

Enterprise Network Surveillance Solution - Overview

Today's Internet based services rely upon ensuring that the end-to-end path from the source to the destination is secure and reliable. When services are affected, tracking root-cause (hacker, malicious user, sub-optimal configuration ...) in a complex environment is a laborious and challenging task. Traditional methods rely upon uncorrelated and coarse grained analysis of event data which is highly inefficient.

NIKSUN NetTrident is a real-time data-mining application that intelligently & hierarchically aggregates, correlates and analyzes packet, flow, Simple Network Management Protocol (SNMP), as well as other types of data from multiple sources and presents analyzed results to the end-user. NetTrident's intelligent analytics provides users with exponentially fast analysis of security or network information to determine root-cause on an enterprise wide scale or for user-defined logically aggregated domains. NetTrident provides users with tools to perform security forensics, as well as enterprise network & resource planning including trending, baselining and forecasting. Users can analyze complete bi-directional transaction information even from asymmetrically routed networks with multiple peering points.

Enterprise Network Security & Service Management

NIKSUN NetTrident collects, correlates, aggregates and analyzes information in real-time to provide a host of unique & powerful benefits:

- Enables rapid root-cause identification of security, application & network issues that span across different (physical) network links and/or locations
- Provides seamless analysis of issues in an asymmetrically routed network by virtual aggregation across locations and data sources
- Data correlation from the application down to the packet layer along a serial or parallel path
- Provides the ability to view in real-time multiple logically aggregated views of the same environment; i.e. physically by type of interface, building or logically by service, domain, region, etc.
- Enables cross-organizational and geographic-based network security monitoring, application and service analytics
- Provides data for benchmarking new applications and services for end-to-end security compliance while ensuring desired SLAs
- Enables enterprise-wide event aggregation, security breach detection and analysis
- Merges packet traces from multiple links

Enterprise-Wide Security Analytics

NetTrident enables true enterprise wide centralized intrusion/anomaly detection, enterprise level forensics for compliance, H/R & information asset protection, session reconstruction/replay for lawful intercept & asset protection.

Full Reconstruction of TCP Sessions and Applications

NetTrident supports reconstruction of all major applications, including application-level reconstruction of Web (HTTP), Email (SMTP/POP3/IMAP4), Telnet, FTP with embedded images, MIME attachments, and files transferred, Instant Messaging (Yahoo, MSN, AOL & ICQ), Voice & Video over IP, ASCII based transactions, HEX & much more. NetTrident also offers strong search capabilities, including string search inside

NIKSUN NetTrident

Enterprise Security & Performance Management

Enterprise Alerts

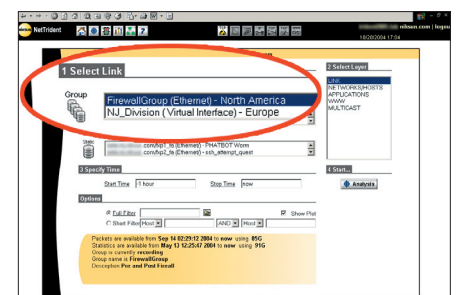
Real-time Forensics and Analytics

Compliance Monitoring and Surveillance

*An Integrated and Scalable Enterprise-wide Network Performance and Security Management Solution that increases **productivity** and **reduces overall costs***

Benefits

- Compliance Monitoring and Auditing
- Superior drill-down forensic analysis
- 100% visibility and real-time enterprise network monitoring
- Rapid root-cause identification of enterprise-wide applications, service and network issues
- Secure and easy-to-use web interface
- Extensive 3rd-party applications compatibility
- All capabilities integrated into a turnkey solution



Enterprise-wide analysis spanning geographies



encoded data for compliance, audit & interception applications. It enables session reassembly across multiple links even across many diverse physical locations to provide true application level analytics.

