Configurable IP Platform for Network Analytics

NARUS presentation to SCAMPI

Georg Pöll/Andrew Cockburn

May, 2004
Carrier Class IP Platform for the largest, most profitable networks in the world

“Total Network View” decision making through the real time collection and analysis of one packet to billions of packets across multiple networks

Customers and Partners extend NARUS’ IP Platform with IP Application including Mediation, Security, and others
Narus Product Configuration - Technical View

Logic Server

Customer IP Apps

Rulesets

Virtual Analyzer

STA

Network 1

Network 2

Network 3

Proprietary and Confidential
Narus Traffic Aggregation and First Level Analysis

STA
Semantic Traffic Analyzer

- Network transparent collection and semantic analysis of traffic
- Captures detailed, protocol-specific data in addition to collecting standard data
- Interfaces directly to the network using Narus Semantic Traffic Analysis™ technology

VA
Virtual Analyzer

- Extracts information from network devices and service elements using standard protocols:
  - SNMP
  - Voice Mediated CDRs
  - CGF
  - LDAP
- Highly configurable with the Narus VA Toolkit
Captures detailed, protocol-specific data in addition to collecting standard data directly from the network using Narus’ Semantic Traffic Analysis™ technology.

- Extracts information directly off the wire
- Not a sniffer: session modeling and reconstruction
- Detailed visibility into user traffic
- Network transparent, non-intrusive

Vendor and protocol independent: IP standards based
Highly tuned appliance: 300-500Kbps
Network efficient: 95-99% data reduction
Network transparent collection and semantic analysis of traffic
Narus LogicServer
Rules Based Correlation and Analysis

Executes Narus RuleSets in real time
- RuleSets represent the desired business rules
- Event-driven, in-memory, data-flow engine
- High-performance, low-latency, on-the-fly analysis
Narus Developer’s Studio

- Flexible Aggregation and Filtering
  - Arbitrary keys and time intervals
  - Concentrator: multiple in, single out
  - Splitter: single in, multiple out
  - Boolean XOR, NAND, IOR
  - Relops =, !=, <, >, =>, =<, !<, !>
- Merging multiple instances as defined by arbitrary key values
  - Within single or multiple data streams
  - Same or different classes of data
- Categorization
  - Logical “Case” structure
  - Based on object attribute value, or function output
- Correlation
  - Create linkages between asynchronous data streams and other data sources
  - RADIUS, DHCP, LDAP, Database, DNS, Flat Files...

Create, modify, extend analysis to meet expanding needs and address new services

Filters and Filter Packages
Output window
Filters grouped to form RuleSets
Filter properties
NARUS Enabled IP Applications

- **Mediation**
  - Postpaid Billing
  - Prepaid Billing
  - Fraud

- **Security**
  - Information Assurance
  - Infrastructure Protection

- **OEM**
  - Business Intelligence
  - OEM Applications
  - Other

Customer IP Solution reference designs
Postpaid Billing

- Narus System configuration for billing for value-based data services
  - Facilitates rapid revenue capture
  - Speeds service deployment
  - Ensures proper ongoing billing plan management
  - Leverages existing infrastructure
    - Uses production 3rd party billing applications
    - Interfaces with any number of network elements

- Flexible information processing
  - Multiple billing plan variants
    - Total volume or volume per consumed application
    - Quantity of events
    - Detailed content usage
  - Enables rapid changes as user trends change
Prepaid Billing

- Narus System configuration to provide revenue assured prepaid data service
- Focuses on the customer experience
  - “Soft Landing” – subscriber redirection
  - Flexible enforcement mechanism
  - Ensures access to selected “free” sites, even with a zero balance
  - No impact on un-enforced quality of service
  - Immediately brings customer back to where they were enforced after exhausted balance is updated
- Enables single balance source for converged offerings
  - Voice and data
  - Prepaid and postpaid
Fraud

- Narus System configuration to detect and manage fraud
  - Designed for mobile networks
  - Captures usage data for delivery to a central database
    - Integrated with Business Support Systems
  - Analyzes IP traffic by content and categorizes the applications being used

- Key features
  - Information on customers’ service usage
  - Assistance with network optimization
  - Alarm generation as thresholds are reached
  - API to common reporting tools
IP Policy Management

- Narus system Configured for Real-time network analysis
  - Normalizes across large networks, carrier grade

- Determines usage patterns
  - Collects and categorizes network usage from Network to Application layers
  - Programmable event and policy management system
  - Programmable Full Packet Capture for forensic analysis
  - Visualization of activities, Real-time event notification and actions

- Enforces usage policies
  - Programmable policy management for enforcement
IP Infrastructure Protection

- Narus system configured for Real-time network analysis
  - Normalizes across large networks, carrier grade
- Determines anomalous traffic for ensuring continuous network throughput
  - Collects and categorizes network usage from Network to Application layers
  - Programmable threat detection, unauthorized use
  - Baselining of normal network activity, alerts for anomalies
  - Programmable FPC for Forensics analysis
  - Visualization of current historical activity, baselines and anomalies
- Enforcement
  - Supports mitigation techniques

Proprietary and Confidential
IP Platform for the largest, most Profitable Networks

- **Production Proven**
  - Tier-1 carrier-grade solutions suite
  - Installed worldwide in multiple configurations
  - Industry-leading mediation and security offerings

- **Flexible and Scalable**
  - Component and module approach allows flexible and scalable customer specific implementations
  - Standard ability to create and manage highly differentiated mediation and security services

- **High Performance**
  - Industry leading benchmarked performance, processing 10s of billions of events per day
  - Real-time IP data collection and interactive enforcement