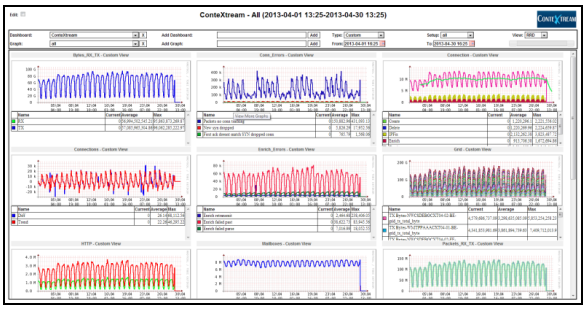
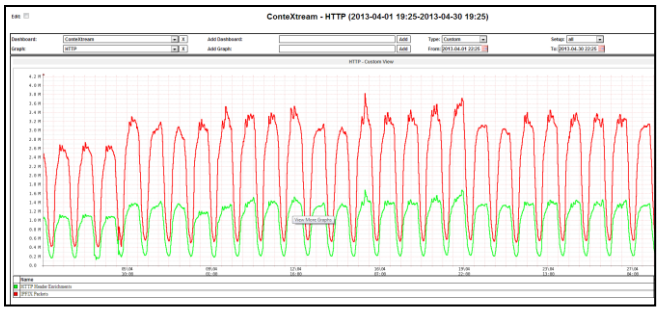
ContexView™

Visibility & Monitoring

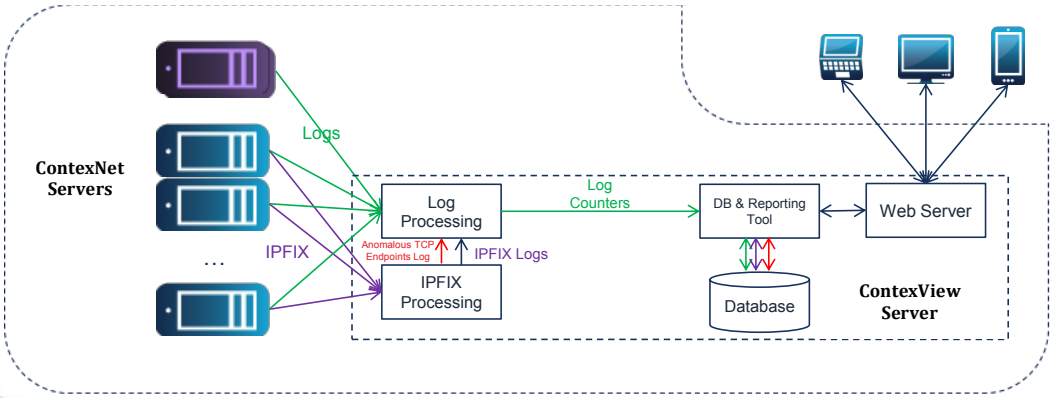
ContexView provides service providers with the visibility they need to run a carrier grade service in an SDN environment. It monitors network performance, potential issues and subscriber usage patterns. It collects counters from ContexNet™ (ConteXtream's Carrier-SDN solution) logs and IPFIX records and presents this data in the form of graphical reports that can be used for myriad applications, including performance analysis, insight into subscriber usage patterns, client types and network types, observing the detailed effect of optimization and troubleshooting.

It also consists of a TCP Anomaly Detection tool, which detects and alerts the network operator of possible TCP related issues that may be caused by the ContexNet TCP Bridge. The TCP Anomaly Detector analyzes these IPFIX records generated by ContexNet and identifies endpoints that continuously exhibit certain TCP behavior that can be an indication of an issue with the TCP Bridge. For each such endpoint, the TCP Anomaly Detector records and displays the IP address and port number, issues traps and can email the operator.





ContexView enables extensive performance monitoring (as shown in the graphs above) of both ContexNet and the mobile network, highlighting unexpected changes in network performance or functionality, showing the effect of configuration changes on the performance and viewing the impact of network equipment changes. ContexView eases troubleshooting, allowing the operator to isolate performance issues to device type, locate areas of network congestion, identify problematic end user devices, file types etc., analyze Media Optimization and Analytics issues or view CPU, memory and disk utilization trends.
ContexView collects data from ContexNet logs and IPFIX records and stores them in a database, which is used by the reporting system. It also provides an option of a central server that collects data from all the operator sites, allowing for a centralized view of the entire operator network.



Example: ContexView Deployment with ContexNet

Technical Specifications	
Features & Functions	
Data Collection	• ContexNet counters from logs • Performance counters from HTTP and TCP IPFIX records • Traffic: Rx, Tx, packets, bytes, latency, retransmissions • RADIUS and Pilot Packets: Total, 3G, 4G, port chunk allocation and de allocation • TCP Connection: Created, deleted, ignored • HTTP header enrichment: Successful, unsuccessful • Media optimization: Total, re-directed, un-optimized • Resources: CPU, memory, disk, memory packet pools • Database: Reads & writes • Steering Sessions: Registrations, Active, high rate subscriber • Subscriber Traffic: Average, Average high rate subscriber
Reporting	• Choice of any ContexView counter or IPFIX derived counter as data source • Individual source or sum, average, max, min over data sources • Data points at selectable intervals (sum, average, latest, min or max) • Time shifted graphs for comparison • Calculated / derived data • Line or area graphs with stacking option • Individual graphs or dashboard showing multiple graphs • Data export to XML and/or CSV files • Ability to segregate traffic by, download size, device type, operating system, browser, network type • Calculation of average download and upload data rates • Summary data, Example: - Every minute for 7 days - Average of every 20 minutes for 28 days • Average of every hour for 1 year
TCP Anomaly Detection	• Endpoints for which all optimized connections were terminated before establishment • Endpoints for which no optimized connections were ever terminated with FIN • Endpoints for which all optimized connections always had traffic only in one direction • Endpoints for which all optimized connections had less than a configurable amount of traffic
Operations	
Element & Network Management	• Command Line Interface for configuration & control • Graphical User Interface for alert and report displays • SNMP traps • Network Time Protocol (client) • Software installation, upgrade and rollback
Security	• Role based user access • User authentication and authorization using RADIUS/LDAP/TACACS+ • Local user authentication when external not available • Secure encrypted management access • Strong passwords • Multiple, role based access levels • Encryption of user information • Secure file transfer
Platforms, Performance and Scale	
Sample Hardware Platform	• HP C7000 BladeSystem with BL460 G6/G8 blade servers or equivalent • Intel x86 systems: Westmere, SandyBridge and IvyBridge • Required Memory: 48GB
Software Platform	• Linux CentOS 6.4
Performance and Capacity	• 300,000 IPFIX records per second • 200,000 TCP connections per second • 20 ContexNet Grid Servers and 2 Management Servers