Enterprise-Wide Super Analyzer

NetTrident aggregates and analyzes actual packet traffic captured and warehoused in the NIKSUN appliances. NetTrident is an “enterprise-wide super analyzer” that troubleshoots elusive network or service performance and security problems in seconds. NetTrident makes trouble-shooting and root-cause analysis across a network a snap by simply allowing users to easily “rewind” back to the time of occurrence of an event, automatically correlating and aggregating relevant packet level data to identify the root-cause in a matter of seconds.

Real-time Proactive End-to-end SLM & QoS Monitoring

NetTrident correlates real-time alarms for proactive surveillance. It supports various type of alarms including NetSLM (service level management, quality of service monitoring), NetRTX (real-time experts), NetMulticast (multicast experts), etc. to provide:

- By virtually aggregating packet data from multiple locations, multiple hops/segments, NetTrident can do end-to-end performance, e.g., one way latency, application response time, round trip time, per-hop delay, loss & retransmission, etc.
- Enterprise wide application, service (including url) level analytics
- Switch / router monitoring & correlation including flow & MIB data
- Correlated event management and integrated drill-downs

Web Based Packet Viewer

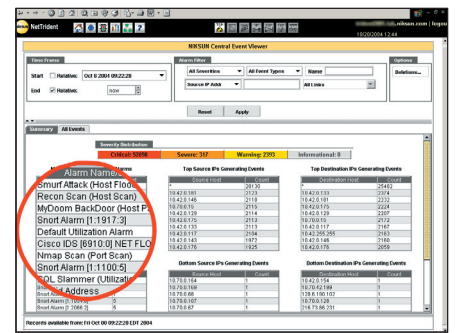
A correlated and decoded view of packet information from multiple physically distributed interfaces are virtually aggregated and displayed. The display includes the corresponding links of the packets. The highest level of application protocol decode is presented. The packet viewer supports over 700 protocol decodes. Since the decoding is performed on the appliance, there is no need to download packets over the network. The packet viewer also supports multi-language string search on the packets.

Xperts Analysis

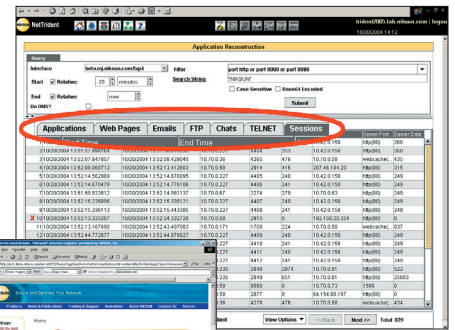
NetTrident includes the enterprise edition of NetXperts which allows users to discover performance and security related events across multiple distributed interfaces.

NetTrident Central Manager

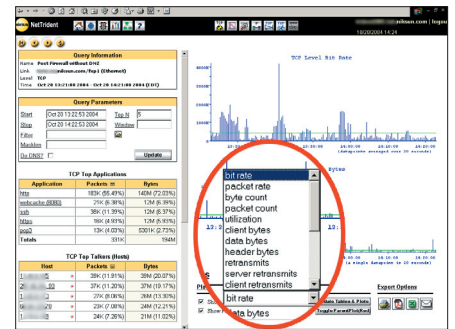
NetTrident Central Manager, an integrated lite version of NIKSUN Central Manager, manages NIKSUN appliances remotely. Services include appliance provisioning, configuration, health monitoring & configuration backup. Users can view & modify appliance/interface settings, backup appliance configuration/setup files at any interval, transfer files from local computers to any registered appliance or from one appliance to another. Appliance health and status information such as connection status, recorder status, used disk space & CPU utilization, etc. is also maintained.



Correlated Events



Application Reconstruction (sample web-page with header information)



Traffic Analysis Screen displaying statistics and plots



NIKSUN NetTrident appliance (2U Chassis)

NIKSUN, the NIKSUN logo, NetDetector, NetVCR are either registered trademarks or trademarks of NIKSUN, INC. in the United States and/or other countries. Other product & company names mentioned herein may be the trademarks of their respective owners. NIKSUN, INC. shall not be liable for damages of any kind for use of this information, which is subject to change without notice. Copyright© 2005 NIKSUN, INC. All rights reserved. NK-DS-TR06.1

