time against data that is actively flowing. This approach makes IBM InfoSphere Streams the ideal platform for analyzing the variety and volume of network traffic at the velocities required in real time, which significantly reduces the time to produce actionable results. The IBM InfoSphere Streams platform is...
openly extensible on a distributed runtime environment, with inherent clustering capabilities. As the throughput of network data needed for analysis grows, and as analytics and modeling become more complex, this solution can be easily scaled up on more powerful hardware or scaled out and clustered across multiple physical machines.

APPLICATIONS

Governments, telecommunications service providers, and enterprises are faced with a myriad of wide-ranging business and technical demands. In order to provide a minimum baseline level of security, all users need to be protected from malicious and harmful content on the network. The joint Brocade MLXe and IBM InfoSphere Streams solution addresses this need in real time, while processing the large volume of data seen on networks every day. For example, IBM InfoSphere Streams can be programmed to provide complex behavior analysis on traffic patterns, user interactions, and the sentiment expressed in messages carried over the network. When higher levels of security are needed to protect against more advanced security threats, IBM InfoSphere Streams can further enrich the results by showing the location or country from which a threat emanates, as well as providing offerings to defend from such infiltration.

Complex text analytics can explore patterns and identify non-normal behavior, which can lead to the detection of “botnets” and other cyber-attacks. Brocade MLXe can also replicate traffic to other permanent repositories, like IBM Netezza® or IBM InfoSphere BigInsights, for later analysis or long-term storage. For example, Voice over IP (VoIP) calls may be monitored for keywords showing the location or country from which In some cases, deep packet inspection and content analysis of traffic can provide clues to security administrators about potential threats. IBM InfoSphere Streams combines this ability with data at line rate from other static and dynamic sources, which can enrich the results.

Lawful intercept may require the active tracking and monitoring of a person of interest across the network. Sophisticated algorithms can be used to build relationship graphs showing who a person of interest has interacted with, classifying the type of interactions the user is having with the various data sources, and also correlating different aliases that the person of interest may be using across different media platforms. IBM InfoSphere Streams can be programmed to interface with an existing mediation platform and deliver the results in a secure fashion.

For more information, visit www.brocade.com.

© 2012 Brocade Communications Systems, Inc. All Rights Reserved. 02/12 GA-AG-429-00

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.