SD-WAN
Security Analytics

Telesystem SD-WAN Security Analytics

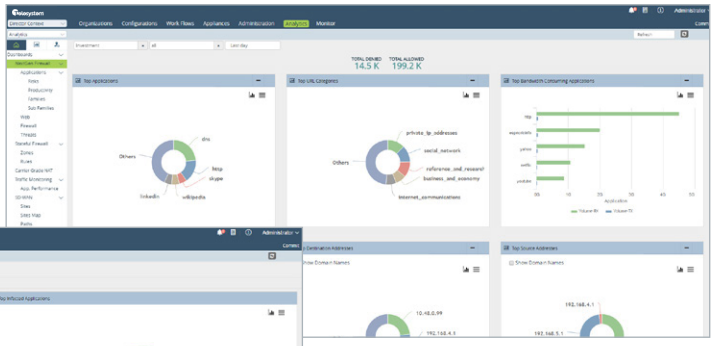
Networking is strategic to business. As per the latest industry data, through 2017 networks will see a 28% compound annual growth rate for bandwidth. While 50% of application deployments will suffer performance impact due to networking limitations. There will be a three-fold increase in security attacks year over year. Therefore, more important than ever, network visibility and control, predictability, adaptability and a feedback loop based on analytics data is a necessity for a trouble free and secure network. A strong analytics solution increases both the degree of seeing and the degree of timely action.

Telesystem Security Analytics is purpose-built for SD-WAN and managed services. It is a rich real-time big data solution that provides visibility and control, base-lining, correlation, prediction and feedback loop into VNFs. It provides real-time and historical search, reports on usage patterns, trends, security events, and alerts. SD-WAN Security Analytics analyzes huge amounts of data sent from VNFs to present critical data points as actionable analytics and reports. Tight native integration with Telesystem VNFs ensures optimized storage, search and performance.

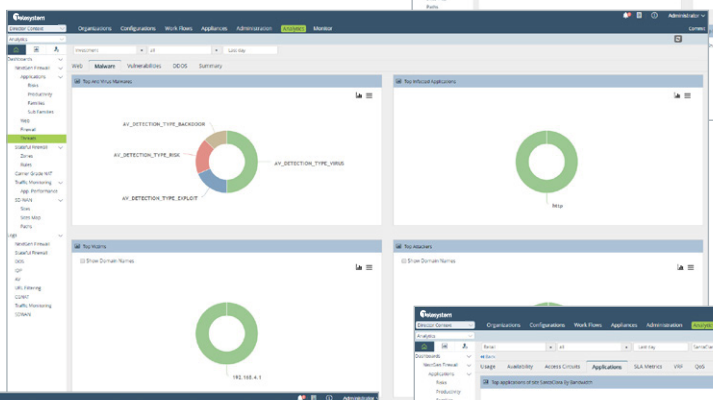
SD-WAN Security Analytics has built-in multi-tenancy that enables a single cluster to provide service for hundreds of customers, enabling deployment flexibility and economy of scale. It tightly integrates with our Director for complete role-based access control. It is operations-ready and supports standard protocols and log formats, such as Syslog and IPFIX, making it compatible with existing SIEM, monitoring, and reporting systems. SD-WAN Security Analytics is extensible and flexible via REST APIs.

It is also drastically less expensive compared to other third party solutions.

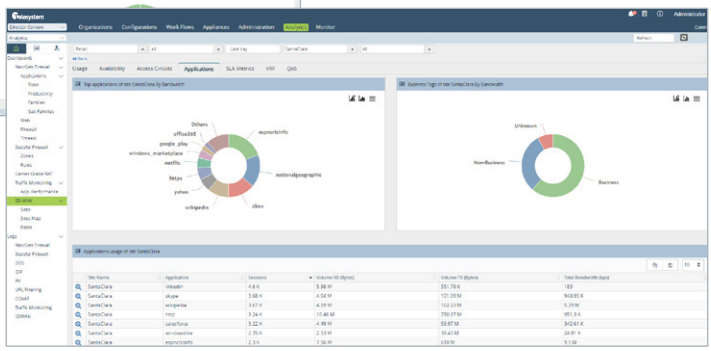
The result is carrier-grade, multi-tenant big data analysis for realizing the full value proposition of Telesystem software-defined solutions.



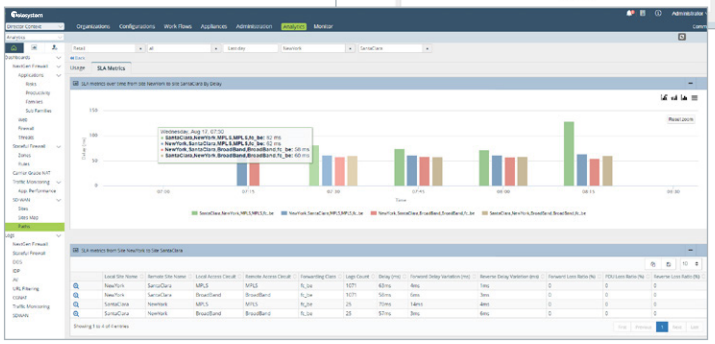
Analytics Dashboard



Threats Dashboard



Top Applications Usage (Site View)



SLA Metrics Dashboard

6.25.18

SD-WAN Security Analytics

Product Features

Data Logging Framework
Highly scalable, reliable, optimized, policy-driven data logging framework
Multiple transports
Multiple log formats – IPFIX, syslog
Streaming of logs to one or more 3rd party collectors
Reports & Analytics
Real & historical time series log event reporting for various VNFs
Traffic usage/protocol anomaly detection through trend lines and confidence band
Prediction-based on extrapolation of trending data
Ad-hoc and scheduled reports
Predefined and custom report templates
Report export formats: csv, pdf, xls, email notification
Search
Multi-column search with drilldown
Generic and custom queries
Correlation searches
Network Reports
Traffic reports per site: availability, bandwidth usage per access circuit, bandwidth usage per application, latency/loss, QoS per access circuit
Multi-site reports: connectivity, bandwidth usage and SLA metrics between sites
CGNAT reports: NAT events, pool utilization etc.

Security Reports
Firewall reports per tenant: top rules, zones, source, destination by IP/domain name/geo location, ports, protocols, session duration, QoS, DDoS and Flood detection
Application reports: top L7 applications by risk, productivity, family and sub-families based on sessions, volume and throughput
Web traffic reports: top web traffic by URL categories and reputation
Threat profile reports: URL filtering and captive portal actions, IDS/IPS, anti-virus, SSL certificate anomalies, etc.
Forensics: packet capture for known/unknown applications and detected vulnerabilities
Anomalies
Support of anomaly detection in traffic pattern/usage
Support for custom applications to detect anomalies and take actions (send traps, program policies, etc.)
GUI
Dashboard views for SD-WAN, security, vCPE functionality per tenant, per VNF
Visualization using charts, real-time views, maps, grids
Drilldown support to analyze data instantly for a given time range, detect trends and anomalies
Automatic data enrichment
Flexible reporting framework
Management
Role-based access control
REST APIs for Versa and 3rd party Apps
Historical log archival and cleanup

System Requirements

In production networks, we recommend using bare metal for running Telesystem SD-WAN Security Analytics functionality to get optimal scaling and performance.

Storage
512GB or more. SSD, SATA/SAS drives. SSD is recommended
Processor
2 socket server – 12 cores per socket, Intel Xeon 64bit processor
RAM
64GB-128GB

Operating System
Ubuntu 14.04
Web Browser
Chrome, Firefox

Document Resource: Versa Networks, Inc.