Traffic Sentinel

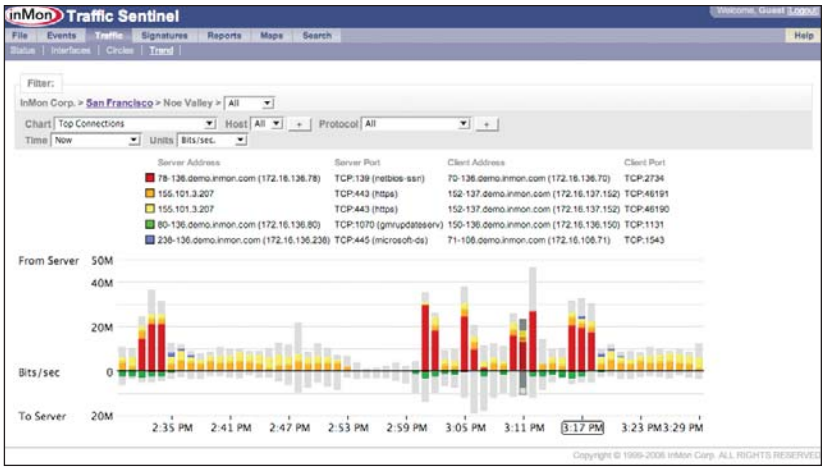
Complete Network Visibility and Control

Providing high performance and reliable network services is central to the success of today's organizations. As the business cost of network malfunctions continues to increase, rapid identification and mitigation of threats to network performance and reliability becomes critical. Such threats can include propagating worms, denial of service attacks, peer-peer activity, misuse of services, and data traffic interfering with real-time traffic. InMon Traffic Sentinel's network-wide surveillance of complex, multilayer, switched, and routed environments together with its unique combination of features is specifically designed to meet the challenge of pin-pointing and resolving any such threat.

- Enforce security policies
- Identify suspicious behavior
- Respond quickly to security threats
- Ensure quality of service
- Account for network usage
- Reduce network costs

At its core, Traffic Sentinel has a highly scalable traffic correlation engine capable of continuously monitoring tens of thousands of switch/router ports. Sophisticated statistical algorithms integrate traffic data and routing/switching data to build accurate and detailed picture of real-time and historical traffic flows across the whole network.

A network manager must continuously defend against external and internal security threats. A continuous onslaught of denial of service attacks, port scans, system infiltration, and unauthorized usage requires constant vigilance. Traffic Sentinel supports automated NBAD (Network Behavior Anomaly Detection) for identifying internet worms, compromised hosts, policy violations, and misuse of services. It also supports signature-based intrusion detection using Snort™ rules. Alarms are generated on detection of threats or suspicious activity. These alarms are supported by audit trail analysis and precise host location information so that hosts can be isolated rapidly.



In a converged network environment, performance of VoIP (Voice over IP) and other real-time streaming applications can be severely impacted by other network traffic. It is essential to control packet loss and jitter for such applications if adequate quality of service is to be maintained. Traffic Sentinel uses an innovative technique to measure the packet loss and jitter and provide assurance that quality of service metrics are being met.

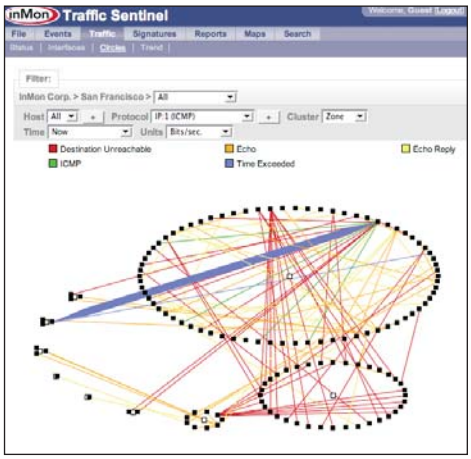
Charging for use of network services can be an effective method to encourage proper use as well as to recover the costs of providing value-added services. However, obtaining the detailed information required to charge users fairly for services can be challenging. Traffic Sentinel uses traffic data collected from switches and routers throughout the network to account for traffic by configurable groups or individuals.

Traffic Sentinel's intuitive, drill-down interface makes navigation through its detailed data simple. Real-time, overall network status can be seen at a glance, clicking on alerts brings up additional detail and guides you to the cause of the problem. Detailed historical traffic flow information is accessed by standard and customizable automatic reports.

Traffic Sentinel makes use of embedded instrumentation within switches and routers. The break-through technology, sFlow, provides the richest information, greatest scalability and is supported by a wide variety of vendors; however, Traffic Sentinel also accepts IPFIX and a number of proprietary monitoring technologies, including: Cisco NetFlow, HP Extended RMON and Riverstone LFAP. The use of embedded switch and router monitoring eliminates the need for probes, providing a cost effective way of providing detailed, network-wide coverage.

Traffic Sentinel

Key Features



- Network-wide thresholds and alarms
- Signature-based intrusion detection using Snort™ rules
- Automated NBAD (Network Behavior Anomaly Detection)
- Real-time top n visualization
- Historical audit trail analysis
- Host location
- Automated L2 and L3 topology discovery and mapping
- Detailed analysis of BGP (Border Gateway Protocol), including traffic by AS Path
- Customizable interactive and scheduled reporting
- Continuous monitoring and analysis of network traffic across tens of thousands of switch ports, even at 10Gb speeds
- Access to traffic data from any web browser or web-aware application
- Easy integration with other applications through open interface and web-based queries

Technical Specifications

Protocols Monitored

Full layer 2 - layer 7 analysis:

Ethernet/802.3/SNAP
IPv4/IPv6/ICMP/UDP/TCP
IPX
AppleTalk
DecNet4
BGP4 source, destination, peer, full AS path analysis
RTP jitter and loss

Layer 2 analysis:

Full duplex port statistics
Traffic priority by port
VLAN statistics

Standard reports

Event frequency SLA analysis
Compromised or infected host
Illicit server
Unauthorized network service access
Unauthorized wireless access points and routers
Traffic profiling and trending (host, protocol, link)
IP multicast sources, channels and trends
RTP delay and jitter
BGP AS Path analysis
Usage accounting

Data Sources

sFlow
IPFIX (over UDP)
Cisco NetFlow Versions 1, 5, 7 and 9 (non-aggregated)
Juniper j-flow (non-aggregated)
Riverstone LFAP
HP Extended-RMON
Monitors 40,000+ switch ports from a single server

System Requirements

Traffic Sentinel is a web-based application that runs on dedicated hardware under RedHat Enterprise Server or Fedora.

Typical small configuration (branch office)

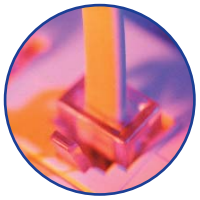
CPU	1 x Pentium III 1GHz
Memory	1GB
Disk	80GB IDE
Network	100Mbps

Typical medium configuration (small campus or data center)

CPU	2 x Pentium III 2GHz
Memory	1GB
Disk	80GB SCSI
Network	100Mbps

Typical large configuration (large campus, data center or Internet backbone)

CPU	4 x Pentium III 2GHz
Memory	2GB
Disk	200GB SCSI
Network	100Mbps



sFlow ENABLED

www.inmon.com

Tel: (415) 283-3260 • Fax: (415) 283-3360 • 580 California Street, 5th Floor, San Francisco, CA 94104